ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA BIOMEDICÍNSKÉHO INŽENÝRSTVÍ
Katedra biomedicínské informatiky

Vzdělávání zdravotnického personálu v IT bezpečnosti

Training of medical staff in IT security

Bakalářská práce

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

Autor bakalářské práce:	Vladimír Čermák
Vedoucí bakalářské práce:	RNDr. Dagmar Brechlerová, Ph.D.

Kladno, 2023

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení:	**Čermák**	Jméno:	**Vladimír**	Osobní číslo:	**487479**
Fakulta:	**Fakulta biomedicínského inženýrství**				
Garantující katedra:	**Katedra biomedicínské informatiky**				
Studijní program:	**Biomedicínská a klinická technika**				
Studijní obor:	**Biomedicínská informatika**				

II. ÚDAJE K BAKALÁŘSKÉ PRÁCI

Název bakalářské práce:

Vzdělávání zdravotnického personálu v IT bezpečnosti

Název bakalářské práce anglicky:

Training of medical staff in IT security

Pokyny pro vypracování:

Student vytvoří vzdělávací materiály, které budou použity v již vytvořené vzdělávací platformě http://proambulance.cz/. Tyto materiály se budou týkat následujících částí: fyzická bezpečnost malé ordinace, autentizace, zálohování, sociální inženýrství. Materiály vyjdou z potřeb lékařů a sester, laborantů. Pro odpovídající úroveň materiálů student použije již vytvořený průzkum (D. Jirsa) a dále své znalosti tohoto prostředí. Materiál bude sloužit lékařům a dalšímu zdravotnickému personálu, nikoli tedy pracovníkům IT, tomu musí uzpůsobit úroveň. V rešeršní části zhodnotí dostupné vzdělávací materiály zejména NUKIBu i další. V praktické části student vytvoří materiály http://proambulance.cz/. Materiály ověří na menší (cca 10 až 15) skupině zdravotníků.

Seznam doporučené literatury:

[1] KOLOUCH, Jan a Pavel BAŠTA, Cyber Security, CZ.NIC, z.s.p.o., 2019, ISBN 978-80-88168-31-7
[2] Josef Požár, Informační bezpečnost, ed. vysokoškolská učebnice, Aleš Čeněk , 2005, ISBN 80-86898-38-5
[3] NUKIB, https://osveta.nukib.cz/local/dashboard/, 2020, https://osveta.nukib.cz/local/dashboard/
[4] Thorsten Petrowski, Bezpečí na internetu pro všechny, 2014, ISBN 978-80-7424-066-9

Jméno a příjmení vedoucí(ho) bakalářské práce:

RNDr. Dagmar Brechlerová, Ph.D.

Jméno a příjmení konzultanta(ky) bakalářské práce:

Ing. David Jirsa

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

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

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

PROHLÁŠENÍ

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

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

V Kladně, dne ……..……..……...

PODĚKOVÁNÍ

Rád bych tímto velmi poděkoval vedoucí mé bakalářské práce, paní RNDr. Dagmar Brechlerové, Ph.D. Za úvod do problematiky bezpečnosti, odborné vedení bakalářské práce, cenné rady a připomínky v průběhu zpracování této práce. Velké díky patří též zaměstnancům Oftalmologické kliniky Fakultní nemocnice Královské Vinohrady, především vedoucímu biomedicínského oddělení, panu Ing. Patriku Pluhovskému, MBA.

Děkuji také členům mé rodiny a všem, kteří mi během zpracování této bakalářské práce pomohli a poradili.

ABSTRAKT

Vzdělávání zdravotnického personálu v IT bezpečnosti

V této práci je cílem přispět ke vzdělávání zdravotníků a zdravotnického personál v bezpečnosti při práci s informačními technologiemi. Tato oblast se jeví v současné době jako velmi důležitá a v budoucnu bude tato důležitost nepochybně stoupat. Práce se zaměřuje na tyto hlavní části: fyzická bezpečnost malé ordinace, autentizace, zálohování, sociální inženýrství. Jelikož se jedná o materiály, které mají sloužit zdravotníkům a zdravotnickému personálu, je tomu uzpůsobena i úroveň obsahu a formy jednotlivých částí.

Klíčová slova

Bezpečnost, zdravotnictví, informační technologie, autentizace, zálohování, sociální inženýrství

ABSTRACT

Training of medical staff in IT security

The aim of the thesis is to help in training of medical staff in security while using and working with information technology. The importance of this field seems to be on a very high level at the moment with the potential to grow even higher in the future. The main topics of the thesis are: physical security of a small surgery, authentication, backup, social engineering. As these materials are determined to be used by medical staff, therefore the content level as well as difficulty are adapted correspondingly.

Keywords

Security, medicine, information technology, authentication, backup, social engineering

Obsah

Seznam symbolů a zkratek

Seznam symbolů

Symbol	Jednotka	Význam
b	bit	Jednotka velikosti počítačové paměti
B	Byte	Násobek bitu (8 bitů)
MB	Mega-byte	Násobek bytu (milion bytů)
GB	Giga-byte	Násobek bytu (miliarda bytů)
TB	Tera-byte	Násobek bytu (bilion bytů)

Seznam zkratek

Zkratka	Význam
IT	Informační technologie
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
ČVUT	České vysoké učení technické
FBMI	Fakulta biomedicínského inženýrství
FAQ	Frequently Asked Questions
ICT	Information and Comunication Technology
HW	Hardware – fyzické počítačové komponenty
SW	Software – počítačový program
FNKV	Fakultní nemocnice Královské Vinohrady
HDD	Hard Disk Drive
SSD	Solid-state Drive
GDPR	General Data Protection Regulation
ARO	Anesteziologické a resuscitační oddělení

1 Úvod

S rozvojem informačních a komunikačních technologií a s jejich stále se zvyšujícím využitím napříč různými obory, rostou zároveň i nároky kladené na bezpečnost v této oblasti. Rozvoj nových technologií s sebou nese, navzdory výhodám, také nové hrozby a rizika. S tímto je třeba počítat a také je nutno dát si na to pozor při práci s informačními technologiemi a při pohybu v kyberprostoru.

1.1 Kyberprostor

Co je to kyberprostor? V současnosti nejpřesnější a nejvíce používaná definice kyberprostoru zní takto:

> *„Kyberprostor je globální a vyvíjející se doména charakterizovaná užíváním elektrických sítí a elektromagnetického spektra, jejíž smysl je vytvářet, uchovávat, upravovat, vyměňovat, sdílet, vybírat, používat či vymazávat informace. Kyberprostor zahrnuje: a) fyzická i telekomunikační zařízení, která umožňují spojení technologií a komunikaci sítí systému, chápáno obecně (SCADA zařízení, smartphony/tablety, počítače, servery, atd.), b) počítačové systémy a komplementární software, který zaručuje spojení a funkčnost systému, c) spojení počítačových sítí, d) uživatelské vstupy a uzly zprostředkovatelů spojení, e) informace – uživatelská data.“* [1]

V kyberprostoru se tedy pohybuje každý, kdo pracuje s informačními technologiemi a nějakým způsobem je používá. Je to nehmotný prostor tvořený počítačovými, informačními a komunikačními systémy, které jsou navzájem propojeny. Toto vzájemné propojení dává možnost vytvářet, ukládat, používat a sdílet informace. Ačkoliv tomu dříve tak nebývalo, v kyberprostoru se stále více pohybují také osoby pracující ve zdravotnictví. Je to podobný vývoj jako i v ostatních oblastech kromě medicíny. Dříve informační technologie neexistovaly. Avšak s jejich příchodem se zjistilo, že mohou být velmi užitečné, a to v mnoha různých specializacích.

[1] MAYER, Marco, Pablo MAZURIER a Gergana TZVETKOVA. How would you define Cyberspace?. *Academia* [online]. Draft Pisa, 19.05.2014 [cit. 2022-03-01]. Dostupné z: https://www.academia.edu/7096442/How_would_you_define_Cyberspace

1.2 Informační technologie ve zdravotnictví

Informační technologie, jejich rozsah a možnosti využívání ve zdravotnictví neustále rostou. Je tedy nutné, aby zdravotnický personál věděl, jak bezpečně pracovat s těmito novými technologiemi, a jak se bezpečně pohybovat v kyberprostoru. Ve zdravotnictví, stejně jako v kterémkoliv jiném oboru, je důležitá bezpečnost při používání informačních a komunikačních technologií. Technologie používané ve zdravotnictví mají velkou důležitost, a to z toho důvodu, že pracují s lidským zdravím a lidskými životy. Nové technologie ve všech oblastech mají za úkol pomáhat při práci a zjednodušovat jak úkony, tak i celé postupy. Pokud jde však o lidské zdraví, mají nároky na technologie nepochybně vyšší prioritu.

1.3 Témata probíraná v práci

1.3.1 Fyzická bezpečnost malé ordinace

První část této práce se zaměřuje na fyzickou bezpečnost malé ordinace. Fyzická bezpečnost v sobě zahrnuje mnoho disciplín, které přímo s informačními technologiemi nesouvisí. Avšak v současnosti se v ordinacích vyskytuje velké množství elektronických zařízení, přístrojů a informačních systémů, u kterých je nutno zajistit jejich fyzickou bezpečnost. Nároky na fyzickou bezpečnost informačních systémů v ordinacích jsou do značné míry shodné s požadavky na fyzickou bezpečnost informačních systémů i v jiných prostředích. A je proto důležité zajistit bezpečnost těchto systémů v ordinaci, stejně jako kdekoliv jinde.

1.3.2 Autentizace

Autentizace je velmi důležité téma. Autentizací se totiž označuje proces ověření identity uživatele. Objevuje se ve všech oblastech, kde je třeba ověřovat identitu člověka, konkrétního software nebo datové zprávy. Využívá se tedy například při přihlašování na internetové stránky, služby, sociální sítě a přihlašování do informačních systémů. Všechny informační systémy musí znát identitu uživatele, který do nich přistupuje. O to více pak informační systémy, využívané ve zdravotnických zařízeních. Cílem je ochrana proti neoprávněnému přístupu, aby například k informacím určeným pouze pro lékaře neměla přístup zdravotní sestra. Pokud se do systému přihlašujeme klasicky – pomocí přihlašovacího jména a hesla – jedná se standardní způsob autentizace. Autentizace však může mít více úrovní (faktorů).

Zpravidla platí, že čím více úrovní autentizace má, tím je bezpečnější. Zároveň se však stává časově náročnější a zdlouhavou, což je také nežádoucí. Mezi takzvané přídavné faktory (kromě klasického jména a hesla) patří například zasílání kódu pomocí SMS zprávy do našeho mobilního telefonu. Tento způsob ověření identity uživatele, který se chce do systému přihlásit, je tedy bezpečnější než klasický způsob. A to z toho důvodu, že pokud by případný útočník znal naše jméno a heslo, podařilo by se mu do systému proniknout pod naším jménem. Pokud však do procesu přidáme další faktor (v našem případě kód z SMS zprávy), musel by útočník kromě jména a hesla mít přístup i k našemu mobilnímu telefonu, což se stává zřídkakdy. Pravděpodobnost vniknutí do systému neoprávněnou osobou je tedy v tomto případě mnohonásobně menší. A systém s lépe propracovanou autentizací je v souvislosti s tím také bezpečnější. V současné době stále se vyvíjejících, modernějších a vyspělejších technologií, se pro autentizaci využívají více a více takzvané biometrické údaje. Jsou to fyzické znaky a charakteristiky osob. Patří sem například otisky prstů, rysy ve tváři, nebo vzhled duhovky či sítnice v oku. Jejich bezpochyby nesmírnou výhodou je to, že jsou pro každého člověka unikátní. Můžeme tedy jejich prostřednictvím prokazovat svoji identitu.

1.3.3 Zálohování

Správně a bezpečně zálohovat data je potřeba ve všech oborech. Při zálohování vytvoříme kopii našich dat, kterou uložíme na bezpečném místě. Ideálně by to mělo být jiné místo, než na kterém se nachází původní data. Pokud by došlo ke ztrátě dat v důsledku poškození nebo z kteréhokoliv jiného důvodu, můžeme tuto zálohu využít. Ztráta dat je velmi nepříjemná, a to v jakékoliv situaci. Můžeme přijít o veškerá data, dokumenty nebo fotografie, které jsme ukládali někdy i v průběhu několika let. Zálohování je třeba provádět pravidelně, a tím snížit riziko ztráty dat na minimum. Pokud v datech, například v průběhu jednoho týdne, provedeme veliké změny, a data zálohujeme až po jednom týdnu, tak v případě ztráty dat jsme přišli o týdenní práci. Kdybychom však data zálohovali pravidelně každý den, jednalo by se o ztrátu dat „pouze“ za jeden den. Ve zdravotnictví, kde se pracuje s osobními daty pacientů, ve kterých jsou obsaženy často velmi citlivé a důležité údaje, je nutnost správného a pravidelného zálohování velmi vysoká. Ztrátu dat může způsobit uživatel sám, ať už úmyslně, nebo z důvodu neznalosti, nedbalosti, nebo obyčejné nepozornosti při práci s daty. Na vině může být též technický problém se zařízením, na kterém data uchováváme. A to v důsledku opotřebení zařízení nebo jiného poškození. Ke ztrátě dat může dojít i v důsledku přírodních pohrom. Velké riziko zde představuje například požár. Ostatní přírodní pohromy, jako jsou povodně či zemětřesení, jsou spíše méně pravděpodobné. Pravděpodobnost jejich výskytu záleží především na konkrétní geografické poloze (např. povodeň nelze očekávat na vyvýšeném místě, kopci atd…).

1.3.4 Sociální inženýrství

Sociální inženýrství (sociotechnika) se zabývá ovlivňováním a přesvědčováním lidí, s cílem získání citlivých informací, nebo donucení oběti k provedení určité akce. Bohužel nejslabší částí v oblasti bezpečnosti informačních systémů je vždy člověk (uživatel). Platí pravidlo, že nejnebezpečnější uživatel je ten s přístupovými právy. Důvodem, proč případný útočník (sociotechnik) bývá v mnoha případech úspěšný, je, že má velmi dobré schopnosti manipulace ostatních lidí. Nemusí se tedy zabývat složitým prolamováním hesel nebo jinými metodami. Jednodušší je přinutit, nebo zmanipulovat někoho jiného, aby útočníkovi (třeba i nechtěně) přístupové údaje sdělil. V pokročilých metodách sociotechniky si oběť mnohdy vůbec neuvědomí, že tyto citlivé údaje vyzradila. Lidé si totiž často neuvědomují cenu a hodnotu informací, které mají. Nevěnují tedy dostatečnou pozornost jejich ochraně a nenapadne je, že by se tyto informace mohly stát terčem útoku.

2 Přehled současného stavu

2.1 NÚKIB

V České republice se problematice bezpečnosti v oblasti informačních technologií věnuje především NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost, který sídlí v Brně. Vznikl v roce 2017 a převzal pracovní náplně tehdejšího Národního centra kybernetické bezpečnosti. Toto Národní centrum kybernetické bezpečnosti (NCKB) fungovalo od roku 2011. Národní úřad pro kybernetickou a informační bezpečnost vykonává mnoho činností, mezi které patří např.: vydávání opatření, ukládání příslušných správních testů, zajišťuje prevenci, věnuje se vzdělávání a podpoře v oblasti kybernetické bezpečnosti a v oblastech ochrany tajných informací, provádí analýzu a sledování kybernetických rizik atd. Za zmínku stojí také, že působí v oblasti veřejné regulované služby Evropského programu družicové navigace Galileo. NÚKIB pravidelně vydává zprávy, ve kterých sleduje aktuální dění. V současné době psaní této práce probíhá válka na Ukrajině. V souvislosti s tím NÚKIB analyzuje rizika týkající se produktů, které se vyrábí (v případě SW vyvíjí) v Rusku. Dále v návaznosti na současnou situaci NÚKIB vydává také varování související s ekonomickými sankcemi uvalenými na Ruskou federaci. Toto varování se týká rostoucí hrozby nedodržení smluvních závazků ze strany dodavatelů ICT služeb a produktů, které mají významný vztah k Rusku. Těmto organizacím, které podléhají Zákonu o kybernetické bezpečnosti, se doporučuje provést preventivní kroky, aby případné nedodržení závazků ze strany dodavatelů se vztahem k Rusku neohrozilo funkčnost jejich systémů.[2] V souvislosti s válkou na Ukrajině NÚKIB také vydal zprávu o tom, že na některé české weby utočí tzv. proruští hackeři. Úřad situaci průběžně vyhodnocuje, závažné dopady se však zatím neobjevily. Ve většině případu jde o takzvané DDos útoky. Princip těchto útoků spočívá v tom, že z mnoha náhodných IP adres v jeden okamžik nebo ve velmi krátkém časovém úseku přijde na server mnoho dotazů, server se v důsledku toho „zahltí“, a stránky přestanou fungovat. Stránky potom nejsou k dispozici, protože server není schopen takto velké množství dotazů v čase zpracovat. Řešení se nabízí v podobě zakázání přístupu ze zahraničních IP adres, a server je poté opět funkční, a přístupný alespoň pro tuzemské uživatele. Mezi instituce, které podobné útoky zaznamenaly, patří například České dráhy, letiště v Karlových Varech, letiště v Pardubicích nebo také weby ministerstva vnitra a policie.

[2] *Varování v souvislosti s ekonomickými sankcemi spojenými s Ruskou federací* [online]. NÚKIB, 21.03.2022 [cit. 2022-04-01]. Dostupné z: https://www.nukib.cz/cs/infoservis/hrozby/1823-nukib-vydal-varovani-v-souvislosti-s-ekonomickymi-sankcemi-spojenymi-s-ruskou-federaci/

NÚKIB v souvislosti s válkou na Ukrajině upozorňoval na zvýšené riziko kybernetických útoků už od konce ledna, potom též ke konci února. Snaží se české organizace podléhající Zákonu o kybernetické bezpečnosti varovat a vyzývá ke zvýšené opatrnosti. Je důležité, aby správci těchto serverů věnovali pozornost nejčastěji používaným technikám kybernetických útoků.

2.1.1 Vzdělávací kurzy

NÚKIB se zároveň věnuje vzdělávání široké veřejnosti v oblasti kybernetické bezpečnosti. Na základě svých zkušeností a znalostí tvoří dostupné online kurzy.[3] Tyto kurzy slouží jako otevřený, volně dostupný zdroj informací pro každého, kdo má zájem se v této oblasti vzdělávat. Nabídka kurzů je velmi široká. NÚKIB nabízí vzdělávací kurzy pro tyto oblasti:

1. Zdravotnictví
2. Statní správa a samospráva
3. Veřejnost
4. Školství

Forma kurzů, které NÚKIB tvoří, je velmi jednoduchá. Snaží se upoutat, a předkládat informace zajímavě. Každé téma je na začátku uvedeno praktickým příkladem, na kterém je ukázáno, jaké nebezpečí hrozí v reálném světě. Na konci každého tématu je část věnována takzvanému FAQ (Frequently Asked Questions – Nejčastěji Kladené Dotazy). Mezi témata, probíraná v těchto kurzech, patří základní instrukce a rady k používání přístupových údajů a hesel. Je zde zmínka také o dvou faktorovém ověřování, které je též později obsaženo v této práci. Kurzy se též věnují bezpečnosti mobilních telefonů. Tomu, jaké jsou možnosti odemykání těchto telefonů (kód PIN, otisk prstu a další). A v případě chytrých mobilních telefonů je třeba také dávat pozor na aplikace, které do mobilu instalujeme. Aplikace se doporučuje instalovat jen přes důvěryhodné obchody s aplikacemi (pro zařízení firmy Apple je to „AppStore“ a pro telefony se systémem Android se obchod nazývá „Google Play“). NÚKIB se rovněž věnuje problematice nedůvěryhodných e-mailů. V současné době stále existuje velký počet uživatelů, kteří uvěří obsahu těchto zpráv. E-mailové zprávy též v sobě mohou obsahovat škodlivé přílohy. Část kurzů je věnována také bezpečnému pohybu na internetu, aby uživatel neklikal na podezřelé odkazy, u kterých není jasné, na jaké stránky odkazují. Při používání všech druhů zařízení (mobilní telefony, stolní PC, notebooky…), jsou důležité také pravidelné aktualizace těchto zařízení, aby nedocházelo ke zneužívání známých mezer ve starších verzích systémů. Čím je systém starší, tím delší dobu mají útočníci na objevení případných mezer a chyb. S vydáním nové aktualizace se zároveň uvádí, které

[3] *Vzdělávací portál NÚKIB* [online]. Brno: NÚKIB, 2021 [cit. 2022-04-11]. Dostupné z: https://osveta.nukib.cz/local/dashboard/

chyby byly odstraněny a tím pádem se starší verze stává o to více zranitelnou. Je tedy třeba aktualizace neodkládat a provádět je pravidelně. Pro běžného uživatele nastává možné riziko také ve chvíli, kdy se připojí na veřejnou síť Wi-Fi. Fakt, že veřejné sítě jsou přístupny skutečně každému, zvyšuje riziko, že k nim může být připojen zkušený uživatel, který je schopen sledovat naši aktivitu. Na těchto veřejných sítích je lepší provádět jen základní prohlížení internetu, a nepřihlašovat se do žádných citlivých služeb, aby o nás útočník nemohl vysledovat důležitější, a více „lákavá“ data. V případě kurzů pro školy se kurzy dále dělí na témata zaměřená zvlášť pro učitele, jednotlivé žáky a stejně tak i na třídu jako celek. V době průběhu pandemie covid-19 bylo velmi aktuální téma bezpečnosti během online výuky. Národní úřad pro kybernetickou a informační bezpečnost se snaží o to, aby výuka v těchto kurzech byla nanejvýše efektivní a intenzivní. Aby během krátké doby bylo možné získat co nejvíce nových informací. Jednotlivá témata na sebe vhodně navazují.

V kurzech je lidem opakovaně sdělováno, že terčem útoku se může stát opravdu každý. Velkou roli v úspěšnosti takových útoků hraje především lidská neopatrnost, pochybení, podcenění situace nebo neznalost. Stále totiž u většiny uživatelů trvá přesvědčení, že se jich to netýká, že oni nemohou být terčem útoku. To dává prostor útočníkům zneužít neznalosti takových uživatelů, a zvyšuje to pravděpodobnost úspěšnosti útoku. Pokud si méně zkušený uživatel v kterékoliv organizaci není jistý, NÚKIB doporučuje jednu univerzální radu – obrátit se na IT oddělení. Každá firma nebo organizace takové oddělení má, a jeho účelem je problémy tohoto typu řešit.

Osobně kurzy NÚKIBU hodnotím velice kladně. Samotná úvodní stránka má povedený design a je přehledná. Na úvodní stránce jsou vypsány jednotlivé kurzy, každý má svůj název a k tomu přidanou fotografii. Pro snazší orientaci je možno též využít tzv. „Průvodce portálem“. V tomto průvodci se nachází základní informace o kurzech, přehled jaké kurzy NÚKIB nabízí, a také přehled témat obsažených v těchto kurzech. Při kliknutí na konkrétní kurz se otevře stránka tohoto kurzu. Každý kurz se skládá z několika okruhů. Okruhy je možno vypracovat i jednotlivě, nezávisle na ostatních. Kurzy kromě textu obsahují též velké množství obrázků, grafů nebo různých diagramů.

Je velmi dobře, že v České republice máme úřad, který se zabývá kybernetickou bezpečností na takové úrovni.

2.2 Útoky na zdravotnická zařízení

V červnu roku 2018 napadl hacker síť plicní nemocnice v Janově. Některá data zašifroval tak, že k nim nemocnice neměla několik dnů přístup. Lékaři se po tuto dobu nemohli dostat ke kartám pacientů. Nemocnice však odmítla vyplatit výkupné a většinu dat obnovila ze svých záloh.

Koncem roku 2019 se terčem útoku stala nemocnice Rudolfa a Stefanie v Benešově. Na nemocnici zaútočil počítačový vir typu ransomware, který šifruje a získává data z napadených počítačů. Za získaná data potom útočníci požadují výkupné. V důsledku tohoto útoku nemocnice přišla o objednávkový systém pro dárce krve, dále i některá administrativní a ekonomická data. Nebyla však ztracena žádná data o složkách pacientů. Nejednalo se o cílený útok pouze na Benešovskou nemocnici, současně byly napadeny i jiné instituce státní správy. Nemocnice následně této situace využila k posílení svých obraných mechanizmů před kybernetickými útoky, jako například investicí do nového firewallu v ceně dvou miliónů korun.[4]

Během března v roce 2020 se terčem útoku staly hned dvě nemocnice. Fakultní nemocnice Brno a psychiatrická nemocnice Kosmonosy. V Brněnské fakultní nemocnici bylo nutno nejdříve vypnout všechny počítače. Nemocnice potom postupně zapojovala jednotlivé systémy zpět do provozu.

O měsíc později zaznamenalo hackerské útoky několik různých nemocnic. Napadena byla například ostravská nemocnice, Fakultní nemocnice Olomouc, nemocnice Pardubického kraje nebo Karlovarská krajská nemocnice. Všechny tyto útoky byly úspěšně odraženy.

V březnu 2021 byly napadeny tři soukromé polikliniky v centru Prahy. Konkrétně polikliniky Legerově, Myslíkově a Kartouzské ulici, kterým nefungovala elektronická pošta (e-mail) ani systém pro objednávání pacientů. Nefunkční byl také systém pro správu laboratoří, k jejichž databázím lékaři ztratili přístup.[5]

---

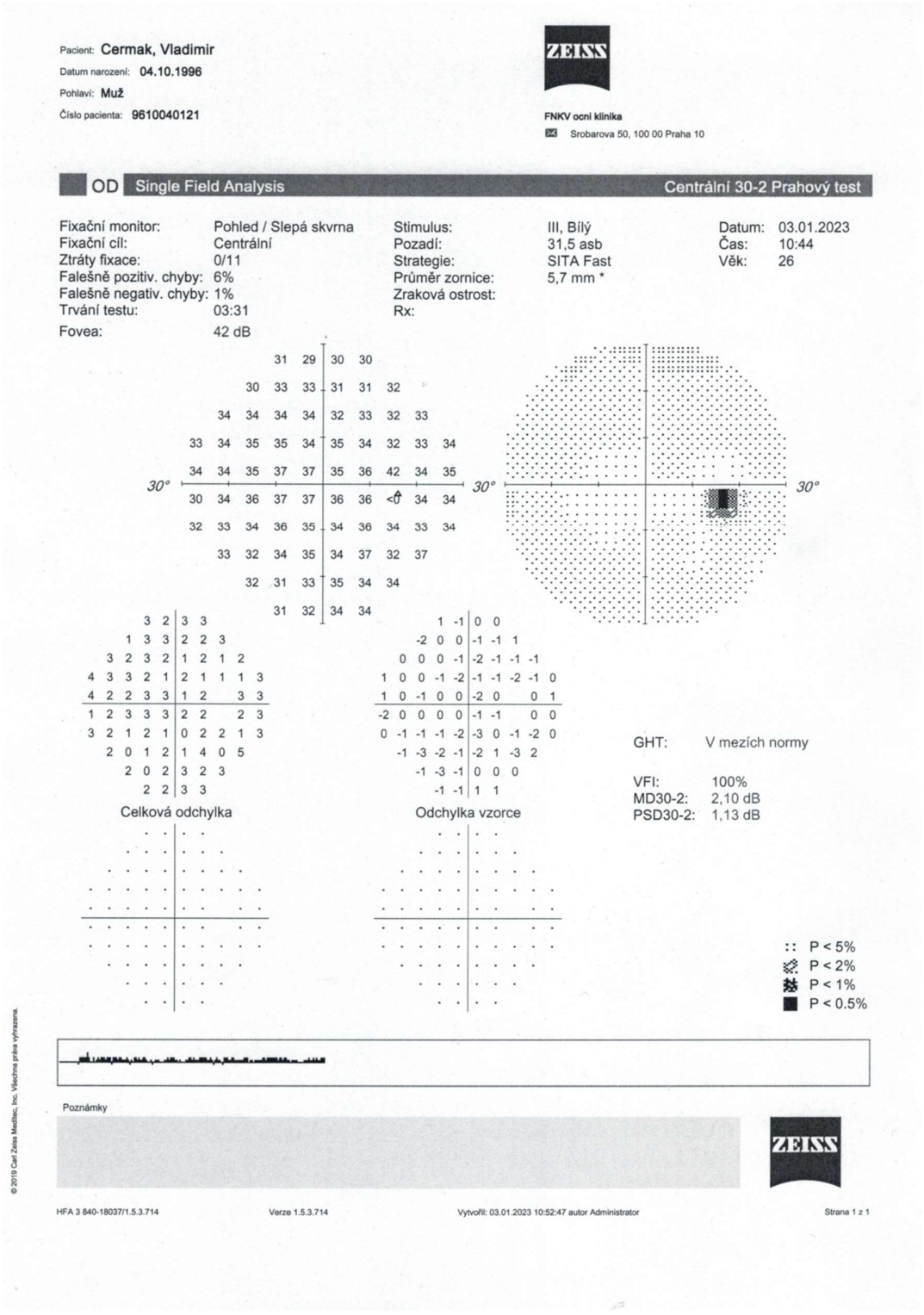
[4] *Kyberútok na nemocnici v Benešově* [online]. Praha: Čerský rozhlas, 2020 [cit. 2023-08-01]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/kyberutok-kyberneticky-utok-nemocnice-v-benesove-skoda-pachatel-hacker_2008180912_ako

[5] *Hackerské útoky na nemocnice*[online]. Praha: ČTK, 2022 [cit. 2023-08-02]. Dostupné z: https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-hackerskym-utokum-celily-v-cesku-nemocnice-narodni-knihovna-ci-volebni-web-40394428

2.3 Oftalmologická klinika FNKV

Během svých studií na vysoké škole v bakalářském oboru Biomedicínská informatika jsem brigádně pracoval na Oftalmologické klinice ve Fakultní nemocnici Královské Vinohrady. Obsluhoval jsem zde přístroje, které provádí různá měření očí. Mezi měřící přístroje, se kterými jsem pracoval, patří například perimetr. Perimetr je přístroj, jehož pomocí je možno změřit (zmapovat) zorné pole oka, a také zmapovat přibližnou polohu černé skvrny v oku. Princip měření spočívá v tom, že oko je po celou dobu měření fixováno na bod umístěný ve středu plochy, na kterou pacient má možnost vidět. V okolním prostoru na náhodných místech s krátkým časovým odstupem blikají body o různé intenzitě jasu. Pokud pacient bod zaznamená, stiskne tlačítko. Perimetr uloží informaci o tom, že pacient v této poloze bod viděl, a také, jaká byla intenzita jasu tohoto bodu. Přístroj později zkusí umístit na stejné místo bod s nižší intenzitou jasu. Tímto způsobem se testuje, jak silné, respektive slabé impulzy na daném místě je oko ještě schopno zaznamenat. V principu jde o velmi prosté vyšetření s jasným postupem měření. Nevýhoda takového měření spočívá v jeho délce – typicky zabere řádově několik minut. Pro pacienta je náročné udržet po takovou dobu pozornost. Řada pacientů (především těch starších) má problémy fixovat svůj pohled stále na jeden bod nacházející se ve středu. Pokud pacient takzvaně „švindluje“ a nefixuje pohled na středový bod, výsledek měření je potom nerelevantní, a celé měření bylo zbytečné (neposkytne nám pravdivé výsledky o zorném poli oka).

Doba měření se však může lišit u každého pacienta. Perimetr na začátku každého měření nechává body na náhodných místech „blikat“ relativně rychle a zkouší, zda se pacient „chytá“, a zda je schopen „problikávající“ body zachytit, i při této zvýšené rychlosti. Mladší pacienti jsou většinou schopni větší rychlost „problikávání“ bodů zvládnout. Celý zbytek měření pak probíhá v podobném rytmu, rychlost je zvýšená, a měření tím pádem trvá kratší dobu. Může být hotovo v rozmezí pěti až deseti minut. Pokud však perimetr nezaznamená žádnou odpověď od pacienta na „problikávající“ body, vyhodnotí situaci tak, že pacient danou rychlost nestíhá. A na základě této skutečnosti přístroj zvýší časový interval mezi jednotlivými „bliknutími“ bodů. U starších a „pomalejších“ pacientů se doba měření přibližuje k patnácti, ve výjimečných případech až ke dvaceti minutám.



Obrázek 1 – Výsledek perimetrického vyšetření

Takto vypadá výsledek vyšetření zorného pole mého pravého oka na perimetru. Zorné pole je zde znázorněno jak graficky, tak i číselně. U číselných výsledků platí tato vlastnost: čím větší číslo, tím lépe pacient v dané oblasti vidí. Čísla blížící se k nule (a zároveň nula samotná) znamenají, že pacient na daném místě nebyl schopen zaznamenat ani bod o velké intenzitě jasu. Na těchto místech perimetr zkoušel dávat velmi jasné body, pacient je však, navzdory velikému jasu bodů, ani tak neviděl. Větší číselná hodnota na konkrétním místě znamená, že pacient zaznamenal i méně jasné a méně výrazné body. V případě grafického znázornění je schopnost pacienta zaznamenat bod v dané oblasti reprezentována stupni šedi. V oblastech, kde je souvislá černá výplň, oko vidí velmi špatně anebo vůbec. Z grafu na pravé straně je jasně patrná přítomnost slepé skvrny v oku (černá oblast v pravé části grafu). V tomto místě se nachází vyústění očního nervu do oční bulvy. Nenachází se zde tedy žádné fotocitlivé buňky (tyčinky a čípky). Našedivělé oblasti znamenají, že schopnost zraku je v těchto oblastech omezená. A čím je oblast světlejší, tím lepší zde má pacient zrak, a snáze zaznamenává „problikávající“ body.

Dalším přístrojem, se kterým jsem se často setkával, a prováděl na něm měření pacientů, byl takzvaný tonometr. Na tomto přístroji byl vždy změřen každý nově příchozí, ale i stávající pacient, který přišel po dlouhé době na kontrolu. Tonometr umí provádět přibližné měření dioptrií, přesné měření poté provádí oční lékař. Především ale také bezkontaktně měří nitrooční tlak. Přístroj se zacílí na střed oka a vypustí (foukne) do něj soustředěný proud vzduchu. Vzduch svým tlakem „promáčkne“ rohovku oka. A na základě míry „promáčknutí“ rohovky přístroj určí hodnotu nitroočního tlaku. Tento způsob měření, kdy je do oka vypuštěn soustředěný proud vzduchu, může být pro pacienta nepříjemný. Za žádných okolností není příjemné, pokud nám na oka proudí vzduch o vyšších rychlostech. Pacienta je třeba předem informovat a principu měření. V opačném případě se může stát, že pacient sebou v průběhu měření trhne, jelikož nečekal, že se něco podobného stane.

2.3.1 Fyzické zabezpečení přístrojů na FNKV

Oba dva tyto přístroje, jak perimetr tak i tonometr, jsou velmi úzce specializované měřící přístroje, a jsou zároveň drahé. U takovýchto přístrojů je nutné, aby byly adekvátně zabezpečeny. Je třeba zajistit fyzickou bezpečnost, aby nedošlo k poškození na přístrojích a tím k velké finanční škodě. Na Oftalmologické klinice ve FNKV se perimetr nachází ve zvláštní, menší místnosti. Za okny této místnosti jsou mříže, perimetr je tedy chráněn před vniknutím skrze okno. Avšak dveře této místnosti jsou z lehkého, dřevěného materiálu a mají obyčejný zámek. Nejsou tedy nijak zvlášť bezpečné. Bezpečnější variantou by v tomto případě byly silnější, pevnější a odolnější bezpečnostní dveře. Tonometrů se na této klinice nachází mnoho, a prakticky v každé oční ordinaci je umístěn jeden, aby jej měl k dispozici ordinující oční lékař. Tonometry tedy nejsou dostatečně fyzicky zabezpečeny, avšak to je dáno tím, že jsou velmi využívané, a přístup k nim musí být snadný a rychlý, aby měření pacientů probíhalo plynule a efektivně.

2.3.2 Webové stránky FNKV

Když jsem pracoval na Oftalmologické klinice, tak mne vedoucí biomedicínského oddělení, pan Ing. Patrik Pluhovský, MBA též požádal, abych navrhl změnu ve vzhledu webové stránky kliniky. Požadavkem bylo vzít současný obsah webové stránky a pouze podat návrh změny v designu, aby se zlepšil vzhled stránky. Tento návrh by potom pan vedoucí předložil IT oddělení nemocnice, které by změny už samo implementovalo. Důležité pro webové stránky zdravotnických zařízení je, aby byly přehledné, dobře čitelné, a bylo možné na nich snadno a rychle dohledat informace. Není za potřebí, aby obsahovaly mnoho designových prvků, různé druhy barev atp. Hlavní je především to, aby text byl snadno čitelný například i pro starší pacienty a návštěvníky webových stránek. Ideální je co největší kontrast mezi textem a pozadím (typicky použití černého textu s bílým pozadím). Je to sice obyčejné, ale snadné na čtení. A právě to je velmi důležité u webových stránek zdravotnických zařízení.

Webové stránky Fakultní nemocnice Královské Vinohrady jsou dobře strukturované. Na úvodní stránce se na horní straně nachází hlavní menu, kde jsou tři hlavní sekce: 1. Pro pacienty, 2. Zdravotnická pracoviště, 3. Odborná veřejnost.[6] Návštěvník se tak jednoduše jedním kliknutím může dostat na informace pro pacienty (kontakt, adresa, možnosti jak se do nemocnice dostat), nebo na informace o jednotlivých klinikách nemocnice a kontakty přímo na konkrétní kliniku. U hlavního menu je nevýhoda ve volbě barvy textu a různých barev pozadí. Text je zde bílou barvou a pozadí buď modré, zelené nebo růžové, což pro staršího pacienta může být komplikované na čtení. Co se týče samotného obsahu stránky, tak ten už je psán černým písmem, které je na čistém, bílém pozadí. Text je tedy správně kontrastní a mnohem lépe čitelný. Ideální by však bylo použít větší velikost písma.

[6] *Fakultní nemocnice Královské Vinohrady* [online]. Praha: FNKV, 2023 [cit. 2023-08-02]. Dostupné z: https://www.fnkv.cz/

3 Cíle práce

V rámci FBMI vznikly jako projekt studentů této fakulty webové stránky http://proambulance.cz/.[7] Tyto stránky mají sloužit, jak už jejich název napovídá, především malým ambulancím a jejich zaměstnancům. Stejně tak ale mohou sloužit i zaměstnancům v jiných profesích. Hlavním tématem, kterému se stránky věnují, je nařízení GDPR. Mezi slabiny běžného občana patří (ne)schopnost vyznat se v legislativních textech. Nařízení jsou psána složitou formou, aby byla „neprůstřelná“, a obsahovala kompletní vymezení veškerých souvisejících pojmů. Proto návštěvníci na stránkách proambulance.cz naleznou veškeré informace týkající se této problematiky v přehledné podobě. Jednodušeji vše pochopí a budou nařízením více rozumět. GDPR je hlavní náplní těchto webových stránek. Kromě toho se zde také nachází jednoduché rady a zásady například pro tvorbu hesel, kontrolu smluv a další. Záměrem je nabídku témat do budoucna postupně rozšiřovat, aby se ke zdravotníkům, ale i zaměstnancům jiných oborů, dostaly důležité informace na jednom místě, a z oblastí, které s jejich zaměstnáním souvisí. Ke stávajícím tématům, aktuálně dostupným na stránkách proambulance.cz, mají být přidány i tyto materiály, týkající se bezpečnosti IT pro zdravotníky. Cílem této bakalářské práce je pokud možno co nejvíce přispět v oblasti vzdělávání zdravotníků. Materiály mají sloužit zdravotníkům a zdravotnickému personálu v oblastech, které za současného stavu nejsou dostatečně důkladně rozpracovány. Případně alespoň nejsou v podobě vhodné pro zaměstnance pohybující se ve zdravotnictví. Rozsah, obsah i forma práce jsou uzpůsobeny tak, aby byly vhodné pro zdravotníky a běžné uživatele.

[7] *Projekt studentů FBMI proAmbulance.* [online]. Kladno: FBMI, 2022 [cit. 2022-05-09]. Dostupné z: http://proambulance.cz/

4 Fyzická bezpečnost malé ordinace

Fyzická bezpečnost malých ordinací je první ze čtyř hlavních témat v této práci. Ordinace všeobecně nepatří mezi pracoviště s vysokým rizikem nebezpečí, nicméně zde rizika i přesto existují. Může jít o relativně vysoká rizika.

4.1 Fyzická bezpečnost informačních systémů

Fyzická bezpečnost těchto systémů má obecně za cíl předejít rizikům a nebezpečím, která hrozí fyzicky z okolí. Převážně se jedná o hrozbu lidského, výjimečně i o hrozbu abiotického charakteru. Jde o fyzickou ochranu počítačů, přístrojů a různých zařízení. Pokud nám jde o ochranu před neoprávněným přístupem, pak fyzická bezpečnost je systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k systému. Případně tento neoprávněný přístup, nebo pokus o něj, zaznamenat. Zajištění fyzické bezpečnosti je velmi důležité a měla by se tomu bezpochyby věnovat náležitá pozornost, stejně jako se věnuje pozornost kybernetické bezpečnosti. V současné době je oblast kybernetické bezpečnosti spíše tou více důležitější. A kybernetická bezpečnost bývá upřednostňována na úkor té fyzické.

4.2 Fyzická bezpečnost v ordinaci

Nároky na fyzickou bezpečnost informačních systémů v ordinacích jsou do značné míry shodné s požadavky na fyzickou bezpečnost informačních systémů i v jiných prostředích. Zajistit fyzickou bezpečnost je i pro ordinaci velmi důležité. Existují v zásadě dva hlavní způsoby fyzického zabezpečení. A těmi jsou:

1. Mechanické zabezpečení
2. Elektronické zabezpečení

Podle České státní normy ČSN P CEN/TS 14383-3 je definováno 5 úrovní zabezpečení pro jednotlivé úrovně rizika:

Úroveň zabezpečení	Úroveň rizika	Preventivní opatření
1	Velmi nízké	Jednoduché mechanické zabezpečení
2	Nízké	Zvýšené mechanické zabezpečení
3	Střední	Zvýšené mechanické zabezpečení a minimální elektronické zabezpečení
4	Vysoké	Zvýšené mechanické zabezpečení a střední elektronické zabezpečení
5	Velmi vysoké	Zvýšené mechanické zabezpečení a vysoké elektronické zabezpečení

Tab. 1. Úroveň rizika a stupeň zabezpečení[8]

4.2.1 Zabezpečení mechanické

Ne každou situaci lze vyřešit elektronickými alarmy a podobnými zabezpečovacími zařízeními. V mnoha případech je nutno využít mechanického zabezpečení nebo uzamykacích systémů. Mechanické zabezpečení je základní složkou ochrany. V současné době nároky na bezpečnost stále rostou. Jedná se o dlouholetý trend projevující se v oblasti střežení jak soukromých prostor a stejně tak firemních či státních. Soukromníci, firmy i stát dnes investují nemalé peníze, aby zabezpečili své objekty. Dalším velmi důležitým důvodem k realizaci kvalitního zabezpečení je bezpochyby ochrana majetku. Mezi prvky mechanického zabezpečení patří všechny prostředky, které mají za cíl případnému útočníkovi znemožnit, nebo alespoň znesnadnit přístup. Tyto prvky poskytují ochranu svými mechanickými vlastnostmi. Především pevností a odolností vůči fyzickým vlivům. Jejich základní úlohou je vytvořit překážku mezi útočníkem a tím, co je třeba zabezpečit. Cílem je zabránit násilnému proniknutí nepovolané osoby, což by mohlo mít za následek znehodnocení, případně krádež zařízení, techniky a informačních systémů.

[8] *ČSN P CEN/TS 14383-3*. 12/2006. Praha: Český normalizační institut, 2006.

Patří sem všechny mechanické (kovové i nekovové) prvky, jako například:

- Zámky
- Bezpečnostní dveře
- Mříže
- Rolety
- Bezpečnostní folie
- Tvrzená bezpečnostní skla
- Trezory a bezpečnostní skříně

Prvky mechanického zabezpečení jsou nepostradatelnou součástí v oblasti fyzické bezpečnosti. Skutečnost, že stále dochází ke zločinům a pokusům o krádeže, má za následek neustálý vývoj v oblasti zabezpečení. Moderní technologie využívají nové, odolnější materiály a také vyspělejší návrhy konstrukčních řešení. To vše má za následek delší dobu, kterou potřebuje případný útočník k překonání prvků mechanického zabezpečení. Každý prvek mechanického zabezpečení musí být dostatečně spolehlivý. Tím se zvyšuje míra bezpečnosti, kterou nám daný prvek poskytuje. Každé mechanické zabezpečení je překonatelné. Důležitá je však míra vynaložené energie, času a prostředků potřebných k překonání tohoto zabezpečení. Při kombinaci zabezpečení mechanického a elektronického vzniká nová úroveň zabezpečovacích možností.

4.2.2 Zabezpečení elektronické

Mechanické zabezpečovací prvky mají výhodu ve své odolnosti. Avšak nejsou schopny zaznamenat případný pokus o neoprávněný přístup, ani nás o něm informovat. Naopak prvky elektronického zabezpečení touto vlastností disponují, je to jejich hlavní výhoda, a zároveň také důvod, proč jsou využívány. Mezi prvky elektronického zabezpečení patří především:

- Kamerové systémy
- Detektory pohybu
- Alarmy

Kamerové systémy mají za úkol snímat požadované prostory. Při jejich instalaci je potřeba respektovat nařízení GDPR. Nesmí být narušeno soukromí jiných osob. Všechny osoby, kterým by kamerový systém teoreticky zasahoval do jejich soukromí, musí k nahrávání dát nejprve svůj souhlas. Kvůli tomuto mohou vzniknout potíže a prodlevy při zavádění kamerových systémů.

Existují 4 základní typy kamerových systémů:

1. Bezdrátové
2. Digitální IP kamery
3. Autonomní
4. Analogové[9]

Základním typem kamerových systémů jsou analogové. Jejich výhodou je nízká pořizovací cena, avšak mají nízkou kvalitu záznamu. Autonomní kamerový systém se skládá pouze z jedné kamery. Instalace tohoto typu kamer je rychlá a jednoduchá. Dnes nejvíce rozšířené jsou IP kamerové systémy. Jsou dražší, ale mají spousty výhod, jako je například pořizování záznamu ve vyšší kvalitě. Nejlepším způsobem, jak využívat kamerové systémy, je kombinovat jednotlivé typy na základě toho, kde konkrétně je chceme využívat. Pokud jde o kameru využívanou venku, rozhodně by měla být odolná vůči vodě a větru. Důležitá funkce je také schopnost nočního vidění a možnost snímání prostoru za nedostatku světla. Další z podstatných funkcí je též například detekce pohybu, kdy kamera provádí záznam jen tehdy, zaznamená-li pohyb. Šetří se tak místo v úložišti a tím je možno nahrávat delší časový úsek.

4.2.3 Elektrická zařízení

Zdravotnický personál musí pracovat bezpečně s elektrickými zařízeními a vědět, jak tato zařízení správně používat. Zásah elektrickým proudem představuje velké riziko závažného úrazu v ordinaci. Pokud se s elektrickými zařízeními pracuje neodborně, může dojít k závažným následkům. Pro zdravotníky je důležité nikdy se nesnažit opravovat elektrická zařízení, protože k tomu nemají dostatečné odborné znalosti a koneckonců ani povolení. Nesmí se odstraňovat kryty zařízení a dotýkat se částí přístrojů, které mohou být pod elektrickým proudem. V ordinacích se nachází mnoho elektrických zařízení, proto je povinností každého dodržovat požadavky týkající se používání a revizí těchto zařízení. Pouze takto lze předcházet pracovním úrazům efektivně. Elektrická zařízení mají za účel pomáhat, zjednodušovat práci a dokážou být velkými pomocníky. Mohou být také ovšem velmi nebezpečné, a to především při práci s nimi. Pokud chceme být při používání elektrických zařízení v bezpečí, po celou dobu musíme být ve střehu. Únava stejně jako například nevolnost nebo nemoc mohou též způsobit riziko. Patří sem i kterýkoliv jiný příznak zhoršeného vědomí. Pro udržení bezpečnosti práce s elektrickými zařízeními je důležité udržet soustředěnost.

[9] *Rozdělení kamerových systémů* [online]. Příbram: Security Agencies, 2022 [cit. 2022-04-04]. Dostupné z: https://www.securityagencies.cz/clanek/co-to-jsou-kamerove-systemy-cctv-proc-je-mame-chtit-a-jak-se-rozdeluji

Všechny kontakty, spoje elektrických obvodů a také všechny součástky mohou být pod velmi silným elektrickým napětím. Lidé si často myslí, že v řadě případů na nějakém místě žádná elektřina neproudí. Nikdy se ale nesmíme dotýkat žádného vedení, i pokud si myslíme, že v něm neproudí elektrický proud. Zdravotníci většinou znají elektrická zařízení, která se vyskytují v ordinacích a se kterými pracují. Větší riziko nastává, pokud pracují na nových a dosud neznámých zařízeních. Při práci na nových elektrických zařízeních je potřeba vyhnout se činnostem, pro které chybí dostatečná kvalifikace.

4.3 Kontrolní otázky k tématu fyzické bezpečnosti

1) Hlavní způsoby realizace fyzického zabezpečení?
2) Rozdělení zabezpečení na základě velikosti rizika podle ČSN?
3) Co patří mezi prvky mechanického zabezpečení?
4) Co patří mezi prvky elektrického zabezpečení?
5) Jaké jsou typy kamerových systémů?

5 Autentizace

Dalším z hlavních témat je autentizace. Což je v zásadě proces označující ověření identity uživatele. Autentizace patří mezi bezpečnostní opatření a zajišťuje ochranu před falešnou identitou. Objevuje se ve všech oblastech, kde je třeba ověřovat identitu člověka, konkrétního software nebo datové zprávy. Využívá se tedy například při přihlašování na internetové stránky, služby, sociální sítě a přihlašování do informačních systémů. Všechny informační systémy musí znát identitu uživatele, který do nich přistupuje. Důležitá je také jistota, nebo alespoň dostatečně vysoká úroveň jistoty, že tento konkrétní uživatel je skutečně tím, za koho se vydává. Cílem je snaha o zabezpečení dat a ochrana proti neoprávněnému přístupu, aby se nikdo nedostal k našim datům. V informatice se toto ověření nejčastěji provádí zadáním tzv. loginu (přihlašovacího jména), a hesla. Přístupová hesla se dále mohou dělit na jednorázová, statická a dynamická. Statická hesla jsou ta základní, jednou je nastavíme a přihlašujeme se pomocí nich do systému. Hesla dynamická se naopak snaží odstranit nedostatky, které statická hesla mohou mít. Po každém našem přihlášení se heslo pozmění. Je tedy složitější pro útočníka heslo vypozorovat a časem prolomit. Jednorázová hesla, jak už jejich název napovídá, můžeme použít jen pro jedno přihlášení. Tento typ hesel se používá spíše do málo zabezpečených počítačů. Klasický přístup k zabezpečení, kdy ve většině případů stačilo právě jméno a heslo, přestává v současné době stačit. V řadě systémů je třeba vyšší úrovně zabezpečení. S příchodem například bankovních aplikací se zavedlo používání certifikátu, sloužícího jako autentizační nástroj. Těmto novým úrovním zabezpečení se říká dvou a více faktorová autentizace.

5.1 Dvou faktorová autentizace

U dvou faktorové autentizace musíme kromě přihlašovacího jména a hesla znát také další „faktor“. Příkladem může být například kód z SMS zprávy zaslané na náš osobní mobilní telefon, nebo kód z naší e-mailové schránky. Tento způsob autentizace přináší vyšší úroveň zabezpečení, než při použití pouze přihlašovacího jména a hesla. Pokud by se útočník chtěl neoprávněně přihlásit do systému pod našimi přístupovými údaji, musel by kromě znalosti našich přihlašovacích údajů mít přístup i k našemu mobilnímu telefonu, nebo e-mailové schránce. Tento způsob se v současné době používá například v online bankovnictví. Některé banky vydávají vlastní mobilní aplikace, které slouží právě k tomuto způsobu autentizace. Pokud si zařizujeme online bankovnictví, na pobočce banky si podle pokynů nainstalujeme mobilní aplikaci. Při pokusu o přihlášení do online bankovnictví nám aplikace v mobilním telefonu zašle upozornění a vyzve nás, abychom přihlášení potvrdili. Dnešní chytré telefony používají ve většině případů k ověření identity uživatele snímek otisku prstů, nebo také ověření pomocí skenování obličeje.

S

5.2 Nejznámější typy dvou faktorové autentizace

5.2.1 Hardwarový klíč

Jde o fyzické zařízení, které se při autentizaci připojuje k počítači. Může jít také o malé zařízení zobrazující heslo, které uživatel opíše do počítače. Tento způsob má tu nevýhodu, že uživatel musí mít konkrétní hardwarový klíč stále u sebe. Uživatel tedy musí mít na paměti, že pokud chce provést autentizaci, nesmí zapomenout brát si klíč sebou. Většina klíčů se připojuje pomocí portu USB. Jsou však i takové, které umí technologii bluetooth. Mohou být tedy použity na telefonech či tabletech. Nevýhodou může být také relativně vysoká pořizovací cena těchto hardwarových klíčů. Z tohoto důvodu se tento typ klíčů vyskytuje především ve větších firmách a korporacích.

5.2.2 Softwarový klíč

V tomto případě u sebe nemusíme fyzicky mít nějaký klíč. Softwarovým klíčem se myslí speciální aplikace, kterou si nainstalujeme do našeho chytrého mobilního telefonu. Aplikace opakovaně po určitém časovém intervalu (většinou 30 sekund) vygeneruje číselný bezpečnostní kód, který během přihlašování vyplníme a tím ověříme naší identitu. Aplikace pro tento způsob dvou faktorové autentizace vyvíjí společnosti jako například Google nebo Microsoft.

5.2.3 Kód ze zprávy SMS

Tento způsob autentizace je pro uživatele v zásadě jednoduchý a nenáročný. Není třeba pořizovat hardwarový klíč nebo disponovat chytrým telefonem a do něj instalovat specializovanou aplikaci. Stačí vlastnit kterýkoliv mobilní telefon, třeba i klasický „tlačítkový“. Při pokusu o autentizaci nám do našeho mobilního telefonu přijde SMS zpráva s bezpečnostním kódem, který vložíme do systému.

5.2.4 Využití biometrických údajů

Biometrické údaje jsou fyzické znaky a charakteristiky osob. Pro každého člověka jsou unikátní. Můžeme tedy jejich prostřednictvím prokazovat svoji identitu. Snímání těchto biometrických údajů se využívá k ověření pravosti a totožnosti jejich držitele. Mezi biometrické údaje využívané k autentizaci patří:

- Otisky prstů
- Skenování duhovky či sítnice v oku
- Skenování obličeje a rysů ve tváři

- Tón hlasu případně jeho rytmus

Z těchto způsobů se nejvíce využívá autentizace pomocí otisku prstů. V dnešní době většina chytrých telefonů již disponuje snímačem otisku prstů. Některé dražší modely současných telefonů umí provádět detailní, přesné a bezpečné skenování obličeje.

5.2.5 Nevýhody dvou faktorové autentizace

Dvou faktorová autentizace nabízí vyšší úroveň zabezpečení, nevýhod tedy není mnoho. Jelikož se ale jedná o nějaký proces navíc, který musí uživatel podniknout, znamená to, že nad autentizací stráví více času, než by bylo normálně za potřebí. Hlavní nevýhodou je tedy časová náročnost, protože tento způsob uživatele zdržuje. Kromě vyplnění přihlašovacího jména a hesla, je třeba navíc provést dvou faktorovou autentizaci. Uživatelé většinou nemají v oblibě, že musí tyto kroky provádět. Avšak tento způsob autentizace přináší zvýšenou míru bezpečnosti.

5.3 Autentizace pomocí certifikátu

Certifikát je veřejný elektronický dokument, který spojuje fyzickou osobu, instituci nebo server s veřejným klíčem. Veřejný klíč je řetězec znaků dané délky, určený pro použití podle účelu, ke kterému byl vydán certifikát. Kromě veřejného klíče existuje také soukromý klíč. Tímto klíčem disponuje pouze držitel konkrétního certifikátu. Certifikáty vydávají takzvané certifikační autority. Ty také ručí za každý certifikát, který vydávají. Při vydání certifikátu je certifikát následně stvrzen digitálním podpisem příslušné certifikační autority, která ho vydala. Princip autentizace pomocí certifikátu je založen na tom, že soukromý klíč má pouze majitel certifikátu. Pokud by se útočníkovi podařilo získat soukromý klíč, mohl by se falešně vydávat za majitele certifikátu a podepisovat za něj dokumenty.

5.4 Autorizace

Autorizace je proces, který zpravidla nastává po úspěšné autentizaci a navazuje na ni. Poté, co se úspěšně přihlásíme do systému (provedeme autentizaci), jsme tzv. „autorizováni“ a máme přidělena nějaká oprávnění. Autorizace ověřuje, jestli uživatel má oprávnění provádět určitou činnost uvnitř systému. Nejprve tedy autentizací ověřujeme, že uživatel je skutečně tím, za koho se vydává. A následně autorizace kontroluje, zda má tento uživatel oprávnění vykonávat konkrétní akce.

5.5 Kontrolní otázky k tématu autentizace

1) Co je to autentizace? Jaký proces označuje?
2) Jaké jsou typy dvou faktorové autentizace?
3) Výhody/nevýhody dvou faktorové autentizace?
4) Které biometrické údaje se využívají pro účely autentizace?
5) Co je to certifikát? K čemu se využívá?

6 Zálohování

Důležitost zálohování dat se objevuje ve všech oborech. Zálohou se rozumí vytvoření kopie našich dat, kterou následně uložíme na jiném místě. Kdyby došlo ke ztrátě dat v důsledku poškození nebo z kteréhokoliv jiného důvodu, můžeme tuto zálohu využít. Ztráta dat je nepříjemná v jakékoliv situaci. Můžeme přijít o veškerá data, dokumenty nebo fotografie, které jsme ukládali někdy i v průběhu několika let. Mezi nejčastější příčiny, kvůli kterým dochází ke ztrátě dat, patří:

1. Lidský faktor
    - Nedbalost, omyl, chyba obsluhy
    - Virus
    - Úmyslná krádež
2. Technický faktor
    - Chyba úložiště nebo programová chyba
    - Výpadek napájení
    - Opotřebení
3. Přírodní pohromy
    - Požár
    - Povodeň
    - Zásah blesku
    - Zemětřesení

Ze všech ostatních příčin, lidský faktor představuje zdaleka nejčastější důvod ztráty dat. 85% případů, kdy dojde ke ztrátě dat, je způsobeno jedním z lidských faktorů.[10]

Na vině je často neopatrné zacházení ze strany uživatele a provádění různých úkonů bez rozvahy. Uživatel často pracuje ve spěchu, snaží se šetřit časem. A tak dojde k nechtěnému smazání často i důležitých dat. Ztráta dat však může být v mnoha případech také úmyslná, kdy se o to postará například virus nebo jiný uživatel, který data úmyslně smaže. Důležité je mít v datech pořádek, vědět, jaká data kde ukládáme a se stejnou vážností přistupovat i k jejich zálohování. V některých případech může dojít k poškození paměťového média, na kterém máme data uložena. Děje se tak, pokud s nimi neopatrně zacházíme. U klasického pevného disku HDD je riziko ztráty dat při otřesu nebo jiném pohybu, ke kterému dochází, je-li disk právě v provozu. Novější SSD disky na toto již náchylné nejsou a nedochází tak k jejich poškození.

[10] BRECHLEROVÁ, Dagmar. *FYZICKÁ BEZPEČNOST INFORMAČNÍCH SYSTÉMŮ, 2007*. Praha. KIT PEF ČZU.

Důvodem ztráty dat může být i stáří a jím způsobené opotřebení součástí. Čím starší elektronická zařízení používáme, tím vyšší je s postupem času také riziko, že dojde ke ztrátě dat.

Proces zálohování nám tedy slouží k tomu, abychom minimalizovali ztrátu dat. Zálohovat je třeba vše důležité, veškerá data, která by už nebylo možno opětovně vytvořit. V takovém případě by jejich ztráta představovala velkou komplikaci. Naopak nedůležitá data, která nejsou užitečná, není nutno zálohovat. Může jít o vadná data, nebo nepotřebné soubory. Zbytečně se tak zabírá místo, které bychom mohli využít pro zálohování jiných, pro nás více důležitých dat. Aby záloha plnila svůj účel, je potřeba ji ukládat na odlišné datové úložiště než to, na kterém pracujeme, a na kterém máme originální data. Úložiště určená pro účely zálohování by měla sloužit výhradně k tomu, aby se na ně ukládaly pouze zálohy. Pokud bychom záložní médium využívali k ostatním účelům, pracovali na něm, přenášeli pomocí něho data mezi další zařízeními, nebo na něj instalovali nové programy, můžeme se na tomto úložišti, původně určenému k zálohování, dopustit chyby. A to by mohlo mít za následek ztrátu dat. Dat, která měla sloužit jako naše záloha.

6.1 Možnosti zálohování

Při rozhodování, kam budeme data zálohovat, jaké pro to použijeme technologie a jaká média, musíme vzít v úvahu několik faktorů. Podle toho, jaké množství dat chceme zálohovat, záleží i na kapacitě média pro zálohování. U zálohování dokumentů a malých pracovních souborů probíhá zálohování velmi rychle, svižně a není zapotřebí mít pro zálohu úložiště o velké kapacitě. Paradoxem je, že většinou méně důležitá data zabírají více místa. Jako například fotky, videa, filmy nebo hry mají velikost v řádech mnohdy jednotek, někdy i desítek GB. Oproti tomu textové dokumenty, které velmi často obsahují důležité pracovní texty a informace, mají „zanedbatelnou“ velikost. Většinou se jedná o desítky až stovky MB. Zálohování v tak malém měřítku není v dnešní době problém. Před lety byla jiná situace. Počítače se každým rokem zrychlují a zvyšuje se i objem dat, který jsou schopny za jednotku času zpracovat. Zároveň se zvyšuje také kapacita paměťových médií. Možností, kam data zálohovat, existuje v současné době mnoho.

6.1.1 CD/DVD

Optická média, kam patří například CD, DVD, nebo také Blu-ray. Jedná se o klasický a starší způsob, jak data ukládat a zálohovat. Zároveň jde o levné a velmi dostupné řešení otázky zálohování a ochrany dat. Abychom mohli vytvářet zálohu na tato média, musíme mít k dispozici vypalovací mechaniku. A pomocí ní na dané médium můžeme data zapisovat. Existují různé druhy médií podle toho, jestli na ně lze zapisovat opakovaně, anebo jen jednorázově. Přepisovatelná média ale mají kratší životnost. Pokud uložíme data na jednorázová média, není možné je v budoucnu přepsat novými daty, záloha však na tomto médiu vydrží déle.

S optickými médii je třeba zacházet šetrně a dávat pozor, aby se nepoškodila. Nevýhodou těchto médií je jejich omezená kapacita, v dnešní době už často a stále více nedostačující.

6.1.2 Externí disky

Zálohování na externí disky nabízí výrazně lepší možnosti a vlastnosti, než média optická. Tyto disky mají výrazně větší kapacitu a jsou proto vhodné pro zálohování velkých objemů dat. Výhodou je také jejich rychlost, která při zálohování hraje důležitou roli. Máme-li potřebu zálohování často a zálohujeme velké objemy dat, potom díky vyšším rychlostem proces zálohování nezabírá tolik času. Dva nejpoužívanější druhy externích disků jsou:

- HDD (Hard Disk Drive)
    - Elektromechanické médium pro ukládání a čtení adresovatelných dat o velké kapacitě. HDD mají pomalejší přístup k datům nežli SSD. Používají se v osobních počítačích jako hlavní paměť. První takovýto pevný disk byl vyroben roku 1956 firmou IBM. Tento typ disku se velmi rozšířil díky velké kapacitě. Důležitá vlastnost také je, že k udržení dat nevyžaduje trvalý přísun napájení. Disk je tvořen kovovými deskami, kterým se říká „plotny“, na kterých se nachází magnetická vrstva. Práci s daty, čtení a zápis, zajišťují čtecí a zápisové hlavy. Jelikož se jedná o disk kulatého tvaru, data jsou na něm organizována do kružnic. Pevný disk obsahuje mechanické části, které se pohybují. Je tedy náchylný k poruchám a v souvislosti s tím také ke ztrátě dat. Obzvlášť, pokud je disk v provozu, musí se s ním zacházet velmi opatrně, a vyvarovat se pohybům, či nárazům. U stolních počítačů je toto riziko poměrně nízké. Počítače za provozu povětšinou jen stojí na jednom místě. Větší riziko však nastává při použití pevných disků v notebooku. Pokud notebook přenášíme, případně s ním jakýmkoliv způsobem manipulujeme, když je zapnutý, hrozí nevratné poškození plotének pevného disku a s tím související ztráta dat.[11]
- SSD (Solid State Drive)
    - Polovodičové médium, dražší alternativa pevného disku. Na rozdíl od HDD neobsahuje mechanické ani pohyblivé části. Tyto disky používají flash paměť pro uložení dat. Je to soustava flash pamětí,

[11] *Rozbor HDD* [online]. Vše o HW, 2006 [cit. 2022-04-11]. Dostupné z: http://vseohw.net/clanky/recenze/rozbor-hdd

které jsou navzájem energeticky nezávislé. Jejich velkou výhodou, oproti pevným diskům, je jejich zvýšená odolnost. Jelikož nemají žádné pohyblivé mechanické součásti, nejsou náchylné k poškození při vibracích, nebo nárazech. SSD umožňuje také vyšší rychlosti jak čtení, tak i zápisu dat. Oproti pevným diskům jsou lehčí a mají menší rozměry díky jejich konstrukci. Tím se stávají praktičtějšími pro použití v osobních přenosných počítačích. Další výhodou, oproti klasickým pevným diskům, je absence hluku. Jelikož pevné disky mají pohyblivé části jako například plotýnky, vydávají při jejich roztáčení hluk. Moderní verze pevných disků však v současné době bývají už poměrně tiché. Nevýhodou SSD disků je jejich vyšší pořizovací cena.[12]

6.1.3 USB flash disk

Velmi podobné, jako externí SSD disk. Flash disk používá stejnou technologii, jako SSD. Jsou tedy rychlé, odolné vůči nárazům a otřesům. Jedná se však ze své podstaty o kompaktní média s malými rozměry. Jejich výhodou tedy je, že jsou kompaktní, a nezabírají mnoho místa. Z toho však plyne nevýhoda – a tou je omezená kapacita úložiště. Dříve se jednalo o stovky MB až jednotky GB. Dnes jsou běžné flash disky o kapacitě v řádu desítek až stovek GB.

[12] *Vše o SSD* [online]. Svět Hardware, 2010 [cit. 2022-04-13]. Dostupné z: https://www.svethardware.cz/vse-co-jste-chteli-vedet-o-ssd/26524

6.1.4 Cloudové servery

K využití této možnosti potřebujeme být připojeni k internetu. Cloudové servery jsou provozovány velkými firmami, mezi nejznámější patří například Google, Microsoft, Dropbox nebo Apple. Tyto společnosti provozují datová centra v různých místech po celém světě, a nabízí uživatelům prostor pro ukládání dat. Základní využívání těchto služeb je zdarma, máme však omezenou kapacitu pro naše data. Za větší kapacitu úložiště se platí většinou v měsíčních intervalech. Výhodou tohoto řešení je, že servery a datová centra, na nichž máme uložená data, jsou spravována velkými, bohatými společnostmi, které mají zdroje a možnosti zajistit kvalitu a bezpečnost těchto serverů. Svěříme tedy svá data (i důvěru) jednomu z těchto velkých hráčů. Nevýhodou je, že často nevíme, kde přesně se naše data nachází a kde mohou být uložena. Může to být v jednom z mnoha datových serverů, vlastněných touto společností, které se nachází různě po světě.

6.2 Kontrolní otázky k tématu zálohování

1) Jaké jsou nejčastější příčiny ztráty dat?
2) Co za proces označuje zálohování?
3) Na jaká média je možno zálohovat?
4) Rozdíly mezi HDD a SSD?
5) Výhody/nevýhody cloudových serverů?

7 Sociální inženýrství

Sociální inženýrství nebo také sociotechnika je ovlivňování a přesvědčování lidí s cílem oklamat je tak, aby uvěřili, že sociotechnik je osoba s totožností, kterou předstírá a kterou si vytvořil pro potřeby manipulace. Díky tomu je sociotechnik schopný využít lidi, se kterými hovoří, případně použít dodatečné technologické prostředky, aby získal hledané informace.[13]

Téma sociálního inženýrství je velice rozsáhlé a existuje tudíž řada definic. Hlavní myšlenkou je, že nejslabší částí všech informačních systémů je vždy člověk (uživatel). S tím souvisí fakt, že čím více přístupových práv uživatel má, tím vyšší riziko může pro systém představovat. Útočník se nemusí zaměřovat na prolamování hesel nebo jiné složité metody při snaze proniknout do systému. Existuje totiž jednodušší způsob – a tím je buď přinutit, nebo zmanipulovat někoho jiného, kdo přístupové údaje zná, aby je útočníkovi (třeba i nechtěně) sdělil. Pokud si navíc útočník povede chytře a promyšleně, často si oběť tohoto útoku vůbec neuvědomí, že vyzradila citlivé údaje. Úspěšný útočník je ten, který umí efektivně dohledávat, získávat a vyhodnocovat informace. Stále je možno narazit na lidi, kteří si neuvědomují důležitost a hodnotu informací, a tedy je ani nemusí napadnout, že některé informace je třeba střežit. Takovýto typ útoků je možné úspěšně provádět i z toho důvodu, že probíhají ve virtuálním prostředí. Pokud z obchodu ukradneme zboží, je velmi jednoduché tento čin prokázat, protože u sebe fyzicky držíme ukradené zboží. Avšak pokud od někoho jiného okopírujeme program či jeho seminární práci, fyzický důkaz neexistuje.

7.1 Metody útoku

7.1.1 Phishing

Forma kybernetického útoku, která využívá techniky sociálního inženýrství. Útočník se vydává za důvěryhodnou osobu s cílem získat citlivá data oběti, nebo získat přístup do systému. Pokud se útočníkovi podaří získat data oběti, může je použít k následnému vydírání, například s cílem získání finančních prostředků. Ve zdravotnických zařízeních jsou uložena obzvlášť citlivá data pacientů. Ochrana těchto dat je bezpochyby velmi důležitá. Pokud by v nemocnici nebo zdravotnickém zařízení byl ošetřen člověk, o kterého se případný útočník zajímá, takováto data zdravotnického charakteru by byla pro útočníka velmi „atraktivní“.

[13] MITNICK, Kevin a William SIMON. *Umění klamu*. Gliwice: Helion, 2003. ISBN 83-7361-210-6. Zkráceno, upraveno.

7.1.2 Způsoby provedení útoků

1. **Přímý přístup**
    - Útočník bez váhání a studu jednoduše přímo požádá oběť, aby mu sdělila své přístupové údaje. Tato žádost může mít různou formu a argumenty. Ačkoliv se to zdá až nemožné, může mít i tento primitivní způsob šanci na úspěch.
2. **Spearphishing**
    - Jedná se o cílenou formu phishingu. Útočník rozesílá přizpůsobené zprávy jednotlivci, nebo omezené skupině lidí. S cílem získat jejich citlivá data, nebo je zmanipulovat k provedení akce, která by pro ně byla škodlivá.
3. **„Důležitý“ uživatel**
    - V tomto případě útočník předstírá, že ve firmě zastává jednu z vyšších funkcí. Vymýšlí si, že má problémy, které potřebuje naléhavě vyřešit. Po oběti si žádá informace často zdůvodňované tím, že má vyšší autoritu. Tento typ útoků je většinou cílen na zaměstnance, kteří ve firmách působí jako pracovníci technické podpory. Ti pochopitelně nestojí o problémy a „nadřízenému“ raději pomohou, než aby vznikl konflikt.
4. **„Bezmocný“ uživatel**
    - Útočník zde předstírá, že je novým zaměstnancem firmy, případně že není zručný, co se týče ovládání počítače. Může předstírat neznalost firemního systému, nebo problémy například s prvním přihlášením či nastavením. Obětí je v tomto případě skutečný zaměstnanec firmy, který se snaží „novému kolegovi“ poradit. Dočasně například poskytne útočníkovi své přístupové údaje. Pokud je obětí administrátor, může pro daný účet vygenerovat nové heslo.
5. **Falešná technická podpora**
    - Tento způsob představuje efektivní a ve většině případů úspěšné získání informací od běžných uživatelů. Útočník se vydává za pracovníka technické podpory firmy. Typickým příkladem je rozesílání e-mailu, ve kterém útočník požaduje zaslání přístupového jména a hesla, ať už pod jakoukoliv smyšlenou záminkou.
6. **Scareware**
    - Software snažící se vyvolávat strach a úzkost, a zmanipulovat tak oběť k instalaci škodlivého kódu na své zařízení. Útočník obvykle za tento nefunkční či škodlivý software vybírá finanční prostředky. Typickým příkladem je falešná zpráva, že došlo k napadení zařízení uživatele. A současně je uživateli nabídnuta instalace falešného antivirového programu.

7. **Obrácená sociotechnika**
    - Opačná situace než v předchozích případech. Útočník zorganizuje okolnosti tak, že se na něj oběť obrátí s prosbou o pomoc.

Sociotechnik na základě svých schopností může manipulovat s lidmi. Schopnost umění manipulace je ve většině případů natolik propracovaná, že stačí k tomu, aby byl útočník úspěšný. Nicméně důležité jsou také jeho znalosti o počítačových systémech, do kterých se snaží proniknout. Prolomení systému je útočníkovi v některých případech usnadněno, a to z toho důvodu, že si správce systému ulehčil práci, a nezměnil výchozí (defaultní) hesla. Jako je například u většiny routerů z továrny nastaveno přístupové jméno „admin„ a heslo rovněž „admin“.

7.2 Kontrolní otázky k tématu sociálního inženýrství

1) Co je to sociotechnika?
2) Kdo je sociotechnik?
3) Kdo nebo co je neslabším článkem každého informačního systému?
4) Co je to phishing?
5) Jaké jsou způsoby provedení útoku?
6) Co je to scareware?

8 Závěr

Bezpečnost je důležitou disciplínou napříč všemi obory. Je potřeba věnovat jí náležitou pozornost při práci ve kterékoliv specializaci. Výjimkou nejsou ani informační a komunikační technologie. Za poslední desítky let nastal veliký rozmach těchto technologií, které jsou nyní využívány v širokém spektru oborů. Využívají je zaměstnanci ve všech sférách a je tedy důležité, aby také věděli, jak je využívat bezpečně.

8.1 Hodnocení zdravotníků

Práce byla předložena lidem zaměstnaným ve zdravotnictví. Poprosil jsem své známé z České i Slovenské republiky, a také kolegy z FNKV, aby si práci pročetli, a zaslali zpět své osobní hodnocení. Uvedu zde některá z nich. Pro účely práce neuvádím jména konkrétních lidí, pouze jejich funkci a zdravotnické pracoviště.

„Bakalářská práce dle mého názoru svým obsahem odpovídá danému tématu a metodice práce. Je psána srozumitelně a v dostatečné míře, aby se mohl dle náležitého textu instruovat či edukovat jakýkoliv zdravotnický personál, který v daném odvětví není zdatný či potřebuje proškolit. Co mohu vytknout jsou občasná slovní spojení, která místy do textu nepatří, a která se pochopitelně v díle tohoto obsahu mohou vyskytovat. Doporučil bych proto korekturu daného textu kompetentní osobou."

- Zdravotnický záchranář, Nemocnice ve Frýdku-Místku

„Bakalářská práce se zabývá velice důležitým a pro dnešní dobu nepostradatelným tématem. Práce je zpracována přehledně, a i pro laiky pochopitelně, působí edukativně a zároveň odborně. Téma je zvoleno velmi vhodně a jistě je důležité zdravotníkům připomínat nezbytnost IT bezpečnosti a základní pravidla pro bezpečnou práci s IT technologiemi. V dnešní době je čím dál tím více kladen důraz na citlivost osobních údajů, které jsou nedílnou součástí elektronické dokumentace pacientů. V době válečných konfliktů ve 21. století zároveň stoupá počet pokusů o kyber zločiny a je tedy nezbytné navyšovat zabezpečení zdravotnických systémů a zvyšovat gramotnost zdravotnických pracovníků v oblasti IT bezpečnosti."

- Pracovník na ARO a zdravotnický záchranář, Nemocnice ve Frýdku-Místku

„Bakalárska práca popisuje tieto témy jednoducho a zrozumiteľne. Je to vhodné pre zamestnancov, ktorí sa nepohybujú v IT oblasti. Môže im to pomôcť získať viac informácií, ktoré sa týkajú bezpečnosti. Spôsob práce je zameraný skôr na bežných užívateľov ako iba pre zdravotníkov.“

- Dětská lékařka, Detská ambulancia Ľubica

„Předmětem této bakalářské práce byla edukace zdravotnického personálu v IT bezpečnosti. Student uvádí svou prací jasně do dané problematiky. Vysvětluje a klade důraz na nutnost zabezpečení zdravotnického objektu. Rozvádí možnosti zabezpečení a jejich výhody i nevýhody. Zároveň upozorňuje na bezpečnost zacházení s elektrickými zařízeními. Student se dále zabývá autentizací a zálohováním důležitých dat. Samotná autentizace je popsána velmi podrobně, pro potřeby zdravotníků možná až příliš podrobně. Věřím, že takto obsáhle zpracované téma by spíše ocenilo IT zázemí daného zdravotnického zařízení, nežli zdravotník. Důležitost zálohování a uschovávání dat je ve zdravotnickém oboru nezbytná. Většina nemocnic v České republice využívá již platformy založené na informačních technologiích pro ukládání dat o svých pacientech, avšak velká část nemocnic si stále uchovává i tištěnou formu (chorobopisy). Někteří doktoři využívají také externí disky a optická média (CD/DVD).“

- Praktická sestra, Fakultní nemocnice Brno

„Vámi předložené materiály shrnují a formou pro širokou (a často nejen IT nepolíbenou) skupinu nejen zdravotníků základní metody zabezpečení dat v rámci zdravotnictví, konkrétně malé ordinace. Chybí mi zmínka o "nefyzické" bezpečnosti, která by doplňovala kapitolu o té fyzické. Oceňuji kapitolu o autentizaci, protože z praxe znám otázky typu "proč musím mít tolik hesel?" apod., jejichž počet by podobný materiál mohl snížit. V případě zálohování jsou shrnuty základní řekněme hardware způsoby zálohy, bylo by dobré zmínit i možnosti "softwarové" zálohování dat (RAID). Velké plus je potom kapitola o sociálním inženýrstvím, které osobně vnímám jako největší problém kybernetické bezpečnosti, protože je zcela závislé na lidském faktoru. Krátké až rejstříkové shrnutí jednotlivých typů útoků tohoto druhu je skvělé.

Celkově mi práce přijde jako dobrý start pro užití v praxi k edukaci zdravotnického personálu. Jednotlivé kapitoly bych ovšem nenazval materiálem. Podle zadání budou materiály dostupné na proambulance.cz, kde jsem ovšem nic nenašel.“

- Vedoucí biomedicínského oddělení, Oftalmologická klinika FNKV a 3. LF UK

„Bakalářská práce je psána s logickou posloupností, odborně, zároveň ale velice srozumitelně a přehledně. Dle mého názoru je vhodná pro edukaci, rozšíření povědomí, a to ať pro zdravotnický personál, či, jak sám autor uvádí, ostatní uživatele informačních technologií."

- Záchranář a pracovník na infekčním oddělení, Soukromá záchranná služba v Praze

8.2 Shrnutí jednotlivých kapitol

8.2.1 Fyzická bezpečnost malé ordinace

V kapitole o fyzické bezpečnosti jsme si ukázali, že hrozby nehrozí jen prostřednictvím hackerských útoků a počítačových virů. IT systém, přístroje a elektronické příslušenství je třeba zabezpečit rovněž fyzicky. Ve většině případů se jedná o drahá zařízení, na kterých fyzické poškození může napáchat vysokou škodu. Je tedy důležité mít zavedený systém opatření, jejichž účelem je minimalizovat, nebo v ideálním případě odstranit riziko fyzických hrozeb. Způsoby, jak zajistit fyzickou bezpečnost, jsou v zásadě dva: mechanické a elektronické. Co možná nejbezpečnější úroveň zabezpečení je realizována vhodnou kombinací obou těchto způsobů najednou. Systém je bezpečnější, pokud zároveň použijeme elektronické zabezpečení, než kdybychom použili jen to mechanické. Účinnost mechanických zabezpečovacích prvků spočívá v jejich mechanické pevnosti. Vytváří tedy překážku, jakousi fyzickou bariéru, mezi případným útočníkem, a systémem, který je třeba ochránit. Řadíme sem všechny zámky, bezpečnostní dveře, mříže a tak podobně. Ačkoliv mechanické zabezpečovací prvky mají bezpochyby své výhody, nejsou schopny případný pokus o neoprávněné vniknutí zaznamenat, ani nás o něm informovat. V této chvíli přichází na scénu elektronické zabezpečovací prvky. Jejich hlavním účelem je to, co jejich mechanické protějšky neumí – zaznamenat útočníka při činu a informovat o tom majitele. Patří sem kamery, detektory pohybu a různé alarmy. Následuje další důležité téma ve všech IT systémech, a tím je autentizace.

8.2.2 Autentizace

Pod pojmem autentizace je myšleno vše, co spadá do procesu označujícího ověření identity uživatele. Tento proces zajišťuje ochranu před tím, aby do systému nevstoupila nepovolaná osoba. Každý informační systém musí znát identitu uživatele, který do něj vstupuje, a je nutno ověřit, zda tento uživatel je skutečně tím, za koho se vydává. Základní způsob autentizace je realizován pomocí přístupových údajů – zpravidla jméno a heslo. Pokud chceme mít vyšší úroveň zabezpečení, přidáme vedle klasického jména a hesla další způsob ověření. Hovoříme pak o takzvané dvou a více faktorové autentizaci. Způsobů, jak realizovat dvou faktorovou autentizaci, existuje několik. Jmenovitě jde o použití hardwarového nebo softwarového klíče, kód z SMS zprávy, nebo využití biometrických údajů.

Uživatelům nejznámější je nejspíše dvou faktorová autentizace s využitím kódu z SMS zprávy. Po zadání našeho jména a hesla do systému na náš mobilní telefon přijde SMS zpráva s kódem (většinou číselným). Tento kód zadáme do systému, a tak prokážeme, že jsme skutečně tím, za koho se vydáváme. Může se stát, že nám případný útočník zcizí naše přístupové údaje (jméno a heslo). Pravděpodobnost, že útočník má současně i přístup k našemu mobilnímu telefonu, je však velmi nízká. Tento způsob je tedy bezpečnější, nežli základní autentizace pouze pomocí jména a hesla. Dvou faktorová autentizace nabízí větší míru zabezpečení, avšak za cenu, že proces je potom delší. Uživatel obecně nerad ztrácí čas. Všechno by mělo být co nejrychlejší, aby se uživatel nezdržoval. A právě to je důvod, proč dvou faktorová autentizace není příliš populární u uživatelů – jednoduše proto, že ji považují za ztrátu času.

8.2.3 Zálohování

Kapitola zálohování pojednává především o důležitosti našich dat, a o tom, jak je třeba vyvarovat se případným ztrátám těchto dat. Ztráta dat je něco, co si nepřeje žádný uživatel. Avšak veliká část lidí věří, že by se jim něco takového nemohlo nikdy stát, nevěnují tudíž zálohování dat dostatečnou pozornost. Štěstí však přeje připraveným – jak praví staré české přísloví – a v tomto směru připravený uživatel je ten, který zodpovědně zálohuje svá data. Způsobů zálohování má uživatel na výběr několik. Je třeba se rozhodnout, který způsob je pro jeho potřeby nejvhodnější, a tento způsob poté zvolit. K nejstarší možnosti, kam data zálohovat, patří optická média (CD, DVD nebo Blu-ray). Jde o levné řešení, avšak tyto disky už pro potřeby většiny dnešních uživatelů nabízejí nedostatečnou úložnou kapacitu. V současné době aktuálním a nejpoužívanějším řešením jsou takzvané externí disky, jejichž hlavní výhodou je velká kapacita (řádově desítky GB až jednotky TB). Uživatel má na výběr mezi dvěma druhy: HDD a SSD. HDD externí disk představuje levnější variantu. Disk tohoto typu se používá především u stolních počítačů. Oproti tomu disk SSD je rychlejší, v porovnání s diskem HDD o stejné kapacitě má menší rozměry a hmotnost, a je také odolnější. Menší variantou disku SSD je USB flash disk, který používá stejnou technologii. Má jen menší rozměry a stejně tak i kapacitu. V současné době jsou velmi populární online úložiště, takzvané „cloudové servery“. Uživatel v tomto případě provádí zálohu svých dat na servery, které jsou provozovány jinou společností (například Google, Microsoft nebo Apple). Zdarma je k dispozici omezené úložiště, za příplatek je však možno kapacitu úložiště navýšit. Důvod, proč je toto řešení populární, je bezpochyby ten, že se uživatel nemusí starat o bezpečnost zálohování dat, jednoduše jí svěří do rukou jedné z těchto velkých společností. Je na každém, do jaké společnosti se rozhodne vložit svou důvěru, a svěřit jí svá data k ochraně.

8.2.4 Sociální inženýrství

K nejvíce úspěšným metodám útoku patří způsob, kdy se útočník vydává za někoho jiného. Touto problematikou se zabývá sociální inženýrství. Útočník (sociotechnik) se snaží ovlivnit a přesvědčit oběť, aby získal citlivé informace, nebo oběť donutil k provedení určité akce. Bohužel, nejslabší částí, v oblasti bezpečnosti informačních systémů, je vždy člověk (uživatel). A čím více přístupových práv uživatel má, tím větší nebezpečí může nastat, pokud by k jeho účtu získala přístup jiná neoprávněná osoba. Důvodem, proč sociotechnik bývá v mnoha případech úspěšný je, že má velmi bohaté zkušenosti v oblasti manipulace ostatních lidí. Nemusí se tedy zabývat složitým prolamováním hesel nebo jinými náročnými metodami, protože mnohem jednodušší je přinutit, nebo zmanipulovat někoho jiného, aby útočníkovi (třeba i nechtěně) přístupové údaje sdělil. V některých případech si sociotechnik počíná natolik chytře a promyšleně, že si oběť mnohdy vůbec neuvědomí, že se stala terčem útoku a tyto citlivé údaje vyzradila. Lidé si totiž často neuvědomují cenu a hodnotu informací, které mají. Nevěnují tedy dostatečnou pozornost jejich ochraně a nenapadne je, že by se tyto informace mohly stát terčem útoku.

Věřím, že tato práce pozitivně přispěje ke vzdělávání především zdravotníků, na které je primárně cílena, ale také všech ostatních uživatelů informačních technologií, kterým může lépe pomoci zorientovat se v problematice IT bezpečnosti.

Seznam použité literatury

[1] MAYER, Marco, Pablo MAZURIER a Gergana TZVETKOVA. How would you define Cyberspace?. *Academia* [online]. Draft Pisa, 19.05.2014 [cit. 2022-03-01]. Dostupné z: https://www.academia.edu/7096442/How_would_you_define_Cyberspace

[2] *Varování v souvislosti s ekonomickými sankcemi spojenými s Ruskou federací* [online]. NÚKIB, 21.03.2022 [cit. 2022-04-01]. Dostupné z: https://www.nukib.cz/cs/infoservis/hrozby/1823-nukib-vydal-varovani-v-souvislosti-s-ekonomickymi-sankcemi-spojenymi-s-ruskou-federaci/

[3] *Vzdělávací portál NÚKIB* [online]. Brno: NÚKIB, 2021 [cit. 2022-04-11]. Dostupné z: https://osveta.nukib.cz/local/dashboard/

[4] *Kyberútok na nemocnici v Benešově* [online]. Praha: Čerský rozhlas, 2020 [cit. 2023-08-01]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/kyberutok-kyberneticky-utok-nemocnice-v-benesove-skoda-pachatel-hacker_2008180912_ako

[5] *Hackerské útoky na nemocnice*[online]. Praha: ČTK, 2022 [cit. 2023-08-02]. Dostupné z: https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-hackerskym-utokum-celily-v-cesku-nemocnice-narodni-knihovna-ci-volebni-web-40394428

[6] *Fakultní nemocnice Královské Vinohrady* [online]. Praha: FNKV, 2023 [cit. 2023-08-02]. Dostupné z: https://www.fnkv.cz/

[7] *Projekt studentů FBMI proAmbulance.* [online]. Kladno: FBMI, 2022 [cit. 2022-05-09]. Dostupné z: http://proambulance.cz/

[8] *ČSN P CEN/TS 14383-3*. 12/2006. Praha: Český normalizační institut, 2006.

[9] *Rozdělení kamerových systémů* [online]. Příbram: Security Agencies, 2022 [cit. 2022-04-04]. Dostupné z: https://www.securityagencies.cz/clanek/co-to-jsou-kamerove-systemy-cctv-proc-je-mame-chtit-a-jak-se-rozdeluji

[10] BRECHLEROVÁ, Dagmar. *FYZICKÁ BEZPEČNOST INFORMAČNÍCH SYSTÉMŮ*, 2007. Praha. KIT PEF ČZU.

[11] *Rozbor HDD* [online]. Vše o HW, 2006 [cit. 2022-04-11]. Dostupné z: http://vseohw.net/clanky/recenze/rozbor-hdd

[12] *Vše o SSD* [online]. Svět Hardware, 2010 [cit. 2022-04-13]. Dostupné z: https://www.svethardware.cz/vse-co-jste-chteli-vedet-o-ssd/26524

[13] MITNICK, Kevin a William SIMON. *Umění klamu*. Gliwice: Helion, 2003. ISBN 83-7361-210-6. Zkráceno, upraveno.