ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA BIOMEDICÍNSKÉHO INŽENÝRSTVÍ

Katedra zdravotnických oborů a ochrany obyvatelstva

Analýza rizik úniku informací z lůžkového zdravotnického zařízení ve Středočeském kraji

Analysis of Risks of Information Leakage from Inpatient Medical Facility in the Central Bohemian Region

Diplomová práce

Studijní program: Civilní nouzové plánování

Autor diplomové práce: Bc. Dominika Koevová

Vedoucí diplomové práce: doc. RNDr. Josef Požár, CSc., dr. h. c.

Kladno 2021

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení:	**Koevová**	Jméno:	**Dominika**	Osobní číslo:	**469770**
Fakulta:	**Fakulta biomedicínského inženýrství**				
Garantující katedra:	**Katedra zdravotnických oborů a ochrany obyvatelstva**				
Studijní program:	**Civilní nouzové plánování**				

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Analýza rizik úniku informací z lůžkového zdravotnického zařízení ve Středočeském kraji

Název diplomové práce anglicky:

Analysis of Risks of Information Leakage from Inpatient Medical Facility in the Central Bohemian Region

Pokyny pro vypracování:

Předmětem diplomové práce bude identifikace rizik úniku informací z lůžkového zdravotnického zařízení ve Středočeském kraji. V teoretické části budou vymezeny základní pojmy z oblasti kybernetické bezpečnosti. Budou stanovené možné bezpečnostní incidenty s případnými dopady na činnost lůžkového zdravotnického zařízení. Praktická část bude zaměřena na analýzu vybraných forem útoků s následkem úniku dat a informací z organizace. K tomu bude využita kvalitativní metoda sběru dat formou řízeného rozhovoru s IT specialistou zajišťující bezpečnost dat a informací v organizaci a kvantitativní metoda výzkumu formou dotazníkového šetření určená pro zaměstnance zařízení. Závěrem práce bude provedeno celkové zhodnocení řešené problematiky, na jehož základě budou navržena případná doporučení pro zkvalitnění ochrany dat a informací v lůžkovém zdravotnickém zařízení ve Středočeském kraji.

Seznam doporučené literatury:

[1] JIRÁSEK, Petr, NOVÁK, Luděk, POŽÁR, Josef, Výkladový slovník kybernetické bezpečnosti: Cyber security glossary, ed. 3. aktualiz., Praha: Policejní akademie ČR v Praze, 2015, ISBN 978-80-7251-436-6
[2] KOLOUCH, Jan, BAŠTA, Pavel, CyberSecurity, Praha: CZ.NIC, 2019, ISBN 978-80-88168-31-7
[3] POŽÁR, Josef, KRULÍK, Oldřich, HNÍK, Václav, KNÝ, Milan, Joint Cybercrime Action Taskforce a European Financial Coallition, Bezpečnost na sociálních sítích : sborník příspěvků ze semináře na PA ČR v Praze, pořádaného v rámci Evropského měsíce kybernetické bezpečnosti ve spolupráci s NCKB a ČP AFCEA dne 26. října 2015, 2015, ISBN 978-80-7251-449-6
[4] DRASTICH, Martin, Systém managementu bezpečnosti informací, Praha: Grada, 2011, ISBN 978-80-247-4251-9

Jméno a příjmení vedoucí(ho) diplomové práce:

doc. RNDr. Josef Požár, CSc.

Jméno a příjmení konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: **15.04.2021**
Platnost zadání diplomové práce: **18.09.2022**

doc. Mgr. Zdeněk Hon, Ph.D.
podpis vedoucí(ho) katedry

prof. MUDr. Jozef Rosina, Ph.D., MBA
podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Student(ka) bere na vědomí, že je povinnen(a) vypracovat diplomovou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v diplomové práci.

22. 4. 2021
Datum převzetí zadání

Podpis studenta(ky)

PROHLÁŠENÍ

Prohlašuji, že jsem diplomovou práci s názvem Analýza rizik úniku informací z lůžkového zdravotnického zařízení ve Středočeském kraji vypracovala samostatně pouze s použitím pramenů, které uvádím v seznamu bibliografických odkazů.

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

V Kladně dne 13.05.2021

…….

Bc. Dominika Koevová

PODĚKOVÁNÍ

Touto cestou bych ráda poděkovala mému vedoucímu práce panu doc. RNDr. Josefu Požárovi, CSc. za odborné vedení. Velké díky patří panu Robertu Modlingerovi za čas, který mi věnoval, za jeho ochotu, vstřícnost a veškeré poskytnuté podklady do diplomové práce. Zároveň bych ráda poděkovala respondentům z řad zaměstnanců lůžkového zdravotnického zařízení ve Středočeském kraji. Největší poděkování patří mé rodině, příteli a kamarádům, kteří mě po celou dobu studia podporovali.

ABSTRAKT

Tato diplomová práce je zaměřena na identifikaci rizik a analýzu vybraných forem metod kybernetických útoků s následkem úniku dat a informací z organizace. Práce se především specializuje na lůžkové zdravotnické zařízení ve Středočeském kraji.

V úvodu teoretické části práce je vymezena odborná terminologie kybernetické a informační bezpečnosti. Další kapitoly se zabývají hrozbami a riziky informační bezpečnosti. Poté je pojednáváno o útocích na data a informace, jejich klasifikace a motiv samotných útočníků. Nadcházející kapitoly se věnují kybernetické kriminalitě, kde je pojednáno o technikách sociálního inženýrství a malware. V závěru teoretické části jsou uvedeny příklady kybernetických útoků na zdravotnická zařízení v České republice a jeden příklad i ze zahraničí.

V praktické části práce jsou porovnávána získaná výsledná data. Ta byla zjištěna odbornými výzkumy za pomoci polostrukturovaného rozhovoru se specialistou informačních technologií a nestandardizovaného anonymního dotazníku, který byl distribuován zaměstnancům v lůžkovém zdravotnickém zařízení ve Středočeském kraji.

V závěru práce jsou porovnány moje výsledky s výsledky jiných autorů. Následně jsou navržena doporučení na zlepšení zabezpečení dat a informací v zařízení.

Klíčová slova

Riziko; informační bezpečnost; kybernetická bezpečnost; únik informací; kybernetický útok; zdravotnické zařízení; Středočeský kraj.

ABSTRACT

This thesis focuses on the analysis and risk identification of different forms and methods of cyber attacks, especially on attacks which cause information leaks. The thesis more specifically focuses on healthcare organisations in the central Bohemia region of the Czech Republic.

The introduction of the theoretical part of the thesis outlines professional terminology of cyber information security. In the next part the thesis looks at information security topics regarding threats and risks. Further more the thesis mentions attacks on data and information, its classification and the attackers. Other subchapters talk about cyber criminality focusing on social engineering and malware techniques. At the end of the theoretical part, the thesis mentions examples of cyber attacks on healthcare facilities in the Czech Republic and one example from outside of the country.

Results are compared in the practical part of the thesis. The results were collected through professional research in the form of a semi-structured interview with an IT specialist and a non-standardised anonymous questioner which was distributed to the employees of a healthcare facility in central Bohemian Region.

In the conclusion the thesis compares my results with results of different authors. According to the results improvements are suggested in order to enhance data and information security of a facility.

Keywords

Risk; information security; cyber security; information leakage; cyberattack; medical facility; Central Bohemian Region.

Obsah

1 ÚVOD

Lidstvo se seznámilo s pojmem "Internet" teprve před 34 lety (r. 1987). Nicméně za tak krátkou dobu si již vybudoval pozici největšího úložiště dat na globální sféře. Každý rok se na celosvětovou síť ukládá více a více informací a jejich cena roste na hodnotě. Již dnes lze považovat informace za nejcennější aktivum. S tím ovšem roste i nutnost data více zabezpečit. I přesto každoročně dochází k rostoucímu počtu úspěšných útoků v kybernetickém prostoru.

Diplomová práce je zaměřena na rizika úniku informací z organizace. Teoretická část práce se věnuje odborné terminologii kybernetické a informační bezpečnosti. Následující podkapitoly pojednávají o hrozbách a rizicích informační bezpečnosti a útocích na data a informace. Rovněž se práce zabývá kybernetickou kriminalitou, kde jsou představeny a charakterizovány techniky sociálního inženýrství a malware (škodlivý kód). V závěru teoretické části práce jsou uvedeny příklady útoků na zdravotnická zařízení v České republice a jeden příklad i ze zahraničí.

Cílem diplomové práce je identifikace rizik úniku informací z lůžkového zdravotnického zařízení ve Středočeském kraji. Dále práce analyzuje a popisuje vybrané formy útoků s následkem úniku dat a informací ze zařízení. Na základě námi dosažených výsledků budou navržena případná doporučení pro zkvalitnění ochrany dat a informací v zařízení. Dílčím cílem je seznámit čtenáře s problematikou kybernetické a informační bezpečnosti. Práce se opírá především o českou odbornou literaturu. Rovněž je čerpáno z českých a anglických internetových zdrojů.

Výsledků bude dosaženo za pomoci odborných výzkumů provedených v lůžkovém zdravotnickém zařízení. První metodou výzkumného šetření je nestandardizovaný anonymní dotazník, který byl distribuován mezi

zaměstnance. Druhou metodou je polostrukturovaný rozhovor, který byl vedený s IT specialistou zajišťujícím bezpečnost dat v zařízení.

2 SOUČASNÝ STAV ŘEŠENÉ PROBLEMATIKY

Internet vznikl současně se vznikem počítačů před více než 70 lety, nicméně naprostá většina všech existujících dat v kyberprostoru vznikla v posledním desetiletí. Je to způsobeno nejen stále se rozšiřujícímu tzv. viditelnému webu, ale především Deep webu, který je složen převážně ze zaheslovaných datových souborů typu internetové bankovnictví, přístup k facebookovému účtu a jiné.

Součástí Deep webu jsou veškeré zaheslované soubory, ke kterým se běžný uživatel nedostane – pouze majitel těchto přihlašovacích údajů. Deep web stručně řečeno zahrnuje vše, co nám běžný internetový prohlížeč nevyhledá.

Internet tvoří z 96 % tzv. Deep web, zatímco viditelná část webu je tvořena pouhými 4 %. Deep web si mnozí pletou s tzv. Dark webem (neboli internetovým podsvětím), to je ovšem pouze malá část Deep webu, která je dohledatelná specializovanými prohlížeči (např. Tor). Dark web je tvořen již známým výskytem kriminální činnosti typu objednání vraždy, obchodu s drogami, dětskou pornografií a jiné. Dark web ovšem není tvořen pouze těmito zločineckými službami. Člověk zde také může najít zajímavé návody, recepty či názory na různá téma. Nejčastějšími návštěvníky a účastníky Dark webu tedy nemusejí být vyloženě kriminálníci.

V dnešním světě již nejsou nejcennějším aktivem majetky v podobě financí, nemovitostí, strojů apod. nýbrž informace – především ta datová. Proto se stává čím dál tím větší potřebou hledání způsobů, jak zefektivnit bezpečnost těchto dat.

Ačkoli se bezpečnost v kybernetice stále vyvíjí a přichází se na nové mechanismy zabezpečení v kyberprostoru, tak i zároveň útočníci se vyvíjí a přichází na nové způsoby útoků.

2.1 Vymezení základních pojmů v oblasti informační a kybernetické bezpečnosti

Aktiva jsou majetky hmotné i nehmotné, které mají pro daného jednotlivce a organizaci jistou důležitost, hodnotu. Jedním z nejcennějších aktiv této doby jsou informace a data, jejichž důležitost stoupá na hodnotě, ať už se jedná o soukromý nebo státní sektor [1].

Bezpečnost můžeme chápat jako vlastnost určující míru a úroveň ochrany subjektu nebo objektu. Také se může jednat o ochranu proti ztrátám. Do bezpečnosti v oboru informačních technologií se řadí ochrana integrity a diskrétnosti [2, 3].

Citlivá data jsou jedním z faktorů, které při jejich zneužití či krádeži mají zásadní dopad na chod organizace. Je zapotřebí tato data chránit [4].

Data jsou čísla, události, mapy, grafy. Seskupení dat dohromady tvoří informaci, která je důležitým materiálem pro adresáta [1].

Hrozba je jakýmsi jevem, událostí či procesem, který způsobuje poruchu, škodu nebo ztrátu aktiva. Hrozba může být příčinou kybernetické události poškozující organizaci [4].

Informační systém je jakýsi soubor zajišťující uspořádané shromažďování, zpracovávání a zachování informací a dat [5].

Internet je celosvětově propojený systém počítačových sítí používající normalizovaný internetový protokol (TCO/IP) [4].

IP adresa je souhrn čísel, které definují síťové rozhraní v počítačové síti [4].

Kybernetický prostor je digitální (umělé) prostředí, které zprostředkovává zpracování a vznik informací. Tvořen je informačními systémy a sítěmi elektronických komunikací [3].

Kybernetický útok lze chápat jako nezákonnou, nepovolenou činnost prováděnou útočníkem v kyberprostoru, a to za účelem krádeže a šíření osobních údajů, spam či obtěžování druhé osoby. Dle Jiráska a kol. je definicí kybernetického útoku: *„Útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace“* [55, s. 2].

Organizace může být jednotlivec nebo skupina jdoucí za stejným cílem [4].

Počítačová kriminalita je páchání trestné činnosti za pomoci počítače či trestné činy zaměřené proti počítači [6].

Riziko je jakýmsi nebezpečím. Jedná o pravděpodobnost, že určitá hrozba způsobí škodu organizaci, k čemuž využije zranitelnost aktiva organizace [1].

Uživatel je osoba používající počítačové zařízení a systémy pro vyhledávání informací [4].

Útok na počítačovou síť je druh kybernetického útoku. Útok je činnost způsobující narušení, omezení, ztrátu či úplnou destrukci informací uložené na sítích nebo v samotných počítačích [4].

Vektor útoku označuje způsob, jakým je využívána zranitelnost k napadení systému za použití malware či technik sociálního inženýrství [7].

Zranitelnost je slabé místo bezpečnostního systému, které může být využité hrozbou pro poškození aktiva [1].

Zranitelné místo je využitelnou slabinou informačního systému k zapříčinění ztrát [4].

2.2 Kybernetická bezpečnost

Bezpečnost je vlastnost prvku, jejímž hlavním úkolem je ho chránit. Kybernetická bezpečnost je jakýsi souhrn technických, organizačních, vzdělávacích i právních nástrojů, používané pro zajištění ochrany kybernetického prostoru. Tato oblast je odvětvím informační bezpečnosti uplatňované v počítačových sítí i samotné počítačové technice. Hromadnými postupy a nástroji mají být služby, citlivé údaje a cenné informace chráněné před jejich poškozením, zveřejněním nebo neoprávněnou manipulací [3, 4].

Důležitým orgánem a hlavním gestorem zajišťující kybernetickou bezpečnost v České republice je od roku 2017 – Národní úřad pro kybernetickou a informační bezpečnost [8].

Na základě zákona č. 205/2017 Sb., který novelizoval zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, vznikl Národní úřad pro kybernetickou a informační bezpečnost (dále jen NÚKIB), jehož hlavní činností je šířit osvětu a podporovat vzdělávání v oblasti kybernetické bezpečnosti. Dále chrání utajované informace v oblasti informačních komunikačních systémů. Také spolupracuje s ostatními národními týmy, kterými jsou CERT a CSIRT. NÚKIB je ústředním správním orgánem pro kybernetickou bezpečnost sídlící v Brně. V čele úřadu stojí ředitel, jenž je členem Výboru pro kybernetickou bezpečnost, což je stálý pracovní orgán Bezpečnostní rady státu (dále jen BRS) pro koordinaci plánování opatření k zajišťování kybernetické bezpečnosti České republiky [8, 9].

2.2.1 Soubor právních předpisů

Zákony a vyhlášky uplatňované v České republice v oblasti kybernetické bezpečnosti jsou následující:

- Ústava České republiky č. 1/1993 Sb.,
- Listina základních práv a svobod č. 2/1993 Sb.,
- Zákon č. 121/2000 Sb., autorský zákon,
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy,
- Zákon č. 127/2005 Sb., o elektronických komunikacích,
- Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti,
- Zákon č. 40/2009 Sb., trestní zákoník,
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti,
- Zákon č. 104/2017 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších přepisů, zákon č. 181/2014 Sb., o kybernetické bezpečnosti,
- Zákon č. 205/2017 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony,
- Zákon č. 110/2019 Sb., o zpracování osobních údajů,
- Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti [10].

2.2.2 Principy kybernetické bezpečnosti

V kybernetické bezpečnosti jsou uplatňovány principy tzv. triády kybernetické bezpečnosti.

1. Triáda CIA;
2. Prvky kybernetické bezpečnosti (lidé, technologie, procesy);
3. Životní cyklus bezpečnosti (prevence, detekce, reakce).

1. Triáda CIA

Triáda CIA je jednou z nejznámějších a nejvíce aplikovaných principů kybernetické bezpečnosti. Cílem je zajistit bezpečnost dat a informací v době jejich zpracovávání. Pod zkratkou CIA se skrývá význam tří základních atributů bezpečnosti [3].

- C (Confidentiality) – Důvěrnost;
- I (Integrity) – Celistvost;
- A (Availability) – Dostupnost.

Důvěrnost

V době nakládání s informacemi představuje důvěrnost jakousi jistotu, že jsou data chráněna a přístup k nim má pouze autorizovaná osoba. Narušení důvěrnosti nastává v době útoku, kdy dojde ke vstupu neověřeného uživatele do systému. Chránit tento atribut je možné šifrováním, a to současně s ukládáním dat. Důležité je zabezpečit veškeré přístupy do databází a zamezit tak neautorizovaným osobám přístup do systému. Taktéž se nesmí zapomenout na metody sociálního inženýrství. Zapotřebí je tedy povolit přístupy do databází pouze konkrétním zaměstnancům určené vrcholovým managementem organizace a předejít tak možným únikům dat a narušování důvěrnosti [11].

Pokud se zaměříme na důvěryhodnost v lůžkovém zdravotnickém zařízení, přístupy do databází mají v tomto případě zdravotní sestry, lékaři, radiologičtí asistenti, zdravotní laboranti, fyzioterapeuti a mnoho dalších zaměstnanců. K narušení důvěrnosti může v tomto případě dojít velice snadno, jelikož zaměstnanců je příliš mnoho, a tak nejde uhlídat veškeré jejich kroky. Dojde-li k narušení důvěrnosti, nemocniční pacienty to na životě nijak neohrozí. Ale může dojít k ohrožení z hlediska odcizení jejich osobních údajů či lékařské

anamnézy. Odcizení dat může pacientům způsobit finanční a psychickou újmu. V tento moment tedy pacient ztrácí důvěryhodnost v nemocnici. Útočník se za pomoci metody např. phishing zmocní utajených dat, které odcizí s vidinou finančního zisku. Tento útok může poškodit nemocnici na jejím jméně a ztratit tak důvěryhodnost i u dalších lidí [3].

Integrita

Exaktně se jedná o přesnost a správnost dat. Integrita je zachována, pokud obsah dat zůstává beze změny. To znamená, že na jejich ochranu jsou učiněna opatření zajišťující změnu neautorizujícím uživatelem. K narušení integrity může útočník docílit vpravením počítačového viru do systému nebo na síť. V případě použití trojského koně prostřednictvím infikovaného programu chovající se jako bezpečný program, dochází k odesílání dat ze systému organizace tzv. zadními vrátky. Útočník tak získá přístupová oprávnění, jejichž pomocí může bezmezně tato data měnit. Dalším možným narušením integrity organizace jsou její vlastní zaměstnanci, kteří svou neopatrností nebo zcela úmyslně odstraní soubory s tajnými daty (sabotáž) [3].

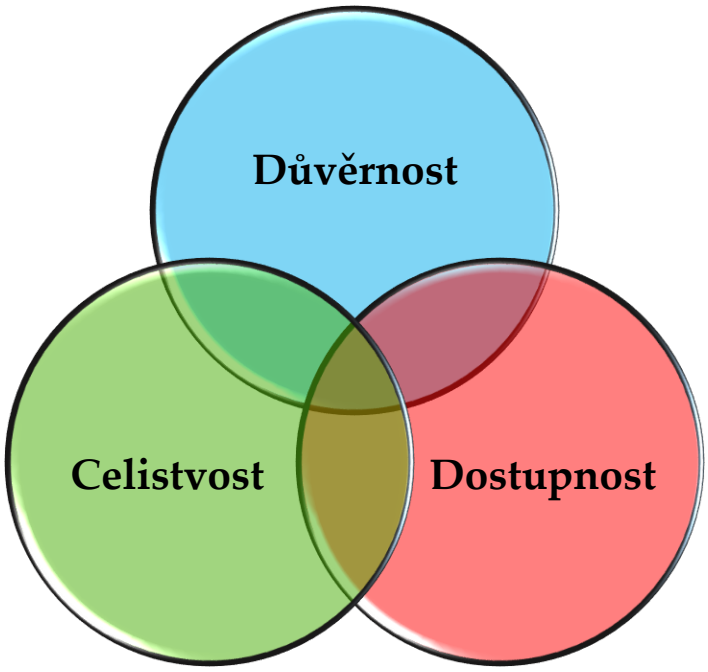
Pacienta může poškodit narušení integrity ve zdravotnickém zařízení, pokud dojde ke změně druhu nebo množství jeho předepsaných medikamentů [11].

Dostupnost

Posledním třetím atributem bezpečnosti je dostupnost, což je neustálá možnost přístupu k informacím. Na tuto část CIA triády se útočníci zaměřují nejvíce, jelikož mají dostatek informací a prostředků dostat se přes veškerá zabezpečení organizace a odcizit tak utajená data. Zároveň prostřednictvím ransomware mohou zablokovat celý systém a pro dešifrování vyžadovat

výkupné (finanční obnos). Jediným možným způsobem, jak chránit dostupnost je tvorba kopií na záložních zařízeních [11].

Tento útok by mohl napáchat fatální škody pacientům v lůžkové zdravotnické zařízení. Lékaři, zdravotní sestry, fyzioterapeuti a další personál by se nemohl dostat do systému, tím by došlo k narušení chodu nemocnice. Taktéž by došlo k ohrožení pacientů připojených na přístrojích, jelikož by mohlo dojít k zašifrování a automatickému odpojení ze sítě či elektrické energie. V takovémto případě je nutné mít náhradní zdroj elektrické energie. Tímto se dostupnost stává nekritičtějším místem z triády CIA [3].



Obrázek 1 - Triáda CIA [vlastní]

Propojením těchto tří základních atributů je zajišťována bezpečnost dat a informací v organizaci. Proto je velice důležité chránit tyto základní atributy bezpečnosti, a to před veškerými pokusy jimi proniknout a ohrozit tak bezpečnost dat.

2.3 Informační bezpečnost

Jedná se o multidisciplinární obor věnující se zabezpečení informačních a komunikačních technologií. Tyto systémy chrání informace a data v době jejich ukládání a zpracování za pomoci opatření (technická, organizační, fyzická a programová) působící proti poškození základních atributů bezpečnosti (integrity, důvěrnosti a dostupnosti) aktiv [1].

Neřeší se pouze bezpečnost systémů a technologií, ale také procesy organizace a chování osob, poněvadž největším zájmem jsou osobní data státních příslušníků a majetkové informace. Ochrana takovýchto dat je zaštítěna Ústavou České republiky (dále jen ČR) a Listinou základních práv a svobod [12].

Dle Martina Světlíka lze informační bezpečnost chápat jako obapolně propojená opatření mnoha typů bezpečnosti, pro zajištění dostupnosti, důvěryhodnosti a integrity informací [12].

Informační bezpečnost nabývá v současné době veliké důležitosti, jelikož hodnota informací roste, a to nejen v oblasti soukromého podnikání, ale i ve státní správě. Úkolem informační bezpečnosti je zajistit dostatečnou ochranu dat a informací organizace před vniknutím nepovolaných osob nebo subjektů, které se je snaží získat. Pomocí systémů a určitých postupů je možné zabezpečit organizace před okolními vlivy, nežádoucím chováním z řad pracovníků, úniku či až k destrukci důležitých dat. Dále je dbáno na nechtěné úniky dat, které by mohly organizaci poškodit a jiný subjekt by tak mohl získat jakousi výhodu. Každá organizace má však své vlastní postupy, jak zajistit informační bezpečnost. Existují však určitá pravidla, která musí být ze stran organizací splněna např. dostupnost služeb, zachování důvěrnosti a integrity dat [1, 13].

2.4 Hrozby informační bezpečnosti

Hrozba využívá zranitelnost, slabé místo aktiv (např. informační systém) pro jejich poškození. Útočníci je jejich prostřednictvím zneužívají pro získání cenných informací, souborů nebo pro samotné proniknutí do informačních systémů, které chtějí poškodit. Tím způsobí organizaci potíže a může dojít až k ochromení jejího chodu [14].

Na informační systém působí značné množství všelijakých hrozeb, kterým musí organizace čelit. Nejprve však musí rozpoznat, o jaký typ hrozby se jedná a na co se zaměřuje. K tomu jim dopomůže proces identifikace [15].

Hrozby můžeme souhrnně rozdělit do 2 skupin, a to dle míry zavinění člověkem:

1. **Objektivní hrozby**

   Mezi tuto skupinu patří hrozby přírodního, fyzického a technického charakteru. Pod přírodními hrozbami si můžeme představit například povodeň, požár, poruchu a výpadek proudu způsobený bleskem. Pro řešení těchto hrozeb je zpracováván havarijní plán. Technickými hrozbami jsou krádeže informací případně jejich poškození [14].

2. **Subjektivní hrozby**

   Tyto hrozby vyplívají z lidského činitele počínaje úmyslnými hrozbami, které jsou páchány vnějším útočníkem (špion, hacker, terorista), ale také i z řad personálu organizace (vnitřní útočník), jenž se stane z propuštěného, zhrzeného nebo nenasytného zaměstnance. Takřka 80 % útoků je iniciováno právě zevnitř interními zaměstnanci [15].

Tabulka 1 - Základní typy hrozeb [14]

Hrozby	Náhodné/ Objektivní	Úmyslné/ Subjektivní
Externí	Přírodní	Hacking
Interní	Lidský faktor	Sabotáž

Důležité je také posoudit, z jakého důvodu je vnější či vnitřní útok hrozbou uskutečňován. Útočníkovi může jít o poškození organizace a jejího chodu. Další možností je snaha poškodit dat, finanční profit, případně snaha vyvolat strach a paniku [1].

2.5 Rizika informační bezpečnosti

Riziko je jakousi pravděpodobností nebo potencialitou vzniku negativního jevu (škody, ztráty). Může být vyjádřeno mírou ohrožení. Procesem analýzou rizik je zjišťována míra rizika působící na organizaci. Tkví v odkrytí hrozeb, které s určitou pravděpodobností využijí nedostatky k realizaci. Výsledkem analýzy jsou doporučená protiopatření, která pomohou snížit rizika. Existuje ovšem také zbytkové riziko, do kterého se nevyplatí investovat, jelikož nezpůsobuje tak velkou škodu, anebo se nachází velmi výjimečně. Ochrana proti riziku závisí především na financích. To znamená, že čím je vyšší míra zabezpečení, tím jsou samozřejmě vyšší finanční náklady [16, 17].

Důležité je poukázat na rizika přicházející skrz internet. Jsou jimi např. viry, červi, spamy, spawery nebo může docházet k odposlechu. Riziko může být znázorněno jako vzorec: **R= P x N x H**

- R = míra rizika;
- P = pravděpodobnost vzniku;
- N = pravděpodobnost následků;
- H= názor hodnotitelů [18].

K realizaci analýzy rizik je možné využít 4 přístupy, jenž se se svým rozsahem od sebe liší především vstupním kapitálem. Důvodem, proč dochází k analýzám, je ten, že je potřeba předejít bezpečnostnímu incidentu nebo aspoň snížit pravděpodobnost vzniku a jeho možným následkům [19].

Možné 4 přístupy k provedení analýzy rizik jsou následující:

1. **Základní přístup** analýzy vychází ze všeobecných standardů. Samotně se nijak neprovádí. Pouze jsou přijata určitá opatření v oblasti bezpečnosti.
2. **Neformální přístup** je realizován bezpečnostními znalci na základě jejich znalostí a zkušeností. I když se jedná o rychlou metodu, je doporučována pouze pro okamžité východisko. Důležité je poté provést detailnější analýzu.
3. **Podrobná analýza rizik** je nejpřesnější a zároveň i finančně nejnáročnější metodou mající určitou posloupnost stanovení úrovně zranitelnosti organizace. Nejprve se identifikují aktiva organizace, která se poté ohodnotí, a na základě toho se posoudí hrozby jej ohrožující. Poté je určena míra rizika pro každé jednotlivé aktivum. Následně jsou navržena protiopatření eliminující tato rizika.
4. **Kombinovaný přístup** hodnotí výlučně jen některá odvětví a na zbytek využívá zároveň přístup základní a neformální [20].

Analýza rizik se zaměřuje na veškerá aktiva organizace. Nezapomíná ani na další jednotlivé oblasti bezpečnosti, do kterých spadá:

- datová bezpečnost;
- komunikační bezpečnost;
- fyzická a personální bezpečnost;
- programová bezpečnost;
- technická bezpečnost;
- režimová bezpečnost [20].

2.6 Útoky na data a informace

Jak už bylo v předchozích kapitolách naznačeno, nejslabším článkem bezpečnostního prostředí je právě člověk, který je zároveň nejčastějším faktorem úniku dat a informací z organizace [21].

Podle průzkumů společnosti Accenture je ¾ útoků iniciováno právě z řad zaměstnanců. Pouze z ¼ je útok iniciován hackerem. Jedná se především o odesílání citlivých údajů na špatnou e-mailovou adresu, nahrání citlivých informací na externí disk, který nakonec ztratí, anebo uložení tajných souborů na veřejné úložiště [22].

Výjimkou nejsou ani nasmlouvaní pracovníci (externí). Někdy dochází k nahrazení bývalého pracovníka za podplaceného pracovníka od konkurenční organizace, který sbírá tajné (citlivé) informace a poté je organizaci poskytuje [1].

Předejít únikům dat a informací z organizace není nijak snadné. Je ale možnost, jak lze snížit nebo předejít nebezpečí úniku. Důležité je nepodcenit riziko už při přijímacím řízení. Při přijímání nového pracovníka na podstatné místo v organizaci je zásadní položit základní otázky týkající se konkurenční společnosti: zda u konkurence někdy pracoval či u konkurenční společnosti nepracuje osoba blízká [23].

Nejjednodušším odcizením informací je tzv. přímá krádež, kdy zaměstnanec má volný přístup do všech laboratoří a kanceláří. Ke krádežím dochází převážně v noci, kdy jsou tyto místnosti prázdné. Samozřejmě to není pravidlem, tyto krádeže se provádí i za bílého dne přímo před očima ostatních zaměstnanců [12, 24].

2.6.1 Klasifikace útočníků na informační systém organizace

Informační systémy jsou napadány různými způsoby. Útočníci využívají zranitelná místa organizace k provedení útoku a proniknutí tak do informačního systému. Hrozby využívají tyto slabiny informační bezpečnosti k ohrožení aktiv organizace. Kombinací útočníka, hrozby a zranitelného místa vzniká riziko [25].

Základní klasifikace útočníků dle jejich logické polohy je:

- **Vnitřní útočník** je osoba mající přístup do komunikační sítě organizace. Primárně se jedná o jejího zaměstnance. Nicméně to mohou být taktéž i lidé, kteří nepracují v organizaci. K činu přimějí některého ze zaměstnanců pod hrozbou nebo mu za spolupráci nabídnou finanční odměnu. Existují jakési dvě pomyslné linie bezpečnostních incidentů vykonané vnitřním útočníkem. Můžeme je rozdělit na incidenty z nedbalosti, kdy zaměstnanec svou neopatrností odstraní citlivá data nebo incidenty provedené za vidinou zbohatnutí či pomsty [1].
- **Vnější útočník** je osoba nemající přístup do komunikační sítě v organizaci. Pokud chce napadnout vnitřní komunikační systém, musí očekávat nelehkost tohoto úkonu, poněvadž tyto systémy mají ochranné zabezpečení, kterým se budou bránit proti neautorizovanému vniknutí. Proti vnitřním útočníkům tak mají nevýhodu. Na druhou stranu vystopovat takového to útočníka je pro správce sítě velmi obtížné [12].

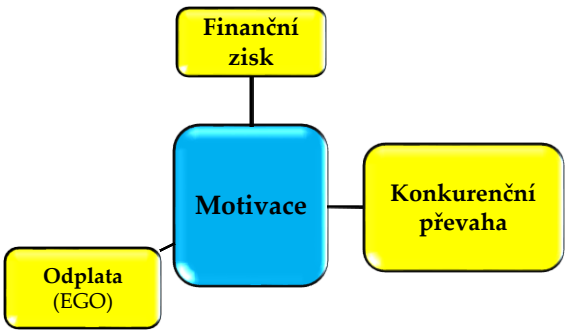
Dále můžeme útočníky rozdělit do 3 skupin dle nebezpečnosti:

- **Amatéři** jsou nezkušená skupina lidí útočící na server dle postupů volně dostupných na internetu nebo prostřednictvím staženého primitivního programu. Ke zdařilému útoku dochází velmi výjimečně, jelikož dokáže napadnout pouze nezabezpečené informační systémy [26].

- **Hackeři** jsou velmi vzdělaní lidé v oblasti výpočetní techniky. Jedná se především o vysokoškolské studenty, kteří po dobu jejich studia sbírají zkušenosti a nabývají znalostí. Záměrem útoků není vždy někomu uškodit. Především se jedná o studentskou zvědavost a ověření svých schopností a znalostí získaných při studiu. Pokud ale půjde o záměr poškodit informační systém, jsou tito útočníci pro organizaci nebezpeční [25].
- **Profesionálové** jsou skupinou zločinců, která má veškeré potřebné vybavení, dostatek času i znalostí. Pro organizace jsou největším nebezpečím, jelikož se zejména zajímají o jejich citlivá data, informace a tajné soubory. Většina organizací není proti těmto útokům zajištěná, jelikož na to finančně nedostačují. Jsou jimi např. zdravotnická zařízení. Zastavit je mohou jen velmi silná bezpečnostní protiopatření [25–27].

2.6.2 Motivace útoku

Hlavním motivem útočníků je primárně finanční zisk. Většina kyberzločinců své útoky míří na banky, finanční společnosti nebo na zdravotnická zařízení, čímž získají utajená citlivá data, která pak mohou prodat či si říct o výkupné za navrácení. Ovšem finanční zisk není jediným motivem. Další motivací pro útok může být zisk konkurenční převahy. Mnohdy je motivem jakýsi způsob odplaty, kdy se např. bývalý zaměstnanec mstí bývalému zaměstnavateli [28].



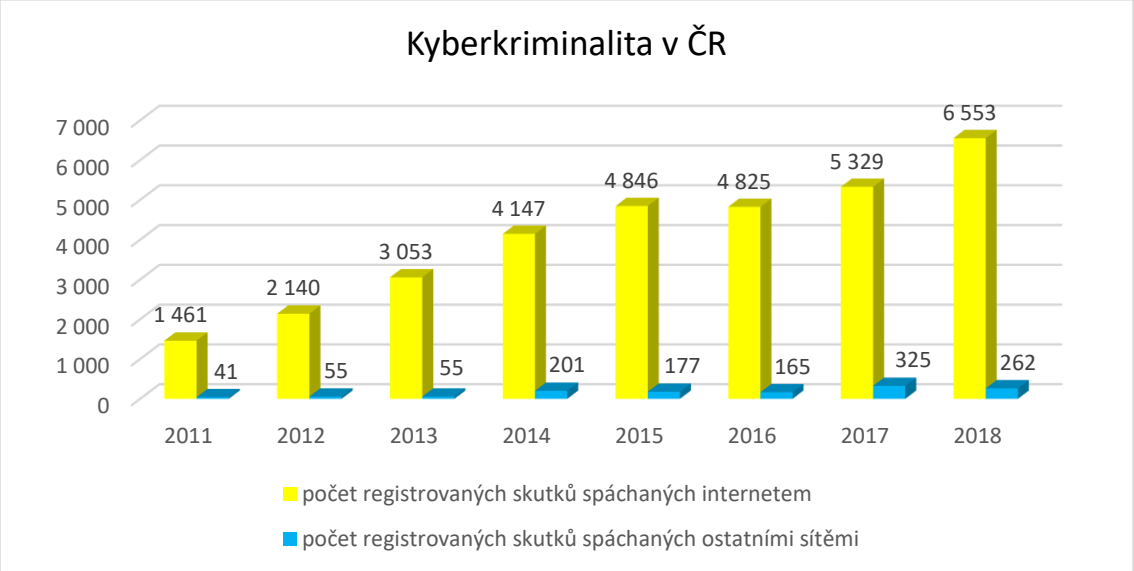
Obrázek 2 - Diagram motivace útočníků [vlastní]

2.7 Kybernetická kriminalita

„Trestná činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení (včetně dat), případně větší množství počítačů samotných nebo propojených do počítačové sítě, a to buď jako předmět zájmu této trestné činnosti (s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité) nebo jako prostředí (objekt) nebo jako nástroj trestné činnosti“ [1, s. 33].

Projev kybernetické kriminality můžeme vnímat pouze prostřednictvím strojů a přístrojů mající přístup do kyberprostoru. V tomto prostředí se útočníci mohou velmi nenápadně pohybovat, měnit své identity či dokonce nepozorovatelně mizet. Útočník využívá kybernetického prostoru pro tvorbu hrozeb a její následnou realizaci. Ať už se jedná o kriminální trestnou činnost v reálném či virtuálním světě, vždy bude představovat jakousi hrozbu pro společnost [29].

V České republice bylo od roku 2011 do roku 2018 napácháno škod v hodnotě 3 372 453 Kč v registrovaných skutcích spáchaných internetem a ostatními sítěmi [30].



Obrázek 3 - Kyberkriminalita v ČR roku 2011 - 2018 [28]

2.8 Sociální inženýrství

„Pouze dvě věci jsou nekonečné: vesmír a lidská hloupost. Ačkoli tím prvním si nejsem jist.“ Albert Einstein

Sociální inženýrství se mnohdy nepovažuje jako druh kybernetického útoku, nicméně je častým předpokladem, aby řada kybernetických útoků byla úspěšná. Dochází k přemlouvání, ovlivňování nebo manipulaci lidí s cílem přimět je provést nezákonnou činnost či získat informace, které jsou pro útočníka nepřístupné. Jedná se především o citlivé informace týkající se organizace, osobních údajů zaměstnanců nebo ve zdravotnických zařízeních i pacientů. Bezpečnostní systémy nebudou nikdy dokonalé, jelikož jsou v určité fázi vždy závislé na člověku, který je tím nejslabším článkem systému. Útočník (sociotechnik) tak využívá získané důvěry oběti, lidské hlouposti i neopatrnosti [2, 31, 32].

Existují 3 způsoby útoků sociálního inženýrství, jež jsou vzájemně propojovány. Jsou jimi:

- Sběr veřejně dostupných dat;
- Fyzický útok;
- Psychologický útok [2].

Častými metodami útoků sociálního inženýrství jsou:

- Telefonický hovor;
- Útok tzv. „tváří v tvář“;
- Falešný servisní technik;
- Nabídky online služeb organizaci;
- Podvodný e-mail;
- Ponechání paměťového média v zájmové oblasti (např. USB obsahující malware) [2, 12].

Cílem útoků se může stát např.:

- IT oddělení;
- Recepční pracovníci;
- Bezpečnostní pracovníci;
- Správci budov;
- Řídící pozice [2].

2.8.1 Phishing

Jedná se o metodu sociálního inženýrství snažící se získat osobní citlivé informace jako jsou hesla, rodná čísla či bankovní platební údaje. Šíří se e-mailem nebo odkazem, který hacker infikuje. Uživatel, který na odkaz klikne, bude přesměrován na falešně vytvořené webové stránky [33].

První znaky phishingu se začaly objevovat už v roce 1995, kdy se útočníci soustředili především na finanční společnosti a banky. Rozesílali zaměstnancům e-maily pobízející k obnově jejich platebních a přihlašovacích údajů z důvodu výskytu problému s vyúčtováním. Tímto způsobem se útočníci snadno dostávali k osobním údajům a bankovním účtům, ze kterých poté vybrali peníze [34].

V minulých letech byla tato metoda získávání dat a informací velmi úspěšná, ovšem to dříve nezasáhlo tolik lidí, jako by tomu mohlo být v současné době a s dnešní formou phishigu [34].

2.8.2 Pharming

Pharming je novější verzí phishingu. Pro svůj útok používá speciální počítačové programy, jimiž dokáže napodobit např. stránky internetového bankovnictví. To znamená, že uživatel při přihlašování do online bankovnictví bude přesměrován na stránku vytvořenou útočníkem. Tímto způsobem získá

útočník potřebné informace (přihlašovací login a heslo) a může dojít k odcizení finančních prostředků z klientova účtu [35].

2.9 Malware

Zjednodušeně se jedná o infikovaný software, který se využívá k narušení počítačových systémů pro získání informací či k dosažení vstupu do systému. Malware se šíří do počítačového zařízení prostřednictvím e-mailu. Napadená zařízení nemající schráněný software se stávají jednoduchými cíli pro hackery [36].

Existuje několik forem malwaru. Už samotný název některých odkrývá jejich působení na počítačový systém. Mezi druhy malware patří: **Adware, Spyware, počítačové viry, Keylogger, Trojský kůň a Ransomware**.

2.9.1 Adware

Celým anglickým názvem advertising-supported software je v překladu software podporující reklamu na webových stránkách. Poprvé se objevil v roce 1987. Adware je zobrazován formou vyskakovacího okna (pop-up okna) v prohlížeči nebo v panelu nástrojů. Patří mezi ty méně nebezpečné malwary, které nepředstavují značné riziko, akorát obtěžuje uživatele. Většina se snaží sledovat aktivitu uživatele a tím odcizit osobní data [37].

2.9.2 Spyware

Tento druh malware je používám na sledování ostatních uživatelů pro zisk osobních a bankovních údajů. Tyto informace sbírá skrytě, takže jeho odhalení bývá velmi těžké. Existuje i typ spyware, který hackerovi dovolí odposlouchat veškeré informace, které prostřednictvím klávesnice napíšete [38].

Jak se spyware objeví ve vašem počítači? Jednoduše je stažený spolu s aplikací, programem nebo se nainstaluje otevřením infikovaného e-mailu. Jelikož odhalení takovéhoto typu je velmi obtížné, většina populace o jeho nainstalování ani neví. Jediným východiskem je mít nainstalovaný antivirový program, jehož součástí je i funkce ochrany specializující se na spyware. Tím je zajištěno jeho odhalení a následné odstranění ze zařízení [39].

2.9.3 Keylogger

Jedná se o typ spyware, který zaznamenává přesné pohyby klávesnice provedené uživatelem na počítači. Dochází k tomu na napadnutém počítačovém systému. Útočníci ho využívají pro získání uživatelova přihlašovacích údajů k jeho účtům (číslo účtu, bankovní informace, platební karty, uživatelská jména, hesla), ke kterým se prostřednictvím počítače přihlásí [2].

Odhalení keylogger je pro laika velmi obtížné. Jedinými náznaky infikovaného počítačového systému je zpomalený kurzor myši či chybné zobrazení stránek. Obranou před tímto typem spyware je dvoufázové přihlašování a ověřování. Nejdůležitější je mít ale antivirový program, který před takovýmto napadením systém ochrání [40].

2.9.4 Počítačový vir

Jedná se o samovolně spustitelný závadný kód nebo program v počítači. V momentě, kdy k takovému spuštění dojde, virus se začne množit. Dokáže se šířit z jednoho počítače na druhý počítač. Napadne informační systém a převezme nad ním veškerou kontrolu. Projevy těchto virů bývají různorodé. Od těch méně škodlivých, které způsobí přeplnění systému až po ty, co provedou ztrátu nebo zničení dat [41].

Počítačové viry se dají rozdělit dle souborů které napadají:

- Boot viry;
- Souborové viry;
- Multiparitní viry;
- Makroviry [2].

2.9.5 Trojský kůň

Jedná se o počítačový program obsahující skryté funkce, o kterých uživatel nemá povědomí. Trojský kůň se snaží narušit základní atributy bezpečnosti, o kterých je více pojednáváno v podkapitole 2.2.2. Tento typ malware se oproti počítačovému viru nedokáže samostatně šířit. K jeho replikaci je zapotřebí uživatelova pomoc. Obvykle se šíří prostřednictvím infikované přílohy v e-mailu nebo je ukryt v programech či filmech, které se dají bezplatně stáhnout [19].

Odhalení takového malware není nijak těžké. Většinou se projeví rapidním zpomalením procesoru, jelikož dojde k zesílení zátěže. Zbavit se trojského koně lze pouze postupným odstraněním veškerých programů, které jsou jím infikovány [42].

2.9.6 Spam

Spam je jakákoli forma nevyžádané hromadné digitální komunikace reklamního charakteru. Nejčastěji má podobu e-mailové zprávy. Lze se s ním také setkat v SMS a MMS zprávách, na Skype nebo sociálních sítích. Podstatnou část spamu tvoří scam, který obsahuje kriminální obsah [43].

Existují tři druhy scam, kterými jsou:

- Scam 419 (Nigerijské dopisy) – přenos podvodu z reálného světa do kyberprostoru;
- Hoax – řetězová zpráva uvádějící nepravé informace;

- Podvodné nabídky – nabídky na výhodné půjčky a práce z domova [2].

Proti tomuto typu malware je však možné se chránit pouze nainstalovaným antivirovým programem s funkcí antispam [44].

2.9.7 DoS, DDoS útoky

Denial of Service a Distrubuted Denial of Service jsou, jak už název vypovídá, úmyslné odmítnutí služeb nebo přístupu autorizovaným uživatelům k informačnímu systému v počítači. DDoS útok zajistí zahlcení systému množstvím dat (e-mailů) z mnoha zařízení, a to v krátkém čase, čímž dojde k omezení serveru. Může dojít až ke krátkodobému výpadku celého systému. Nicméně jsou často využívány jako dodatkový útok, pro zakrytí stop [29, 45].

2.9.8 Ransomware

Jedná se o škodlivý druh programu, který zamezí přístupu všem autorizovaným uživatelům do počítačového systému nebo do potřebných složek. Útočník, který provádí tento úkon, poté požaduje výkupné za prozrazení dešifrovacího klíče (hesel) k obnovení přístupu do složek a systému [46].

Za nejnebezpečnější útoky v ČR na nemocnice může právě tento typ malware. Existuje mnoho typů Ransomware. Mezi ty známější patří:

- WannaCry;
- Phobos (Eking);
- Defray;
- Cryptolocker;
- Petya;
- Locky [47].

Dle pana Koloucha můžeme rozeznávat 2 druhy ransomware, a to podle omezení operačního systému:

1. Ransomware, který omezuje funkce celého počítačového systému. Dochází k úplnému zablokování.
2. Ransomware, který uzamkne soubory pro autorizované uživatele, ale operační systém zůstane bez dotčení. Tento druh útoku se nazývá Crypto-ransomware [2].

Cílem a hlavním motivem těchto útoků je finanční zisk. Obvykle si útočníci žádají o vyplacení výkupného v kryptoměnách (např. Bitcoin), jelikož platbu nelze stornovat. Další výhodou transakce Bitcoinem je fakt, že odesílatel/příjemce je nedohledatelný za předpokladu, že svojí bitcoinovou adresu v minulosti nikdy neztotožnil se svou osobou. Na druhou stranu, pokud již je znám vlastník bitcoinové adresy, jsou v blockchainu (decentralizovaná účetní kniha neboli databáze všech transakcí Bitcoinem) zaznamenány všechny historické transakce, které byly spojeny s danou bitcoinovou adresou. Existují ovšem mnohem více anonymizované kryptoměny (např. Monero, Zcash, apod.) [48].

2.10 Kybernetické útoky na zdravotnická zařízení

V této kapitole budou popsány případy kybernetických útoků na zdravotnická zařízení v České republice a jeden případ, který se uskutečnil v německém Düsseldorfu.

Proč všechny tyto kybernetické útoky fungují, a to včetně těch, které jsou zaměřeny na zdravotnická zařízení?

Prvním způsobem, který je nejčastěji využíván k jakémukoli kybernetickému útoku, je uživatel. Lidský faktor je nejslabším článkem organizace. Jeho mozek, únava, jeho neohleduplnost, toho všeho si útočníci všímají. Útoky plánují tak,

aby sociální inženýrství směřovalo na tu část mozku, která musí jednat okamžitě. Více o sociálním inženýrství je projednáno v kapitole 2.8. Druhým způsobem útoku na nemocnice jsou tzv. DoS/DDoS útoky (kapitola 2.9.7). Útočníky je napsán e-mail či dojde k vybídnutí, aby nemocnice zaplatila výkupné a pokud tak neučiní, útočníci podniknou DoS/DDoS útok, který pozastaví veškerou její činnost. Další možnou metodou je zveřejnění odcizených dat. Tato cesta se ještě neobjevila, podle docenta Jana Koloucha je ale otázkou, kdy se objeví [49].

Národní úřad pro kybernetickou a informační bezpečnost upozorňuje na nedostatečnost ochrany proti kybernetickým útokům, a to především ve větších organizacích, zejména pak ve zdravotnických zařízeních [8].

2.10.1 Horažďovická nemocnice

Jeden z prvních případů kybernetického útoku v České republice se stal na začátku ledna roku 2018. Terčem útoku bylo zdravotnické zařízení na Klatovsku. Horažďovická nemocnice následné péče se specializuje především na péči o dlouhodobě nemocné. Zde útočník směřoval svůj útok na počítačové sítě rentgenového oddělení k odcizení RTG (rentgenových) snímků. Dle mluvčího Horažďovické nemocnice pana Jiřího Kokošky, ale k úniku dat nedošlo. Útočník se přes zabezpečení počítačového systému nedostal. Podařilo se mu ale zašifrovat jeho část, která ale neomezovala nijak chod nemocnice a pacientům tak byla poskytnuta potřebná péče [50].

V lednu o 3 roky později byla nemocnice opět terčem útoku. Tentokrát se ale jednalo o phishing útok instruovaný skupinou hackerů, kterým se povedlo zašifrovat část informačních systémů a neoprávněně smazat některá data. Celý útok trval necelé 2 dny a způsobil škody v hodnotě 150 tis. Kč. Nemocnice se z útoku vzpamatovávala necelý týden, a to i přes poradenství a informace poskytnuté NÚKIB [51].

2.10.2 Léčebna v Janově na Rokycansku

Velký kybernetický útok proběhl na léčebnu tuberkulózy a respiračních onemocnění v Janově koncem června roku 2018. Zde se jednalo o útok malware – ransomware. Hacker napadl počítačovou síť a jelikož léčebna disponuje pouze 30 počítači, většina byla útokem zasažena a data z nich zcela smazána. Hackerovi se podařilo získat hlavní přístup k úložišti dat, které poté zašifroval a požadoval výkupné ve virtuální měně BTC. Vedení ovšem na tuto výzvu nereagovalo. Systém se jim podařilo obnovit během následujících 2 dnů díky zálohám dat [52].

2.10.3 Nemocnice Rudolfa a Stefanie Benešov

Nemocnice Rudolfa a Stefanie Benešov byla dne 11. prosince 2019 ve 3 hodiny ráno napadena kybernetickým útokem. Prvními náznaky útoku byly neobvyklé aktualizace systému, kterých si povšimnul IT technik nemocnice. Ve 3:30 v noci došlo k vypnutí celé sítě. Zdravotnické zařízení přišlo tímto útokem o objednávkový systém dárců krve sdílený na internetu a zároveň byla odcizena ekonomická a administrativní data. Největší omezení ale nastalo v poskytování péče, jelikož nemohlo dojít k několika lékařským zákrokům. Dále se odložila plánovaná vyšetření a zároveň došlo k omezení prodeje a výroby krevních derivátů. Jelikož nemocnice nemohla poskytnout dostatečnou péči, byla poskytnuta pouze hospitalizovaným pacientům. Vážnější případy byly převezeny záchrannou službou do okolních nemocnic v Příbrami, Říčanech, Sedlčanech, Mladé Boleslavi, Kolína a do nemocnice Krč v Praze [53].

Vektorem útoku byl phishing v kombinaci se třemi malware – ransomware Ryuk, trojského koně a botnet Emotet. Komunikace mezi nemocnicí a aktéry útoku neproběhla přímo, jelikož žádost o výkupné aktéři zaslali prostřednictvím e-mailu. Nemocnice na tuto žádost ovšem nereagovala. Cílem útoku nebyla

pouze tato nemocnice, ale i další instituce státní správy. Po dobu 7 dnů byl provoz nemocnice plně paralyzován. Do plné funkce se ji podařilo dostat po 19 dnech. Tento kybernetický útok způsobil nemocnici Rudolfa a Stefanie Benešov škody v hodnotě 59 tis. Kč. Tento útok poukazuje na zranitelnost nemocnic [54, 55].

2.10.4 Zdravotnické zařízení XY Středočeského kraje

Kybernetický útok započal 13. 1. 2020, kdy byl napaden server dvěma aktéry. První jej zneužil k těžbě kryptoměny MONERO (dále jen XMR). Druhý útočník získal přístup k administrátorskému účtu skrze RDP (Remote Desktop Protocol), který zašifroval server ransomware Eking [56].

Dle informací IT oddělení se jedná o dva servery mimo správu a IT infrastrukturu zdravotnického zařízení. Na serverech byl provozován manažerský informační systém společnosti XYZ, která také měla k virtuálním serverům výhradní přístup. V tomto případě nebyla narušena bezpečnost zdravotnického zařízení, byl však napaden server firmy, která jej spravovala. Z důvodu udání interních údajů a stále probíhajícího vyšetřování, zůstane zdravotnické zařízení a firma v anonymitě [56].

Na serveru taktéž došlo k neautorizovaným odchozím RDP spojením a puštěním několika podezřelých souborů, které ovšem byly druhým aktérem zašifrovány a nebylo je tedy možné analyzovat [56].

Dne 13. 1. 2020 byl stroj kompromitován a vzhledem k nedostatečně nastavenému systému Windows bylo možné zjistit, jakým způsobem byl stroj kompromitován. O měsíc později, dne 13. 2. 2020 byly zaznamenány 2 odchozí RDP spojení na IP adresy a poté byl na stroji vytvořen a spuštěn soubor Microsoft.exe. Další aktivita útočníka byla zaznamenána na konci měsíce května.

Bylo uskutečněno další odchozí RDP spojení, a to na další IP adresu, a poté byly spuštěny další programy [56].

V analyzovaném stoji bylo nalezeno několik nestandartních programů. AntiRecuvaAndDB.exe je ransomware Eking patřící do rodiny Phobos. Po spuštění souboru vypíná firewall a znemožňuje spuštění či obnovení systému. Šifruje všechny soubory na lokálních i sdílených discích. Jelikož šifrovací algoritmus byl útočníky použit správně, není dostupná žádná možnost, jak ztracená data získat zpět [56].

Provoz IT infrastruktury a aplikací nemocnice nebyl nijak narušen. Na základě testů a analýzy nedošlo k proniknutí škodlivého software k IT aktivům nemocnice a nedošlo k úniku dat nebo narušení základních atributů bezpečnosti [56].

2.10.5 Fakultní nemocnice Brno

Fakultní nemocnice Brno (dále jen FN Brno) byla napadena kybernetickým útokem 13. března 2020, a to den po vyhlášení nouzového stavu v České republice z důvodu pandemie SARS–CoV–2. Tímto útokem byly napáchány škody v hodnotě 100 mil. Kč [57].

Útok započal ve 2 hodiny v noci, kdy byl útočníkem postupně vyřazován systém a jednotlivé složky. IT oddělení na útok zareagovalo rychle a vyplo všechna počítačová zařízení v nemocnici. Lékaři se tak nemohli dostat do databází a zapisovat tam veškerá potřebná data. Taktéž nebylo možné používat RTG. Ve FN Brno musely být odloženy veškeré naplánované operace a akutní případy byly převáženy do okolních nemocnic. Útok zasáhl Dětskou nemocnici a porodnici na Obilním trhu [57].

K útoku byl použit phishing v kombinaci s ransomware – Defray. K jeho úspěšnosti přispěla unavenost a přepracovanost zaměstnanců v důsledku pandemie, poněvadž otevřeli infikovanou přílohu, jenž byla součástí e-mailu, a to mělo za následek stažení ransomware – Defray. Omezeny tak byly některé systémy. Nicméně základní provoz nemocnice byl zachován. Došlo k odcizení administrativních a ekonomických dat a ke smazání internetového objednávkového systému dárců krve podobně jako v nemocnici Rudolfa a Stefanie Benešov. To bylo poté dočasně nahrazeno telefonickým systémem. FN Brno požádalo o pomoc náměstka pro informatiku a digitální transformaci Vlastimila Černého z Fakultní nemocnice v Praze. Naštěstí se většina záznamů pacientů dokázala obnovit z historie a z konverzace e-mailové komunikace [58].

2.10.6 Univerzitní klinika v Düsseldorfu

Ve středu 10. září 2020 se stala terčem kybernetického útoku Univerzitní klinika v Düsseldorfu. Vektorem útoku byl ransomware, jehož následkem došlo k selhání 30 serverů. Útočníci využili zranitelné místo v zabezpečení software, který je běžně dostupný. Personál tak neměl přístup do databází s lékařskými záznamy pacientů. Museli tak odložit veškeré plánované operace a akutní pacienti museli být převezeni do okolních nemocnic [59].

Ve čtvrtek v noci z 11. 9. na 12. 9. byl záchrannou službou oznámen příjezd pacientky ve stavu ohrožení života. Kvůli útoku ji klinika nemohla přijmout, a tak byla převezena do nemocnice vzdálené 30 km. Pacientka po převozu do nemocnice zemřela. Jedná se o jeden z prvních případů, kdy si kybernetický útok vyžádal lidský život [60].

Podle německé policie hackeři neměli v úmyslu útočit na kliniku v Düsseldorfu. Jejich cílem byla Univerzitní škola Heindricha Heine. Když se skupina kyberzločinců dozvěděla, že jejich útokem bylo zašifrováno

zdravotnické zařízení, okamžitě útok ukončila a předala veškeré šifrovací kódy na obnovení systému [61].

2.10.7 Rok 2021

Kybernetické útoky na zdravotnická zařízení se v roce 2021 zvýšily o 45 %, uvedla bezpečností firma Check Point [62].

V lednu byla terčem kybernetického útoku opět Horažďovická nemocnice. Dne 4. 3. 2021 byl spáchán kybernetický útok na Ministerstvo práce a 16. 3. 2021 byly napadeny další 3 polikliniky. Ve většině případů byl použit phishing útok s kombinací nějakého typu ransomware [51].

NÚKIB upozorňuje na zvýšené riziko výskytu kybernetických útoků v České republice, jelikož aktuální dění tomu všemu napomáhá. Proto byla vytvořena analýza nejčastějších technik, které jsou využívány útočníky a zároveň, jaká zranitelná místa k tomu zneužívají. Tuto analýzu lze nalézt na stránkách NÚKIB [63].

3 CÍLE PRÁCE A HYPOTÉZY

Diplomová práce si především klade za cíl identifikaci rizik úniku informací. Dále práce popisuje vybrané formy útoků, jejichž následkem je únik dat a informací z lůžkového zdravotnického zařízení ve Středočeském kraji.

Dílčí cíle práce:

- V teoretické části seznámit čtenáře s problematikou kybernetické a informační bezpečnosti;
- Zjistit, zda zaměstnanci lůžkového zdravotnického zařízení jsou školeni v oblasti kybernetické bezpečnosti;
- Potvrdit nebo vyvrátit naformulované hypotézy;
- Navrhnout případná doporučení pro zkvalitnění ochrany dat a informací.

3.1 Stanovené hypotézy

Do diplomové práce byly zvoleny následující hypotézy:

HYPOTÉZA 1 *Alespoň 70 % respondentů absolvovalo školení v oblasti kybernetické bezpečnosti.*

HYPOTÉZA 2 *Více jak polovina respondentů se při odchodu od počítače odhlásí.*

HYPOTÉZA 3 *Alespoň 10 % respondentů se setkalo s nabádáním k šíření osobních údajů o pacientovi.*

HYPOTÉZA 4 *IT oddělení má sepsané postupy, jak reagovat na případný kybernetický útok.*

4 METODIKA

Pro zpracování praktické části diplomové práce byl sběr dat uskutečněn na základě kvantitativní metody výzkumného šetření pomocí nestandardizovaného anonymního dotazníku (viz příloha 1) určeném zaměstnancům nemocnice. Dále byla použita metoda kvalitativního výzkumného šetření v podobě rozhovoru (viz příloha 2), který byl proveden s IT specialistou zajišťujícím bezpečnost dat a informací lůžkového zdravotnického zařízení ve Středočeském kraji.

4.1 Anonymní nestandardizovaný dotazník

Do diplomové práce byla zvolena metoda kvantitativního výzkumného šetření formou nestandardizovaného anonymního dotazníku vlastní konstrukce. Podmínkou výběru respondentů byl pracovní poměr (zaměstnanec) ve zkoumaném lůžkovém zdravotnickém zařízení ve Středočeském kraji.

Šetření nebylo omezeno věkem, pohlavím a ani délkou profesní praxe. Odkaz na dotazník v elektronické podobě byl vložen na intranet zdravotnického zařízení, kam mají všichni pracovníci umožněn přístup. Dotazníkové šetření probíhalo od 26. března 2021 do 26. dubna 2021 ve formě online dotazníků z důvodu nastalé pandemie SARS–CoV–2.

4.1.1 Výzkum šetření

Do diplomové práce byl použit již zmiňovaný anonymní nestandardizovaný dotazník vlastní konstrukce, který se skládal celkem z 21 otázek. Rozdělen byl na jakési 4 pomyslné části. První část pojednávala o dotazované osobě. Druhá část se zaměřovala na školení v oblasti kybernetické bezpečnosti. Třetí část byla zaměřena na přístupy do informačního systému. Poslední čtvrtá část obsahovala doplňující otázky týkající se kybernetické a informační bezpečnosti.

Výsledky výzkumného šetření byly následně zpracovány a zaneseny do přehledných grafů a tabulek.

4.2 Polostrukturovaný rozhovor

Jedná se o částečně řízený rozhovor s otázkami, které jsou předem připraveny tazatelem. Vytvořen je jakýsi návod určující směr rozhovoru. Jejich pořadí není nijak striktně stanoveno, nicméně je důležité odpovědět na každou jednotlivou otázku. Tazatel může na základě odpovědí dotazovaného rozhovor doplnit o další doplňující otázku. Taktéž může požádat o rozvedení odpovědi pro její lepší pochopení [64].

4.2.1 Výzkum šetření

Polostrukturovaný rozhovor byl proveden s IT specialistou zajišťujícím bezpečnost dat a informací v lůžkovém zdravotnickém zařízení ve Středočeském kraji. Prostřednictvím e-mailové korespondence mu byl dostatečně s předstihem zaslán dokument s výzkumnými otázkami, které byly poté použity pro účely diplomové práce.

Rozhovor byl rozdělen pro přehlednost do 5 okruhů, jimiž jsou:

1. Operační systém zařízení;
2. Funkčnost Informační a komunikační techniky;
3. Přístup k datům (bezpečnost);
4. IT kontroly a odpovědnost;
5. Testování a školení.

5 VÝSLEDKY

Formy kybernetických útoků byly charakterizovány výše v kapitole 2.8 a 2.9. Zde bude uvedena analýza sociálního inženýrství, která bude dále doplněna o data z výzkumného dotazníkového šetření provedeného ve zkoumaném zdravotnickém zařízení. V tomto zařízení pracuje 1333 zaměstnanců. Dotazníkového šetření se zúčastnily pouhé 4 %.

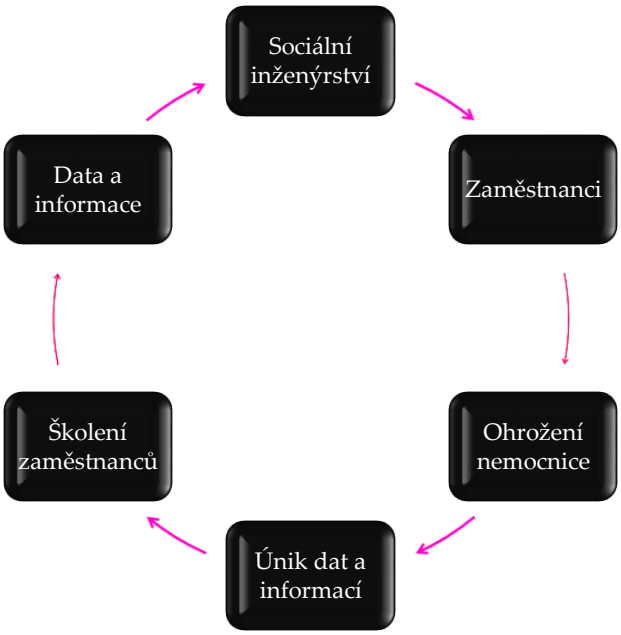
Dále budou uvedeny metody malware, díky nimž dochází k únikům dat a informací ze zdravotnických zařízení. K těmto metodám bude doplněn polostrukturovaný rozhovor s IT specialistou, který zajišťuje bezpečnost dat a informací zkoumaného zdravotnického zařízení.

5.1 Analýza sociálního inženýrství

Sociální inženýrství je obecně metoda kybernetického útoku, která je cílena především na zaměstnance nejen ve zdravotnictví, ale také ve státní správě či soukromých firmách. Jedná se o formu lidské komunikace, kdy se útočníci snaží svými dobrými komunikačními technikami a manipulací získat ze zaměstnanců konkrétní informace. Často zaměstnanci ani nevědí, že se právě stali obětí a poskytli neoprávněné osobě např. přístupová oprávnění. Ve zdravotnictví tak může jít i o sdělení citlivých informací neoprávněné osobě přes telefonní hovor či SMS zprávu.

Nejčastějšími technikami sociálního inženýrství jsou phishing útoky, pharming, vishing, baitling a trashing. Tyto metody využívají lidské slabosti, hlouposti, důvěryhodnosti, zvědavosti, touhou pomoci a dalších lidských vlastností pro svůj úspěch. Cílem a zároveň motivem těchto technik je především odcizení osobních údajů, dat a informací, popřípadě i následná finanční odměna.

5.1.1 Sociální inženýrství v prostředí zdravotnictví.



Obrázek 4 - Diagram sociálního inženýrství [vlastní]

Sociální inženýrství zneužívá zdravotnického personálu (zranitelnosti) vedoucí k ohrožení nemocnice představující riziko úniku dat a informací, zmírňující opatření v podobě školení a vzdělávání personálu, chránící aktiva nemocnice, jimiž jsou data a informace, které hrozba ohrožuje.

Ve zdravotnickém odvětví jde především o citlivost osobních údajů pacientů. Je důležité pacienty chránit před újmou, kterou by jim únik jejich osobních údajů mohl způsobit. Zároveň je nutné chránit citlivé informace zdravotnického zařízení, které by se neměly dostat do cizích rukou. Odcizené informace ze zdravotnického zařízení mohou být dále zneužity pro vznik dalších útoků. Důležité je tedy zaměřit se na vzdělávání a školení personálu v této oblasti, jelikož zaměstnanci jsou zneužíváni technikami sociálního inženýrství a stávají se tak zranitelným místem nemocnice. Proto byl uskutečněn výzkum mezi zaměstnanci zdravotnického zařízení, který byl směřován na techniky sociálního inženýrství a školení zdravotnického personálu v oblasti kybernetické bezpečnosti.

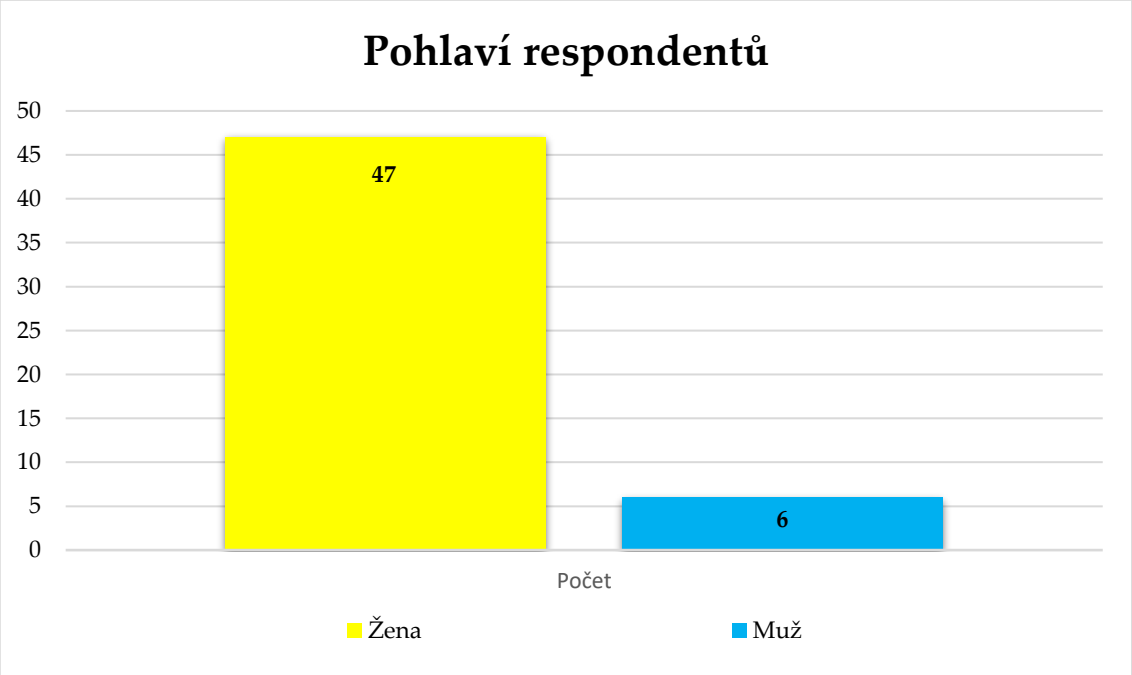
5.1.2 Vyhodnocení dat z dotazníkového šetření

Níže budou interpretovány odpovědi z výzkumného šetření pomocí nestandardizovaného anonymního dotazníku, jejichž cílem bylo zjistit, jaké mají zaměstnanci povědomí o kybernetické bezpečnosti a zároveň, zda se setkali alespoň někdy s jednou technikou sociálního inženýrství.

Otázka č. 1: Jste muž nebo žena.

Tabulka 2 – Pohlaví respondentů

Pohlaví	Počet	Podíl
Žena	47	89 %
Muž	6	11 %



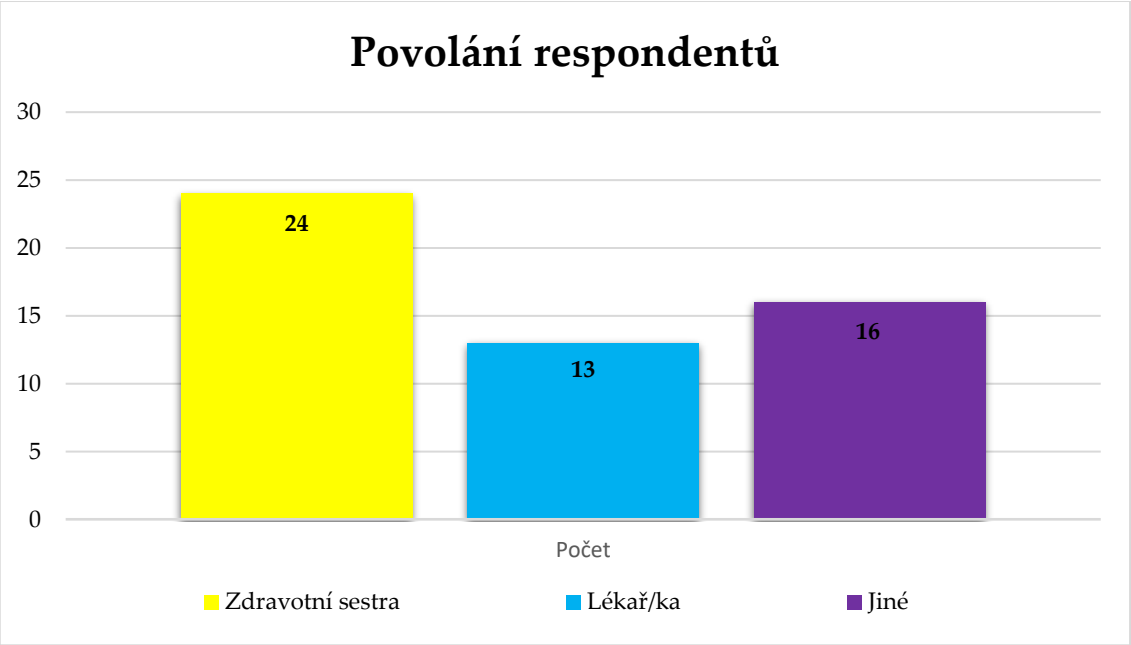
Obrázek 5 - Pohlaví respondentů

Otázka č. 1 zjišťovala pohlaví respondentů. Z celkového počtu oslovených bylo 47 (89 %) žen a 6 (11 %) mužů.

Otázka č. 2 – Uveďte své povolání.

Tabulka 3 - Povolání respondentů

Povolání	Počet	Podíl
Zdravotní sestra	24	45 %
Lékař/ka	13	25 %
Jiné	16	30 %



Obrázek 6 - Povolání respondentů

Otázka č. 2 se tázala na profesi respondentů zdravotnického zařízení. Z celkového počtu dotazovaných bylo 24 (45 %) povoláním zdravotní sestra, 13 (25 %) odpovědělo, že jejich profesí je lékař/ka a 16 (30 %) respondentů označilo odpověď jiné.

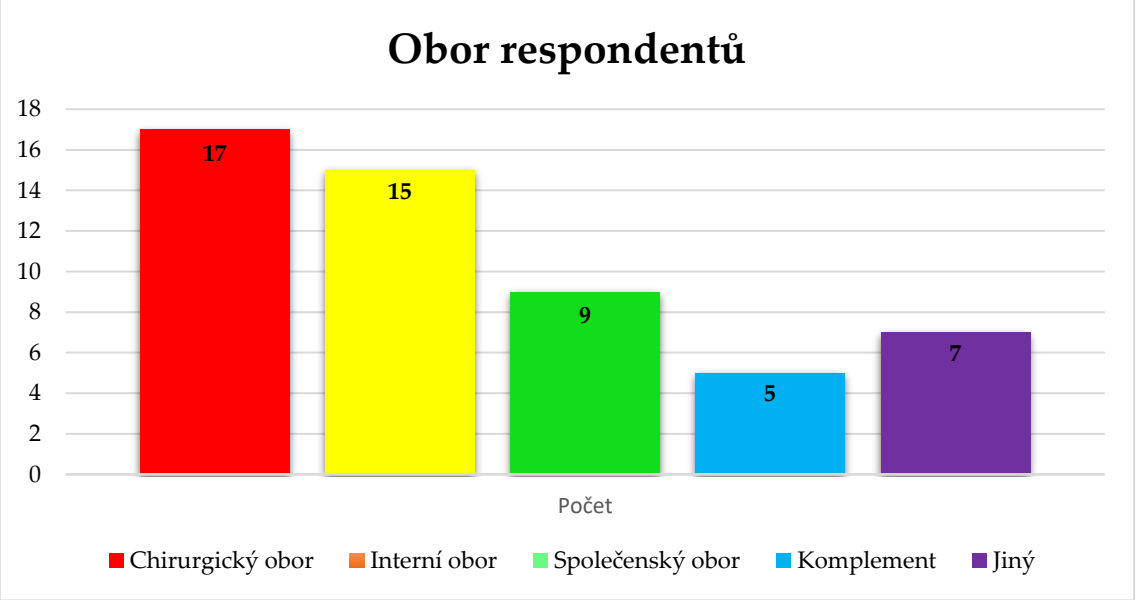
Odpověď jiné zahrnovala profesi:

Medik, Fyzioterapeut (2x), Psycholog, Nutriční terapeut, Farmaceutický asistent, Klinický farmaceut, Zdravotní laborant (2x), Sanitář (2x), Radiologický asistent (2x), Zdravotně sociální pracovník, Referent, Sekretářka.

Otázka č. 3 – Uveďte, v jakém oboru pracujete.

Tabulka 4 - Obor respondentů

Obor	Počet	Podíl
Chirurgický obor	17	32 %
Interní obor	15	28 %
Společenský obor	9	17 %
Komplement	5	10 %
Jiný	7	13 %



Obrázek 7 - Obor respondentů

Nejvíce respondentů, tj. 17 (32 %) pracuje v chirurgickém oboru. Nejméně respondentů pracuje v oboru komplement, který zahrnuje Patologické oddělení, Hematologicko-transfuzní oddělení, Radiodiagnostické oddělení (RDG) a Klinickou laboratoř, kde odpovědělo pouze 5 (10 %) respondentů.

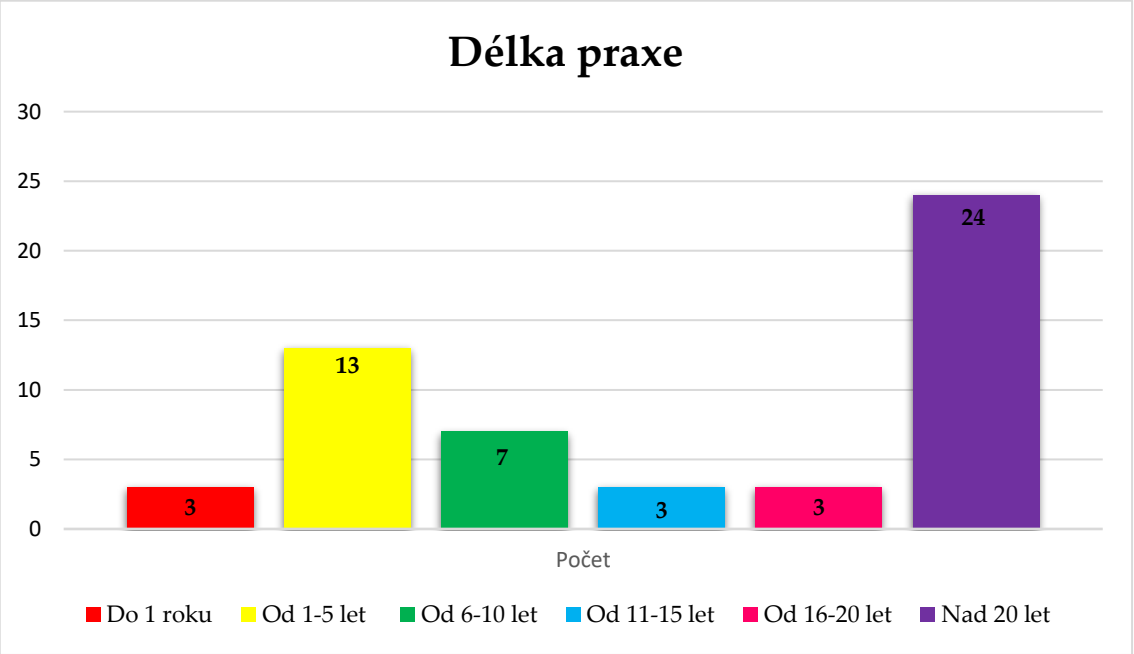
Odpověď jiný zahrnovala obor:

Administrativa, Personalistika, Urgentní medicína, Zdravotnická záchranná služba (2x), Covid oddělení a Klinická farmacie.

Otázka č. 4 – Uveďte délku Vaší praxe v nemocnici.

Tabulka 5 - Délka praxe respondentů

Délka praxe	Počet	Podíl
Do 1 roku	3	5,7 %
Od 1–5 let	13	24,5 %
Od 6–10 let	7	13,1 %
Od 11–15 let	3	5,7 %
Od 16–20 let	3	5,7 %
Nad 20 let	24	45,3 %



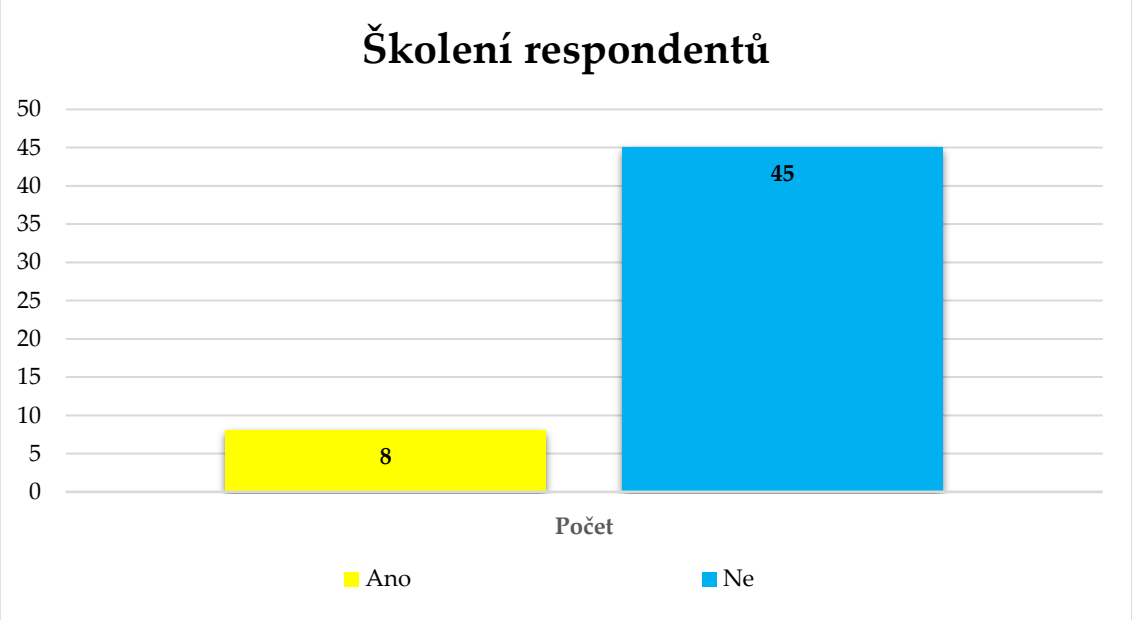
Obrázek 8 - Délka praxe respondentů

Otázka č. 4 zjišťovala délku praxe dotazovaných respondentů v nemocnici. Praxi do 1 roku měli 3 respondenti, 13 respondentů od 1–5 let, 7 respondentů mělo praxi od 6–10 let, 3 respondenti měli praxi od 11–15 let, další 3 respondenti odpověděli, že jejich praxe je od 16–20 let. Nejvíce respondentů, tj. 24 (45 %) přesahuje praxí nad 20 let.

Otázka č. 5 – Uveďte, jestli jste školen/a zaměstnavatelem v oblasti kybernetické bezpečnosti.

Tabulka 6 - Školení respondentů

Školení	Počet	Podíl
Ano	8	15 %
Ne	45	85 %



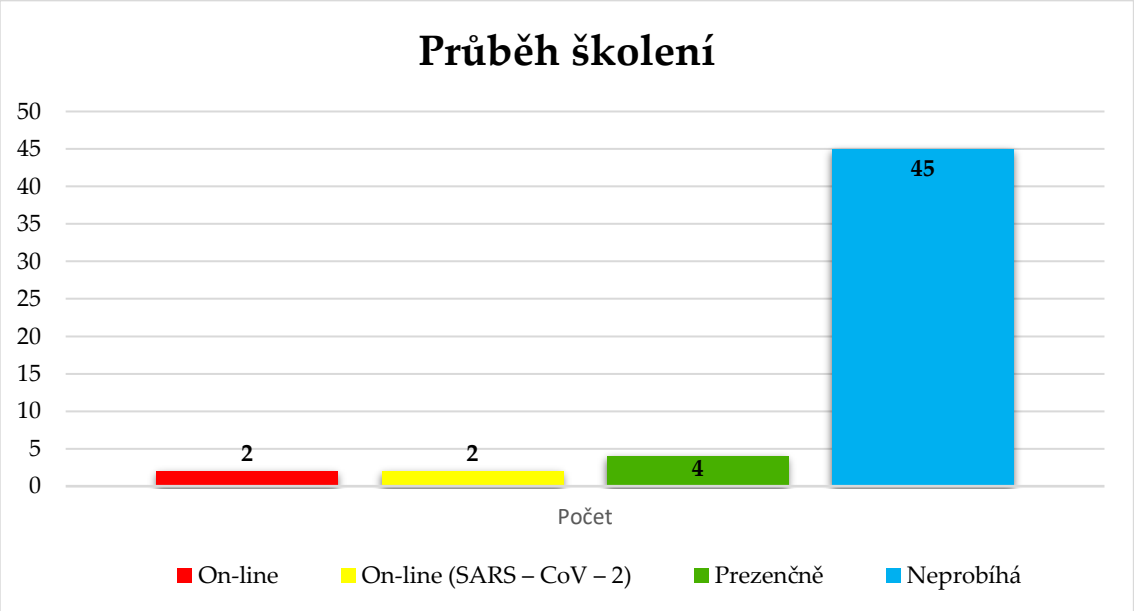
Obrázek 9 - Školení respondentů

V otázce č. 5 se tázalo respondentů, zda jsou zaměstnavatelem školeni v oblasti kybernetické bezpečnosti. Celých 85 % (45) dotazovaných školeno nebylo, pouze 15 % (8) respondentů prošlo školením od zaměstnavatele.

Otázka č. 6 – Uveďte, jak probíhá Vaše školení v oblasti kybernetické bezpečnosti.

Tabulka 7 - Průběh školení respondentů

Průběh školení	Počet	Podíl
On-line	2	3,8 %
On-line (SARS–CoV–2)	2	3,8 %
Prezenčně	4	7,5 %
Neprobíhá	45	84,9 %



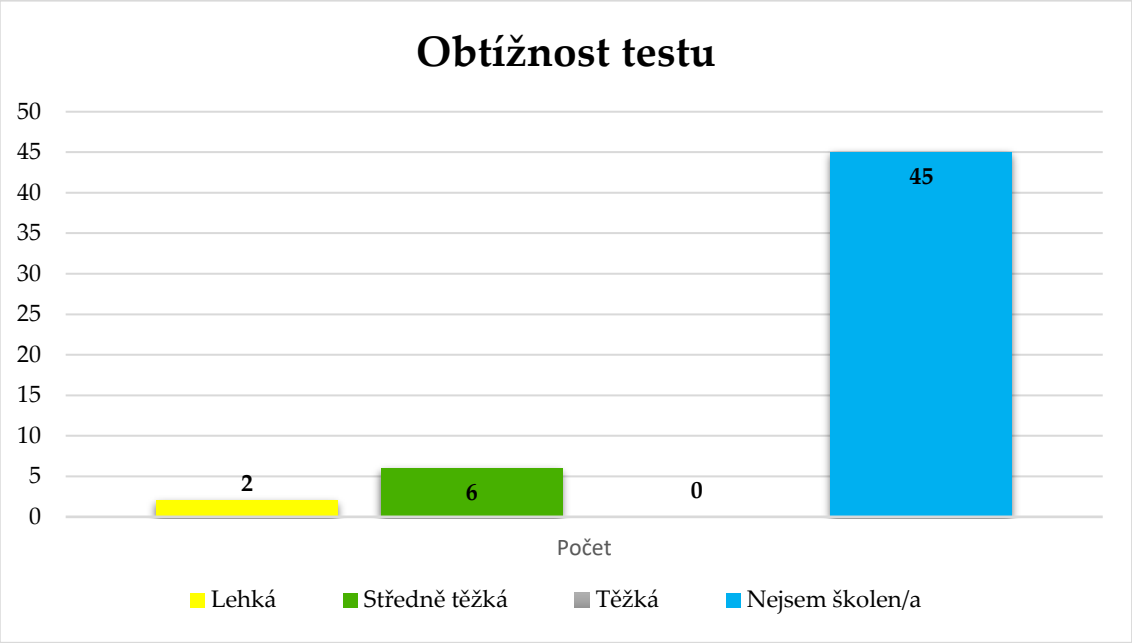
Obrázek 10 - Průběh školení

Otázka č. 6 zjišťovala, jakým způsobem probíhá školení respondentů v oblasti kybernetické bezpečnosti. Tato otázka navazuje svou odpovědí na otázku č. 5. Jak lze z grafu vyčíst, 45 (84,9 %) respondentů odpovědělo, že školení neprobíhá, jelikož nejsou školeni. Prezenční školení probíhá u 4 (7,5 %) respondentů. Z důvodu probíhající pandemie SARS-CoV-2, probíhá školení 2 (3,8 %) respondentů momentálně on-line. U zbylých 2 (3,8 %) respondentů toto školení probíhá vždy ve formě on-line.

Otázka č. 7 – Uveďte obtížnost závěrečného testu školení.

Tabulka 8 - Obtížnost testu

Obtížnost testu	Počet	Podíl
Lehká	2	4 %
Středně těžká	6	11 %
Těžká	0	0 %
Nejsem školen/a	45	85 %



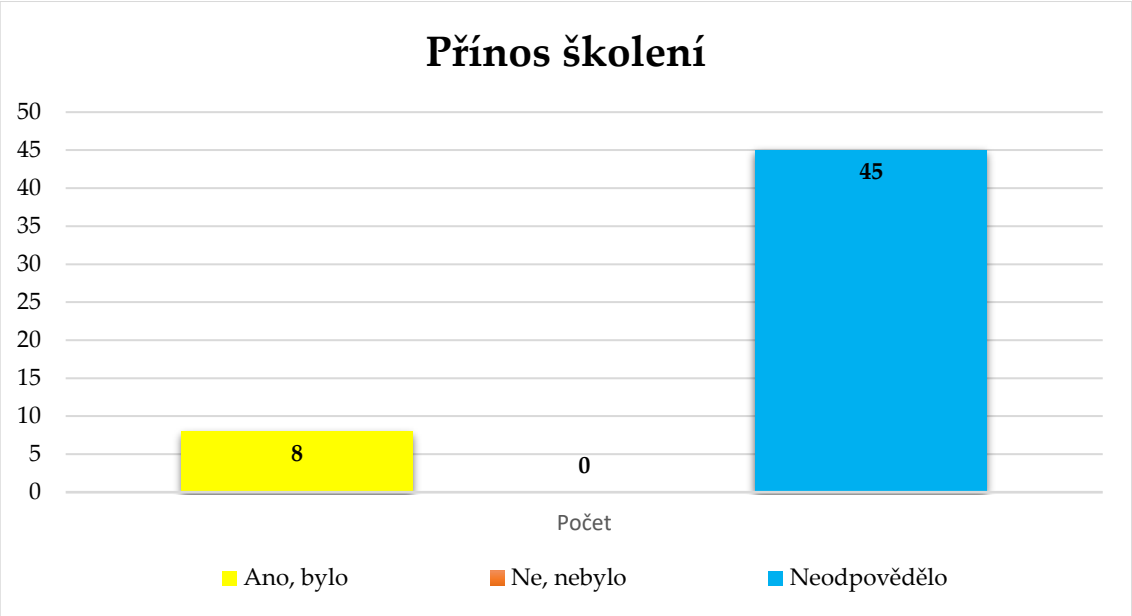
Obrázek 11 - Obtížnost testu

Otázka č. 7 navazovala na předešlé položené otázky (č. 5 a č. 6) týkající se školení v oblasti kybernetické bezpečnosti. Odpovědělo pouze 8 respondentů z 53 tázaných. Tito respondenti odpověděli, že obtížnost testu byla pro 2 respondenty lehká a pro zbylých 6 středně těžká.

Otázka č. 8 – Uveďte, zda bylo pro Vás školení přínosné.

Tabulka 9 - Přínos školení

Přínos školení	Počet	Podíl
Ano, bylo	8	15 %
Ne, nebylo	0	0 %
Neodpovědělo	45	85 %



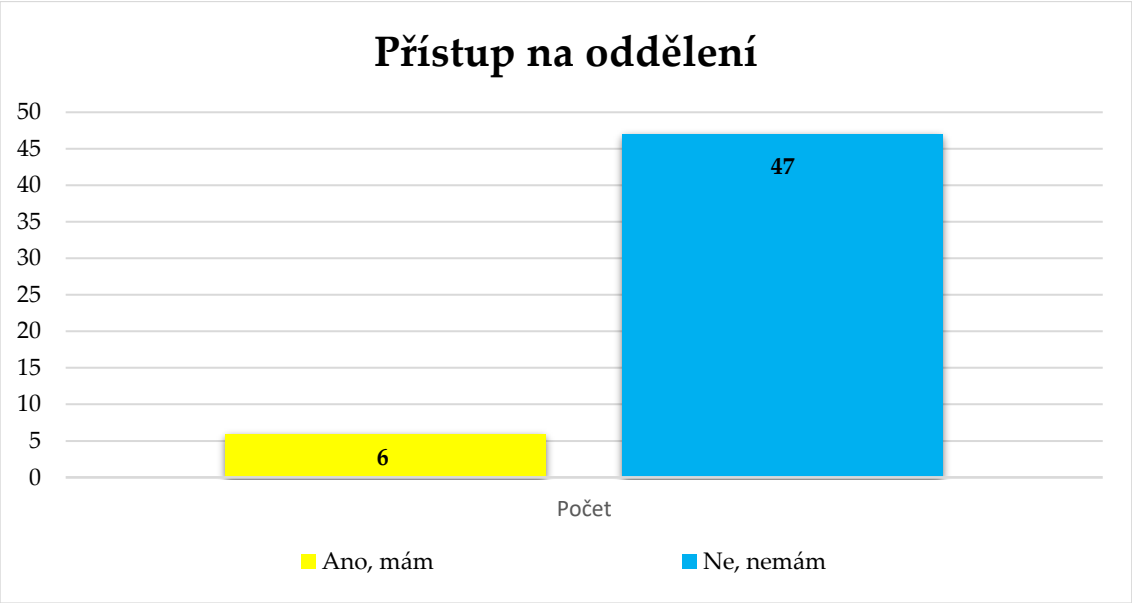
Obrázek 12 - Přínos školení

Z tohoto grafu lze vyčíst, že pro všech 8 školených respondentů bylo školení přínosné a dozvěděli se i nové užitečné fakty.

Otázka č. 9 – Uveďte, zdali máte přístup na všechna oddělení v nemocnici.

Tabulka 10 - Přístup na oddělení

Přístup	Počet	Podíl
Ano, mám	6	11 %
Ne, nemám	47	89 %



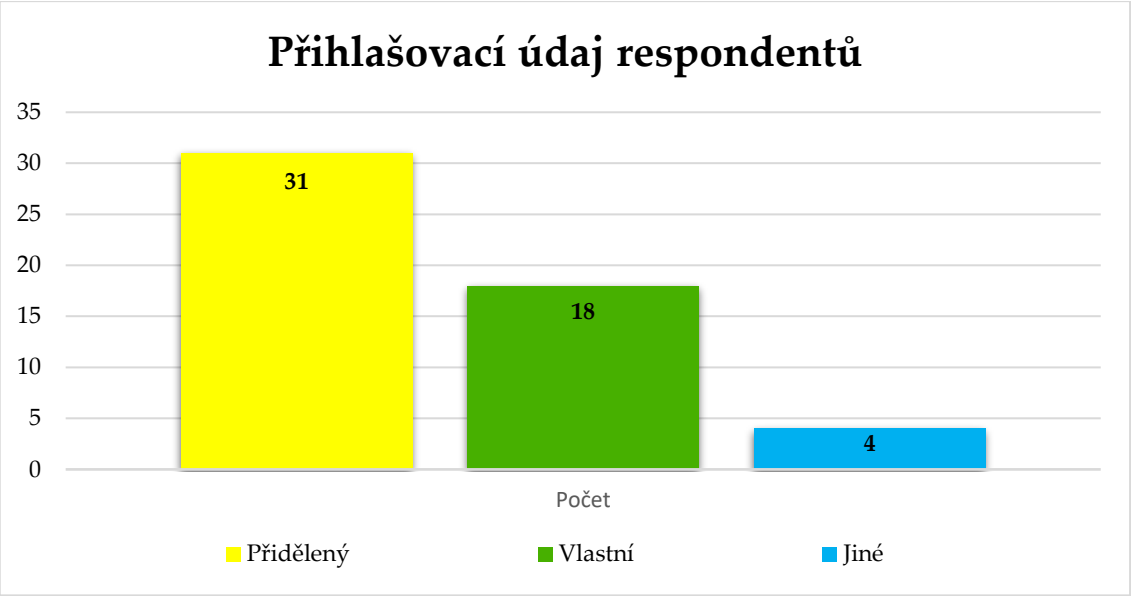
Obrázek 13 - Přístup na oddělení

Otázka č. 9 zjišťovala, zda mají respondenti volný přístup na všechna oddělení v nemocnici. Pouze 6 (11 %) respondentů odpovědělo, že tímto povolením disponují. Především se jedná o zdravotní sestry z chirurgického oboru, lékařku z interního oboru a urgentní medicíny a klinického farmaceutika. Celých 47 (89 %) respondentů nedisponuje přístupy na všechna oddělení.

Otázka č. 10 – Uveďte, jestli máte přihlašovací údaj (login) do informačního systému.

Tabulka 11 - Přihlašovací údaj respondentů

Přihlašovací údaj	Počet	Podíl
Přidělený	31	59 %
Vlastní	18	34 %
Jiné	4	7 %



Obrázek 14 - Přihlašovací údaj respondentů

V otázce č. 10 respondenti odpovídali, zda přihlašovací údaje do nemocničního informačního systému (dále jen NIS) mají vlastí nebo přidělené zaměstnavatelem. Taktéž měli respondenti možnost i odpovědi jiné. Nejvíce respondentů 31 (51 %) odpovědělo, že jejich přihlašovací údaje do NIS jsou přidělené zaměstnavatelem. Dalších 18 (34 %) respondentů označilo odpověď, že přihlašovací údaje mají vlastní. Možnost jiné odpovědi využili 4 (7 %) respondenti.

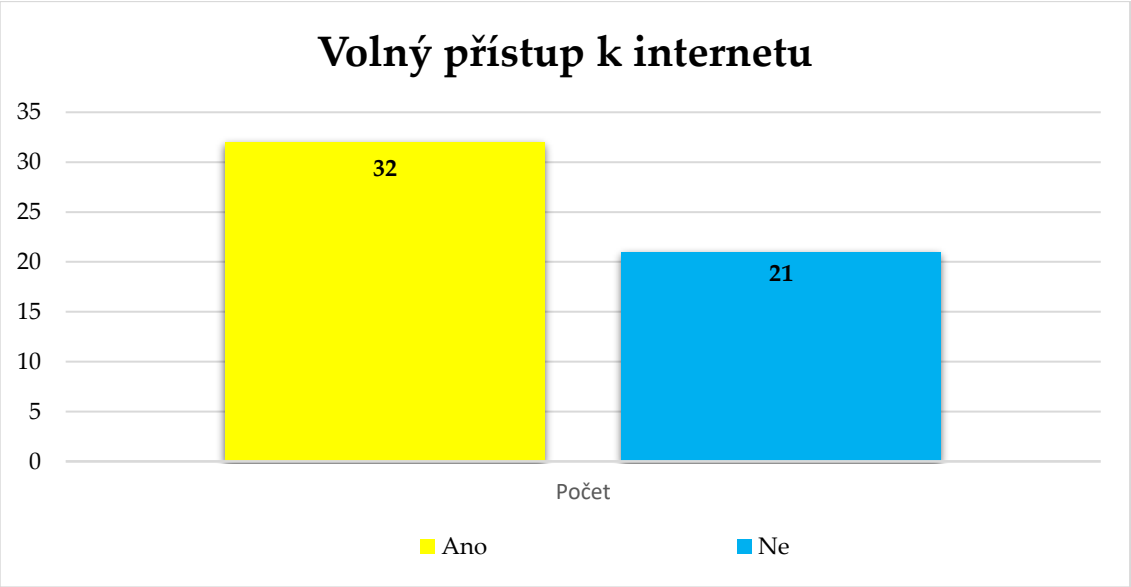
Odpověď jiné zahrnovala:

přidělené číslo, pouze příjmení, osobní číslo v kombinaci s vlastními znaky.

Otázka č. 11 – Uveďte, jestli máte volný přístup k internetu.

Tabulka 12 - Volný přístup respondentů k internetu

Volný přístup	Počet	Podíl
Ano	32	60 %
Ne	21	40 %



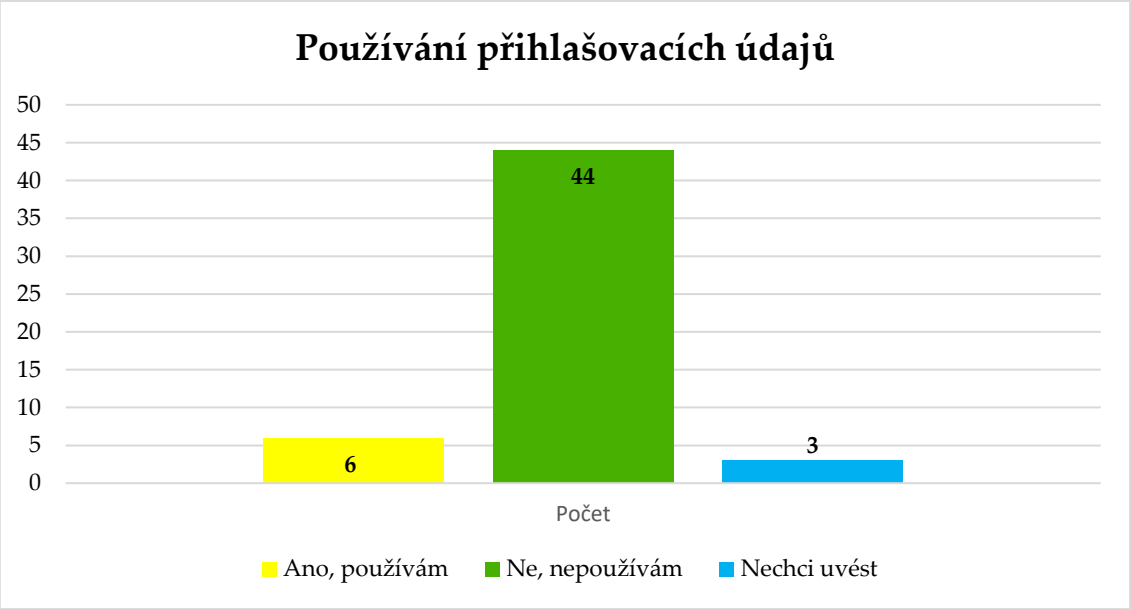
Obrázek 15 - Volný přístup k internetu

Tento graf znázorňuje počet respondentů mající volný přístup k internetu. Možnost ano označilo 32 (60 %) respondentů. Jedná se především o lékaře, lékařky a zdravotní sestry z chirurgického a interního oboru.

Otázka č. 12 – Uveďte, zda přihlašovací údaje, které používáte pro přístup do nemocničního informačního systému, používáte i jinde, např. e-mail, sociální sítě.

Tabulka 13 - Použití přihlašovacích údajů

Přihlašovací údaje	Počet	Podíl
Ano, používám	6	11 %
Ne, nepoužívám	44	83 %
Nechci uvést	3	6 %



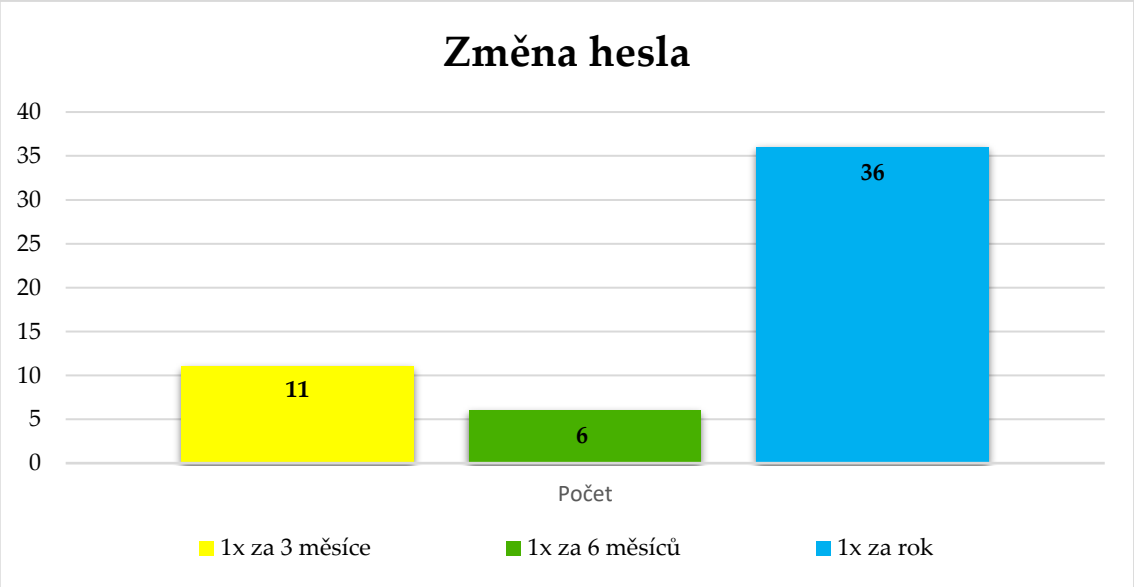
Obrázek 16 - Přihlašovací údaje

Otázka č. 12 zjišťovala, zda respondenti používají přihlašovací údaje určené pro přihlášení do NIS i pro přihlášení na jiný účet, např. přihlášení na e-mail nebo na sociální sítě. Jak už graf znázorňuje, 6 (11 %) respondentů jej využívá i pro přihlášení na jiné účty mimo nemocnici. Dalších 44 (83 %) respondentů je nepoužívá mimo NIS a 3 (6 %) respondenti označili možnost nechci uvést.

Otázka č. 13 – Uveďte, jak často si měníte heslo.

Tabulka 14 - Změna hesla

Změna hesla	Počet	Podíl
1x za 3 měsíce	11	21 %
1x za 6 měsíců	6	11 %
1x za rok	36	68 %



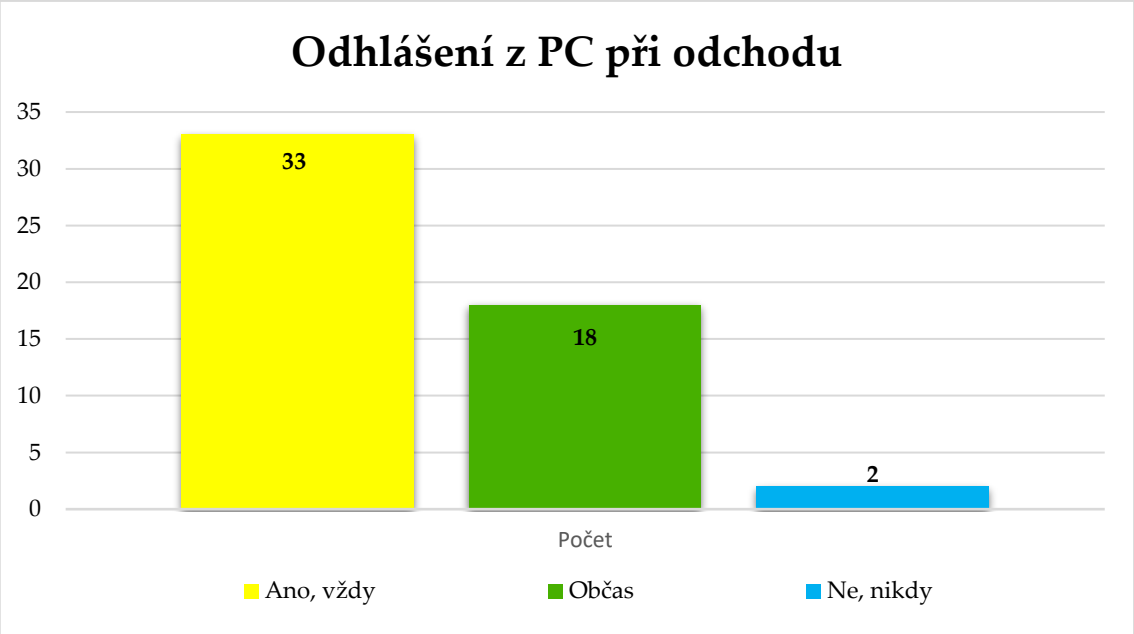
Obrázek 17 - Změna hesla

Otázka č. 13 se dotazovala na četnost obměny hesla respondentů. Změnu 1x za 3 měsíce realizuje 11 (21 %) dotazovaných a 6 (11 %) dotazovaných obměnu hesla provádí 1x za 6 měsíců. Celých 68 % (36) dotázaných mění své heslo 1x za rok.

Otázka č. 14 – Odhlašujete se vždy, když odcházíte od počítače?

Tabulka 15 - Odhlášení z PC při odchodu

Odhlášení	Počet	Podíl
Ano, vždy	33	62 %
Občas	18	34 %
Ne, nikdy	2	4 %



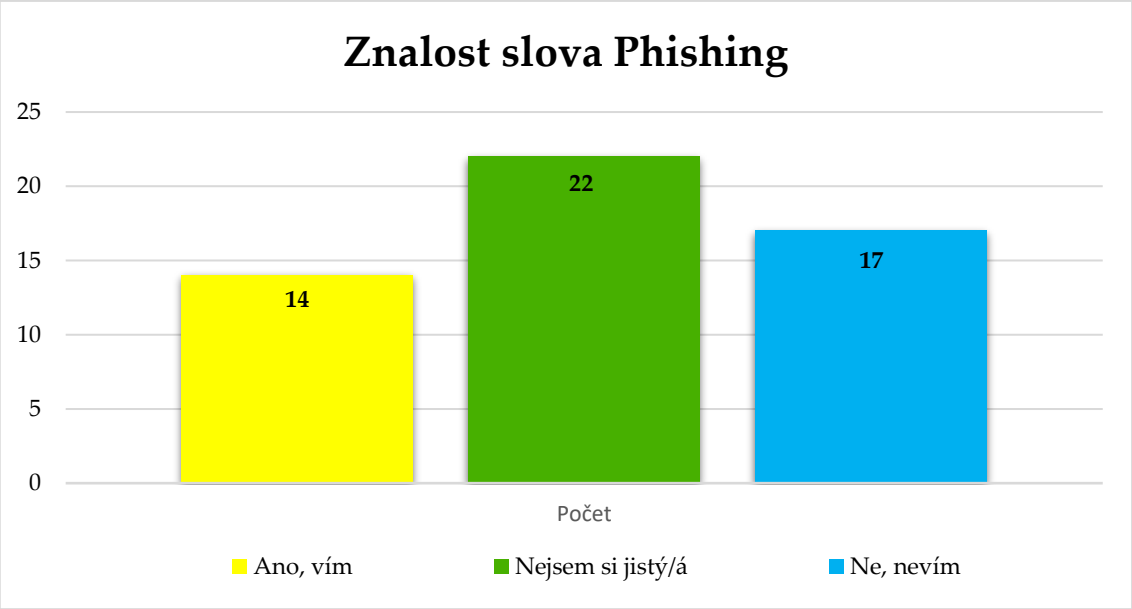
Obrázek 18 - Odhlášení z PC při odchodu

Otázka č. 14 zjišťovala, zda se respondenti vždy odhlašují, když odcházejí od počítače. Možnost "**ano, vždy**" označilo 33 (62 %) respondentů. Možnost "**Občas**" označilo 18 (34 %) respondentů a "**ne, nikdy**" odpověděli pouze 2 (4 %) respondenti.

Otázka č. 15 – Víte, co znamená phishing?

Tabulka 16 - Znalost slova phishing

Phishing	Počet	Podíl
Ano, vím	14	26 %
Nejsem si jistý/á	22	42 %
Ne, nevím	17	32 %



Obrázek 19 - Znalost slova phishing

Otázka č. 15 se dotazovala všech zaměstnanců, zda znají význam slova phishing. 14 (26 %) zaměstnanců odpovědělo, že vědí, co znamená slovo phishing. Dalších 22 (42 %) zaměstnanců odpovědělo, že si nejsou jistí a zbylých 17 (32 %) neví, co slovo phishing znamená.

Otázka č. 16 – Pokud jste u předchozí otázky dal/a "Ano, vím", napište slovně co phishing znamená.

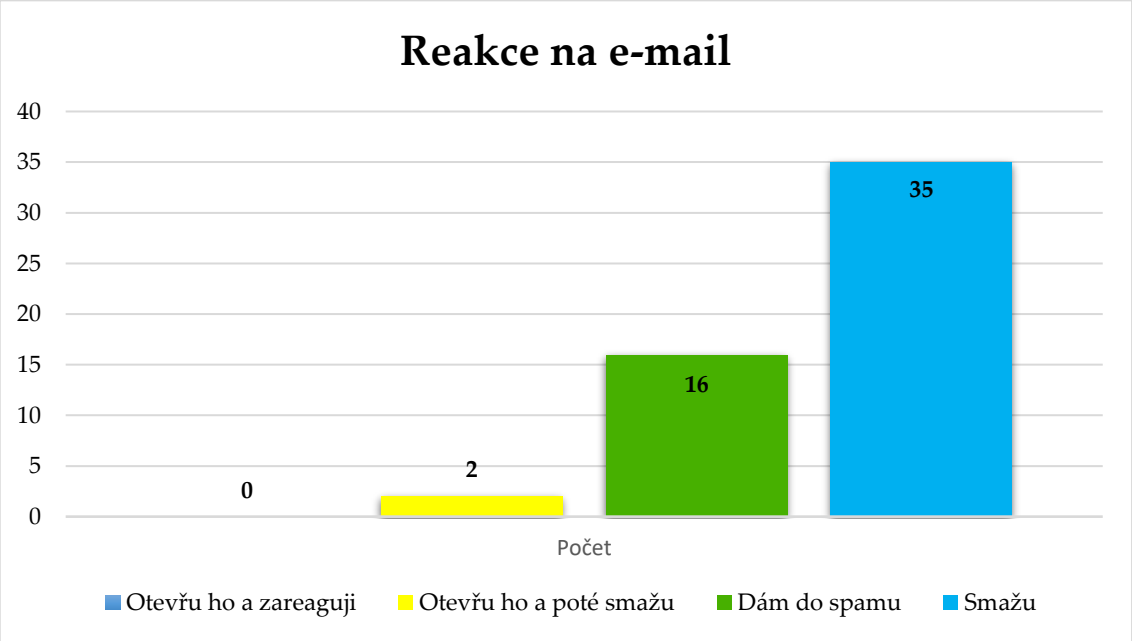
Tato otázka byla plně otevřená a nepovinná. Navazovala na předchozí otázku č. 15. Ta se tázala, zda respondenti mají znalost v kybernetické oblasti a vědí, co znamená slovo phishing. Otázka č. 16 je vyzývala k popsání slova phishing vlastními slovy.

Celkem na otázku odpovědělo 36 respondentů. Odpovídali i respondenti, kteří v předchozí otázce (č. 15) uvedli, že si nejsou významem slova jistí. Všech 36 respondentů popsalo význam slova phishing správně.

Otázka č. 17 – Co byste udělal/a, kdyby Vám přišel e-mail s neznámým obsahem?

Tabulka 17 - Reakce na e-mail

Reakce na e-mail	Počet	Podíl
Otevřu ho a zareaguji	0	0 %
Otevřu ho a poté smažu	2	4 %
Dám do spamu	16	30 %
Smažu	35	66 %



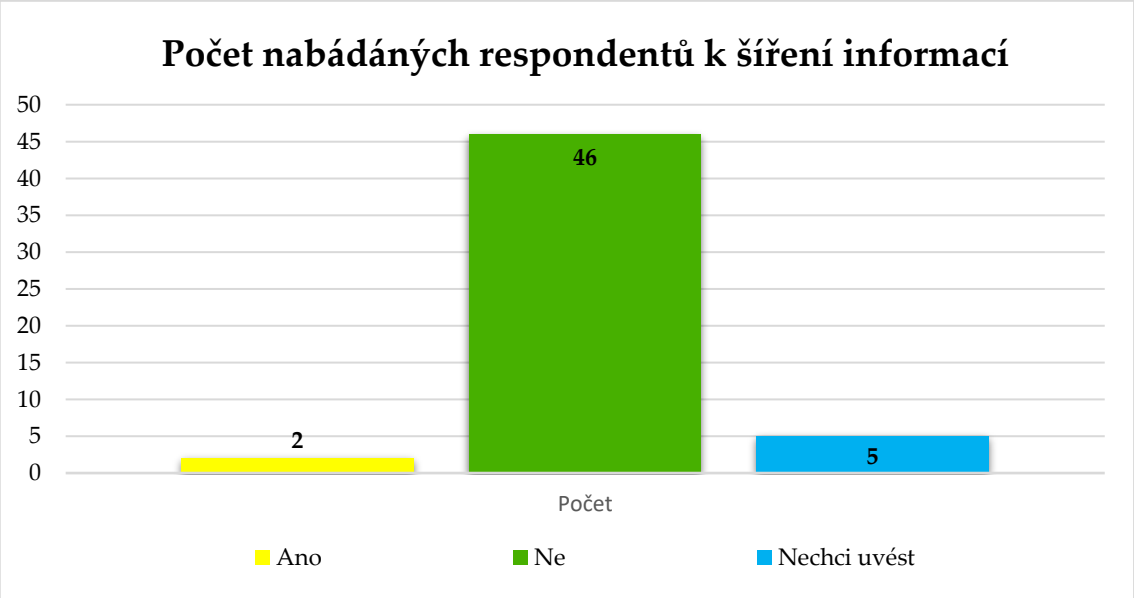
Obrázek 20 - Reakce na e-mail

Otázka č. 17 se tázala zaměstnanců, jak by zareagovali na e-mail s neznámým obsahem. Většina zaměstnanců, přesněji 35 (66 %) odpovědělo, že by e-mail smazala. 16 (30 %) zaměstnanců by e-mail dalo do složky spam a 2 (4 %) zaměstnanci, by e-mail otevřeli a poté by jej smazali. Možnost "**Otevřu ho a zareaguji!**" nikdo z dotazovaných neoznačil.

Otázka č. 18 – Uveďte, zda jste byl/a někdy nabádán/a k šíření osobních informací o pacientovi.

Tabulka 18 - Počet nabádaných respondentů k šíření informací

Šíření informací	Počet	Podíl
Ano	2	4 %
Ne	46	87 %
Nechci uvést	5	9 %



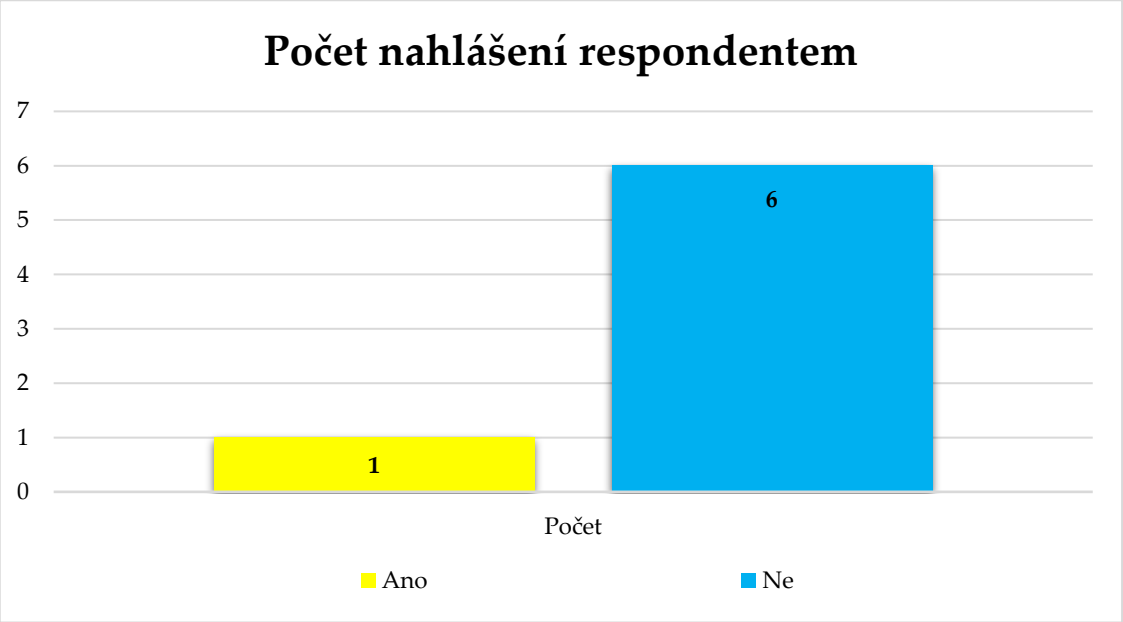
Obrázek 21 - Počet nabádaných respondentů k šíření informací

Celých 46 (87 %) respondentů se osobně nesetkalo s nabádáním k šíření osobních informací o pacientovi. Pouze 2 (4 %) respondenti uvedli, že se s tímto nabádáním setkali. Zbylých 5 (9 %) respondentů nechtělo odpověď uvést. Nicméně i přesto tito respondenti reagovali v následující otázce, zdali tento čin nahlásili zaměstnavateli, PČR apod.

Otázka č. 19 – Pokud jste u předchozí otázky odpověděl/a "ANO", nahlásil/a jste to zaměstnavateli, na IT oddělení nebo na Policii ČR?

Tabulka 19 – Počet nahlášení respondentem

Nahlášení	Počet	Podíl
Ano	1	2 %
Ne	6	11 %



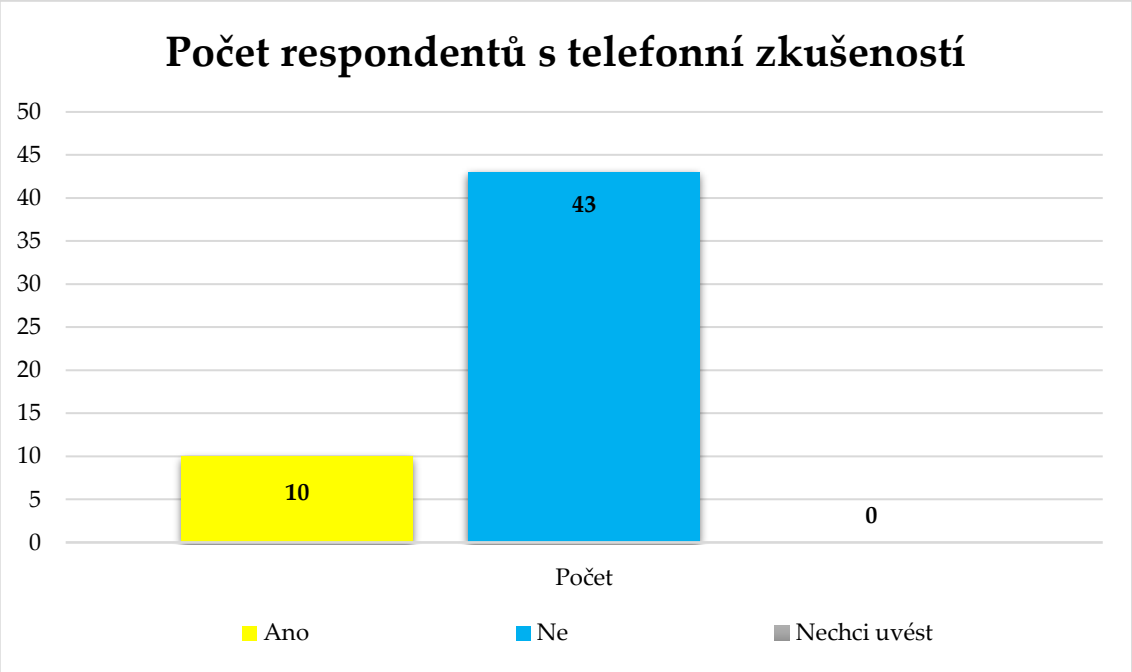
Obrázek 22 – Počet nahlášení respondentem

Tato otázka navazovala na otázku č. 18, která se tázala respondentů, zda byli někdy nabádáni k šíření osobních informací o pacientovi. Možnost ano označili pouze 2 respondenti a 5 respondentů dalo možnost nechci uvést. Na otázku č. 19 odpovědělo celkem 7 respondentů. Pouze 1 respondent odpověděl, že tento čin nahlásil zaměstnavateli. Dalších 6 respondentů čin neohlásilo.

Otázka č. 20 – Setkal/a jste se někdy s telefonátem, kdy se někdo vydával za někoho jiného či osobu blízkou a snažil se z Vás dostat informace?

Tabulka 20 – Počet respondentů s telefonní zkušeností

Telefonát	Počet	Podíl
Ano	10	19 %
Ne	43	81 %
Nechci uvést	0	0 %



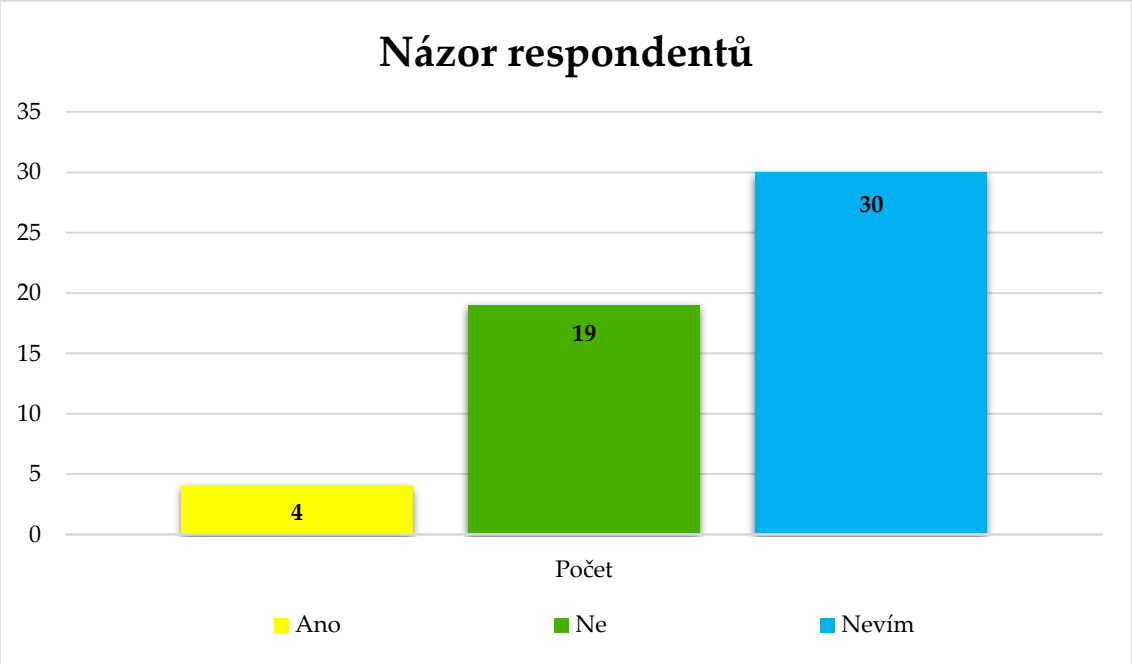
Obrázek 23 – Počet respondentů s telefonní zkušeností

Otázka č. 20 zjišťovala, zda se respondenti setkali s telefonátem, kdy se někdo vydával za někoho jiného či osobu blízkou a snažil se od nich získat informace. Z celkových 53 dotazovaných respondentů označilo 10 (19 %) respondentů odpověď "**Ano**", že se s tímto telefonátem osobně setkali. Nicméně 43 (81 %) respondentů označilo odpověď "**Ne**". Tedy více jak polovina uvedla, že se s takovýmto telefonátem ještě nikdy nesetkala.

Otázka č. 21 – Myslíte si, že zdravotnické zařízení, ve kterém pracujete, je připraveno na případný kybernetický útok?

Tabulka 21 - Názor respondentů na připravenost zdravotnického zařízení

Připravenost ZZ	Počet	Podíl
Ano	4	7 %
Ne	19	36 %
Nevím	30	57 %



Obrázek 24 - Názor respondentů na připravenost zdravotnického zařízení

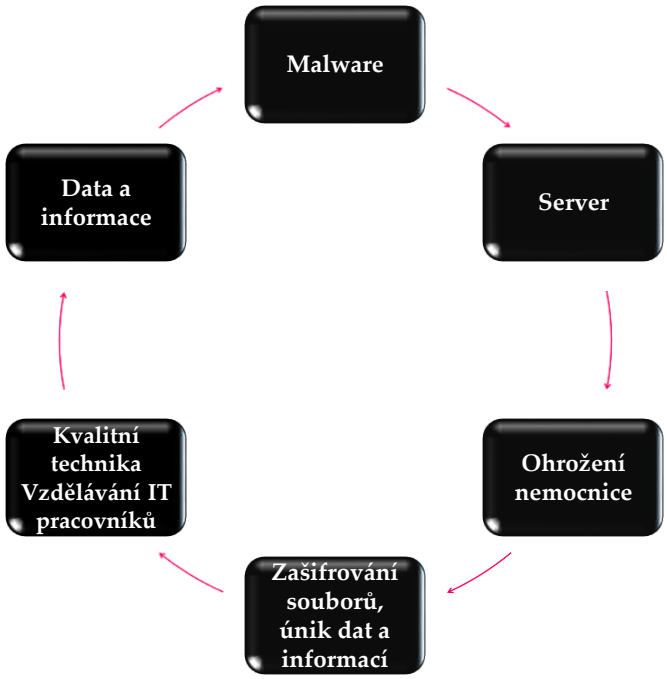
Otázka č. 21 se tázala respondentů, zda si myslí, že zdravotnické zařízení, v němž pracují, je připraveno na případný kybernetický útok. O dobré připravenosti zdravotnického zařízení si myslí pouze 4 (7 %) respondenti. Naopak 19 (36 %) respondentů si myslí, že zdravotnické zařízení není připraveno na případný kybernetický útok. A více než 30 (57 %) respondentů označilo možnost **"Nevím".**

5.2 Analýza malware

Kybernetický útok, uskutečněn pomocí malware spolu se sociálním inženýrstvím, bývá často tím nejefektivnějším kybernetickým útokem a zároveň tou největší hrozbou pro organizace. Malware je škodlivý software, který útočníci používají k narušení činnosti sytému pro získání přístupu do databází, dalších jiných souborů či k získání informací.

Neznámější druhy malware, šířící se např. prostřednictvím příloh v e-mailu, jsou: ransomware, keylogger, adware, spyware a vir. Většina dokáže vykonávat i více úkonů najednou.

5.2.1 Využití malware proti zdravotnickému zařízení



Obrázek 25 - Analýza malware [vlastní]

Malware využívá server (zranitelné místo nemocnice) vedoucí k ohrožení nemocnice, představující riziko úniku dat a informací, zmírňující opatření, kterým je vzdělávání IT pracovníků i zdravotního personálu a novější technika, která chrání aktiva nemocnice, jimiž jsou data a informace.

Malware mířený proti zdravotnickému zařízení může napáchat obrovské škody. Ztráta dat znamená problém při poskytování potřebné péče pacientům, jelikož není dostupná dokumentace. V podstatě se zastaví veškerá léčba a je zapotřebí čekat na obnovu systému. V poslední době je nejvíce ke kybernetickým útokům používán malware-ransomware, který dokáže zašifrovat celý systém v zařízení. Motivem útočníků je především získání finanční odměny.

Důležité je tedy dbát na zajištění bezpečnosti dat a informací v organizaci. Jakým způsobem je zajištěna bezpečnost ve zkoumaném zařízení bylo zjišťováno pomocí polostrukturovaného rozhovoru, který byl proveden s IT specialistou.

5.3 Výsledky z polostrukturovaného rozhovoru

Níže budou interpretovány odpovědi na výzkumné otázky, jejichž cílem bylo zjistit, jakým způsobem je zdravotnické zařízení zabezpečeno proti případným kybernetickým útokům a jakým způsobem je zajištěna bezpečnost dat a informací ve zdravotnickém zařízení. Pro následující odpovědi byl veden rozhovor s IT specialistou zkoumaného zdravotnického zařízení ve Středočeském kraji.

5.3.1 1. Tematický okruh „Operační systém zařízení“

Nejprve byly pokládány otázky směřované na operační systém, kterým zdravotnické zařízení disponuje. Dále byly položeny otázky týkající se zajišťování bezpečnosti dat.

1. **Jaký/é operační systémy je/jsou používán/y ve Vašem zdravotnickém zařízení?**

IT specialista: Operační systémy, které používáme v našem zdravotnickém zařízení, jsou od společnosti Microsoft. Jedná se o Windows XP, Windows 7 a Windows 10.

2. **Jak často dochází k aktualizacím operačních systémů?**

IT specialista: Vždy dochází k aktualizacím operačních systémů dle vydávání aktualizací od společnosti Microsoft.

3. **O bezpečnost Vašich uložených dat se stará nasmlouvaná firma, popřípadě se o jejich bezpečnost staráte sami?**

IT specialista: O bezpečnost uložených dat se staráme sami.

4. **Byly někdy zaznamenány nějaké významné poruchy či problémy s fungováním systému a zpracováním dat?**

IT specialista: Ne, doposud nebyly zaznamenány žádné poruchy s fungováním systému a zpracováním dat.

Tabulka 22 - Souhrn odpovědí tematického okruhu 1

SYSTÉM ZDRAVOTNICKÉHO ZAŘÍZENÍ	
Operační systém	Windows XP, Windows 7, 10
Četnost aktualizace OPS	Dle vydání aktualizaci Microsoftu
Starost o bezpečnost dat	Zaměstnanci zařízení
Záznam o problému	Žádný problém nenastal

5.3.2 2. Tematický okruh „Funkčnost Informační a komunikační techniky“

V této části polostrukturovaného rozhovoru se zjišťovalo, jakým způsobem funguje výpočetní technika ve zdravotnickém zařízení a zda jsou zavedeny určité postupy pro zajištění dat.

1. **Jsou zajištěny postupy pravidelného zálohování a uchovávání IT dat?**

IT specialista: Ano, postupy pravidelného zálohování i uchovávání IT dat máme zajištěny.

Dále byly položeny doplňující otázky:

a. Jak často je systém zálohován?
b. Jsou vytvářeny kopie?

IT specialista: Systém je zálohován kvůli velikému množství dat každý den a kopie jsou vytvářeny a dávají se na externí disky, které se poté ukládají mimo serverovnu.

2. **Je k dispozici plán obnovy pro případ nešťastných událostí, kterými jsou např. přírodní katastrofy, krádež nebo kybernetický útok tak, aby chod nemocnice mohl pokračovat v činnosti bez významného přerušení?**

IT specialista: Žádný plán obnovy není.

Dále byly položeny doplňující otázky:

a. Jak je tato nahodilá událost řešena z pohledu IT?
b. Můžete mi popsat postupy při kybernetickém postupu?

IT specialista: Z pohledu IT se provádí obnova funkčnosti dle priorit. Na prvním místě je vždy nemocniční informační systém. Postupy při kybernetickém útoku jsou následující: okamžité odpojení od internetu,

odizolování napadeného stroje, zjištění rozsahu napadení a v neposlední řadě kontaktování úřadů.

3. **Mají zaměstnanci k dispozici technickou podporu?**

IT specialista: Ano, technická podpora v podobě 5 techniků zdravotnického zařízení je k vždy k dispozici.

Dále byla položena doplňující otázka:

Obrátil se na Vás někdy zaměstnanec s problémem, že omylem zaslal údaje o pacientovi jinam, než měl nebo že smazal důležitou složku a potřebuje data zpět?

IT specialista: Údaje jinam zatím nikdo neposlal nebo se s tím alespoň nepochlubil. Nicméně mazání složek, stejně tak, jako zapsání lékařské zprávy do složky jiného pacienta, je už spíše takový folklór.

Tabulka 23 - Souhrn odpovědí tematického okruhu 2

VÝPOČETNÍ TECHNIKA ZDRAVOTNICKÉHO ZAŘÍZENÍ	
Pravidelné zálohování dat	Probíhá každý den
Je k dispozici plán obnovy	Ne, plán není
Technická podpora pro zaměstnance	Ano, neustále

5.3.3 3. Tematický okruh „Přístup k datům (bezpečnost)“

V této části rozhovoru se pojednávalo o přístupech a heslech, která zajišťují bezpečnost dat ve zdravotnickém zařízení.

1. **Jsou přijata a realizována dostatečná bezpečnostní pravidla a opatření pro zabezpečení výpočetní techniky?**

IT specialista: Ano, podle mého jsou realizována dostatečná bezpečnostní pravidla i opatření pro zajištění bezpečnosti výpočetní techniky.

Dále byly položeny doplňující otázky:

a. Je nastaven systém hesel a oprávnění?
b. Jak často probíhá obnova hesel?
c. Lze nastavit již jednou použitá hesla?
d. Existuje fyzické zabezpečení serveru? (chráněná místnost)

IT specialista: Nastavený systém hesel máme na AD (databáze zdravotnického zařízení). Co se týče obnovy hesel, tak na AD se provádí každé 3 měsíce a v NIS je to na samotném uživateli (zaměstnanci). Nelze natavit stejná ani podobná hesla.

Chráněnou místnost bychom měli moc rádi. Momentálně jsou fyzickým zabezpečením pouze dvakrát zamykatelné dveře.

2. Došlo někdy k narušení bezpečnosti?

IT specialista: Ano, na našem železe, ale na serveru firmy, která server spravovala.

Dále byly položeny doplňující otázky:

a. Jak byla případně tato událost řešena?
b. Jaký dopad může mít ztráta dat a informací na chod nemocnice, popřípadě zaměstnance a pacienty?

IT specialista: Případ byl předán PČR a NÚKIB. Tento případ nijak chod nemocnice nenarušil. Nicméně by ztráta dat znamenala problém při léčení, jelikož nebude dostupná dokumentace, jak lékařská, tak obrazová. V podstatě se zastaví veškerá léčba a čeká se na obnovu. Odcizení dat znamená narušení důvěry zařízení a velké finanční prostředky na obnovu provozu.

3. **Je zavedena kontrola uživatelských práv pro přístup do sítě a do souborů (požadavek autentizace)?**

IT specialista: Ano, kontrola uživatelských práv pro přístup je zavedena.

4. **Jsou nastaveny a zavedeny kontroly pro ochranu dat zdravotnického zařízení v rámci sítě?**

IT specialista: Ne, žádné kontroly v rámci sítě neprobíhají.

Dále byly položeny doplňující otázky:

a. Používáte antivirus? Jaký?
b. Jaké další zabezpečovací programy sítě využíváte?

IT specialista: Samozřejmě, že antivirus používáme. Máme VirusFree před firewallem. A co se týče dalších zabezpečovacích programů sítě, tak žádné jiné nemáme.

5. **Jsou vhodným způsobem zaznamenány případy neoprávněného vstupu do systému?**

IT specialista: Ano, loguje se to.

Dále byla položena doplňující otázka:

Byl každému bývalému zaměstnanci odebrán přístup do systému?

IT specialista: Ano, každému zaměstnanci je přístup z AD smazán a z NIS je přístup zneplatněn.

6. **Jsou omezeny přístupy pracovníků IT k datům – prostřednictvím hesel či oddělených funkcí?**

IT specialista: Ne, nejsou omezeny.

7. **Je přístup k IT zařízením omezen pouze na oprávněné osoby? Je možný vzdálený přístup?**

IT specialista: Ano, k IT zařízením mají přístup pouze autorizované osoby. A zda je možný vzdálený přístup? Samozřejmě, i tohle umíme za pomoci VPN.

Tabulka 24 - Souhrn tematického okruhu 3

BEZPEČNOST DAT ZDRAVOTNICKÉHO ZAŘÍZENÍ	
Přijata bezpečnostní pravidla	Ano, jsou
Došlo k narušení bezpečnosti	Ano, ale na serveru jiné firmy
Odebrán přístup ex-zaměstnanci	Ano
Nastavené kontroly sítě	Ne
Záznam neoprávněných vstupů	Ano
Omezeny přístupy pracovníku IT	Ne
Omezen přístup k zařízení	Ano

5.3.4 4. Tematický okruh „IT kontroly a odpovědnost“

1. **Probíhá ve společnosti průběžné monitorování fungování vnitřních kontrol v oblasti IT?**

IT specialista: Víceméně monitorování probíhá.

2. **Je vedení včas informováno o případných problémech?**

IT specialista: Ano, informováni jsou v jednom kuse.

3. **Považujete rozdělení pravomocí a odpovědnosti v oblasti informačního systému za dostatečné?**

IT specialista: Ne, bohužel je potřeba předělat všechny přístupy a momentálně na to není čas a ani dostatek lidí.

Dále byly položeny doplňující otázky:

a. Myslíte si, že úroveň znalostí a zkušeností pracovníků IT oddělení odpovídají povaze jejich činnosti?
b. Kolik má zdravotnické zařízení pracovníků v IT oddělení?
c. Nachází se u Vás všechny tyto role? (Manažer KB, Architekt KB, Auditor KB, Incident Manager)

IT specialista: Ano, myslím si, že všichni mají dostatečnou úroveň vzdělání a zkušeností, které dalšími roky nabývají. IT pracovníků je přesně 5. Z uvedených rolí se u nás nenachází ani jedna.

Tabulka 25 - Souhrn tematického okruhu 4

IT KONTROLY A ODPOVĚDNOST VE ZDRAVOTNICKÉM ZAŘÍZENÍ	
Průběžné monitorování vnitřních kontrol	Probíhá
Včasné informování vedení	Ano
Dostatečné rozdělení pravomocí a odpovědnosti	Nedostatečné

5.3.5 5. Tematický okruh „Testování a školení“

V poslední části rozhovoru byly otázky směřovány především na školení a vzdělávání pracovníků ve zdravotnickém zařízení.

1. **Myslíte si, že dochází k dostatečnému testování a ověřování stavu ochrany?**

IT specialista: K žádnému testování či ověřování stavu ochrany nedochází.

2. **Myslíte si, že zaměstnanci všech oddělení zdravotnického zařízení jsou dostatečně vzděláváni a připravováni na možné kybernetické incidenty?**

IT specialista: Myslím si, že určitě nejsou.

Dále byly položeny doplňující otázky:

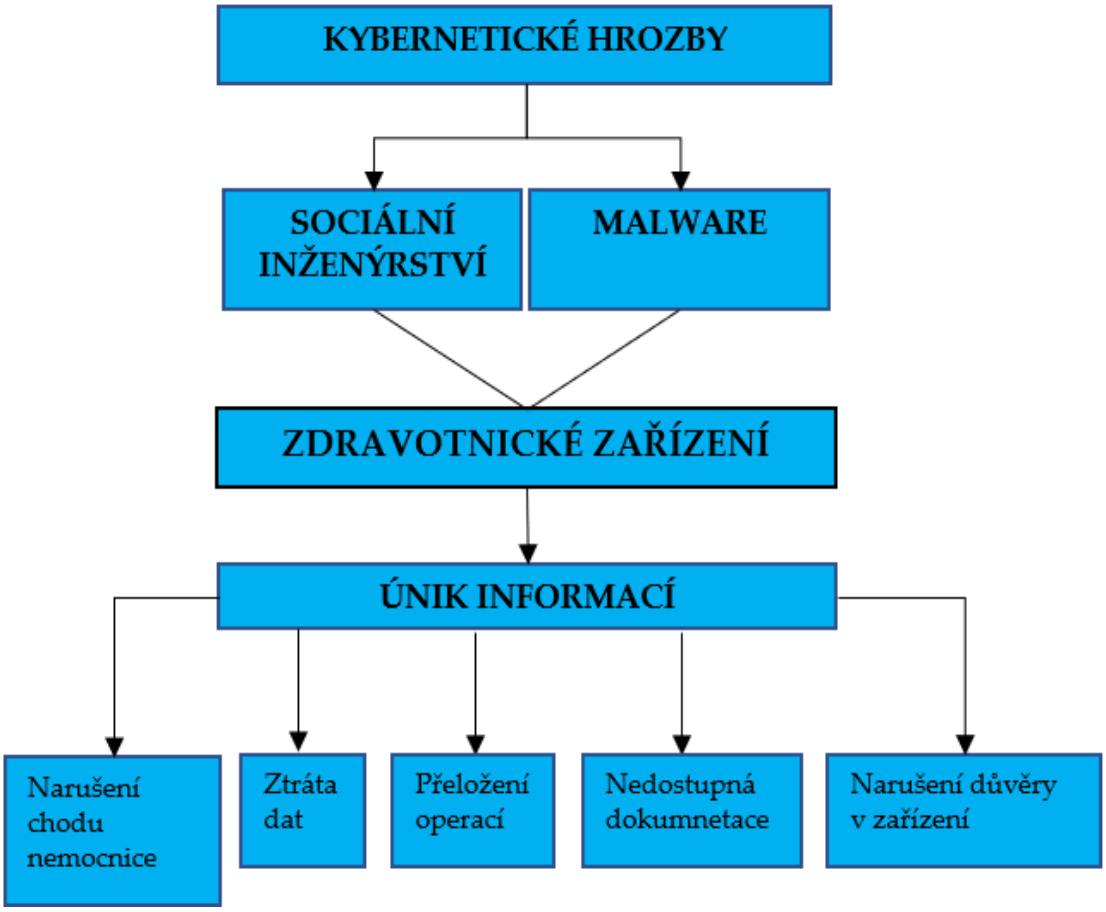
a. Kdo ve Vašem zdravotnickém zařízení provádí školení personálu na kybernetickou bezpečnost? Jedná se o internistu nebo externistu?
b. Jak často probíhá Vaše školení?

IT specialista: Školení by mělo provádět IT, nicméně ještě neproběhlo ani jedno. A školení u nás probíhá maximálně tak jednou za deset let.

Tabulka 26 - Souhrn tematického okruhu 5

ŠKOLENÍ A TESTOVÁNÍ OCHRANY VE ZDRAVOTNICKÉM ZAŘÍZENÍ	
Testování a ověřování stavu ochrany	Nedochází k testování a ověřování
Školení zaměstnanců	Nedostatečné

5.4 Rizika úniku informací



Obrázek 26 - Diagram rizik úniku informací [vlastní]

Pomocí odborných výzkumů bylo zjištěno, jaké je způsobeno riziko úniku informací z lůžkového zdravotnického zařízení. Především se jedná: o narušení chodu zařízení, přerušení veškeré léčby, nemožnost poskytnutí potřebné péče, nedostupnost databází s dokumentací pacientů, nutnost odložení plánovaných operací, narušení důvěrnosti v zařízení a v neposlední řadě naložení velkého obnosu financí na obnovu provozu.

5.5 Doporučení pro zlepšení ochrany dat

Ve zdravotnictví je problematika kybernetické bezpečnosti zásadně personálně a finančně podhodnocena. Je zapotřebí si uvědomit sílu technologií, stejně jako potencionální nebezpečí, které představuje vlastní aktivita. Lidský

faktor představuje největší problém organizace, nicméně žádný systém nemůže bez zásahu lidského faktoru fungovat. Na podkladech uskutečněného rozhovoru s IT specialistou a dotazníkového šetření, které proběhlo mezi zaměstnanci ve zdravotnickém zařízení, byla navržena následná doporučení pro zlepšení ochrany dat a informací v zařízení.

Doporučení pro vedení zdravotnického zařízení:

- Pravidelné školení všech zaměstnanců v oblasti kybernetické bezpečnosti, a to minimálně 1x do roka;
- Omezit volný přístup k internetu (zakázat především veškeré sociální sítě, YouTube atp.);
- Pečlivé prověření nových zaměstnanců;
- Nastavení bezpečnostní politiky a pravidel v nemocnici;
- Nastavení silných hesel (minimální délka 9-12 znaků, mělo by obsahovat velká a malá písmena, číslice a speciální znaky).

Doporučení pro zaměstnance:

- Přihlašovací údaje do NIS používat pouze pro přihlášení do systému, nikoli mimo něj;
- Nikdy nikomu nesdělovat heslo;
- Při odchodu od počítače se vždy odhlásit;
- Zvážit každý e-mail, telefonát nebo textovou zprávu požadující údaje;
- Nikdy nereagovat ani neotevírat přílohy e-mailu, které přijdou už od prvního pohledu zvláštní [65].

5.6 Vyhodnocení hypotéz

HYPOTÉZA 1 *Alespoň 70 % respondentů absolvovalo školení v oblasti kybernetické bezpečnosti.*

S hypotézou 1 souvisela otázka z dotazníkového šetření č. 5.

V této otázce bylo zjišťováno, zda respondenti absolvují školení v oblasti kybernetické bezpečnosti. Výsledky dotazníkového šetření ukázaly, že pouze 8 respondentů (15 %) absolvovalo školení v oblasti kybernetické bezpečnosti. 45 respondentů (85 %) takovéto školení neabsolvovalo (viz Tab. 6 - Školení respondentů, Obr. 8 - Školení respondentů).

HYPOTÉZA 1 NEBYLA POTVRZENA

HYPOTÉZA 2 *Více jak polovina respondentů se při odchodu od počítače odhlásí.*

S hypotézou 2 souvisela otázka z dotazníkového šetření č. 14.

Otázka číslo 14 zjišťovala, zda se respondenti pokaždé, co odchází od počítače, odhlašují. Výsledky dotazníkového šetření ukázaly, že 33 respondentů (62 %), tedy více jak polovina dotazovaných, se při odchodu od počítače vždy odhlašuje. Dalších 18 respondentů (34 %) se při odchodu od počítače odhlašuje pouze občas. Zbylí 2 respondenti (9 %) označili odpověď, že se nikdy při odchodu od počítače neodhlašují (viz Tab. 15 - Odhlášení z PC při odchodu, Obr. 17 - Odhlášení z PC při odchodu).

HYPOTÉZA 2 BYLA POTVRZENA

HYPOTÉZA 3 *Alespoň 10 % respondentů se setkalo s nabádáním k šíření osobních údajů o pacientovi.*

S hypotézou 3 souvisela otázka z dotazníkového šetření č. 18.

Otázka číslo 18 se tázala, zda byli někdy respondenti nabádáni k šíření osobních informací o pacientovi ze zdravotnického zařízení. Z odpovědí vychází, že 46 respondentů (87 %) se s tímto nikdy nesetkalo. Pouze 2 respondenti (4 %) odpověděli, že se s nabádáním k šíření informací o pacientovi osobně setkali. Zbylých 5 respondentů (9 %) svou odpověď nechtělo uvést (viz Tab. 18 - Počet nabádaných respondentů k šíření informací, Obr. 20 - Počet nabádaných respondentů k šíření informací).

HYPOTÉZA 3 NEBYLA POTVRZENA

HYPOTÉZA 4 *IT oddělení má sepsané postupy, jak reagovat na případný kybernetický útok.*

S hypotézou 4 souvisela doplňující otázka z polostrukturovaného rozhovoru.

Doplňující otázka okruhu 2 „Fungování výpočetní techniky" zjišťovala, zda IT oddělení má sepsané postupy, jak reagovat na případný kybernetický útok. IT specialista odpověděl, že těmito postupy disponují a rovnou jej postupně vyjmenoval: okamžité odpojení od internetu, odizolování napadeného stroje, zjištění rozsahu napadení a v neposlední řadě kontaktování úřadů (viz 2. tematický okruh „Fungování výpočetní techniky").

HYPOTÉZA 4 BYLA POTVRZENA

6 DISKUZE A HODNOCENÍ VÝSLEDKŮ

„Každý řetěz je silný jen tak, jak je silný jeho nejslabší článek."

Arthur Conan Doyle

V této části práce se budou pojednávat a zhodnocovat dosažené výsledky z praktické části získané odbornými výzkumy.

Cílem práce bylo především identifikovat rizika úniku informací z lůžkového zdravotnického zařízení ve Středočeském kraji. Dále práce popisovala vybrané formy útoků s následkem úniku dat a informací z organizace.

Pro dosažení výsledků byla zvolena kvantitativní metoda výzkumu formou dotazníkového šetření, které proběhlo mezi zaměstnanci a kvalitativní metoda sběru dat formou řízeného rozhovoru s IT specialistou zajišťujícím bezpečnost dat ve zdravotnickém zařízení

Praktická část byla zaměřena na dvě vybrané formy útoků s následkem úniku dat a informací ze zdravotnického zařízení. První zkoumanou formou útoku na zdravotnické zařízení bylo sociální inženýrství. Pro výzkum dotazníkového šetření byli zvoleni zaměstnanci. Dotazníkové šetření bylo rozděleno na 4 části. Celkem se dotazníkového šetření zúčastnilo 53 zaměstnanců. První část se zajímala o samotné respondenty. Nejvíce respondentů bylo žen (celkem 47), zbylých 6 respondentů byli muži. Dotazník dále zjišťoval, v jakém oboru dotazovaní pracují. Výsledky ukazují, že nejvíce respondentů pracuje v chirurgickém oboru, a to celkem 17. Do chirurgického oboru spadá Gynekologické oddělení, ARO, Chirurgické oddělení, ORL a chirurgie hlavy a krku, Ortopedicko-úrazové oddělení, Oční oddělení, Urologické oddělení a Centrální operační sály. Dále 15 respondentů pracuje v oboru interním. Do tohoto oboru spadá Dětské oddělení, Interní oddělení, Neurologické

oddělení, Kožní oddělení, Pneumologické oddělení, Koronární jednotka, Radiační klinická onkologie, Metabolická jednotka a Kardiostimulační centrum. Dalších 9 respondentů pracuje ve společenském oboru. Zde je zahrnuto Rehabilitační oddělení, Stomatologická ordinace, Klinická psychologie, Psychiatrická ambulance, Dietní oddělení, Centrální a urgentní příjem, Sociální oddělení a Oddělení pracovního lékařství. V Komplementu pracuje pouhých 5 dotazovaných respondentů, kam spadá Hematologicko-transfuzní oddělení, Patologické oddělení, RDG a Klinická laboratoř. Zbylých 7 dotazovaných respondentů označilo možnost jiné. Ta zahrnovala Administrativu, Personalistiku, Zdravotnickou záchrannou službu nebo Covid oddělení z důvodu stále probíhající pandemii SARS-CoV-2.

V druhé části dotazníkového šetření bylo zjišťováno, zda jsou respondenti zdravotnického zařízení školeni v oblasti kybernetické bezpečnosti. V hypotéze 1 bylo stanoveno, že alespoň 70 % respondentů absolvovalo školení v oblasti kybernetické bezpečnosti. Na základě výsledků se hypotéza 1 nepotvrdila, neboť z celých 53 dotazovaných (100 %) bylo proškoleno pouze 8 (15 %) z nich. Především se jednalo o zdravotní sestry a lékaře z chirurgického a interního oboru. Celých 45 (85 %) respondentů odpovědělo, že takovéto školení neabsolvovalo (viz Obr. 8 - Školení respondentů). Další otázka navazovala a tázala se respondentů, jak školení probíhá a zda je pro ně přínosné. Z 8 školených respondentů odpověděli 4, že jejich školení probíhá prezenčně. Další 2 respondenti odpověděli, že školení probíhá on-line a zbylí 2 respondenti odpověděli, že z důvodu probíhající pandemie SARS-CoV-2 mají školení výjimečně on-line. Před pandemií byli tito respondenti školeni zaměstnavatelem prezenčně. Na otázku, zda bylo pro respondenty školení v oblasti kybernetické bezpečnosti přínosné, odpovědělo všech 8 "Ano, bylo".

Ochrana proti sociálnímu inženýrství spočívá především ve školení zdravotnického personálu. To samé tvrdí i autor Novák ve své práci. Uvádí, že: *„Z pohledu organizace je důležité školení zaměstnanců a pravidelná dlouhodobá osvěta“* [66]. Dle náměstka informačních technologií Fakultní nemocnice v Olomouci Antonína Hlavinky *„je vzdělávání a edukace zaměstnanců velmi důležitá. Zejména je zapotřebí navrhnout, zpracovat a průběžně realizovat rozvoj bezpečnostního povědomí jinou formou (aktivitami), než pouze pomocí školení/vzdělávání“* [67]. Jelikož výsledky dotazníku poukazují, že více jak polovina dotazovaných zaměstnanců není školena, bylo zkoumanému zdravotnickému zařízení doporučeno, aby alespoň 1x za rok došlo k proškolení celého personálu v oblasti kybernetické bezpečnosti a předešlo se tak případným útokům technikami sociálního inženýrství.

Třetí část dotazníkového šetření se zaměřovala na přístupy a hesla do informačního systému. Nejprve se tázalo respondentů, zda mají přístup na všechna oddělení v nemocnici. Celých 89 % (47) respondentů odpovědělo, že nedisponují přístupy na všechna oddělení nemocnice. Disponuje jimi pouze 11 % (6) respondentů. Jedná se o lékařku z urgentní medicíny, nutriční terapeutku, lékařku z interního oboru a 3 zdravotní sestry z chirurgického oboru.

Dále bylo zjišťováno, zda zaměstnanci používají přihlašovací údaje (login a heslo) do NIS i mimo nemocnici, např. pro přihlášení na sociální sítě. Celých 83 % (44) respondentů je používá pouze pro přihlášení do NIS. Oproti tomu 6 respondentů své přihlašovací údaje nepoužívá pouze pro přihlášení do NIS, ale také pro přihlášení do účtů na sociálních sítí. Zbylí 3 respondenti svou odpověď nechtěli uvést. Riziko v používání přihlašovacích údajů i mimo organizaci tkví především v napadnutí neautorizovanou osobou a ohrožením tak nejen systému, ale i činnosti organizace.

Mikušová ve své diplomové práci uvádí, že: „*Řada zaměstnanců například často neví, že na Facebooku existuje archiv, který shromažďuje veškerá data, která kdy na Facebook vložili, a to od dob založení jejich profilu. Pokud se někdo dostane k soukromému uživatelskému účtu, může prostřednictvím tří kliknutí získat celé historie všech jejich konverzací, místa, ze kterých se na Facebook přihlašovali, čísla kreditních karet, pokud platili za nějaké aplikace prostřednictvím Facebooku, mohou získat data o rozpoznání tváře uživatele a mnoho dalších velmi jednoduše zneužitelných a citlivých informací. Je velice vhodné, aby zaměstnancům bylo v rámci interních školení doporučeno pro takové účely využívat zcela odlišné heslo od těch, které využívají pro přístup k účtům v rámci organizace a samozřejmě aby v takových případech využívali soukromou e- mailovou adresu*“ [68, s. 39].

S otázkou, zda se respondenti vždy odhlašují, pokud odchází od počítače, souvisela hypotéza 2. Stanovila, že více jak polovina respondentů se při odchodu od počítače odhlásí. Z výsledků dotazníkového šetření je zřejmé, že více jak polovina se při odchodu vždy odhlašuje. Přesně se jedná o 62 % (33) dotazovaných. Tímto byla hypotéza 2 potvrzena. Dalších 18 respondentů se při odchodu ohlašuje pouze občas a zbylí 2 respondenti se nikdy neodhlašují, pokud odchází od počítač. Jaké riziko z tohoto činění nebo spíše nečinění plyne? Jestliže se k počítači, který nebude odhlášený od systému, dostane neautorizovaná osoba, mohlo by dojít k zašifrování či odcizení veškerých dat nemocnice. Následky tohoto činu pak mohou být vyčísleny v hodnotě až několika stovek tisíc Kč.

Čtvrtá část dotazníkového šetření se zaměřila na techniky sociálního inženýrství, se kterými by se zaměstnanci zdravotnického zařízení mohli setkat či se s nimi už setkali. Zpočátku se respondentů dotazovalo, zda se někteří s nabádáním k šíření informací setkali. S otázkou souvisela hypotéza 3, ve které bylo stanoveno, že alespoň 10 % respondentů se setkalo s nabádáním k šíření

osobních údajů o pacientovi. Podle námi dosažených výsledků se s tímto setkalo pouze 4 % (2) respondentů, což nepotvrdilo stanovenou hypotézu 3. Dalších 9 % (5) respondentů svou odpověď uvést nechtělo. Celých 87 % (46) respondentů se s nabádáním k šíření nikdy nesetkalo. Načež navazovala další otázka tázající se respondentů, kteří se s nabádáním setkali, zda tento čin nahlásili na vedení nemocnice, IT oddělení nebo na PČR. Pouze 1 z respondentů tento čin nahlásil.

Poté se respondentů v dotazníku tázalo, zda se setkali s telefonátem, kdy se někdo vydával za někoho jiného či osobu blízkou a snažil se tak zjistit citlivé informace. Zde odpovědělo 43 respondentů, že se s takovýmto telefonátem nikdy nesetkalo, zatímco zbylých 10 respondentů tuto zkušenost má.

Nabádání k šíření, odcizení informací nebo telefonní hovory pro získání informací jsou běžnými technikami sociálního inženýrství, které nelze jednoznačně odhalit. Většina útočníků má velmi dobré manipulační i komunikační dovednosti, kterým lidé snadno podlehnou.

Autorka Mikušová taktéž uvádí, že: *„Útočníci prostřednictvím manipulace zaměstnanců dokážou získat i ty nejcitlivější informace. Útočníci dokážou díky sociálnímu inženýrství obejít úplně bez povšimnutí a bohužel často i velice jednoduše i ty nejdražší bezpečnostní nástroje. V případě útoku často oběť ani netuší, že někomu poskytla důležitá přístupová oprávnění, a to zákeřnost sociálního inženýrství ještě zvyšuje“* [68, s. 36].

Druhou zkoumanou formou kybernetického útoku na zdravotnické zařízení byl malware. Pro výzkum byl zvolen polostrukturovaný rozhovor realizován s IT specialistou zajišťujícím bezpečnost dat ve zdravotnickém zařízení. Rozhovor byl rozdělen do 5 okruhů. Otázky směřovaly zejména na systém nemocnice, výpočetní techniku, bezpečnost přístupů, IT kontroly a v neposlední řadě na vzdělávání a školení. Tato místa představují zranitelnost nemocnice,

které malware využívá za pomocí svých technik (ransomware, spam, keylogger atp).

K útokům na zdravotnická zařízení prostřednictvím malware a jeho technik dochází čím dál tím častěji. Kybernetické útoky na zdravotnická zařízení se v roce 2021 zvýšily o 45 %. Dnešní doba tomu samozřejmě napomáhá. Zdravotnický personál je vyčerpaný, ztrácí koncentraci, a tak se stává snadným cílem pro kyberzločince.

Zdravotnické zařízení zatím s žádným přímým kybernetickým útokem zkušenost nemá. Přesto to neznamená, že zařízení disponuje tou nejvyšší kybernetickou bezpečností, přes kterou žádný malware neprojde. Nicméně se zdravotnické zařízení snaží předcházet veškerým útokům nastavenými pravidly a procesy.

Frys z Vojenského technického ústavu na webináři uskutečněném AFCEA přednášel o problematice kybernetické ochrany nemocnic. Při analýze došel k závěru, že: *„Z hlediska technického a organizačního je úroveň zajištění kybernetické bezpečnosti nemocnic velmi nízká spíše až kritická. Současná úroveň zajištění kybernetické bezpečnosti nedokáže ochránit provoz a data nemocnic ani před náhodnými úroky páchané roboty, natož pak před cílenými a připravenými útoky zkušených hackerů“* [67].

Za pomocí postupů se ale snaží těmto útokům předcházet. Především disponuje nejnovějšími operačními systémy od společnosti Microsoft, které se po vydání nových aktualizací snaží obnovit. Ty chrání antivirus VirusFree před firewallem. Nicméně dle společnosti Gartner: *„Běžná antivirová řešení neposkytují dostatečnou ochranu před dnešními pokročilými hrozbami, postrádají rychlou odezvu a nejsou schopná odhalit příčinu nebo rozsah škody“* [67].

Dále dochází k zálohování a uchovávání IT dat, a to dle zajištěných procesů. Systém je zálohován kvůli velikému množství dat každý den. Pro větší ochranu se utvářejí kopie dat, které se umisťují na externí disky uložené mimo serverovnu, a to především pro případ, kdyby došlo k napadení systému prostřednictvím malware, jehož následkem by byla ztráta dat či jejich zašifrování. I pro tento případ má IT oddělení sepsané postupy, jak proti kybernetickému napadení reagovat. Mezi postupy patří okamžité odpojení od internetu, odizolování napadeného stroje, zjištění rozsahu napadení, a nakonec kontaktování úřadů. Tímto byla stanovená hypotéza 4 potvrzena.

Pro bezpečnost dat ve zdravotnickém zařízení jsou přijata dle IT specialisty dostatečná bezpečnostní pravidla a opatření pro zabezpečení výpočetní techniky. Zabezpečení systému a tím i výpočetní techniky spočívá především v kvalitně sestavených heslech, kterými se zaměstnanci přihlašují do NIS a AD. Pokud by došlo k prolomení hesla a nabourání se tak do systému, znamenalo by to problém obzvlášť při léčení pacientů. Jelikož by nebyla dostupná dokumentace, došlo by k zastavení léčby, plánované operace by musely být odloženy a důvěra v nemocnici by byla narušena.

Technici z IT oddělení si uvědomují závažnosti dopadu útoku na nemocnici, proto se snaží předcházet výše uvedeným rizikům. Kupříkladu je zavedena kontrola uživatelských práv pro přístup do sítě a všechny neoprávněné vstupy se logují. Taktéž je omezen přístup k důvěrným informacím. Zpřístupněn je pouze pro autorizované osoby. Jelikož může za útokem stát i bývalý zaměstnanec nemocnice, je důležité i takovému nebezpečí předejít. Z toho důvodu je všem bývalým zaměstnancům odebrán přístup z AD a do NIS je přístup zneplatněn.

Jako shrnutí tématu bude provedena komparace dosažených výsledků odborným výzkumem s výsledky autora Štusáka, který se ve své práci zabýval kybernetickými hrozbami proti kritické infrastruktuře ČR [69].

Tabulka 27 - Komparace kybernetických útoků

KYBRNETICKÉ HROZBY	CÍL	ÚTOČNÍK	TECHNIKY	DOPADY
Sociální inženýrství	Zaměstnanci; Zdravotnictví; Státní správy;	Zhrzený zaměstnanec; Kyberzločinec	Phishing; Trashing; Vishing; Pharming	Únik informací
Malware	Síť	Skupina kyberzločinců	Ransomware; Trojský kůň; Keylogger; Spam	Zašifrování dokumentace; Ztráta dat
Kryptomining	Výpočetní technika uživatele	Kyberzločinci	Útok na výpočetní výkon zařízení	Výpočetní výkon zařízení oběti
Kybernetická špionáž	Veřejný sektor; Zdravotnictví; Školství	Státní aktéři; Státem sponzorovaná skupina	Zranitelnost nultého dne; Spear-phishing útok	Ztráta dat; Ztráta obchodních tajemství
DDoS	Zdravotnictví; Kritická infrastruktura	Státní aktéři; Hacktivisté; Teroristé; Kyberzločinci	Botnety; UDP/ TCP flood	Narušení dostupnosti služeb; Ztráta dat

Tabulka 27 znázorňuje komparaci kybernetických hrozeb. Zobrazuje: cíle, techniky, typ útočníka i jaké dopady daná hrozba způsobí. S autorem Štusákem se shodneme, že kybernetické hrozby mají především za následek únik dat a informací z organizací, jelikož jsou tím nejcennějším, čím organizace disponují.

Závěru bylo dosaženo za pomoci odborných výzkumů. Zdravotnické zařízení ve Středočeském kraji se snaží možným kybernetickým útokům předcházet zajištěnými postupy a procesy, autorizací uživatelů AD a NIS, pravidelným zálohováním dat a tvorbou jejich kopií. Dále pravidelně aktualizují operační

systémy, které jsou zabezpečeny antivirem. Chybou je především nedostatečné vzdělávání a školení všech zaměstnanců v zařízení.

Nicméně, neexistuje jednotné řešení pro všechny nemocnice, byť existuje nějaký rámec a standart. Bezpečnost nemocnic je personálně i finančně podhodnocena. Hlavním nedostatkem je fakt, že problematika kybernetické bezpečnosti je v pozadí a je jí věnována pouze minimální pozornost.

7 ZÁVĚR

Cílem této diplomové práce bylo identifikovat rizika úniku informací z lůžkového zdravotnického zařízení ve Středočeském kraji. Dále práce popisovala vybrané formy útoků s následkem úniku dat a informací z organizace.

Riziko úniku informací ze zdravotnického zařízení bylo zjištěno za pomoci provedených odborných výzkumů. Zásadní riziko úniku informací tkví zejména v zastavení veškeré léčby a narušení tak běžného chodu nemocnice. Z pohledu zdravotnického zařízení znamená ztráta dat problém při poskytování potřebné péče pacientům. Zdravotnický personál tak nemůže vykonávat svou práci, jelikož není přístupná lékařská dokumentace pacientů. Rovněž tím dojde k odložení plánovaných operací. Odcizení dat pro nemocnici představuje vynaložení velkých finančních prostředků na obnovu systému. Dalším faktem je, že riziko úniku dat způsobí narušení důvěry zařízení. Z pohledu pacienta se jedná zejména o odcizení jeho osobních údajů či lékařské anamnézy. Tímto může dojít k finanční i psychické újmě pacienta. V tento moment ztrácí pacient důvěru v nemocnici.

Zkoumané zdravotnické zařízení ve Středočeském kraji se snaží možným kybernetickým útokům předcházet zajištěnými postupy a procesy, autorizací uživatelů v databázi a nemocničním informačním systému, pravidelným zálohováním dat a tvorbou jejich kopií. Dále pravidelně aktualizují operační systémy, které zabezpečují antivirem. Nicméně byly zjištěny určité nedostatky, které by mohly být zneužity technikami útoků k odcizení informací.

Na podkladech odborných výzkumů byla navržena doporučení pro vedení nemocnice a zaměstnance pro zlepšení ochrany dat. Hlavním viditelným nedostatkem je školení a vzdělávání zdravotnického personálu v oblasti

kybernetické bezpečnosti. Dle dotazníkového šetření dělají zaměstnanci chyby, které mohou mít fatální dopad na nemocnici. Jedná se především o používání přihlašovacích údajů do NIS mimo nemocnici, špatné nastavení hesel či odchod od počítače bez odhlášení ze systému. Školení či edukace by pomohly zaměstnancům takovýmto chybám předejít a zabránit tak případnému zneužití pro úspěšný útok. Dalším doporučením je omezení přístupu k volnému internetu. To znamená, že by zaměstnanci v pracovní době nemohli na počítačích nemocnice využívat sociální sítě jakými jsou např. Facebook, Instagram, YouTube atp. Tím se znemožní nainstalování škodlivého kódu a nedojde tak k narušení systému. Nadcházející doporučení je obecné a může být interpretováno i v jiném zdravotnickém zařízení. Jedná se o pečlivé prověření nových zaměstnanců, kteří jsou přijímáni do provozu nemocnice. Jelikož za většinou útoků stojí vlastní zaměstnanci organizace, pečlivým prověřením může být zabráněno případné sabotáži.

V diplomové práci bylo stanovených cílů dosaženo. Práce může sloužit všem lůžkovým zdravotnickým zařízením jako inspirace či návod, jak zajistit bezpečnost dat a předejít tak možným útokům s následkem úniku informací.

8 SEZNAM POUŽITÝCH ZKRATEK

AD – Databáze zdravotnického zařízení (Active Directory)

BRS – Bezpečnostní rada státu

BTC – Bitcoin

CERT – Computer Emergency Readiness Team

CSIRT – Computer Security Incident Response Team

ČR – Česká republika

FN Brno – Fakultní nemocnice Brno

IT – Informační technologie

NIS – Nemocniční informační systém

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

RDP – Remote Desktop Protocol

VPN – Virtuální privátní síť

XMR – Monero

9 SEZNAM POUŽITÉ LITERATURY

[1] KALAMÁR, Štěpán, Josef POŽÁR, POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY, a KATEDRA KRIMINÁLNÍ POLICIE. *Vybrané aspekty informační bezpečnosti*. Praha: Policejní akademie České republiky v Praze, 2010. ISBN 978-80-7251-339-0.

[2] KOLOUCH, Jan. *CyberCrime*. 1. vydání. Praha: CZ.NIC, z.s.p.o, 2016. Edice CZ.NIC, 14. publikace. ISBN 978-80-88168-15-7.

[3] PJG. *CyberSecurity.CZ* [online]. [vid. 2021-04-09]. Dostupné z: https://www.cybersecurity.cz/main.html

[4] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti = Cyber security glossary*. 2015. ISBN 978-80-7251-436-6.

[5] POŽÁR, Josef. *Manažerská informatika*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010. ISBN 978-80-7380-276-9.

[6] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o, 2015. Ediční řada Pro praxi. ISBN 978-80-7380-501-2.

[7] ČERMÁK, Miroslav. Přečtěte si, co je to vektor útoku, zranitelnost, exploit a payload - CleverAndSmart Management Consulting. *CleverAndSmart Management Consulting | Komplexní koncentrované know-how z oblasti strategického managementu, výkonnostního marketingu, kybernetické bezpečnosti a řízení rizik.* [online]. 2016 [vid. 2021-04-27]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/prectete-si-co-je-to-vektor-utoku-zranitelnost-exploit-a-payload/

[8] *Národní úřad pro kybernetickou a informační bezpečnost - O NÚKIB* [online]. [vid. 2021-04-03]. Dostupné z: https://nukib.cz/cs/o-nukib/

[9] *Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní management ve vzájemných souvislostech = Cyber security, economic crime and security management in mutual context*. 2020. ISBN 978-80-7251-505-9.

[10] INFO@AION.CZ, AION CS-. Nalezené předpisy. *Zákony pro lidi* [online]. [vid. 2021-04-12]. Dostupné z: https://www.zakonyprolidi.cz/hledani?text=kybernetick%C3%BD%20z%C3%A1kon

[11] *Bezpečnost dat v praxi* [online]. [vid. 2021-04-09]. Dostupné z: https://www.systemonline.cz/clanky/bezpecnost-dat-v-praxi.htm

[12] POŽÁR, Josef, POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY, a KATEDRA TEORIE POLICEJNĚ BEZPEČNOSTNÍCH ČINNOSTÍ. *Základy teorie informační bezpečnosti*. Praha: Vydavatelství PA ČR, 2007. ISBN 978-80-7251-250-8.

[13] MOLNÁR, Zdeněk. *Efektivnost informačních systémů*. 1. vyd. Praha: Grada Pub, 2001. Information systems. ISBN 978-80-7169-410-6.

[14] *Pozar2.pdf* [online]. [vid. 2021-03-31]. Dostupné z: https://www.cybersecurity.cz/data/Pozar2.pdf

[15] KNÝ, Milan, Josef POŽÁR, POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY, a FAKULTA BEZPEČNOSTNÍHO MANAGEMENTU. *Aktuální pojetí a tendence bezpečnostního managementu a informační bezpečnosti*. Brno: Tribun EU, 2010. ISBN 978-80-7399-067-1.

[16] *candik2.pdf* [online]. [vid. 2021-04-03]. Dostupné z: https://www.cybersecurity.cz/data/candik2.pdf

[17] NOVÁK, Luděk a Josef POŽÁR. Systém řízení informační bezpečnosti. nedatováno, 10.

[18] *RIZIKA.pdf* [online]. [vid. 2021-04-09]. Dostupné z: http://fei1.vsb.cz/kat420/vyuka/Magisterske%20nav/prednasky/web/RIZIKA.pdf

[19] POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 978-80-86898-38-4.

[20] *IT Security s.r.o.* [online]. [vid. 2021-04-11]. Dostupné z: http://www.it-security.cz/sluzby/analyza-rizik.html

[21] HROMADA, Martin, Petr HRŮZA, Josef KADERKA, Oldřich LUŇÁČEK, Miroslav NEČAS, Bohumil PTÁČEK, Leopold SKORUŠA a Richard SLOŽIL. *Kybernetická bezpečnost: teorie a praxe*. 2015. ISBN 978-80-87994-72-6.

[22] REDAKCE, od. *Únik dat způsobuje často neopatrnost nebo neznalost | IT SECURITY NETWORK NEWS* [online]. 19. listopad 2019 [vid. 2021-04-12]. Dostupné z: https://www.itsec-nn.com/unik-dat-zpusobuje-casto-neopatrnost-nebo-neznalost/

[23] *ÚNIK INFORMACÍ A DAT* [online]. [vid. 2021-04-12]. Dostupné z: https://www.acsa.cz/verejnasprava/uzitecne/informacni-bezpecnost/unik-informaci-a-dat/

[24] DRASTICH, Martin. *Systém managementu bezpečnosti informací*. Praha: Grada, 2011. ISBN 978-80-247-4251-9.

[25] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Brno: Computer Press, 2004. ISBN 978-80-251-0106-3.

[26] *zav_prace_soubor_verejne.pdf* [online]. [vid. 2021-04-14]. Dostupné z: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=150131

[27] MCCARTHY, Linda a Denise WELDON-SIVIY. *Buď pánem svého prostoru: jak chránit sebe a své věci, když jste online*. Praha: CZ. NIC, 2013. ISBN 978-80-904248-6-9.

[28] *kyberneticke_utoky.pdf* [online]. [vid. 2021-04-22]. Dostupné z: https://csirt.cesnet.cz/_media/cs/documents/kyberneticke_utoky.pdf

[29] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. ISBN 978-80-247-1561-2.

[30] *Statistika kyberkriminality - Policie České republiky* [online]. [vid. 2021-04-18]. Dostupné z: https://www.policie.cz/clanek/statistika-kyberkriminality.aspx

[31] KUNEŠ, Jaku. Co je sociální inženýrství? - 1. díl - PCWorld.cz. *PCWorld* [online]. [vid. 2021-04-09]. Dostupné z: https://www.pcworld.cz/clanky/co-je-socialni-inzenyrstvi-1-dil/

[32] MITNICK, Kevin D a William L SIMON. *Umění klamu*. Gliwice: Helion, 2003. ISBN 978-83-7361-210-5.

[33] *Co je phishing? | Vyhněte se e-mailovým podvodům a útokům | Avast* [online]. [vid. 2021-04-15]. Dostupné z: https://www.avast.com/cs-cz/c-phishing?

[34] JAMES, Lance. *Phishing bez záhad*. Praha: Grada, 2007. ISBN 978-80-247-1766-1.

[35] *Bezpečný internet | Phishing a pharming* [online]. [vid. 2021-04-16]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/phishing-a-pharming.aspx

[36] *Co je malware a jak ho odstranit | Ochrana proti malware | Avast* [online]. [vid. 2021-04-06]. Dostupné z: https://www.avast.com/cs-cz/c-malware?

[37] *Co je Adware a jak ho spolehlivě odstranit? | ESET* [online]. [vid. 2021-04-14]. Dostupné z: https://www.eset.com/cz/adware/

[38] *Co je Spyware a jak ho spolehlivě odstranit? | ESET* [online]. [vid. 2021-04-14]. Dostupné z: https://www.eset.com/cz/spyware/

[39] *Co je spyware | Nástroj na detekci a odstranění spyware zdarma | Avast* [online]. [vid. 2021-04-11]. Dostupné z: https://www.avast.com/cs-cz/c-spyware?

[40] *Keylogger a Anti-keylogger | Avast* [online]. [vid. 2021-04-14]. Dostupné z: https://www.avast.com/cs-cz/c-keylogger?

[41] *Co je počítačový virus? | Nástroj na nalezení a odstranění virů | Avast* [online]. [vid. 2021-04-14]. Dostupné z: https://www.avast.com/cs-cz/c-computer-virus?

[42] *Trojský kůň | Kybernetická bezpečnost* [online]. [vid. 2021-04-14]. Dostupné z: https://www.avast.com/cs-cz/c-trojan?

[43] SOCIÁLNÍ INŽENÝRSTVÍ, informační etika, SPAM a infoware a ČESKÁ SPOLEČNOST UŽIVATELŮ OTEVŘENÝCH SYSTÉMŮ EUROPEAN. CZ, ed. *Sociální inženýrství, informační etika, SPAM a infoware: 5.12.2003, Penzion Fousek, Štědronín*. Praha: Česká společnost uživatelů otevřených systémů European. CZ, 2003. ISBN 978-80-86583-05-1.

[44] *Co je spam? | Jak se mu vyhnout a jak odstranit spam | Avast* [online]. [vid. 2021-04-15]. Dostupné z: https://www.avast.com/cs-cz/c-spam?

[45] HALLER, Martin. Denial of Service (DoS) útoky: úvod. *Lupa.cz* [online]. [vid. 2021-04-20]. Dostupné z: https://www.lupa.cz/clanky/denial-of-service-dos-utoky-uvod/

[46] *Konec vyděračských virů – Nástroje k odstranění ransomware - Kaspersky* [online]. [vid. 2021-04-15]. Dostupné z: https://noransom.kaspersky.com/cz/faq/

[47] *Co je ransomware a jak se ho zbavit | Avast* [online]. [vid. 2021-04-14]. Dostupné z: https://www.avast.com/cs-cz/c-ransomware?

[48] *Diplomova_prace_Svoboda_Patrik.pdf* [online]. [vid. 2021-04-20]. Dostupné z: https://dspace.tul.cz/bitstream/handle/15240/154501/Diplomova_prace_Svoboda_Patrik.pdf?sequence=1&isAllowed=y

[49] Meet virtually with Cisco Webex. Anytime, anywhere, on any device. *Cisco Webex Site* [online]. [vid. 2021-04-18]. Dostupné z: https://cisco.webex.com/

[50] KILIÁN, Milan. Horažďovickou nemocnici napadl hacker, zmizely rentgeny. *Klatovský deník* [online]. 2018 [vid. 2021-04-19]. Dostupné z: https://klatovsky.denik.cz/zpravy_region/horazdovickou-nemocnici-napadl-hacker-zmizely-rentgeny-20180130.html

[51] TELEVIZE, Česká. Hackeři zaútočili na nemocnici následné péče v Horažďovicích. Vyřadili její informační systém. *ČT24 - Nejdůvěryhodnější zpravodajský web v ČR - Česká televize* [online]. [vid. 2021-04-19]. Dostupné z: https://ct24.ceskatelevize.cz/domaci/3254892-hackeri-zautocili-na-nemocnici-nasledne-pece-v-horazdovicich-vyradili-jeji-informacni

[52] ŠOPEJSTALOVÁ, Božena. Hackeři napadli počítačovou síť léčebny v Janově, chtějí výkupné. *Rokycanský deník* [online]. 2018 [vid. 2021-04-19]. Dostupné z: https://rokycansky.denik.cz/zlociny-a-soudy/hackeri-napadli-pocitacovou-sit-lecebny-v-janove-vydiraji-vedeni-20180629.html

[53] HOLAKOVSKÝ, Zdeněk Kellner, Milan. Útok na Nemocnici Benešov způsobil škodu 59 milionů korun, pachatel se nenašel. *Benešovský deník* [online]. 2020 [vid. 2021-04-19]. Dostupné z: https://benesovsky.denik.cz/zlociny-a-soudy/utok-na-nemocnici-benesov-zpusobil-skodu-59-milionu-korun-20200818.html

[54] *pdf-export.pdf* [online]. [vid. 2021-04-19]. Dostupné z: https://www.bozpinfo.cz/node/77565/pdf-export

[55] *Napadení Nemocnice Rudolfa a Stefanie Benešov krok po kroku – Nemocnice Rudolfa a Stefanie Benešov, a.s.* [online]. [vid. 2021-04-19]. Dostupné z: https://www.hospital-bn.cz/novinky/napadeni-nemocnice-rudolfa-a-stefanie-benesov-krok-po-kroku/

[56] Rozhovor s Robertem Modlingerem, IT specialistou. 14. duben 2021

[57] HALUZA, Michal Hrabal, Iva Haghofer ,Oldřich. Hackerský útok na bohunickou nemocnici: Pachatelům může hrozit i dvanáct let. *Brněnský deník* [online]. 2020 [vid. 2021-04-19]. Dostupné z: https://brnensky.denik.cz/zpravy_region/brno-nemocnice-hacker-bohunice.html

[58] Na nemocnici v Brně zaútočil vyděračský virus, špitál povolal krizového IT manažera | Aktuálně.cz. *Aktuálně.cz - Víte, co se právě děje* [online]. 20. březen 2020 [vid. 2021-04-19]. Dostupné z: https://zpravy.aktualne.cz/domaci/na-nemocnici-v-brne-zautocil-vyderacsky-virus-spital-povolal/r~ff91a02c6aa011eab1110cc47ab5f122/

[59] Kvůli hackerskému útoku na nemocnici v Německu zemřela pacientka. *Zdravotnický deník* [online]. 2020 [vid. 2021-04-20]. Dostupné z: https://www.zdravotnickydenik.cz/2020/09/kvuli-hackerskemu-utoku-nemocnici-nemecku-zemrela-pacientka/

[60] *V německé nemocnici zemřela pacientka během ransomwarového útoku – oTechnice.cz* [online]. [vid. 2021-04-20]. Dostupné z: https://otechnice.cz/v-nemecke-nemocnici-zemrela-pacientka-behem-ransomwaroveho-utoku/

[61] KOTOUČOVÁ, Hana. Kybernetické útoky na nemocnice a zdravotnické prostředky. nedatováno, 87.

[62] Kybernetická bezpečnost ve zdravotnictví. *EPRAVO.CZ* [online]. [vid. 2021-04-25]. Dostupné z: https://www.epravo.cz/top/clanky/kyberneticka-bezpecnost-ve-zdravotnictvi-112849.html

[63] *Národní úřad pro kybernetickou a informační bezpečnost - Hrozí zvýšené riziko kybernetických útoků vůči České republice* [online]. [vid. 2021-04-22]. Dostupné z: https://www.nukib.cz/cs/infoservis/aktuality/1703-hrozi-zvysene-riziko-kybernetickych-utoku-vuci-ceske-republice/

[64] REICHEL, Jiří. *Kapitoly metodologie sociálních výzkumů*. Praha: Grada, 2009. ISBN 978-80-247-3006-6.

[65] KNÝ, Milan, ed., [2015]. Bezpečnost na sociálních sítích: sborník příspěvků ze semináře na PA ČR v Praze, pořádaného v rámci Evropského měsíce kybernetické bezpečnosti ve spolupráci s NCKB a ČP AFCEA dne 26. října 2015. Praha: Policejní akademie České republiky v Praze. ISBN 978-80-7251-449-6.

[66] NOVÁK, Martin. Vybrané aspekty bezpečnosti informačních a komunikačních systémů [online]. 2016 [vid. 2021-05-07]. Dostupné z: http://dspace5.zcu.cz/handle/11025/23153

[67] S.R.O, Pixelfield. *Webinář: Řešení KB pro zdravotnictví | AFCEA* [online]. [vid. 2021-05-07]. Dostupné z: https://www.afcea.cz/akce/webinar-reseni-kb-pro-zdravotnictvi/

[68] MIKUŠOVÁ, Věra. *Hrozby a rizika úniku informací z organizace* [online]. Praha, 2017. POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE. Dostupné z: file:///C:/Users/HP/Downloads/Diplomov%C3%A1_pr%C3%A1ce_%C3%BAnik_informac%C3%AD_14.3..2017.pdf

[69] ŠTUSÁK, Michal. *Kybernetické hrozby proti kritické informační infrastruktuře v ČR* [online]. Kladno, 2020. ČVUT FBMI. Dostupné z: file:///C:/Users/HP/Downloads/2019_2020_LS_f_bc_34537_12421_xstusak_1590044102%20(2).pdf

10 SEZNAM POUŽITÝCH OBRÁZKŮ

11 SEZNAM POUŽITÝCH TABULEK

12 SEZNAM PŘÍLOH

Příloha 1 - Dotazník pro zaměstnance lůžkového zdravotnického zařízení

Dobrý den,

jmenuji se Dominika Koevová a jsem studentkou navazujícího magisterského studia na Českém vysokém učení technickém, fakulta Biomedicínského inženýrství, program Civilní nouzové plánování.

Ráda bych Vás touto cestou požádala o vyplnění dotazníku, který mi bude podkladem do mé diplomové práce s názvem: Analýza rizik úniku informací z lůžkového zdravotnického zařízení ve Středočeském kraji. Dotazník je zcela anonymní.

Předem mockrát děkuji za Váš čas a ochotu.

Bc. Dominika Koevová

1. **Jste:**
   - Žena
   - Muž
2. **Uveďte své povolání:**
   - Zdravotní sestra
   - Lékař/ka
   - Jiné
3. **Uveďte, v jakém oboru pracujete:**
   - Chirurgický obor
   - Interní obor
   - Společenský obor
   - Komplement – Hematologicko-transfuzní oddělení Patologické oddělení, RDG, Klinická laboratoř,
4. **Uveďte délku Vaší praxe v nemocnici:**
   - Do 1 roku
   - Od 1 roku do 5 let
   - Od 6 let do 10 let

- Od 10 let do 15 let
- Od 16 let do 20 let
- Nad 20 let

----------**ŠKOLENÍ**----------

5. **Uveďte, jestli jste školen/a zaměstnavatelem v oblasti kybernetické bezpečnosti:**

   Nápověda k otázce: Alespoň 1x ročně

   - Ano, jsem
   - Ne, nejsem

6. **Uveďte, jak probíhá Vaše školení v oblasti kybernetické bezpečnosti:**

   - On-line
   - On-line (mimořádně – SARS – CoV – 2)
   - Prezenčně
   - Neprobíhá

7. **Uveďte obtížnost závěrečného testu školení:**

   - Lehká (zvládl/a bych to i bez školení)
   - Středně těžká
   - Těžká (bez školení bych to nezvládl/a)
   - Nejsem školen/a)

8. **Uveďte, zda bylo pro Vás školení přínosné:**

   - Ano, bylo (dozvěděl/a jsem se něco nového)
   - Ne, nebylo (ztráta času)

----------**PŘÍSTUPY A HESLA**----------

9. **Uveďte, zdali máte přístup na všechna oddělení v nemocnici:**

   - Ano, mám
   - Ne, nemám

10. **Uveďte, jestli máte přihlašovací údaj (login) do informačního systému:**

    - Vlastní
    - Přidělený (systém jméno a příjmení)
    - Jiné.

11. **Uveďte, jestli máte volný přístup k internetu:**

    Nápověda k otázce: Volný přístup znamená, že se můžete připojit na pracovním počítači na sociální sítě např. Facebook, Instagram

    - Ano, mám
    - Ne, nemám

12. **Uveďte, zda přihlašovací údaje, které používáte pro přístup do nemocničního informačního systému, používáte i jinde, např. e-mail, sociální sítě:**

    Nápověda k otázce: Přihlašovací údaje = login a heslo

    - Ano, používám.
    - Ne, nepoužívám.
    - Nechci uvést.

13. **Uveďte, jak často si měníte heslo:**

    - 1x za 3 měsíce
    - 1x za 6 měsíců
    - 1x za rok

14. **Odhlašujete se vždy, když odcházíte od počítače?**

    - Ano, vždy
    - Občas
    - Ne, nikdy

----------**OSTATNÍ**----------

15. **Víte, co znamená phishing?**

    - Ano, vím
    - Ne, nevím
    - Nejsem si jistý/á

16. **Pokud jste u předchozí otázky dal/a "Ano, vím", napište slovně co phishing znamená:**

17. **Co byste udělal/a, kdyby Vám přišel e-mail s neznámým obsahem?**

    - Otevřu ho a zareaguji!
    - Otevřu ho a poté smažu!
    - Dám do spamu!
    - Smažu!

18. **Uveďte, zda jste byl/a někdy nabádán/a k šíření osobních informací o pacientovi:**
    - Ano
    - Ne
    - Nechci uvést
19. **Pokud jste u přechozí otázky odpověděl/a "ANO", nahlásil/a jste to zaměstnavateli, na IT oddělení nebo na Policii ČR?**
    - Ano
    - Ne
20. **Setkal/a jste se někdy s telefonátem, kdy se někdo vydával za někoho jiného či osobu blízkou a snažil se z Vás dostat informace?**
    - Ano
    - Ne
    - Nechci uvést
21. **Myslíte si, že zdravotnické zařízení, ve kterém pracujete, je dobře připraveno na případný kybernetický útok?**
    - Ano
    - Ne
    - Nevím

Příloha 2 – Výzkumné otázky polostrukturovaného anonymního dotazníku

KATEGORIE 1: Operační systém zařízení

1. Jaký/é operační systém/y je/jsou používán/y ve Vašem zdravotnickém zařízení?

2. Jak často dochází k aktualizacím operačních systémů?

3. O bezpečnost Vašich uložených dat se stará nasmlouvaná firma, popřípadě se o jejich bezpečnost staráte sami?

4. Byly někdy zaznamenány nějaké významné poruchy či problémy s fungováním systému a zpracování dat?

KATEGORIE 2: Funkčnost Informační a komunikační techniky

1. Jsou zajištěny postupy pravidelného zálohování a uchovávání IT dat?

- Jak často je systém zálohován?
- Jsou vytvářeny kopie?

2. Je k dispozici plán obnovy pro případ nešťastných událostí, kterými jsou např. přírodní katastrofy, krádež nebo kybernetický útok tak, aby chod nemocnice mohl pokračovat v činnosti bez významného přerušení?

- Jak je tato nahodilá událost řešena z pohledu IT?
- Můžete mi popsat postupy při kybernetickém útoku?

3. Mají zaměstnanci k dispozici technickou podporu?

- Obrátil se na Vás někdy zaměstnanec s problémem, že omylem zaslal údaje o pacientovi jinam, než měl nebo že smazal důležitou složku a potřebuje ta data zpět?

KATEGORIE 3: Přístup k datům (bezpečnost)

1. Jsou přijata a realizována dostatečná bezpečnostní pravidla a opatření pro zabezpečení výpočetní techniky?

- Je nastaven systém hesel a oprávnění?
- Jak často se provádí obnova hesel?
- Lze nastavit již jednou použitá hesla?
- Existuje fyzické zabezpečení serveru? (chráněná místnost)

2. Došlo někdy k narušení bezpečnosti?

- Jak byla případně tato událost řešena?
- Jaký dopad může mít ztráta dat a informací na chod nemocnice, popřípadě zaměstnance a pacienty?

3. Je zavedena kontrola uživatelských práv pro přístup do sítě a do souborů (požadavek autentizace)?

4. Jsou nastaveny a zavedeny kontroly pro ochranu dat zdravotnického zařízení v rámci sítě?

- Používáte antivirus? Jaký?
- Jaké další zabezpečovací programy sítě využíváte?

5. Jsou vhodným způsobem zaznamenávány případy neoprávněného vstupu do systému?

- Byl každému bývalému zaměstnanci odebrán přístup do systému?

6. Jsou omezeny přístupy pracovníků IT k datům – prostřednictvím hesel či oddělených funkcí?

7. Je přístup k IT zařízením omezen pouze na oprávněné osoby? Je možný vzdálený přístup?

KATEGORIE 4: IT kontroly a odpovědnost

1. Probíhá ve společnosti průběžné monitorování fungování vnitřních kontrol v oblasti IT?

2. Je vedení včas informováno o případných problémech?

3. Považujete rozdělení pravomocí a odpovědnosti v oblasti informačního systému za dostatečné?

- Myslíte si, že úroveň znalostí a zkušeností pracovníků IT oddělení odpovídají povaze jejich činnosti?
- Kolik má zdravotnické zařízení pracovníků v IT oddělení?
- Nachází se u Vás všechny tyto role? (Manažer KB, Architekt KB, Auditor KB, Incident Manager)

KATEGORIE 5: Testování a školení

1. Myslíte si, že dochází k dostatečnému testování a ověřování stavu ochrany?

2. Myslíte si, že zaměstnanci všech oddělení zdravotnického zařízení jsou dostatečně vzděláváni a připravováni na možné kybernetické incidenty?

- Kdo ve Vašem zdravotnickém zařízení provádí školení personálu na kybernetickou bezpečnost? Jedná se o internistu nebo externistu?
- Jak často probíhá Vaše školení?