Kybernetická bezpečnost nemocničních zařízení

Bc. Tereza Krajíčková

Diplomová práce
2021

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení

Akademický rok: 2020/2021

ZADÁNÍ DIPLOMOVÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Tereza Krajíčková**
Osobní číslo:	**L19404**
Studijní program:	**N1032A020002 Bezpečnost společnosti**
Studijní obor:	**Rizikové inženýrství**
Forma studia:	**Prezenční**
Téma práce:	**Kybernetická bezpečnost nemocničních zařízení**

Zásady pro vypracování

1. Zpracujte rešerši vztahující se k dané problematice s důrazem na monografie.
2. Proveďte analýzu úrovně kybernetické bezpečnosti nemocničních zařízení.
3. Na základě předchozí analýzy navrhněte případná opatření ke zkvalitnění stávajícího stavu.
4. Sumarizujte získané výstupy diplomové práce.

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

Seznam doporučené literatury:

1. JOHNSON, Thomas A. *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*. 6000 Broken Sound Parkway NW, Suite 300: CRC Press Taylor & Francis Group, 2015. ISBN 978-1-4822-3923-2.
2. MCCARTHY, N. K. *The computer incident response planning handbook: executable plans for protecting information at risk*. New York: McGraw-Hill, 2012. ISBN 978-0-07-179039-0.
3. SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 9788073807658.

Další odborná literatura dle doporučení vedoucího diplomové práce.

Vedoucí diplomové práce: **Ing. Petr Svoboda, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání diplomové práce: **1. prosince 2020**
Termín odevzdání diplomové práce: **14. května 2021**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

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

V Uherském Hradišti dne 2. prosince 2020

PROHLÁŠENÍ AUTORA DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

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

Prohlašuji,

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

V Uherském Hradišti, dne: 7. 5. 2021

Jméno a příjmení studenta: Bc. Tereza Krajíčková

.....
podpis studenta

ABSTRAKT

Předkládaná diplomová práce se zabývá aktuální problematikou spočívající v kybernetické bezpečnosti nemocničních zařízení v České republice. Tato práce má primární rozdělení na teoretickou a praktickou část. Teoretická část shrnuje na základě zpracované literární rešerše základní a důležité poznatky pro komplexní pochopení řešené problematiky. Druhá část představuje analytickou část provedenou na základě vybraných metod. Ze všeho nejdřív se zaměřuje na samotný sběr informací pomocí řízených rozhovorů s vybranými odborníky na danou problematiku. Pro další zpracování sloužila Kvalitativní analýza rizik s využitím jejich souvztažností (KARS) a rizikový kalkulátor RISKAN. V souladu se zjištěnými výsledky z analýzy rizik bylo navrženo opatření a zpracován plán zvládání bezpečnostních incidentů. Tento plán je rozdělen na organizační a technická opatření. Vzhledem k rozsahu tématu je práce zaměřena pouze na vybraná opatření.

Klíčová slova: kybernetická bezpečnost, nemocniční zařízení, ransomware, spear-phishing

ABSTRACT

The presented master's thesis deals with current issues related to the cyber security of hospital facilities in the Czech Republic. This thesis has a primary division into theoretical and practical part. The theoretical part summarizes on the basis of the processed literature search basic and important knowledge for a comprehensive understanding of the problem. The second part presents the analytical part performed on the basis of selected methods. First of all, it focuses on the actual collection of information through guided interviews with selected experts on the issue. Qualitative risk analysis using their correlations (KARS) and the RISKAN risk calculator were used for further processing. In accordance with the results of the risk analysis, measures were proposed and a Security Incident Management Plan was prepared. This plan is divided into organizational and technical measures. Due to the scope of the topic, the work is focused only on selected measures.

Keywords: Cyber Security, Hospital Facilities, Ransomware, Spear-Phishing

Na tomto místě patří poděkování vedoucímu Ing. Petru Svobodovi, Ph.D. za jeho odborné vedení, poskytnutí podnětných a cenných rad, připomínek a doporučení k řešené problematice v této práci. Poděkování je dále věnováno odborníkům v oblasti informačních a komunikačních technologií vybraných nemocničních zařízení za zodpovězení otázek v řízeném rozhovoru. V neposlední řadě mé poděkování náleží zvláště rodině a taktéž přátelům za jejich značnou podporu při studiu a zpracování diplomové práce.

Motto:

„I malé zranění může způsobit velké následky.“

OBSAH

ÚVOD

V souvislosti s nedávnými útoky na nemocniční zařízení a nezbytným řešením kybernetické bezpečnosti považuje autorka vybrané téma za vysoce aktuální, které je z jejího pohledu nutno řešit kontinuálně a věnovat náležitou pozornost neustále vznikajícím rizikům v kyberprostoru. Přínos práce shledává v rozšíření povědomí kybernetické bezpečnosti, kdy na základě dodržování jistých bezpečnostních pravidel může dojít ke snížení rizika vzniku nežádoucích událostí a naopak zvýšení šance na lidský život či na jeho zdravotní stav.

Informační a komunikační technologie se bezpochyby staly součástí každodenního života. Vzrůstající riziko spojené s hrozbami v kybernetickém prostoru představují neustále se rozvíjející technologie, které kladou vysokou náročnost na jejich zabezpečení. Při běžném používání si samotný uživatel nemusí uvědomit důležitost kybernetické bezpečnosti, a tudíž neřeší otázku, jakým hrozbám je v kybernetickém prostoru vystaven. Respektive neřeší, dokud nenastane situace, na základě které ztratí všechna svá cenná data například v důsledku neopatrnosti a omylem tato data smaže, která navíc neopatřil zálohou.

Otázka kybernetické bezpečnosti právě v sektoru zdravotnictví hraje významnou roli v souvislosti se zdravím a životem pacientů. Základní zabezpečení, která fungovala dříve, ztrácí v důsledku času na účinnosti, a z toho důvodu by se do popředí a na vědomí měla dostat ta, která odpovídají danému systému či technologii. Právě z důvodu neustále se rozšiřujících a sofistikovanějších útoků vznikla celá řada bezpečnostních rámců souvisejících s kybernetickou bezpečností. Na základě nich pak byly postaveny právní předpisy a technické normy. V tomto případě stojí za zmínku zákon č. 181/2014 Sb., o kybernetické bezpečnosti, který vychází z rodiny norem ČSN ISO/IEC 2700x. Problém však mohou představovat samotní uživatelé, v tomto případě personál nemocnice, kdy odmítají zavedení nových bezpečnostních opatření v domnění, že jsou zbytečná a nic přeci nehrozí. Z tohoto důvodu je nezbytné neustále připomínat bezpečnost informací a jejich význam.

A právě zmíněný lidský faktor představuje ten pomyslný nejslabší článek v celém systému a stává se tak nejzranitelnější prvkem v oblasti kybernetické bezpečnosti. Na úrovni zajištění kybernetické bezpečnosti ve zdravotnickém sektoru nepřidává ani ta skutečnost, že je zde značný nedostatek potřebných odborníků na danou problematiku, ale i její nízké zabezpečení v podobě investic do IT v důsledku nedostatku financí.

CÍL PRÁCE A POUŽITÉ METODY

Hlavní cíl předkládané práce spočívá v analýze rizik kybernetické bezpečnosti nemocničních zařízení v České republice. Dílčím cílem práce je identifikace rizik, dále identifikaci aktiv a hrozeb. Další dílčím cílem je jejich hodnocení a v návaznosti na zjištěné informace navrhnutí vhodných opatření ke zlepšení stavu. Vzhledem k rozsahu tématu se práce omezuje na rozdělení návrhu na organizační a technická opatření.

Prvotní sběr informací byl proveden na základě řízeného rozhovoru s odborníky informačních a komunikačních technologií ve vybraných nemocnicích (které z bezpečnostních důvodů a uvedení citlivých údajů nebudou zveřejněny). Rozhovor byl proveden ve dvou nemocničních zařízeních, přičemž jedno z nich je fakultní nemocnice a druhá krajská. Jelikož obě nemocnice disponují více než 400 lůžky, spadají tak pod zákon o kybernetické bezpečnosti. Otázky k rozhovoru byly rozeslány předem, aby se vybrané subjekty mohly na tyto lépe připravit. Při samotném rozhovoru byly otázky v případě nejasností objasněny. Základ tohoto rozhovoru představoval zjištění stavu úrovně zabezpečení dat ve vybraných nemocničních zařízeních, kde informace takto získané sloužily pro další analýzu.

V rámci práce je použito několik základních vědeckých metod, které jsou založeny na určitém postupu. Především se jedná o analýzu, na základě které je postavena analýza rizik pomocí vybraných metod. Problematika byla řešena v kapitole Analýza rizik. V rámci této kapitoly byla vybrána Kvalitativní analýza rizik s využitím jejich souvztažností. Na analýzu navazuje syntéza, kde na základě provedené analýzy byly získány výsledky této práce. Jednotlivé části syntézy se skládaly ze sběru informací řízených rozhovorů vybraných subjektů. Pro sběr informací bylo využito metody indukce a dedukce. Především se jednalo o odborníky na informační a komunikační technologie. Poznatky z řízených rozhovorů byly aplikovány pro analýzu rizik ve vybrané metodě a dále v nástroji pro analýzu rizik. Na základě dedukce byly vyvozeny závěry z analýzy rizik. Následně po vyhodnocení uvedené metody a nástroje byly navrženy vhodná opatření ke zkvalitnění stavu. Využití metody komparace shrnuje především teoretická část, ve které jsou porovnávány za pomoci rešerše zdrojů dostupné literatury názory jednotlivých autorů na danou problematiku. Dále se jednalo o rozlišení pojmů phishing a spear-phishing především z důvodu jasného vymezení pojmu spear-phishing. Metoda byla využita při vyhodnocení analýzy rizik v softwaru RISKAN a Kvalitativní analýze rizik s využitím jejich souvztažností (dále jako „KARS“), kde byly porovnané jejich výstupy. Na základě provedených rozhovorů

ve dvou vybraných nemocničních zařízeních se prvky komparace vyskytují také u obsahu jednotlivých odpovědí. Tyto podobnosti či rozdíly jsou pak shrnuty v závěru.

V práci byla zvolena metoda KARS a dále multikriteriální hodnocení, které bylo provedeno pomocí softwaru RISKAN, kalkulátoru pro tvorbu analýzy rizik. Identifikace rizik pro zvolenou metodu KARS byla zhotovena na základě brainstormingu a metody What-If s odborníky na informační a komunikační technologie ve vybraných nemocničních zařízeních, kde tato identifikace byla podpořena zkušenostmi daných odborníků. V rámci identifikace aktiv a hrozeb v rizikovém kalkulátoru RISKAN byla stěžejním podkladem norma ČSN ISO/IEC 27005, příloha B. Detailnímu zpracování výše uvedené metody a nástroje pro analýzu rizik se zabývá praktická část. Tato kapitola má za cíl pouze seznámit čtenáře s aplikovanými metodami.

I. TEORETICKÁ ČÁST

1 INFORMAČNÍ A KOMUNIKAČNÍ TECHNOLOGIE

V současnosti ovlivňují informační a komunikační technologie (dále jako „ICT“) všechny aspekty každodenního lidského života. Nejedná se tedy pouze o samotné hardwarové prvky (dále jako „HW“), kterými jsou fyzické součásti systému: počítače, periferní zařízení apod., ale také o softwarové vybavení (dále jako „SW“) představující například operační systém. Ve Výkladovém slovníku kybernetické bezpečnosti (2015, s. 55) se nachází pojem definovaný následovně: *„Informační a komunikační technologií se rozumí veškerá technika, která se zabývá zpracováním a přenosem informací, tj. zejména výpočetní a komunikační technika a její programové vybavení.“* Pojem ICT obecně zahrnuje technologie, systémy a procesy podílející se na zobrazení, zpracování, uchování a přenosu informací a dat digitální formou (Smejkal, 2015).

Jak již bylo uvedeno v úvodu, ICT jsou součástí všech aspektů všedního života, které nám poskytují rychlejší a novější způsoby interakce, vytváření sítí, komunikace napříč kontinenty (například: pomocí sociálních sítí, mobilních telefonů) a mimo jiné poskytují přístup k nepřebernému množství informací v jakékoli oblasti zájmu. Jedná se o oblast rozvíjející se nejdynamičtěji, a proto by v tomto ohledu měla směřovat pozornost k bezpečnosti a edukaci uživatelů (Kolouch a Bašta, 2019).

Podobně, jako například ve výrobě, jsou ICT v odvětví zdravotnictví stejně tak důležité a představují mnoho zařízení, které ovlivňují péči o pacienty, veřejné zdraví, provozní náklady a tradiční byrokracii spojenou s lékařskou profesí. Elektronické zdravotní záznamy umožňují pracovníkům ve zdravotnických zařízeních vkládat údaje o pacientech do centrálního digitalizovaného systému, který je přístupný příslušným zainteresovaným stranám. Systémy lze integrovat se zásadami ověřování a zabezpečení uživatelů, aby umožnily pacientům přístup k jejich zdravotním informacím. Mobilní zařízení a přenos videa jsou ústředním bodem poskytování tzv. „telemedicíny“, kdy je odborníkům umožněno provádět oboustranné videokonference s pacienty nebo odborníky, a dokonce provádět chirurgický zákrok během tohoto hovoru (Brown, 2020).

Prvky ICT představují určitou pomocnou ruku v dnešním světě, kdy potřebujeme být neustále online a být v obraze o aktuálním dění ve světě, šetří nám čas, práci, ale i peníze. Bezpochyby jsou IT důležitým stavebním prvkem ve zdravotnictví v souvislosti zefektivnění poskytování zdravotní péče (Informační technologie a jejich využití ve zdravotnictví, 2020).

1.1 Informační systém

K ICT se bezpochyby pojí i informační systém (dále jako „IS“), kterým se rozumí zařízení nebo skupina vzájemně propojených nebo souvisejících zařízení (Kolouch a Bašta, 2019). Jedná se o soubor technických prostředků (HW a SW), lidské složky a organizačního zajištění udržující a poskytující data (informace) pro požadovaný účel jeho uživatelů – lidí (Informační systém (Information System), 2020).

Informačním systémem se rozumí systém, jehož prvky jsou ICT, data a lidé. Cílem informačního systému je efektivní podpora informačních a rozhodovacích procesů na všech úrovních řízení organizace. Jednoduše řečeno se IS skládá z výše uvedených komponent, které zajišťují sběr, zpracování, ukládání, vyhledávání a šíření informací (Smejkal, 2015).

- **Informační systémy ve zdravotnictví**

Nemocniční informační systém (dále jako „NIS“) by měl být základním kamenem pro každou správně fungující nemocnici, jak uvádí Šuráň (2015). NIS má zajistit podklady k léčbě, urychlit práci, spolehlivost a rychlost, zkvalitnění a zajištění správnosti vykazování zdravotní pojišťovně. Je třeba dbát na zabezpečení a přístupová opatření z důvodu ochrany osobních údajů, aby mohl personál zaznamenávat informace o stavu hospitalizace pacienta.

Zdravotnický informační systém je úložiště, které obsahuje osobní zdravotní informace pacienta. Jedná se o informace o identifikovatelné osobě (viz *Tab. 3*), které se vztahují na jeho fyzické a duševní zdraví nebo na poskytování zdravotních služeb (Šuráň, 2015).

1.1.1 Hardware

Pojem hardware představuje souhrn fyzických technických prostředků, které umožňují nebo rozšiřují provozování počítačového systému a zajišťují funkci zpracování informací. Je to počítač sám o sobě. Za HW lze považovat i to, co není jednoduše SW vybavením. Dělí se na dvě skupiny: vnitřní vybavení počítače a periferie. Kde vnitřní vybavení počítače představují zejména součásti, bez kterých by činnost počítače nebyla možná. Základní deska, paměť, procesor, napájecí zdroj jsou nezbytnými prvky pro funkci počítače. Mezi standardní vnitřní vybavení dále považujeme například grafickou kartu, paměťová média (CD, DVD, čtečky karet, …) a síťové komponenty. Periferie představují pouze doplňující funkci a nejsou tak nezbytně nutné pro funkci počítače. Jsou to ty, kterými se samotný PC (HW) ovládá, tedy externě připojená zařízení pomocí kabelů, Bluetooth, Wi-Fi aj. Jedná se o klávesnici, myš, externí paměťová zařízení, tiskárna atd. (Kolouch, 2016).

1.1.2 Software

Dle Koloucha (2016) představuje software veškerá programová či netechnická vybavení, která jsou nutná k provozu počítačů. Jedná se především o základní/vstupní systémy (BIOS), operační systémy (Microsoft Windows, Linux) a grafická rozhraní. Dle Slovníku (2015, s. 107) můžeme software rozdělit: *„a) systémový software – vstupně/výstupní systémy, operační systémy nebo grafické operační systémy; b) aplikační software – aplikace, jednoduché utility (program vykonávající jisté pomocné činnosti) nebo komplexní programové systémy; c) firmware – ovládací program hardwaru.“*

1.1.3 Data a informace (dataware)

Data představují veškeré grafy, čísla, mapy, transakce a jsou základním kamenem (surovinou, materiálem) pro následné zpracování a utvoření informace, které jsou pak užitečné pro příjemce. Prvky zpracovávané počítačem, uchovávané v ucelených souborech různého tipu – textové, obrazové (Kolouch, 2016).

Informace jsou tedy ty údaje, které byly zpracovány do užitečné podoby pochopitelné pro příjemce (uživatele). Lze je považovat za něco, co pro příjemce představuje rozšíření, ověření či zdokonalení jeho znalostí (Kolouch, 2016).

1.1.4 Lidská složka (peopleware)

V prostředí IS se jedná o adaptaci a efektivní fungování člověka v něm, znalosti, motivace, kompetence zaměstnanců. Představuje toho, kdo bude uživatelem jednotlivých služeb (Hronek, 2007), (Smejkal, 2015).

1.1.5 Organizační prostředky (orgware)

Souvisí s nařízením a pravidly, která definují provozování a řízení IS, dále pokyny pro obsluhu, návody k obsluze, provozní pokyny, zodpovědnost za správnost vkládaných dat, pokyny k archivaci dat, pořizování bezpečnostních kopií apod. (Hronek, 2007).

2 KYBERNETICKÁ BEZPEČNOST

Kybernetická bezpečnost (dále jen „KB“) je odvětví výpočetní techniky, které se uplatňuje jak u počítačů, tak i u sítí. Jak uvádí Kolouch a Bašta (2019) může být vymezení pojmu KB do určité míry problematické, neboť tato oblast je chápána řadou lidí odlišně. Jejich představu o pojmu KB tvoří myšlenka, že se jedná o oblast, kterou se zabývají především oddělení ICT. Tento předpoklad je ovšem chybný, neboť se KB týká všech, kteří využívají jakékoliv prvky ICT. Jestliže se nebude brát zřetel na stěžejní prvek KB, kterými jsou lidé, rapidně se tak může zvýšit riziko kybernetických útoků na ICT, a to právě v důsledku selhání zmíněného lidského faktoru jakožto nejslabšího článku v kyberprostoru. Johnson (2015) popisuje KB jako opatření určené k ochraně informačních systémů – včetně technologií (zařízení, sítě a SW), informací a pracovníků.

Od bezpečnosti informačních systémů se KB liší prostředím, kde jsou data zpracována a kde se přinejmenším mohou odehrávat útoky zaměřené na tento IS a ICT či jejich části (Smejkal, Sokol a Kodl, 2019).

Termín KB trpí absencí všeobecně uznávanou definicí a v současnosti není ani žádnou normou definován. Definici neobsahuje ani zákon č. 181/2014 Sb., o kybernetické bezpečnosti, ve kterém jsou vymezeny pouze ty pojmy, které se KB týkají (například: kybernetický prostor, kritická informační infrastruktura apod.). Avšak tento pojem můžeme shledat ve Výkladovém slovníku kybernetické bezpečnosti, kde je popsán následovně jako: *„Souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru“* (Jirásek, Novák a Požár, 2015, s. 69).

Jak uvádí Johnson (2015) lze kyberprostor definovat jako prostor, ze kterého informace kolují z jednoho média na druhé, kde jsou zpracovány, duplikovány a uloženy. Prostor, kde nástroje komunikují a tento prostor sestává tedy z komunikace systémů, počítačů a sítí.

Kvůli nejednotnosti definic představuje jeden z autorů vlastní formulaci na základě analýzy těch předchozích: *„Schopnost počítačových systémů a využívaných služeb reagovat na kybernetické hrozby či útoky a jejich následky, jakož i plánování obnovy funkčnosti počítačových systémů a služeb s nimi spojených“* (Kolouch a Bašta, 2019, s. 45).

Kybernetická bezpečnost je pro mnoho organizací, ale i jednotlivců, rozhodující, a to z toho důvodu, že ji nelze nijak zlehčovat či podceňovat, by měla být tato problematika řešena systematicky a dlouhodobě (Kolouch a Bašta, 2019).

2.1 Terminologická východiska

Pro porozumění kontextu jednotlivých pojmů, vyskytujících se napříč práce, obsahuje tato část jejich určení a následnou formulaci. Vzhledem k rozsahu práce není tento výčet kompletní, avšak dostačující pro potřeby z hlediska řešené problematiky. Pojmy pochází především z oblasti informačních a komunikačních technologií, které vycházejí z Výkladového slovníku kybernetické bezpečnosti (Jirásek, Novák a Požár, 2015) a některé z nich doplňuje publikace CyberSecurity (Kolouch a Bašta, 2019).

- **Aktivum –** všechno, co má danou hodnotu pro uživatele, organizaci či stát. Může být hmotné – člověk, budova, počítače apod. a nehmotné – data, programy apod. (Kolouch a Bašta, 2019).
- **Analýza hrozeb –** zkoumání činností a událostí, které mohou negativně ovlivnit kvalitu a služby informačních technologií (systém přenosu a zpracování dat).
- **Analýza rizik** – proces pochopení povahy rizika a stanovení jeho úrovně.
- **Bezpečnost dat –** bezpečnost aplikovaná na data, kde je zahrnuto řízení přístupů, definování politik a procesů a zajištění integrity dat.
- **Bezpečnostní incident –** bezprostřední hrozba porušení bezpečnostních politik, zásad nebo standardních bezpečnostních pravidel provozu ICT. Podle Koloucha a Bašty (2019) pak bezpečnostní incident představuje skutečné narušení bezpečnosti informací v infomačních systémech s nepříznivým účinkem (spuštění škodlivého kódu).
- **Bezpečnostní událost –** způsobí nebo vede k narušení informačních systémů, technologií a pravidel definovaných k jeho ochraně. Např. doručení e-mailu s přílohou obsahující škodlivý malware, který nelze bez dalších kroků nainstalovat (Kolouch a Bašta, 2019).
- **Bezpečnost informací** – problematiku vystihuje tzv. triáda CIA (viz níže – Triáda CIA), která se zaměřuje na to, aby byly zajištěny tyto tři atributy bezpečnosti informací: důvěrnost (Confidentality), integrita (Integrity) a dostupnost (Availability). Definice ze Slovníku zní: *„Zachování (ochrana) důvěrnosti, integrity a dostupnosti informací“* (Jirásek, Novák a Požár, 2015, s. 23).
- **Botnet –** síť infikovaných počítačů ovládaných jediným crackrem. Umožňuje provádět kybernetické útoky ve velkém rozsahu (zejména DDoS a distribuce viru).

- **Citlivá data –** taková data mající význam pro danou organizaci, kde při vyzrazení, zneužití, neautorizované změně či nedostupností vznikne organizaci škoda a nemůže řádně vykonávat svou činnost.
- **Cracker –** jednotlivec, který se snaží získat (prolomit) neoprávněný přístup k počítačovému systému. Činnost provádí za pomocí sofistikovaných činností. Tento význam bývá mylně zaměňován s pojmem **hacker**, kdy diferenciace těchto osob spočívá v jejich zájmu na informačním systému. Hacker se zabývá studiem programování systému a dále tyto znalosti neustále prohlubuje.
- **Dostupnost dat** – přístup a použitelnost informací na žádost oprávněné osoby (entity).
- **Důvěrnost dat –** vlastnost, že informace není dostupná pro neautorizované jednotlivce či entity.
- **Hrozba** – jedná se o případnou příčinu nechtěného výsledku, který představuje výsledek možného poškození aktiva.
- **Integrita dat –** jistota neprovedení změny, označuje platnost, konzistenci a přesnost dat.
- **Kritická infrastruktura –** systémy a služby, kdy by v případě jejich nefunkčnosti nebo špatné funkčnosti představovala závažný dopad na bezpečnost, ekonomiku a veřejnou správu státu.
- **Kritická informační infrastruktura –** nefunkčnost informačních systémů by měla závažný dopad na bezpečnost státu, ekonomiku, veřejnou správu a zabezpečení základních životních potřeb obyvatelstva.
- **Kybernetická bezpečnost –** soubor právních, organizačních, technických a vzděláváních opatření zajišťujících ochranu KB a všech jejích součástí před neoprávněným přístupem či útokem.
- **Kybernetický prostor –** digitální prostředí umožňující vznik, zpracování a výměnu informací, které jsou tvořeny IS.
- **Kybernetický útok –** jedná se o útok na IT infrastrukturu s cílem způsobit poškození a získání citlivých či jinak strategicky důležitých dat.

- **Malware –** obecně název pro škodlivé programy (kódy), mezi které patří trojské koně, počítačové viry, červy, špionážní software apod.
- **Ransomware –** škodlivý program, který zašifruje data a nabízí dešifrování po zaplacení výkupného.
- **Riziko –** pojem bezprostředně souvisí s některými pojmy již zde definovanými. Jedná se o pravděpodobnost vzniku nežádoucího specifického účinku, který nastane během určité doby nebo za určitých okolností (Richter, 2018). Výkladový slovník kybernetické bezpečnosti definuje riziko následovně: *„(1) Nebezpečí, možnost škody, ztráty, nezdaru. (2) Účinek nejistoty na dosažení cílů. (3) Možnost, že určitá hrozba využije zranitelnosti aktiva nebo skupiny aktiv a způsobí organizaci škodu“* (Jirásek, Novák a Požár, 2015, s. 99). Z hlediska ICT to je možnost, že daná hrozba využije zranitelnosti aktiva (tedy informačního a komunikačního systému kritické informační infrastruktury) a způsobí tak jeho škodu (Česko, 2018).
- **Spear-phishing –** šíření podvodné zprávy prostřednictvím emailové komunikace. Rozdíl od phishingu je takový, že tento je cílený přímo na konkrétní organizace/osoby (více viz podkapitola Spear-phishing).
- **Zranitelnost –** využití slabého místa aktiva hrozbou, které je způsobeno v důsledku jednání lidského či technologického faktoru (Kolouch a Bašta, 2019).

2.2 Principy kybernetické bezpečnosti

Tato část je věnována principům, které jsou implementovány při uplatňování kybernetické bezpečnosti. Jedná se o následující tři triády:

1) **CIA** (Confidentality – důvěrnost, Integrity – celistvost, Availability – dostupnost).
2) **Prvky KB** (lidé, technologie, procesy).
3) **Životní cyklus KB** (prevence, detekce, reakce).

Tyto tři základní principy (triády) kybernetické bezpečnosti můžou předcházet negativním událostem, avšak za předpokladu respektování jednotlivci a organizacemi (Kolouch a Bašta, 2019).

Spojení těchto tří kategorií pak v rámci kybernetické bezpečnosti představuje efektivní využívání lidí, procesů a technologií k prevenci, detekci a reakci na kybernetické útoky

či jiné hrozby, které stojí za narušením triády CIA, tedy důvěrnosti, integrity nebo dostupnosti informací či dat v daném systému (Pačka, 2019).

2.2.1 Triáda CIA

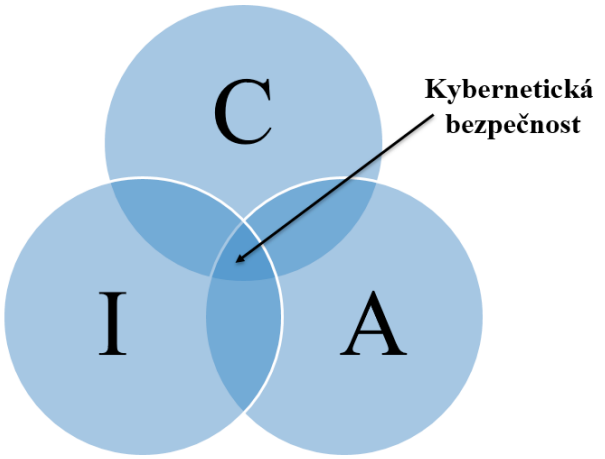
Jedná se o nejznámější a nejpoužívanější triádu KB. Kybernetická bezpečnost se týká jak ICT jako takových, ale i dat a informací, které jsou těmito prvky přenášeny, zpracovávány a uchovány (Kolouch a Bašta, 2019).

V současné době k udržení odpovídající úrovně KB se využití základních principů triády považuje za nedostatečné. Aby byla úroveň KB na adekvátní úrovni, je třeba přidat další atributy. Parkerian Hexad je sadou šesti prvků informační bezpečnosti, který tři klasické bezpečnostní atributy triády CIA (důvěrnost – Confidentality; integrita – Integrity; dostupnost – Availability) doplňuje o další tři, kterými jsou: držení a kontrola – Possesion or Control; pravost – Autenticity; užitečnost – Utility (Marks, 2019).

Níže jsou uvedeny a popsány ty tři základní z nich:

1) **Důvěrnost (Confidentality)** – k informacím, datům, či ICT jsou zpřístupněny pouze autorizovaným (oprávněným) subjektům.
2) **Integrita (Integrity)** – je znakem přesnosti a úplnosti. Integrita dat znamená jistotu, že data nebyla změněna. Tato nezměněnost systému značí vlastnost, že je vykonávána zamýšlená činnost bez jejího přerušování bez záměrné nebo náhodné manipulace se systémem.
3) **Dostupnost (Availability)** – garance možnosti přístupu k informacím, datům nebo počítačovému systému, kdy je to potřeba. Svým způsobem jde o vlastnost přístupnosti a použitelnosti na zažádání u oprávněné entity (Kolouch a Bašta, 2019).

Často se tato triáda vztahuje právě k informacím, což vyplývá z definice bezpečnosti informací zabývající se právě jejich ochranou: *„Zachování (ochrana) důvěrnosti, integrity a dostupnosti informací“* (Jirásek, Novák a Požár, 2015, s. 23). Tato bezpečnost je pak aplikovatelná na informace po celý jejich životní cyklus, a proto není podstatný nosič těchto informací (papír či elektronika) či v jakém systému jsou zpracovávány (Kolouch a Bašta, 2019). Dále Kolouch (2019) uvádí, že pro *informační bezpečnost*, v souvislosti s využíváním ICT, je vhodnější pojem *kybernetická bezpečnost*.



Obr. 1 – Triáda CIA a kybernetická bezpečnost.
Zdroj: (Kolouch a Bašta, 2019).

2.2.2 Prvky kybernetické bezpečnosti

Dalším a posledním principem této kategorie jsou prvky kybernetické bezpečnosti. Vzájemná interakce těchto prvků umožňuje do značné míry vytvořit či nastolit KB. Jakýkoli systém je bezpečný tak, jak bezpečný je jeho nejslabší článek (prvek). Těmito prvky jsou:

1) **Lidé** – představují nejslabší článek v bezpečnostním řetězci a nese zodpovědnost za selhání bezpečnostních systémů. Interakce lidí s kybernetickou bezpečností je možné považovat za tvůrce této bezpečnosti, jelikož se snaží prosadit a implementovat prvky KB ve vztahu k sobě či organizaci. Subjekty, které je třeba chránit před kybernetickými útoky a neustále proškolovat o pravidlech a principech KB a zejména představují riziko či hrozbu v oblasti KB. Představují nejslabší článek z několika důvodů, kdy jedním z nich může být krátká doba využívání moderních technologií. Další důvod nese otázku z hlediska bezpečnosti těchto SW, které se neustále dynamičtěji vyvíjejí, což představuje mnohdy pro řadu uživatelů nemožnost se těmito otázkami zabývat. Poslední důvod nese tu skutečnost, že život bez ICT se stává již nemyslitelným, respektive nemožným, a právě tím, že ICT a aplikace s nimi spojenými nesou daleko více informací, než kolik si je člověk schopný zapamatovat, se právě lidé stávají cílených obětí kybernetických útoků (Kolouch a Bašta, 2019).

2) **Technologie** – je rozuměn nějaký prostředek (PC, tablet, mobilní telefon), kterým jsme schopni připojit se k Internetu, sociálním sítím a dalším podobným softwarovým vybavením (aplikacím). Aby byla zajištěna KB těchto technologií,

je potřeba tyto udržovat ve stavu schopném reagovat na změny, zejména by měly být technologie udržovány pravidelně aktualizované (Kolouch a Bašta, 2019).

3) **Procesy** – jedná se o činnosti, díky kterým je umožněno lidem používat technologie a s nimi spojené služby. Těmito procesy jsou: řízení aktiv a rizik, autorizace a autentizace, audit KB, reakce na kybernetické útoky či jiné incidenty, školení apod. (Kolouch a Bašta, 2019).

2.2.3 Životní cyklus kybernetické bezpečnosti

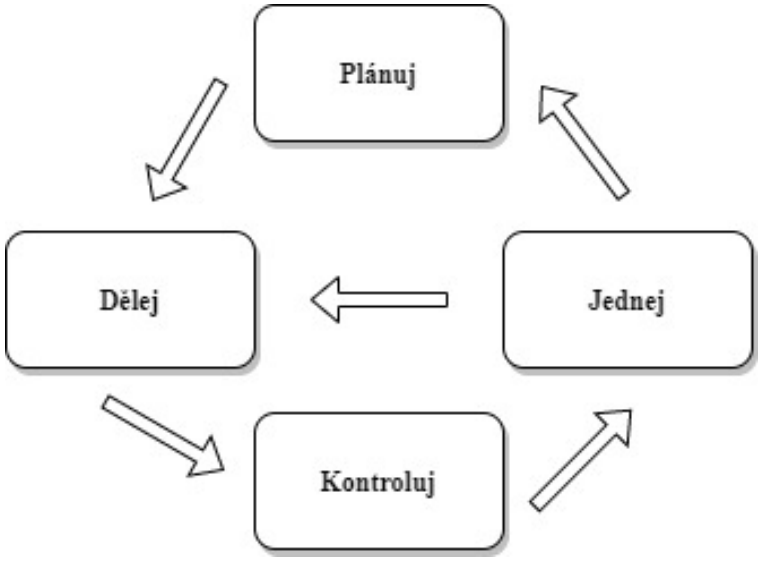
Při realizaci KB je třeba z hlediska času uplatňovat jak triádu CIA, tak jednotlivé prvky (lidé, technologie, procesy) během jejich celého životního cyklu. Především se jedná o prevenci, detekci a reakci na útok. Při řešení KB neexistuje nějaký záchytný bod, kdy by se dalo stanovit, že byla zvládnuta situace ochrany před kybernetickými útoky či hrozbami. Jedná se o nikdy nekončící proces analýzy rizik doplněnou o další podpůrné procesy, které pomáhají zvýšit KB v organizaci. Jde především o identifikaci, analýzu, realizace opatření, monitoring a kontrolu (Kolouch a Bašta, 2019).

Vzhledem k tomu, že neexistuje jednotná univerzální bezpečnost a jedno opatření aplikovatelné na všechny, závisí na koncových uživatelích, tedy nás samotných, pochopení těchto principů KB, kdy si tyto upravíme dle svých potřeb a zejména jejich respektování (Kolouch a Bašta, 2019).

2.3 Systém řízení bezpečnosti informací

Systém řízení bezpečnosti informací, z angl. Information Security Management System (dále jako „ISMS“), je systém řízení a správy informačních aktiv organizace. Za cíl si klade minimalizovat či eliminovat hrozby způsobující ztrátu či poškození těchto aktiv. Zakládá se na modelu PDCA (Plan - Do - Check - Act) aplikovaný na procesy ISMS v ČSN ISO/IEC 27001 – Systém řízení bezpečnosti informací – Požadavky (Smejkal, Sokol a Kodl, 2019).

Model PDCA, známý taky jako Demingův cyklus, je jedním ze základních principů, které spočívají v postupném zlepšování kvality procesů, služeb, dat, a to z důvodu opakovatelnosti jeho činností, které jsou uvedeny níže na obrázku (Kolouch a Bašta, 2019).



Obr. 2 – Princip Demingova modelu PDCA. Zdroj: (Doucek, Konečný a Novák, 2019).

2.4 Stav kybernetické bezpečnosti v České republice

Ze všeho nejdřív je třeba zmínit právní předpisy, kterými je ohraničena KB. Vymezení samotného zákonu a vyhlášky o kybernetické bezpečnosti je věnována celá kapitola uvedená níže. Kybernetickou bezpečnost chápeme jako součást celkové bezpečnosti. Dne 13. srpna 2014 byl podepsán prezidentem České republiky (dále jako „ČR“) Milošem Zemanem zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů a následně publikován ve Sbírce zákonů (Čapek et al., 2015). S tímto zákonem souvisejí další právní předpisy, kterým je věnována další kapitola.

- **Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2019**

V roce 2019 byla provedena pomocí spear-phishingového útoku kybernetická špionáž proti strategické instituci české státní správy, kterou zaznamenal NÚKIB s jeho partnery. Dále se jednalo o zvýšený počet útoků na instituce a organizace. Zpráva také odhaduje další problém týkající se nedostatku expertů (zejména ve zdravotnictví) a podfinancování oblasti kybernetické bezpečnosti. Zpráva (2020) je výsledkem řady institucí v oblasti KB. Díky široké spolupráci, podpoře a úsilí všech subjektů ve prospěch bezpečného kyberprostoru je ČR schopna čelit kybernetickým hrozbám.

- **Národní strategie kybernetické bezpečnosti České republiky 2021–2025**

Národní strategie KB České republiky byla schválena dne 30. listopadu 2020. Vzhledem k neustálému nárůstu nových kybernetických hrozeb, k technologickému vývoji a taktéž

stále větší závislosti na ICT, dosahují kybernetické hrozby značné úrovně. Hrozby tak mohou ve svém důsledku narušit stabilitu společnosti a demokratické uspořádání státu, a právě proto je aktuálním bezpečnostním hrozbám ve strategii věnována samostatná kapitola. Strategie je založená na vizi odolné společnosti a infrastruktury ČR sebevědomé vystupování v kyberprostoru a aktivní čelení celému spektru kybernetických hrozeb za pomoci spolehlivých spojenectví. Stanovuje tři základní pilíře: **Sebevědomě v kyberprostoru**, **Silná a spolehlivá spojenectví** a **Odolná společnost**, kdy společně tvoří základ budoucí KB ČR. Je nezbytné, aby byl stát schopen na vývoj bezpečnostního prostředí správně a včas reagovat a umožnil včas a správně identifikovat a vyhodnocovat rizika v něm (NÚKIB, 2020, a).

2.5 Kybernetická bezpečnost v nemocnicích

Za poslední dobu se nemocniční zařízení potýkala s vyděračskými kybernetickými útoky, které měly za cíl získat citlivá data pacientů. Představují rostoucí hrozbou pro oblast zdravotní péče obecně, zejména pro nemocnice. Zdravotnický průmysl zaostával v ochraně svých pacientů za ostatními průmyslovými odvětvími, kdy nemocnice musejí investovat značné prostředky do ochrany svých systémů. Kybernetické incidenty pak představují narušení citlivých údajů, což představuje hrozbu pro zdravotní sektor vzhledem k tomu, že se jedná nejen o útoky na zdravotnická zařízení, ale i o poškození dobrého jména (Jalali a Kaiser, 2018).

Podle Kačice, bezpečnostního experta (2020), je potřeba si uvědomit, že i nejlépe zabezpečený systém má jeden nejslabší článek (lidský faktor). Dalším problém představují finance, kde podpora ze strany státu není čerpána efektivně. Nemocnice jsou zranitelná, což bezpochyby ukazuje na potřebu komplexního zabezpečení (Healthcare And Hospital Security, 2020).

3 PRÁVNÍ VÝCHODISKA KYBERNETICKÉ BEZPEČNOSTI

V této kapitole jsou uvedeny právní předpisy týkající se kybernetické bezpečnosti, bezpečnosti, zdravotnictví a ochrany osobních údajů.

3.1 Zákon o kybernetické bezpečnosti a související předpisy

Tato podkapitola je věnována základním a souvisejícím právním předpisům týkajících se KB.

- **Zákon č. 181/2014 Sb., o kybernetické bezpečnosti**

Zákon o kybernetické bezpečnosti (dále jako „ZoKB“) a o změně souvisejících zákonů vychází z norem řady ČSN ISO/IEC 27000. Nabyl účinnosti 1. ledna 2015, upravuje práva a povinnosti osob, pravomoc a působnost orgánů veřejné moci v oblasti KB. Hlavním cílem zákona je stanovit základní úroveň bezpečnostních opatření, zlepšit detekci kybernetických bezpečnostních incidentů, zavést hlášení kybernetických bezpečnostních incidentů, zavést systém opatření k reakci na kybernetické bezpečnostní incidenty a upravit činnost dohledových pracovišť (Česko a, 2014).

Dle Smejkala (2019) se z hlediska posledních novel ZoKB může konstatovat, že jeho účelem je ochrana té části infrastruktury, která má význam pro fungování státu, kde při narušení informační a komunikační infrastruktury, významných informačních systémů, by došlo k poškození nebo ohrožení zájmů ČR. Vytvoření zákonného postavení státní instituce, která bude odpovědná za zajišťování KB státu a oprávněná k regulaci klíčových subjektů, bylo cílem kybernetického zákona (Doucek, Konečný a Novák, 2019).

- **Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti**

Zpracovává Směrnici NIS a pro informační a komunikační technologie upravuje obsah a strukturu bezpečnostní dokumentace, obsah a rozsah bezpečnostních opatření, náležitosti a způsob hlášení kybernetického bezpečnostního incidentu, náležitosti oznámení o provedení reaktivního opatření a jeho výsledku, způsob likvidace dat, provozních údajů, informací a jejich kopií (Česko, 2018).

- **Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritérií**

Vyhláška obsahuje nejen kritéria pro určení tzv. významných IS, ale také seznam těchto systémů. Dle NÚKIB by však nově neměla například obsahovat seznam konkrétních

regulovaných systémů a samotná určující kritéria by měla být přehlednější (Česko b, 2014), (Doucek, Konečný a Novák, 2019).

- **Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby**

Vyhláška zpracovává požadavky Směrnice NIS a upravuje odvětvová a dopadová kritéria pro určení provozovatele základní služby a vymezení významnosti dopadu narušení základní služby na zabezpečení společenských nebo ekonomických činností (Česko, 2017). Základní službou se rozumí dle ZoKB poskytování služeb, které je závislé na sítích elektronických komunikací nebo IS a narušení této služby by mohlo mít dopad na významné instituce (Česko a, 2014).

3.2 Krizový zákon a prováděcí předpisy

Níže uvedené zákony pojednávají o bezpečnosti České republiky a krizovém zákonu.

- **Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky**

V zákoně je stanoveno, že základní povinností státu je zajištění svrchovanosti a územní celistvosti ČR. Dále pak ochrana jejích demokratických základů a ochrana životů, zdraví a majetkových hodnot. Je zde definováno, kdo zajišťuje bezpečnost republiky a stanovuje povinnosti státních orgánů, orgánů územních samosprávných celků a právnické a fyzické osoby podílející se na zajišťování bezpečnosti státu (Česko, 1998).

- **Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)**

Stanovuje působnost a pravomoc státních orgánů a orgánů územních samosprávných celků, práva a povinnosti právnických a fyzických osob při přípravě na krizové situace nesouvisející se zajišťováním obrany České republiky před vnějším napadením (Česko, 2000).

3.3 Zdravotnictví a ochrana osobních údajů

Z hlediska podmínek poskytování zdravotních služeb, zpracování osobních údajů, je věnována následující část zákonů uvedených níže.

- **Zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách)**

Zákon upravuje zdravotní služby a podmínky jejich poskytování, druhy a formy zdravotní péče, práva a povinnosti pacientů, zdravotnických pracovníků, jiných odborných pracovníků a dalších osob v souvislosti s poskytováním zdravotních služeb. Dále stanovuje zpracování osobních údajů ve zdravotnické dokumentaci v listinné i elektronické podobě či kombinace obou, a upravuje jejich podmínky (Česko, 2011). Zdravotnickou dokumentaci upravuje vyhláška č. 98/2012 Sb., jejímž obsahem jsou údaje o zdravotnickém stavu pacienta a skutečnostech souvisejících s poskytováním zdravotnických služeb pacientovi – viz *Tab. 3 – Primární aktiva: Informace* (Česko, 2012).

- **Zákon č. 110/2019 Sb., o zpracování osobních údajů**

Zákon upravuje zpracování osobních údajů podle nařízení Evropského parlamentu a Rady (EU) 2016/697 (obecné nařízení o ochraně osobních údajů – GDPR), zpracování osobních údajů při zajišťování obranných a bezpečnostních zájmů ČR. Nakládání s osobními údaji ve zdravotnictví jsou pro potřeby prevence a léčení pečlivě váženy. Zdravotníci jsou školeni v oblasti GDPR, a to z hlediska mlčenlivosti, délce evidování a jejich ochrany v počítačích (Česko, 2019), (Právo na ochranu osobních údajů, 2021).

- **Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti**

Upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a výkon státní správy (Česko, 2005).

3.4 Normy, standardy a metodiky pro bezpečnost IS/IT

Pojmy „standard“ a „norma“ jsou označovány za ekvivalentní, avšak nepatrný rozdíl v těchto významech především závisí na tom, kde byly vydány. Jednoduše řečeno je označení norma (ČSN ISO/IEC) pro dokument vydaný či přejatý agenturou ČAS (Česká organizace pro standardizaci) a standard (ISO/IEC) pro dokumenty vydávané zahraničními organizacemi. V České republice se na vydávání českým technických norem podílejí dvě instituce – Úřad pro technickou normalizaci, metrologii a státní zkušebnictví (ÚNMZ) a Česká agentura pro standardizaci (ČAS) (Smejkal, Sokol a Kodl, 2019).

3.4.1 Mezinárodní organizace pro standardizaci

Mezinárodní organizace pro standardizaci, z anglického International Organization for Standartization (dále jako „ISO“), je nevládní organizace se sídlem v Ženevě ve Švýcarsku (About us, © All Rights Reserved). Oficiální činnost zahájila 23. února 1947 (The ISO Story - founding, 2011). Zjednodušeně řečeno ISO normy (standardy) představují určitý postup popisující způsoby, jak něco dělat (McCarthy, 2012).

3.4.2 Technické normy v souvislosti s bezpečností informací

Poskytují přehled řady norem ČSN ISO/IEC 2700x (v samotné ČSN ISO/IEC 27000 Systémy a řízení bezpečnosti informací – Přehled a slovník) a řadu dalších norem (27002, 27003) pokrývajících tyto oblasti (McCarthy, 2012).

Níže je uveden přehled těchto norem ČSN ISO/IEC série 2700x v kontextu s KB a z hlediska se zaměřením na tuto práci:

- **ČSN ISO/IEC 27000:2020 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník**

  Jedná se o terminologický slovník pro ostatní normy z rodiny 27000, který obsahuje přehled ISMS, termínů a definic v této řadě obecně používaných. Je použitelná pro všechny typy a velikosti organizací (Smejkal, Sokol a Kodl, 2019), (Hrazdil, 2020).

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

  Hlavní norma pro ISMS, poskytuje návod pro implementaci, udržování a neustálé zlepšování tohoto systému v rámci kontextu organizace. Dále zahrnuje požadavky na posuzování a ošetření rizik (Smejkal, Sokol a Kodl, 2019).

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

  Norma je určena zejména pro použití organizacemi mající v úmyslu vybrat opatření v rámci procesu zavádění ISMS založeném na ISO/IEC 27001; zavést obecně uznávaná opatření a vypracovat vlastní směrnice k řízení bezpečnosti informací (Smejkal, Sokol a Kodl, 2019).

- **ČSN ISO/IEC 27003:2018 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Pokyny k implementaci systémů řízení bezpečnosti informací**

  Představuje pokyny k požadavkům na ISMS a ve vztahu k nim poskytuje doporučení, možnosti a oprávnění. Zdůrazňuje důležitost následujících fází: a) z hlediska politiky bezpečnosti informací a cílů bezpečnosti informací pochopení potřeb organizace a nutnosti ustanovení této politiky; b) posouzení rizik organizace v oblasti bezpečnosti informací; c) opatření pro ošetření rizik; d) monitorování a přezkoumávání výkonnosti a efektivnosti ISMS a e) provádět neustálé zlepšování (Smejkal, Sokol a Kodl, 2019).

- **ČSN ISO/IEC 27004:2018 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Monitorování, měření, analýza a hodnocení**

  Obsahuje směrnice, které pomáhají organizacím při monitorování a měření výkonnosti, prezentaci efektivity ISMS a jejich analýzu a vyhodnocení výsledků tohoto měření (Smejkal, Sokol a Kodl, 2019).

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

  Norma je navržena pro implementaci informační bezpečnosti založené na přístupu k řízení rizik. Poukazuje na nepřetržitý proces činností: stanovení kontextu řízení rizik – dodržování předpisů, přístupy, které mají být použity nebo akceptace zbytkových rizik (Smejkal, Sokol a Kodl, 2019).

- **ČSN ISO/IEC 27006:2016 Informační technologie – Bezpečnostní techniky – Požadavky na subjekty poskytující audit a certifikaci systému řízení bezpečnosti informací**

  Specifikuje požadavky, které musí být demonstrované ve smyslu odborné způsobilosti, a poskytuje orgánům pokyny, které se zabývají auditem a certifikací ISMS (Smejkal, Sokol a Kodl, 2019), (Hrazdil, 2020).

- **ISO/IEC 27032:2013 Informační technologie – Bezpečnostní techniky – Směrnice pro kybernetickou bezpečnost**

  Tato norma obsahuje doporučení ohledně zlepšení bezpečnosti kyberprostoru. Řeší základní bezpečnostní postupy pro oblasti, jako jsou bezpečnost informací, sítí, internetu a ochrana kritické informační infrastruktury (Hrazdil, 2020).

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

  Norma ISO/IEC 27002 je způsobem, který zvažuje vhodné uplatnění bezpečnostních kontrol za účelem ochrany osobních zdravotních informací, aplikována do oblasti zdravotnictví. Poskytuje pokyny, jak nejlépe chránit důvěrnost, integritu a dostupnost informací, a to především zdravotnickým organizacím a dalším správcům osobních zdravotních informací. Z hlediska efektivity výkonu zdravotní péče je také rozhodující dostupnost těchto informací (Smejkal, Sokol a Kodl, 2019).

Lze zneužít i ty nejsofistikovanější podniky s pečlivým dodržováním standardů. Normy nemusí být použity všude nebo nemusí být použity důsledně. Poskytovatelé služeb mohou mít mezery představující významné riziko. Je nezbytné pamatovat na to, že interní nebo externí týmy budou posuzovat pouze ty oblasti, které mají hodnotit, a že ve většině případů musí věřit v to, co tvrdí daný subjekt (McCarthy, 2012).

3.4.3 Metodiky

Při budování informační bezpečnosti lze využívat technické standardy, které stanovují základní parametry v oblasti bezpečnosti informačních systémů, kde jsou také stanoveny základní požadavky pro certifikaci, klasifikaci a posuzování IS. Nejznámějšími jsou celosvětové metodiky Control Objectives for Information and Related Technology (dále jako „COBIT“) a Information Technology Infrastructure Library (dále jako „ITIL“).

- **COBIT** – kontrolní cíle pro informační a související technologie je rámec pro správu a řízení vyvinutý organizací ISACA. Jedná se o soubor praktik umožňující dosažení strategických cílů organizace díky efektivnímu řízení informací a IT. (Smejkal, Sokol a Kodl, 2019).

- **ITIL –** rámec osvědčených postupů pro poskytování služeb IT. Systematický přístup ITIL ke správě služeb IT může subjektům pomoci řídit rizika a mimo jiné budovat stabilní prostředí IT. Aktuální je ITIL 2014, což je rámec poskytující komplexní,

praktické a osvědčené pokyn pro správu IT služeb po celou dobu jejich životního cyklu (Smejkal, Sokol a Kodl, 2019).

3.5 Národní úřad pro kybernetickou a informační bezpečnost

Se vzrůstající potřebou zajišťovat kybernetickou bezpečnost vznikl dne 1. srpna 2017 na základě zákona č. 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (ZoKB), Národní úřad pro kybernetickou a informační bezpečnost (dále jako „NÚKIB“ nebo „Úřad“). Jedná se o ústřední správní orgán zaměřený na KB včetně ochrany utajovaných informací v oblasti IS/ICT a kryptografické ochrany (Smejkal, Sokol a Kodl, 2019).

Ředitelem Úřadu je od 20. března 2020 Ing. Karel Řehka, který je pravidelným účastníkem jednání Bezpečnostní rady státu (dále jako „BRS“) a je taktéž členem Výboru pro KB, stálého pracovního orgánu BRS, pro koordinaci plánování opatření k zajišťování KB ČR (Vedení úřadu, 2020), (O NÚKIB, 2017).

3.5.1 Bezpečnostní týmy

Tým pro reakce na počítačové bezpečnostní incidenty – Computer Emergency Response Team (dále jako „CERT“) a tým pro reakci na počítačové hrozby – Computer Security Incident Response Team (dále jako „CSIRT“) řeší kybernetické bezpečnostní incidenty, snaží se o jejich prevenci a koordinaci. Dále poskytují informace o odhalených slabinách HW a SW a o možných útocích na ně. Na rozdíl od označení CSIRT je CERT registrovaná ochranná známka, tudíž je jiným užívaným názvem pro CSIRT (Smejkal, Sokol a Kodl, 2019), (Jirásek, Novák a Požár, 2015).

V ZoKB byla zavedena terminologie pro národní a vládní CERT. Národní CERT je provozován sdružením CZ.NIC dle veřejnoprávní smlouvy uzavřené s NÚKIB. Vládní CERT je součástí Úřadu, u kterého se můžeme setkat i s názvem GovCERT.cz (Smejkal, Sokol a Kodl, 2019), (Doucek, Konečný a Novák, 2019). Pro řešení kybernetických bezpečnostních incidentů (dále jako „BI“) kritické informační infrastruktury a významných IS (dle ZoKB) je určen vládní CERT, pro řešení ostatních BI v počítačových sítích, které jsou provozovány v ČR je určen národní CERT (NBÚ vybral provozovatele).

4 KYBERNETICKÉ ÚTOKY NA NEMOCNIČNÍ ZAŘÍZENÍ

Kapitola je věnována jednak popisu ransomwaru a spear-phishingu a jednak kybernetickým útokům na nemocnice v České republice, ale i na zasažené zahraniční nemocniční zařízení tímto útokem. Dále poukazuje na to, že tyto útoky nejsou směřovány pouze na sektor zdravotnictví, nýbrž i na rozsáhlé organizace. S možností využívání ICT roste i možnost jejich zneužívání v podobě kybernetických útoků. Vzhledem k tomu, že roste významnost v užívání těchto technologií, jak v organizacích, tak i v kritické infrastruktuře, je třeba věnovat náležitou pozornost, jak se před těmito útoky chránit či jim případně předcházet (Johnson, 2015).

Pod ZoKB nyní nově (od 1. ledna 2021) na základě vyhlášky č. 573/2020 Sb., kterou se mění vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby, spadají ty nemocnice, které disponují nejméně 400 lůžky (v loňském roce tento počet činil 800 lůžek), kde kromě statutu traumacentra povoluje i vysoce specializovaná centra onkologické, cerebrovaskulární nebo mimo jiné kardiovaskulární péče. Dále přidává kritérium urgentního příjmu s nejméně 40 lůžky intenzivní péče a kritérium poskytovatele akutní lůžkové péče s průměrným počtem unikátních ošetřených pacientů v posledních třech kalendářních letech nejméně 100 000 za rok. Celkový počet činí 46 nemocničních zařízení jako poskytovatelů základních služeb v odvětví zdravotnictví. Dle nových kritérií je k uvedenému datu nově určených 30 těchto zařízení (NÚKIB, 2021, a), (Česko, 2017), (Česko, 2020).

Důvodem rozšíření může být například to, že kybernetický útok nebyl cílen pouze na velké nemocnice, nýbrž i na psychiatrickou nemocnici v Kosmonosech a v neposlední řadě z hlediska zajištění kybernetické bezpečnosti daného nemocničního zařízení (Magdoňová, 2020).

Dle odborného článku (Bínek, 2020) stojí za zmínku obsah vektorů kybernetické ochrany dat – bezpečí, dostupnost, soukromí, pravost a jejich ochrana před ztrátou či napadením. Autor článku dále zmiňuje 7 kroků zaměřených na KB (zastavení úniku citlivých dat, nastavení ochrany proti malwaru, soulad s obecnými i specifickými požadavky – GDPR, přesun aplikací a uložišť na cloud, nepřetržitá dostupnost dat, ochrana mobilních zařízení – tablet, mobil lékaře, účinné a srozumitelné nástroje – srozumitelná pravidla pro přístup k citlivým datům pacienta). Avšak zmíněné kroky jsou pouze obecného charakteru. Opatřením v KB je věnována samostatná kapitola uvedená na konci této práce.

4.1 Upozornění na zvýšené riziko kybernetických útoků proti ČR

V souladu s aktuálním děním kvůli kauze Vrbětice hrozí zvýšené riziko kybernetických útoků vůči ČR, jejím zájmům, organizacím či dalším významným institucím. Na základě deklarovaného podezření výbuchu muničního skladu bylo vyhoštěno 18 pracovníků ruské ambasády, kde podle zjištění Bezpečnostní informační služby (BIS) z roku 2018 se jednalo o příslušníky GRU (z ruského akronyma: *Glavnoje razvedyvatělnoje upravlenije*, česky: Hlavní správa rozvědky). NÚKIB tak v důsledku na uvedenou kauzu vydal upozornění ke dni 20. dubna 2021. Tyto činnosti mohou mít podobu špionážních kybernetických operací a útoků prostřednictvím ransomwaru/wiperu. Mezi ohrožené subjekty, kde je vyšší pravděpodobnost tohoto útoků, patří zvláště vládní instituce, ozbrojené síly a sektory nejen energetiky a průmyslu, ale i další (například zdravotnictví). V souvislosti s tím pak Úřad doporučuje ostražitost před těmito útoky a zneužitím konkrétních zranitelností, které jsou součástí vydaného dokumentu či opatření uvedených v kapitole *Plán zvládání bezpečnostních incidentů* (NÚKIB, 2021, b).

4.2 Kybernetické útoky na nemocniční zařízení

Jedním z důvodů napadení je slabá ochrana proti útokům v podobě zastaralé techniky a SW či nízkého rozpočtu na aktualizaci systémů, která představuje vysokou míru zranitelností v IT bezpečnosti nemocničních zařízení. Počet kybernetických útoků na zdravotnictví vzrostl za poslední dva měsíce (údaj k 11. 1. 2021) celosvětově o 45 % (na další odvětví o 22 %). Průměr činil 625 útoků na zdravotnickou organizaci za týden, přitom největší vlna kybernetických útoků je ve střední Evropě (nárůst o 145 %). Důvodem nárůstu útoků na zdravotnictví představuje nejen atraktivní cíl kvůli jejich zranitelnosti a ochotě zaplatit, ale také současná situace pod náporem pacientů s onemocněním COVID-19 a v neposlední řadě spuštění vakcinačních programů (Řeháček, 2021).

4.2.1 Ransomware

Ransomware (z angl. r*ansom* – výkupné) je druh škodlivého softwaru (malware), který po otevření přílohy, stáhnutím infikovaného souboru, kliknutím na odkaz či cíleným útokem nainstaluje škodlivý kód, který se následně šíří po sítí celé instituce a zašifruje přístup k datům. Ke zpřístupnění těchto dat je většinou požadováno výkupné v bitcoinech. Avšak zaplacení výkupného se nedoporučuje z toho důvodu, že neexistuje žádná záruka odblokování a vrácení dat, a dále skutečnost, že v případě odblokování těchto dat nedojde

k odstranění samotného malwaru. Motivace útočníků spočívá ve finančním zisku (existují ale i případy, kdy výkupné nebylo požadováno, ale data byla jednoduše zničena), dále se jedná o zveřejnění citlivých dat pacientů (Jak se bránit útoku ransomwarem, 2020).

Jde o druh útoku, který může zcela paralyzovat jakoukoli firmu, nemocnici i celou obec. Chybou koncových uživatelů (lidský faktor) tak dochází k nejčastějším útokům prostřednictvím tzv. phishingu nebo cíleného spear-phishingu (viz níže), kdy se jedná o podvodný e-mail (NÚKIB, 2020, c). Vůbec první zmínka o odhalení případu ransomwaru byla zdokumentována v roce 1989, kterým byl trojan AIDS a šířil se pomocí klasické pošty a v podobě fyzického média – diskety (Ransomware, 2020).

Typy ransomwaru

Níže jsou uvedeny typy ransomwaru:

- **Locker ransomware** – uzamkne počítač nebo zařízení, pro umožnění přístupu je požadováno výkupné. Jako příklad je uveden Reveton.
- **Cryptoransomware** – soubory a data šifruje, pro jejich dešifrování požaduje výkupné. Existuje několik desítek ransomwaru tohoto typu, dále jsou uvedeny některé z nich: Locky, WannaCry, Bad Rabbit, Ryuk, Troldesh, Jigsaw, CryptoLocker, Petya, GoldenEye, GandCrab atd. (Rubens, 2017), (Ransomware útoky, definice, příklady, ochrana, odstranění 2021, 2021).
- **Doxware** – typ ransomwaru, který hrozí zveřejněním osobních údajů, jestliže uživatel nezaplatí výkupné (Ransomware – definice a jak se úspěšně bránit, 2020).
- **Scareware –** zobrazuje se prostřednictvím vyskakovacího okna, ve kterém je napsáno, že data byla zašifrována a zařízení bude uzamčeno (Ransomware – definice a jak se úspěšně bránit, 2020).

4.2.2 Spear-phishing

Jedná se o sofistikovanější typ útoku phishing prostřednictvím e-mailové komunikace. Tento typ útoku je cílenější na konkrétního uživatele, a proto dosahuje většího úspěchu než zmíněný běžný typ útoku (Jirásek, Novák a Požár, 2015). Z toho důvodu, že je právě spear-phishing cílenější a slouží především k získání citlivých informací, jsou právě pro tento typ útoku instituce (nemocniční zařízení) disponující citlivými údaji pacientů tak vyhledávána.

Základní rozdíl (viz *Tab. 1*) mezi těmito dvěma typy spočívá v jejich rozsahu zacílení na konkrétní organizaci či osobu. V případě phishingu se útočník snaží z uživatele vylákat data v podobě osobního charakteru a snaží se tak uživatele přesvědčit, aby klikl na uvedený odkaz, který ovšem vede na podvodnou stránku (Král, 2015).

Aby nedošlo k potencionálnímu napadení kybernetickými útoky, jsou vydávána různá doporučení pro uživatele, jak se před nimi chránit. I přes dostatečnou informovanost ohledně daného jevu existují lidé, kteří si i po přečtení této hrozby podvodnou stránku vyzkouší (Kožíšek a Písecký, 2016).

Tab. 1 – Rozdíl mezi phishingem a spear-phishingem

	Phishing	**Spear-phishing**
Rozsah příjemců	Velký počet e-mailových adres.	Pouze jeden příjemce.
Odkaz na internet	Obsahuje odkaz na internet.	Neobsahuje odkaz na internet.
Důvěryhodná osoba/firma	E-mail od osoby/firmy, která je známa.	E-mail od osoby/firmy, která je známa.
Požadavek na zadání určitých údajů	Požadováno zadání určitých údajů.	Není požadováno zadání údajů.
Příloha	Neobsahuje zpravidla žádnou přílohu, ale odkaz.	Obsahuje přílohu.
Cíl	Získání přihlašovacích údajů.	Získání citlivých informací.

Zdroj: (Čermák, 2021).

4.3 Kybernetické útoky v České republice

Technologický vývoj se týká i oblasti zdravotnictví. Na sálech se operuje s pomocí mobilního zařízení (mobil, tablet) v ruce, zdravotnická zařízení umožňují zobrazení pacientova stavu, data mezi jednotlivými odděleními nebo nemocnicemi jsou posílány prostřednictvím ICT. Stačí malá chyba, nepozornost především lidského faktoru a nemocnice a jejich zařízení pak čelí úspěšnému kybernetickému útoku, který zapříčil jejich někdy i úplné vyřazení z provozu na dobu v rozmezí dnů až týdnů.

Nemocniční zařízení

Oběťmi kybernetických útoků se staly níže uvedené nemocnice. Ovšem útoky nejsou prováděny pouze na nemocniční zařízení, nýbrž i na jiné organizace.

- **Nemocnice Rudolfa a Stefanie Benešov**

Dne 11. prosince 2019 ve 2.50 hodin došlo k útoku na klíčové ICT systémy středočeské Nemocnice Rudolfa a Stefanie Benešov. K útoku došlo pomocí ruského ransomwaru Ryuk,

který byl stažený po otevření závadné přílohy a kterému předchází malware Emotet a Trickbot. Emotet představuje vstup viru do PC přes otevření přílohy (spear-)phishingového e-mailu a poté spuštěním makra, který následně stáhne další malware Trickbot sbírající citlivá data (přihlašovací údaje apod.) a pomocí nich se pak v sítí šíří dál. Poté útok pokračuje instalací Ryuku, který data zašifruje, ochromí síť a je požadováno výkupné. Po útoku nešly spustit žádné přístroje včetně počítačových sítí a všechny plánované operace byly zrušeny. Pacienti tak museli navštívit jiná nemocniční zařízení. Provoz nemocnice byl po dobu sedmi dnů zcela paralyzován, nefungoval ambulantní provoz a péče byla poskytována pouze již hospitalizovaným pacientům (Kyberútok na nemocnici v Benešově: nefungují žádné přístroje, 2019), (Danihelka, Schreiberova a Jurásek, 2020), (NÚKIB, 2019).

- **Kybernetický útok ve Fakultní nemocnici Brno**

Dalšímu kybernetickému útoku čelila v březnu 2020 Fakultní nemocnice Brno, kdy byly, podobně jako u Benešovské nemocnice, omezeny některé počítačové provozy, zrušení plánovaných operací a částečný odklon pacientů do okolních nemocnic (FN Brno se stala terčem kybernetického útoku, 2020). Za kybernetickým útokem stál šifrovací vir Defray, který je typický pro zdravotnická zařízení. Podstata spočívala v podvodném vylákání citlivých informací na základě důvěryhodně vypadajícího e-mailu, kde po jeho otevření vir pronikne do systému a zašifruje klíčové složky (Horák, 2020).

K cíleným kybernetickým útokům došlo i v Ostravské nemocnici, která však tento útok odrazila. Kybernetické útoky na nemocnice mohou způsobit provozní ztráty v desítkách milionů korun. Dle IT expertů může jeden útok nemocnici vyřadit i na několik dnů (Fakultní nemocnice Ostrava se stala terčem kybernetického útoku, 2020).

Jiné organizace

Jak je uvedeno výše jediným cílem pro kybernetický útok nejsou jen samotné nemocnice či jiná nemocniční zařízení, terč pro tyto útoky představují i další (významné) instituce. V roce 2019 se stala obětí útoku těžařská společnost Ostravsko-karvinských dolů, který způsobil okamžitý výpadek a nefunkčnost celé firmy a jejich serverů.

Dále je uvedeno několik dalších organizací cíleného kybernetického útoku: Autoklub ČR, Gransy s.r.o, eD systém a.s., Povodí Vltavy, Správa Pražského hradu, Avast, T-Mobile, Česká spořitelna, Internetové bankovnictví, Zpravodajské portály, Česká pojišťovna a další (Čermák, 2021), (Danihelka, Schreiberova a Jurásek, 2020).

4.4 Kybernetické útoky v zahraničí

Nejen tuzemské nemocniční zařízení představují terč pro kybernetické útoky prostřednictvím ransomware, který má mnohdy na svědomí nejen zašifrování dat či nefunkční zařízení, ale i lidské životy. Z důvodu rozsahu práce jsou popsány jen některé z nich.

Nemocniční zařízení

Na nemocnice a zdravotnická zařízení se zaměřila rostoucí vlna útoků ransomwaru, kde většina útoků využívala ransomware Ryuk. Společnosti CISA, FBI vydaly společné doporučení o KB varující před zvýšenými a bezprostředními hrozbami na americké nemocnice a poskytovatele zdravotní péče. Narůst kybernetických útoků zahrnuje jednak ransomware, botnet, vzdáleného spuštění kódu a útoků DDoS (Attacks targeting healthcare organizations spike globally as COVID-19 cases rise again, 2020).

- **Kybernetický útok na fakultní nemocnici v Düsseldorfu**

Dosud nebyl útok ransomwarem zaznamenán v souvislosti s úmrtím pacienta. To se změnilo kvůli útoku na univerzitní nemocnici v Düsseldorfu, kde musela být pacientka převezena do jiné nemocnice a na následky zpoždění zemřela. Zdravotníci neměli přístup k datům pacientů a museli odložit všechny plánované operace a nemohli přijímat nové. Útok byl zvláštní tím, že nebylo požadováno výkupné, tudíž se mohlo jednat o nešťastnou náhodu (Kilián, 2020).

- **Kybernetické útoky ve Francii**

Během jednoho týdne byly zasaženy hned dvě francouzské nemocnice. Útok byl proveden prostřednictvím kryptoviru Ryuk. Nemocnice okamžitě stanovily omezené postupy zajišťující výměnu informací nezbytných pro péči o pacienty (Cyber attacks hit two French hospitals in one week, 2021).

Jiné organizace

Dopad kybernetického útoku na Světovou zdravotnickou organizaci (WHO) znamenal únik zhruba 450 e-mailů a hesel jejích představitelů a e-mailové podvody zaměřené na veřejnost. Zároveň bylo zveřejněno doporučení kvůli vzrůstajícím kybernetickým útokům v souvislosti s COVID-19 (Shein, 2020).

DÍLČÍ ZÁVĚR

Teoretická část byla věnována oblastem, které blíže popisovaly danou problematiku kybernetické bezpečnosti. Na úvod byla vybrána kapitola vymezující oblast informačních a komunikačních technologií, které mimo jiné úzce souvisí s obsahem kybernetické bezpečnosti. Další kapitola uvedla do samotné problematiky kybernetické bezpečnosti, na které staví tato práce. Byla zaměřena na podstatu kybernetické bezpečnosti, kde byly blíže specifikovány její tři principy, kterými jsou triáda CIA, prvky kybernetické bezpečnosti a životní cyklus. Dále zmiňuje systém řízení bezpečnosti informací a mimo jiné také Národní strategii kybernetické bezpečnosti České republiky 2021–2025. Základní právní předpisy kybernetické bezpečnosti shrnuje další kapitola, ve které byly uvedeny také technické normy v souvislosti s bezpečnosti informací a Národní úřad pro kybernetickou a informační bezpečnost s bezpečnostními týmy. Poslední kapitola byla věnována samotným kybernetickým útokům a popisu stěžejního škodlivého kódu ransomwaru, jeho typům a jeho šíření prostřednictvím spear-phishingu.

II. PRAKTICKÁ ČÁST

5 CHARAKTERISTIKA VYBRANÝCH NEMOCNIČNÍCH ZAŘÍZENÍ

Z důvodu bezpečnosti vybraných nemocničních zařízení a v souvislosti poskytnutých citlivých údajů, nebudou tyto charakterizovány konkrétně. Níže je uvedená charakteristika nemocničních zařízení v obecné rovině. Sektor zdravotnictví spadá pod provozovatele základních služeb, které jsou definovány jako základní z hlediska zachování kritických společenských nebo ekonomických činností, přičemž toto poskytování je závislé na ICT a případný kybernetický bezpečnostní incident by mohl způsobit vážné narušení poskytování této služby (Doucek, Konečný a Novák, 2019). Dle zákona č. 372/2011 Sb. poskytovatelem zdravotních služeb se dle § 2 zmíněného zákona rozumí fyzická nebo právnická osoba (zdravotní a odborní pracovníci), která má k tomuto poskytování oprávnění. Zdravotnickým zařízením se dle § 4 výše uvedeného zákona rozumí prostory určené pro poskytování zdravotních služeb, zejména pro pacienty. Poskytnutí péče se pak dělí dle časové naléhavosti na neodkladnou, akutní, nezbytnou a plánovanou péči, a dle jejího účelu na druhy například preventivní, diagnostické, léčebné či ošetřovatelské péče (Česko, 2011). Běžná struktura nemocnic se člení na vedení nemocnice v čele s ředitelem a managementu. Dále se dělí na jednotlivá oddělení (biochemie, chirurgické, farmakologie, radiologie a zobrazovací metody), kliniky (alergologie, imunologie), centra (vysoce specializovaná centra, například kardiovaskulární) či ústavy (soudní lékařství) (Vyhledávání poskytovatele, 2021). Vybraná nemocniční zařízení spadají pod ZoKB, kde jedno zařízení disponuje více než 900 lůžky, v případě druhého zařízení tento počet překračuje jeden tisíc. Jak je uvedeno výše, na základě vyhlášky č. 437/2017 Sb. bylo k letošnímu roku sníženo kritérium odvětvových a dopadových pro učení provozovatele základní služby, a to na nejméně 400 lůžek.

5.1 Řízený rozhovor

Prvotní sběr informací byl proveden na základě metody řízeného rozhovoru, která je blíže specifikována v úvodní kapitole Cíl práce a použité metody. Pro řešenou problematiku byli zvoleni IT odborníci z vybraných nemocnic. Z důvodu snadnějšího průběhu rozhovoru byly otázky k rozhovoru poslány s předstihem. V průběhu rozhovoru bylo přistoupeno k nestandardizovanému typu rozhovoru, kde autorkou byly objasněny a vysvětleny některé otázky v případě jejich nejasností. Na základě poznatků z uskutečněných rozhovorů byla provedena analýza vybraných rizik a dále šetřena. Problematika je předmětem kapitoly Analýza rizik. Tyto řízené rozhovory jsou obsahem přílohy II a III této práce.

6 AKTIVA OBJEKTU

Tato kapitola identifikuje aktiva týkající se obecně nemocničních zařízení. Aktiva představují hodnotu pro daný objekt, která je bezpodmínečně nutné chránit. Zejména pak, co se týká osobních citlivých údajů pacientů a jejich ochrany, je důležité věnovat pozornost především před jejich odcizením, tzn. krádeží, jelikož se jedná o stěžejní data pro výkon činností nemocničních zařízení.

Pro identifikaci aktiv sloužila především norma ČSN/IEC 27005, příloha B a dále zákon č. 372/2011 Sb. pro identifikaci citlivých dat pacienta. Norma definuje dvě skupiny aktiv:

- **Primární** – představují obchodní procesy a informace, kde v případě ztráty, modifikace či jiných negativních aspektů je ovlivněna činnost organizace.
- **Podpůrná** – obsahují hardware, software, zaměstnance či strukturu organizace důležité pro podporu primárních aktiv (ČSN ISO/IEC 27005, 2019).

6.1 Identifikace primárních aktiv

Vymezení primárních aktiv předkládá zmíněná norma ČSN ISO/IEC 27005 jako obchodní procesy, činnosti a informace. Tato skupina je charakteristická zejména pro činnosti a procesy vrcholového vedení, vedoucích pracovníků, uživatelů a odborníků v oblasti IS. Z důvodu přehlednosti jsou tato aktiva rozdělena do dvou skupin, a to na procesy a informace, které budou dále přiblíženy. Dále slouží jako přehled pro další analýzu, kde je uveden pouze výčet zodpovědných osob či systémů. Hodnocením aktiv se věnuje jiná kapitola.

6.1.1 Procesy a činnosti

V souvislosti s procesy a činnostmi lze pro primární aktiva definovat následující rysy:

- Při jejich ztrátě dojde k neuskutečnění poskytnutí hlavních činností.
- Obsahují tajné procesy či jinak chráněné technologie.
- Značné ovlivnění představuje jejich změna.
- Jsou nezbytné pro plnění smluvní, právní či jiných požadavků.

Primární aktiva vztahující se k vybraným objektům představují především poskytování zdravotní neodkladné, akutní či jiné péče pacienta, kde vznik nežádoucích událostí

by způsobil závažný dopad pro poskytování výše uvedené péče. Následující tabulka přibližuje stěžejní činnosti.

Tab. 2 – Primární aktiva: Procesy a činnosti

P. č.	Zdravotní dokumentace
1.	Poskytovatel je povinen vést a uchovávat zdravotnickou dokumentaci a nakládat s ní podle zákona a jiných právních předpisů.
Informační systémy (nemocniční, radiologický, laboratorní, ambulantní)	
2.	Představují soubor lidí, technických prostředků a postupů zajišťují sběr, přenos, zpracování, uchování dat za účelem prezentace informací pro budoucí potřeby uživatelů.
Správa IT	
3.	Správa technického zařízení nemocnice.
Manažer kybernetické bezpečnosti	
4.	Odpovídá za systém řízení bezpečnosti informací.
5.	Odpovídá za pravidelné informování vedení o činnostech vyplývajících z rozsahu jeho odpovědnosti.
6.	Odpovídá za informování o stavu systému řízení bezpečnosti informací.
Architekt kybernetické bezpečnosti	
7.	Je odpovědný za zajištění návrhu implementace bezpečnostních opatření tak, aby byla zajištěna bezpečná architektura informačního a komunikačního systému.
Auditor kybernetické bezpečnosti	
8.	Odpovídá za provedení auditu kybernetické bezpečnosti.

Zdroj: (Česko, 2011).

Každá organizace (nemocniční zařízení) disponuje zaměstnanci, kteří jsou zodpovědní za výše uvedené procesy a činnosti. Zvláště pak, jedná-li se o zařízení spadající pod ZoKB, na základě kterého se musí řídit určitými bezpečnostními pravidly.

6.1.2 Informace

Primární informace jsou charakteristické obsahem:

- Životně důležitých informací pro umožnění činností organizace.
- Osobní informace týkajících se soukromí.
- Strategické informace pro splnění cílů.
- Informace, které vyžadují hodně času při jejich zpracování.

V nemocničním zařízení se nakládá s informacemi, resp. údaji, které jsou nezbytné pro výkon povinností. Především se jde o nakládání a zpracování osobních údajů. Osobní údaje

jsou informace, jejichž nutnost ochrany vyplývá z Obecního nařízení o ochraně osobních údajů (GDPR) – Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (Doucek, Konečný a Novák, 2019). Za osobní údaj lze také považovat každou informaci o identifikovatelné fyzické osobě, zejména pomocí určitého identifikátoru. Jedním z dostupných SW identifikující a evidující údaje o pacientech, může představovat zdravotnický SW Wintropos. Jedná se o SW, který je moderní, dostupný a snadno ovladatelný a zakládá se na zkušenostech s danou problematikou i s potřebami lékařů. Mimo jiné umožňuje především vedení kartotéky pacientů, tisk receptů apod. (Vše o programu Wintropos, 2020). Obsah citlivých údajů vymezuje příslušný zákon, který dále uvádí, že vedení zdravotnické dokumentace může být v listinné či elektronické podobě nebo v kombinaci obou. V elektronické verzi je tato dokumentace pořizována, zpracovávána, ukládána a zprostředkována v digitální formě za využití IT. Tyto údaje shrnuje níže uvedená tabulka.

Tab. 3 – Primární aktiva: Informace

P. č.	Dokumentace
9.	Zdravotní dokumentace pacienta.
10.	Zpráva z auditu kybernetické bezpečnosti.
Identifikační údaje pacienta	
11.	Jméno, příjmení.
12.	Datum narození.
13.	Rodné číslo.
14.	Číslo pojištěnce zdravotního pojištění.
15.	Adresa místa pobytu trvalého bydliště na území České republiky.
16.	Místa hlášeného pobytu cizince na území České republiky.
17.	Pohlaví pacienta.
Identifikační údaje poskytovatele	
18.	Jméno, případně jména, příjmení poskytovatelů.
19.	Adresa místa poskytování zdravotních služeb fyzických osob.
20.	Adresa sídla nebo místa podnikání právnických osob.
21.	Identifikační číslo.
Informace o zdravotním stavu pacienta	
22.	Průběh a výsledky poskytovaných zdravotních služeb.
23.	Údaje zjištěné z rodinné, osobní a pracovní anamnézy pacienta, a je-li to důvodné, též údaje ze sociální anamnézy.
24.	Údaje vztahující se k úmrtí pacienta.

Zdroj: (Česko, 2011).

6.2 Identifikace podpůrných aktiv

Podpůrná aktiva jsou rozdělena dle normy ČSN ISO/IEC 27005, přílohy B následovně:

- Hardware.
- Software.
- Síť.
- Osoby.
- Organizace.

Jednotlivé položky výše uvedených typů aktiv jsou určena na základě řízeného rozhovoru ve vybraných nemocničních zařízení. Tyto položky předkládají následující tabulky.

6.2.1 Hardware

V tabulce jsou uvedeny pouze položky z obecného pohledu, které se vztahují na nemocniční zařízení. Hardware lze rozdělit na pevné a mobilní zařízení. Samotná tabulka s vybranými položkami je pouze informativní pro účely vybraného nástroje pro analýzu aktiv a hrozeb – viz podkapitola RISKAN.

Tab. 4 – Podpůrná aktiva: Hardware

P. č.	Hardware
1.	Databázové servery.
2.	Síťové prvky.
3.	Zálohovací zařízení.
4.	Notebooky.
5.	Stolní PC.
6.	Laboratorní zařízení.
7.	Radiologická zařízení.
8.	Zobrazovací zařízení.
9.	Ultrazvuk.
10.	CT přístroj.
11.	Mamograf.
12.	RTG přístroj.

Zdroj: (Řízený rozhovor, 2021).

6.2.2 Software

Za software se považují programy, které se podílí na provozu a zpracování dat. Primárně se jedná o operační systémy tvořící základ každého PC. Software dále zajišťuje fungování IS, či předávání zpráv napříč nemocničním zařízením. Tato aktiva uvádí tabulka č. 5 níže.

Tab. 5 – Podpůrná aktiva: Software

P. č.	Software
13.	Operační systémy (Windows XP, Linux, …).
14.	SW pro elektronické předávání zpráv (Exchange).
15.	Antimalwarový SW.
16.	Zálohovací SW.
17.	Zdravotnický informační systém.

Zdroj: (Řízený rozhovor, 2021).

6.2.3 Osoby

Lidé představují nejzranitelnější prvek v kyberprostoru. Osoby neboli zaměstnanci tvoří všechny ty, kteří jsou spojeni s užíváním IS a jsou úzce spojeny s provozem nemocničních zařízení. Tito pracovníci zastávají především funkci rozhodovací vzhledem k přijímaným opatřením apod. Tyto osoby blíže specifikuje tabulka č. 6.

Tab. 6 – Podpůrná aktiva: Osoby

P. č.	Osoby
18.	Vrcholové vedení nemocnice.
19.	Vedoucí pracovníci.
20.	Uživatelé IS.
21.	IT pracovníci.
22.	Správci IT.
23.	Pacienti.
24.	Manažer KB.
25.	Architekt KB.
26.	Auditor KB.

Zdroj: (Řízený rozhovor, 2021).

6.2.4 Organizace

Organizace představují organizační rámec popisující organizační strukturu, pod kterou spadají určité osoby a jsou určeny pro řízení činností. Uvedené organizace byly sestaveny z hlediska základní struktury nemocničních zařízení.

Tab. 7 – Podpůrná aktiva: Organizace

P. č.	Organizace
27.	Správa IT.
28.	Ekonomický úsek.
29.	Personální řízení.
30.	Ošetřovatelská péče.
31.	Léčebná péče.
32.	Technický úsek.
33.	Krizové řízení a bezpečnost.

Zdroj: (Řízený rozhovor, 2021).

7 HROZBY OBJEKTU

Hrozba představuje náhodně nebo úmyslně vyvolanou událost, která může mít negativní dopad na důvěrnost, integritu a dostupnost aktiv. Tato část identifikuje vybrané hrozby pro zvolená nemocniční zařízení. Pro identifikaci hrozeb sloužila výše zmíněná norma.

7.1 Identifikace hrozeb

Při identifikaci lze vycházet z různých typů hrozeb. Ať už se jedná o lidské úmyslné či neúmyslné selhání ze strany organizačního opatření nebo ty technické, které na rozdíl od těch přírodních jsou do jisté míry předvídatelné. Přičemž některé z těchto hrozeb mohou působit na více aktiv zároveň. Pro identifikaci hrozeb byly zvoleny pouze ty hrozby, které budou použity pro následnou analýzu rizik – viz podkapitola RISKAN. Jedná se o vymezení několika hrozeb zmíněných typů, kde zvládnutí všech možných hrozeb je do jisté míry nemožné už jen z hlediska finančních prostředků. Nicméně by neměla být upozaděna ta, která jednotlivá aktiva ohrožují nejvíce. V následujících tabulkách jsou hrozby přehledně rozděleny dle jejich původu a účelu. Hodnocením hrozeb je věnována samostatná kapitola.

Rozdělení hrozeb:

- Lidské neúmyslné selhání.
- Lidské neúmyslné selhání – organizační.
- Lidské úmyslné poškození.
- Technická selhání.
- Přírodní.

7.1.1 Lidské neúmyslné selhání

Tyto hrozby jsou způsobeny zejména neopatrným jednáním či neznalostí zaměstnanců.

Tab. 8 – Lidské selhání: neúmyslné

P. č.	Lidské neúmyslné selhání
1.	Ztráta důvěrnosti/integrity dat.
2.	Zničení PC vybavení.
3.	Nevhodné užívání IT systému.
4.	Neúmyslná manipulace s daty.
5.	Neautorizované použití IS.
6.	Nesprávná segmentace sítě.

Zdroj: (ČSN ISO/IEC 27005, 2019).

P. č.	Lidské neúmyslné selhání
7.	Pochybení zaměstnanců.
8.	Spuštění škodlivého kódu.
9.	Neautorizované užití nebo stažení SW.
10.	Vyzrazení citlivých údajů pacienta.

Zdroj: (ČSN ISO/IEC 27005, 2019).

7.1.2 Lidské neúmyslné selhání – organizační

Hrozby z hlediska organizačního selhání mohou nastat například v případě nedostatečného počtu potřebných IT pracovníků nebo nedostatečného školení bezpečnosti informací.

Tab. 9 – Lidské neúmyslné selhání – organizační

P. č.	Organizační selhání
11.	Nedostatek personálu.
12.	Minimální bezpečnostní povědomí.
13.	Nesprávné přidělení odpovědností.
14.	Neformální postup při autorizaci veřejných dat.
15.	Nízká kvalifikace zaměstnanců.
16.	Neautorizované chování zaměstnanců.
17.	Nedostatečné školení bezpečnosti informací.
18.	Nedostatečná bezpečnostní pravidla.

Zdroj: (ČSN ISO/IEC 27005, 2019).

7.1.3 Lidské úmyslné poškození

Tyto hrozby mohou pocházet z různých důvodů. Ten stěžejní představuje úmyslný kybernetický útok z externích zdrojů (cracker). Dalším důvodem mohou být narušené vztahy pracovníků, osobní selhání, výpověď apod.

Tab. 10 – Lidské úmyslné poškození

P. č.	Úmyslné lidské poškození
19.	Záměrná manipulace s daty.
20	Záměrná manipulace s IS.
21.	Neautorizovaný přístup do systému.
22.	Neautorizované použití systému.
23.	Zneužití uživatelských práv.
24.	Kybernetický útok.
25.	Spear-phishing.
26.	Ransomware.
27.	Zneužití citlivých dat.
28.	Zničení zařízení nebo médií.

Zdroj: (ČSN ISO/IEC 27005, 2019).

7.1.4 Technická selhání

Technická selhání představují celou řadu hrozeb. Například v důsledku přerušení dodávky elektrické energie mohou přestat fungovat některá nebo všechna zařízení v případě, kdy dojde k tomuto přerušení neočekávaně a dané nemocniční zařízení na toto připraveno v podobě záložních generátorů. Níže uvedená tabulka představuje zásadní technická selhání.

Tab. 11 – Technická selhání

P. č.	Technická selhání
29.	Bezpečnostní mezery v systému.
30.	Nechráněné přenosy dat.
31.	Neprovedená aktualizace.
32.	Chybná záloha dat.
33.	Přerušení dodávky el. energie.
34.	Nefunkční zařízení.
35.	Nefunkčnost SW.
36.	Poškození nosiče dat.
37.	Výpadek interní sítě.
38.	Chyba v šifrování.
39.	Porucha odeslání zprávy.

Zdroj: (ČSN ISO/IEC 27005, 2019).

7.1.5 Přírodní

Těmito hrozbami je taktéž daný objekt ohrožen, avšak pro účely této práce jsou méně významné z hlediska na zaměření práce.

Tab. 12 – Přírodní hrozby

P. č.	Přírodní
40.	Blesk.
41.	Požár.
42.	Voda.
43.	Prach.

Zdroj: (ČSN ISO/IEC 27005, 2019).

8 ANALÝZA RIZIK

Tato kapitola je zaměřená na výstupy z několika analýz. Prvotní analýza rizik je provedena pomocí metody KARS, na základě které budou získány oblasti rizik, kde každá jednotlivá oblast představuje významnost na ohrožení daného objektu. Dále bude sloužit jako podklad pro návrh opatření. Využití této metody bude pouze na rizika představující hrozbu v kybernetické oblasti. Další analýzu bude představovat rizikový kalkulátor RISKAN. Jedná se o nástroj, který slouží pro sestavení semi-kvantitativní analýzy rizik. Tento nástroj se zaměřuje na vztah aktivum-hrozba a dále posuzuje zranitelnost aktiv vůči těmto hrozbám. Zatímco metoda KARS je zaměřena pouze na rizika a vzájemný vztah mezi nimi. Výběr metody se zakládal především na tom, jaká rizika na sebe navzájem působí (souvztažnost rizik) a na která je potřeba se dále zaměřit. Zvolený nástroj RISKAN byl určen z hlediska působení hrozby na významné aktivum.

8.1 Kvalitativní analýza rizik s využitím jejich souvztažností (KARS)

Metodou KARS se ve své disertační práci zabýval Štefan Pacinda z Institutu ochrany obyvatelstva, Lázně Bohdaneč. Metoda byla vytvořena pro stanovení prioritních rizik a pro ta, která se mohou řešit s určitým časovým odkladem. I přes to, že se jedná o kvalitativní analytickou metodu, je důležité dodržet postup jednotlivých kroků vedoucí ke zjištění míry rizika (Jelšovská a Peterková, 2013), (Košťál, 2015).

Tato metoda byla zvolena z důvodu posouzení souvztažností vybraných rizik a pro následné opatření pro nejkritičtější rizika pro vybrané nemocniční zařízení. Pro provedení správné aplikace slouží níže uvedený postup. Detailní zpracování těchto kroků bude provedeno v následujících podkapitolách.

1. Zpracování soupisu rizik.
2. Sestavení tabulky souvztažností rizik.
3. Vyplnění tabulky souvztažností rizik.
4. Vytvoření součtů souvztažnosti rizik.
5. Výpočet koeficientu aktivity a pasivity jednotlivých rizik.
6. Grafické vyhodnocení rizik.
7. Výpočet os koeficientů aktivity a pasivity.
8. Vyhodnocení analýzy KARS.

8.1.1 Soupis rizik

První krok spočívá v identifikaci rizik. První krok analýzy rizik je vytvoření soupisu rizik. Měl by být co nejvíce obsáhlý a podrobný pro odpovídající hodnotu analýzy rizik (Jelšovská a Peterková, 2013), (Košťál, 2015).

Identifikace rizik byla provedena na základě brainstormingu s IT odborníky vybraných nemocnic a metody What-If, kde se jedná o analýzu otázky *„Co se stane, když…?“*.

Identifikace představuje následující rizika:

1. Kybernetický útok.
2. Ransomware.
3. Spear-phishing.
4. Přerušení provozu.
5. Únik citlivých dat.
6. Odcizení dat.
7. Selhání SW.
8. Selhání HW.
9. Selhání lidského faktoru.
10. Neautorizovaný přístup do systému.
11. Selhání zabezpečení sítě.
12. Otevření nakažené přílohy.
13. Zašifrování souborů.
14. Finanční ztráta.
15. Narušení dostupnosti dat.
16. Narušení důvěrnosti dat.
17. Narušení integrity dat.

8.1.2 Sestavení a vytvoření tabulky souvztažností rizik

Dalším krokem je sestavení tabulky souvztažnosti rizik do podoby matice, kde počet řádků a sloupců je roven počtu všech identifikovaných rizik.

Tabulka je vyplněna následovně:

a) Riziko R_i nemůže vyvolat samo sebe, na hlavní diagonále matice budou pro všechna rizika $r_{ij} = 0$ (pro $i = j$).

b) Pro vyplnění dalších pozic postupujeme po řádcích zleva doprava. Do pozic r_{ij} (pro $i \neq j$) vyplníme hodnoty:

1 – reálná možnost, že riziko R_i může vyvolat riziko R_j,

0 – v případě, že riziko R_i nevyvolá riziko R_j.

Dalším krokem analýzy je doplnění tabulky o jeden řádek a sloupec. Tyto pozice budou představovat součty jednotlivých řádků a sloupců. Tím se získá výsledná podoba tabulky souvztažnosti rizik, která se dále použije pro výpočet koeficientu aktivity a pasivity (Jelšovská a Peterková, 2013), (Košťál, 2015).

Souvztažnost výše identifikovaných rizik zobrazuje následující tabulka č. 13.

Tab. 13 – Tabulka souvztažností rizik

Riziko	**1.**	**2.**	**3.**	**4.**	**5.**	**6.**	**7.**	**8.**	**9.**	**10.**	**11.**	**12.**	**13.**	**14.**	**15.**	**16.**	**17.**	**$\sum K_{ARi}$**
1. Kybernetický útok	0	1	1	1	1	1	1	1	1	1	1	0	0	1	1	1	1	**14**
2. Ransomware	0	0	0	1	1	1	1	1	0	1	1	0	1	1	1	1	1	**12**
3. Spear-phishing	1	1	0	1	1	1	1	0	1	1	1	1	0	1	1	1	1	**14**
4. Přerušení provozu	0	0	0	0	0	1	0	1	0	1	0	0	0	1	1	0	0	**5**
5. Únik citlivých dat	0	0	0	0	0	1	1	0	0	1	0	0	0	1	1	1	1	**7**
6. Odcizení dat	0	0	0	1	1	0	1	0	1	1	0	0	0	1	1	1	1	**9**
7. Selhání SW	1	1	1	1	1	1	0	1	0	1	1	0	1	1	1	1	1	**14**
8. Selhání HW	0	0	0	1	0	0	1	0	0	0	0	0	0	1	1	0	0	**4**
9. Selhání lidského faktoru	1	1	1	1	1	1	1	1	0	1	1	1	0	0	1	1	1	**14**
10. Neautorizovaný přístup do systému	0	1	0	1	1	1	1	0	1	0	0	1	1	0	1	1	1	**11**
11. Selhání zabezpečení sítě	1	1	1	0	1	1	0	0	0	1	0	1	0	0	1	0	0	**8**
12. Otevření nakažené přílohy	0	1	0	1	1	1	0	1	1	1	0	0	1	1	1	1	0	**11**
13. Zašifrování souborů	0	0	0	1	1	1	0	0	0	0	0	0	0	1	1	1	1	**7**
14. Finanční ztráta	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**0**
15. Narušení dostupnosti dat	0	0	0	1	0	1	0	0	0	0	0	0	0	1	0	1	1	**5**
16. Narušení důvěrnosti dat	0	0	0	1	1	1	1	0	1	1	0	0	0	0	1	0	1	**8**
17. Narušení integrity dat	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	**2**
$\sum K_{PRi}$	**4**	**7**	**4**	**12**	**11**	**13**	**9**	**6**	**6**	**11**	**5**	**4**	**4**	**11**	**15**	**12**	**11**	

Zdroj: (Jelšovská a Peterková, 2013), (Řízený rozhovor, 2021), zpracování: (autorka práce).

8.1.3 Výpočet koeficientů aktivity a pasivity

Cílem analýzy KARS je posouzení přítomných rizik, ke kterému se využijí právě koeficienty aktivity a pasivity. Pro vyjádření koeficientu aktivity a pasivity bylo nezbytné sestavit počet kombinací. Jedním z předpokladů bylo, že riziko R_i nemůže vyvolat samo sebe, avšak může nastat situace, kdy riziko R_i vyvolá riziko další nebo může být vyvoláno na základě působením jiných rizik. V případě této práce se počet rizik rovná x = 17 a počet možných kombinací vyjádřen jako x – 1 z toho důvodu, že se riziko samo o sobě nemůže vyvolat. Dle výše zmíněného se tedy jedná o: x – 1, tedy 17 – 1 = 16. Výpočty jednotlivých koeficientů jsou uvedeny níže.

- **Koeficient aktivity –** K_{ARi} (procentuální vyjádření počtu závažných rizik, která mohou být vyvolána působením rizika R_i.
- **Koeficient pasivity –** K_{PRi} (procentuální vyjádření počtu rizik, která mohou vyvolat působení rizika R_i (Jelšovská a Peterková, 2013).

Výpočet koeficientu aktivity K_{ARi} pro jednotlivá rizika R_i:

$$K_{ARi} = \frac{\sum R_i}{x-1} \,.\, 100\ [\%] \qquad (1)$$

1. $K_{ARi} = \frac{\sum R_i}{x-1} \,.\, 100\ [\%] = \frac{14}{17-1} \,.\, 100 = \frac{14}{16} \,.\, 100 = 87{,}5\ \%$
2. $K_{ARi} = \frac{\sum R_i}{x-1} \,.\, 100\ [\%] = \frac{12}{17-1} \,.\, 100 = \frac{12}{16} \,.\, 100 = 75\ \%$
3. $K_{ARi} = \frac{\sum R_i}{x-1} \,.\, 100\ [\%] = \frac{14}{17-1} \,.\, 100 = \frac{14}{16} \,.\, 100 = 87{,}5\ \%$
4. $K_{ARi} = \frac{\sum R_i}{x-1} \,.\, 100\ [\%] = \frac{5}{17-1} \,.\, 100 = \frac{5}{16} \,.\, 100 = 31{,}25\ \%$
5. $K_{ARi} = \frac{\sum R_i}{x-1} \,.\, 100\ [\%] = \frac{7}{17-1} \,.\, 100 = \frac{7}{16} \,.\, 100 = 43{,}75\ \%$
6. $K_{ARi} = \frac{\sum R_i}{x-1} \,.\, 100\ [\%] = \frac{9}{17-1} \,.\, 100 = \frac{9}{16} \,.\, 100 = 56{,}25\ \%$
7. $K_{ARi} = \frac{\sum R_i}{x-1} \,.\, 100\ [\%] = \frac{14}{17-1} \,.\, 100 = \frac{14}{16} \,.\, 100 = 87{,}5\ \%$
8. $K_{ARi} = \frac{\sum R_i}{x-1} \,.\, 100\ [\%] = \frac{4}{17-1} \,.\, 100 = \frac{4}{16} \,.\, 100 = 25\ \%$
9. $K_{ARi} = \frac{\sum R_i}{x-1} \,.\, 100\ [\%] = \frac{14}{17-1} \,.\, 100 = \frac{14}{16} \,.\, 100 = 87{,}5\ \%$
10. $K_{ARi} = \frac{\sum R_i}{x-1} \,.\, 100\ [\%] = \frac{11}{17-1} \,.\, 100 = \frac{11}{16} \,.\, 100 = 68{,}75\ \%$

11. $K_{ARi} = \frac{\sum R_i}{x-1} . 100\ [\%] = \frac{8}{17-1} . 100 = \frac{8}{16} . 100 = 50\ \%$

12. $K_{ARi} = \frac{\sum R_i}{x-1} . 100\ [\%] = \frac{11}{17-1} . 100 = \frac{11}{16} . 100 = 68{,}75\ \%$

13. $K_{ARi} = \frac{\sum R_i}{x-1} . 100\ [\%] = \frac{7}{17-1} . 100 = \frac{7}{16} . 100 = 43{,}75\ \%$

14. $K_{ARi} = \frac{\sum R_i}{x-1} . 100\ [\%] = \frac{0}{17-1} . 100 = \frac{0}{16} . 100 = 0\ \%$

15. $K_{ARi} = \frac{\sum R_i}{x-1} . 100\ [\%] = \frac{5}{17-1} . 100 = \frac{5}{16} . 100 = 31{,}25\ \%$

16. $K_{ARi} = \frac{\sum R_i}{x-1} . 100\ [\%] = \frac{8}{17-1} . 100 = \frac{8}{16} . 100 = 50\ \%$

17. $K_{ARi} = \frac{\sum R_i}{x-1} . 100\ [\%] = \frac{2}{17-1} . 100 = \frac{2}{16} . 100 = 12{,}5\ \%$

Výpočet koeficientu pasivity K_{PRi} pro jednotlivá rizika Ri:

$$K_{PRi} = \frac{\sum \boldsymbol{R_i}}{\boldsymbol{x-1}} . 100\ [\%] \qquad (2)$$

1. $K_{PRi} = \frac{\sum R_i}{x-1} . 100\ [\%] = \frac{4}{17-1} . 100 = \frac{4}{16} . 100 = 25\ \%$

2. $K_{PRi} = \frac{\sum R_i}{x-1} . 100\ [\%] = \frac{7}{17-1} . 100 = \frac{7}{16} . 100 = 43{,}75\ \%$

3. $K_{PRi} = \frac{\sum R_i}{x-1} . 100\ [\%] = \frac{4}{17-1} . 100 = \frac{4}{16} . 100 = 25\ \%$

4. $K_{PRi} = \frac{\sum R_i}{x-1} . 100\ [\%] = \frac{12}{17-1} . 100 = \frac{12}{16} . 100 = 75\ \%$

5. $K_{PRi} = \frac{\sum R_i}{x-1} . 100\ [\%] = \frac{11}{17-1} . 100 = \frac{11}{16} . 100 = 68{,}75\ \%$

6. $K_{PRi} = \frac{\sum R_i}{x-1} . 100\ [\%] = \frac{13}{17-1} . 100 = \frac{13}{16} . 100 = 81{,}25\ \%$

7. $K_{PRi} = \frac{\sum R_i}{x-1} . 100\ [\%] = \frac{9}{17-1} . 100 = \frac{9}{16} . 100 = 56{,}25\ \%$

8. $K_{PRi} = \frac{\sum R_i}{x-1} . 100\ [\%] = \frac{6}{17-1} . 100 = \frac{6}{16} . 100 = 37{,}5\ \%$

9. $K_{PRi} = \frac{\sum R_i}{x-1} . 100\ [\%] = \frac{6}{17-1} . 100 = \frac{6}{16} . 100 = 37{,}5\ \%$

10. $K_{PRi} = \frac{\sum R_i}{x-1} . 100\ [\%] = \frac{11}{17-1} . 100 = \frac{11}{16} . 100 = 68{,}75\ \%$

11. $K_{PRi} = \frac{\sum R_i}{x-1} . 100\ [\%] = \frac{5}{17-1} . 100 = \frac{5}{16} . 100 = 31{,}25\ \%$

12. $K_{PRi} = \frac{\sum R_i}{x-1} . 100\ [\%] = \frac{4}{17-1} . 100 = \frac{4}{16} . 100 = 25\ \%$

13. $K_{PRi} = \frac{\sum R_i}{x-1} . 100\ [\%] = \frac{4}{17-1} . 100 = \frac{4}{16} . 100 = 25\ \%$

14. $K_{PRi} = \frac{\sum R_i}{x-1} . 100\ [\%] = \frac{11}{17-1} . 100 = \frac{11}{16} . 100 = 68{,}75\ \%$

15. $K_{PRi} = \frac{\sum R_i}{x-1} . 100\ [\%] = \frac{15}{17-1} . 100 = \frac{15}{16} . 100 = 93{,}75\ \%$

16. $K_{PRi} = \frac{\sum R_i}{x-1} . 100\ [\%] = \frac{12}{17-1} . 100 = \frac{12}{16} . 100 = 75\ \%$

17. $K_{PRi} = \frac{\sum R_i}{x-1} . 100\ [\%] = \frac{11}{17-1} . 100 = \frac{11}{16} . 100 = 68{,}75\ \%$

Níže uvedená tabulka zobrazuje hodnoty koeficientů aktivity a pasivity, které jsou stěžejní pro výsledný graf s vymezenými oblastmi (oblast I. – IV.). Pro dosažení výsledného grafu byly uvedené hodnoty doplněny do tabulkového programu Microsoft Excel, který následně vygeneroval graf.

Tab. 14 – Koeficienty aktivity a pasivity

P. č.	Riziko	K_{ARi} [%]	K_{PRi} [%]
1.	Kybernetický útok	**87,5**	**25**
2.	Ransomware	**75**	**43,75**
3.	Spear-phishing	**87,5**	**25**
4.	Přerušení provozu	**31,25**	**75**
5.	Únik citlivých dat	**43,75**	**68,75**
6.	Odcizení dat	**56,25**	**81,25**
7.	Selhání SW	**87,5**	**56,25**
8.	Selhání HW	**25**	**37,5**
9.	Selhání lidského faktoru	**87,5**	**37,5**
10.	Neautorizovaný přístup do systému	**68,75**	**68,75**
11.	Selhání zabezpečení sítě	**50**	**31,25**
12.	Otevření nakažené přílohy	**68,75**	**25**
13.	Zašifrování souborů	**43,75**	**25**
14.	Finanční ztráta	**0**	**68,75**
15.	Narušení dostupnosti dat	**31,25**	**93,75**
16.	Narušení důvěrnosti dat	**50**	**75**
17.	Narušení integrity dat	**12,5**	**68,75**

Zdroj: (autorka práce).

8.1.4 Výsledný graf souvztažností rizik

Hlavním cílem vyhodnocení grafu souvztažností je stanovení významnosti (rizikovosti) jednotlivých rizik dle jejich souvztažností s ostatními riziky. Graf představuje 4 oblasti (kvadranty), které rozdělují dvě osy, a to **O₁** a **O₂**. Níže jsou uvedeny zmíněné oblasti rizik:

I. Oblast **primárně i sekundárně** nebezpečných rizik.

II. Oblast **sekundárně** nebezpečných rizik.

III. Oblast **primárně** nebezpečných rizik.

IV. Oblast **relativně bezpečná**.

Ze všeho nejdřív je nezbytné určit, jaká rizika budou pokrývat kterou oblast. Pro I. oblast (primárně i sekundárně nebezpečných rizik) se doporučuje pokrytí 80 % z celkových rizik. Ve výsledném grafu je osa **O₁** sestrojena jako kolmice na osu *x* a osa **O₂** na osu *y.* Níže jsou uvedeny výpočty pro sestrojení uvedených os (Jelšovská a Peterková, 2013), (Košťál, 2015).

Vzorce pro výpočet os **O₁** (koeficient aktivity) a **O₂** (koeficient pasivity):

$$O_1 = K_{Amax} - \frac{K_{Amax} - K_{Amin}}{100} \cdot 80 \qquad (3)$$

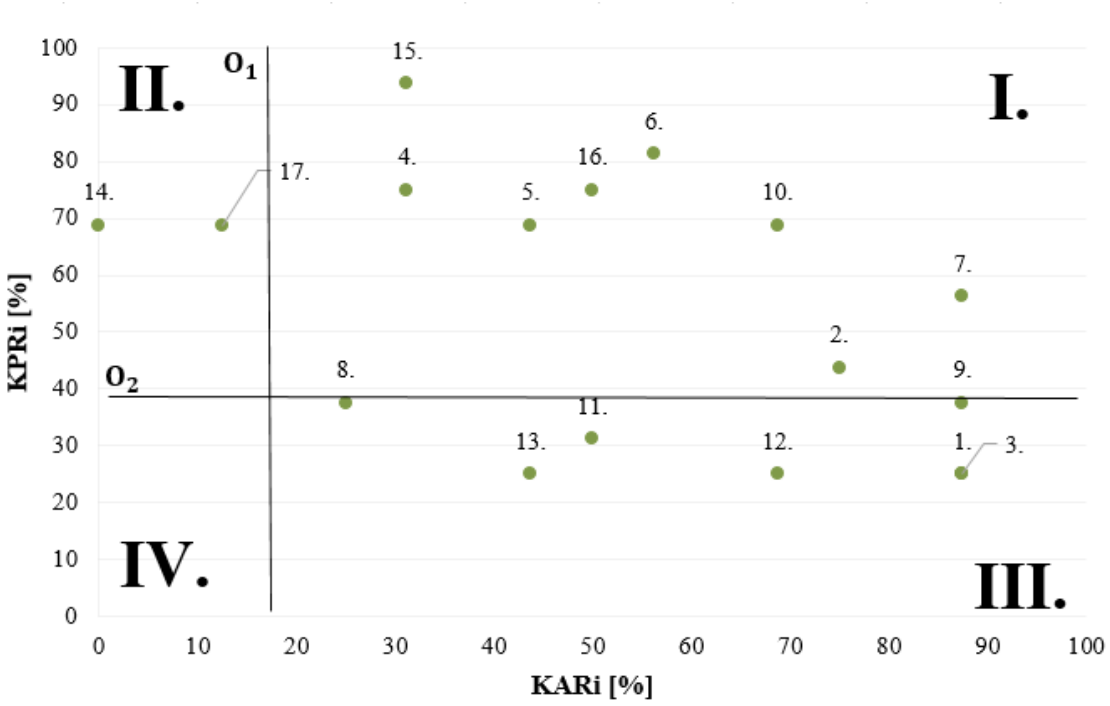
$$O_1 = 87{,}5 - \frac{87{,}5-0}{100} \cdot 80 = 87{,}5 - 70 = \underline{\mathbf{17{,}5}}$$

$$O_2 = K_{Pmin} - \frac{K_{Pmax} - K_{Pmin}}{100} \cdot 80 \qquad (4)$$

$$O_2 = 93{,}75 - \frac{93{,}75-25}{100} \cdot 80 = 93{,}75 - 55 = \underline{\mathbf{38{,}75}}$$

Dle předchozího výpočtu jsou do grafu souvztažností rizik umístěny na osu **O₁** a **O₂** uvedené výsledky. Pro osu **O₁** to bude v bodě **17,5** na ose *x* a osa **O₂** v bodě **38,75** na ose *y.*

Grafické zobrazení je zpracováno v již zmíněném tabulkovém programu Microsoft Excel z důvodu přehlednosti výsledků získaných z předchozích kroků. Výsledkem metody je graf souvztažností rizik zpracovaný na základě údajů z tabulky koeficientů aktivity a pasivity. Graf vykresluje rozdělení rizik podle jejich souvztažností s ostatními riziky. Konečný výsledek s vyznačenými kvadranty zobrazuje *Obr. 3 – Výsledný graf souvztažností rizik* (Jelšovská a Peterková, 2013), (Košťál, 2015).



Obr. 3 – Výsledný graf souvztažností rizik. Zdroj: (autorka práce).

8.1.5 Shrnutí získaných výsledků jednotlivých oblastí

Cílem vyhodnocení grafu souvztažností rizik bylo stanovení významnosti jednotlivých rizik dle souvztažností jiných rizik v daném systému. Následovalo rozdělení do 4 základních oblastí, a to na základě os **O1** a **O2**. Oblasti zobrazují významnost stanovených rizik, které se v nich nacházejí (Košťál, 2015). Přičemž **IV. oblast** neobsahuje riziko žádné.

I. Oblast primárně i sekundárně nebezpečných rizik

Do této oblasti spadají následující rizika: 2. ransomware, 4. přerušení provozu, 5. únik citlivých dat, 6. odcizení dat, 7. selhání SW, 10. neautorizovaný přístup do systému, 15. narušení dostupnosti dat a 16. narušení důvěrnosti dat. Pro tuto oblast jsou rizika vyznačována tím, že mohou představovat důsledek i příčinu. Působení těchto rizik může být vysvětleno tak, že spouštějí další rizika a v tomto případě mohou vést až například k přerušení celého provozu nemocničního zařízení. Což je spojeno s narušením dostupnosti dat, kde se odpovědné osoby nemohou dostat k potřebným datům o pacientech, což může představovat komplikace ve vyšetření apod. Z hlediska narušení důvěrnosti se jedná o to, že má k datům přístup neoprávněná osoba, která může tato data neúmyslně či úmyslně poškodit. V neposlední řadě se může jednat o odcizení (krádež) dat nebo jejich únik pro konkrétní účely. Tato rizika lze shrnout tak, že se navzájem ovlivňují z obou stran.

II. Oblast sekundárně nebezpečných rizik

Oblast zahrnuje tato rizika: 14. finanční ztráta a 17. narušení integrity. Riziko v podobě narušení integrity, tedy modifikaci dat může vést k tomu, že pozměněná data způsobí jednak narušení důvěrnosti dat, tedy že k datům má přístup neoprávněná osoba a tudíž lze uvažovat o vzniku dalších rizik. Především pak z toho důvodu, že není zdravotnictví dostatečně financováno a kybernetická bezpečnost dost možná bývá podhodnocena, může dojít k výše identifikovaným rizikům, která dojdou až do bodu přerušení provozu, což souvisí s finanční ztrátou. Zabezpečení IT v rámci celého nemocničního zařízení pak představuje velice nákladnou investici, avšak dopad na zdraví pacientů v případě přerušení provozu může být nevyčíslitelný. Nedostatek finančních prostředků mnohdy představuje zastaralé IS a technologie, které jsou daleko zranitelnější vůči kybernetickým hrozbám. Zvláště pak v situacích, jakou představuje například koronavirová pandemie, kde je otázka kybernetické bezpečnosti opomíjena v důsledku zvýšené zatíženosti nemocničních zařízení.

III. Oblast primárně nebezpečných rizik

Do této oblasti spadají následující rizika: 1. kybernetický útok, 3. spear-phishing, 8. selhání HW, 9. selhání lidského faktoru, 11. selhání zabezpečení sítě, 12. otevření nakažené přílohy a 13. zašifrování souborů. Typickým rysem těchto rizik je to, že mohou předatovat latentní riziko, to znamená, že jejich dopad je zjištěn až po uplynutí určité časové doby. Je třeba si ale uvědomit, do jaké míry je určité riziko provedeno. Například co se týká selhání HW, to je zaznamenáno ihned po jejich selhání. Avšak zašifrování souborů v důsledku otevřené nakažené přílohy z e-mailu se může projevit až v případě, kdy zašifrované soubory potřebujeme. V případě spear-phishingu se může jednat o snadný útok, kdy stačí malá nepozornost uživatele (pracovníka) a zjednodušeně řečeno stačí jedno kliknutí, které nemocnici dělí od jejího ochromení. Selhání lidského faktoru hraje nejvýznamnější roli v kyberprostoru.

Předcházet výše uvedeným rizikům je možné v případě, že jsou dodržována určitá bezpečnostní pravidla. Avšak každé opatření představuje slabé místo a využije zranitelnosti aktiva, který má pak větší či menší dopad. Na základě známých kybernetických útoků na nemocniční zařízení lze poukázat na to, že způsobují jednak finanční škody, ale mají dopad i na zdraví pacientů, které je značně ohroženo v případě přerušení provozu. To představuje přesun pacienta, kde rychlost přesunu souvisí se zdravotním stavem pacienta.

8.2 RISKAN

Nástroj vytvořený společností T-Soft a.s. Nástroj slouží pro sestavení semi-kvantitativní analýzy rizik. Tento rizikový kalkulátor pracuje se třemi základními prvky: aktiva, hrozby a zranitelnost, kde se posuzuje zranitelnost jednotlivých aktiv vůči jednotlivým hrozbám. Hodnocení se provádí dle stupnice hodnot definovaných předem dle hodnotitele, kde se stanoví: rozsah hodnot aktiv (0–5), rozsah hrozeb (0–6) a rozsah zranitelností (0–3). Dále se v textovém editoru vytvoří seznam aktiv a hrozeb (Šaur, 2014).

V rámci samotné analýzy byly vytvořeny seznamy aktiv a hrozeb. Dále se jednalo o vytvoření číselníků pro hodnocení aktiv, hrozeb a zranitelností. Na základě číselníků byly ohodnoceny jednotlivé zranitelnosti vztahující se na vztah hrozba-aktivum. Aktiva jsou vybrána v souvislosti s vybranými nemocničními zařízeními. Identifikace aktiv a hrozeb je blíže specifikována v kapitole 6 a 7.

8.2.1 Vyhodnocení zranitelností

Jak je uvedeno výše, bylo nezbytné nejprve vyhodnotit zranitelnost na základě vztahu hrozba-aktivum. Kvantifikace zranitelností aktiv byla stanovena na základě níže uvedených hodnot:

- 0 – žádná zranitelnost aktiva,
- 1 – nízká zranitelnost aktiva,
- 2 – střední zranitelnost aktiva,
- 3 – vysoká zranitelnost aktiva.

Dle výše uvedených hodnot byly v tabulkovém programu Microsoft Excel vyhodnoceny zranitelnosti v rámci vymezených hrozeb. Stanovení hodnot se odvíjelo od významnosti jednotlivých aktiv pro nemocniční zařízení a identifikovaných hrozeb na základě příslušné normy viz *Obr. č. 4 – Vyhodnocení zranitelností aktiv*.

RISKAN RIZIKOVÝ KALKULÁTOR T-SOFT			Aktiva	AKTIVA - CELKEM	Primární aktiva	Procesy a činnosti	Zdravotní dokumentace	Informační systémy	Správa IT	Manažer kybernetické b	Architekt kybernetické b	Auditor kybernetické bez	Informace	Dokumentace	Osobní údaje pacienta	Podpůrná aktiva	Hardware	Software	Osoby	Organizace
			Hodnoty aktiv	5	5	5	5	5	5	4	4	4	5	5	5	4	4	4	4	4
				velmi vysoká	velmi vysoká	velmi vysoká	velmi vysoká	velmi vysoká	velmi vysoká	vysoká	vysoká	vysoká	velmi vysoká	velmi vysoká	velmi vysoká	vysoká	vysoká	vysoká	vysoká	vysoká
Hrozby		Pravděpodobnost																		
HROZBY - CELKEM		5	velmi vysoká	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
1	Lidské neúmyslné - selhání	4	vysoká	3	3	3	3	3	3	3	2	2	3	3	3	3	3	3	3	3
1.1	Ztráta důvěrnosti/integrity dat	3	střední	3	3	3	3	3	3	2	2	2	3	3	3	2	2	2	2	2
1.2	Zničení PC vybavení	1	zanedbatelná	3	3	3	3	3	3	2	2	2	3	3	3	2	2	2	2	2
1.3	Nevhodné užívání IT systému	2	nízká	3	3	3	3	3	3	1	2	1	3	3	3	2	2	2	2	2
1.4	Neúmyslná manipulace s daty	2	nízká	3	3	3	3	2	2	2	2	2	3	3	3	2	2	2	2	2
1.5	Neautorizované použití IS	2	nízká	3	3	3	3	3	2	2	2	1	3	3	3	2	2	2	2	2
1.6	Nesprávná segmentace sítě	2	nízká	3	3	2	1	1	2	2	2	1	3	3	3	3	2	3	2	2
1.7	Pochybení zaměstnanců	4	vysoká	3	3	2	2	2	2	2	2	1	3	3	3	2	1	1	2	2
1.8	Spuštění škodlivého kódu	3	střední	3	3	3	3	3	3	3	2	1	3	3	3	3	3	3	3	3
1.9	Neautorizované užití nebo stažen	3	střední	2	2	2	2	2	1	1	2	1	2	2	2	2	2	2	2	2
1.10	Vyzrazení citlivých údajů pacient	2	nízká	3	3	2	0	0	0	0	2	0	3	0	3	3	0	0	3	2
2	Lidské neúmyslné - organizační	4	vysoká	3	3	3	3	3	3	3	2	2	3	3	3	3	3	3	2	2
2.1	Nedostatek personálu	4	vysoká	2	2	2	1	1	2	2	2	2	2	1	2	2	0	0	2	2
2.2	Minimální bezpečnostní povědom	3	střední	3	3	3	1	1	3	2	2	2	2	0	2	2	2	2	1	1
2.3	Nesprávné přidělení odpovědnos	2	nízká	3	3	2	0	2	1	1	1	0	3	3	3	1	1	1	0	0
2.4	Neformální postup při autorizaci	2	nízká	2	2	2	1	1	0	0	2	0	2	2	2	0	0	0	0	0
2.5	Nízká kvalifikace zaměstnanců	2	nízká	2	2	2	0	0	2	2	2	0	2	0	2	2	0	0	2	2
2.6	Neautorizované chování zaměst	2	nízká	2	2	2	0	0	2	2	2	2	2	2	2	2	2	2	1	1
2.7	Nedostatečné školení bezpečnos	3	střední	3	3	3	3	3	2	3	1	0	3	3	3	2	2	2	1	1
2.8	Nedostatečná bezpečnostní prav	3	střední	3	2	2	2	2	2	2	2	0	2	2	2	3	3	3	2	2
3	Lidské úmyslné - poškození	5	velmi vysoká	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
3.1	Záměrná manipulace s daty	2	nízká	3	3	3	3	3	2	2	2	2	3	3	3	3	0	0	3	2
3.2	Záměrná manipulace s IS	2	nízká	3	3	3	3	3	3	2	2	2	3	3	3	3	0	3	1	1
3.3	Neautorizovaný přístup do systé	3	střední	3	3	3	3	3	3	2	2	2	3	3	3	3	0	3	3	2
3.4	Neautorizované použití systému	3	střední	3	3	3	2	3	3	2	2	2	2	2	2	3	2	3	0	0
3.5	Zneužití uživatelských práv	2	nízká	3	3	3	2	3	3	3	1	2	3	3	3	3	1	1	3	1
3.6	Kybernetický útok	5	velmi vysoká	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
3.7	Spear-phishing	5	velmi vysoká	3	3	1	1	1	0	1	1	1	3	3	3	3	3	3	3	3
3.8	Ransomware	5	velmi vysoká	3	3	3	3	3	3	3	3	2	3	3	3	3	3	3	3	3
3.9	Zneužití citlivých dat	5	velmi vysoká	3	3	3	3	0	1	1	1	0	3	3	3	3	0	0	3	3
3.10	Zničení zařízení nebo médií	4	vysoká	3	3	3	3	3	2	1	1	1	3	3	3	3	3	3	0	0
4	Technické selhání	5	velmi vysoká	3	3	3	3	3	3	2	2	1	3	3	3	3	3	3	2	3
4.1	Bezpečnostní mezery v systému	5	velmi vysoká	3	3	1	0	0	0	0	1	0	3	0	3	3	3	3	0	2
4.2	Nechráněné přenosy dat	4	vysoká	3	3	2	2	2	1	1	1	1	3	3	3	3	3	3	0	2
4.3	Neprovedená aktualizace	2	nízká	3	2	2	2	2	0	0	2	0	2	2	2	3	3	3	0	2
4.4	Chybná záloha dat	2	nízká	3	3	3	3	0	0	0	1	0	0	0	0	0	0	0	0	0
4.5	Přerušení dodávky el. energie	3	střední	3	1	1	0	0	0	0	1	0	0	0	0	3	3	3	0	3
4.6	Nefunkčnost zařízení	2	nízká	3	3	3	2	3	3	2	2	0	2	2	2	3	3	3	0	3
4.7	Nefunkčnost SW	2	nízká	3	3	3	2	3	3	1	1	0	0	0	0	3	3	3	2	0
4.8	Poškození nosiče dat	2	nízká	2	2	2	2	2	1	0	1	0	0	0	0	0	0	0	0	0
4.9	Výpadek interní sítě	3	střední	3	3	3	3	3	2	2	1	0	2	2	2	3	1	3	2	2
4.10	Chyba šifrování	3	střední	3	3	2	2	1	1	1	1	0	3	3	3	1	1	1	1	1
4.11	Porucha odeslání zprávy	2	nízká	3	3	3	0	3	1	1	1	0	3	3	3	2	2	2	2	2
5	Přírodní	3	střední	3	3	3	3	3	3	1	1	0	3	3	3	3	3	2	2	0
5.1	Blesk	3	střední	3	3	3	3	3	3	0	0	0	3	3	3	2	2	2	0	0
5.2	Požár	2	nízká	3	3	3	3	2	1	1	1	0	2	2	2	2	2	2	0	0
5.3	Voda	1	zanedbatelná	3	3	3	3	3	2	0	0	0	3	3	3	3	3	0	0	0
5.4	Prach	1	zanedbatelná	2	1	1	1	1	1	0	0	0	1	1	1	2	0	0	2	0

Obr. 4 – Vyhodnocení zranitelnosti aktiv. Zdroj: (ČSN ISO/IEC 27005, 2019), (Řízený rozhovor, 2021).

8.2.2 Vyhodnocení analýzy rizik

Po vytvoření těchto seznamů se SW RISKAN vygenerujte do programu Microsoft Excel, kde se následně stanoví hodnoty jednotlivě pro daná aktiva (0–6) a hrozeb (0–5) dle jejich významnosti. Poté se posoudí zranitelnost aktiv vůči každé hrozbě (0–3). Výsledné riziko je pak vyjádřeno jako součin dle následujícího vzorce:

$$R = A * H * Z \tag{5}$$

kde:

- R – výsledné riziko.
- A – hodnota aktiva.
- H – pravděpodobnost vzniku hrozby.
- Z – zranitelnost aktiv.

Dle konečné hodnoty výsledků rizika je ve výsledné matici (viz *Obr. 5 – Výsledná matice rizik*) stanoveno barevné rozlišení pro:

- Nízké riziko (zelená brava).
- Střední riziko (žlutá brava).
- Vysoké riziko (červená barva).

Na níže uvedeném obrázku lze pozorovat, jakou míru ohrožení v souvislosti s vyznačenými barvami představuje jaká hrozba pro analyzovaný objekt. Především pak ty, které jsou vyznačené červenou barvou, budou sloužit pro další řízení rizik, tedy návrhu vhodných opatření. Takto vyznačené hrozby představující vysoké riziko jsou následující: kybernetický útok, spear-phishing, ransomware, zneužití citlivých dat, zničení zařízení nebo médií, což bylo z hlediska lidského úmyslného jednání. Technické selhání pak představovaly bezpečnostní mezery v systému, které mohou být příčinou například nedostatečné aktualizaci systému. Tyto hrozby jsou ve vztahu hrozba-aktivum, tudíž ty výše uvedené pak představují největší ohrožení v souvislosti s primárními aktivy, kterými jsou: zdravotní dokumentace, informační systémy a správa IT.

Na základě vyhodnocené analýzy v SW RISKAN můžeme pozorovat vztah hrozba-aktivum, kde pozorujeme do jaké míry, jaká hrozba ohrožuje aktivum. Naproti tomu v předešlé analýze rizik zase jednotlivé souvztažnosti rizik, tedy jak jedno riziko ovlivní další riziko.

Riskan RIZIKOVÝ KALKULÁTOR T-SOFT			Aktiva	AKTIVA - CELKEM	Primární aktiva	Procesy a činnosti	Zdravotní dokumentace	Informační systémy	Správa IT	Manažer kybernetické b	Architekt kybernetické b	Auditor kybernetické bez	Informace	Podpůrná aktiva	Hardware	Software	Osoby	Organizace
					PA	PČ	ZD	IS	SIT	MKB	AKB	AUKB	INF	SA	HW	SW	STF	ORG
			Hodnoty aktiv	5	5	5	5	5	5	4	4	4	5	4	4	4	4	4
Generátor grafů	Export do XML			velmi vysoká	velmi vysoká	velmi vysoká	velmi vysoká	velmi vysoká	velmi vysoká	vysoká	vysoká	vysoká	velmi vysoká	vysoká	vysoká	vysoká	vysoká	vysoká
Hrozby		Pravděpodobnost																
HROZBY - CELKEM		5	velmi vysoká	75	75	75	75	75	75	60	60	60	75	60	60	60	60	60
1	Lidské neúmyslné - selhání	4	vysoká	60	60	45	45	45	45	36	32	24	60	36	36	36	36	36
1.1	Ztráta důvěrnosti/integrity dat	3	střední	45	45	45	45	45	45	24	24	24	45	24	24	24	24	24
1.2	Zničení PC vybavení	1	zanedbatelná	15	15	15	15	15	15	8	8	8	15	8	8	8	8	8
1.3	Nevhodné užívání IT systému	2	nízká	30	30	30	30	30	30	8	16	8	30	16	16	16	16	16
1.4	Neúmyslná manipulace s daty	2	nízká	30	30	30	30	20	20	16	16	16	30	16	16	16	16	16
1.5	Neautorizované použití IS	2	nízká	30	30	30	30	30	20	16	16	8	30	16	16	16	16	16
1.6	Nesprávná segmentace sítě	2	nízká	30	30	20	10	10	20	16	16	8	30	24	16	24	16	16
1.7	Pochybení zaměstnanců	4	vysoká	60	60	40	40	40	40	32	32	16	60	32	16	16	32	32
1.8	Spuštění škodlivého kódu	3	střední	45	45	45	45	45	45	36	24	12	45	36	36	36	36	36
1.9	Neautorizované užití nebo stažen	3	střední	30	30	30	30	30	15	12	24	12	30	24	24	24	24	24
1.10	Vyzrazení citlivých údajů pacient	2	nízká	30	30	16	0	0	0	0	16	0	30	24	0	0	24	16
2	Lidské neúmyslné - organizační	4	vysoká	45	45	45	45	45	45	36	32	32	45	36	36	36	32	32
2.1	Nedostatek personálu	4	vysoká	40	40	40	20	20	40	32	32	32	40	32	0	0	32	32
2.2	Minimální bezpečnostní povědom	3	střední	45	45	45	15	15	45	24	24	24	30	24	24	24	12	12
2.3	Nesprávné přidělení odpovědnos	2	nízká	30	30	20	0	20	10	8	8	0	30	8	8	8	0	0
2.4	Neformální postup při autorizaci	2	nízká	20	20	16	10	10	0	0	16	0	20	0	0	0	0	0
2.5	Nízká kvalifikace zaměstnanců	2	nízká	20	20	20	0	0	20	16	16	0	20	16	0	0	16	16
2.6	Neautorizované chování zaměst	2	nízká	20	20	20	0	0	20	16	16	16	20	16	16	8	8	8
2.7	Nedostatečné školení bezpečnos	3	střední	45	45	45	45	45	30	36	12	0	45	24	24	24	12	12
2.8	Nedostatečná bezpečnostní prav	3	střední	36	30	30	30	30	30	24	24	0	30	36	36	36	24	24
3	Lidské úmyslné - poškození	5	velmi vysoká	75	75	75	75	75	75	60	60	60	75	60	60	60	60	60
3.1	Záměrná manipulace s daty	2	nízká	30	30	30	30	30	20	16	16	16	30	24	0	0	24	16
3.2	Záměrná manipulace s IS	2	nízká	30	30	30	30	30	30	16	16	16	30	24	0	24	8	8
3.3	Neautorizovaný přístup do systé	3	střední	45	45	45	45	45	45	24	24	24	45	36	0	36	36	24
3.4	Neautorizované použití systému	3	střední	45	45	45	30	45	45	24	24	24	30	36	24	36	0	0
3.5	Zneužití uživatelských práv	2	nízká	30	30	30	20	30	30	24	8	16	30	24	8	8	24	8
3.6	Kybernetický útok	5	velmi vysoká	75	75	75	75	75	75	60	60	60	75	60	60	60	60	60
3.7	Spear-phishing	5	velmi vysoká	75	75	25	25	25	0	20	20	20	75	60	60	60	60	60
3.8	Ransomware	5	velmi vysoká	75	75	75	75	75	75	60	60	40	75	60	60	60	60	60
3.9	Zneužití citlivých dat	5	velmi vysoká	75	75	75	75	0	25	20	20	0	75	60	0	0	60	60
3.10	Zničení zařízení nebo médií	4	vysoká	60	60	60	60	60	40	16	16	16	60	48	48	48	0	0
4	Technické selhání	5	velmi vysoká	75	75	45	45	45	30	24	20	16	75	60	60	60	24	40
4.1	Bezpečnostní mezery v systému	5	velmi vysoká	75	75	20	0	0	0	0	20	0	75	60	60	60	0	40
4.2	Nechráněné přenosy dat	4	vysoká	60	60	40	40	40	20	16	16	16	60	48	48	48	0	32
4.3	Neprovedená aktualizace	2	nízká	24	20	20	20	20	0	0	16	0	20	24	24	24	0	16
4.4	Chybná záloha dat	2	nízká	30	30	30	30	0	0	0	8	0	0	0	0	0	0	0
4.5	Přerušení dodávky el. energie	3	střední	36	12	12	0	0	0	0	12	0	0	36	36	36	0	36
4.6	Nefunkčnost zařízení	2	nízká	30	30	30	20	30	30	16	16	0	20	24	24	24	0	24
4.7	Nefunkčnost SW	2	nízká	30	30	30	20	30	30	8	8	0	0	24	24	24	16	0
4.8	Poškození nosiče dat	2	nízká	20	20	20	20	20	10	0	8	0	0	0	0	0	0	0
4.9	Výpadek interní sítě	3	střední	45	45	45	45	45	30	24	12	0	30	36	12	36	24	24
4.10	Chyba šifrování	3	střední	45	45	30	30	15	15	12	12	0	45	12	12	12	12	12
4.11	Porucha odeslání zprávy	2	nízká	30	30	30	0	30	10	8	8	0	30	16	16	16	16	16
5	Přírodní	3	střední	45	45	45	45	45	45	8	8	0	45	24	24	24	8	0
5.1	Blesk	3	střední	45	45	45	45	45	45	0	0	0	45	24	24	24	0	0
5.2	Požár	2	nízká	30	30	30	30	20	10	8	8	0	20	16	16	16	0	0
5.3	Voda	1	zanedbatelná	15	15	15	15	15	10	0	0	0	15	12	12	0	0	0
5.4	Prach	1	zanedbatelná	8	5	5	5	5	5	0	0	0	5	8	0	0	8	0

Obr. 5 – Výsledná matice rizik. Zdroj: (ČSN ISO/IEC 27005, 2019), (Řízený rozhovor, 2021).

9 NÁVRH OPATŘENÍ

Navrhovaná opatření vyplývají z předchozí analýzy rizik, podle kterých byla zjištěna rizika ohrožující vybrané objekty. Na základě toho bylo rozhodnuto o rozdělení na organizační a technická opatření, která jsou rozebrána dále v rámci plánu zvládání bezpečnostních incidentů v následující kapitole. Tato kapitola slouží pouze pro shrnutí zvolených opatření.

Pro případ, že dojde k selhání, napadení či zhroucení informačního systému v důsledku kybernetického útoku nebo v případě, kdy dojde k selhání nejslabšího článku v oblasti kybernetické bezpečnosti, a to lidského faktoru, je třeba brát v úvahu možná opatření. Lidský faktor je stěžejním prvkem pro zajištění bezpečného chodu celé nemocnice. Proto je bezpodmínečně nutné ošetřit rizika plynoucí z lidského selhání důsledným a efektivním bezpečnostním školením. Předmětem tohoto školení je především pojednání o důležitosti bezpečnosti informací, především tedy citlivých údajů, které jsou zpracovávány v nemocničním informačním systému či jak je snížena funkce nemocničního zařízení při poskytování zdravotnické péče pacientům v situaci, kdy nemá jednoduše přístup k těmto údajům. Z toho dále plyne, že rizika spojená s narušením dostupnosti, důvěrnosti a integrity dat spolu s poskytováním zdravotních služeb hraje v mnoha případech zásadní roli, především pak v době trvání znepřístupnění potřebných dat. Technická opatření pak shrnují určité kroky k ochraně před hrozícím útokem a v opačném případě jak na něj reagovat.

10 PLÁN ZVLÁDÁNÍ BEZPEČNOSNTÍCH INCIDENTŮ

Tato kapitola pojednává o obsahu plánu zvládání bezpečnostních incidentů, který je zaměřen především na zvládání kybernetických bezpečnostních incidentů. Plán byl vytvořen na základě provedených analýz a jejich vyhodnocení. Je rozdělen na dvě části, a to na organizační a technická opatření, které blíže specifikují jednotlivé činnosti ke zmírnění dopadu výsledných rizik. Tato část práce poskytuje detailní přehled výše uvedených opatření, která jsou určená nejen pro vedení nemocničních zařízení, ale zejména také pro personál, tedy zaměstnance (uživatele), kteří se dostávají dennodenně do kontaktu s IS/ITC.

Pro stanovení zvládání rizik byla využita opatření, která jsou definována normou ČSN ISO/IEC 27002. Tato norma jednotlivá opatření kategorizuje, které dále rozděluje. Pro potřeby této práce a z důvodu jejího rozsahu byla bezpečnostní opatření rozdělena dle ZoKB na organizační a technické opatření. Z hlediska organizačního zabezpečení se práce zaměřuje na bezpečnostní školení a bezpečnostní pokyny (zaměstnance) v souvislosti se spear-phishingem. Vybraná technická opatření se řídí dle výše uvedené normy například na ochranu před malwarem, aktualizace, zálohování apod.

Z hlediska organizačních opatření, která jsou určena především pro samotné zaměstnance a zodpovědné osoby, které za provedení níže uvedených činností zodpovídají. Je nutno určit zodpovědnou osobu za provádění pravidelných bezpečnostních školení v souvislosti s bezpečností informací. Řešení bezpečnosti informací z hlediska technického opatření se tato opírají o rešerši dostupných dokumentů. Tyto obsahují určitá řešení, která jsou určena především pro odborníky (správce) IT. Obsah a podoba jednotlivých opatření jsou uvedeny v následujících podkapitolách.

Je třeba brát na vědomí, že výše uvedená opatření musí být prováděna především se zaměřením na řízení kontinuity činností (dále jako „BCM“), kde je cílem zajistit spojitost a obnovu důležitých činností nemocničních zařízení, a to především v souladu se všemi schválenými medicínskými zásadami. V rámci BCM je právě zmíněný plán zvládání bezpečnostních incidentů. Tento plán se však zaměřuje pouze na vymezení jednotlivých organizačních a technických opatření. Prioritní činností je zachování zdravotních pracovníků z důvodu poskytování zdravotní péče pacientům.

Jde především o situaci, kdy nebudou mít zaměstnanci přístup k počítačům a dalším zařízením, které jsou určeny pro zpracovávání, evidenci a ukládání důležitých dat ohledně

pacienta. Na takovou situaci je nezbytné reagovat rychle a mít připravené procesy pro off-line řešení. To představuje dostatečné zásoby kancelářských potřeb, papírů a především informování o tom, kde jsou uloženy potřebné věci.

Tento plán má za cíl zvýšit povědomí o bezpečnosti informací, ve kterém je řešeno:

a) Poučení uživatelů o významnosti bezpečnosti informací.

b) Vstupní a pravidelné školení zaměstnanců.

c) Vymezení technických opatření.

10.1 Organizační opatření

Zajištění organizačního opatření představuje bezpečnostní školení. Toto školení je rozděleno do dvou částí na vstupní a pravidelné školení. Dále je stanovena forma a rozsah tohoto školení a osoby odpovídající za realizaci těchto činností. Z důvodu rozsahu tématu se tato práce omezuje pouze na některé oblasti z organizační bezpečnosti. Na základě rozdělení dle ZoKB se bude jednat o řízení lidských zdrojů a řízení kontinuity činností. Jednotlivá opatření jsou pak dále rozvedena v normě ČSN ISO/IEC 27002 – Soubor postupů pro opatření bezpečnosti informací. Jednotlivým výše uvedeným kategoriím jsou stanovena opatření dle příslušné normy.

Oblast bezpečnostních opatření definující požadavky na organizaci bezpečnosti informací, je rozdělena na dvě základní kategorie (ČSN ISO/IEC 27002, 2014):

1. **Interní organizace**
    a. Role a odpovědnosti bezpečnosti informací.
    b. Princip oddělení povinností.
    c. Kontakt s autoritami.
    d. Kontakt se zájmovými skupinami.
    e. Bezpečnost informací v řízení projektů.
2. **Mobilní zařízení a práce na dálku**
    a. Politika mobilních zařízení.
    b. Práce na dálku.

Ad. 1. Pro role a odpovědnosti byla zhotovena přehledná tabulka, která vymezuje jednotlivé činnosti a zodpovědné osoby za provedení těchto činností. Princip oddělení povinností pak řeší situace, kdy je potřebné snížit určité riziko úmyslného zneužití, a proto nesmí být tato činnost prováděna pouze jednou osobou. To může znamenat, že manažer KB má jiné povinnosti než například auditor KB. Kontakt s autoritami a zájmovými skupinami slouží k hlášení bezpečnostních incidentů, kde v tomto případě je otázka pomoci směřována na NÚKIB – vládní či národní CERT. Kontakt se zájmovými skupinami (např. ISACA) mohou posloužit k výměně zkušeností a také pomoc manažerům. Pozornost bezpečnosti informací by neměla být opomenuta ani při řešení různých projektů. To znamená pro vedoucího projektu zavedení KB mezi cíle projektu.

Ad. 2. Práce na dálku v nemocničním zařízení představují především mobilní zařízení v podobě mobilních telefonů, notebooků, tabletů, chytrých hodinek apod., které vykazují určitou zranitelnost vůči kybernetickým útokům a neměla by být proto opomenuta jejich bezpečnost. Zde je nutné zmínit i to, kdy je pracovník z patřičného oddělení (personální apod.) nucen pracovat z domu (současná koronavirová situace). Pro tyto situace je na místě věnovat náležitou pozornost pro vzdálený přístup. Proti rizikům je nutné prosadit jak organizační, tak technická opatření. Z hlediska organizační opatření se pak jedná o pravidelné bezpečnostní školení personálu (viz bezpečnostní školení), technickým opatřením je věnována další podkapitola – viz 10.4 Technická opatření.

10.2 Bezpečnostní školení

Školení o bezpečnosti informací vymezuje výše zmíněná norma v kapitole s názvem Bezpečnost lidských zdrojů. Každé nemocniční zařízení (veřejné či soukromé) vzhledem ke zpracovávání, evidování citlivých údajů pacienta by se měla edukaci zaměstnanců věnovat kontinuálně a věnovat mu náležitou pozornost. Školení by se pak mělo zaměřit na zaměstnance dle jejich významu pro zastávanou pracovní funkci. Tato podkapitola pojednává o bezpečnostním školení, které je rozděleno na dvě části:

- **Vstupní školení**

Předmětem vstupního školení by mělo být zejména seznámení s pracovním prostředím a pracovní činností. Je určena jednak pro nové pracovníky a jednak pro přesun na jinou funkci. Od pracovní funkce daného zaměstnance (personál, zaměstnanec IT) se pak dále odvíjí rozsah vědomostí o bezpečnosti informací, tzn. pro IT odborníka je školení zaměřeno spíše na technická opatření apod. Prvotní školení by mělo být na základě obecného hlediska:

a) Seznámení se a dodržování platných pravidel a povinností v oblasti bezpečnosti informací s ohledem na klasifikaci informací, ke kterým budou mít přístup.

b) Seznámení se s vlastní odpovědností za jednání a činnosti vzhledem k zachování důvěrnosti, integrity a dostupnosti dat.

c) Základní postupy při bezpečnostním incidentu (komu podávat hlášení) a dále dodržování bezpečnostních pravidel (heslová politika, prázdná pracovní plocha apod.).

d) Kontaktní místo s informacemi o dalším vzdělávání, poradenství v oblasti bezpečnosti informací apod.

e) Je nezbytné také uvědomit zaměstnance, proč je význam bezpečnosti informací důležitý pro pochopení cílů dané organizace s jejich možným pozitivním či negativním dopadem.

- **Pravidelné školení**

Primárním zaměřením tohoto školení by mělo být neustálé zvyšování povědomí bezpečnosti informací. Interval konání tohoto školení souvisí s nutností každého nemocničního zařízení. Na významnosti tohoto školení přidávají zejména hrozící útoky na tato zařízení. Vzdělávání uživatelů jakožto nejslabšího článku organizace (užití silných hesel, rozpoznání podvodných e-mailů, poučení o potenciálně nových hrozbách apod.).

10.3 Bezpečnostní povědomí

I když jsou zavedeny různé nejmodernější bezpečností nástroje, jejich význam se ztrácí ve chvíli, kdy jejich uživatelé nebudou schopni dodržovat daná pravidla chování v oblasti bezpečnosti informací a kybernetické bezpečnosti nebo vyzradí citlivá data, aniž by si ověřili, komu tyto citlivé údaje sdělují. Což může jednoznačně způsobit osobní selhání (vyčerpání) pracovníka. Pro předcházení podobným incidentům je nutné věnovat pozornost a všem uživatelům (zaměstnancům) neustále připomínat a vysvětlovat bezpečnostní principy a pravidla a seznamovat s možnými riziky, kterým dokáží účelně předcházet. Na základě toho může být posílena odolnost nejslabšího článku nejen v kybernetickém prostoru. Cílem je zajistit odpovídající a účinný přístup před bezpečnostními incidenty. Zaměstnanci by měli být povinní zaznamenat a následně hlásit jakékoliv bezpečnostní nedostatky. Níže jsou uvedeny základní bezpečnostní slabiny.

Zpozornit by měli především při těchto neobvyklých činnostech:

- Nestandardní chování IS.
- Zpomalení systému.
- Nemožnost přihlášení do systému.
- Chybné fungování technického a programového vybavení.
- Porušení přístupu.
- Lidské selhání – porušování nastavených pravidel, osobní selhání.

Personál nemocnic se může řídit dle níže uvedených bodů pro zvýšení bezpečnosti. Je však bráno na vědomí, že ne vždy, a ne všechna pravidla či pokyny lze vědomě dodržet. Při přetížení nemocničního zařízení je pozornost věnována zcela jistě na poskytování nezbytné zdravotní péče pro pacienta. Avšak pravidelným uvědomováním a dodržováním uvedených opatření se může zdraví či život pacientů zvýšit a bude tak sníženo riziko vzniku nežádoucích událostí, které ohrožují tento stav pacienta.

Desatero pro personál nemocnic v oblasti bezpečnosti informací

Níže uvedené doporučení představuje jedno z navržených opatření.

1. Neklikat bez rozmyšlení na příchozí e-mail, zejména tehdy, když žádný neočekávám.
2. V případě takového e-mailu nejlépe telefonicky ověřit u odesilatele odeslání zprávy.
3. Upozornit o možné hrozbě především vedení nemocnice či další osoby v blízkosti.
4. V případě otevření e-mailu neklikat na přiložené soubory (dále viz 2. bod).
5. Zpozornit by se mělo u rozsáhlých přípon souboru („txt.exe“ apod.).
6. Omezení sdílení citlivých údajů o pacientech (zejména nesdílet informace pacientovi „jen tak“ na chodbě, nýbrž ujistit se, že je informace sdělena pouze jemu).
7. V případě otevření potřebného souboru nepovolovat makra (soubory Microsoft Office).
8. Zpozornit v případě neobvyklých požadavků v obsahu e-mailu (v případě, kdy je požadováno zadání citlivých údajů apod.).
9. Komunikovat výhradně přes pracovní e-mail – tady platí totéž, co v bodě č. 2, tzn. zvýšená pozornost při příchozích e-mailech (adresa odesilatele se jeví věrohodně – zaměření se na tečky či překlepy v doméně: .cz, .eu apod.).

10. Řídit se výše uvedeným.

Osoby odpovědné za realizaci jednotlivých činností

V plánu bezpečnostního povědomí jsou stanoveny odpovědné osoby za realizaci jednotlivých činností v rámci školení personálu z hlediska organizační bezpečnosti. Tyto osoby a vymezení jejich rolí reprezentuje matice RACI zákonných bezpečnostních rolí (Bezouška, Švanda a Borej, 2019). Jednotlivé role jsou obecně popsány. Podrobnější klíčové činnosti jsou obsaženy ve VoKB, příloha 6.

Těmito osobami jsou:

a) Manažer KB

Odpovídá za systém řízení bezpečnosti informací. Výkon této role provádí vyškolená a odborně způsobilá osoba s praxí řízení KB nebo bezpečnosti informací.

b) Architekt KB

Zajišťuje návrh implementace bezpečnostních opatření pro zajištění bezpečné architektury informačního a komunikačního systému. Výkon této funkce je podobný s předchozí funkcí.

c) Auditor KB

Odpovídá za provedení auditu KB a zaručuje jeho nestranné provedení a nesmí být pověřen výkonem jiných funkcí.

d) Garant aktiva

Odpovídá za zajištění rozvoje, použití a bezpečnost aktiva.

Níže uvedená tabulka představuje bezpečnostní role v oblasti zajištění uvedených činností pro KB. Ty jsou představovány osobami, které vymezuje VoKB. Název matice tvoří akronym anglických slov, kde jednotlivá písmena představují následující:

- **R (Responsible)** – Kdo je odpovědný za vykonání svěřeného úkolu.
- **A (Accountable)** – Kdo je odpovědný za celý úkol a je odpovědný za to, co je vykonáno.
- **C (Consulted)** – Kdo může poskytnout cennou radu či konzultaci k úkolu.
- **I (Informed)** – Kdo má být informován o průběhu úkolu či rozhodnutí v úkolu.

Tab. 15 – Matice RACI zákonných bezpečnostních rolí

	Manažer KB	**Architekt KB**	**Auditor KB**	**Garant aktiva**
Celkové řízení a rozvoj KB	C, I	C, I	C, I	C, I
Audit KB	C, I	C, I	R	C, I
Systém řízení bezpečnosti informací	R	C, I	C	C, I
Návrh bezpečnostních opatření	A, C, I	R	C	C, I
Implementace bezpečnostních opatření	A, C, I	R	C	C, I
Zajištění rozvoje, použití a bezpečnosti aktiva	A, C, I	C, I	C	R

Zdroj: (Česko, 2018), (Bezouška, Švanda a Borej, 2019).

10.4 Technická opatření

Tato podkapitola je věnována zejména technickým opatřením opírajících se o dokumentace, které pravidelně vydává NÚKIB v závislosti na aktuální situaci. Technická opatření doplňují opatření organizační se zaměřením na vykonávanou funkci pracovníků. Pro řešenou problematiku v této práce byla vybrána dokumentace zaměřující se právě na preventivní bezpečnostní opatření z hlediska technického zaměření. Tato část je primárně určena vedení a správcům IT a některými se mohou řídit i běžní uživatelé. Níže uvedené kroky (postupy) mohou sloužit nejenom pro nemocniční zařízení, nýbrž na základě nich mohou své IS/ITC chránit i jiné organizace. Napříč různých vydaných odborných časopisů se může dočíst, že jsou zdravotnická zařízení pro útočníky stále větším terčem zejména pak z důvodu neustálého růstu důvěrnosti dat. Tato zařízení představují vyšší pravděpodobnost zaplacení výkupného, kde jedním z důvodů může být rychlost obnovení potřebných dat. Avšak zaplacení výkupného se nedoporučuje a navíc zde není garance vrácení dat apod.

Jednotlivá opatření byla zpracována přehledně do tabulek, které byly rozděleny následovně:

- **Spear-phishing** (doporučení pro: běžné uživatele a správce sítě).
- **Ransomware** (preventivní opatření, reakce na útok).

Spear-phishing představuje jeden z nejčastějších vektorů kybernetických útoků. Úřad v souvislosti s touto hrozbou doporučuje provedení konkrétních úkonů, které jsou přehledně zobrazeny v následující tabulce. Podrobnější zpracování je v příloze P I.

Tab. 16 – Doporučení a ochrana: Spear-phishing – běžní uživatelé

Spear-phishing		
Běžní uživatelé	**Bezpečnostní zásady**	**Poznámka**
	Nepovolovat makra v programech (Microsoft Office).	V případě potřeby ověřit autentičnost souboru u odesílatele.
	Neotvírat bez uvážení přílohy a odkazy v e-mailech (od neznámých uživatelů).	V případě nejistoty ověřit odeslání souboru u odesílatele (telefonicky).
	Kontrola e-mailové adresy odesilatele (především jde-li o žádost důvěrných informací apod.).	Obsah e-mailu vyzývá například k okamžité činnosti (zaplacení, zadání údajů).
	Při nejistotě či podezření závadného e-mailu kontaktovat IT oddělení.	Nepokoušet se závadu opravit.
	Nesdílet informace o zaměstnání.	Interní informace sdílené na sociálních sítích apod.

Zdroj: (NÚKIB, 2020, d), zpracování: (autorka práce).

Měl by být kladen důraz na to, co a s kým je sdíleno na internetu. V tomto ohledu se nabízí informovat uživatele sociálních sítí o možnostech nastavení soukromí. Rozhodně pak nesdílet na žádných těchto sítích interní informace. Následující tabulka shrnuje doporučené zásady pro správce IT.

Tab. 17 – Doporučení a ochrana: Spear-phishing – správci IT

Spear-phishing		
Správci IT	**Bezpečnostní zásady**	**Poznámka**
	Omezení přístupu útočníka k uživateli.	Pomocí technologií ověřovat odesilatele a filtrovat e-maily pro uživatele a spam (tzv. anti-spoofing nástroje: DMARC, DKIM, SPF). Povědomí o tom, jaké informace jsou sdíleny třetími stranami (dodavatelé).
	Pomoc uživatelům při identifikaci a hlášení podvodných e-mailů.	Cílem je zabránit tomu, aby uživatelé (personál) neměli obavy nahlásit podezřelé e-maily určené osobě. K rozpoznání slouží školení.
	Univerzální zásady	Použití anti-virového SW. Omezení maker u Microsoft Office. Pravidelné zálohy dat. Kontrolovat nutnost potřeby autorizace uživatele. Odstranění účtů již nepracujících pracovníků. Upozornit na možnost maskování přípon souborů („obrázek.png.exe“, „text.txt.exe“, dokument.pdf.exe“).

Zdroj: (NÚKIB, 2020, d), (NÚKIB, 2020, e), zpracování: (autorka práce).

Útoky pomocí ransomwaru jsou čím dál cílenější a mohou postihnout jakoukoli instituci. Pro útočníky je ale stále atraktivní cílit na nemocniční zařízení z onoho známého důvodu, a to, že tato zařízení zpracovávají obrovské množství citlivých dat. Úřad vydává sérii doporučení, jak těmto útokům předcházet a postup v případě útoku. Dokument (NÚKIB, 2020, b) shrnuje především technická opatření ochrany proti útokům.

Výčet jednotlivých opatření interpretuje následující tabulka.

Tab. 18 – Doporučení a ochrana: Ransomware

Ransomware		
Preventivní opatření	**Bezpečnostní zásady**	**Poznámka**
	Systém zálohy dle pravidla: 3–2–1.	Nejméně 3 kopie na 2 různých zařízeních a z toho 1 uložené někde mimo organizaci. Zálohu je nutno provádět pravidelně a testovat také její funkčnost.
	Segmentace sítě.	Rozdělení sítě na jednotlivé segmenty s ohledem na důležitost poskytovaných služeb z toho důvodu, aby se malware nešířil po celé síti, nýbrž po napadeném úseku.
	Pravidelné aktualizování SW a OS.	Staré verze jsou snadnějším terčem kybernetických útoků. Možnost automatické aktualizace.
	Omezit administrátorské účty pouze pro administrátory.	Přidělit uživateli pouze běžná práva, aby se zamezilo jiným činnostem (neautorizované surfování po síti).
	Různá hesla.	Nepoužívat stejná hesla ke všem službám (přístupové heslo k PC, e-mail, …). Doporučená délka dle VoKB, § 19 (12 znaků – uživatel, 17 znaků – administrátor).
Reakce na útok	Odpojit zálohovací server ze sítě (popř. odpojit zdroj el. energie).	Neprodleně po zjištění útoku.
	Zajištění rozsahu napadení – izolace napadených systémů.	Zjistit napadené sítě a izolovat je od těch nenapadených.
	Neplatit výkupné.	Zaplacení motivuje útočníka k dalším útokům. Žádná garance vrácení dat.
	Kontaktovat kompetentní osobu.	Manažer KB, IT oddělení, NÚKIB, Policii ČR.

Zdroj: (NÚKIB, 2020, b), zpracování: (autorka práce).

11 SHRNUTÍ

Vzhledem k tomu, že vybraná nemocniční zařízení spadají pod ZoKB, mají povinnost se zabývat kybernetikou bezpečností a náležitě ji řešit. Diplomová práce byla zaměřena na kybernetickou bezpečnost vybraných nemocničních zařízení v ČR, přičemž pozornost byla věnována pouze vybraným oblastem z důvodu její obsáhlosti.

Za problematické je shledán především nedostatek IT odborníků v dané oblasti. S tímto zásadním problémem se všehovšudy potýkají i nemocniční zařízení, ve kterých byl proveden řízený rozhovor. Další problém spočívá v neochotě pracovníků spolupracovat na zavedení nových bezpečnostních opatřeních. Samotným problémem obecně sužují bezpochyby kybernetické útoky z důvodu jejich zranitelnosti, což bylo především stěžejním pro předkládanou práci. Za pomoci vybraných metod a nástroje byla provedena analýza rizik. Za nejvíce pravděpodobné byly zjištěny zmíněné kybernetické útoky provedených zejména přes spear-phishingové e-maily, které většinou obsahují ransomware, se kterým souvisí rizika další. Ovšem za nejzranitelnější je považován lidský faktor, který se přerušení provozu v důsledku útoku podílí ať už vědomě či nevědomě.

Byl vytvořený plán zvládání bezpečnostních incidentů, který je rozdělen na organizační opatření, které řeší především opatření před vznikem nežádoucí události v podobě bezpečnostního školení a bezpečnostního povědomí, a technická opatření opírající se zejména o dokumentace, které vydává NÚKIB.

Na základě řízených rozhovorů v rámci vybraných nemocničních zařízení, kterým byly předloženy stejné otázky, může být pozorován patřičný rozdíl mezi těmato dvěma nemocnicemi. Zvláště pak byly shledány rozdíly v provádění bezpečnostních školení a jeho zpětné vazby, dále pak rozsah školených zaměstnanců, kde v případě jednoho subjektu nejsou školeni správci sítě. Další komparace těchto dvou zařízení uvádí šifrování dat uložených na serveru. Z autorčina pohledu by se školení měli zúčastnit všechny zainteresované strany v rámci užívání IS/ICT. Obsah školení pak upraven dle vykonávané funkce pracovníka. Pro efektivnost školení by měla být zavedena určitá zpětná vazba například v podobě dotazníku nebo pomocí závěrečných testů (e-learning), jak bylo zjištěno. Autorka však kvituje, že zdravotnický personál je především zaměřen na poskytování neodkladné a další zdravotní péče pacientům. Ovšem věnovaná pozornost zmiňované KB může zvýšit šanci na záchranu lidského života či na jeho kvalitu a naopak snížit riziko vzniku nežádoucích událostí s KB spojených. Výše zmíněné může být splněno za předpokladu, že není opomíjena významnost bezpečnosti informací a KB.

ZÁVĚR

V rámci řešené problematiky předložené diplomové práce byl pro prvotní sběr informací zvolen řízený rozhovor, který se uskutečnil ve vybraných nemocničních zařízení. Dále byla zvolena metoda KARS a dále multikriteriální hodnocení, které bylo provedeno pomocí softwaru RISKAN, kalkulátoru pro tvorbu analýzy rizik. Identifikace rizik pro zvolenou metodu KARS byla zhotovena na základě brainstormingu a metody What-If s odborníky na informační a komunikační technologie ve vybraných nemocničních zařízeních, kde tato identifikace byla podpořena zkušenostmi daných odborníků. Významnost analyzovaných rizik specifikují vymezené kvadranty (I. – IV.) v uvedené analýze, které byly určeny na základě přesně daných výpočtů, přičemž pro oblast relativně bezpečnou nebyla zjištěna žádná rizika. V rámci identifikace aktiv a hrozeb v rizikovém kalkulátoru RISKAN byla stěžejním podkladem norma ČSN ISO/IEC 27005, příloha B. Na základě zjištěných nedostatků prostřednictvím zmíněné metody a rizikového kalkulátoru byla navržena opatření logicky rozdělena na organizační a technická. Následně na to byl vypracován plán zvládání bezpečnostních incidentů. Tento plán byl rozdělen, jak je výše uvedeno, na dvě části, a to na organizační a část technických opatření.

Ne všechna opatření jsou účinná na 100 %, to znamená, že každé opatření může selhat. Nicméně bezpečnostním opatřením by měla být věnována značná část pozornosti. Avšak vnímání rizik jednotlivými zdravotníky je různorodé a stále tato oblast pro ně nepředstavuje významnou prioritu. Pozornost věnována těmto opatřením snižuje dopad rizik v důsledku úspěšného kybernetického útoku. Především, dojde-li již k narušení provozu nemocnice v důsledku narušení důvěrnosti, dostupnosti či integrity dat. To je pak určitým krokem a opatřením před nežádoucími dopady. Nefunkčnost nemocničního informačního systému či ochromení chodu celé nemocnice se pak odráží od toho, jak je dané nemocniční zařízení připraveno vzniklé situace řešit. Avšak ne v každém případě lze pojmout veškeré řízení kybernetických rizik. Nicméně vzhledem k důležitosti dané kritické infrastruktury a poskytované péče, je vhodné daná rizika snížit na minimum.

Přínos práce z autorčina pohledu spočívá v rozšíření povědomí o řešené problematice, zvláště pak na základě jakých opatření může dojít k minimalizaci či eliminaci potenciálních rizik. Výstupy z analýzy rizik byly předloženy vybraným subjektům z nemocničních zařízení, na základě kterých může být zvýšena jejich úroveň kybernetické bezpečnosti.

Na základě získaných výstupů se lze domnívat, že byl cíl práce splněn.

SEZNAM POUŽITÉ LITERATURY

TIŠTĚNÉ DOKUMENTY

Kniha

DOUCEK, Petr, Martin KONEČNÝ a Luděk NOVÁK, 2019. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing. ISBN 978-80-88260-39-4.

ČAPEK, Jan et al., 2015. *Vybrané aspekty kybernetické bezpečnosti*. Pardubice: Univerzita Pardubice. ISBN 9788073959531.

JOHNSON, Thomas, 2015. *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare* [online]. 6000 Broken Sound Parkway NW, Suite 300: CRC Press Taylor & Francis Group [cit. 2020-11-07]. ISBN 978-1-4822-3923-2.

KOŽÍŠEK, Martin a Václav PÍSECKÝ, 2016. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing. ISBN 9788024755953.

KRÁL, Mojmír, 2015. *Bezpečný internet: chraňte sebe i svůj počítač*. První vydání. Praha: Grada Publishing, a.s. Průvodce (Grada). ISBN 9788024754536.

MCCARTHY, N., 2012. *The computer incident response planning handbook: executable plans for protecting information at risk*. New York: McGraw-Hill. ISBN 978-0-07-179039-0.

PAČKA, Roman, 2019. *CSIRT: v přední linii boje proti kybernetickým hrozbám*. Brno: Centrum pro studium demokracie a kultury. Politologická řada. ISBN 9788073254735.

SMEJKAL, Vladimír, 2015. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. Pro praxi. ISBN 9788073805012.

SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL, 2019. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o. ISBN 9788073807658.

ŠUPŠÁKOVÁ, Petra, 2017. *Řízení rizik při poskytování zdravotních služeb: manuál pro praxi*. Praha: Grada Publishing. ISBN 978-80-271-0062-0.

ELEKTRONICKÉ DOKUMENTY

Elektronická kniha

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR, 2015. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary* [online]. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze [cit. 2020-12-20]. ISBN 978-80-7251-436-6. Dostupné z: https://www.cybersecurity.cz/data/slovnik_v310.pdf

KOLOUCH, Jan, 2016. *CyberCrime* [online]. Praha: CZ.NIC, z.s.p.o. [cit. 2020-12-20]. CZ.NIC. ISBN 978-80-88168-18-8. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf

KOLOUCH, Jan a Pavel BAŠTA, 2019. *CyberSecurity* [online]. Praha: CZ.NIC, z.s.p.o. [cit. 2020-12-20]. CZ.NIC. ISBN 978-80-88168-34-8. Dostupné z: https://knihy.nic.cz/files/edice/cybersecurity.pdf

RICHTER, Rostislav, 2018. *Slovník pojmů krizového řízení* [online]. Vydání první. Praha: Ministerstvo vnitra, Generální ředitelství Hasičského záchranného sboru ČR [cit. 2020-11-07]. ISBN 978-80-87544-91-4. Dostupné z: https://www.hzscr.cz/soubor/slovnik-pojmu-krizoveho-rizeni-2018-pdf.aspx

Elektronická akademická práce

JELŠOVSKÁ, Katarína a Andrea PETERKOVÁ, 2013. *Řešení krizových situací - metody a jejich aplikace* [online]. Opava [cit. 2020-12-20]. Dostupné z: https://www.slu.cz/file/cul/67f86af0-d484-45dc-87cf-52b7d488c52a. Studijní opory. Slezská univerzita v Opavě.

KOŠŤÁL, Jaroslav, 2015. *Posouzení rizik jaderné elektrárny Temelín* [online]. České Budějovice [cit. 2021-04-04]. Dostupné z: https://theses.cz/id/fslm7f/Posouzen_rizik_JE_Temeln.pdf. Diplomová práce. Jihočeská univerzita v Českých Budějovicích, Zdravotně sociální fakulta, Katedra radiologie, toxikologie a ochrany obyvatelstva.

Elektronický článek

ČERMÁK, Miroslav, © 2008 – 2021, a. Spear phishing je cílený phishing, kterému se lze jen těžko bránit. *Clever and Smart* [online]. [cit. 2021-03-31]. ISSN 2694-9830. Dostupné

z: https://www.cleverandsmart.cz/spear-phishing-je-cileny-phishing-kteremu-se-lze-jen-tezko-branit/

ČERMÁK, Miroslav, © 2008 – 2021, b. Seznam organizací v ČR, na které byl veden kybernetický útok. *Clever and Smart* [online]. [cit. 2021-02-22]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/seznam-organizaci-v-cr-na-ktere-byl-veden-kyberneticky-utok/

Článek v elektronickém periodiku

BÍNEK, Vojtěch, 2020. 7 kroků ke kybernetické ochraně ve zdravotnictví. *IT Systems* [online]. Systém online, **2020**(7-8) [cit. 2020-11-29]. ISSN 1802-615X. Dostupné z: https://m.systemonline.cz/it-security/7-kroku-ke-kyberneticke-ochrane-ve-zdravotnictvi.htm

DANIHELKA, Pavel, Lenka SCHREIBEROVA a Jan JURÁSEK, 2020. Kybernetický útok jako hrozba pro BOZP v podnicích. *Časopis výzkumu a aplikací v profesionální bezpečnosti* [online]. **13**(4) [cit. 2021-02-22]. ISSN 1803-3687. Dostupné z: https://www.bozpinfo.cz/josra/kyberneticky-utok-jako-hrozba-pro-bozp-v-podnicich

JALALI, Mohammad a Jessica KAISER, 2018. Cybersecurity in Hospitals: A Systematic, Organizational Perspective. *Journal of Medical Internet Research* [online]. United States, **20**(5) [cit. 2020-11-18]. ISSN 1438-8871. Dostupné z: doi:10.2196/10059

ŠAUR, David, 2014. Využití informační podpory pro krizové řízení. *Trilobit* [online]. Zlín: Thomas Bata University in Zlín, Faculty of Applied Informatics, **2014**(2) [cit. 2020-11-29]. ISSN 1804-1795. Dostupné z: http://trilobit.fai.utb.cz/vyuziti-informacni-podpory-pro-krizove-rizeni

ŠURÁŇ, Petr, 2015. NIS je pro nemocnici kritickým systémem. *Systém online* [online]. Systém online, **2015**(7) [cit. 2020-11-29]. ISSN 1802-615X. Dostupné z: https://m.systemonline.cz/it-pro-verejny-sektor-a-zdravotnictvi/nis-je-pro-nemocnici-kritickym-systemem-1.htm

Elektronický dokument

BEZOUŠKA, Tomáš, Martin ŠVANDA a Jiří BOREJ, 2019. Metodický pokyn poskytovatelům zdravotních služeb ke kybernetické bezpečnosti: Bezpečnostní politika.

In: *Národní centrum elektronického zdravotnictví* [online]. Praha: Ministerstvo zdravotnictví České republiky [cit. 2021-04-01]. Dostupné z: https://ncez.mzcr.cz/sites/default/files/Attachment/Bezpe%C4%8Dnostn%C3%AD_politika_informac%C3%AD_organizace.docx

HRONEK, Jiří, 2007. Informační systémy. In: *Katedra informatiky: Univerzita Palackého v Olomouci* [online]. Olomouc: Univerzita Palackého, přírodovědecká fakulta, Katedra informatiky [cit. 2021-02-18]. Dostupné z: https://phoenix.inf.upol.cz/esf/ucebni/infoSys.pdf

NÚKIB, 2021, b. Upozornění na zvýšené riziko kybernetických útoků proti České republice. In: *NÚKIB* [online]. Brno: NÚKIB [cit. 2021-4-27]. Dostupné z: https://www.nukib.cz/download/publikace/analyzy/Upozorneni_na_zvysene_riziko_kybernetickych_utoku_proti_CR.pdf

NÚKIB, 2020, a. Národní strategie kybernetické bezpečnosti České republiky. In: *NÚKIB* [online]. Brno: NÚKIB [cit. 2020-12-19]. Dostupné z: https://www.nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf

NÚKIB, 2020, b. Ransomware: Doporučení pro mitigaci, prevenci a reakci. In: *NÚKIB* [online]. Brno: NÚKIB [cit. 2020-12-19]. Dostupné z: https://www.nukib.cz/download/publikace/podpurne_materialy/Ransomware%20-%20Doporuceni_pro_mitigaci_prevenci_a_reakci.pdf

NÚKIB, 2020, c. Vyděračské útoky ransomwarem jsou cílenější: míří na velké firmy, státní a veřejné instituce. In: *NÚKIB* [online]. Brno: NÚKIB [cit. 2020-12-19]. Dostupné z: https://www.nukib.cz/download/publikace/analyzy/Analyza_hrozby_ransomware.pdf

NÚKIB, 2020, d. Podvodné e-maily nebo zprávy na sociálních sítích na míru: Spear-phishing a jak se před ním chránit. In: *NÚKIB* [online]. Brno: NÚKIB [cit. 2021-04-16]. Dostupné z: https://nukib.cz/download/publikace/doporuceni/Doporuceni_spear_phishing_2.0.pdf

NÚKIB, 2020, e. Varování před hrozbou kybernetických útoků na nemocnice a jiné významné cíle ČR. In: *NÚKIB* [online]. Brno [cit. 2020-12-19]. Dostupné z: https://www.nukib.cz/download/uredni_deska/Varovani_NUKIB_2020-04-16.pdf

Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2019, 2020. In: *Národní úřad pro kybernetickou a informační bezpečnost* [online]. NÚKIB [cit. 2020-11-16]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/NUKIB_ZSKB_2019.pdf

Webová stránka

About us, © All Rights Reserved. *International Organization for Standardization* [online]. Switzerland: International Organization for Standardization [cit. 2020-11-13]. Dostupné z: https://www.iso.org/about-us.html

Attacks targeting healthcare organizations spike globally as COVID-19 cases rise again, 2020. *Check point software* [online]. United States [cit. 2021-02-22]. Dostupné z: https://blog.checkpoint.com/2021/01/05/attacks-targeting-healthcare-organizations-spike-globally-as-covid-19-cases-rise-again/

BROWN, Terry, 2020. The Importance of Information and Communication Technology (ICT). *Itchronicles* [online]. [cit. 2020-11-17]. Dostupné z: https://itchronicles.com/information-and-communication-technology/the-importance-of-information-and-communication-technology-ict/

Cyber attacks hit two French hospitals in one week, 2021. *Today news post* [online]. Francie [cit. 2021-02-20]. Dostupné z: https://todaynewspost.com/news/world/europe-news/cyber-attacks-hit-two-french-hospitals-in-one-week/

Fakultní nemocnice Ostrava se stala terčem kybernetického útoku, 2020. *Český rozhlas Ostrava* [online]. Ostrava [cit. 2020-12-19]. Dostupné z: https://ostrava.rozhlas.cz/fakultni-nemocnice-ostrava-se-stala-tercem-kybernetickeho-utoku-8184954

FN Brno se stala terčem kybernetického útoku, 2020. *Zdravotnický deník* [online]. [cit. 2020-12-19]. Dostupné z: https://www.zdravotnickydenik.cz/2020/03/fn-brno-se-stala-tercem-kybernetickeho-utoku/

Healthcare And Hospital Security, 2020. *Security MPS* [online]. 25020 Las Brisas Rd, Murrieta, CA 92562, United States: MPS Security [cit. 2020-12-19]. Dostupné z: https://security-mps.com/markets-served/healthcare-and-hospital-security/

HORÁK, Jan, 2020. Na nemocnici v Brně zaútočil vyděračský virus, špitál povolal krizového IT manažera. *Aktuálně.cz* [online]. Praha: © Economia [cit. 2021-4-27]. Dostupné z: https://zpravy.aktualne.cz/domaci/na-nemocnici-v-brne-zautocil-vyderacsky-virus-spital-povolal/r~ff91a02c6aa011eab1110cc47ab5f122/

HRAZDIL, Jiří, 2020. ČSN EN ISO/IEC 27000 (369790): Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník. *Shop normy biz* [online]. [cit. 2020-12-12]. Dostupné z: https://shop.normy.biz/detail/510056

HRAZDIL, Jiří, 2020. ČSN ISO/IEC 27006 (369790): Informační technologie - Bezpečnostní techniky - Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací. *Shop normy biz* [online]. [cit. 2020-12-12]. Dostupné z: https://shop.normy.biz/detail/500567

HRAZDIL, Jiří, 2020. ČSN ISO/IEC 27032 (369790): Informační technologie - Bezpečnostní techniky - Směrnice pro kybernetickou bezpečnost. *Shop normy biz* [online]. [cit. 2020-12-12]. Dostupné z: https://shop.normy.biz/detail/93691

Informační systém (Information System), 2020. *Managementmania* [online]. [cit. 2020-11-25]. Dostupné z: https://managementmania.com/cs/informacni-system

Informační technologie a jejich využití ve zdravotnictví, 2020. *Český statistický úřad* [online]. Praha: Český statistický úřad [cit. 2020-12-19]. Dostupné z: https://www.czso.cz/csu/czso/informacni_technologie_ve_zdravotnictvi

Jak se bránit útoku ransomwarem, 2020. NÚKIB [online]. Brno: NÚKIB [cit. 2020-12-19]. Dostupné z: https://www.nukib.cz/cs/infoservis/aktuality/1662-jak-se-branit-utoku-ransomwarem/

KILIÁN, Karel, 2020. Ransomwarový útok na německou nemocnici si vyžádal život pacientky. *Živě* [online]. CZECH NEWS CENTER [cit. 2021-02-20]. Dostupné z: https://www.zive.cz/clanky/ransomwarovy-utok-na-nemeckou-nemocnici-si-vyzadal-zivot-pacientky/sc-3-a-206043/default.aspx

Kyberútok na nemocnici v Benešově: nefungují žádné přístroje, 2019. *Centrum kybernetické bezpečnosti* [online]. [cit. 2020-12-19]. Dostupné z:

https://centrumkyberbezpecnosti.cz/kyberutok-na-nemocnici-v-benesove-nefunguji-zadne-pristroje/

MAGDOŇOVÁ, Jana, 2020. Pod kyberzákon by měly nově spadat i menší nemocnice. Nová kritéria budou úřady užívat už od ledna. *IRozhlas* [online]. Praha [cit. 2021-03-18]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/nemocnice-it-kyberneticka-bezpecnost-kyberurad-kraje-rozsireni_2012100730_tzr

MARKS, Paul, 2019. Cybersecurity and the Parkerian Hexad. *Staffhosteurope* [online]. [cit. 2020-11-03]. Dostupné z: https://www.staffhosteurope.com/blog/2019/03/cybersecurity-and-the-parkerian-hexad

NBÚ vybral provozovatele národního CERT (CSIRT.CZ), je jím CZ.NIC, 2015. *Národní bezpečnostní úřad* [online]. Praha: NBÚ [cit. 2020-12-05]. Dostupné z: https://www.nbu.cz/cs/aktualne/820-621-nbu-vybral-provozovatele-narodniho-cert-csirtcz-je-jim-cznic/

NÚKIB, 2019. Varování o hrozbě Emotet-Trickbot-Ryuk. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Brno: NÚKIB [cit. 2021-4-27]. Dostupné z: https://www.nukib.cz/cs/infoservis/hrozby/1478-varovani-o-hrozbe-emotet-trickbot-ryuk/

NÚKIB, 2021, a. Nová pravidla pro určování provozovatelů základních služeb v odvětví zdravotnictví. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Brno: NÚKIB [cit. 2021-04-01]. Dostupné z: https://nukib.cz/cs/infoservis/aktuality/1673-nova-pravidla-pro-urcovani-provozovatelu-zakladnich-sluzeb-v-odvetvi-zdravotnictvi/

O NÚKIB, [2017]. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Brno: NÚKIB [cit. 2020-11-13]. Dostupné z: https://nukib.cz/cs/o-nukib/

Právo na ochranu osobních údajů, 2021. *Národní zdravotnický informační portál* [online]. Praha 2 – Nové Město: Ministerstvo zdravotnictví České republiky [cit. 2020-11-29]. Dostupné z: https://www.nzip.cz/clanek/243-pravo-na-ochranu-osobnich-udaju

Ransomware, © 1992 – 2020. *Eset* [online]. Praha [cit. 2021-02-19]. Dostupné z: https://www.eset.com/cz/ransomware/

Ransomware – definice a jak se úspěšně bránit, 2020. *Uloz to a sdilej* [online]. Praha [cit. 2021-02-23]. Dostupné z: https://www.uloztoasdilej.cz/ransomware-definice-a-jak-se-uspesne-branit/#Typy_ransomwaru

Ransomware útoky, definice, příklady, ochrana, odstranění 2021, © 2021. *Joecomp* [online]. [cit. 2021-02-19]. Dostupné z: https://cs.joecomp.com/ransomware-attacks-definition-examples-protection-removal-faq

RUBENS, Paul, 2017. Common Types of Ransomware. *ESecurity Planet* [online]. [cit. 2021-02-19]. Dostupné z: https://www.esecurityplanet.com/threats/common-types-of-ransomware/

SHEIN, Esther, 2020. World Health Organization has been the target of significant cyberattacks. *Techrepublic* [online]. [cit. 2021-02-20]. Dostupné z: https://www.techrepublic.com/article/world-health-organization-has-been-the-target-of-significant-cyberattacks/

The ISO Story - founding, 2011. *Wayback Machine* [online]. ISO [cit. 2020-11-14]. Dostupné z: https://web.archive.org/web/20120315031458/http://www.iso.org/iso/about/the_iso_story/iso_story_founding.htm

Vedení úřadu, [2020]. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Brno: NÚKIB [cit. 2021-02-23]. Dostupné z: https://www.nukib.cz/cs/o-nukib/vedeni-uradu/

Vše o programu Wintropos, © 2020. *Wintropos* [online]. Turnov [cit. 2021-02-18]. Dostupné z: http://wintropos.cz/Program.aspx

Vyhledávání poskytovatele, 2021. *Národní registr poskytovatelů zdravotních služeb* [online]. Praha: Ústav zdravotnických informací [cit. 2021-04-04]. Dostupné z: https://nrpzs.uzis.cz/index.php?pg=vyhledavani-poskytovatele

ZAJÍC, David, 2020. Nemocnice ochromily kybernetické útoky. *Hospodářské noviny* [online]. [cit. 2020-11-22]. Dostupné z: https://ictrevue.ihned.cz/c3-66768270-0ICT00_d-66768270-nemocnice-ochromily-kyberneticke-utoky

LEGISLATIVNÍ DOKUMENTY

Zákony

ČESKO A, 2014. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-181

ČESKO, 1998. Zákon č. 110/1998 Sb., o bezpečnosti České republiky. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/1998-110

ČESKO, 2000. Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon). In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2000-240

ČESKO, 2005. Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-412

ČESKO, 2011. Zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách). In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2011-372

ČESKO, 2019. Zákon č. 110/2019 Sb., o zpracování osobních údajů. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2019-110

Vyhlášky

ČESKO B, 2014. Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-317

ČESKO, 2020. Vyhláška č. 573/2020 Sb., kterou se mění vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2020-573

ČESKO, 2018. Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti

kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2018-82

ČESKO, 2017. Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2017-437

ČESKO, 2012. Vyhláška č. 98/2012 Sb., o zdravotnické dokumentaci. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2012-98

Normy

ČSN ISO/IEC 27002, 2014. *Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Třídící znak 36 9798.

ČSN ISO/IEC 27005, 2019. *Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Třídící znak 36 9790.

Jiné

Řízený rozhovor, 2021.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

a.s.	Akciová společnost
AD	Active Directory
AIDS	Aids Info Disk
apod.	a podobně
atd.	a tak dále
BCM	Business Continuity Management
BIOS	Basic Input/Output System
BIS	Bezpečnostní informační služba
BRS	Bezpečnostní rada státu
CD	Compact Disc
CERT	Computer Emergency Response Team
CISA	Cybersecurity and Infrastructure Security Agency
COBIT	Control Objetives for Information Technologies
CSIRT	Computer Security Incident Response Team
CT	Computer Tomograph
ČR	Česká republika
ČSN	Česká technická norma
DDoS	Distributed Denial-of-Service
DKIM	DomainKeys Identified Mail
DMARC	Domain Message Authentication Reporting and Conformance
DVD	Digital Versatile Disc
FBI	Federal Bureau of Investigation
GDPR	General Data Protection Regulation
GPO	Group Policy
HA	High Availability

HW	Hardware
ICT	Information and Communication Technology
IEC	Interantional Elektrotechnical Commission
IS	Information System
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ISO	International Organization for Standartization
IT	Information Technology
ITIL	Information Technology Infrastucture Library
KB	Kybernetická bezpečnost
LIS	Laboratory Information System
NIS	Nemocniční informační systém
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OP	Občanský průkaz
P. č.	Pořadové číslo
PACS	Picture Archive and Communication System
PC	Personal Computer
PDCA	Plan-Do-Check-Act
PSČ	Poštovní směrovací číslo
RTG	Rentgen
SIEM	Security Information and Event Management
SPF	Sender Policy Framework
SW	Software
tzn.	to znamená
VLAN	Virtual Local Area Network
VoKB	Vyhláška o kybernetické bezpečnosti

WHO	World Health Organization
Wi-Fi	Wireless Fidelity
WLC	Wireless LAN Controller
ZoKB	Zákon o kybernetické bezpečnosti

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: SPEAR-PHISHING A DOPORUČENÍ PRO PERSONÁL NEMOCNIC

Zdroj: (NÚKIB, 2020, d).

PŘÍLOHA P II: ŘÍZENÝ ROZHOVOR SUBJEKT X

Obecné otázky v rámci normy ISO/IEC 27 001

- *„Jsou identifikována a evidována aktiva?“*

  Ano, evidence spadá pod ZoKB a VoKB. Vede se centrálně přes Intranet nemocnice.

- *„Jsou prováděna školení o bezpečnosti informací?“*

  Formou e-learningu. Jednotlivé oblasti v rámci učebního testu s 70% úspěšností.

- *„Je prováděna zpětná vazba, zda bylo školení přínosné?“*

  Zpětná vazba na základě závěrečného testu.

- *„Účastní se školení zaměstnanců i správci sítě?“*

  Penzum školení zaměstnanců je široké. Vysoce postavení IT odborníci jsou školeni a certifikováni v oblasti bezpečnosti informací.

- *„Jak je řízen přístup k informacím?“*

  Vydaná směrnice, která obsahuje ISMS. Pomocí kartičky, hesel, identifikátorů. Informace jsou důvěrné.

- *„Je dodržen princip oddělení sítí?“*

  Ano.

- *„Jak často jsou prováděny aktualizace?“*

  Aktualizace jsou prováděny pravidelně. Neexistuje místo, kde by nebyly prováděny. Jsou prováděny z toho důvodu, aby správně probíhaly přenosy informací.

- *„Je implementován antimalware?“*

  Jsou speciální detekce. Zastaralost, rigidita. Přesvědčování zaměstnanců pro dobro.

- *„Provádíte audit informačních systémů?“*

  Probíhá na úrovni kybernetické bezpečnosti, kam informační systém spadá (nemocniční, patologický, radiologický systém).

- *„Jsou implementovány nástroje pro detekci kybernetických útoků?“*

  SIEM.

- *„Jaké vybavení je použito pro přístup k informacím?“*

Silná hesla, kartičky, čtečky na E-recepty.

- *„Kdo má přístup k sítím a síťovým službám?“*

  Administrátoři.

- *„Jak je zabezpečen postup při přenosu informací?“*

  Šifrováním.

- *„Využíváte systém správy hesel?“*

  Ne.

- *„Jak probíhá elektronické předávání zpráv?“*

  E-maily (Exchange).

- *„Je zajištěna integrita provozu systému?“*

  Ano.

- *„Provádíte testování bezpečnosti?“*

  Jednou ročně analýza stavu bezpečnosti. Testování zranitelnosti (Závěrečná zpráva z NÚKIB).

- *„Jak je zabezpečeno hlášení bezpečnostních incidentů?“*

  Konkrétní pravidla. Hlášeno do několika hodin na NÚKIB. Interně pak zapsáno do IS.

Technický a organizační okruh otázek

- *„Jaký operační systém využíváte?“*

  V rámci nemocnice jsou využívány všechny operační systémy.

- *„Jak často probíhá aktualizace tohoto systému?“*

  Pravidelně.

- *„Kdo má fyzický přístup k serveru?“*

  K datovým centrům mají přístup ti, kteří mají právo - IT pracovníci pomocí čteček karet.

- *„Jsou data uložená na serveru šifrována?“*

  Nejsou.

- *„Jaké je použito zabezpečení Wi-Fi?*

  VLC. Přístup do interní Wi-Fi na základě přidělených certifikací.

- *„Jsou pracovníkům odebrána všechna přístupová hesla po ukončení pracovního poměru?“*

  Ano.

- *„Jak je zajištěn fyzický přístup k PC?“*

  Heslem.

- *„Jak často probíhá zálohování dat?“*

  Centrální zabezpečení systému každou hodinu.

- *„Probíhá kontrola zálohovaných dat?“*

  Musí probíhat kontrola zálohovaných dat.

- *„Jsou k dispozici údaje, kdo se kdy přihlásil k PC?“*

  Ano.

PŘÍLOHA P III: ŘÍZENÝ ROZHOVOR SUBJEKT Y

Obecné otázky v rámci normy ISO/IEC 27 001

- *„Jsou identifikována a evidována aktiva?“*

  Ano.

- *„Jsou prováděna bezpečnostní školení o bezpečnosti informací?“*

  Částečně (online).

- *„Je prováděna zpětná vazba, zda bylo školení přínosné?“*

  Ne.

- *„Účastní se školení zaměstnanců i správci sítě?“*

  Ne.

- *„Jak je řízen přístup k informacím?“*

  Nastavení práv přes AD skupiny, něco je definováno ve směrnicích, něco je „pocitově“.

- *„Je dodržen princip oddělení sítí?“*

  Ano – VLAN.

- *„Jak často jsou prováděny aktualizace?“*

  Minimálně 1x za měsíc, hotfixy ihned.

- *„Je implementován antimalware?“*

  Ano.

- *„Provádíte audit informačních systémů?“*

  Ano.

- *„Jsou implementovány nástroje pro detekci kybernetického útoku?“*

  Ano.

- *„Jaké vybavení je použito pro přístup k informacím?“*

  Jedná se o běžná PC. SW – nemocnice provozuje cca 50 různých systémů pro přístup k informacím. Mezi hlavní (identifikované pod ZoKB) patří NIS (nemocniční IS), PACS (rentgeny), LISy (3 laboratorní systémy).

- *„Kdo má přístup k sítím a síťovým službám?“*

  Doménový uživatel.

- *„Jak je zabezpečen postup při přenosu informací?“*

  To záleží na druhu zprávy, ale většinou není šifrováno, protože jde o přenos end2end (přesně napojené systémy s ověřením pomocí certifikátu). Přenos informací na koncové stanice např. v NIS šifrován není.

- *„Využíváte systém správy hesel?“*

  Používáme standartní pravidla přes GPO.

- *„Jak probíhá elektronické předávání zpráv?“*

  Nemocniční zprávy jsou vytvářeny v NISu a tam "putují spolu s pacientem. Nepředávají se mimo tento systém, pokud nedojde k tisku pro pacienta nebo externího lékaře.

- *„Je zajištěna integrita provozu systému?“*

  Částečně ano, ale HA (vysoká dostupnost) provozováno není.

- *„Provádíte testování bezpečnosti?“*

  Ano.

- *„Jak je zabezpečeno hlášení bezpečnostních incidentů?“*

  Jsme pod ZoKB, takže plně dodržujeme nařízené postupy.

Technický a organizační okruh otázek

- *„Jaký operační systém používáte?“*

  Spoustu – Windows (různé verze). CentOS, Debian.

- *„Jak často probíhá aktualizace tohoto systému?“*

  Minimálně 1x za měsíc.

- *„Kdo má fyzicky přístup k serveru?“*

  Správci serverovny.

- *„Jsou data uložená na serveru šifrována?“*

  Ano.

- *„Jaké máte zabezpečení Wi-Fi?“*

  Různé úrovně zabezpečení dle druhu použití Wi-Fi (od filtru Mac adres, až po otevřenou pacientskou Wi-Fi).

- *„Jsou pracovníkům odebrána všechna přístupová hesla po ukončení pracovního poměru?“*

  Ano.

- *„Jak je zajištěn fyzický přístup k PC?“*

  PC na pracovnách jsou volně přístupná chráněná loginem a heslem.

- *„Jak často probíhá zálohování dat?“*

  Servery minimálně 1x denně (databáze cca 15 minutový interval).

- *„Probíhá kontrola zálohovaných dat?“*

  Ano.

- *„Jsou k dispozici údaje, kdo se kdy přihlásil k PC?“*

  Ano.