ČESKÉ VYSOKÉ
UČENÍ TECHNICKÉ
V PRAZE

FAKULTA
BIOMEDICÍNSKÉHO
INŽENÝRSTVÍ

BAKALÁŘSKÁ PRÁCE

2019

TOMÁŠ
KRAJČA

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA BIOMEDICÍNSKÉHO INŽENÝRSTVÍ

Katedra biomedicínské informatiky

Kurs pro školení v IT bezpečnosti

IT security training course

Bakalářská práce

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

Autor bakalářské práce:	Tomáš Krajča
Vedoucí bakalářské práce:	RNDr. Dagmar Brechlerová, Ph.D.

Kladno 2019

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení:	**Krajča**	Jméno:	**Tomáš**	Osobní číslo:	**465559**
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:

Kurs pro školení v IT bezpečnosti

Název bakalářské práce anglicky:

Course for training in IT security

Pokyny pro vypracování:

Cílem bakalářské práce je navázat na úlohy z předešlých kurzů a aktualizovat je o další metody v kybernetické bezpečnosti. Student se bude zabývat elektronickými certifikáty, hesly, typy médií a jejich zálohováním, malwerem a antivirovými programy, případně dalšími problémy dle potřeby. Zmapuje současné problémy v bezpečnosti IT z hlediska lékařů a sester a navrhne jejich možné řešení. Materiály kurzu budou upraveny tak, aby se daly využít pro uživatele bez informatického vzdělání.

Seznam doporučené literatury:

[1] Thorsten Petrowski, Bezpečí na internetu pro všechny, 2014, ISBN 978-80-7424-066-9
[2] Zvárová, Jana - Lhotská, L. - Přibík, Vladimír - Adášková, Jana - Brechlerová, Dagmar - Hanzlíček, Petr - Huptych, M. - Kopecký, M. - Papíková, Vendula - Potůček, J. - Přečková, Petra - Říha, Antonín - Svátek, Vojtěch - Šárek, Milan - Zitová, Barbara - Zv, Biomedicínská informatika, 4, ed. Biomedicínská informatika, 4, ročník 2010, kapitola ---, 2010, Karolinum
[3] KOLOUCH, Jan a Pavel BAŠTA, Cyber Security, CZ.NIC, z.s.p.o., 2019, ISBN 978-80-88168-31-7
[4] KOLOUCH, Jan, CyberCrime, CZ.NIC, 2016, ISBN 978-80-88168-15-7
[5] DOSEDĚL TOMÁŠ, Počítačová bezpečnost a ochrana dat. , ed. 1, Brno : Computer , 2004, ISBN 80-251-0106-1
[6] PETERKA, Jiří, Báječný svět elektronického podpisu, CZ.NIC, 2011, ISBN 978-80-904248-3-8

Jméno a příjmení vedoucí(ho) bakalářské práce:

RNDr. Dagmar Brechlerová, Ph.D.

Jméno a příjmení konzultanta(ky) bakalářské práce:

Mgr. Radim Krupička, Ph.D.

Datum zadání bakalářské práce: **19.02.2019**
Platnost zadání bakalářské práce: **20.09.2020**

doc. Ing. Zoltán Szabó Ph.D.	prof. MUDr. Ivan Dylevský, DrSc.
podpis vedoucí(ho) katedry	podpis děkana(ky)

PROHLÁŠENÍ

Prohlašuji, že jsem bakalářskou práci s názvem Kurs pro školení 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 16.5.2019 …..……..……...

Tomáš Krajča

PODĚKOVÁNÍ

Rád bych tímto poděkoval vedoucí práce RNDr. Dagmar Brechlerové, Ph.D., za její cenné rady, připomínky a její starostlivost v průběhu psaní práce. Dále bych rád poděkoval mé skvělé rodině a přítelkyni, kteří mě podporují po celou dobu studia.

ABSTRAKT

Kurs pro školení v IT bezpečnosti

Hlavním cílem této práce je vytvořit teoretický kurz a k němu příslušný praktický materiál zaměřený na edukaci zdravotnického personálu v rámci kybernetické bezpečnosti. Zejména se jedná o pochopení problematiky autentizace, elektronických certifikátů, antivirové ochrany a škodlivého malwaru a poslední část tvoří dotazník, který byl předložen zdravotnickému personálu, zejména lékařům a sestrám s cílem identifikovat jejich současné znalosti a problémy související s používáním výpočetní techniky. Jednotlivé kapitoly byly vybrány tak, aby aktualizovaly již obhájené práce s podobným tématem, a také pro vytvoření několika nových témat. Výsledkem je teoretický materiál a praktické návody vztahující se k teoretickým kapitolám a také vyhodnocení dotazníku.

Klíčová slova

Autentizace, elektronický podpis, zálohování, malware,

ABSTRACT

IT security training course

The main goal of this thesis is to create a theoretical curse with practical exercises. It is focused to education of medical staff in cyber security. In thesis are described problematics about authentication, electronic certificates, antivirus protection and malware and the last part of thesis is dedicated to questionnaire. The questionnaire was given to medical staff, doctors and nurses to identify actual problems with using computing systems and to identify their common knowledge of cyber security. Every topic was selected to update passed bachelor's theses based on similar way and to create new interesting topics. Result will be a theoretical part and practical exercises related to selected theoretical topics and as the last part is the result of questionnaire.

Keywords

Authentication, Electronic Signature, Backup, Malware

Obsah

1 Úvod

Nápad tvorby edukativních kurzů pro zdravotnický personál vznikl na naší fakultě biomedicínského inženýrství již před lety a během té doby bylo několik prací obhájeno. Jako vlastní cíl jsem si stanovil vytvořit aktualizovaný kurz, který klade důraz nejen na teoretickou stránku kybernetické bezpečnosti, ale také na vytvoření praktických podrobně popsaných návodů. Jednou z podmínek je vytvořit výukový materiál, kterému může porozumět i člověk s opravdu základními znalostmi výpočetní techniky a kybernetické bezpečnosti. Navíc jsem do své práce zahrnul průzkum pro zdravotnický personál, který má za úkol zmapovat současný stav znalostí kybernetické bezpečnosti a znalosti výpočetní techniky respondentů. Kapitoly v teoretickém základu mají primárně edukovat čtenáře o vybraných základních pojmech v rámci kybernetické bezpečnosti a kapitoly v praktické části nabízí několik užitečných návodů, které se pojí k teoretické části.

V současné době digitalizace může často docházet k únikům informací, které mohou mít v některých případech nevyčíslitelnou hodnotu. Je důležité, aby všichni uživatelé výpočetních zařízení byli dostatečně proškoleni, především uživatelé zařízení ze zdravotnického sektoru.

2 Vymezení vybraných pojmů a teoretický základ

Tato část práce obsahuje potřebnou teorii k pochopení vybraných pojmů a k následujícím praktickým návodům.

2.1 Autentizace – vymezení pojmů

Existuje více pojmů, které mohou neproškolení uživatelé výpočetních zařízení považovat za stejně významné. Patří mezi ně autentizace, autentifikace, autentikace identifikace, identita a autorizace. Zatímco autentizace, autentifikace, autentikace a verifikace jsou významově identické pojmy, tak identifikace, identita a autorizace se významově liší od ostatních pojmů, přestože spolu navzájem souvisí. Pro pochopení následujících způsobů autentizace je nutné těmto pojmům rozumět a znát jejich vzájemné rozdíly.

2.1.1 Identita a identifikace

Identita je pojem, který se vyskytuje v mnoha vědních oborech s různými významy. V rámci tohoto kurzu je nutné vnímat význam identity jako unikátní charakteristické znaky pro každého člověka, pro příklad rodné číslo, podpis, biometrické charakteristiky a jiné. Proces identifikace znamená určení identity konkrétního jedince. Tento proces je možné laicky vysvětlit jako zařazení lékařské zprávy podle jména a příjmení pacienta, do správného šuplíku obrovské kartotéky a do karty konkrétního pacienta – v případě elektronické identifikace, probíhá proces ověření pomocí specializovaného programu s vyhledáváním v příslušné elektronické databázi.

2.1.2 Autentizace, autentifikace, autentikace, verifikace

Jediný rozdíl v těchto pojmech spočívá v jejich pojmenování, myšlenkově jsou naprosto totožné a v následujícím textu bude použit pouze pojem autentizace. Oproti identifikaci se konkrétní subjekt prokazuje určitým způsobem, viz 2.2 Způsoby autentizace, za účelem ověření jeho identity. Pro připomenutí, identifikace je proces za účelem určení identity. S autentizací se setkáváme v každodenním životě fyzicky, pro příklad povolení přístupu do školy nebo na pracoviště, ale také v elektronickém světě v případě přihlašování do webových nebo počítačových aplikací. Laicky řečeno, subjekt dokazuje, že je tím, za koho se vydává. Tento proces je nezbytný pro zabezpečení veškerých elektronických účtů před možným únikem citlivých dat nebo editací dat neoprávněnou osobou. (1)

2.1.3 Autorizace

Po úspěšné autentizaci, zdali je uživatel tím, za koho se vydává, se mu následně přidělí oprávnění – proces autorizace. Uživatel má pak, na základě své pozice a svých práv, přístup do místností, do aplikací, může provádět změny v informačních systémech a jiné. Tento proces je nezbytný, bez jeho implementace by mohl jakýkoliv uživatel informačního systému provádět stejné úkony jako správce systému. Práva pro jednotlivé skupiny uživatelů nastavuje vlastník nebo určený správce systému. (1)

2.2 Způsoby autentizace

Pojem autentizace je vyložen v oddíle 2.1.2. Samotná autentizace může probíhat mnoha způsoby, prakticky je založená na třech základních otázkách, uživatel něco ví, uživatel něco má, uživatel někým je. Vzhledem k současnému stavu a nejvyšší rizikovosti autentizace způsobem uživatel něco ví, bude tomuto způsobu věnován větší důraz v teoretické i praktické části. (1)

2.2.1 Autentizace důkazem znalostí

Hojně používaná metoda, se kterou se každodenní uživatel výpočetních zařízení setkává nejčastěji. Jedná se o jednoduchý princip, kdy je uživatel požádán o vyplnění příslušných informací, běžně jde o přístupová jména a hesla nebo použití samostatného hesla. Poté, co uživatel požadovaná data vyplní, následuje proces autentizace, pokud autentizace nebyla úspěšná, uživatel je požádán o zkontrolování zadaných údajů, popřípadě k jejich přepsání, pokud je autentizace úspěšná – data se shodují s daty v databázi uživatelů, tak následuje proces autorizace.

Hesla – definice

Termín heslo má více významů, zde se zmiňuje heslo v informatické sféře, které souvisí hlavně s autentizací důkazem znalostí. Heslo je kombinace klávesnicových znaků, která je po uživateli žádána při pokusu o autentizaci a většinou ruku v ruce s uživatelským jménem – pro následnou autorizaci. Pokud máme na zařízení nainstalovaný operační systém a založeného jediného uživatele, pak můžeme být vyzváni k zadání hesla a následně máme přistup k celému zařízení. V jiných případech je počítač pouze prostředkem pro práci a přihlašují se k němu uživatelé na základě jejich přihlašovacích jmen a hesel, zařízení následně vyhodnotí uživatele a přidělí uživateli jeho vlastní práva pro práci se zařízením. Hesla je doporučené obměňovat, pro zvýšení bezpečnosti, ideálně jednou za tři měsíce, záleží především na typu uživatelského účtu. Nejdůležitější heslo pro běžného uživatele je k účtu emailové schránky. Většina aplikací vyžaduje registraci, do které se uvádí email uživatele, při ztrátě hesla do aplikace, je pak možno přes emailovou adresu heslo obnovit. Pokud útočník prolomí heslo do emailové schránky napadeného, pak si může vyžádat přístup do všech aplikací spojených s emailem

napadeného a napáchat tím mnohem větší škody. V praktické části bude uvedeno několik způsobů generování hesel.

Co je to silné heslo a jak vypadá

Správně zvoleným heslem si uživatel chrání své elektronické účty a ztěžuje potencionálním útočníkům snahu o prolomení hesla za účelem úplné kontroly nad účtem.

Kvalitní heslo obsahuje alespoň osm znaků a zároveň se nejedná o slovně pochopitelnou posloupnost znaků, protože existují slovníky hesel a s jejich pomocí lze hesla prolamovat. Při tvorbě hesla je důležité zakomponovat malá a velká písmena, číslice a speciální klávesové zkratky (,-„§¨/)+-). Pro pomoc s výběrem hesla existují náhodné generátory hesel online nebo samostatné aplikace, které mohou uživateli pomoci s vytvářením silného hesla.

Příklad slabého hesla: password, heslo, maruska1995, zuzanka, qwertz, admin, root

Příklad silného hesla: Jk5j-.Kjs-1, P4/ssWo-r-y, Uh6hjuiZl4-), OpYj-135

Kde uchovávat hesla

Hesla můžeme uchovávat ve speciálních aplikacích, které slouží jako soukromá databáze hesel, můžeme je mít napsané ručně, ale nejvhodnějším způsobem je uchovávat hesla pouze ve své paměti. Z ostatních jmenovaných způsobů je vlastní paměť tím nejbezpečnějším místem, pokud jsou hesla napsaná na papíře, může se k nim dostat nežádoucí jedinec, pokud jsou v zabezpečené aplikaci chráněné jednoduchým heslem, pak to může mít stejný negativní dopad, jako slabé heslo k emailové schránce.

2.2.2 Autentizace důkazem vlastnictví

S touto metodou se setkává také mnoho uživatelů, jedná se například o výběr peněz z bankomatu pomocí speciální karty, o přístup do budovy pomocí čipových karet, přístup do aplikací přes USB token, na kterém může být nahrán elektronický certifikát. Uživatel je vyzván k použití speciálního předmětu pro proces autentizace. Použití předmětu může být následováno požádáním o zadání PIN kódu. PIN kód je sled číslic, obvykle se používají čtyři číslice a více s hodnotou jedna až devět, pro druhou fázi autentizace jako kontrolu, že autentizační předmět používá jeho skutečný majitel. Některé tyto předměty disponují zabudovanými mechanismy, které při násilném vniknutí do předmětu nebo při několika nepovedený pokusech o autentizaci zablokují svůj vnitřní klíč a nelze již předmět využít k autentizaci. Výhodou autentizace důkazem vlastnictví je jednoduchý přenos a snadné použití, nicméně tato výhoda se může ukázat vysokým rizikem. Nedá se totiž poznat, kdo předmět pro autentizaci použil, to dává možnost případnému záškodníkovi vydávat se za někoho jiného a následně z toho profitovat. (1)

Výčet několika autentizačních předmětů:

- **SMART card** – mikroprocesorová karta velikosti kreditní karty s mikroprocesorem uvnitř. Pro čtení informací na kartě je potřeba specializovaná čtečka. (2)
- **USB token** – technologií je založen na stejném principu jako SMART card, velkou výhodou je právě USB. Pro ověřování záznamu na tokenu není potřeba specializované čtečky karet, ale jakékoliv zařízení, které disponuje USB portem. (1)
- **Mobilní telefon** – výhodou mobilního telefonu je fakt, že ho většina z uživatelů má neustále u sebe. Následná autentifikace může následovat zobrazením QR kódu na displeji telefonu následované jeho přiblížením ke čtečce QR kódu pro skenování, přeposláním elektronického certifikátu pomocí technologie NFC nebo zavoláním na konkrétní telefonní číslo – takto se pro příklad dá ověřit licence operačního systému Windows. (1; 3)
- **Softwarový token –** je v podobě elektronického certifikátu nebo aplikace, která obsahuje data potřebná k autentizaci a je nainstalována přímo na konkrétní zařízení. Doprovázeno ochranou heslem, pinem nebo frází. (1)

2.2.3 Autentizace důkazem biometrických vlastností

Systém, který ověřuje uživatele na základě některé biometrické veličiny, pro příklad otisk prstu, skenování duhovky. Nejbezpečnějším způsobem autentizace je dvoufázová autentizace, kdy se uživatel musí prokázat kombinací výše zmíněných metod autentizace. Často se jedná o uživatelské jméno, heslo a následný otisk prstu. U člověka se dají porovnávat biometrické charakteristiky fyziologického charakteru nebo behaviorálního charakteru. (1)

Výčet několika biometrických způsobů autentizace na základě fyziologických rysů:

- **Otisk prstu –** způsob autentizace, který je velmi rozšířen díky své implementaci do mobilních telefonů, prakticky může každý uživatel výpočetní techniky mít k dispozici vlastní čtečku. Existuje několik technologií, které snímají otisk prstu a každá z nich má své výhody/nevýhody. (1)
- **Rozpoznávání obličeje –** při tomto způsobu autentizace dochází ke skenování a následnému porovnávání výrazných rysů obličeje. *Existují 2D a 3D systémy, při čemž u 2D systémů nastává riziko, kdy systém lze oklamat fotografií pro následnou autentizaci.* Ke skenování se většinou používá kamera a počítačový algoritmus následně vyhodnocuje výsledky. (1)
- **Rozpoznávání duhovky** – zaručuje nejvyšší možnou přesnost správnosti autentizace. Duhovka je naprosto unikátní pro každého člověka a díky tomu se jedná o nejbezpečnější způsob autentizace.

Výčet několika biometrických způsobů autentizace na základě behaviorálních rysů:

- **Dynamika stisku kláves** – při autentizaci se zkoumá styl psaní na klávesnici, zkoumá se doba stisknuté klávesy, doba mezi stisky kláves, celková rychlost psaní, styl psaní číslic či velkých písmen a jiné další charakteristiky. Tento způsob má své ekonomické výhody – není potřeba dodatečných přístrojů pro autentizaci, ale také spoustu nevýhod – lidský faktor je proměnlivý, nemusí vždy psát stejným způsobem, záleží zde na velké množině proměnných. (1; 4)
- **Analýza psaného podpisu** – tento způsob má základ ve vědním oboru grafologii, kdy dochází ke zkoumání a ověřování podpisů nebo textu psaného rukou. Pro autentizaci je nutné mít speciální snímací podložku podobnou grafickým tabletům a speciální pero, které je pak na podložce snímáno. S touto technologií podpisu se setkáváme v současnosti při vyřizování nových občanských průkazů (2019). Následná autentizace probíhá na vyhodnocování výrazných charakteristik psaného textu – výška písma, sklon písma, tlak na podložku a jiné. (1)

2.2.4 Dvouprvková autentizace

Zkombinováním dvou autentizačních metod je zvýšena bezpečnost autentizace, nejčastěji se jedná o zkombinování autentizace na základě něco vlastním a něco vím. Uživatel se v tomto případě musí prokázat nejenom autentizačním předmětem, ale také svojí znalostí, například hesla. Tento případ nastává při běžném placení nákupu kreditní kartou, kdy je majitel karty, v případě částky vyšší, než je majitelovo zvolený limit, požádán o přiložení ke čtečce a následně musí zadat kód pin k provedení transakce – pin kód zde slouží jako druhý prvek autentizace.

2.2.5 Rizika autentizace

Jednotlivé způsoby autentizace nesou s sebou také svá rizika.

V případě autentizace prokazováním znalostí patří mezi největší rizika odposlouchávání hesel. To může být provedeno aplikacemi pro odposlouchávání zadaných kláves v průběhu práce se zařízením. Tyto aplikace se nazývají keyloggery a jejich princip spočívá v detekci veškerých kláves, stisknutých uživatelem a následném uložení do souboru pro čtení. Pokud si uživatel do počítače omylem nainstaluje podobnou aplikaci, pak útočník může nejen odposlouchávat veškerou komunikaci prostřednictvím vstupních zařízení, ale také získat přístup do účtů napadeného.

Rizika autentizace na základě prokázání se předmětem jsou spojena s lidským faktorem. Pro jednoprvkovou autentizaci právě zmíněným způsobem stačí pouze u sebe mít žádoucí předmět, a konkrétní uživatel se již jinak neověřuje. Dochází tak často ke zcizení takovýchto předmětů za účelem poškození pravého majitele předmětu nebo

k dosažení vyšších cílů útočníka. Proto je doporučeno tento způsob kombinovat s jinými metodami autentizace.

Autentizace na základě biometrických vlastností subjektu je nejbezpečnější z výše jmenovaných metod. Při prokazováním subjektu otiskem prstu lze technologicky nevyspělé čtečky oklamat uměle vytvořeným otiskem – útočník se tak vydává za majitele otisku. Starší systémy, které autentizovaly podle výrazných rysů v obličeji, se daly oklamat fotografií, v současné době je většina systémů vybavena 3D detekcí, při které již fotografii nelze použít. (1)

2.3 Elektronické certifikáty a podepisování

Velké množství informačních pramenů často používá termíny elektronický podpis a elektronický certifikát jako stejné. V následujících odstavcích jsou vysvětleny nejdůležitější pojmy, které souvisí s elektronickým podepisováním a je kladen důraz na osobní elektronické certifikáty.

2.3.1 Asymetrická kryptografie

Kryptografie je metoda, která primárně souvisí s utajováním komunikace. Existují dvě metody kryptografie, symetrická kryptografie a asymetrická kryptografie. Pro vysvětlení, symetrická kryptografie šifruje a dešifruje obsah, mezi její užití patřit posílání zpráv, šifrování souborů a jiné, pomocí jediného klíče. Tato metoda není tolik bezpečná kvůli důležitosti jediného klíče. V minulosti vznikla Caesarova šifra, kdy pro příklad: klíč = +3 znamená zapsání znaku podle abecedy, který je o 3 pozice níže než originální znak, došlo k tím zašifrování zprávy, protože se nedala normálně číst.

Asymetrická kryptografie na rozdíl od symetrické využívá k šifrování a dešifrování dvojici klíčů, klíč soukromý a klíč veřejný. Již z povahy názvu je patrné, že klíč soukromý se nesmí nikde sdílet a je výhradním vlastnictvím majitele. Klíč veřejný je zpravidla možné sdílet veřejně a v mnohých případech je to žádoucí, protože funkcí veřejného klíče je ověřování, zdali použitý soukromý klíč opravdu náleží jeho majiteli a zda s ním může provádět požadované operace. Mezi operace, ke kterým se používá soukromý klíč, patří podepisování elektronických dokumentů a dešifrování dat nebo komunikace. Veřejný klíč se oproti tomu používá k šifrování zpráv nebo určení, zdali je konkrétní elektronický podpis pravý a náleží majiteli, který elektronicky podepisoval. Může být matoucí, že se zrovna veřejný klíč využívá k šifrování zpráv, logicky však lze odvodit, pokud by uživatel šifroval soukromým klíčem, pak by si zprávu mohl dešifrovat každý uživatel vlastnící veřejný klíč. Šifruje se tedy veřejným klíčem, aby mohl požadovaný příjemce zprávu dešifrovat pouze svým soukromým klíčem a data se nedostala k nežádoucímu subjektu. Klíče se nazývají jako párové, nelze tedy použít jakýkoliv soukromý klíč a ověřit ho jakýmkoliv veřejným klíčem, k úkonům je potřeba použít konkrétní pár klíčů, nebo veřejné kořenové certifikáty certifikační autority (vysvětleno v elektronických podpisech). (5)

2.3.2 Elektronické certifikáty

Elektronický certifikát má podobu elektronického souboru obsahující identifikační data a veřejný klíč, primárně slouží k identifikaci uživatele. Certifikáty je možné roztřídit do kategorií podle použití, pro osobní použití, pro systémové použití, nebo podle jejich věrohodnosti z pohledu zákona, kvalifikované a komerční certifikáty. Skladovat elektronické certifikáty lze na USB tokenu, čipové kartě nebo uložené přímo v počítači.

Vyšší bezpečnosti je dosaženo v případě, kdy se soukromý klíč nachází na USB tokenu, nejlépe ještě chráněný heslem pro přístup a jeho majitel ho má bezpečně uložen. (6; 5)

Mnoho elektronických certifikátů lze nalézt již nainstalované v operačním systému, konkrétně systémové certifikáty. Tyto certifikáty jsou nezbytné pro správnou činnost aplikací a samotného systému, není tedy vhodné je nijak nezkušeně upravovat.

Osobní kvalifikované certifikáty

V České republice jsou celkem čtyři kvalifikovaní poskytovatelé služeb vytvářejících důvěru, kteří se řídí Zákonem o službách vytvářejících důvěru pro elektronické transakce (č. 297/2016 Sb.) a tři z nich mohou vydávat důvěryhodné kvalifikované certifikáty. Jedná se o První certifikační autoritu (http://www.ica.cz/), Českou poštu (http://www.postsignum.cz/) a eIdentity (http://www.eidentity.cz/), u všech výše jmenovaných poskytovatelů jsou kvalifikované certifikáty zpoplatněny. Pro elektronické podepisování je nutné mít certifikát od jedné z uvedených certifikačních autorit, v jiném případě může nastat nepřijetí certifikátu a následný podepsaný dokument nebo email nebude brán v potaz, protože nelze ověřit důvěryhodnost certifikátu. To se může stát při podepisování elektronickým certifikátem na zkoušku, lze jej získat od každé certifikační autority a primárně slouží k testování certifikátů, nejsou určeny k jinému použití. Při instalaci osobního kvalifikovaného certifikátu je také nezbytné nainstalovat kořenové certifikáty od kvalifikovaného poskytovatele služeb vytvářející důvěru pro elektronické transakce, který vydal konkrétní certifikát. (5; 6)

Obsah kvalifikovaného certifikátu lze shrnout v těchto bodech:

- Certifikát byl vydán podle zákona kvalifikovaným poskytovatelem služeb vytvářející důvěru
- Název kvalifikovaného poskytovatele a stát, ve kterém sídlí
- Jméno a příjmení majitele certifikátu
- Veřejný klíč majitele certifikátu
- Elektronickou značku poskytovatele certifikačních služeb
- Identifikační číslo certifikátu
- Počátek a konec platnosti certifikátu
- Možná omezení, pro která lze certifikát použít

Všechna kritéria se dají zobrazit při otevření certifikátu v počítači.

Další možné uplatnění elektronických certifikátů může být při tvorbě elektronických značek, vytváření časových razítek, přihlašování do aplikací, nebo při šifrování.

2.3.3 Časové razítko

Časové razítko je elektronické potvrzení, že soubor existoval v čase, kdy byl orazítkován. Může se připojit k elektronickému podpisu pro zpětné ověření, že dokument v tu dobu opravdu existoval a byl podepsán. Dá se získat pouze od kvalifikovaného poskytovatele služeb vytvářející důvěru pro elektronické transakce a stejně jako elektronický certifikát je razítko zpoplatněno. (6)

2.3.4 Elektronický podpis

Nezbytným prostředkem pro elektronické podepisování je elektronický certifikát. Pokud je potřeba komunikovat se státními orgány, významnými institucemi nebo jednoduše s kýmkoliv, kdo potřebuje jistotu, že podpis náleží podepisujícímu subjektu, pak je nutné podepisovat osobním důvěryhodným kvalifikovaným certifikátem vydaným poskytovatelem služeb vytvářejících důvěru pro elektronické transakce. Při podepisování použije uživatel svůj soukromý klíč, pro následné ověření pravosti podpisu se využívá veřejného klíče. Pokud se používá nebo ověřuje elektronický podpis, je také nutné mít v zařízení nainstalované kořenové certifikáty kvalifikovaného poskytovatele služeb vytvářející důvěru pro elektronické transakce, od kterého daný certifikát pochází. (5)

Pro platnost podpisu nesmí být porušena integrita podepsaného souboru, tím se rozumí, že po podepsání nebyla provedena v souboru již žádná změna. Ve věci emailu není potřeba zkoumat integritu, protože podpis se připojí k emailu při odesílání. Musí se ověřit, zdali je certifikát, který byl použit k podpisu, je v době podepsání stále platný. (5)

Soukromý klíč je jako razítko, které však používá pouze subjekt jemuž patří a používá ho v čase, kdy ho legitimně vlastní. Elektronický podpis je pak jako otisk razítka zároveň musí platit integrita dokumentu a dále v něm neměnit data. Následné ověření se pak provádí pomocí veřejného klíče.

2.4 Paměťová média a zálohování

Současný svět se postupně digitalizuje a pro uchovávání elektronických dat je potřeba paměťových médií. Je možné se setkat také s výrazy záznamová média, datové nosiče nebo datová média. Paměťová média se rozlišují podle technologického způsobu zápisu a čtení dat na média magnetická, optická a elektronická. Spolu s ukládáním dat souvisí otázka bezpečnosti uložených dat a rizika, která mohou způsobit modifikaci, kompromitaci nebo zničení dat. V této kapitole je kladen důraz na seznámení se současnými paměťovými médii, rizik jejich používání a na zálohování dat a archivaci.

2.4.1 Magnetická média

Nejpoužívanějšími paměťovými médii a zároveň nejideálnějšími z pohledu poměru výkon/cena jsou média, která pro zapisování a čtení dat využívají principu magnetické

indukce. Existuje mnoho podob, ve kterých se tato média vyskytují či vyskytovala, pro příklad diskety, pevné magnetické disky (HDD), magnetické pásky nebo magnetooptické disky. Tato média se používají pro trvalé uchování velkého objemu dat. Vzhledem k současnému vymizení disket, VHS nebo audio kazet, se pro běžnou práci sester a lékařů v jejich zařízení může vyskytovat, z výše jmenovaných magnetických médií pevný magnetický disk (HDD). (7)

Pevný magnetický disk – HDD (Hard Disk drive)

Elektromechanické zařízení, které pro čtení a zápis dat využívá principu magnetické indukce a je nevolatilního charakteru čili nepotřebuje k uchování dat elektrickou energii. Kapacita disků se v této době pohybuje od 1TB a přenosové rychlosti jsou, vzhledem k tomu, že se jedná o komponentu s mechanickými součástkami, velmi uspokojivé, kolem 200 MB/s. Pevné disky se rozlišují podle toho, zdali jsou interní nebo externí. Interní disky se fyzicky vyskytují uvnitř výpočetního zařízení a většinou se na ně instaluje operační systém a aplikace, nebo slouží pouze jako sekundární disk obsahující data aplikací či uživatelská data. Externí disky jsou většinou používány jako médium určené pro uchovávání a přenášení dat, připojují se podobně jako periferní zařízení počítače, jejich výhoda tkví v přenositelnosti, velké kapacitě a rychlostí přenosu podobně jako u disků interních.

Rizika magnetických pevných disků

Jak bylo uvedeno, magnetické pevné disky obsahují mechanické části, to může časem vést k únavě materiálu a poruchovosti částí disku. Není vhodné disky vystavovat vysokým teplotám, často se jedná o položení externího disku na stůl, který je pod přímým slunečním zářením nebo práce se zařízením v místnostech či venku za vysokých teplot. Pokud je disk v zapnutém stavu, může při neopatrné manipulaci s diskem dojít ke kontaktu ploten a čtecích nebo zapisovacích hlav, tento stav v lepším případě povede ke ztrátě některých dat, v horším případě ke ztrátě veškerých dat na disku. Životnost disku bývá kolem deseti let. (8)

2.4.2 Optická média

Optická média jsou plastové disky kotoučového tvaru s průměrem 12 cm nebo v menší verzi 8 cm obsahující otvor ve středu disku standardizované velikosti pro všechna optická média, primární účel disků je uchovávání elektronických dat. Optická média se v průběhu let vyvíjela natolik, že bylo dosáhnuto vyšších kapacit při zachování stále stejné fyzické velikosti média. Všechny optické disky jsou zpětně kompatibilní, což znamená, že i nová mechanika primárně určena pro čtení technologicky vyspělých Blu-ray disků dokáže přečíst i první CD disky. Ke čtení a zápisu dat je použit laserový

paprsek, jehož vlnová délka se s novějšími technologiemi zkracuje, tím dochází k navýšení možného datového úložiště při zachování stále stejných rozměrů disku. Existuje mnoho různých typů disku, na některé z nich lze zapisovat ve více vrstvách, popřípadě i na obě strany média. Rozdíly jsou také ve čtecích mechanikách, některé slouží pouze ke čtení a některé dokáží i na disk zapisovat, dalším důležitým aspektem je zpětná kompatibilita modernějších čtecích mechanik se staršími optickými disky, což neznamená možnost čtení nejnovějších disků na prvních mechanikách. Optické disky lze rozlišovat do několika základních typů. (9; 10; 7)

CD-R, CD-ROM, CD-RW, první generace optických disků

Tři různá pojmenování pro optické disky první generace a zároveň každé nese odlišné vlastnosti. Datová kapacita disků je až 700 MB dat nebo 80 minut zvukového záznamu. (7; 9)

CD-R (recordable – česky zapisovatelné) disky umožňují jednorázové zapsání elektronických dat.

CD-RW (rewriteable – česky přepisovatelné) disky dokáží přepisovat již zapsaná data, uživatel tedy může až 1000x přepsat data na disku.

CD-ROM (read only memory – česky pouze pro čtení) disky neumožňují další zápis dat, protože jejich obsah je dán již od výroby.

DVD-ROM, DVD-ROM, DVD-RW, druhá generace optických disků

Kapacita zvýšena na 4,7 GB díky novému technologickému postupu zapisování dat pomocí laserového paprsku s nižší vlnovou délkou, než tomu bylo u předchozích CD disků. Zapisování dat je možné až ve dvou vrstvách na obě strany média. Pro čtení a vypalování těchto disků je potřeba alespoň DVD mechanika, která je zpětně kompatibilní s CD disky. (7; 9)

Blu-ray a HD-DVD, třetí generace optických disků

HD-DVD disky jsou již minulostí, ale patří mezi důležité předchůdce nejmodernějších Blu-ray disků. Jejich principem bylo uchovávání elektronických dat, zejména audiovizuálních dat, a jejich zašifrování, tudíž nebylo možné tyto disky nadále kopírovat, před několika lety byla tato ochrana prolomena a vývoj těchto disků zastaven. Blu-ray disky jsou nejrozšířenějším zástupcem třetí generace optických disků s vysokou kapacitou pro záznam, až 128 GB při několikavrstvém zápisu dat na obě strany média. V současnosti se jedná o populární optické médium díky jeho kapacitě a možnosti použití pro sledování filmů ve vysoké kvalitě nebo distribuci video her. (7; 10; 9)

Rizika optických médií

Optická média jsou velmi náchylná na mechanické poškození zejména na poškrábání nebo zlomení, proto je nutné je uchovávat v ochranných obalech, které jsou ve formě pevných nosičů nebo plastikových sáčků, pevné nosiče jsou schopny ochránit médium před větším fyzickým působením, ale plastikové obaly slouží pouze k ochraně záznamové vrstvy před prachem a poškrábáním. Výrobci disků uvádějí životnost médií až na 100 let, při ohleduplném zacházení a správném skladování médií, u M-disků je uvedena životnost až 1000 let. Další rizika souvisí se čtením disků v optických mechanikách, kdy se na platu pro vložení disku můžou vyskytovat nečistoty a při čtení se pak disk může poškrábat. (10)

Výhody a nevýhody používání optických médií

To, zdali jsou optická média vhodná pro dané úkony s daty, souvisí především s požadavky uživatele. Mezi nesporné výhody patří velmi snadná přenositelnost disků, poměrně slušná kapacita pro data, jednoduchá obsluha optické mechaniky a práce s diskem, a v neposlední řadě také nízká pořizovací cena optických médií s nižší kapacitou.

Mezi nevýhody patří především jejich náchylnost k fyzickému poškození disku, hlučnost čtecí mechaniky a vysoká cena těch optických médií, které disponují vysokou kapacitou dat. (9)

2.4.3 Elektronická média

Elektronická média patří mezi technologicky nejmladší záznamová média. Jsou nevolatilního charakteru, což znamená, že nepotřebují elektrickou energii pro uchování již uložených dat, se ztrátou napájení tato média neztrácí již uložená data. Tato média *známe pod názvem paměti typu flash, nebo jednoduše flash paměti*, to znamená, že datová paměť je elektricky programovatelné a data se na ni mohou zapisovat i mazat. Data se zapisují do buněk, které pak následně uchovávají informace, zjednodušeně se dá říci, že celkovým počtem buněk je kostkovaný sešit, do jehož buněk v jednotlivých listech se ukládají informace. Elektronická média jsou populární díky svým kompaktním rozměrům při zachování vysokých kapacit a vysokými přenosovými rychlostmi, a díky absenci mechanických částí, které často vedly k únavě materiálu a poruchovosti. Nevýhodou používání elektronických médií je omezený přepis buněk, proto mají omezenou životnost, a dále vysoká cena oproti jiným záznamovým médiím. (7; 11)

Pevný elektronický disk SSD

V současné době je disk typu SSD velmi populární, především díky vysokým rychlostem čtení a zápisu dat, nárůst oproti magnetickým pevným diskům dokáže rozeznat i nezkušený uživatel. SSD disky se zejména používají pro instalaci operačních

systémů a aplikací, které se často v rámci systému používají a je u nich žádaná rychlá odezva. Vyrábí se ve velikostech srovnatelných s HDD nebo menších, připojení disků je možné pomocí několika standardů, záleží na základní desce zařízení. (10; 7)

Flash disk

Elektronické paměťové médium integrující jak paměť typu flash, tak USB nebo Thunderbolt rozhraní pro snadné připojení do zařízení. Tato média jsou charakteristická svými malými rozměry i při stálé vysoké kapacitě pro data a vysoké přenosové rychlosti. Existují flash disky různých typů, podle vnějšího obalu – kovové, voděodolné, plastové, nebo podle jejich vlastností – mohou obsahovat algoritmus pro zašifrování uložených dat, obsahovat čtečku otisku prstů, nebo jsou uzamykatelné – je potřeba zadat bezpečnostní PIN kód. (10)

Paměťové karty

Obdobná kapacita paměti, jako u Flash disku a ještě menší rozměry. Karty se používají především u přenosných zařízeních, kde je potřeba zajistit dostatečnou kapacitu pro ukládaná data a zároveň nezabírat velký prostor. Vyskytují se u fotoaparátů, chytrých zařízení, čteček knih, kamer a dalších podobných elektronických zařízení. Existují v několika standardizovaných rozměrech pro příklad SD Card, MicroSD card. Rozdíly mezi kartami nejsou pouze po stránce rozměru, ale také podle kapacity média a podle rychlosti přenosu dat. (10)

Výhody a nevýhody elektronických médií

U každého média byly uvedeny některé výhody jejich použití. Celkové výhody spočívají v absenci mechanických částí, které jsou náchylné k únavě materiálu, vysoké přenosové rychlosti dat i při menších rozměrech, u médií připojených pomocí USB je velká výhody v možnosti připojení k většině výpočetní techniky.

Mezi nevýhody patří především vysoká pořizovací cena, oproti jiným druhům záznamových médií a omezená životnost dána maximální možnou přepisovatelností jednotlivých buněk.

Rizika elektronických médií

Bylo řečeno, že rizikem používání elektronických médií je omezená životnost média, kvůli limitu pro přepis paměťových buněk. U velikostně menších elektronických médií je velká pravděpodobnost jejich ztráty, odcizení nebo hrubému mechanickému poškození. U flash disků a paměťových karet se může nacházet vstup do USB portu pouze z jedné strany obsahující kontakty, v tom případě jsou kontakty náchylné k poškození.

2.4.4 Zálohování a hrozby pro data

Proces zálohování znamená vytvoření kopie primárních dat pro možné obnovení, nastane-li případ, kdy se primární data znehodnotí nebo zničí. V případě elektronických dat se jedná o vytvoření kopie elektronických dat, která se následně uchovává na záznamovém médiu vhodném pro zálohování dat na bezpečném místě. Uživatelé si mnohdy neuvědomují, jaký by měla možná ztráta dat dopad, nejedná se pouze o finanční škody, škody mohou být i duševního charakteru, pro příklad ztráta nenahraditelných rodinných audiovizuálních záznamů nebo fotografií, které nelze finančně vyčíslit. Zálohovat se nemusí nutně veškerá data uložená na disku, v případě obnovování by to zabralo mnohem více času, než obnovování konkrétních dat. (12; 13)

Rizika správy dat

Uživatelé výpočetního zařízení mohou být napadeni útočníky, kteří mají za cíl data odcizit, pozměnit, smazat nebo zašifrovat veškerá záznamová média připojená k zařízení, podobně dokáže poškodit data i nevyžádaný software. Speciálními případy jsou aplikování sociálního inženýrství na oběť a živelní pohromy, které mohou znenadání zničit vše včetně špatně skladovaných záloh. A nesmí se opomenout selhání hardwaru, které může náhle přijít téměř kdykoliv a jedinou možnou obranou proti tomu je tvorba záloh. (14)

Sociální inženýrství v rámci kybernetické bezpečnosti nemá jednoznačnou definici, je to však metoda, která se aplikuje na konkrétní vyhlédnutou oběť prostřednictvím elektronické nebo každodenní reálné komunikace. Cílí na emoce oběti, mezilidské vztahy a snaží se oběť ovlivnit ve svůj prospěch. Napadený tak může, i nevědomě, útočníkovi poskytnout velmi cenné informace nebo poskytnout přímý přístup k nim. Jedná se o velmi účinnou metodu, proto je důležitá kybernetická osvěta, být ostražití a snažit se i v těžkých situacích myslet realisticky, poučit se chyb, kterých se mohli dopustit jiní uživatelé, nespěchat, nesdílet zbytečně informace o sobě a nenechávat se vydírat. Příklad takového útoku může být, když žena přijde do nové práce, zjistí si informace o kolezích a vybere si konkrétní oběť, následně se snaží vytvořit sofistikovaný vztah s vybranou obětí, postupně se snaží vztah vyvíjet k tomu, aby měla přístup k informacím, využije tedy oběť a po zisku informací je již může využít podle svého. (15; 16)

Živelní pohromy jsou jedna ze speciálních případů, kdy se při nedostatečném zabezpečení záznamových médií, popřípadě i záloh, mohou zničit data daného subjektu, objektu. Je potřeba vypracovat plán, podle kterého se musí, v případě, že pohroma nastane, postupovat a také dostatečně zabezpečit samotná zařízení obsahující záznamová média.

Zálohování a archivace

Neinformovaní uživatelé výpočetního zařízení mohou tyto pojmy mylně považovat za totožné. Archivace je způsob uchování takových dat, která nejsou již aktivně

používána a není je potřeba v dohledné době obnovovat. Archivovaná elektronická data jsou tedy uložena na záznamová média, která nejsou aktivně připojena k žádnému zařízení, ale v případě potřeby je možné data obnovit. Ve zdravotnictví přímo archivaci dat upravuje *Vyhláška č. 137/2018 Sb., kterou se mění vyhláška č. 98/2012 Sb., o zdravotnické dokumentaci, ve znění pozdějších předpisů*, podle které je nutná archivace zdravotnické dokumentace v listinné nebo elektronické podobě umístěna na nepřepisovatelném médiu s minimální životností 10 let. (13)

Způsoby zálohování

Zálohování elektronických dat se může provádět při dvou stavech. Online zálohování probíhá při aktivním používání zařízení, výhodou je možnost pracovat na zařízení během procesu zálohování. Offline zálohování je prováděno na vypnutém zařízení, nebo vyřazeném pro běžný provoz. Následuje výčet způsobů zálohování.

- Nestrukturovaná záloha

Nestrukturovaná záloha je v případě, kdy se data vyskytují na množství různých paměťových médií bez podrobných informací, která data a na jakém médiu jsou. Nedoporučuje se použití tohoto způsobu.

- Úplná záloha

Proces, při kterém se zálohují veškerá data, která jsou vybrána k zálohování. Provádí se jako první záloha dat. Při každém procesu se ale všechna data znova zálohují, i ta nezměněná od poslední provedené zálohy, to zabírá spoustu času a zároveň výpočetní kapacitu. Jedná se o nejjednodušší typ zálohy po stránce náročnosti a zároveň je i možná obnova dat rychlá. (14)

- Přírůstková záloha

Pro aplikování přírůstkové zálohy se prvně vytvoří úplná záloha a při každém dalším zálohování se aktualizují pouze změněná nebo nová data od poslední provedené první úplné nebo dalších přírůstkových záloh. Nevýhodou je, že při ztrátě nebo zničení jedné z přírůstkových záloh, jsou následně veškerá data na nových přírůstkových zálohách již neobnovitelná. Tomu se dá předejít častějšími úplnými zálohami. Výhodou tohoto způsobu zálohování je nižší náročnost na paměťovou kapacitu záznamových médií, protože se při procesu ukládají pouze samotné přírůstky. (13)

- Rozdílová záloha

Rozdílovému zálohování předchází úplná záloha a při každém dalším aplikování procesu zálohování dochází k ukládání nových nebo změněných souborech od poslední úplné zálohy. Výhodou je, že ztráta nebo zničení některé z rozdílových záloh nevede k neobnovitelnosti dat, každá rozdílová záloha je samostatná a obnovitelná. (17)

- Kompletní záloha systému

Způsob zálohování, který zálohuje všechna data a zároveň operační systém s nainstalovanými aplikacemi. Může se takto zálohovat celý disk nebo jednotlivé oddíly. Při tvorbě této zálohy, která je náročná na kapacitu záznamového média, se vytváří pro snížení datové kapacity zálohy kompletní obraz disku.

Kde uchovávat zálohy

Vzhledem k výčtu rizik spojených se správou dat je nutné vybrat vhodné místo k uchovávání záloh. K takovému místu nesmí mít nikdo neoprávněný přístup a také by se nemělo uchovávat ve stejné budově jako originální data, protože v případě požáru, povodní nebo zemětřesení by mohl zálohy potkat stejný osud, jako originální data v místních zařízeních. Nejvhodnějším řešením je zálohy skladovat v trezorech bank. Je možné disky také zašifrovat, pro jejich obnovení by pak bylo potřeba autentizování subjektem. Vytváření záloh a jejich uchovávání na stejném disku, kde se vyskytují originální data, má stejný dopad jako nezálohování. V případě potřeby by data byla neobnovitelná. (13)

Jak často zálohovat

Obecně vzato by se zálohování mělo provádět po každé větší změně dat v zařízení nebo v pravidelných stanovených intervalech. Každá větší změna dat znamená aktualizace operačního systému, nainstalování nových aplikací na zařízení, nebo nahrání většího množství nových dat. Stanovení intervalu není jednoznačné, v potaz se musí brát několik proměnných, například, zdali se jedná o zálohování osobních dat, firemních dat nebo třeba zálohování serverů. Pokud se zálohují osobní data z počítače, který používáme pouze pro osobní účely, tak je vhodným intervalem provádět zálohu jednou za měsíc způsobem, jaký si uživatel zvolí. U serverů nesmí docházet k výpadkům a také není vhodné zálohovat v čase špičky, kdy bývají velmi vytížené, vhodné je zálohovat každý den tak, aby případná ztráta byla co nejnižší. Firmy dodržují intervaly v rámci jejich předepsaných krizových plánech, aby eliminovaly možné ztráty.

Kompletní mazání a ničení záznamových médií

Většina neproškolených uživatelů je spokojena s přetáhnutím složky do koše a jeho vysypáním, nebo odinstalací aplikace prostřednictvím nainstalovaného operačního systému. Neuvědomují si však fyzikální principy zápisu dat na použité záznamové médium. V případě magnetických disků jsou data, z koše vysypaná nebo operačním systémem odinstalovaná, stále fyzicky na plotnách magnetického disku, procesem mazání nedochází k odstranění dat z ploten. Systém je však ignoruje a pokud je potřeba, příslušná místa na plotnách později zaplní novými daty. To samé existuje u SSD disků, kde jsou v paměťových buňkách stále data, dokud nedojde k přepisu. Toho se využívá hlavně z důvodu, že paměťové buňky SSD disků mají omezenou životnost a jejich přepisování jinými daty kvůli mazání by vedlo ke snížení životnosti. Existují softwarové aplikace, které dokáží kompletně mazat disky, provádí několikanásobný celkový přepis

datových buněk nebo dat na plotnách, aby nebylo možné původní data obnovit, v případě potřeby je vhodné takové programy využít. (18)

Pro ničení záznamových médií je nejvhodnější použít hrubé síly, fyzické zničení média jako roztavení nebo rozdrcení na prach jsou nejbezpečnější volby.

2.5 Malware, spam a scam, a antivirová ochrana

Tato kapitola obsahuje definici pojmu malware, příklady jeho nejčastějších forem, vysvětluje jeho šíření a dopad na zařízení. Také je zde vysvětlen princip těch útoků, které používají praktiky sociálního inženýrství, jak je rozeznat a jakou důležitost jim přikládat.

2.5.1 Co je to malware

Malware je souhrnné pojmenování pro škodlivý kód nebo software, jehož primárním účelem je způsobit škodu v softwarové části výpočetního zařízení. Jako konkrétní škody lze pro příklad uvést editaci nebo mazání dat, odposlouchávání veškeré komunikace napadeného zařízení, neautorizovaný přístup k zařízení a jiné nepříjemné následky. Existuje mnoho typů malwaru, jejichž název je odvozen od jejich podstaty šíření nebo činnosti. Předejít ztrátám dat, plynoucích z nakažení zařízení lze pravidelnými zálohami. (19)

Šíření malwaru

Nejčastěji se škodlivý software šíří prostřednictvím paměťových médií nebo internetu. Prostřednictvím paměťových médií se malware může dostat do zařízení již při pouhém připojením, které může být pro malware automatickým spouštěčem, může také napadat jednotlivé soubory uložené na paměťovém médiu, které se do zařízení dostanou při kopírování, nebo může uživatel nainstalovat neznámou aplikaci z paměťového média, která taktéž může být napadena. Prostřednictvím internetu se malware může šířit přes elektronickou komunikaci, zejména nevyžádanými emaily s přílohami nebo s odkazy na nedůvěryhodné webové stránky (nedůvěryhodné webové stránky nemají certifikát zabezpečení, to znamená, že ve webovém prohlížeči se nevyskytuje před samotnou webovou adresu https://, pro příklad zabezpečená stránka má tvar https://www.nejakastranka.cz/ a nezabezpečená http://www.nejakastranka.cz/ nebo čistě www.nejakastranka.cz).

Základní skupiny malware

V této části se vyskytují základní skupiny malwaru, které byly vybrány na základě toho, aby i neproškolení uživatelé se dokázali seznámit s jejich základními typy, navzájem je odlišit a v případě, že jejich zařízení bude některým z uvedených skupin

malwaru napadnuto, dokáží určit jejich rizika a správně postupovat k eliminaci škodlivého malware.

Adware

Malware, který na základě prohlížení internetu nebo elektronické komunikace navrhuje uživateli reklamní bloky při prohlížení internetu nebo vytváří vyskakující reklamní či jinak obtěžující okna v operačním systému. Může se do počítače nainstalovat nevědomě s jiným softwarem, v současné době je při některých instalacích nabízena možnost v instalačním procesu vybrat jednotlivé komponenty instalace a předejít instalaci nevyžádaného adware. (19)

Spyware

Malware, který špehuje aktivity uživatele a následně je odesílá majiteli tohoto škodlivého software. Jedná se například o historii vyhledávaných webových stránek, o znacích zadaných prostřednictvím klávesnice, o emailovou komunikaci a mnoho dalšího. Do počítače se může nainstalovat samostatně nebo se může vyskytovat jako součást aplikací, kterou si uživatel nevědomě nainstaluje do svého zařízení. (19)

Počítačové viry

Pojmenování získaly díky podobnosti jejich šíření v elektronickém světě s reprodukčním cyklem virů v reálném světě. Viry jsou vázány na hostitele, kterým může být jakýkoliv spustitelný soubor, jejich primárním cílem je reprodukce, dostat se do co největšího možného počtu souborů, aplikací a systémů, poté vyvolávají útok, pro které byly určeny. Útoky virů mohou představovat editaci souborů nebo jejich mazání, zatěžování systémů při reprodukci viru, samovolné uživatelem neřízené spouštění animací, vyskakovacích oken nebo pouštění melodií. Pod souhrnným názvem počítačové viry se vyskytuje mnoha různých poddruhů, je dobré uvést boot viry, makroviry nebo souborové viry. (19; 18)

Počítačoví červi

Počítačoví červi mají určitou spojitost s viry, až na fakt, že nepotřebují ke svému šíření hostitele, vyskytují se jako samostatné programy nebo jako kusy kódu, které vytvářejí vlastní kopie a snaží se je po síti rozeslat na jiná zařízení, snaží se využít bezpečnostních děr softwarových systémů, nebo vytváří zadní vrátka pro další možnosti útoků. (18; 19)

Trojské koně

Jsou softwarové aplikace, které mohou vyvolávat destrukční aktivity vůči zařízení na kterém se nachází. Uživatelé zařízení nemusí být seznámeni se skutečností, že takový software mají ve svém zařízení nainstalovaný, nebo ho mají nainstalovaný úmyslně, protože se na venek tváří jako užitečná aplikace, zatímco provádí škodlivé činnosti.

Trojské koně nemají schopnost reprodukce, k jejich šíření může přispět pouze uživatel svojí činností se zařízením. Trojský kůň dokáže skenovat komunikační porty počítače, za účelem útoku prostřednictvím některého z portů, dokáží editovat a mazat data, formátovat celá záznamová média zařízení a různě narušovat práci se zařízením. (19)

Ransomware

V uplynulých letech se v mnoha informačních pramenech skloňoval pojem Ransomware kvůli jeho častým výskytům, kdy se soustředil na větší celky než obyčejné osobní počítače. Existují dva typy ransomware s odlišným chováním.

První typ omezuje funkčnost zařízení a požaduje po uživateli zaplacení částky, jedním z tohoto typu je „Policejní vir“, který vypadá jako běžné otevřené pracovní okno webového prohlížeče a je zobrazena stránka obsahující grafické prvky připomínající Policii České republiky, zároveň uživatele informuje o nelegální distribuci nebo stahování dat, informuje o existenci nezvratitelných důkazů, že se v počítači nalézá dětská pornografie a mnoho dalších falešných, nepravděpodobných informací. Zároveň nelze zavřít okno, ve kterém se tyto informace vyskytují a běžně používat počítač do doby, než bude zaplacená pokuta. Tento problém se u prvních „Policejních virů“ dal vyřešit pomocí správce úloh a následného vypnutí okna, nebo restartem počítače. Do správce úloh se lze dostat stisknutím kláves ctrl + alt + delete, poté vybrat Správce úloh a ukončit úlohy. U novějších verzí může problém přetrvávat i po restartu zařízení a je nutná obnova systému, nebo ruční odmazání ransomware. (19; 20)

Druhým typem je ransomware, který zablokuje paměťová média nebo určitá data zařízení, ale systém nechá funkční pro informování uživatele o způsobu platby a zbývajícímu času k jejímu provedení. Data jsou většinou zašifrována tak, že je lze obnovit pouze klíčem, který uživatel dostane po zaplacení výkupného útočníkovi.

Pokud uživatel zaplatí požadovanou částku na účet a v časovém rozmezí, které mu útočník určil, většinou ve virtuální měně, aby bylo zachováno anonymity útočníka, pak napadenému uživateli, po připsání částky, útočník zašle heslo k rozšifrování nebo odblokování zakázaného přístupu.

Ransomware se šíří obvykle prostřednictvím emailové komunikace, při stahování a spouštění neznámých aplikací nebo souborů.

2.5.2 Spam a scam

Následující odstavce zmiňují časté případy podvodů nebo šíření poplašných zpráv, kterými je uživatel emailových schránek, sociálních sítí a obecně internetu obklopen téměř pravidelně. Je dobré vůči nim být obezřetný a informovat se o možných nebezpečích.

Spam

Spam lze vyjádřit jako *masové šíření veškerých nevyžádaných sdělení*. Většinou se tyto zprávy, často doprovázené přílohami obsahujícími nevyžádaný software, sdílejí prostřednictvím emailových klientů, diskuzních fór, příspěvků včetně komentářů na webových stránkách a sociálních sítí, nebo přes jiné komunikační aplikace. Účelem nevyžádaných zpráv může být reklamní sdělení, šíření poplašných a nepravdivých informací nebo obchodní nabídky. Ve skutečnosti obsah těchto zpráv nemá žádnou validní hodnotu, mají pouze přinášet zisk autorovi v nejen finanční podobě. (19)

- **Hoax a Joke**

Ve své podstatě jsou tyto pojmy principiálně odvozeny od spamu. Masové šíření nevyžádaných zpráv, které mají formu počeštělé novinářské kachny nebo vtípků. Hoax může být například sdělení o zavedení povinné vojenské služby pro všechny obyvatele České republiky starších deseti let, ve skutečnosti se používá sofistikovanějších titulků a textů, ale ve výsledku mají stejnou informační váhu jako výše uvedený titulek o vojenské službě. Takovéto články jsou obvykle šířeny pomocí emailové komunikace, diskuzních fór, příspěvků na sociálních sítí a také tomu přispívá samotný lidský faktor v reálném světě. Články většinou končí slovy: „Pošli to dál! Pošli to dál, než to smažou! Lidé se musí dozvědět pravdu!“, není vhodné je dále rozesílat ani článkům příliš důvěřovat. Joke jsou aplikace, které mají ve své podstatě udělat vtípek na oběť a nemají nijak významně škodit. Často předstírají chybové hlášky nebo destrukční činnosti na zařízení a na konci obvykle zobrazí omluvnou zprávu nebo vyzradí svoji činnost. Pro uvedení příkladu se spustí program a následné odpočítávání, s informací o probíhajícím formátování disku, po odbytí poslední vteřiny se program uzavře, nebo zobrazí vtipnou odpověď a ve skutečnosti k žádnému formátování nedochází.

Scam

Scam v překladu znamená podvod, obvykle se šíří stejně jako spam, ale jeho účelem je využití praktik sociálního inženýrství na oběť, za účelem zisku financí, přístupu k datům nebo neautorizovaným přístupům do počítačových a webových aplikací. Může mít podobu podvodných nabídek jako „skvělá práce z domova na mateřské, půjčíme peníze a registry neřešíme“ a mnoho dalších, které mají v uživatelích vzbudit pocit nadšení. (19)

- **Phishing**

Phishing je název pro útok, který se může šířit jako spam a zároveň plní činnosti scamu. Podstatou útoku je si získat důvěru oběti, která projde všemi kroky připraveného scénáře útočníka, za účelem finančního zisku, zisku dat nebo infikování zařízení malwarem, který již má vlastní cíl. Pro jednodušší pochopení principu takového útoku je vhodné uvést příklad. (19)

Zde je uveden reálný příklad phishingu, který se útočník pokusil uskutečnit na autora této práce. Na webové aplikaci, která umožňuje inzerci bytů, se vyskytl inzerát: Nabízím 3+1 v klidné části Kladna, byt je plně zařízený, já nemít čas se o něj starat, protože jsem v Italy, cena je 7700,- Kč měsíčně včetně nájem + energie + internet. K bytu je garáž zdarma.“. Takovýto inzerát vzbudí u důvěřivých lidí velké reakce, vidí obrovskou příležitost, která se již nemusí naskytnout, a okamžitě kontaktují prodejce. Prodejce jim velmi rychle odpoví připravenou zprávou, může být v podobě: "Jmenuji se Flavio Alnei, jsem nyní v Italy, byt vlastním již třetím rokem, ale po dobu jeden rok jsem v Italy a jsem zde šťastný, byt raději dlouhodobě půjčuji přes Airbnb, nejkratsi doba je 3 měsíc a nejdelší 3 roky, cena je 7700 včetně všeho, posílám fotky. Pokud souhlasíte s pronájmem prostřednictvím Airbnb, kontaktujte mě. “. Po opětovném kontaktování bude chtít útočník znát některé vaše osobní informace, aby mohl vytvořit objednávku přes Aibnb. Po odeslání všech informací přijde email s odkazem na rezervaci prostřednictvím Airbnb, odkaz ve webovém prohlížeči vypadá takto: „http://airbnb.rentals-reservation.com/1/listing/96/view-oknwb029/BaQe4OrY8A#googtrans(en%7Ccs)“. V odkazu je podtržena nejdůležitější část, která informuje o skutečnosti, že se jedná o doménu třetího řádu, což by při pravém odkazu od společnosti Airbnb nebyla. V rámci otestování, zdali se jedná o phishing, byl bez zaplacení poslán útočníkovi email, že byla provedena platba, během půl hodiny dorazil autorovi email, jehož emailová adresa obsahovala tvar podobný oficiálnímu emailu Airbnb, nicméně nebyla úplně ve správné formě, s potvrzením přijetí platby a požádání o trpělivost, než se ozve zástupce společnosti pro předání klíčů. Nebylo potřeba posílat platbu, pouze útočníka informovat a posléze přišla informace o uskutečněné rezervaci. Tímto došlo k odhalení, že se jedná o phishingový útok, a nikoliv o seriózní nabídku pronájmu. Bohužel mnoho důvěřivých lidí na podobné podvodníky inzerující pronájmy nebo prodeje již narazilo a je důležité šířit mezi nimi osvětu.

Společnost Airbnb na svých webových stránkách informuje uživatele, že platba může být provedena pouze prostřednictvím jejich vlastních zabezpečených stránek, nejdříve však po potvrzení rezervace. Společnost má na svých webových stránkách informace o možných podvodnících a pokyny, jak je poznat. (21)

2.5.3 Antivirová ochrana a detekce škodlivého softwaru

Antivirovou ochranu lze definovat jako software, který dokáže detekovat a eliminovat škodlivý software v zařízení. Dokáže skenovat současný obsah záznamových médií a chránit zařízení při prohlížení internetu a zaručit síťovou ochranu, která filtruje a detekuje komunikaci zařízení po síti. Existuje mnoho antivirových programů a není vždy snadné vybrat ten nejideálnější. Je možné vyhledat podle nezávislých srovnávacích serverů tu nejlepší antivirovou ochranu, která může být dostupná zcela zdarma, zdarma bez vybraných funkcí, nebo celá zpoplatněna. Vzhledem k nabízeným rozšířeným funkcím, které jsou dostupné pouze při zakoupení licence, je doporučené používat

zpoplatnění antivirové aplikace. Mezi možné rozšířené funkce patří Anti-Theft, který dokáže vystopovat a monitorovat zařízení v případě jeho ztráty, dále Ochrana bankovnictví a online plateb a několik dalších funkcí přispívajících k maximální možné ochraně dat uživatele a celého zařízení. Pro návody v praktické části byla použita antivirová aplikace Eset Smart Security (dostupné z: https://www.eset.com). Byla zvolena nejen kvůli jejímu původu, společnost má své kořeny v Československu, ale také kvůli popularitě mezi uživateli a významnou pozicí mezi ostatními antivirovými aplikacemi. Společnost vlastnící tento antivirový software nabízí slevu pro studenty.

Samotný princip činnosti antivirové ochrany spočívá ve skenování veškerých souborů a činností uživatele, během kterého porovnává záznamy s virovou databází. Pokud identifikuje podobnost, pak informuje uživatele a podezřelý soubor uzavře do karantény, kdy je možné poslat tvůrcům zprávu o detekci, smazat podezřelý soubor, nebo ho odstranit z karantény a nechat v zařízení. Z důvodu principu činnosti je důležité pravidelně antivirovou aplikaci aktualizovat pro zajištění aktuální virové databáze.

2.5.4 Jak předejít útokům

V prvé řadě je nutné uvažovat s čistou hlavou a podle svých nejlepších zkušeností a znalostí se při používání výpočetního zařízení chovat obezřetně. Nespouštět a nestahovat neznámé soubory, nenavštěvovat nedůvěryhodné webové stránky a nestahovat z nich obsah, nepřipojovat neznámá paměťová média do zařízení určeného pro běžnou práci, pravidelně aktualizovat operační systém, jeho aplikace a antivirovou ochranu. Být obezřetný vůči lidem, kteří mohou aplikovat praktiky sociálního inženýrství pouze pro jejich zisk.

2.6 Průzkum současného stavu v rámci kybernetické bezpečnosti a proškolení zdravotnického personálu

2.6.1 Cíle dotazníku

Posledním z uvedených cílů práce byl průzkum úzkého kruhu respondentů pracujících s výpočetní technikou ve zdravotnictví ohledně jejich znalosti kybernetické bezpečnosti a znalosti jejich zařízení. Je nutno uvést, že tato anketa je pouze informativního charakteru a výsledky průzkumu nelze označit za jednoznačné dogma, pro zajištění maximálně relevantních výsledků by bylo potřeba vypracovat složitější studii, která by zahrnovala řádově mnohem vyšší a sofistikovanější výběr okruhu respondentů, než bylo zvoleno zde. Tato práce může přispět k vytvoření budoucí relevantní studie.

2.6.2 Vybírání respondentů a určení otázek

Dotazník byl určen pro lékaře a sestry, které aktuálně pracují ve zdravotnickém zařízení a používají výpočetní techniku. Dotazník byl k dispozici v papírové i elektronické formě. Pro eliminování nerelevantních odpovědí prostřednictvím elektronické formy byla vytvořena otázka, jejíž odpověď byla určující pravdivost celého vyplnění dotazníkového formuláře. Papírovou formu dotazníku dostal a vyplnil každý respondent přede mnou, aby bylo průkazné, že respondent pochází ze zdravotnického prostředí a nenechal dotazník vyplnit někým jiným.

Dotazník byl zcela anonymní, jediné získané osobní informace se týkaly věku, pohlaví a pracovní pozice. Při výběru otázek byl kladen důraz na základní znalosti respondentova zařízení, softwarového prostředí, ve kterém respondenti pracují, zdali pravidelně mění svá hesla a odhlašují se z aplikací a otevřené zmapování jejich připomínek k jednotlivým bodům.

Výsledky jsou zpracovány pomocí webového formuláře Google Forms, jehož prostřednictvím mohly být vyplňovány elektronické dotazníky, a protože samotná webová aplikace nabízí přehledné zpracování v grafech. Písemně vyplněné dotazníky jsou odděleny od elektronických dotazníků prostřednictvím doplňující pravdivostní otázky. Celkové vyhodnocení dotazníku se vyskytuje v praktické části této práce.

2.6.3 Výběr otázek

Otázky byly vybírány na základě primárního určení cíle, kterým bylo zmapovat základní kybernetické znalosti a návyky zdravotnického personálu. Otázky byly konzultovány s vedoucí práce a jejich cílem bylo zhodnotit současný stav.

Osobní otázky

Dotazník byl zcela anonymní, jediné osobní otázky sloužící pro sběr byly následující: ”Jakého jste pohlaví? Kolik Vám je let? a Na jaké jste pracovní pozici?“. Otázky byly vytvořeny pro vypracování závěrečného zhodnocení skupin.

Otevřené otázky

Byla potřeba přímá interakce respondentů s dotazníkem, proto byly zvolené otevřené otázky, na které je potřeba odpovědět a otevřené podotázky, na které respondenti odpoví v případě podmínečné odpovědi. Výčet otevřených otázek:“ Co je pro vás největší problém při práci s Vaším zařízením? V jaké pracujete aplikaci a pracuje se Vám v ní dobře? “. Otevřené podotázky se vyskytují u některých znalostních otázkek.

Znalostní otázky

Smyslem znalostních otázek bylo dozvědět se o kybernetických znalostech respondentů a jejich návyků. Jedná se o otázky: „Jaké zařízení převážně používáte pro vykonávání vaší práce? Považujete ovládání vašeho zařízení za vyhovující pro zpracovávání údajů k vykonávání Vaší práce? V jaké pracujete aplikaci a pracuje se vám v ní dobře? Byl/a jste proškolen/a pro práci se zařízením, které pro svoji práci používáte? Máte v zařízení nainstalovaný antivirový program? Obměňujete někdy přístupová hesla k počítači a aplikacím? Odhlašujete se z aplikací v případě, kdy plánovaně opouštíte pracovní místo na dobu delší než 5 minut?“ Některé z otázek obsahují otevřené podotázky, na které v některých případech bylo potřeba odpovědět kvůli upřesnění odpovědi.

3 Návody navazující na teoretickou část a vyhodnocení ankety

V této části práce jsou podrobně popsány praktické návody vztahující se k teoretické části

3.1 Autentizace prakticky

V teoretické kapitole byly popsány jednotlivé způsoby autentizace a vysvětlena nejčastější rizika spojená s autentizací. Následující návody lze využít ke zkvalitnění hesel nebo ke zjištění, zdali heslo k emailu nebylo v minulosti prolomeno a následně vyvěšeno na internetu.

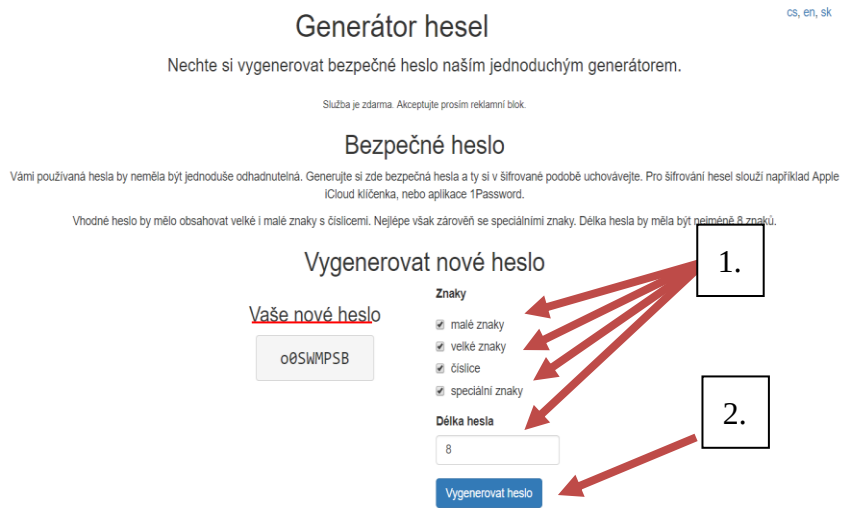
3.1.1 Generování silného hesla

Pokud jsou známy základní pravidla pro tvorbu silného hesla, tak není nutno používat samostatné aplikace pro jejich vytvoření, ale pokud si uživatel není moc jistý, popřípadě ho žádné konkrétní heslo nenapadá, tak mu může pomoci generátor hesel. V následujících dvou částech je podrobný návod pro generování silného hesla pomocí webové i počítačové aplikace.

Generování silného hesla webovou aplikací

Pomocí webového prohlížeče je možné nalézt řadu generátorů silných hesel, pro následnou ukázku jsem použil generátor hesel ze stránky www.generator-hesel.cz. (22)

1. Otevřít webovou stránku www.generator-hesel.cz ve webovém prohlížeči.
2. Vybrat **veškeré možnosti k zabezpečení hesla**. (Krok č. 1)
3. Kliknou na **Vygenerovat heslo** a následně se naučit nové heslo (Krok č. 2)

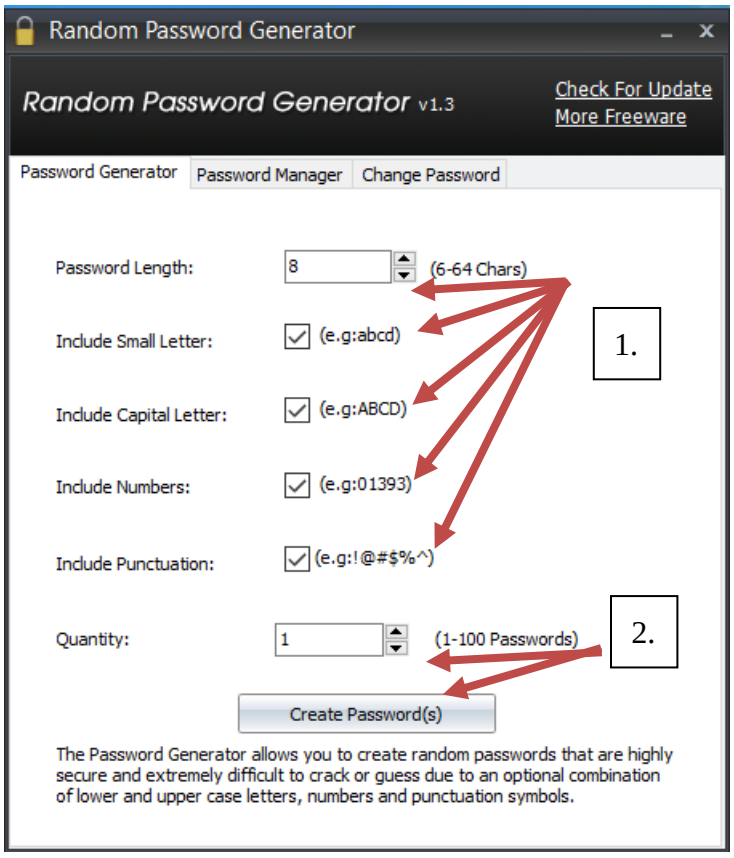


Obrázek 1 - Generování hesla webovou aplikací

Generování hesla počítačovou aplikací

Jako první je nutné nainstalovat program, který zvládá generovat náhodná hesla. Pro demonstraci příkladu jsem si zvolil program Random password generator, který je dostupný zdarma z https://www.iobit.com/en/passwordgenerator.php .

1. Po spuštění programu vybrat kartu **Password generator**
2. Vybrat parametry pro generaci hesla z široké nabídky (doporučuji vybrat vše) (krok č. 1)
3. Lze si zvolit generování více hesel najednou. (Krok č. 2)



Obrázek 2 - Generování hesla počítačovou aplikací

4. Kliknout na **Create Password(s)** a následně si uložit hesla do manažera hesel nebo si zapamatovat nová hesla.

3.2 Elektronické podepisování prakticky

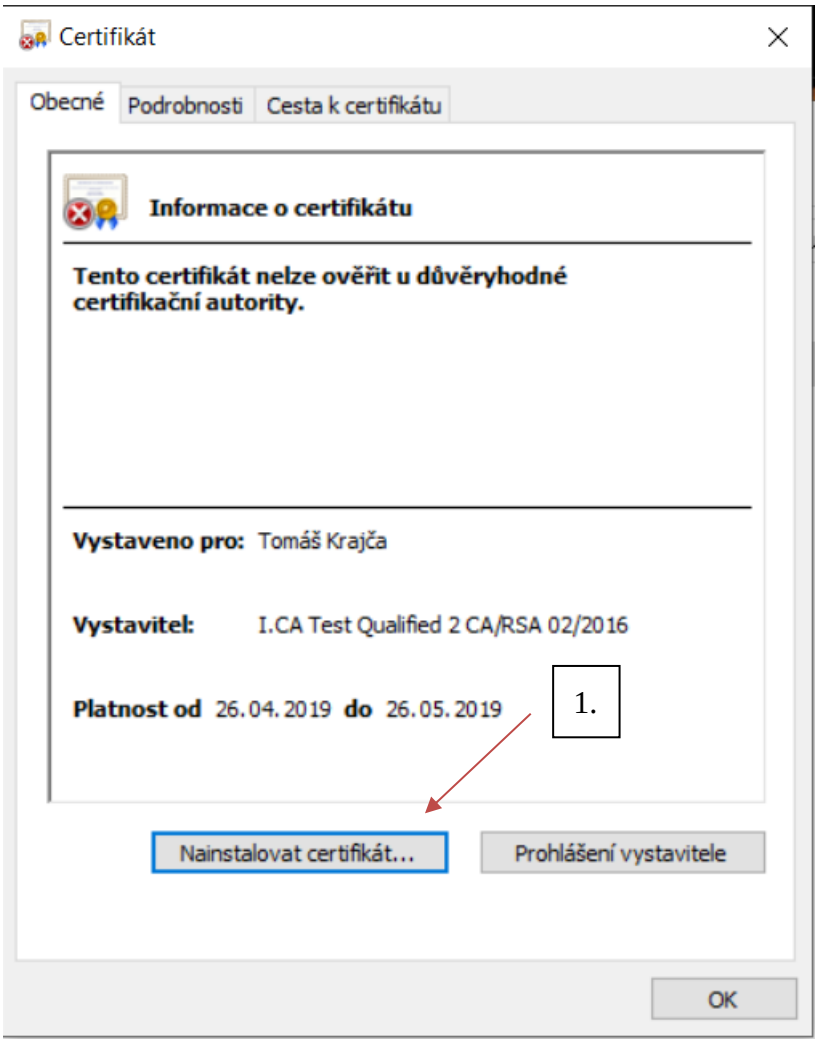
Následující odstavce obsahují návody pro instalaci elektronického certifikátu do operačního systému Windows 10 a do vybraných webových prohlížečů, pro podepisování emailu poštovním klientem Microsoft Outlook a podepisování pdf dokumentu v aplikaci Acrobat Adobe Reader.

3.2.1 Instalace elektronického certifikátu do operačního systému Windows 10

V prvé řadě je nutné elektronický certifikát vlastnit. Pro vytváření návodů byl použit testovací certifikát vydaný První certifikační autoritou (www.ica.cz).

1. Dostat se do umístění certifikátu a poté ho spustit

2. Vybrat možnost: **Nainstalovat certifikát.** (Krok č. 1)



Obrázek 3 - Instalace elektronického certifikátu

3. Vybrat, zda certifikát instalovat pouze pro konkrétního přihlášeného uživatele operačního systému, nebo pro všechny uživatele zařízení.
4. Nechat instalační službu automaticky zvolit nejvhodnější adresář pro uložení certifikátu.
5. Potvrdit vybrané možnosti, instalační služba se o vše postará.

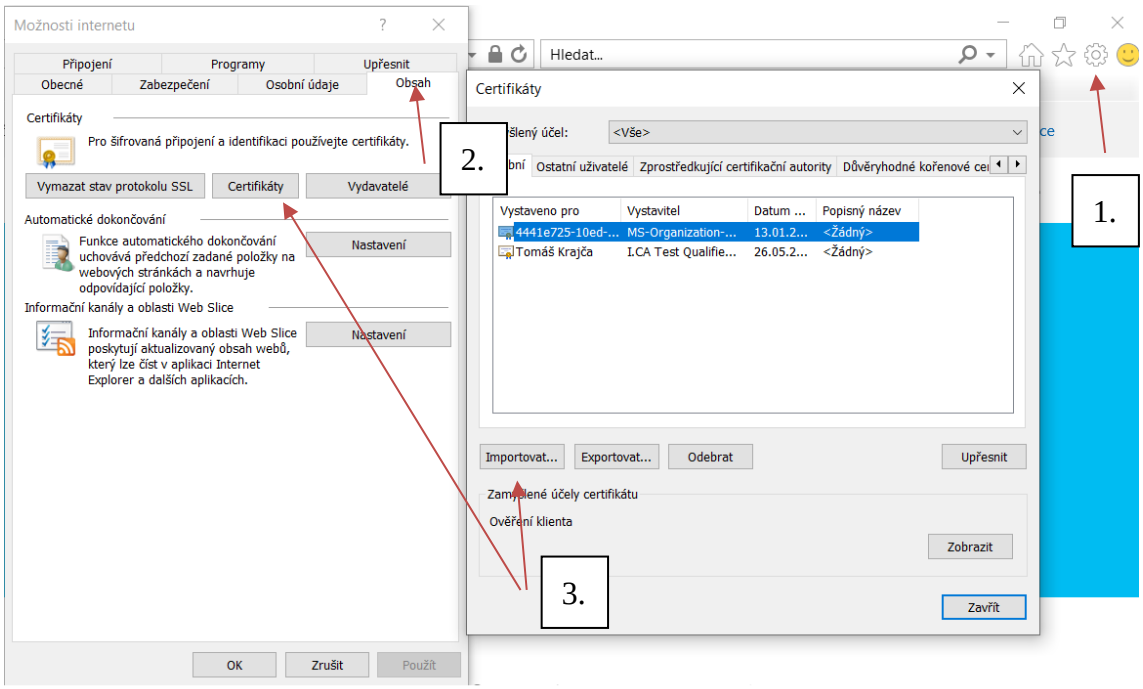
Nyní je elektronický certifikát úspěšně nainstalován do vašeho zařízení.

3.2.2 Instalace elektronického certifikátu do webových prohlížečů

Instalace certifikátů do webových prohlížečů může být klíčová pro přihlašování do webových služeb, vyžadující autentizaci pomocí elektronického certifikátu.

Instalace certifikátu do webového prohlížeče Internet Explorer

1. Otevřít webový prohlížeč Internet Explorer a kliknout na **ozubené kolečko s nastavením prohlížeče**. (Krok č. 1)
2. V nabídce vybrat **Možnosti internetu** a rozbalit kartu **Obsah** (Krok č. 2)
3. Kliknout na **Certifikáty** a v nově otevřeném okně vybrat **Importovat**, poté vybrat konkrétní certifikát, nechat průvodce importu vybrat automaticky úložiště pro certifikát, a následně dokončit celý proces. (Krok č. 3)

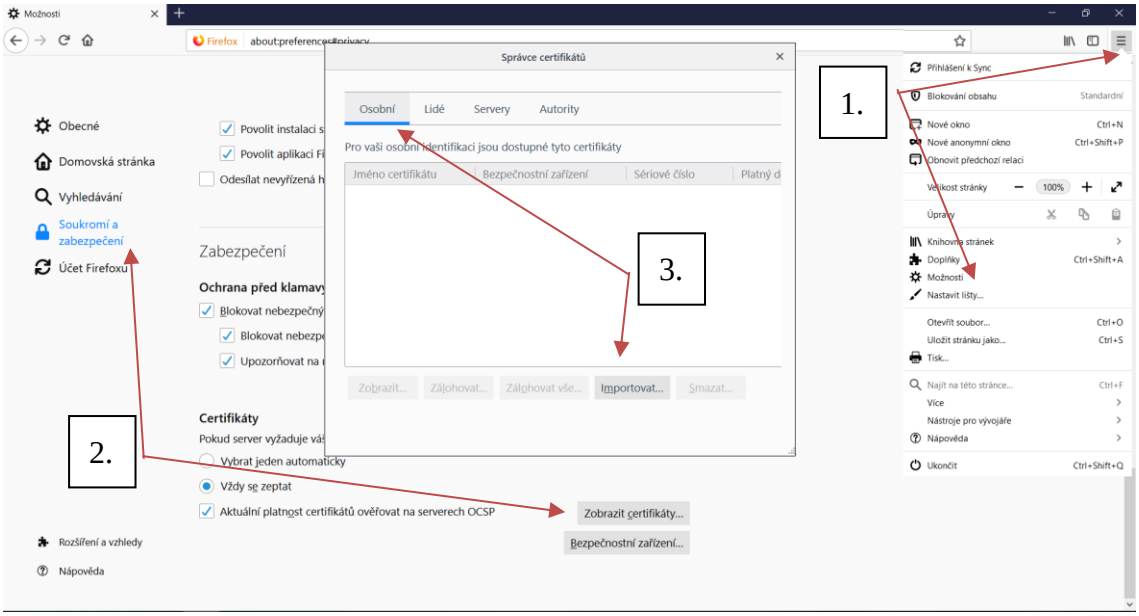


Obrázek 4 - Instalace elektronického certifikátu do Internet Explorer

Nyní je elektronický certifikát nainstalován do webového prohlížeče Internet Explorer.

Instalace certifikátu do webového prohlížeče Mozzila Firefox

1. Spustit prohlížeč Mozzila Firefox, kliknout na **Nastavení** a vybrat záložku **Možnosti**. (Krok č. 1)
2. Na levém panelu zvolit kartu **Soukromí a zabezpečení**, níže se vyskytuje oddíl pro certifikáty, který lze zobrazit. (krok č. 2)
3. Po zobrazení certifikátu je možné v dialogovém okně zvolit **Osobní certifikáty** a následně zvolený certifikát **importovat** z umístění ze záznamového média. (Krok č.3)



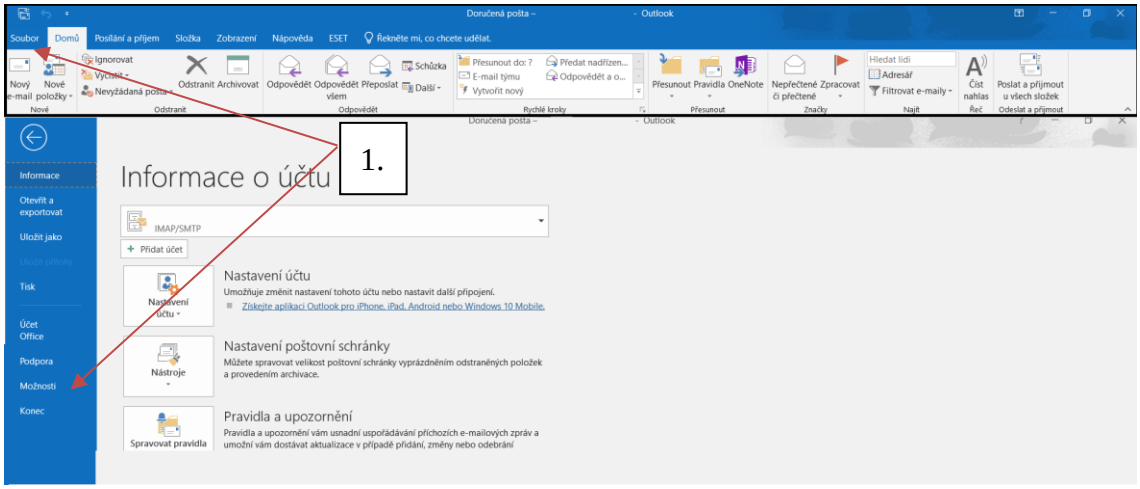
Obrázek 5 - Instalace elektronického certifikátu do Mozzila Firefox

3.2.3 Instalace certifikátu a podepisování pomocí poštovního klienta Microsoft Outlook

Nainstalovaný certifikát v poštovním klientovi umožňuje podepisování elektronických zpráv, je to nutné pro komunikaci se státní správou a jinými institucemi nebo subjekty vyžadujícími elektronické ověření odesílatele. Aplikaci Microsoft Outlook je možné mít nainstalovanou pouze v rámci operačního systému Windows.

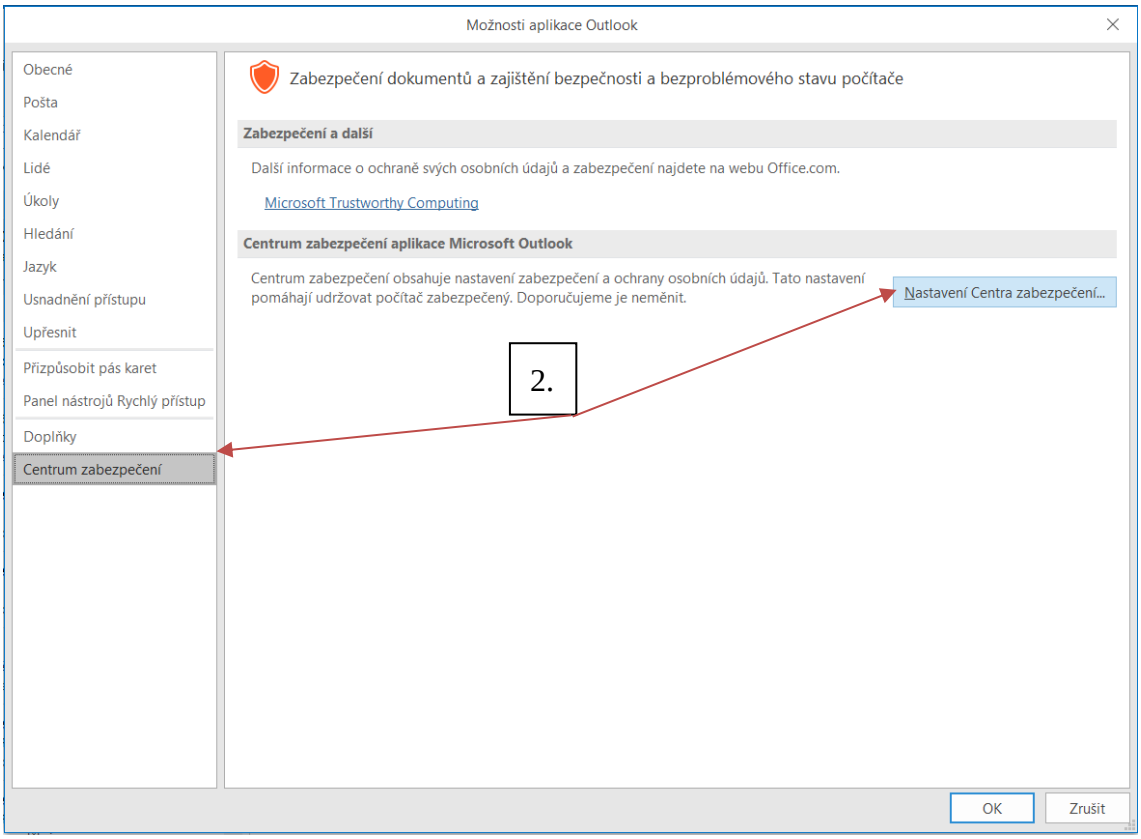
Instalace certifikátu do poštovního klienta Microsoft Outlook

1. Spustit aplikaci, vybrat v horní liště kartu **Soubor** a kliknout na **Možnosti**. (Krok č. 1)



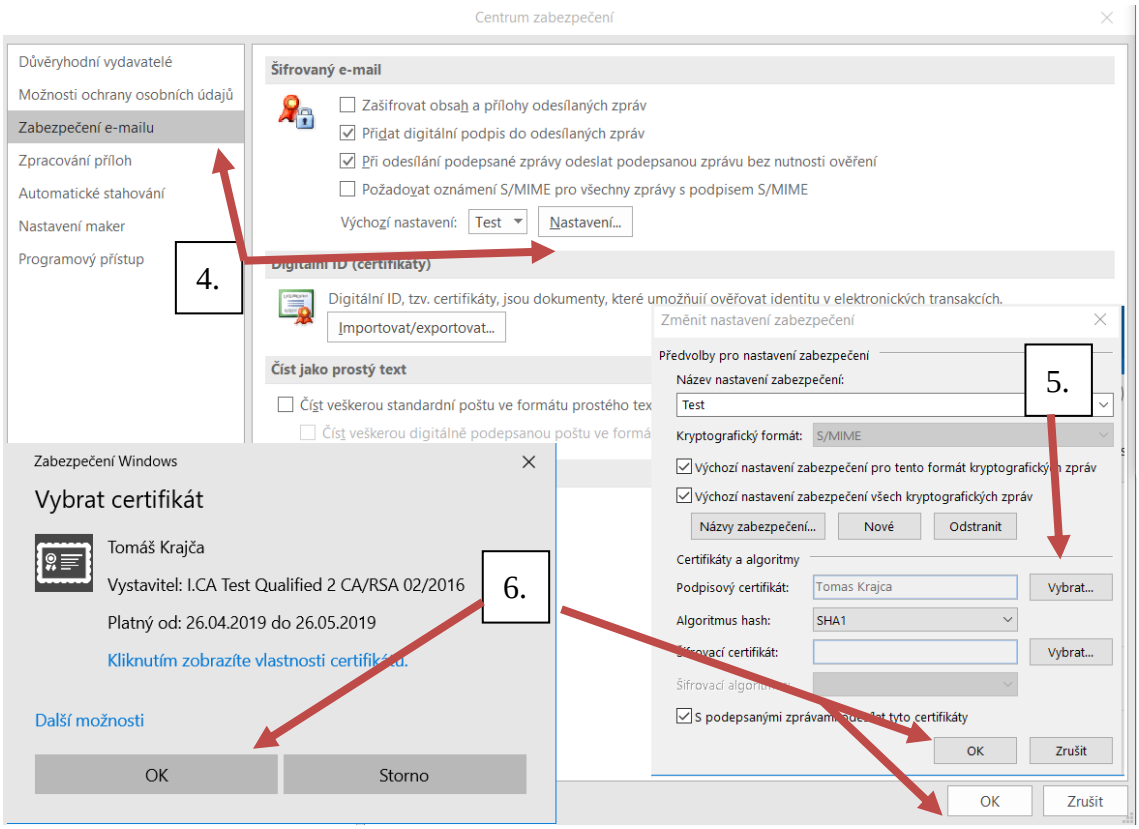
Obrázek 6 - Instalace certifikátu do MS Outlook

2. Otevře se nové okno, v levém panelu vybrat **Centrum Zabezpečení** a kliknout na **Nastavení Centra zabezpečení.** (Krok č. 2)



Obrázek 7 - Instalace certifikátu do MS Outlook

3. V levém panelu vybrat **Zabezpečení emailu** a poté kliknout na **Nastavení** v oddílu **Šifrovaný e-mail**. Následně zvolit **Vybrat** a potvrdit vybraný certifikát, poté uložit. (krok č. 4,5,6)



Obrázek 8 - Instalace certifikátu do MS Outlook

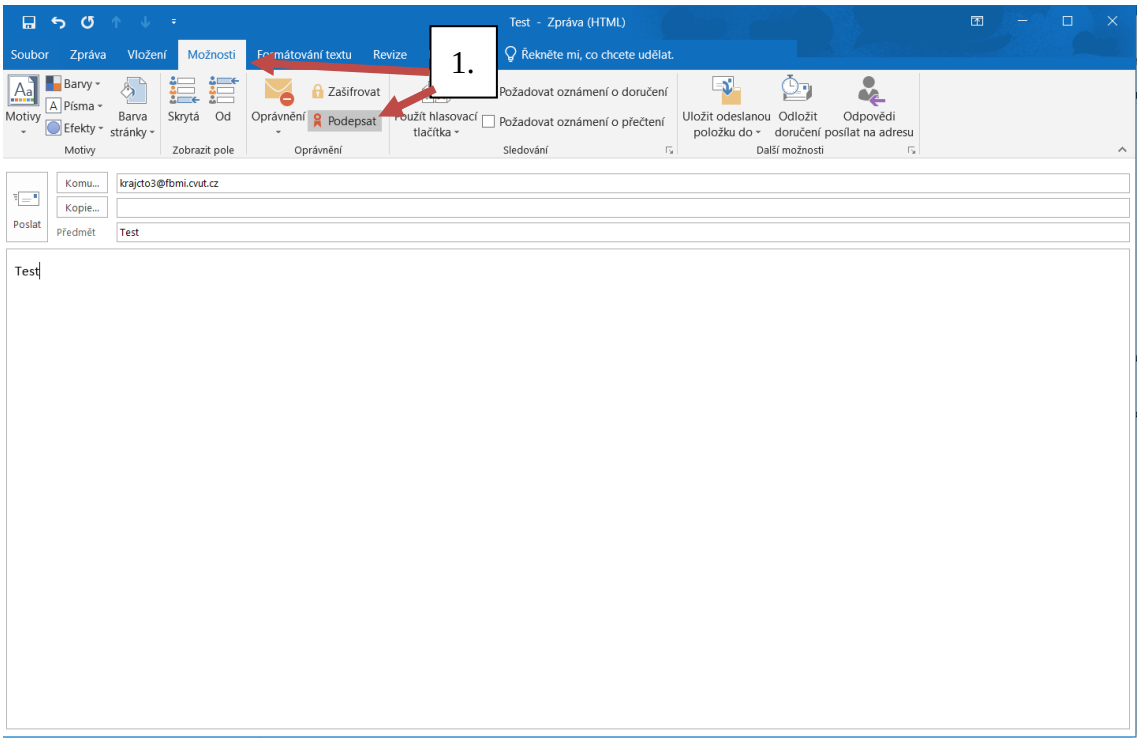
Právě byl certifikát importován do aplikace Microsoft Outlook a je připraven k použití

3.2.4 Podepisování emailu pomocí poštovního klienta Microsoft Outlook

Podepisování emailů musí předcházet instalace certifikátu do operačního systému a následné importování do poštovní aplikace.

1. Spustit aplikace Microsoft Outlook a přihlásit se účtem, ke kterému patří elektronický certifikát.
2. Vybrat záložku **Nový e-mail** a následně jej vytvořit.

3. Před odesláním emailu zvolit kartu **Možnosti** a kliknout na **Podepsat**. (krok č. 1)



Obrázek 9 - Podepisování emailu pomocí MS Outlook

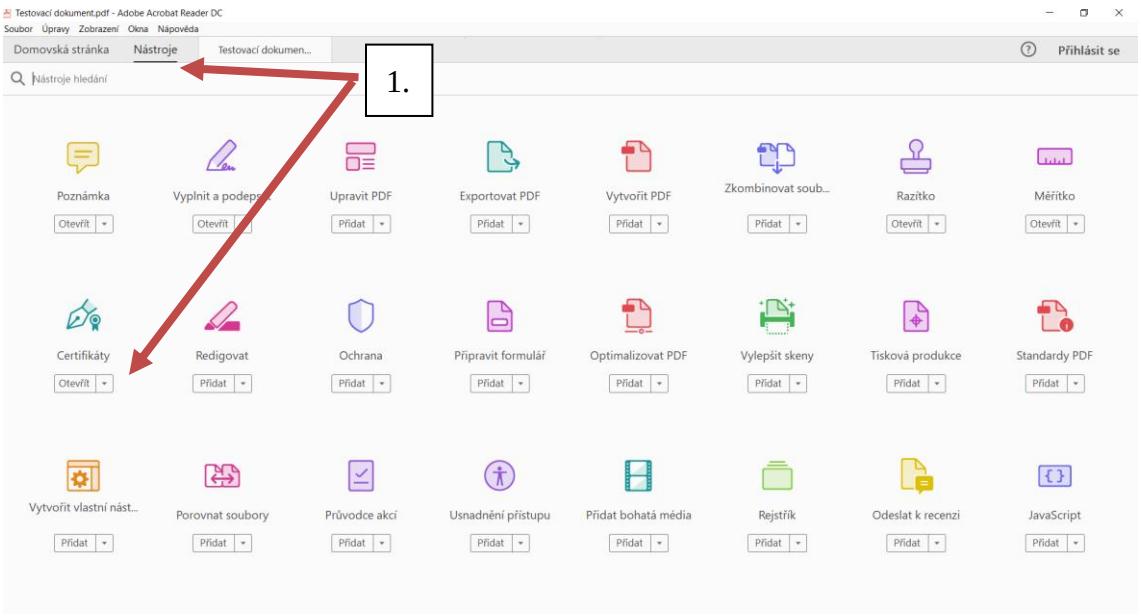
4. Po odeslání bude email podepsaný.

3.2.5 Podepisování dokumentu ve formátu .pdf

Tento návod popisuje způsob, jakým lze podepisovat pdf dokumenty prostřednictvím aplikace Adobe Acrobat Reader. Podepisování dokumentů zvyšuje důvěryhodnost celého obsahu dokumentu a lze s ním jednoznačně spojit podepisujícího jedince.

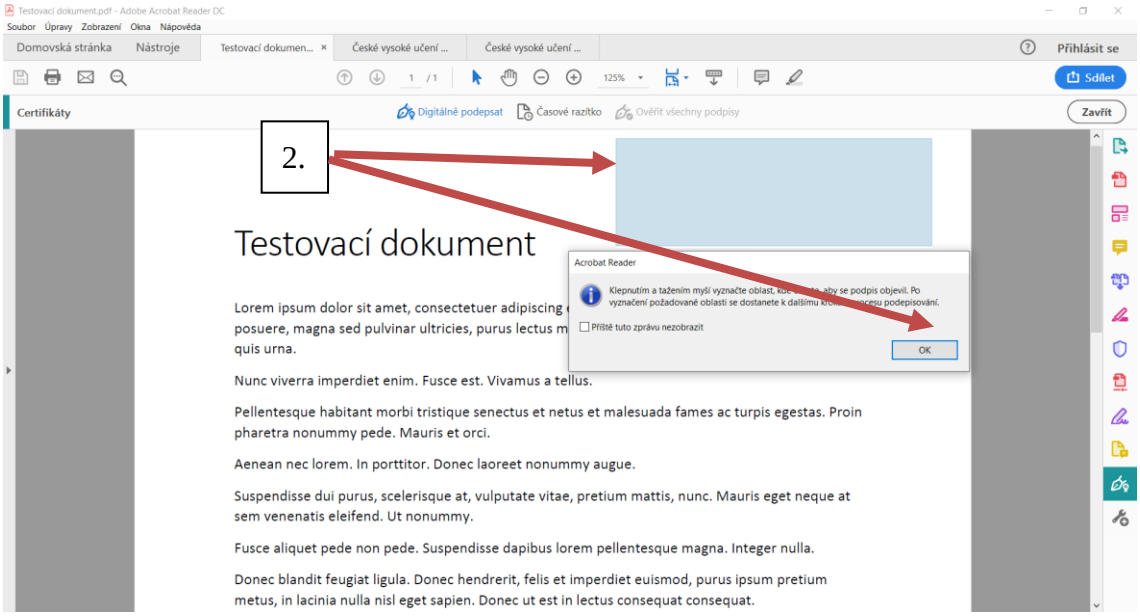
1. V prvé řadě musí být nainstalována aplikace Adobe Acrobat Reader (dostupná z https://www.adobe.com/) a je potřeba mít připravený pdf dokument, který má být podepsán.
2. Spustit aplikaci Adobe Acrobat Reader a otevřít v ní soubor. Popřípadě otevřít soubor napřímo, pokud je Acrobat Reader nastaven jako výchozí aplikace pro otevírání pdf dokumentů.

3. Kliknout na **Nástroje**, vybrat ikonu s **Certifikáty** a **Otevřít**. (Krok č. 1)



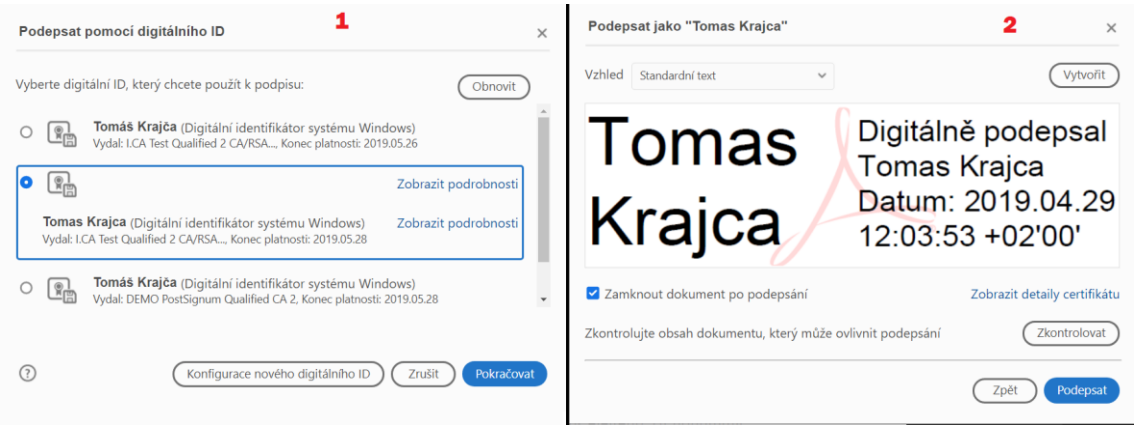
Obrázek 10 - Podepisování PDF dokumentu

4. Uživatel je vyzván k označení místa pro podpis, lze vybrat libovolné místo pomocí polohovacího zařízení a poté potvrdit. (Krok č. 2)



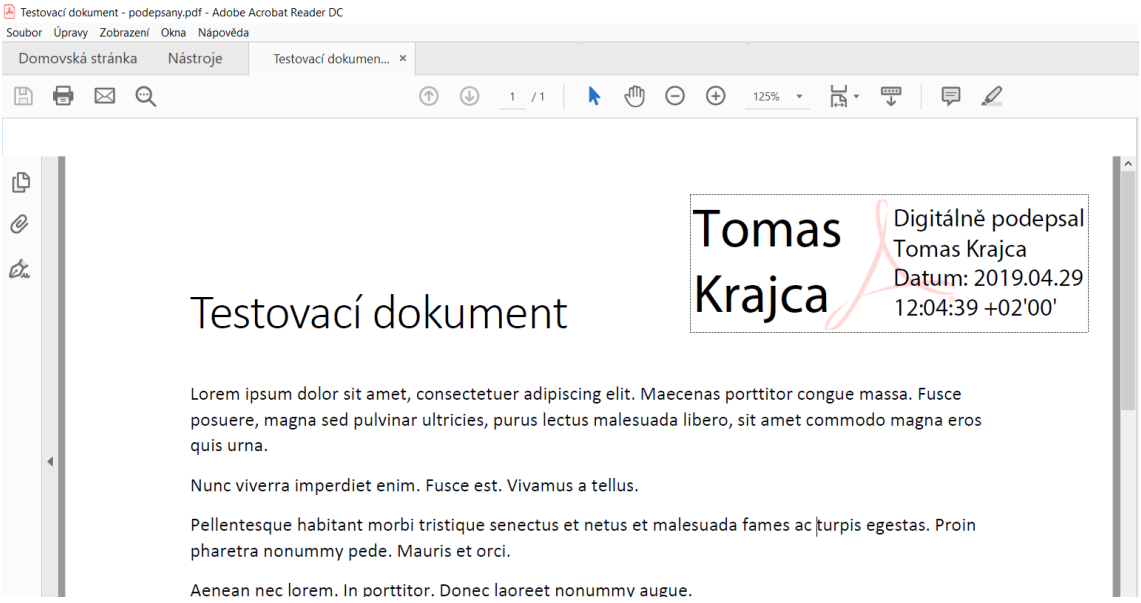
Obrázek 11 - Podepisování PDF dokumentu

5. Po vybrání pozice pro podpis následuje výběr certifikátu (krok č. 1) a nastavení jeho vzhledu (krok č. 2). Po splnění úkonů **Podepsat**.



Obrázek 12 - Podepisování PDF dokumentu

6. Dokument je tímto podepsaný, výsledný dokument pak vypadá následovně. (Obrázek č. 14)



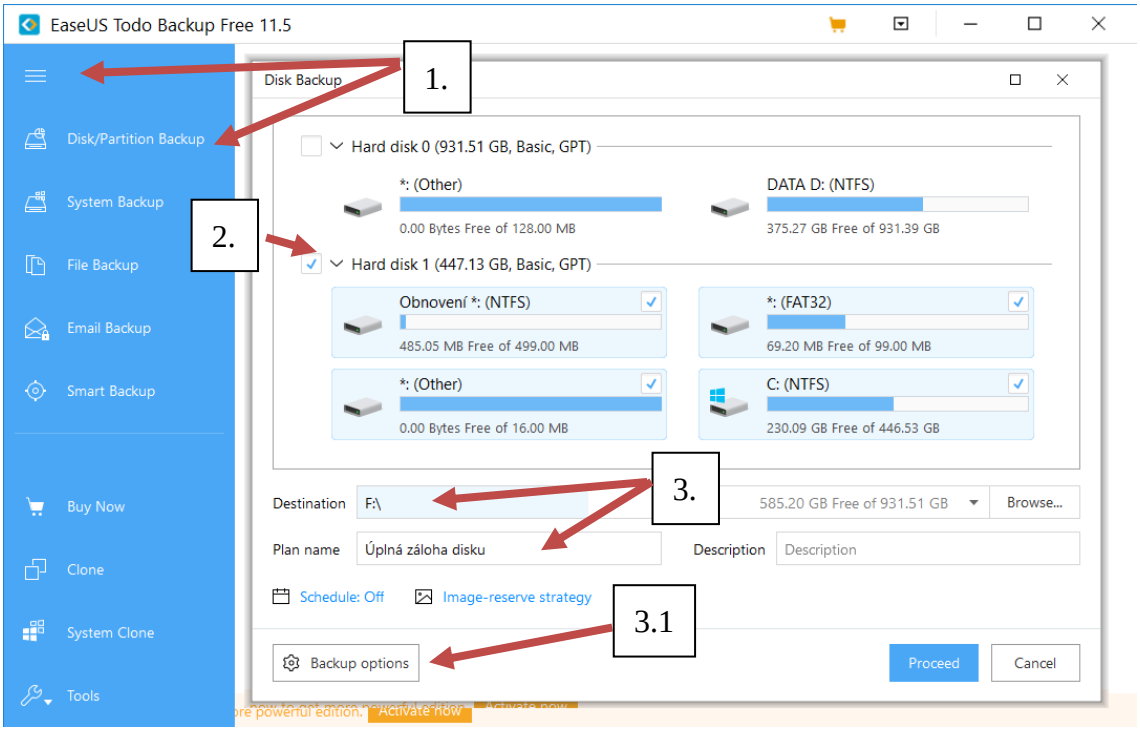
Obrázek 13 - Podepisování PDF dokumentu

3.3 Zálohování prakticky

Pro příklad vytvoření zálohy je použita aplikace EasyUS Todo Backup Free (dostupné z https://www.easeus.com/), jenž byla pro rok 2019 ohodnocena jako nejideálnější, zdarma nabízená zálohovací aplikace podle serveru Techradar.pro, lze si doplatit prémiový účet pro získání rozšířených možností, ale zdarma nabízená verze pro zálohování dat postačí. (23)

3.3.1 Návod pro provedení úplné zálohy pevného disku osobního počítače a její zašifrování

1. Nainstalovat aplikaci EasyUs Todo Backup Free a spustit.
2. Odkrýt rozbalovací nabídku a vybrat **Disk/Partition Backup**, což v překladu znamená záloha Disku nebo jeho oddílu. (Krok č. 1)

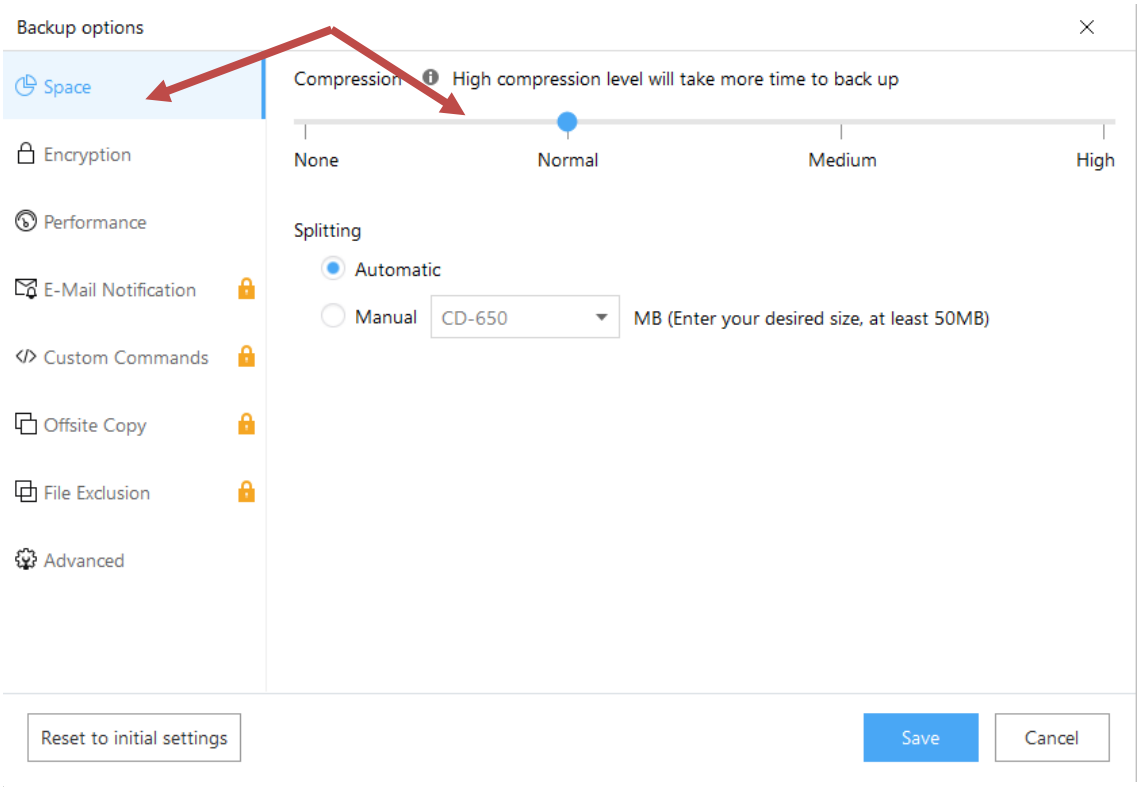


Obrázek 14 - Úplná záloha pevného disku

3. Vybrat oddíl disku nebo celý disk určený k zálohování (Krok č. 2), vybrat místo uložení zálohy (v tomto případě na externí paměťové úložiště) a pojmenování zálohy (Krok č.3). Následně kliknout na **Proceed**, které spustí celý zálohovací proces.

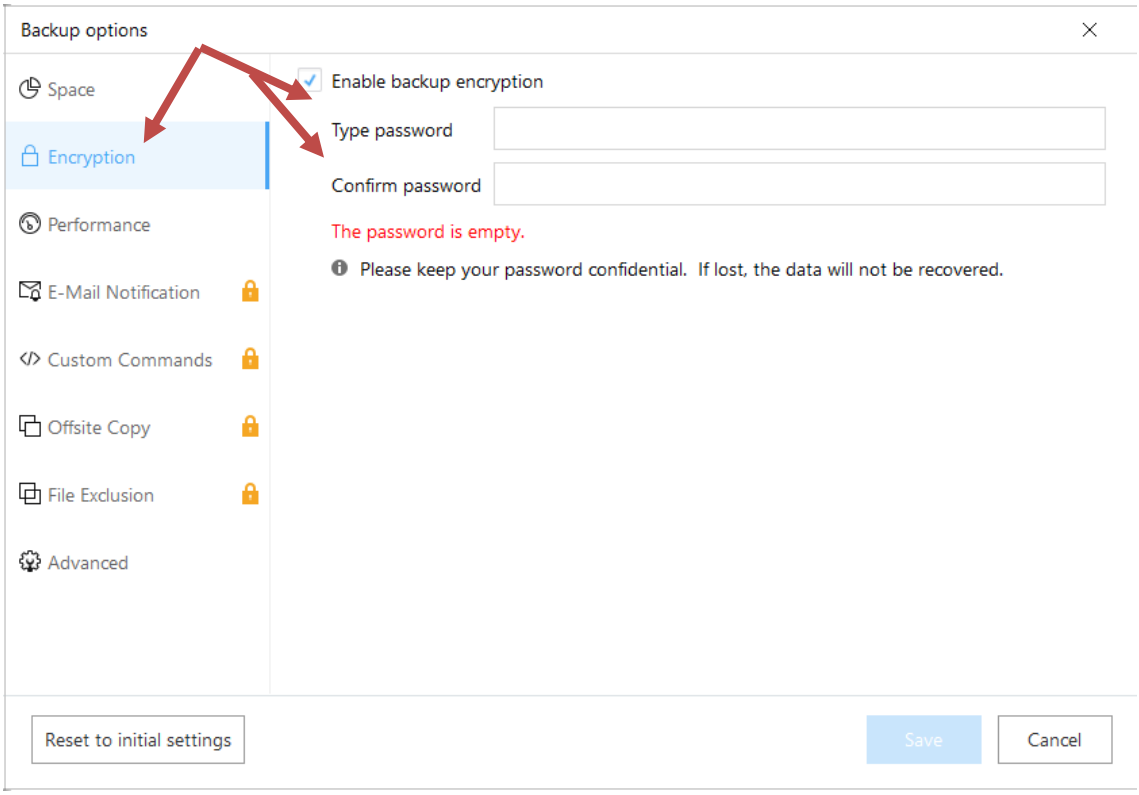
3.1 V případě, že chceme nastavit co možná největší kompresy zálohovaných dat, což znamená snížení kapacitního objemu výsledné zálohy, nebo chceme nastavit šifrování pro zálohu, tak kliknout na **Backup options**, v překladu nastavení zálohy. (Krok č. 3.1)

3.2 Pokud je žádoucí snížit objem zálohy, kliknout na **Space**, v překladu místo a vybrat požadovanou kompresy. S vyšší kompresí stoupá také čas potřebný k vytvoření zálohy. Následně uložit změny. (Obrázek č. 16)



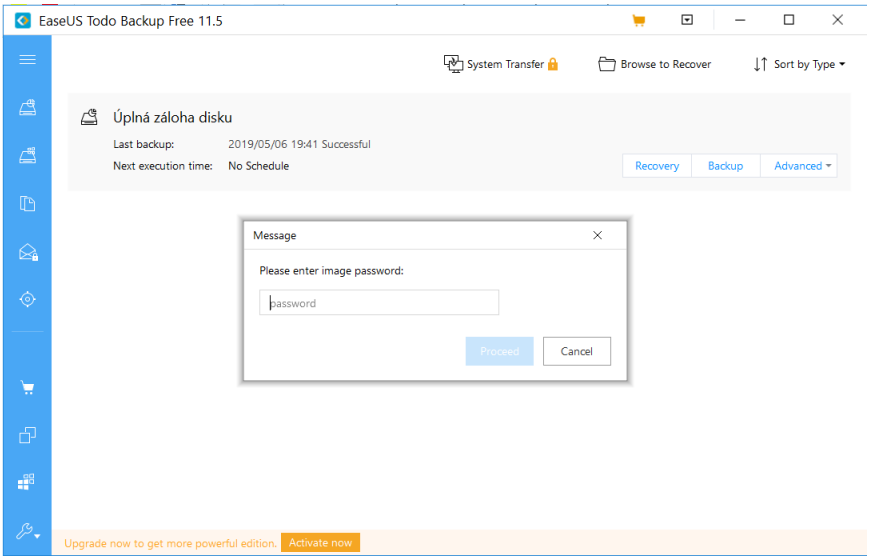
Obrázek 15 - Úplná záloha pevného disku

3.3 Pokud je žádoucí data zašifrovat, kliknout na **Encryption**, v překladu Šifrování. Povolit jej a zvolit heslo pro šifrování. Následně uložit změny. (Obrázek č. 17)



Obrázek 16 - Úplná záloha pevného disku

4. Záloha je nyní provedena, je možné ji obnovit, nebo vytvořit novou zálohu. Pokud bylo zaškrtnuto šifrovat data, tak při následné obnově budete muset zadat heslo. (Obrázek č. 18)



Obrázek 17 - Úplná záloha pevného disku

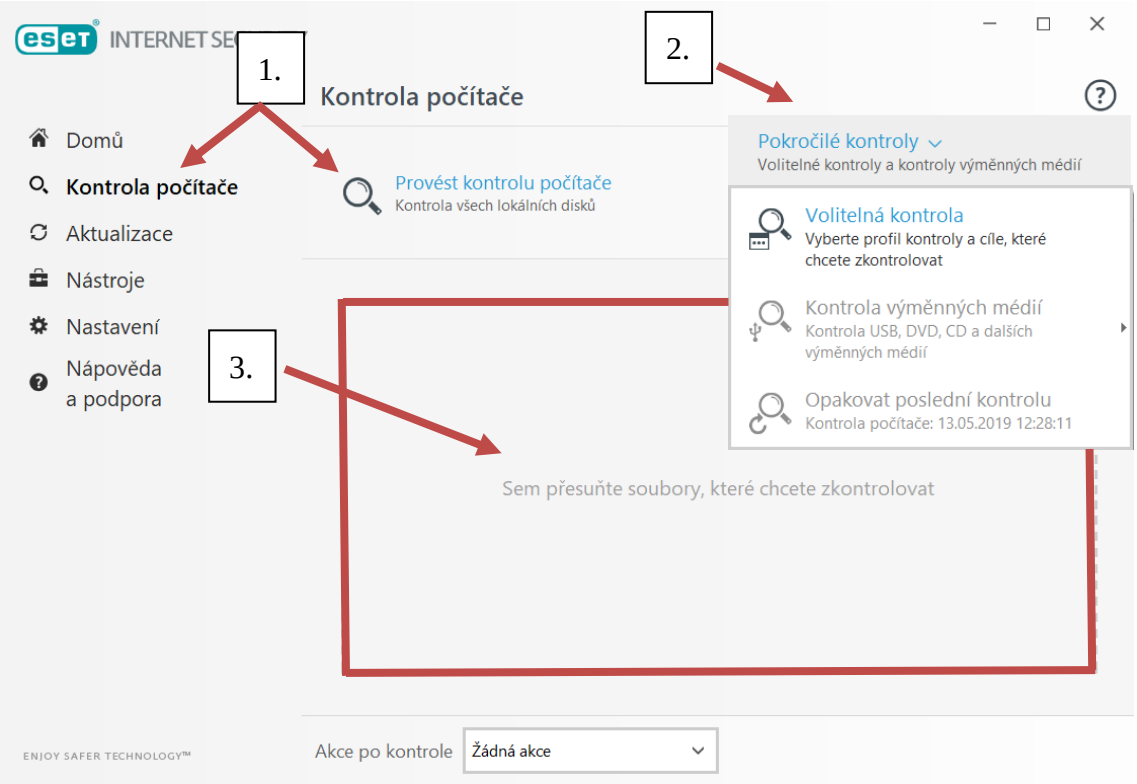
3.4 Použití antivirové programu a anti-malware

Tato kapitola obsahuje skenování počítače antivirovou aplikací a skenování zařízení aplikací pro detekci malware.

3.4.1 Skenování počítače antivirovou aplikací

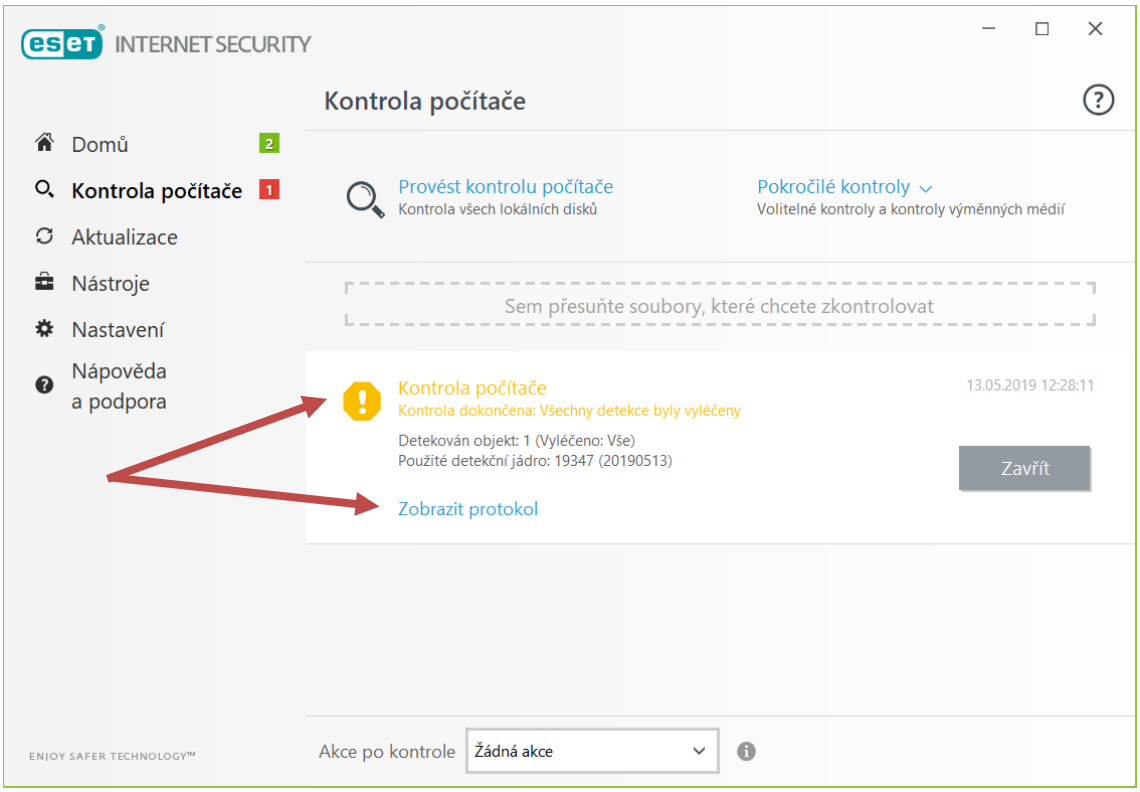
Pro skenování zařízení byla použita antivirová aplikace Eset Smart Security. Skenování počítače za účelem detekování a eliminace hrozeb je vhodné provádět alespoň jednou měsíčně. Při skenování zařízení lze pokračovat v běžné práci na zařízení, avšak může dojít k poklesu výkonu zařízení při používání dalších aplikací, kvůli probíhající činnosti antivirové aplikace.

1. Spustit antivirovou aplikaci Eset Smart Security.
2. Vybrat **Kontrola počítače** a následně kliknout na **Provést kontrolu počítače**. (Krok č. 1).
3. Lze vybrat kontrolu jednotlivých interních nebo externích záznamových médií po rozbalení nabídky Pokročilé kontroly (Krok č.2).
4. Je také možné zkontrolovat samotné jednotlivé soubory.
   4.1 Stačí je snadno přetáhnout na vyznačenou plochu (Krok č. 3)
   4.2 Na soubor kliknout pravým tlačítkem a v rozbalovací nabídce vybrat **Zkontrolovat pomocí Eset Smart Security**.



Obrázek 18 - Skenování zařízení antivirovou aplikací

5. Pokud je skenování dokončené, aplikace informuje uživatele o počtu nalezených hrozeb, nabídne možnosti, co s nimi provést, pro příklad uložit do karantény, pokusit se léčit soubor nebo jej vymazat. Dále je možné zobrazit protokol o celém průběhu kontroly (Obrázek č. 19).



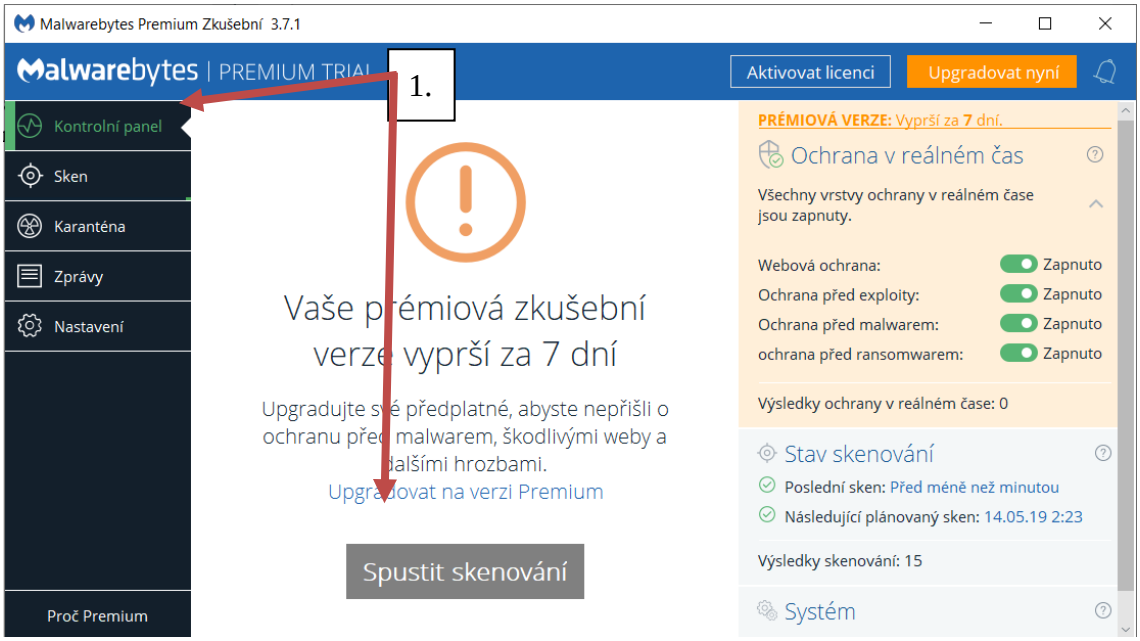
Obrázek 19 - Skenování počítače antivirovou aplikací

Výsledkem skenování byl jeden škodlivý objekt. Po skenování je uživatel dotázán, co má antivirová aplikace s objektem udělat. Byla zvolena možnost léčit, dalo se však také vybrat smazat nebo přesunout do karantény.

3.4.2 Detekování malware pomocí anti-malware aplikací

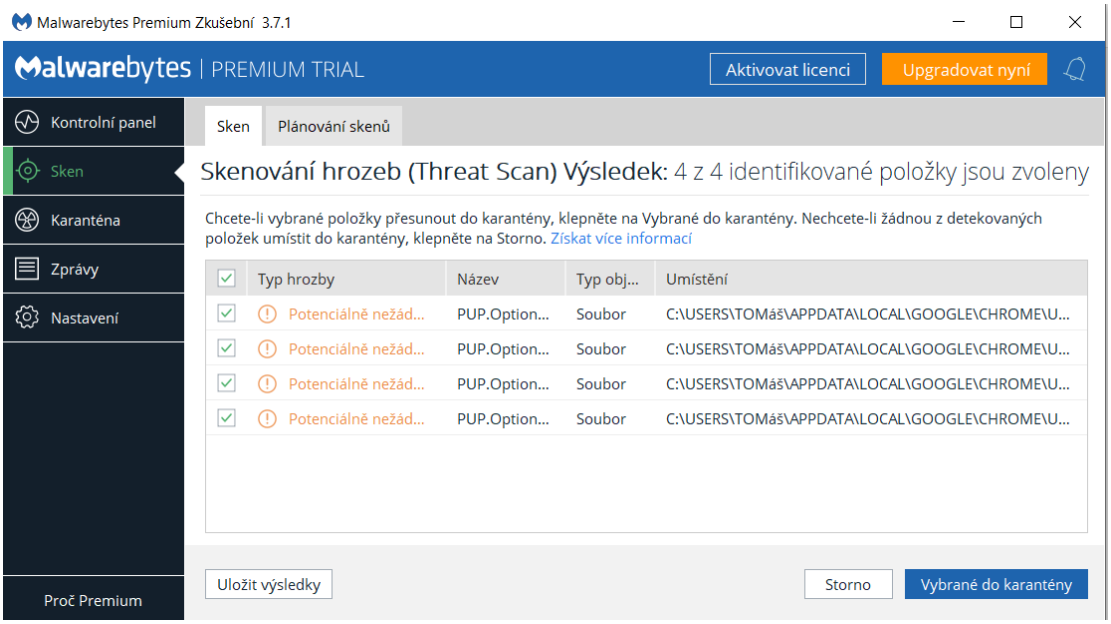
Anti-malware nástroje dokáží vystopovat škodlivý software ve vašem zařízení a následně ho smazat. Pro maximální bezpečnost je doporučeno kombinovat antivirový software a anti-malware software. Pro názornou ukázku byl vybrán volně šiřitelný MalwareBytes (dostupný z https://www.malwarebytes.com/).

1. Spustit aplikaci MalwareBytes, vybrat **Kontrolní panel** a **Spustit skenování**. (Krok č.1)



Obrázek 20 - Skenování zařízení pomocí Anti-malware aplikace

2. Po skenování je uživatel informován o hrozbách a může je přesunout do karantény. (Obrázek č. 22)



Obrázek 21 - Skenování zařízení pomocí Anti-malware aplikace

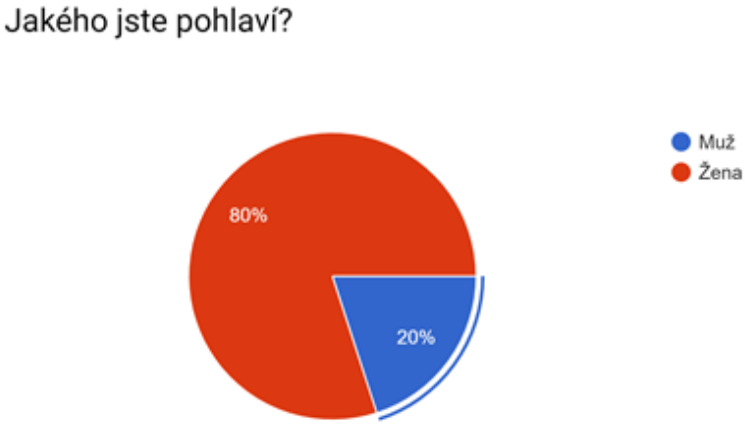
3.5 Vyhodnocení dotazníků a vyvození závěrů

V této kapitole je věnován prostor pro vyhodnocení dotazníku, který byl předložen třiceti respondentům. Pro vyvození validních výsledků v českém zdravotnictví by bylo potřeba zvolit řádově mnohem širší okruh respondentů včetně zvolení sofistikovanějších otázek. Taková studie by zabrala spoustu času, zde jsou výsledky autorova průzkumu.

3.5.1 Rozbor otázek

V této podkapitole se nachází všechny otázky včetně shrnutí otevřených otázek. Výsledky jsou prezentovány pomocí přehledných grafů, v případě podotázek jsou prezentovány zkopírováním identických odpovědí.

Otázka č. 1: Jakého jste pohlaví?

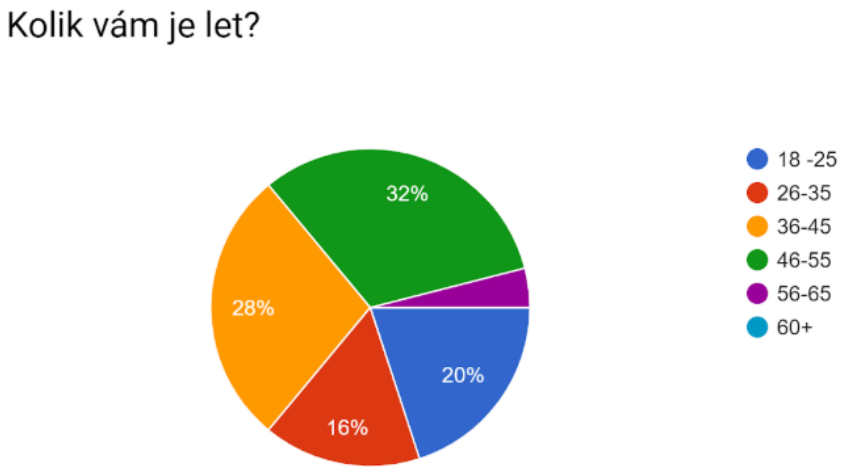


Obrázek 22 Graf dotazníkové otázky

Pro posouzení výsledků je nutné rozdělit respondenty do skupin podle pohlaví.

Je evidentní převaha žen nad muži. Je to způsobeno také tím, že v celém Českém zdravotnictví je až tříčtvrteční převaha žen. (24)

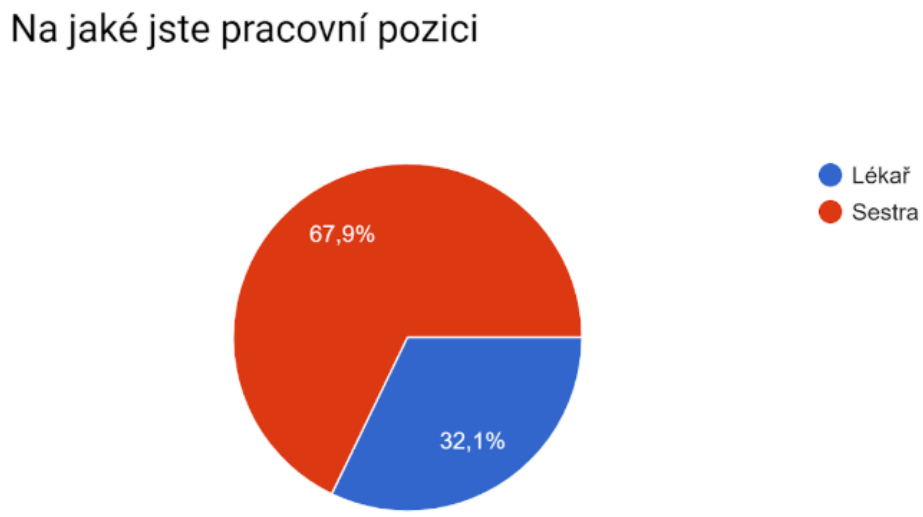
Otázka č.2: Kolik Vám je let?



Je dobré zjistit věk respondentů pro následné vyvozování závěrů

Obrázek 23 - Graf dotazníkové otázky

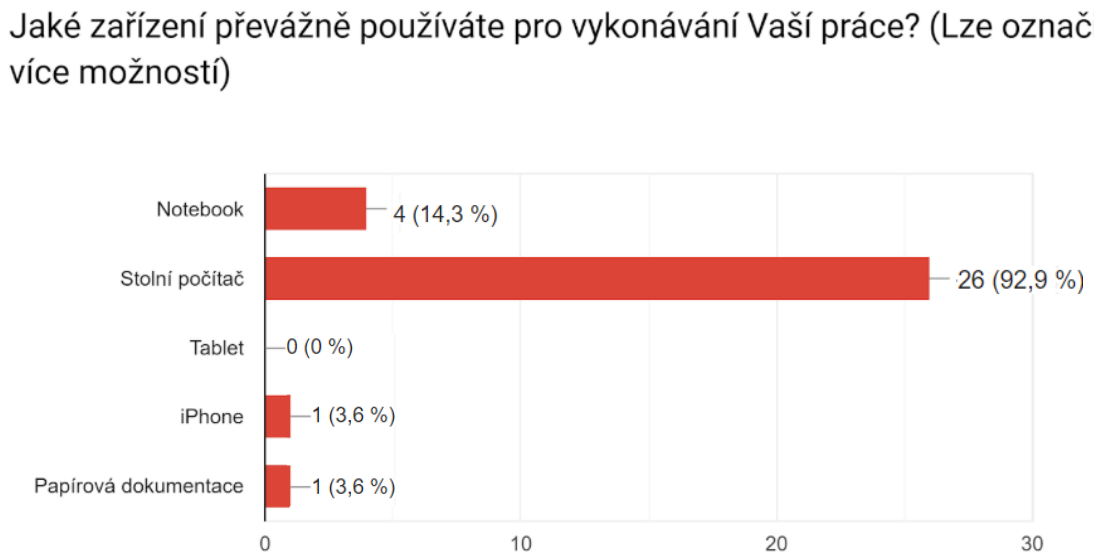
Otázka č.3: Na jaké jste pracovní pozici?



Obrázek 24 - Graf dotazníkové otázky

Zdravotních sester a bratrů se vyskytuje v českém zdravotnictví mnohem více než lékařů, což je patrné už jen z náplně jejich práce. Pro vyhodnocení je nutné zjistit zastoupení vybraných zdravotnických profesí.

Otázka č. 4: Jaké zařízení převážně používáte pro vykonávání Vaší práce? (Lze označit více možností)



Obrázek 25 - Graf dotazníkové otázky

Respondenti měli možnost zaškrtnout více než jednu odpověď. Otázka byla vytvořena pro identifikaci zařízení, s kterými přijdou respondenti nejčastěji do styku.

Otázka č. 5: Považujete ovládání vašeho zařízení za vyhovující pro zpracovávání údajů k vykonávání Vaší práce?

Obrázek 26 - Graf dotazníkové otázky

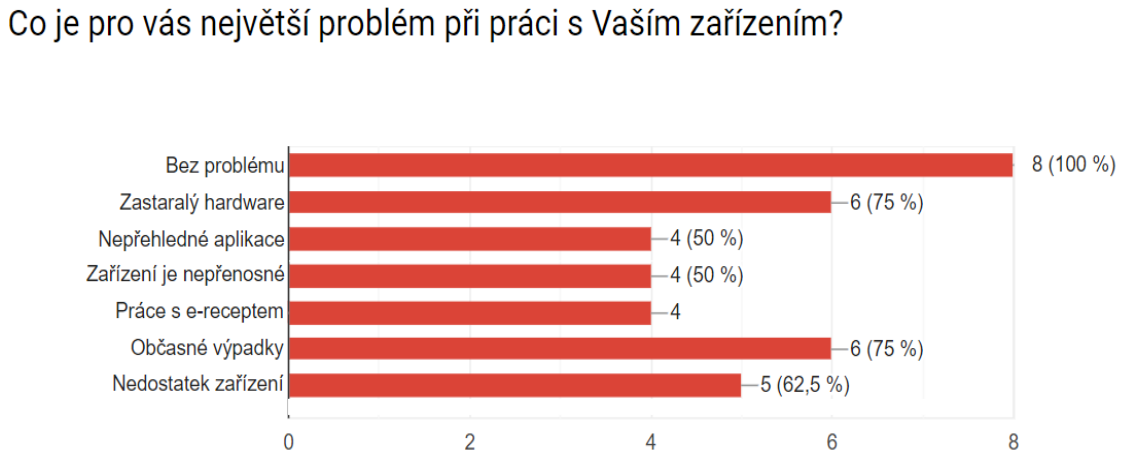
Touto otázkou bylo zjišťováno všeobecné pohodlí při používání výpočetní techniky jako nástroje pro vykonávání práce. Pokud respondenti uvedli Spíše ne/Ne, tak byli vyzváni k podobnějšímu vysvětlení v otevřené podotázce.

Podotázka k otázce č. 5: Pokud jste v minulé otázce zvolili: Spíše ne/Ne. Vysvětlete prosím.

Počet odpovědí: 1

Odpovědi: Přijde mi to strašně zdržující, psát vše do chorobopisů a potom ještě do PC, nebo chyby daná informace v chorobopisu, protože je zadaná v PC, nebaví mě běhat po oddělení k PC.

Otázka č. 6: Co je pro vás největší problém při práci s Vaším zařízením?



Obrázek 28 - Graf dotazníkové otázky

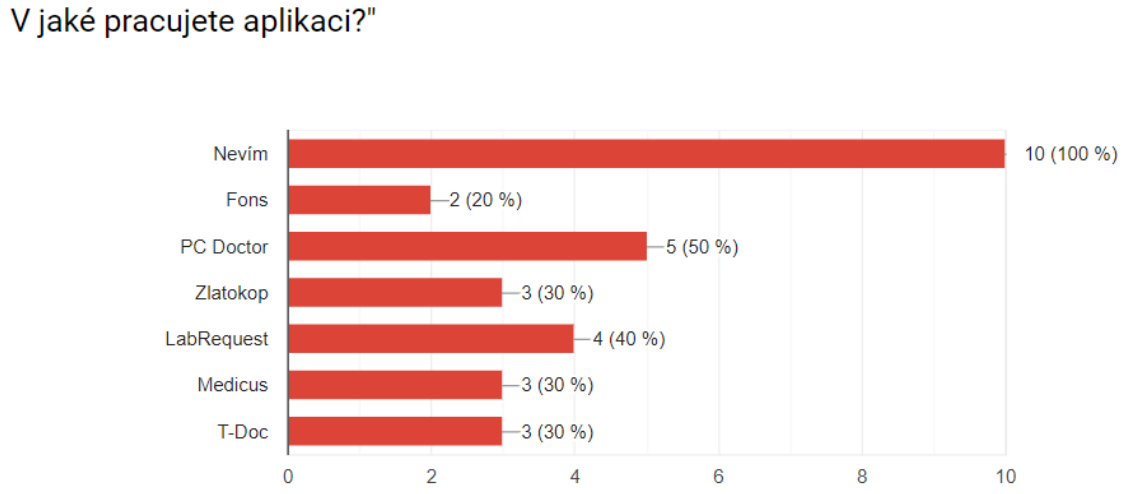
Tato otázka byla otevřená, pro jednodušší prezentaci byly odpovědi roztříděny pro vytvoření přehledného grafu.

Otázka č.7: V jaké pracujete aplikaci a pracuje se Vám v ní dobře? Přidejte název do „Jiné“.

Obrázek 29 - Graf dotazníkové otázky

Respondenti jmenovali aplikaci, kterou používají (Podotázka k otázce č. 9) a v této otázce hodnotili celkovou spokojenost s prací v jejich aplikaci.

Podotázka k otázce č.7: V jaké pracujete aplikaci?



Obrázek 30 Graf dotazníkové otázky

Respondenti sdělili název aplikace, ve které pracují a v hlavní otázce č. 9 obecně zhodnotili, jak se jim se softwarem pracuje. Nejedná se o hodnocení jednotlivých aplikací, proto není každá aplikace hodnocena zvlášť.

Otázka č. 8: Byl/a jste proškolen/a pro práci se zařízením, které pro svoji práci používáte?

Obrázek 31 Graf dotazníkové otázky

Respondenti odpovídají, zdali byli proškoleni pro zařízení, se kterým přijdou do styku a v podotázce odpovídají, kdy naposledy nebo jestli by chtěli navštívit školení.

Podotázka k otázce č. 8: Pokud zvolíte – Ano. Kdy naposledy jste byl/a proškolen/a? a Pokud zvolíte – Ne. Měl/a byste o školení zájem?

Počet odpovědí “Ano byl/a jsem proškolen/a“: 25

Počet respondentů, kteří byli proškoleni v minulých 3 letech: 19

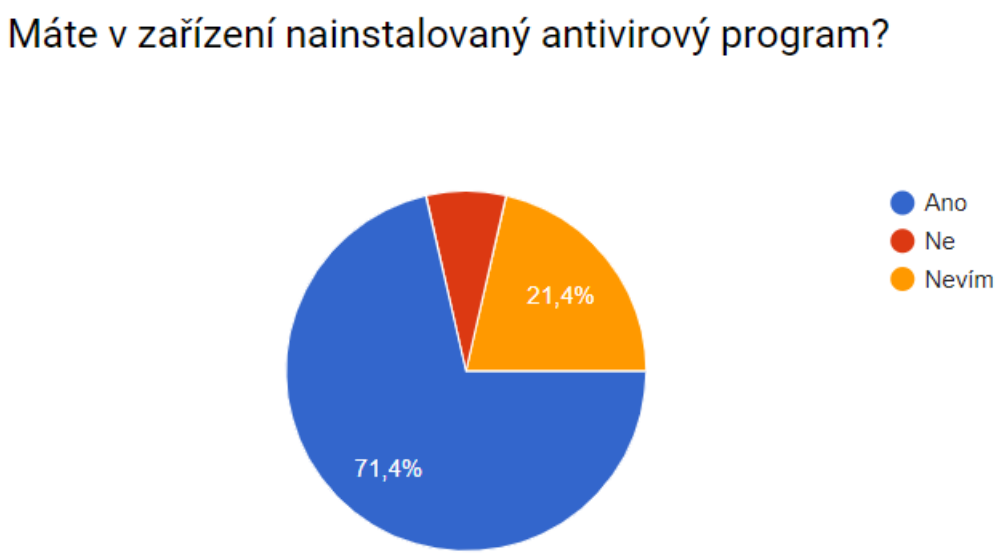
Počet respondentů, kteří byli proškoleni pouze při vstupu do zaměstnání a zároveň je to doba delší než 5 let: 6

Počet odpovědí “Ne, Měl/a byste o školení zájem?“: 5

Počet respondentů, kteří by měli zájem o školení: 2

Počet respondentů, kteří nemají zájem o školení: 3

Otázka č. 9: Máte v zařízení nainstalovaný antivirový program?



Obrázek 32 - Graf dotazníkové otázky

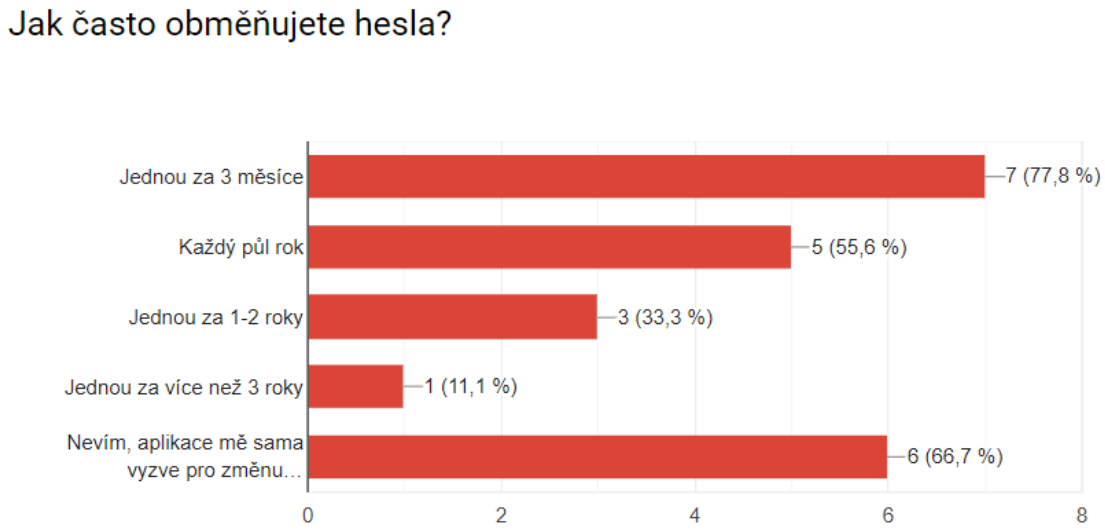
Respondenti byli tázání, zdali mají nainstalovanou některou antivirovou aplikaci na zařízení, s kterým pracují.

Otázka č. 10: Obměňujete někdy přístupová hesla k počítači a aplikacím?

Obrázek 33 - Graf dotazníkové otázky

Jeden ze základů kybernetické bezpečnosti je předcházet neoprávněné autentizaci. Respondenti odpovídají, zdali obměňují svá hesla a v podotázce upřesňují jak často. Pokud neobměňují, jsou tázáni otevřenou otázkou pro zdůvodnění.

Podotázka k otázce č. 10: Pokud obměňujete hesla, jak často?



Obrázek 34 - Graf dotazníkové otázky

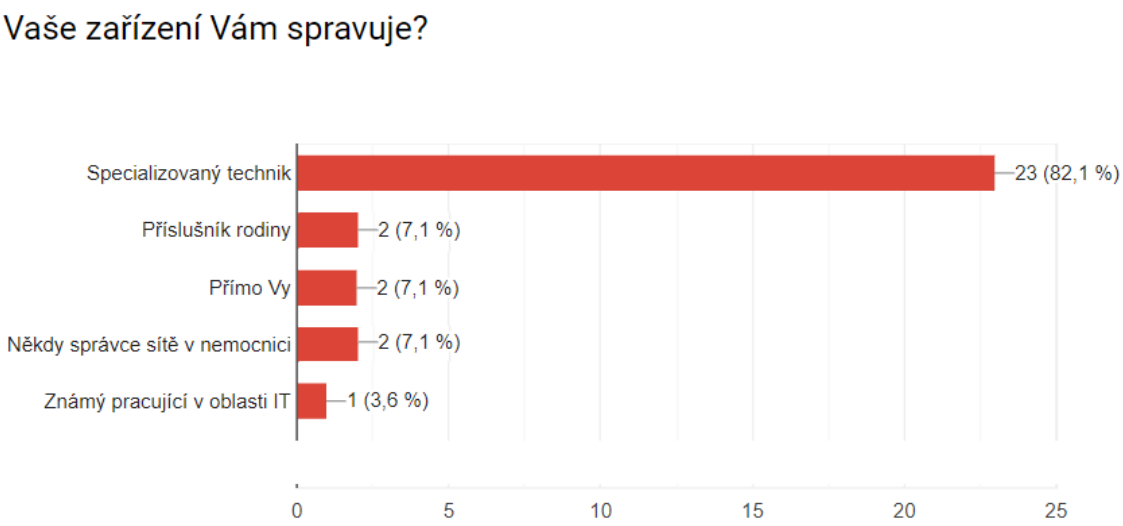
Nutná podotázka k zmapování současných podmínek, které klade zaměstnavatel v rámci obměny hesel k aplikacím.

Podotázka k otázce č. 10: Pokud neobměňujete svá hesla, uveďte prosím důvody.

Celkový počet odpovědí: 8

Odpovědi: Nevidím důvod, počítač je v mé kanceláři. Je to komplikace pro veškerý personál. Nikdo jiný se k mému počítači nedostane. Není důvod měnit. Nikdo mě o změnu nežádá. Není proč měnit hesla, nikdo se je nedozví. Protože to jen zdržuje. Je náročné neustále měnit hesla a pamatovat si je.

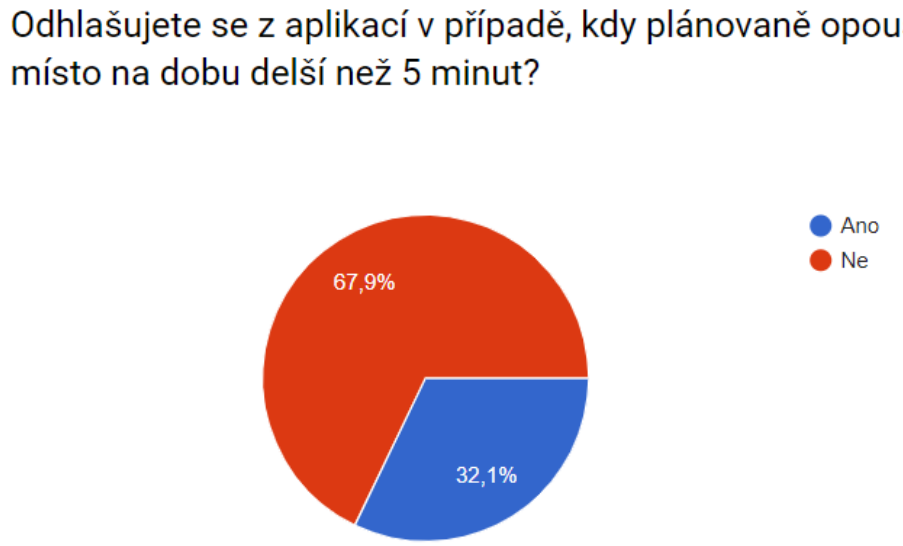
Otázka č. 11: Vaše zařízení Vám spravuje?



Obrázek 35 - Graf anketní otázky

Správa zařízení je důležitá, může se o něj starat někdo, kdo se přímo specializuje na podobné systémy, někdy k tomu postačí příslušník rodiny nebo samotný uživatel zařízení.

Otázka č. 12: Odhlašujete se z aplikací v případě, kdy plánovaně opouštíte pracovní místo na dobu delší než 5 minut?



Obrázek 36 - Graf dotazníkové otázky

Otázka směrovaná na odhlášení z aplikací, ve kterých se pracuje s osobními daty, pokud uživatel odchází od zařízení na plánovaně delší dobu, než je 5 minut. Při opuštění místa bez odhlášení může dojít k zneužití osobních dat pacientů neautorizovaným subjektem.

3.5.2 Vyhodnocení

Vyhodnocení osobních otázek 1-3

Ze získaných odpovědí vyplývá, že více jak 80 % dotazovaných respondentů byly ženy, vzhledem k číslům ohledně zastoupení podle pohlaví je hodnota podobná skutečnému stavu zdravotnictví České republiky. (24)

Nadpoloviční většina respondentů byla ve věku 36-55 let, lze tedy považovat jejich odpovědi za fundované, protože ve zdravotnictví už pracují mnoho let.

Přes 60 % respondentů pracuje jako sestra, což je vzhledem k základní definici jejich povolání pochopitelné.

Vyhodnocení otázek 4–14

4) Většina respondentů používá k vykonávání své práce stolní počítač, někteří používají notebook, který je vhodný pro snadné přenášení a umožňuje práci i v jiných podmínkách, než je vlastní kancelář nebo oddělení. Zmíněn byl také iPhone, bohužel nebylo lépe specifikováno.

5) Téměř všichni dotazovaní označili zařízení, na kterém pracují ve své práci, jako vyhovující zařízení pro práci s údaji pacientů. Jediný respondent označil, že není spokojený s prací s výpočetní technikou z důvodu, že vše, co píše do chorobopisů, musí také přepsat do počítače a někdy může nastat, že informace jsou pouze na jednom ze dvou zmíněných místech. Lze tedy tvrdit, že výpočetní technika neomezuje, ale naopak pomáhá v práci zdravotnickému personálu.
6) Respondenti mohli v otevřené otázce vysvětlit své problémy s výpočetní technikou, otázka poskytla mnoho různých odpovědí. Jedná se o časté výskyty problémů, které mají i zaměstnanci mimo zdravotnický sektor, například zastaralý hardware, díky kterému je práce na zařízení úmorná, nepřehledné a neintuitivní ovládání aplikací, občasné výpadky internetu nebo připojení k datovému serveru, a také nedostatek výpočetní techniky v poměru k počtu zaměstnanců. Objevilo se také několik odpovědí, že respondenti nemají žádný problém s výpočetní technikou.
7) Otázka směrovaná ke zjištění, s kterou aplikací zdravotnický personál pracuje a zdali jim vyhovuje. Podstatná část uživatelů ví, v které aplikaci pracují a napsali její název, nicméně se objevilo deset respondentů, kteří neví, v které aplikaci pracují. Z toho vyplývá, že tito respondenti nejsou dostatečně poučeni v rámci výpočetní techniky, s kterou pracují. Nadpoloviční většina pak však uvedla, že se jim s aplikací na zařízení ve svém pracovišti, i respondenti neznalý názvu aplikace, pracuje spíše dobře a líp. Výsledkem je, že většina respondentů ovládá pracovní prostředí svého zařízení, avšak ho používají hlavně v mechanicky naučených krocích a cokoliv nového by je mohlo vyvést z míry.
8) Respondenti byli tázáni, zdali byli proškoleni pro práci s jejich zařízením, které na pracovišti používají. Nadpoloviční většina uvedla, že proškoleni byli a současně více než 50 % respondentů byli školeni v minulých třech letech. Výsledkem je poměrně slušný počet respondentů, kteří byli proškoleni v nedávné době, neutěšivým výsledkem bylo zjištění, že pět respondentů proškoleno nebylo a více jak polovina z nich o školení nemá ani zájem.
9) Na dotaz, zdali mají respondenti v zařízení nainstalovaný antivirový program, odpovědělo „Ano“ více než 70 % respondentů, bohužel se našlo také několik respondentů, kteří si nejsou jisti přítomnosti antivirové aplikace v zařízení, se kterými pracují.
10) Jedna ze stěžejních otázek, zdali respondenti obměňují přístupová hesla k zařízení a aplikacím, dopadla vcelku chvalitebně. Více než tři čtvrtiny respondentů odpověděli, že hesla mění. V podotázce byli respondenti žádáni k doplnění časového intervalu, po kterém musí heslo změnit, popřípadě pokud hesla nemění, tak zdůvodnit. Bylo zjištěno, že nejčastěji hesla mění jednou za tři měsíce a druhou nejčastější odpovědí bylo, že je aplikace sama vyzve ke změně hesla. Ostatní respondenti, pokud hesla mění, tak po uplynutí určité doby od změny hesla, nejdéle však tři roky. Respondenti, kteří v druhé podotázce zvolili,

že svá hesla neobměňují, to zdůvodnili jako zbytečnou činnost, která je navíc. Neuvědomují si, že tímto potenciálním útočníkům mohou velmi pomoci. Pro celkové zhodnocení odpovědí této otázky, je dobré zvýraznit, že tři čtvrtiny respondentů hesla pravidelně obměňují.

11) Většina respondentů na otázku správy jejich zařízení odpověděla, že se o výpočetní techniku výhradně stará specializovaný technik. Někteří také uvedli příslušníka rodiny, známé pracující z oblasti IT a někteří si zařízení spravují sami. Je potřeba vyzdvihnout, že většina respondentů si nechá poradit od specializovaného technika a nechávají správu zařízení v rukách odborníka.
12) Výsledky poslední otázky, zdali se respondenti odhlašují z aplikací nebo operačního systému v případě, kdy plánovaně opouští pracovní místo na delší dobu než pět minut, dopadly mimo očekávání. Více než 60 % respondentů uvedlo, že se ze zařízení neodhlašují. Lze dojít k závěru, že většina respondentů si neuvědomuje možná rizika ze zneužití přístupu k zařízení neautorizovanou osobou a nepřipouští si, že by k něčemu takovému mohlo dojít.

3.5.3 Závěrečná doporučení na základě výsledků dotazníku

V prvé řadě autor této práce doporučuje provést studii, která dokáže obsáhnout širší a sofistikovanější výběr respondentů s více otázkami pro zmapování současné edukace zdravotnického personálu v oblasti kybernetické bezpečnosti a práce s výpočetní technikou. Na základě získaných odpovědí autor doporučuje častější aktualizovaná školení zdravotnického personálu v rámci zmíněných oblastí, především kybernetické bezpečnosti. Jak je známo, některé informace mohou mít vyšší cenu než materiální předmět, po zjištění některých okolností od respondentů může potenciální útočník snadno získat přístup do zařízení. Edukace zdravotnického personálu může probíhat prostřednictvím této práce.

4 Diskuze

Pro vytvoření výukového kurzu bylo použito mnoho zdrojů, které především tvořily akademické práce nebo odkazy na webové články. Je především důležité si vždy zajistit aktuální informace o řešené problematice. Cílem práce bylo vytvořit kurz, jehož kapitoly jsem vybral podle mnou vytvořené hierarchie důležitosti na základě již proběhlých bezpečnostních kurzů na naší fakultě. Několik témat bylo již obsaženo v proběhlých kurzech, avšak mě dostatečně neuspokojilo jejich vysvětlení a rozhodl jsem se je předělat podle svého nejčistšího vědomí. V praktické části bylo vytvořeno několik návodů, které považuji za velmi užitečné, byly zvoleny na základě důležitosti jednotlivých teoretických témat. Poslední nejrozsáhlejší část tvoří výsledky dotazníku, který byl předložen úzkému okruhu respondentů pracujících v českém zdravotnictví, zejména lékařům a sestrám. Celkové výsledky dotazníků nelze označit za plně uspokojující, ale ani za nedostatečné, je potřeba pokračovat v osvětě ohledně kybernetické bezpečnosti a možných rizik spojených s digitalizací a modernizací současného světa. Bylo by vhodné vytvořit relevantní studii, která by zkoumala současný stav znalostí zdravotnického personálu a zároveň navrhla řešení. Tato práce může posloužit jako prostředek k vytvoření takové studie.

5 Závěr

V úvodu práce byly zmíněny prvotní cíle této práce, které byly naplněny. Byl vytvořen plnohodnotný výukový materiál, který je tvořen tak, aby mu dokázal porozumět i čtenář bez informatického vzdělání. Byly vytvořeny praktické a jednoduše popsané užitečné návody, které mají zásadní vztah k teoretickým kapitolám. V závěru celé práce se nachází vyhodnocení dotazníků, které byly položeny zdravotnickému personálu. Tato práce může posloužit jednak k edukaci zdravotnického personálu, a jednak časem vést k aktualizaci novými kurzy podobně, jako tato práce aktualizovala ty předešlé.

Seznam Citované literatury

(1) ŠULC, Vladimír. *Kybernetická bezpečnost*. První vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-807-3807-375.

(2) FERENC, Jakub. *Odběrová analýza průběhu ověřování PINu na kryptografické čipové kartě*. Brno, 2006. Bakalářská práce. MASARYKOVA UNIVERZITA FAKULTA INFORMATIKY.

(3) Hardware - Software - Návody: Jak aktivovat Windows 10. *Hardware - Software - Návody* [online]. Česká republika: servispckupka, 2018 [cit. 2019-04-13]. Dostupné z: http://www.servispckupka.cz/jak_aktivovat_windows_10_aktivace_po_telefonu.php

(4) REIMER, Michal. *Ověřování identity na základě kontinuálního snímání dynamiky stisku počítačových kláves*. Kladno, 2015. Bakalářská práce. České vysoké učení technické, Fakulta Biomedicínského inženýrství.

(5) PETERKA, Jiří. *Báječný svět elektronického podpisu*. 1. vydání. Praha: CZ.NIC, 2011. CZ.NIC. ISBN 978-80-904248-3-8.

(6) *První certifikační autorita a.s.* [online]. Česko: První certifikační autorita, a.s. (I.CA), b.r. [cit. 2019-05-06]. Dostupné z: https://www.ica.cz

(7) POVOLNÝ, Ondřej. *ZÁZNAMOVÁ MÉDIA PRO UCHOVÁNÍ DAT, OD POČÁTKU PO SOUČASNOST*. Praha, 2010. Bakalářská práce. Bankovní institut vysoká škola Praha.

(8) Data v ohrožení? Vadí diskům magnet, otřesy nebo extrémní teploty?. *Hospodářské noviny: ICT Revue* [online]. 1996-2019 [cit. 2019-05-01]. Dostupné z: https://ictrevue.ihned.cz/c3-65859890-0ICT00_d-65859890-data-v-ohrozeni-vadi-diskum-magnet-otresy-nebo-extremni-teploty

(9) LANGER, Martin. *Optická paměťová média, principy, využití, trendy*. Brno, 2011. Bakalářská práce. Masarykova Univerzita.

(10) JUN, Jan. *DATOVÁ MÉDIA – MINULOST, SOUČASNOST A VÝHLEDY DO BUDOUCNOSTI*. Pardubice, 2016. Bakalářská práce. Univerzita Pardubice, Fakulta elektrotechniky a informatiky.

(11) Záznamová média. *Univerzitní informační systém MENDELU* [online]. Brno: Mendelova univerzita, b.r. [cit. 2019-05-03]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=20891

(12) Co je to zálohování?. *IT-SLOVNIK.cz* [online]. IT-Slovnik.cz team, 2008-2018 [cit. 2019-05-04]. Dostupné z: https://it-slovnik.cz/pojem/zalohovani

(13) BLÁHA, Petr. *Komparativní analýza lokálního a cloudového zálohování dat*. Brno, 2016. Bakalářská práce. Masarykova univerzita v Brně, Filozofická fakulta.

(14) TOMŠŮ, Josef. *Zálohování a šifrování přenosných disků*. Plzeň, 2015. Bakalářská práce. Západočeská univerzita v Plzni, fakulta pedagogická.

(15) KALVODA, Ondřej. *Sociální inženýrství: v kontextu kybernetické bezpečnosti* [online]. Brno, 2014 [cit. 2019-05-04]. Dostupné z: https://is.muni.cz/th/333077/fss_m/Diplomova_prace_ngwzunsd.pdf. Magisterská práce. MASARYKOVA UNIVERZITA, Fakulta sociálních studií.

(16) SOCIÁLNÍ INŽENÝRSTVÍ. *Národní centrum kybernetické bezpečnosti* [online]. ČESKO: NCKB, 2016 [cit. 2019-05-05]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/doporuceni/2486-socialni-inzenyrstvi/

(17) ŠULC, Ondřej. *ZÁLOHOVÁNÍ DAT A DATOVÁ ÚLOŽIŠTĚ*. Brno, 2014. Bakalářská práce. Vysoké učení technické v Brně, fakulta podnikatelská, ústav informatiky.

(18) ZOUL, Jan. *Kybernetická bezpečnost – vytvoření kurzu pro lékaře*. Kladno, 2017. Bakalářská práce. České vysoké učení technické, Fakulta Biomedicínského inženýrství.

(19) KOLOUCH, Jan. *CyberCrime*. 1. vydání. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.

(20) Varování před počítačovým virem. *Policie České republiky* [online]. Česko, 2012 [cit. 2019-05-07]. Dostupné z: https://www.policie.cz/clanek/varovani-pred-pocitacovym-virem.aspx

(21) Co mám dělat, když mě někdo požádá o platbu mimo web Airbnb?. *Airbnb* [online]. Airbnb, b.r. [cit. 2019-05-08]. Dostupné z: https://www.airbnb.cz/help/article/199/what-should-i-do-if-someone-asks-me-to-pay-outside-of-the-airbnb-website

(22) *Generátor hesel* [online]. Praha: www.iweb.cz, 2010 [cit. 2019-04-20]. Dostupné z: https://www.generator-hesel.cz

(23) Best free backup software of 2019. *Techradar.pro: IT insights for business* [online]. New York: Future US Inc, b.r. [cit. 2019-05-06]. Dostupné z: https://www.techradar.com/best/best-free-backup-software

(24) V českém zdravotnictví je převaha žen, mužů je třetina. *Týden.cz* [online]. Česko: EMPRESA MEDIA, a.s, 2018 [cit. 2019-05-08]. Dostupné z: https://www.tyden.cz/rubriky/domaci/zdravotnictvi/v-ceskem-zdravotnictvi-je-prevaha-zen-muzu-je-tretina_502747.html

Seznam obrázků

Seznam příloh

Přílohy na CD

Příloha 1 Klíčová slova (klicovaslova.pdf)

Příloha 2 Abstrakt česky (abstrakt.pdf)

Příloha 3 Abstrakt anglicky (abstract.pdf)

Příloha 4 Naskenované zadání Bakalářské práce (zadani.pdf)

Příloha 5 Celá bakalářská práce (BP_Krajca.pdf)

Příloha 6 Dotazník pro respondenty (dotaznik.pdf)