Ochrana zdravotnických zařízení proti útokům od pacientů

Cybersecurity of healthcare facilities against attacks from patients

Projekt 3

Studijní program: Informatika a kybernetika ve zdravotnictví

Autor práce: Šimon Kochánek

Vedoucí práce: RNDr. Dagmar Brechlerová, Ph.D.

České vysoké učení technické v Praze, Fakulta biomedicínského inženýrství

Katedra informačních a komunikačních technologií v lékařství Akademický rok: 2022/2023

**Z a d á n í P r o j e k t III**

Student: Šimon Kochánek

Obor: Informatika a kybernetika ve zdravotnictví

Téma: Ochrana zdravotnických zařízení proti útokům od pacientů

Téma anglicky: Cybersecurity of healthcare facilities against attacks from patients

Z á s a d y p r o v y p r a c o v á n í :

Pacienti hospitalizovaní ve zdravotnickém zařízení dnes očekávají možnost přístupu k Internetu (práce, kontakt s rodinou ).. Běžně používají zařízení různého typu (telefon, NTB…). Při nedodržení jasné bezpečnostní politiky hrozí nebezpečí, že se pacient dostane do vnitřního IS dané nemocnice. Student zanalyzuje teoreticky stav v menší nemocnici a navrhne jasná pravidla pro zabezpečení. Např. oddělení jednotlivých IS, nemožnost odposlechnout data, fyzická bezpečnost (pacient není sám ponechán v ordinaci s otevřeným počítačem personálu atd.). Student tato nebezpečí shrne a navrhne základní ochranu proti nim.

Seznam odborné literatury:

<https://www.epravo.cz/top/clanky/kyberneticka-bezpecnost-ve-zdravotnictvi-112849.html>

<https://osveta.nukib.cz/mod/page/view.php?id=2385>

<https://pubmed.ncbi.nlm.nih.gov/35062504/>

<https://pubmed.ncbi.nlm.nih.gov/33023808/>

Vedoucí: RNDr. Dagmar Brechlerová, Ph.D.

Konzultanti:

V Praze dne 8.10. .2022

....................................................

studentka / student

....................................................

vedoucí práce

....................................................

vedoucí / zástupce ved. katedry

**PROHLÁŠENÍ**

Prohlašuji, že jsem práci s názvem „Ochrana zdravotnických zařízení proti útokům od pacientů“ vypracoval samostatně a použil k tomu úplný výčet citací použitých pramenů, které uvádím v seznamu přiloženém k práci.

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

V Kladně 25.11.2022 …...….………...………………...

Šimon Kochánek

**PODĚKOVÁNÍ**

Rád bych poděkoval paní doktorce za možnost pracovat na tomto projektu pod jejím vedením. Tento projekt mi umožnil se zaměřit na každodenní problematiku kybernetické bezpečnosti v nemocnic před pacianty a za to jsem jí vděčný.

**ABSTRAKT**

Ochrana zdravotnických zařízení proti útokům od pacientů

Cílem této práce je teoreticky zanalyzovat všechny možné cesty útoku ze strany pacientů a návštěvníků v menší nemocnici. Dalšími cíly je na tyto útoky najít vhodné opatření a navrhnout bezpečnostní politiku v takovémto zařízení. Pomocí analýzy nemocničního systému analyzujeme všechny možné přístupové body a na ty aplikujeme bezpečnostní opatření. Výsledkem této práce bude jasný výsledek analýzy se sadou bezpečnostím opatření a typů na zabezpečení.

**Klíčová slova**

Bezpečnost, IS, nemocnice

**ABSTRACT**

Cybersecurity of healthcare facilities against attacks from patients

One of the main goals of this thesis is to analyze every possible way to attack from patients and visitors in smaller hospital. Next goal is to find the appropriate precautions and implement security politics. With analysis of hospital informational system we can get all the accessible points to hospital network and safe. The another goal is to make clear output of analysis and with security measures and tips on cyber security.

**Keywords**

Security of Hospital informational system, Cybersecurity

Obsah

[Seznam symbolů a zkratek 8](#_Toc476327912)

[1 Úvod 9](#_Toc476327913)

[1.1 Přehled současného stavu 9](#_Toc476327914)

[1.2 Cíle práce 9](#_Toc476327915)

[2 Metody 10](#_Toc476327917)

2.1 Analýza rizik…………………………………………………………………10

2.2 Potenciální hrozby............................................................................................11

[3 Výsledky 1](#_Toc476327918)3

[4 Diskuse 1](#_Toc476327919)4

[5 Závěr 1](#_Toc476327920)5

[Seznam použité literatury 1](#_Toc476327921)6

# Seznam symbolů a zkratek

#### Seznam zkratek

|  |  |
| --- | --- |
| Zkratka | Význam |
| MITM | Man In The Middle ( Označení útočníka mezi dvouma zařízeními) |
| NÚKIB  IS | Národní Úřad pro Kybernetickou a Informační Bezpečnost  Informační Systém |

# Úvod

V našem každodenním životě jsou určité situace kdy se dostanem do zdravotních zařízení a i v nich je potřeba řešit otázku kybernetického zabezpečení. Většina těchto zařízení nabízejí například volně dostupné připojení pomocí wifi. Už to, je jeden přístup, který je třeba hlídat proti útokům. U tohoto problému je například nutno hlídat oddělení síťí a nejlépe je potřeba každého připojeného také oddělit. Na tuto problematiku bych se rád v tomto projektu zaměřil.

## Přehled současného stavu

Náš přehled si můžeme zatím představit na nemocnici v níž platí určitá politika, ale nesplňuje určitá doporučení vydaná Národním úřadem pro kybernetickou(dále jen jako NÚKIB) a informační bezpečnost. Tato nemocnice neni na seznamu 46 zařízení, která spadají do zákona o kybernetické bezpečnosti č. 181/2014 Sb. . Tato zařízení jsou povinny dodržovat příslušné vyhlášky.

Tato nemocnice má bohužel například jednoho pracovníka, který spravuje výpočetní techniku, celou počítačovou síť, připojení k nemocničnímu informačnímu systému. Tento segment je pak ještě většinou podfinancován a v tomto odvětví je velmi důležíté mít finanční prostředky na pořízení nejnovější výpočetní techniky.Když pak máme zastaralou výpočetní techniku, která v sobě nemá nejnovější fyzické i softwarové prvky, vystavujeme se bezpečnostním incidentům.

Náš pracovník by měl také vést analýzu rizik jak interní tak externí a krizový plán v případě kybernetického nebezpečí. Této problematice se budeme v projektu zabývat.

## Cíle práce

Základním cílem je navrhnout základní zabezpečení proti kybernetickým útokům ze stran pacientů. Prvním cílem tedy je zanalyzovat zabezpečení hypotetické menší nemocnice. Prohledat každou cestu kudy by útok mohl přijít. Např. otevřený počítač v ordinaci s pacientem, kdy si lékář někam odskočil.Měli bychom zanalyzovat jak moc personál nemocnice otevírá cestu ke kybernetickému nebezpečí.A také jak moc technika samotná. Dále ještě udělat analýzu rizik odkud může přijít útok a jak na něj reagovat.

Ještě poslední cíl by byl zanalyzovat nemocniční IS a zjistit, jestli má na počítačové síťi nějaké místa náchylná k útoku.

# Metody

## Analýza zabezpečení

Naším prvním úkolem. Je si projít požadavky našeho zadavatele. Přičemž si je můžeme představit takto:

* Např. 10 pracovišť kde je požadavek aby pracovní stanice byla připojena jak k internetu tak k vnitřní síti na informační nemocniční systém.Do toho nám vzniknou například sesterny kde musí být také možnost počítače a nejlépe i možnost se připojit do sítě přes kabel.
* Zaměstananci by měli mít doménové připojení aby se nejlépe mohli přihlásit kdekoli na počítači a ne aby na každém probíhala lokální správa. To znamená skoro každý zaměstnanec má své doménové uživatelské jméno a heslo, a tím přistupuje jak do přihlášení do počítače, tak dále třeba do wifi, email, IS atd...
* S tím také požadavek na dobrý provoz IS a spolu s tím jeho správa a úpravy dle požadavků.Na to se váže komunikace mezi odděleními a její problémy.
* Dále je velký důraz na několik Wifi jak pro personál, tak pro pacienty. Tyto sítě musí být dále velmi dobře nastavené a je tam několik potenciálních problému.
* Pak tady máme take požadavek na dobrou počítačovou síť s dobrým připojením, velkou rychlostí připojení k internetu, kvůli počtu zařízení, a také požadavek na její škálovatelnost.

Dle těchto dosti adekvátních požadavků můžeme definovat problémy a řešit potenciální incidenty a největší rizika. Tyto požadavky projdeme a najdeme rizika.

Při vytvoření pracovní počítačové stanice pro například praktického lékaře se už přidávají rizika. Tento doktor si například může nechat heslo na papírku u počítače a kdyby náhodou odešel z ordinace a pacienta tam nechal o samotě. Nebo lékař nezamkne svůj počítač při odchodu. Tak pacient lehce probourá zabezpečení k přístupu k počítači a může provádět úkony či spouštět programy pod uživatelem lékaře. Případně kdyby pacient zjistil nějaké chyby v zabezpečené pomocí social engineeringu a spustil nějaký sofistikovaný malware nebo rootkit.

Další problém je spouštění neznámých příloh, otevírání neznámých usb od pacientů a další možné cesty útoku.

Problémy s doménou a jejími přístupy jsou kapitola sama o sobě. Pokud to můžeme shrnout jen krátce. Jedná se o vzdálené připojení přes například vzdálenou plochu (Windows Remote Desktop), či přístup do nějakého prvku zdravotnického IS. Toto připojování musí být úzce monitorované a nejlépe dvoufázově oveřené. V praxi si to můžeme představit následovně:

Doktor si chce znovu projít zdravotní kartu pacienta, kterého ten den léčil, ale už je doma. Inicializuje připojení a bude se chtít připojit do své ordinace do kartotéky. Toto spojení bychom mohli dvoufázově ověřit například přes sms. Toto spojení nelze moc dobře ohlídat na jeho straně v rámci jeho připojení k internetu. Tudíž toto spojení není moc důvěrné a měli by být použity všechny možné prvky kybernetické bezpečnosti.

## Potenciální hrozby

Z naší analýzy rizik vycházíme s několika problémy, které je potřeba adresovat jako největší a také je podrobně vysvětlit:

**Social Engineering (Sociální inženýrství)**

Jedná se o manipulaci personálu. Pacient může například odlákat pozornost od otevřeného počítače, či zapojení usb flash disku nebo cd z rentgenu. Neprobíhá pak ani žádná kontrola obsahu před spuštěním ani ověření jestli s obsahem nebylo manipulováno.

Toto je ještě na mnoha pracovištích standard a je to bohužel velká bezpečnostní hrozba.

Může se také jednat o podvodný telefonát nebo email či v hraničních případech i o zprávy na sociálních sítích. Tato zpráva pak žádá personál aby například něco spustil, něco udělal atd.

Celkově pak můžeme shrnout cíle sociálního inženýrství jako snaha získaní neoprávněného přístupu, citlivých dat pacientů a šíření malwarů.

**Nastavení bezdrátového připojení(Wi-Fi)**

Při poskytování už předtím zmíněné veřejné sítě s bezdrátovým připojením je nutné používát nejnovější technologie. Šifrování WPA3. Toto šifrování je dovoleno bohužel jen na nejnovějších zařízeních. Dále také WIFI6. Tyto technologie jsou finačně ve větším měřítku náročnější a zvlášť pro pacienty bude tento výdaj těžké opodstatnit.

Další nutné opatření je segmentace sítí na tzv. VLANy. To znamená krájení počítačových sítí na podsítě. Vezmeme naší kompletní síť a začneme od nejdůležitějších tedy síť mezi ordinacemi a centrem nemocničního IS. Síť připojená na internet pro pacienty a návštěvníky je ta nejméně důležitá a proto ji také oddělíme od všech.

Ještě také za zmínku poslední technologie a to je AP isolation. Jedná se o izolaci bezdrátových a drátových zařízení, jelikož to není nutné pro provoz na veřejné wifi.

**Slabá fyzická ochrana**

Tímto tématem je myšlena fyzická bezpečnost aktivních a pasívních prvků počítačové sítě a programového vybavení. Je potřeba odpojit v racku všechny nepoužívané ethernet porty. Zamykat racky, schovávat kabely do lišt, nejlépe do výšky.Mít zamčené počítačové místnosti a serverové místnosti.

Také bychom měli zvážit pravidelnou vizuální kontrolu členem ochrané služby nebo naším IT specialistou .

**Odposlech**

Při odposlechu se může jednat o tzv. MITM( Man In The Middle) útok. Jedná se o útočníka který tvoří prostředníka mezi komunikací dvou subjektů. Tento útočník pak zpracovává obě strany komunikací a může je odposlouchávat nebo měnit.

Odpovědí na tento útok je jen používaním nejbezpečnějšího nastavení všude kde je to možné. Použitím firewallu s konstantní analýzou provozu. A pokud je to možné tak používat šifrování síťových paketů iPSec.

# Výsledky

Výsledek tohoto projektu se sestává z listu doporučení pro každého IT specialistu, který se případně nachází v takovéto pozici ze zadání .

1. Zavedení běžných bezpečnostních prohlídek kvůli identifikaci hrozeb a potenciálních možností útoku.
2. Zaveďte přísné kontroly přístupu, abyste zajistili, že k citlivým informacím a systémům budou mít přístup pouze oprávněné osoby.
3. Rychlé aktualizace a patche softwaru proti nově objeveným hrozbám.
4. Provádění pravidelného školení pro personál na téma kyberbezpečnosti
5. Zavedení dělení síťí na podsítě pomocí segmentace
6. Pravidelné zálohy s testovaním jejich obnovitelnosti v rámci času
7. Šifrování kde to jde
8. Více faktorové ověřovaní
9. Zavedení krizového plánu a jeho pravidelné iterace
10. Monitorování provozu a bezpečnostních incidentů a vedení dokumentace

# Diskuse

V rámci našich výsledků máme v rukou sérii velmi široce použitelných doporučení. Dodržení těchto doporučení může opravdu zmenšit dopad na menší nemocnici a její provozuschopnost. Problémem je také širokost těchto požadavků a jejich specifičnost daná použitout síťovou infrasktruturou. Nejdražší řešení je většinou od firmy CISCO a tá asi nejkvalitnější síťové prvky s aktivní správou a bezpečnostními prvky. Toto řešení ale menší nemocnice pravděpodobně obejdou a spokojí se s levnější varientou která spoléhá na zkušenost IT specialistů.

# Závěr

Cílem práce bylo vzít v potaz menší nemocnici a její rizika, zanalyzovat je a na toto reagovat. V mé práci jsem prošel celou nemocnici snad v každém scénáři a přivedl na nejpravděpodobnější rizika bezpečnostní politiku. Tato problematika má několik úskalí a to ve finančních možnostech, v nárocích na kordinaci a také ve školení zaměstnanců.

Celkově je mi líto člověka, který toto bude řešit, jelikož se jedná o velmi náročnou práci a velmi zodpovědnou a to s většinou s neodpovídajícím platovým ohodnocením.

# Seznam použité literatury

<https://www.epravo.cz/top/clanky/kyberneticka-bezpecnost-ve-zdravotnictvi-112849.html>

<https://osveta.nukib.cz/mod/page/view.php?id=2385>

<https://pubmed.ncbi.nlm.nih.gov/35062504/>

<https://pubmed.ncbi.nlm.nih.gov/33023808/>