ČESKÉ VYSOKÉ
UČENÍ TECHNICKÉ
V PRAZE

FAKULTA
BIOMEDICÍNSKÉHO
INŽENÝRSTVÍ

BAKALÁŘSKÁ PRÁCE

2017

JAN
ZOUL

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA BIOMEDICÍNSKÉHO INŽENÝRSTVÍ

Katedra biomedicínské informatiky

Kybernetická bezpečnost – vytvoření kurzu pro lékaře

Cyber security – to create a course for doctors

Bakalářská práce

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

Autor bakalářské práce:	Jan Zoul
Vedoucí bakalářské práce:	RNDr. Dagmar Brechlerová, Ph.D.
Konzultant:	Mgr. Radim Krupička, Ph.D.

Kladno 2017

České vysoké učení technické v Praze, Fakulta biomedicínského inženýrství

Katedra biomedicínské informatiky

Akademický rok: 2016/2017

Zadání bakalářské práce

Student:	**Jan Zoul**
Obor:	Biomedicínská informatika
Téma:	**Kybernetická bezpečnost - vytvoření kurzu pro lékaře**
Téma anglicky:	Cyber security - to create a course for doctors

Zásady pro vypracování:

Cílem bakalářské práce je rozšíření virtuální ordinace (testovacího prostředí) dle pokynů vedoucího a konzultanta. V testovací laboratoři zrealizujte následující úlohy:

- Ověření síly hesla, vytvoření hesla, útoky na heslo.
- Viry, antiviry, užití.
- Stopa v prohlížeči a na Internetu.
- Zálohování, mazání, archivace dat.
- Šifrování mailů a dat.
- Užití dalších bezpečnostních programů.

Prezentační materiály k úlohám vytvořte tak, aby byly vhodné i pro uživatele bez informatického vzdělání.

Seznam odborné literatury:

[1] Jirovský Václav, Kybernetická kriminalita -- nejen o hackingu, crackingu, virech a trojských koních bez tajemství, ed. 1, Grada, 2007, ISBN 978-80-247-1561-2
[2] Thorsten Petrowski, Bezpečí na internetu pro všechny, 2014, ISBN 978-80-7424-066-9
[3] Stallings, William, Cryptography and network security : principles and practice , ed. Boston : Prentice Hall, Boston : Prentice Hall, 2011, ISBN 978-0-13-705632-3
[4] DOSEDĚL TOMÁŠ, Počítačová bezpečnost a ochrana dat. , ed. 1, Brno : Computer , 2004, ISBN 80-251-0106-1

Zadání platné do:	11.09.2018
Vedoucí:	RNDr. Dagmar Brechlerová, Ph.D.
Konzultant:	Mgr. Radim Krupička, Ph.D.

.....
vedoucí katedry / pracoviště

.....
děkan

V Kladně dne 20.02.2017

PROHLÁŠENÍ

Prohlašuji, že jsem bakalářskou práci s názvem Kybernetická bezpečnost-vytvoření kurzu pro lékaře 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 ……..……..……...

Jméno autora vč. titulů

PODĚKOVÁNÍ

Rád bych touto cestou poděkoval vedoucí práce paní RNDr. Dagmar Brechlerové, Ph.D., za konzultace, trpělivost a poskytnutí mnoha rad a připomínek při psaní bakalářské práce. Dále bych chtěl poděkovat panu Mgr. Radimu Krupičkovi, Ph.D., za konzultace a rady při vytváření praktické části této bakalářské práce.

ABSTRAKT

Kybernetická bezpečnost – vytvoření kurzu pro lékaře

Zdravotnická data mohou být díky stále se rozvíjejícím IT ohrožena, a proto hlavním cílem této bakalářské práce bylo rozšíření virtuální ordinace (testovacího prostředí), která je umístěna v prostorách fakulty. Cílem práce bylo zrealizovat ve virtuální ordinaci úlohy na ověření síly hesla, vytvoření bezpečného hesla, zjištění digitální stopy v prohlížeči a na internetu, zálohovat, mazat a archivovat data, zašifrovat e-mail a další bezpečnostní programy. Tyto úlohy si mohou studenti ČVUT FBMI a lékařský personál vyzkoušet ve specializované laboratoři bez trestního stíhání.

Klíčová slova

Hesla, Šifrování, Vir, Zdravotnická data

ABSTRACT

Cyber Security - Creating a course for doctors

Medical data may be threatened due to the ever-evolving IT, and therefore the main goal of this bachelor's thesis was the extension of the virtual surgery (testing environment), which is located in the faculty premises. The aim of the thesis was to realize in virtual surgery a password verification task, create a secure password, detect a digital footprint in the browser and on the Internet, back up, delete and archive data, encrypt e-mail, and other security programs. These tasks can be tried by ČVUT FBMI students and medical staff in a specialized laboratory without criminal prosecution.

Keywords

Passwords, Encryption, Virus, Medical data

Obsah

Seznam symbolů a zkratek

Seznam zkratek

Zkratka	Význam
Bat	Batch (rozšíření dávkového souboru)
BIN	BINary archive
COM	Common Objective Model
EXE	Executable (spustitelný)
IT	Informační technologie
IS	Informační Systém
MS-DOS	Microsoft Disk Operation System
NSA	National Security Agency
OVL	OVerlay (překrývání)
PGP	Pretty Good Privacy
SSL	Secure Sockets Layer
SYS	Systém

1 Úvod

Se stále rostoucím rozvojem informačních technologií se setkáváme na každém kroku. S neustálým vývojem informačních technologií je zde také velké množství nových bezpečnostních rizik, kterých je nutno se vyvarovat. Data je nutno chránit před živelnými pohromami, neoprávněným přístupem, vandalismem a zneužíváním důležitých dat. Tato rizika mohou být využita jednotlivcem nebo skupinou osob k získání citlivých dat a informací, mezi které patří i zdravotnická data. Tato bakalářská práce by měla sloužit jako podrobný manuál pro lékaře a další ošetřující personál, aby se zamezilo nejčastějším chybám, které se v oblasti ochrany zdravotnických dat dějí.

Poslední události ukazují závažnost situace v oblasti ochrany dat. Po celém světě se začal rychle šířit nový druh viru ransomware WannaCry, kterému se podařilo vyřadit v květnu roku 2017 z provozu 16 nemocnic a nemocničních zařízení ve Velké Británii a napadl desítky tisíc osobních počítačů. Nejvíce napadené země tímto virem byly Velká Británie, Rusko, Ukrajina a Španělsko. Tento vir je daleko více agresivní než ostatní typy malwaru, a to tím, že infikuje počítač a je schopný zašifrovat veškerá data z počítačů a dalších datových úložišť, nebo zašifruje počítač a žádá po uživateli výkupné ve výši 300 dolarů. Uvedený vir se většinou šíří jako fotografie, která je přílohou v e-mailu. Tento malware byl původně vymyšlen americkou vládní organizací NSA, která byla napadena útočníky, a tento škodlivý kód byl odcizen. Zde vidíme, že nemocniční data nejsou ani zdaleka tak dobře chráněna, jak by měla být a jejich ochrana vyžaduje velkou pozornost a pravidelné školení zdravotnického personálu z hlediska bezpečnosti. [14]

Hlavním cílem této bakalářské práce je vytvořit v již připravené specializované laboratoři různé útoky, které by si mohli studenti ČVUT fakulty Biomedicínského inženýrství a další zájemci (např. zdravotníci) v laboratoři vyzkoušet bez trestního stíhání.

2 Přehled současného stavu

2.1 O laboratoři

Tato bakalářská práce navazuje na bakalářskou práci Davida Stuchlíka na téma *Bezpečnost osobního počítače v ordinaci lékaře zejména z hlediska síťových útoků*, která byla obhájena v roce 2016. V již vytvořené laboratoři bylo mými předchůdci vyzkoušeno několik útoků, mezi které patří znepřístupnění služby, odposlech dat na lokální síti, podvržení webové stránky, zaznamenávání činnosti na počítači a útok na Wi-Fi s WPA2-PSK. Úkolem této nově budované laboratoře je simulovat malou ordinaci lékaře a umožnit studentům ČVUT Fakulty biomedicinského inženýrství a dalším zájemcům prakticky si vyzkoušet některé útoky provést a také vyzkoušet obranu proti nim. V laboratoři jsou použity směrovače CISCO typu RV320-K9-G5, Wi-Fi směrovače výrobce ASUS typu RT-N18U, přepínače od výrobce HP a server od výrobce IBM. Na tomto serveru je nainstalován systém Microsoft Hyper-V Server 2012 R2 určený pro virtuální stroje. Toto nám umožní na jednom počítači spustit více virtuálních strojů. Laboratoř bude také využívána pro školení lékařů a dalšího zdravotnického personálu, a proto zde budou vytvořeny další simulace útoků, které se mohou využít při vzdělávání zdravotnického personálu. [17]

2.2 Hesla

Autentizace neboli ověření znamená ověření identity určité osoby, serveru, počítače atd. Existují minimálně tři základní typy autentizace. První typ autentizace je podle toho, čím se subjekt může prokázat, například nějaký klíč, platební karta nebo identifikační karta. Druhou možností je znalost určitého PINu, přístupové fráze nebo hesla a třetí možností je prokázání osoby nějakou fyzickou vlastností, například otiskem prstu nebo skenem oka. V praxi se většinou tyto možnosti kombinují, aby ověření osoby proběhlo v pořádku. [11]

Identifikace určité osoby je proces, který určí identitu uživatele, například pomocí otisků prstů nebo identifikačního kódu. [11]

Autorizace je proces, při němž se ověří přístupová oprávnění uživatele, který vstupuje do informačního systému. Autorizace navazuje na autentizaci a ověřuje, zda má daný uživatel oprávnění k vykonání příslušné akce, například vkládání záznamů do tabulek. [11]

2.2.1 Bezpečnost hesla

Autentizace se provádí různými způsoby. Autentizace heslem je stále nejpoužívanější typ autentizace, proto je volba silného hesla zásadní. Bezpečným heslem se dá nazvat složitě prolomitelná posloupnost několika znaků, která slouží pro ochranu informačních systémů, informací a dat, k nimž by se nepovolaná osoba neměla dostat. Při přihlašování do jakéhokoliv systému je také zapotřebí zadat přihlašovací jméno nebo e-mailovou adresu. Souhrnně je toto přihlašování do systému nazýváno formulářová autentizace. Volba správného hesla je velmi důležitá. Přihlašujeme se jím do e-mailového účtu, bankovního systému nebo do firemního e-mailu a ve zdravotnictví do IS například nemocnice, laboratoře atd. Problém nastává u většiny běžných uživatelů, kteří si raději vymyslí jednoduché a snadno zapamatovatelné heslo místo složitějšího a hůře prolomitelného hesla. Velmi důležité je také uchovávat heslo v tajnosti. Heslo by se nemělo nikam zapisovat (diář, monitor počítače) a v žádném případě nikomu nesdělovat, což platí i pro blízké kamarády nebo rodinné příslušníky. Dalším pravidlem je heslo nikde neukládat, protože není žádné bezpečné místo pro jeho uložení. [10]

2.2.2 Slabá hesla

Nejčastějším důvodem prolomení hesla je zřejmě slabé heslo. Uživatel, který si zvolí slabé heslo, vystavuje své osobní údaje a soubory vědomě útokům z vnějšího světa. Slabá hesla lze poznat tak, že obsahují málo znaků, pouze malá písmena, pouze velká písmena nebo jen čísla. Dalším rizikem jsou hesla, která prozrazují nějakou informaci o uživateli. Mezi tato hesla patří například jméno domácího mazlíčka, manželky, dítěte, datum nebo město narození. Taková hesla se pak dají často prolomit za pomoci sociálního inženýrství či slovníkovým útokem. [1; 5]

Některé systémy uživateli nepovolí při registraci nebo změně hesla použít slabé heslo a vyžadují, aby uživatel zvolil heslo silnější o určitém minimálním počtu znaků.

2.2.3 Silná hesla

Zkušenější uživatelé si volí pro zabezpečení svých dat a osobních údajů silná hesla. Silné heslo by se mělo skládat z malých písmen, velkých písmen, číslic a několika speciálních znaků. Po zkombinování těchto znaků, kde žádná část není nějak běžně užívané slovo, a při dostatečné délce hesla by nemělo vzniknout jednoduše rozluštitelné heslo. Tímto způsobem se zamezí prolomení hesla pomocí slovníkového útoku, což je vyzkoušení hesel ze slovníků, kterých existuje celá řada i prolomení pomocí hrubé síly. Pro silné heslo je doporučena délka alespoň 8 znaků, i když v tomto případě platí, čím delší heslo, tím lepší. Čím je heslo delší, tím více existuje možných variací a snižuje se šance na prolomení hesla hrubou silou. [5]

2.2.4 Programy na generování hesel

Pokud uživatele nenapadá žádné silné heslo, může najít pomoc v některém z programů nebo internetových stránek pro generování hesel. Programů a internetových stránek pro generování hesel se dá nalézt mnoho. Ve většině z nich si můžeme nastavit, z jakých znaků chceme heslo složit. Na výběr je z malých písmen, velkých písmen, číslic a speciálních znaků. Také si zde můžeme vybrat požadovanou délku hesla. Jedním z těchto programů je program Generátor. [6]

2.2.5 Šifrování hesel

Data a soubory se šifrují, aby data a informace byly ochráněny před případným útočníkem. Heslo může plnit funkci šifrovacího klíče a pomocí něj se dají data znečitelnit. Lze se s ním setkat například u protokolu SSL (Secure Sockets Layer), který šifruje komunikaci mezi uživatelem a serverem. Tento protokol najde své využití i při přihlašování do mailu nebo při provádění bankovních transakcí. Základem šifrování je, že by pro útočníka mělo být nákladnější data rozšifrovat, než získat užitek z rozšifrování. Poté ztrácí rozšifrování pro útočníka smysl. Pokud se útočníkovi podaří šifru rozluštit, pak se tento vztah ruší a zisk pro útočníka stoupne a převýší náklady. [7; 9]

2.3 Viry, antiviry

Mezi počítačový malware se řadí počítačové viry, červi, trojské koně, adware, spyware a crimeware. Slovo malware vzniklo složením malicious a software, čímž vznikne zákeřný software. Termín malware se požívá k označení škodlivého softwaru, který v počítači provádí nechtěné akce nebo ho poškodí. [2; 4]

2.3.1 Trojské koně

Trojský kůň je označován jako vir, i když se spíše jedná o specializovaný program. Většinou se jedná o část programu, o které uživatel neví a je pro počítač škodlivá. Název Trojský kůň je převzatý z antického příběhu o dobytí Tróje. Trojský kůň se liší od dalších virů v tom, že nedokáže sám infikovat další počítače. Jeho šíření je zajištěno pomocí jiných virů, například červů. [2; 4]

2.3.2 Worms (červi)

Počítačový červ je program, který dokáže sám své kopie rozesílat na jiné počítače. Po infikování daného systému převezme kontrolu nad síťovými prvky a využije je pro vlastní šíření. Toto je jeho primární činnost. Sekundární činností červa může být zneprovoznění počítače, mazání některých souborů, hledání osobních souborů či dat v počítači, vytvoření „zadních vrátek“, čímž vzniká možnost infikování počítače dalšími viry nebo zašifrování souborů v počítači, kdy je uživateli přislíbeno dešifrování po zaplacení určitého poplatku. [2; 4]

Před červy neexistuje stoprocentně účinná ochrana. Díky prevenci a znalosti šíření červů se však dá napadením těmito viry vyhnout. Mezi prevenci patří používání firewallu, aktualizování operačního systému, používání antivirového softwaru, který předejde nakažení počítače, nespouštět odkazy z neověřených a pochybných stránek, a hlavně neotvírat přílohy e-mailů, u kterých si nejsme jisti, co obsahují. [2; 4]

2.3.3 Logic bomb

Vir Logic bomb se skládá ze dvou částí, kterými jsou rozbuška a akce. Rozbuška je algoritmus, který sleduje určité události a spouští akci. Fáze akce začíná aktivováním rozbušky. V této fázi má bomba cíl maximálně poškodit, vymazat dostupné disky, nebo poškodit data v databázi. Tyto viry se velmi složitě odhalují. Pokud bombu do systému zanese některý z IT pracovníků, je prakticky nemožné ji odhalit dříve, než bomba začne škodit. Nejnovější bomby se dokáží sami odstranit, čímž se zamezí jejich dohledání. [2; 4]

2.3.4 Souborové viry

Tento typ virů je beze sporu nejrozšířenější z počítačových virů. Souborové viry primárně napadají spustitelné soubory operačního systému. Souborové viry nejčastěji napadají soubory s příponami COM, EXE, BAT, OVL, BIN a SYS. [2; 4]

2.3.5 Polymorfní viry

Polymorfní viry se dokáží v počítači perfektně skrýt a je velmi malá pravděpodobnost, že je vir uživatelem odhalen. Hlavním charakteristickým znakem této

skupiny virů je fakt, že žádné dvě kopie virového těla nejsou totožné. To je důvod, proč v napadených souborech nelze najít žádné sekvence se stejným kódem. [2; 4]

2.3.6 Rezidentní viry

Tento vir je přítomen v počítačové paměti a je schopen neustále ovlivňovat činnosti, které na počítači probíhají. Rezidentní vir nehledá soubory, které by mohl napadnout, ale sleduje soubory, které uživatel nejčastěji používá, a na ty poté útočí. [2; 4]

2.3.7 Přepisující viry

Přepisující viry při napadení souboru nebo programu přepíší část jeho těla svým vlastním kódem. Programy, které jsou napadeny přepisujícím virem, jsou nenávratně zničeny, ale jsou schopné se dál šířit při opětovném spuštění programu. Tento vir je však jednoduše rozpoznatelný. [2; 4]

2.3.8 Doprovodný vir

Tento druh viru se využíval u operačního systému MS-DOS, u kterého nezapsal svůj škodlivý kód přímo do EXE souboru, ale vytvořil stejný soubor, ve kterém byl vložený škodlivý kód s příponou COM. Operační systém MS-DOS dává přednost spuštění souborů s příponou COM před soubory s příponou EXE. [2; 4]

2.3.9 Multipartitní viry

Tento vir je schopný napadnout spustitelné soubory i zavádějící sektor disku. Škodlivý kód je aktivován při spuštění počítače v bootovacím sektoru disku a napadá další soubory, které jsou na disku vytvářeny. [2; 4]

2.3.10 Ransomware

Tento druh viru zabraňuje přístupu k infikovanému počítači do té doby, než majitel počítače zaplatí požadované výkupné. Po zaplacení výkupného je přislíbeno navrácení přístupu k počítači. Ransomware se může šířit podobnou formou jako trojský kůň nebo jako červ a vyhledává chybu v zabezpečení, nebo využívá stažených souborů z internetu. Ransomware patří v současné době mezi největší problémy v IT bezpečnosti. Ransomware lze rozdělit podle implementace na dva typy. [14]

Prvním typem je tzv. locker-ransomware. Tento typ v počítači nic nešifruje, ale znepřístupní počítač nebo zařízení do doby, než je zaplaceno výkupné. Locker-ransomware sice znemožní používání počítače, ale nepoškodí data a soubory. U tohoto případu se dá vyhnout ztrátě dat pomocí přeinstalování operačního systému a obnovením souborů a dat ze záloh. [14]

Druhým typem ransomwaru je crypto-ransomware, který je daleko více rozšířený než locker-ransomware. U tohoto typu jsou zašifrována data, která jsou uložena v zařízení a výkupné je požadováno za jejich rozšifrování. [14]

2.3.11Antiviry

Riziko počítačových virů neustále roste, a proto je důležité počítač co nejlépe ochránit před touto hrozbou. Počet uživatelů, kteří toto riziko berou na lehkou váhu, je v dnešní době stále vysoký. Je velký rozdíl, pokud se snažíme ochránit firemní data nebo data domácích uživatelů. Pro ochranu dat domácích uživatelů zcela stačí stažení a nainstalování jednoho z volně přístupných antivirových programů na internetu. Pro ochranu firemních dat tento postup nestačí. Zde je totiž daleko více míst, která mohou ohrozit její chod, a proto je zabezpečení časově i finančně náročnější než u běžných uživatelů.

Pro firmy na rozdíl od běžných uživatelů je také daleko více náročné nasazení antivirové ochrany. Složitost antivirové ochrany stoupá s rozvojem škodlivých virů. Za běžné uživatele udělá celou ochranu stažený program, avšak pro administrátory firemních sítí je nasazení antivirové ochrany pro celou firmu nelehkým úkolem. S rozšiřujícím se internetem a počítačovými sítěmi se zvětšuje rozsah působení škodlivých virů.

Jednoúčelové antiviry

Jedná se o antivirové programy, jejichž cílem je detekovat a zneškodnit jeden konkrétní typ viru nebo menší skupinu virů. Jednoúčelové antiviry se však nedají použít jako plnohodnotná ochrana před viry. Tento typ antiviru využijeme v případě, že uživatel zjistí napadení počítače určitým virem. Poté se dá využít jeden z jednoúčelových antivirů, které jsou na internetu k dispozici většinou zdarma. [3; 4]

On-demand skenery

On-demand skener je jedna ze součástí antivirového systému a některými antivirovými společnostmi je nabízen zdarma. Tento typ antivirových programů lze využít při dezinfekci počítače například v případě, že operační systém Microsoft Windows není provozuschopný. Některými výrobci antivirových programů jsou na jejich internetových stránkách poskytovány online skenery, které jsou zdarma ke stažení. Většinou se jedná o skript, který za pomoci internetového prohlížeče prohledá pevný disk uživatelova počítače a zjistí výskyt virů na pevném disku. [3; 4]

Antivirové systémy

Antivirové systémy jsou v dnešní době nejčastější a nejrozšířenější antivirovou ochranou. Tyto systémy se skládají z částí, které sledují důležitá vstupní a výstupní místa, jimiž by mohl být počítačový systém infikován. Mezi tato slabá místa patří například elektronická pošta (červi), internetové stránky (škodlivé skripty, stažení infikovaných

souborů) a vstupní média (cédéčka, flash disky). Nezbytnou součástí antivirových systémů je také jejich pravidelná aktualizace prostřednictvím internetu. [3; 4]

2.4 Stopa v prohlížeči a na internetu

2.4.1 Digitální stopy

Digitální stopy jsou informace zanechané uživatelem na internetu nebo přímo ve vybavení počítače, např. v prohlížeči, ale i na pevném disku atd. Za digitální stopy se dají považovat data a metadata, která vzniknou při jakémkoli kontaktu uživatele s počítačem, telefonem a další výpočetní technikou. Pojem digitální stopy je využíván v mnoha oborech, ale v každém má trochu jiný význam. Tyto informace velmi často prozrazují více, než by sám uživatel chtěl, a mohou být snadno zneužity, a proto je důležité z hlediska ochrany soukromí výskyt těchto digitálních stop co nejvíce omezit. Tyto informace zůstávají na internetu roky i nadále přes uživatelovu neaktivitu, například na určitém profilu. Stejně tak zůstávají stopy na médiích, v prohlížeči, v informacích o souborech a na mnoha dalších místech. [8; 13]

Uživatelův pohyb na internetu je sledován i z hlediska marketingu, kde je sledována doba výskytu uživatele na určitých stránkách, na které odkazy uživatel kliká a mnoho dalších aktivit. Tato data jsou o uživateli ukládána a marketingové společnosti s těmito daty obchodují. Digitální stopy na internetu mohou posloužit také jako důkazní materiál pro objasnění určitých trestných činů. Dále je z hlediska marketingu sledován pohyb uživatelů na síti, doba jejich přihlášení na určitých stránkách, soubory nahrané uživatelem na internet nebo aktivita v různých diskuzních fórech. [13; 16]

Při zanechávání stop je nezbytně nutné rozlišovat stopy aktivní a pasivní. Aktivní stopy vznikají díky uživateli, který vytváří profily na sociálních sítích, přispívá na diskuzní fóra, nahrává fotky a soubory. Pasivní stopou nazýváme záznamy serverů o chování konkrétního uživatele, délce jeho návštěvy, aktivitě na daném webu s jeho IP adresou. [13; 16]

2.5 Zálohování, mazání, obnova a archivace dat

2.5.1 Zálohování

Zálohování souborů je jednou z nejdůležitějších operací, která by měla být pravidelně prováděna, aby byly soubory vytvářené na počítači chráněné před ztrátou. Nejsou tím nijak chráněné před poškozením, ale pokud k něčemu špatnému dojde, pak lze použít zálohovaná data a obnovit jejich obsah. Možností zálohování existuje mnoho, ale většina uživatelů a firem zálohování stále nepřikládá velký důraz. Zálohováním se dá předejít ztrátě dat například při smazání souboru, ztrátě nebo odcizení počítače nebo při poškození pevného disku. Cenu dat si většinou uživatel uvědomí až při jejich ztrátě.

Pro zachování možnosti obnovy dat ze záloh je nutné sestavení vhodného plánu, který se bude lišit pro běžné uživatele a pro firmy. Důležité je určit si, co se bude zálohovat, kam a jak často zálohovat. Jako první je důležité určit, co se má zálohovat. Je zde možnost vybrat kompletní zálohu celého počítače, nebo vybrat pouze jeden z disků, či samostatný soubor.

Poté se musí určit místo, kam bude záloha provedena. Toto místo by mělo být maximálně spolehlivé, s dostatečnou kapacitou a fyzicky oddělené od zdroje záloh. Pokud se zálohy budou provádět na disk, odkud pochází zdroj záloh, není zaručena ochrana před viry nebo selháním disku. Toto je důvod, proč se jako vhodné místo pro zálohy využívají flash disky, externí disky nebo jiná externí úložiště, u kterých v případě nepropojení s počítačem nehrozí infikování virem.

Dalším bodem zálohování je, jak často by zálohy měly být prováděny. Frekvenci zálohování je nutno sestavit podle objemu a významu zálohovaných dat. U velkých zařízení či úložišť je nutno zvolit častější zálohování z důvodu velké obměny dat. U běžných domácích uživatelů, kde neprobíhají tak časté změny dat, postačí zálohy jednou za týden nebo za měsíc. Vše toto by mělo být obsahem zálohovací politiky, kterou by měla organizace vytvořit.

2.5.2 Kompletní záloha

Kompletní záloha je taková záloha, u které je možné funkční nebo datový stav kompletně obnovit z poslední zálohy. Mezi tyto zálohy se řadí bitové zálohy, které zálohují celé úložiště. Pro tento typ záloh se musí zajistit integrita dat a také velký úložný prostor. Kompletní zálohy se provádějí pro jejich spolehlivost. [17]

2.5.3 Souborové zálohy

Souborové zálohy jsou učené pro zálohování určitých souborů nebo adresářů. Se souborovými zálohami se většina uživatelů již možná i nevědomky setkala například pří kopírování fotografií a zvukových záznamů z mobilního zařízení do počítače. Zálohy se

většinou provádějí na nějaké externí úložiště, jako je například flash disk, externí disk nebo cloud. [17]

2.5.4 Mazání dat

V oblasti zdravotnictví je ochrana dat velmi důležitá a náročná. Řada lidí či organizací se může pokusit získat citlivá data o stavu pacientů z vyhozených nebo vyřazených disků. Data na discích by měla být smazána takovým způsobem, aby útočník nebyl schopen z daného disku získat byť jen sebemenší informaci o zdravotním stavu pacienta nebo o jeho soukromí. Již jen informace o tom, že v nějakém zdravotnickém zařízení existuje záznam o určitém pacientovi, může být zásadní porušení bezpečnosti i bez znalosti obsahu.

Formátování nebo smazání oddílů na pevném disku není dostatečné k trvalému smazání informací z pevného disku. Existuje mnoho případů, kdy si lidé koupili použitý pevný disk z bazaru a bez nejmenších problémů na něm našli důvěrnou korespondenci, tabulky, dokumenty nebo jiné pracovní soubory. Běžným mazáním dat např. pomocí Shift+Delete nejsou data skutečně odstraněná a jdou obnovit.

2.5.5 Druhy mazání dat

Fyzická likvidace disků

Nejefektivnější možností likvidací dat je fyzická likvidace. Pro likvidaci lékařských záznamů by fyzická likvidace v podobě rozemletí, roztavení či rozpuštění disku byla ideální. Pokud jsou na discích citlivé informace ohledně zdravotního stavu pacientů nebo jejich osobní údaje, popřípadě čísla účtů, je lepší takový disk zničit touto cestou, než riskovat, že se tato citlivá data dostanou do špatných rukou. [18]

Mazání v magnetické peci

Mazání v magnetické peci neboli degausseru je mazání z médií s magnetickým zápisem. Jistota neobnovitelného smazání je zde díky vysoké intenzitě magnetického pole. Mazání v magnetické peci se využívá především u pevných disků, disket a magnetických pásek. U magnetických pevných disků lze využít tzv. odmagnetování, čímž se zničí i data uložená na disku. [18]

Normovaný přepis

Toto přepisování se využívá pro přepisovatelná média, jako jsou pevné disky, diskety nebo magnetické pásky. Normovaný přepis přepisuje data na disku pomocí jedniček a nul. [18]

Mazání obsahu externích disků.

Pro nenávratné odstranění všech dat z externího disku použijeme funkci úplného formátování pevného disku. Před spuštěním formátování je důležité zakázat možnost rychlého formátování. Tato možnost, tedy rychlé formátování, v žádném případě nesmaže všechna data. K tomu je za potřebí úplného formátování. [18]

Přepis náhodnými daty

Přepis náhodnými daty lze vyzkoušet například pomocí programu DBAN. Tento přepis se dá využít před novou instalací operačního systému. Program lze využít pouze na přepis celého disku, jednotlivé soubory mazat neumí. Program DBAN přepíše data na disku novými náhodnými daty. Poté je potřeba nainstalovat na počítač nový operační systém. [18]

Guttmannův přepis

Tento přepis se provádí pomocí jedniček a nul. Rozdíl oproti normovanému přepisu, který disk přepíše pouze jednou je však v tom, že se disk přepíše hned pětatřicetkrát po sobě. Tato metoda je velmi pomalá, ale lze ji využít u všech typů standartních pevných disků i pro komprimované disky. [18]

2.5.6 Obnova dat

Každému z nás se jednou za čas stane, že při dělání pořádku na disku přemístí důležité soubory do koše a koš vysype dříve, než si uvědomí hodnotu dokumentů. Pokud nějaký soubor uživatel smaže v koši, data z disku fyzicky nezmizí, ale jen se označí jako volné místo a v paměti stále setrvávají až do jejich přepsání. Pokud si tedy uvědomíme, že jsme smazali užitečný soubor a potřebujeme jej zpět, musíme zabránit přepsání souboru. Pokud se jedná o data na paměťové kartě, nejlépe ji z přístroje ihned vytáhněme. Pokud jsou data na interní paměti, snažme se interní zařízení používat minimálně, hlavně nic neinstalovat, nepřesouvat, dokonce ani žádná data nemazat.

2.6 Šifrování mailů a dat

Šifrováním se nezabezpečená data pomocí kryptografie převedou na data šifrovaná a rozluštit je může pouze majitel dešifrovacího klíče. Důvodem, proč je důležité data šifrovat, je jejich ochrana před cizí osobou. Pokud osoba nebude mít dešifrovací klíč, data se jeví jako nesmyslná směs znaků, která je bezcenná.

2.6.1 Symetrické šifrování

Při symetrickém šifrování je u šifrovacího algoritmu použit pouze jeden klíč k zašifrování i dešifrování. U symetrického šifrování je velkou výhodou nízká výpočetní náročnost. Velkou nevýhodou však zůstává sdílení soukromého klíče. Oba dva uživatelé musí být dohodnuti na soukromém klíči. [15]

2.6.2 Asymetrické šifrování

Základním rozdílem mezi asymetrickým a symetrickým šifrováním je, že asymetrické šifrování používá dva různé klíče. Asymetrické šifrování se využívá pro utajení komunikace a také pro elektronický podpis. Tento typ šifrování se skládá ze dvou kroků. Při prvním kroku, tj. zašifrování zprávy, se užije jeden klíč, druhý klíč pak pro její opětovné dešifrování. Osoba, která šifruje, nemusí s osobou, která dešifruje, sdílet žádné informace a je zde eliminována nutnost výměny klíče. K tomu se využívají tzv. veřejný a soukromý klíč. Majitel veřejného šifrovacího klíče svůj klíč zveřejní a jemu určené zprávy může šifrovat kdokoliv. Dešifrovací klíč je privátní a je držen majitelem v tajnosti, protože jeho pomocí může zprávy dešifrovat. Při srovnání se symetrickou šifrou jsou šifry asymetrické daleko pomalejší. [15]

2.6.3 Šifrování mailů

Pro ochranu osobních údajů v e-mailových zprávách je vhodné e-mail před odesláním zašifrovat. E-mailové zprávy je možné elektronicky podepsat nebo zašifrovat. U digitálních certifikátů je používána technologie PKI, která je založena na asymetrické kryptografii. Šifrovat email můžeme například díky emailovým klientům, jako je Outlook a Thunderbird, nebo díky technologii PGP (Pretty Good Privacy). PGP uživateli umožní zašifrovat a dešifrovat zprávy, digitálně se podepsat, spravovat klíče a ověřit identitu odesílatele. Program Microsoft Outlook převede text na zašifrovaný text, který může dešifrovat pouze majitel správného privátního klíče. Pokud příjemce zprávy nemá správný privátní klíč, zpráva se mu nezobrazí. [15]

3 Metody

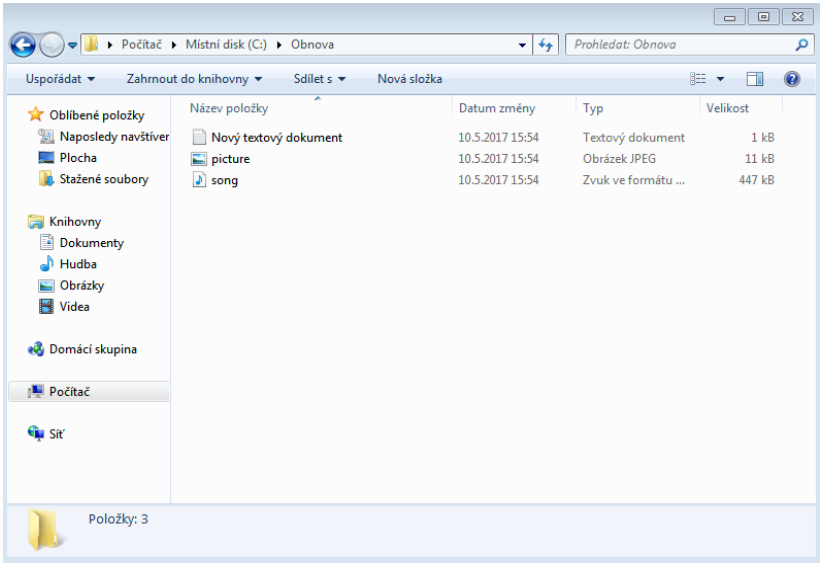
Řada metod a postupů z hlediska síťových útoků je již popsána z loňského roku v bakalářské práci Davida Stuchlíka. V mé práci jsou popsané další úlohy, které jsou vytvořeny především pro vzdělávání zdravotnického personálu. Vybral jsem úlohy, které se hodí pro základní kurz pro zdravotnický personál a které obsáhnou zcela běžné, ale závažné problémy, jež mohou ve zdravotnictví vzniknout a ohrozit tím zdravotnická data nebo soukromí pacientů. Tyto návody jsou psané pro studenty fakulty a pro zdravotnický personál, a proto jsou psané ve druhé osobě.

3.1 Obnovení souborů

Cíl úlohy: v první úloze si vyzkoušíte obnovení špatně smazaných dat ve složce Stažené soubory pomocí programu Recuva. Dále je nadobro odstraníte pomocí programu Recuva. Tato úloha by měla názorně ukázat, jak data skutečně smazat, což je zejména ve zdravotnictví zásadní problém.

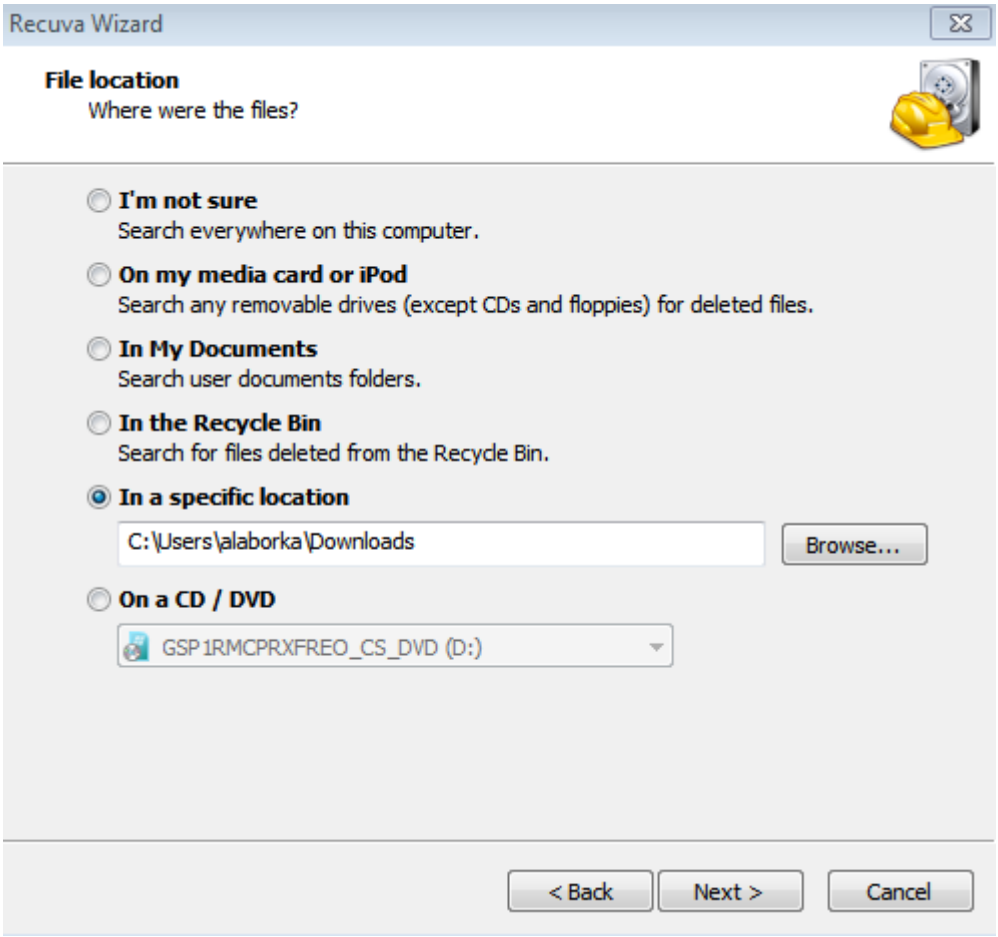
Postup

1. Na počítači v laboratoři vyberte program Virtual box a spusťte ho.
2. Spusťte počítač Win7 – obnova, mazání.
3. Přihlaste se
    a. Uživatelské jméno: root
    b. Heslo: root.
4. Zjistěte, zda se na disku ve složce Downloads nachází soubory picture.jpg, song.mp3 a Nový textový dokument.txt.



Obrázek 1: Nalezení souborů určených ke smazání

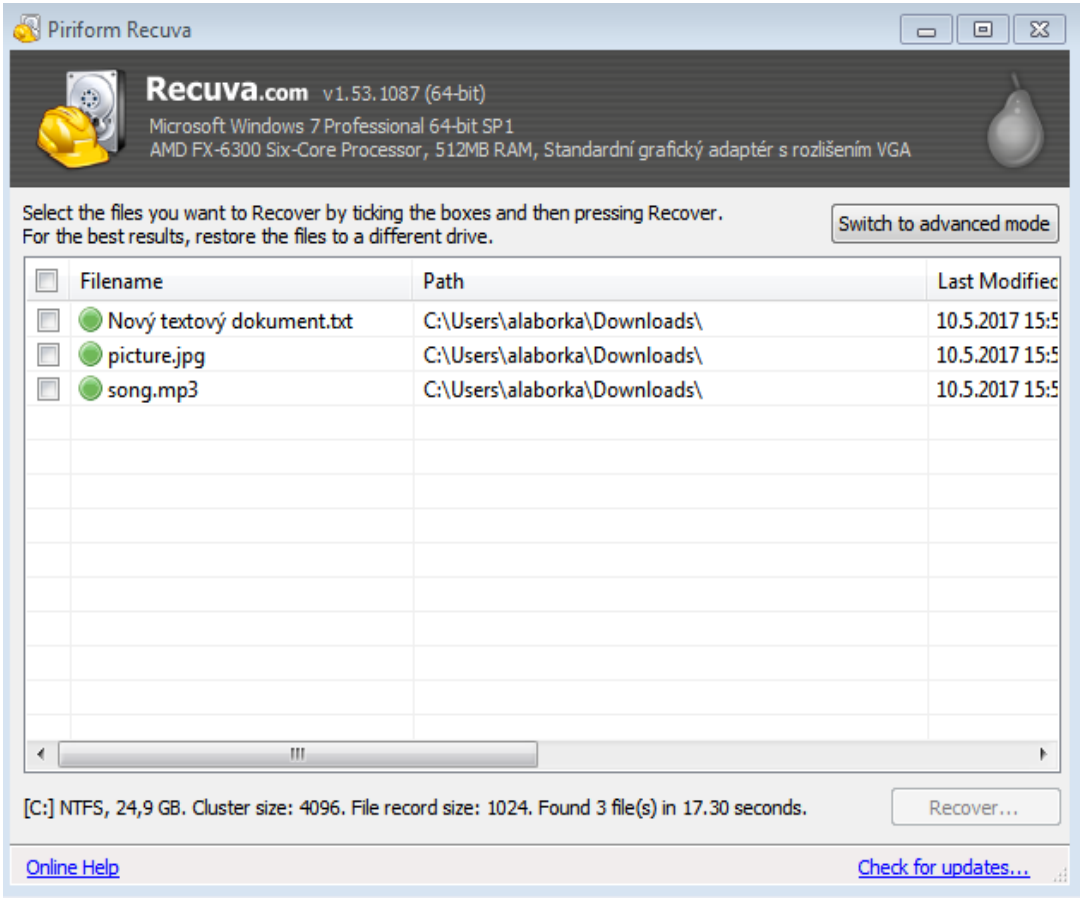
5. Po zkontrolování tyto soubory “nadobro“ odstraňte klávesovou zkratkou Shift+Delete.
6. Najděte na ploše program Recuva a spusťte ho.
7. V prvním okně klikněte na tlačítko Next.
8. V dalším okně je na výběr, jaký typ souborů chcete obnovit, zaškrtněte Všechny soubory.
9. V další nabídce vyberte místo, odkud jste soubory smazali, složku Downloads.



Obrázek 2: Místo uložených souborů

10. V posledním okně zaškrtněte Hloubkové vyhledávání a pokračujte tlačítkem Start.

11. Zde vidíte, že se programu Recuva podařilo obnovit všechny soubory, které byly smazány.



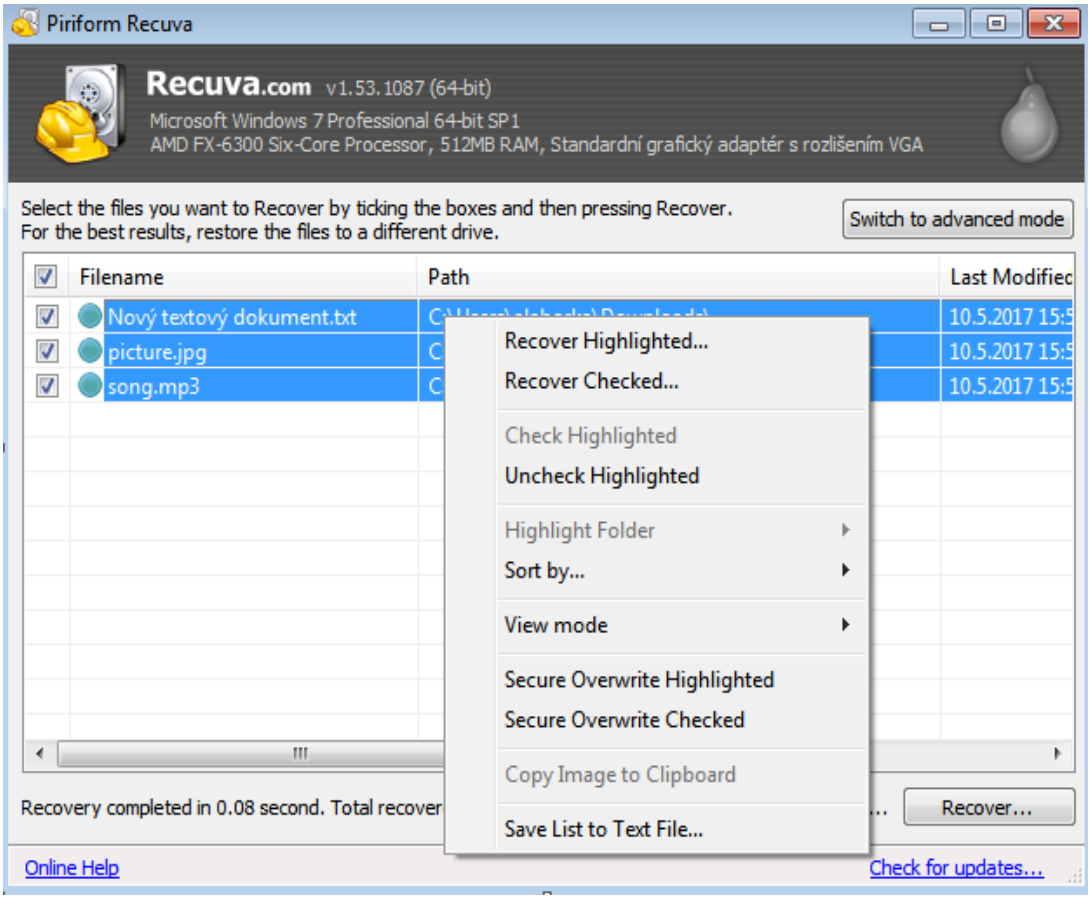
Obrázek 3: Obnovení souborů

12. Poté klikněte na možnost Recover a vyberte složku Obnova, do které soubory obnovte.
13. Zkontrolujte, zda jsou soubory ve složce Obnoveno skutečně v pořádku.

3.2 Smazání souborů

1. Na ploše najděte program Virtual Box a spusťte ho.
2. Spusťte virtuální počítač Win7 – obnova, mazání.
3. Přihlaste se
    a. Uživatelské jméno: root
    b. Heslo: root.

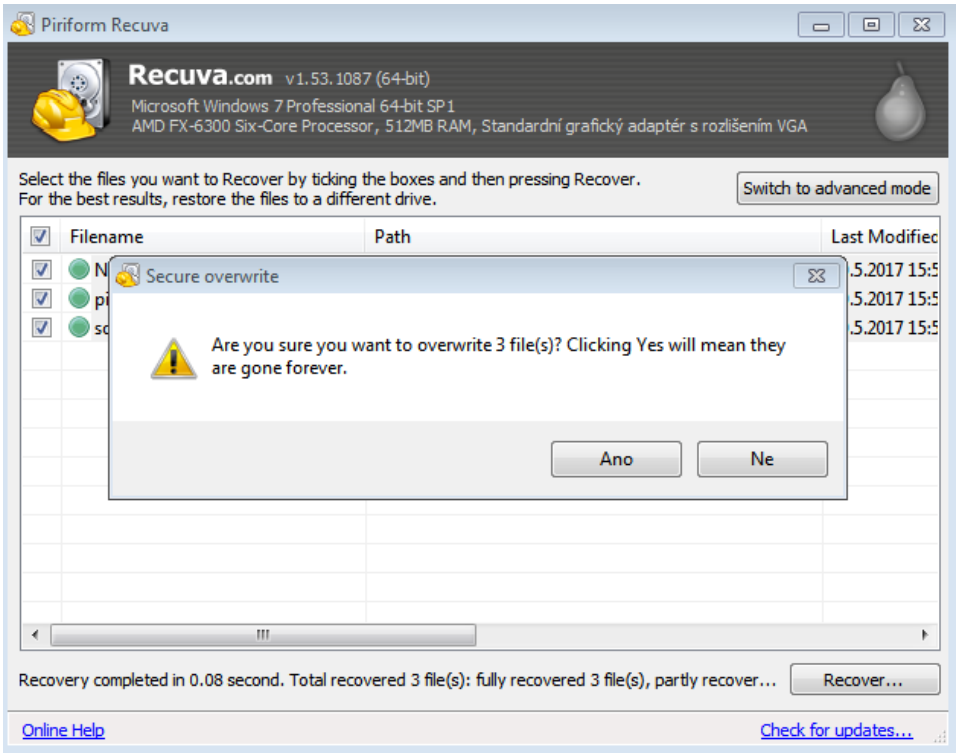
4. Pokud v programu Recuva na obnovené soubory kliknete pravým tlačítkem myši, dostanete na výběr Bezpečně smazat označené, nebo Bezpečně smazat zaškrtnuté.



Obrázek 4: Bezpečné smazání souborů

5. Vyberte Bezpečně smazat označené.

6. Po kliknutí na tlačítko Ano všechny tři soubory nenávratně smažte.



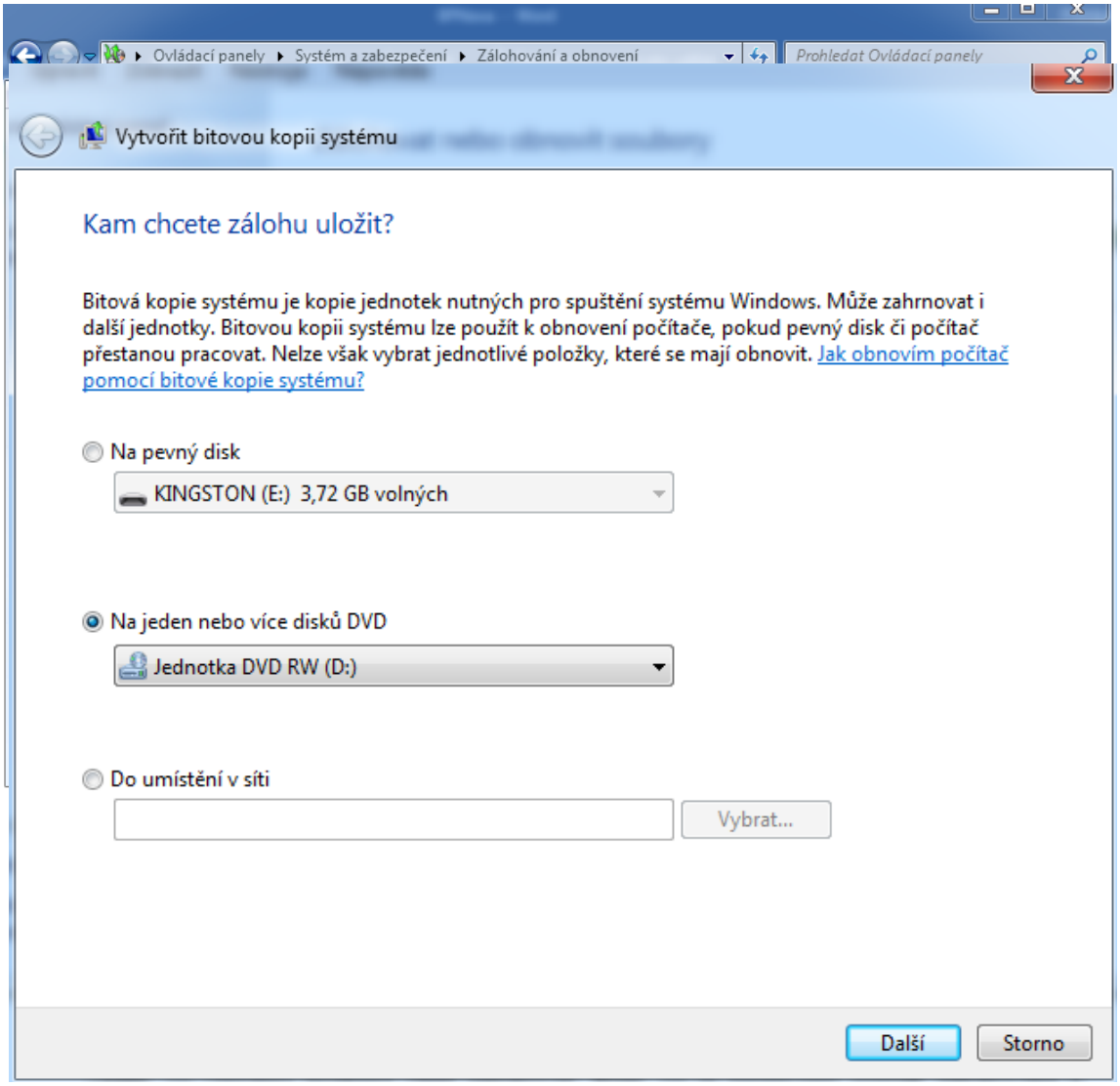
Obrázek 5: Potvrzení smazaných souborů

3.3 Zálohování dat

U operačního systému Windows 7 firma Microsoft myslela i na zálohování a integrovala do operačního systému nástroj pro zálohování dat, který si nyní můžete vyzkoušet.

1. Na ploše najděte program Virtual box a spusťte ho.
2. Vyberte počítač s názvem Win7 zálohování a spusťte jej.
3. Přihlaste se
    a. Uživatelské jméno: root
    b. Heslo: root.
4. Připojte k počítači flash disk nebo jiné externí zařízení, na které budete chtít provést zálohu bitové kopie systému.
5. Dále klikněte na nabídku Start, kde zvolte ikonu Ovládací panely.
6. V dalším okně klikněte na možnost Systém a zabezpečení a zde vyberte možnost Zálohování a obnovení.

7. V tomto okně klikněte na možnost Vytvořit bitovou kopii systému.



Obrázek 6: Vytvoření bitové kopie

8. V této nabídce zvolíme, kam chceme zálohovat, a klikněte na tlačítko další.
9. V posledním okně klikněte na možnost Spustit zálohování a vyčkejte, než operace proběhne.
10. Zálohu je nutno poté uložit na jiné místo, které je dobře zabezpečené, nejlépe i do jiné budovy.

3.4 Vytvoření silného hesla

Vytvořit dostatečně silné heslo si může uživatel sám nebo může využít jeden ze specializovaných programů. V této úloze si můžete vyzkoušet vygenerování hesla pomocí programu Awesome password generator.

1. Na ploše najděte program Virtual box a spusťte ho.
2. Vyberte počítač s názvem Win7 Hesla a spusťte jej.

3. Přihlaste se
    a. Uživatelské jméno: root
    b. Heslo: root.
4. Po přihlášení najděte na ploše program Awesome Password Generator.
5. U tohoto programu vidíte pouze jedno okno.
6. V tomto okně si můžete vybrat, z jakých znaků chcete, aby bylo heslo složeno a jak by mělo být dlouhé. Je zde na výběr z malých písmen, velkých písmen, číslic a speciálních znaků.

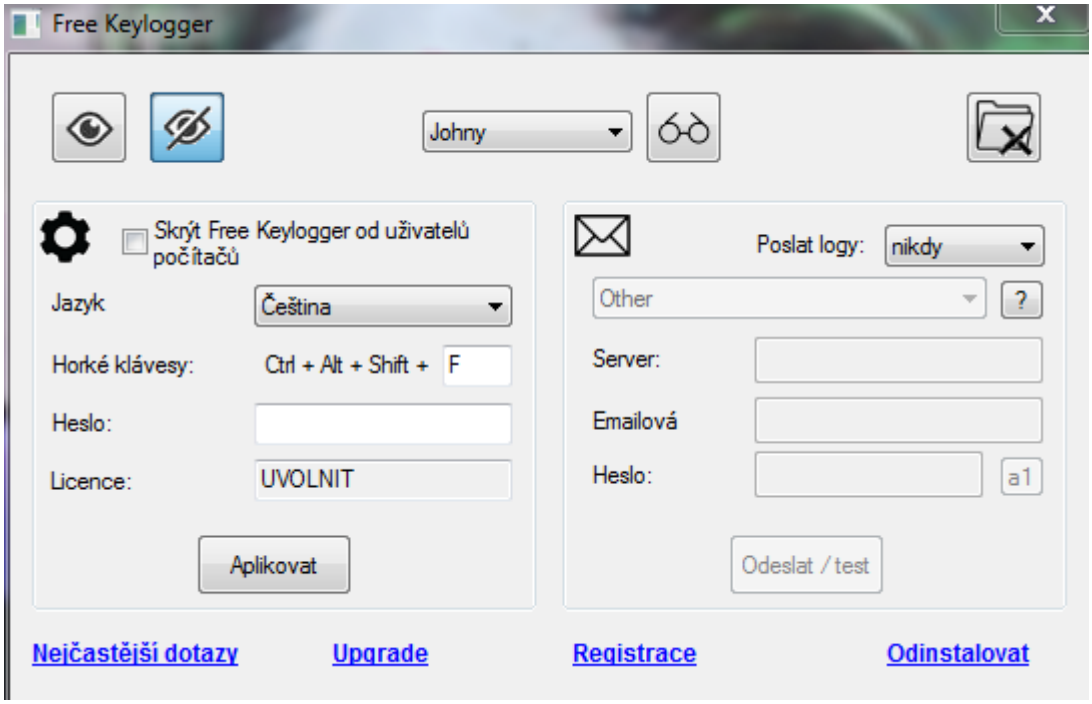
Obrázek 7: Generátor náhodných hesel

7. Tento program vám sám vyhodnotí, jestli je dané heslo dostatečně silné.

3.5 Odchycení hesla

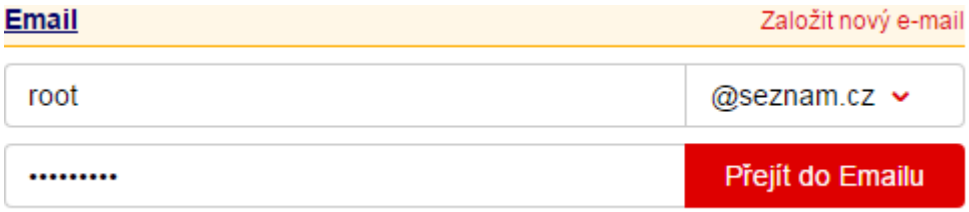
1. Na ploše najděte program Virtual box a spusťte ho.
2. Vyberte počítač s názvem Win7 Hesla a spusťte jej.
3. Přihlaste se
    a. Uživatelské jméno: root
    b. Heslo: root.
4. Po přihlášení najděte na ploše program Free Keylogger a spusťte ho.

5. V programu klikněte na obrázek oka, čímž začne sledování počítače.



Obrázek 8: Začátek odchytávání klávesnice

6. V dalším kroku spusťte internetový prohlížeč Google Chrome a přejděte na internetovou stránku www.seznam.cz.
7. Na této stránce si najděte přihlášení do e-mailu a vložte jakékoliv uživatelské jméno a heslo. Pro tento účel bylo zadáno vymyšlené uživatelské jméno root a heslo 123456789.



Obrázek 9: Přihlášení do e-mailu

8. Nyní se vraťte zpět do programu Free Keylogger a klikněte na obrázek s brýlemi.
9. Po kliknutí na tento obrázek se otevře textový dokument, ve kterém je zaznamenána činnost uživatele včetně dne, času, použitého prohlížeče, jeho zadaného uživatelského jména a hesla na stránce www.seznam.cz.

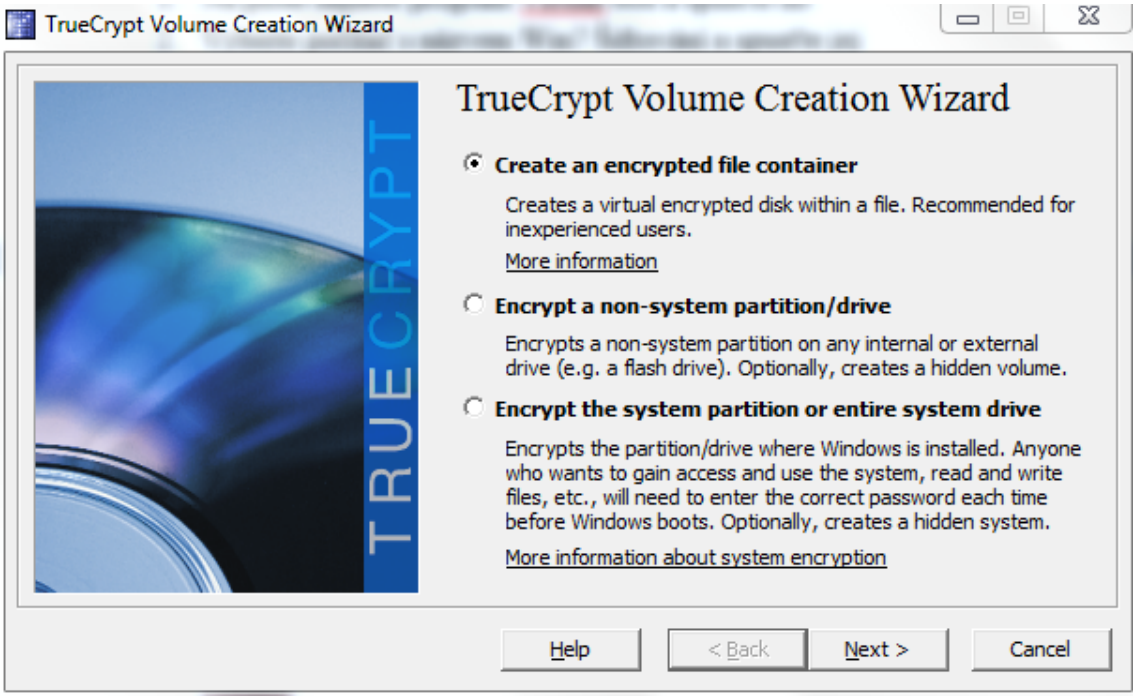
```
May 14 10:29:01 2017 || Google Chrome || Seznam - najdu tam, co neznám - Google Chrome ||
        root 123456789
```

Obrázek 10: Zaznamenané údaje

3.6 Šifrování souborů

V této úloze si prakticky vyzkoušíte, jak zašifrovat a dešifrovat data, aby se k nim nepovolaná osoba nedostala.

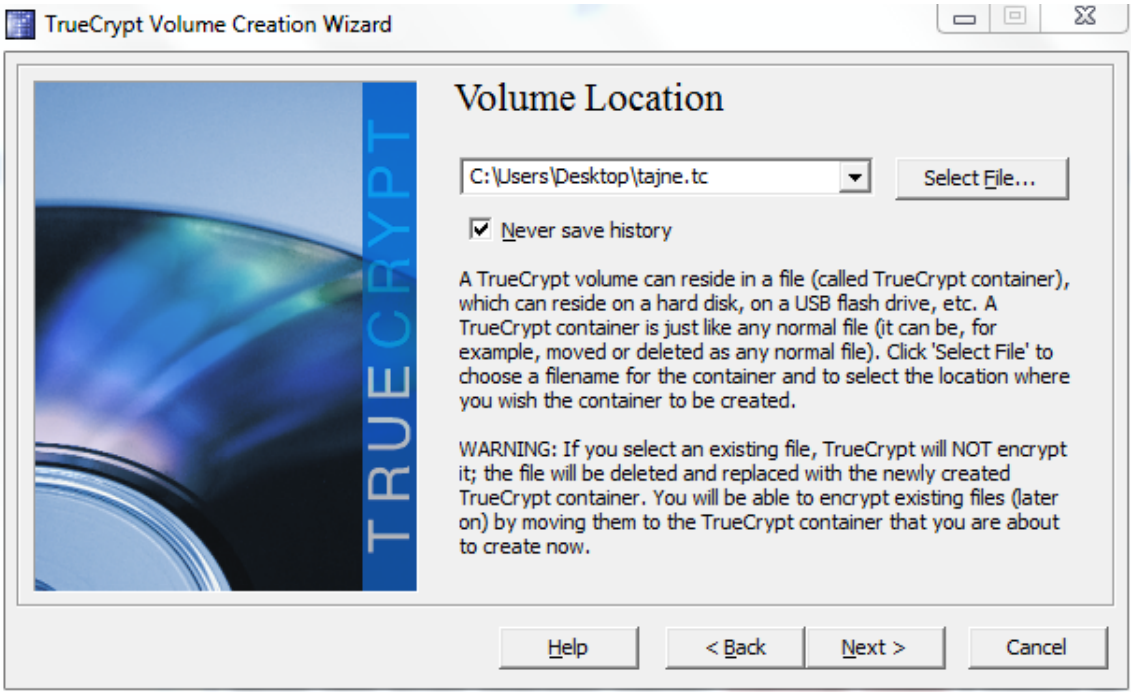
1. Na ploše najděte program Virtual box a spusťte ho.
2. Vyberte počítač s názvem Win7 Šifrování a spusťte jej.
3. Přihlaste se
    a. Uživatelské jméno: root
    b. Heslo: root.
4. Nalezněte na ploše program TrueCrypt a spusťte ho.
5. V horní liště klikněte na možnost Volume a v menu na možnost Create new volume.
6. V novém okně zaškrtněte možnost Create an encrypted file container a klikněte na další.



Obrázek 11: Vytvoření šifrovaného disku

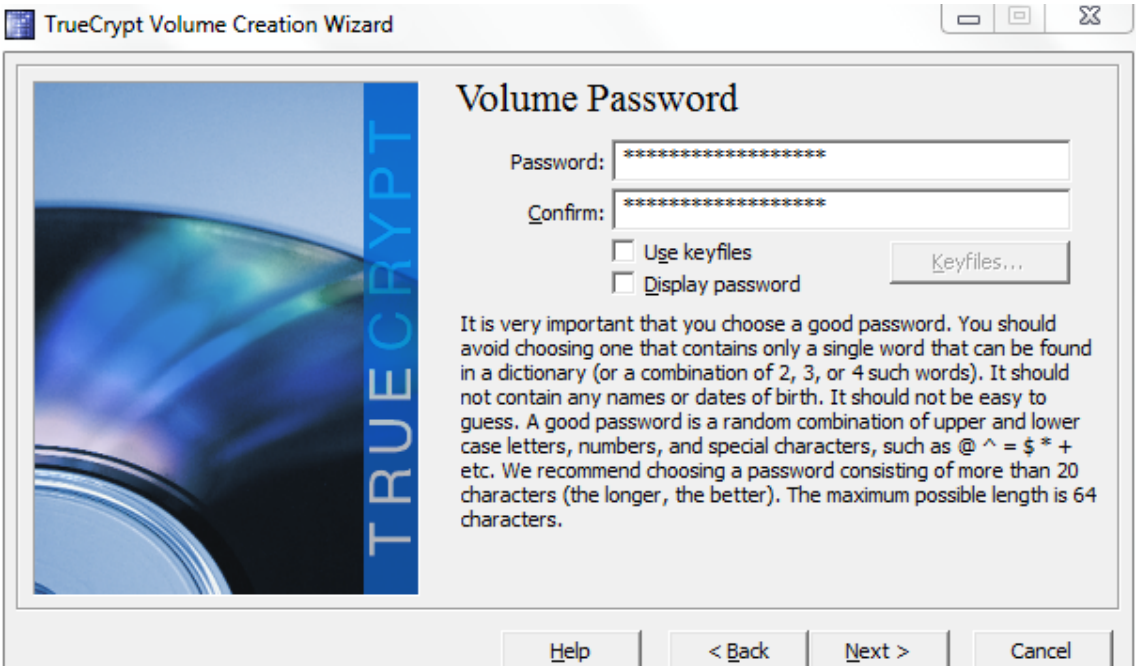
7. V dalším okně nechte zaškrtnuté Standart TrueCrypt volume a klikněte na další.

8. Zde si vyberte, kam chcete uložit nový disk, kde budou zašifrovaná data, a pojmenujte ho například tajne.tc.



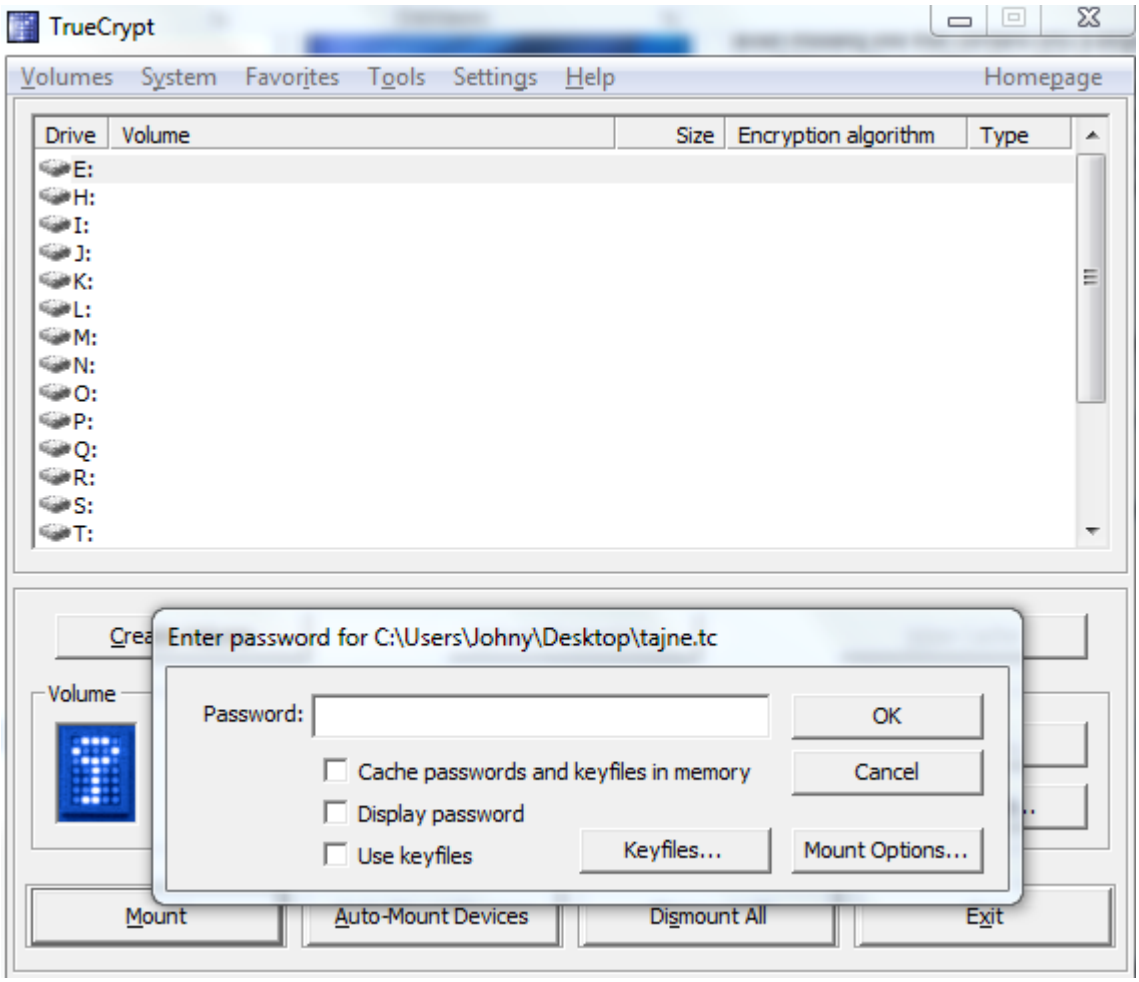
Obrázek 12: Pojmenování šifrovaného disku

9. V následujícím okně si vyberte typ šifrovacího algoritmu a hashovacího algoritmu, můžete ponechat předvolené a klikneme na Next.
10. Zde zvolte velikost nového disku, např. 100 MB.
11. V dalším okně si zvolte vhodné heslo, které si zapamatujete, a klikněte na Další.



Obrázek 13: Zvolení hesla

12. V posledním okně ponechte přednastavené nastavení a klikněte na tlačítko Format.
13. Na ploše se vytvoří soubor tajne.tc, na něj dvakrát klikněte.
14. V programu TrueCryp klikněte na jedno z písmen v nabídce pravým tlačítkem myši a dejte možnost Mount Volume.
15. Otevře se nové okno, kam zadejte dříve zvolené heslo.



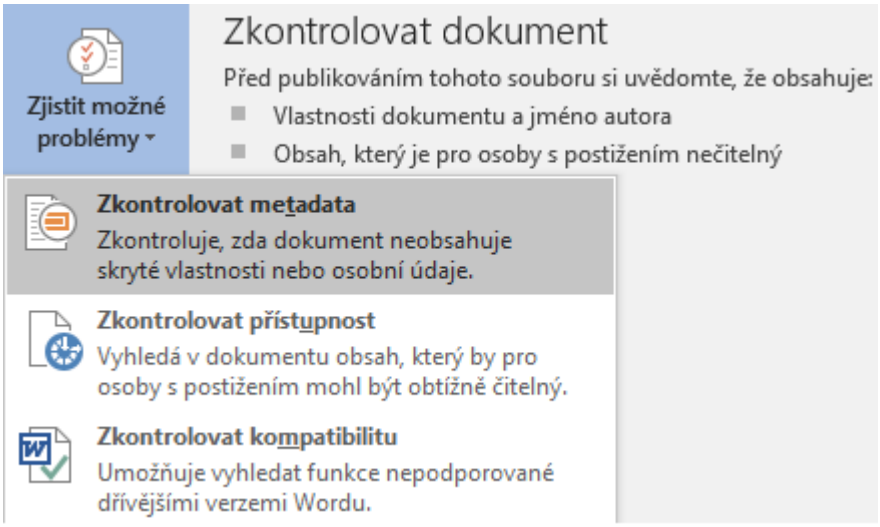
Obrázek 14: Zadání ověřovacího hesla

16. Tímto krokem nám v počítači vznikne nový disk, na který si přetáhněte 2 soubory ze složky Stažené, a to picture.jpg a song.mp3.
17. Poté v okně programu TrueCrypt klikněte na tlačítko Dismount, čímž nově vytvořený disk zmizí a data zůstávají jen v podobě souboru tajne.tc, který je uložen na ploše.
18. Pokud se budete chtít k zašifrovaným informacím dostat, dvakrát klikněte na soubor tajne.tc, v programu TrueCrypt na možnost Mount a zadejte předem zvolené heslo.

3.7 Mazání vlastností souboru

Cíl úlohy: v této úloze se pokusíte najít a vymazat všechna data a osobní údaje z aplikace Microsoft Word.

1. Na ploše najděte a spusťte program Virtual box.
2. V programu Virtual box spusťte počítač Win7 Digitální stopa.
3. Přihlaste se
    a. Uživatelské jméno: root
    b. Heslo: root.
4. Po přihlášení uvidíte na ploše Microsoft Word dokument, který otevřete.
5. V nově otevřeném okně zvolíte možnost Soubor a v něm možnost Informace.
6. Zde zvolíte možnost zjistit možné problémy a po rozkliknutí vyberte možnost zkontrolovat metadata.



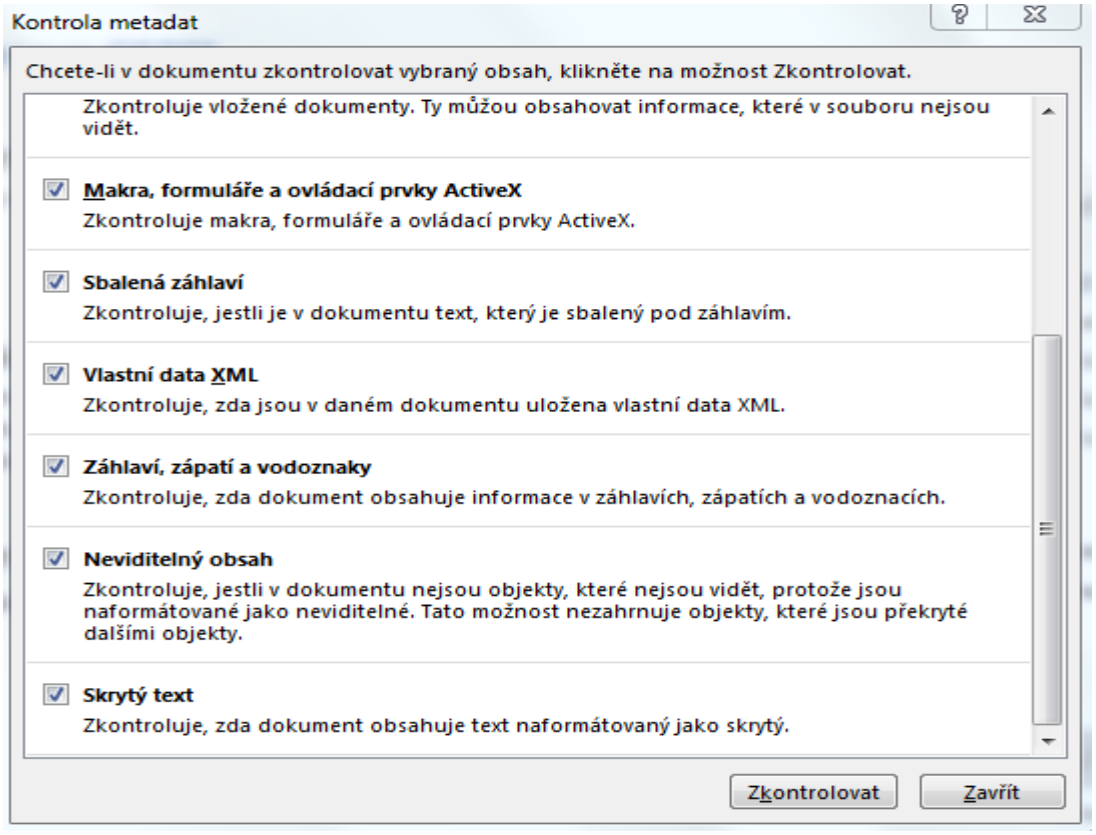
Obrázek 15: Kontrola metadat

7. V nově otevřeném okně vyberte možnost zkontrolovat a po Zkontrolovaní možnost Odebrat.

3.8 Vymazání digitálních stop v prohlížeči

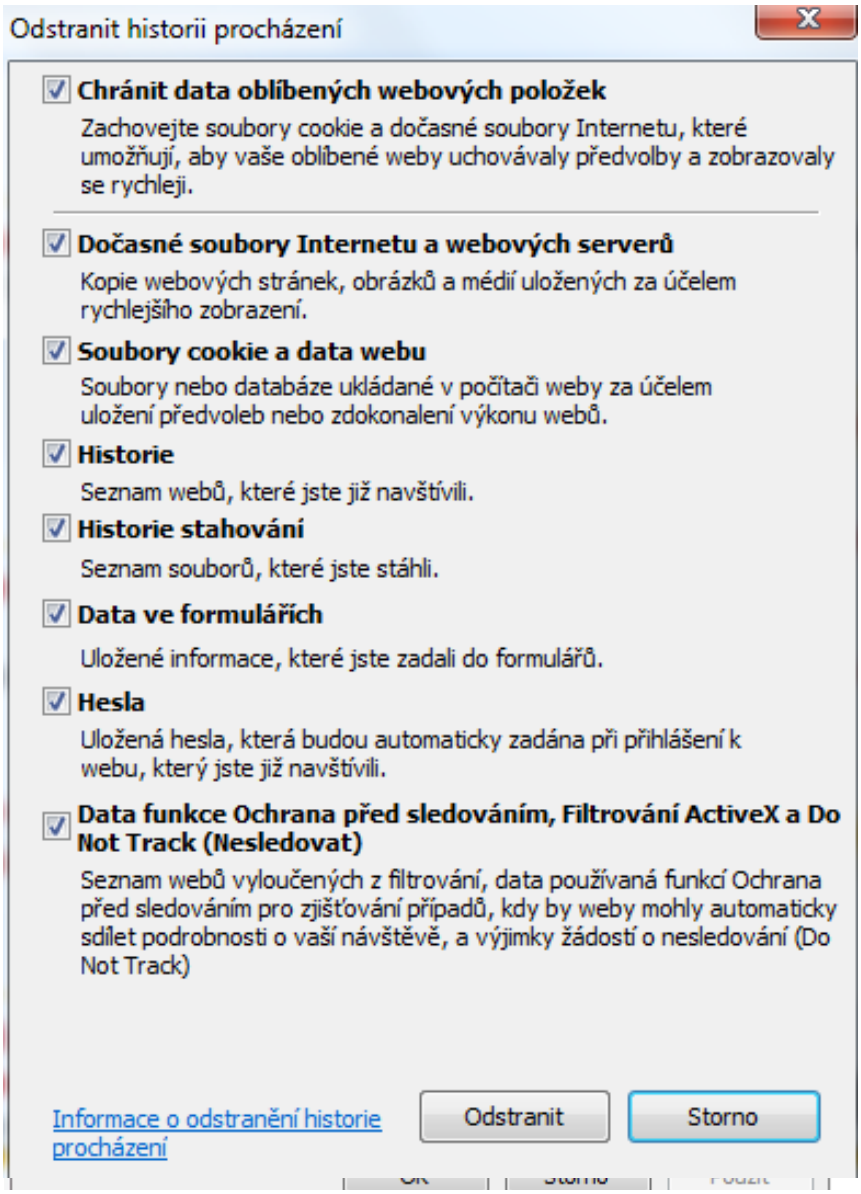
V této úloze si můžete vyzkoušet vymazání historie prohlížení, historie stahování, cookies souborů a dalších digitálních stop v prohlížeči Internet Explorer.

1. Na ploše najděte program Virtual box a spusťte ho.
2. V programu Virtual box spusťte počítač Win7 Digitální stopa.
3. Přihlaste se
   a. Uživatelské jméno: root
   b. Heslo: root.
4. Otevřete internetový prohlížeč Internet Explorer a stiskněte klávesovou zkratku ALT+X.
5. V nové nabídce klikněte na Možnosti internetu.



Obrázek 16: Kontrola metadat

6. V novém okně otevřete záložku obecné a klikněte na možnost Odstranit.



Obrázek 17: Odstranění historie procházení

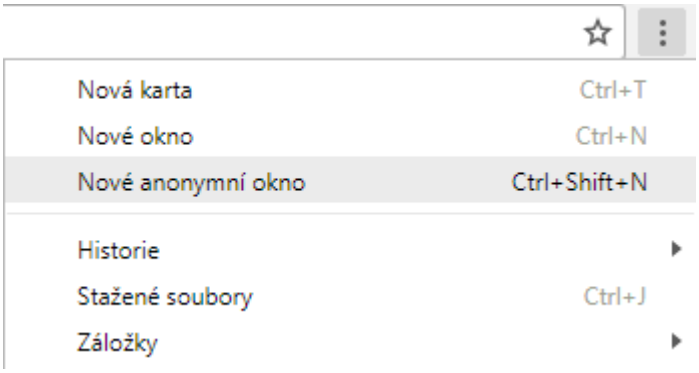
7. V dalším okně zaškrtněte všechny možnosti a klikněte na možnost Odstranit.
8. Po vypnutí a opětovném spuštění prohlížeče je smazaná historie prohlížení, historie stahování, cookies a hesla uložená v prohlížeči.

3.9 Anonymní prohlížení

V předposlední úloze si vyzkoušíte anonymní prohlížení internetu v prohlížeči Google Chrome.

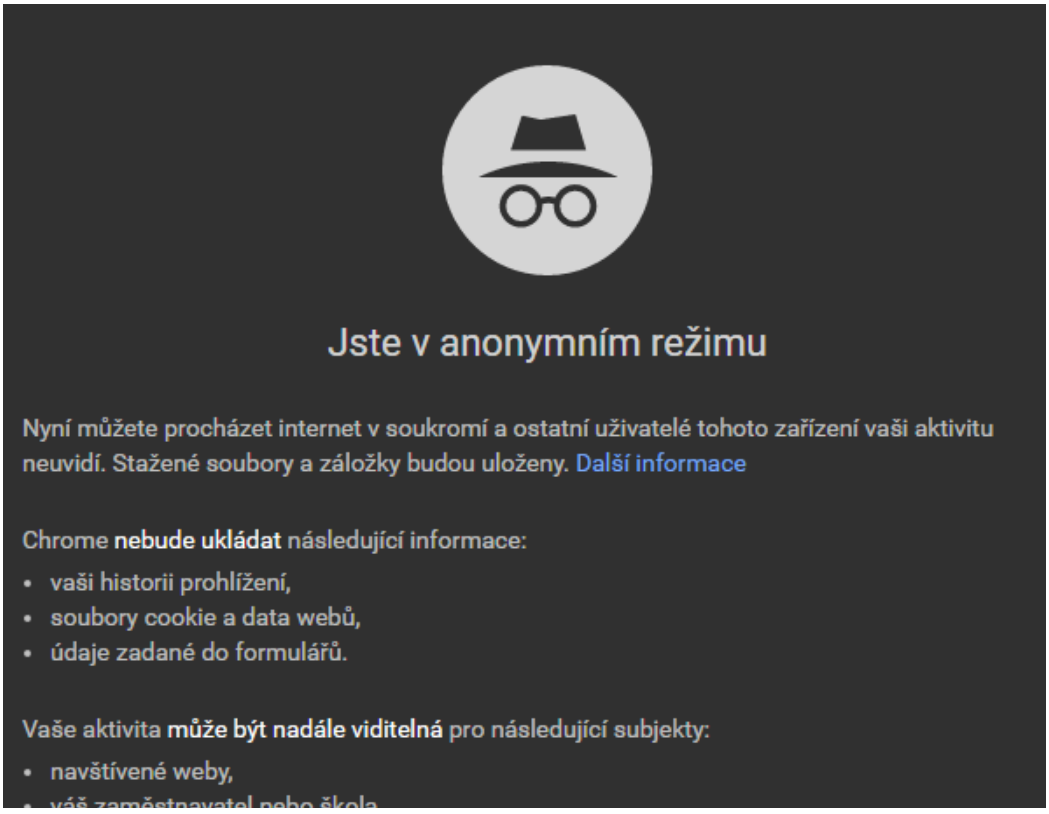
1. Na ploše najděte program Virtual box a spusťte ho.
2. V programu Virtual box spusťte počítač Win7 Digitální stopa.

3. Přihlaste se
    a. Uživatelské jméno: root
    b. Heslo: root.
4. Po přihlášení otevřete internetový prohlížeč Google Chrome.
5. V internetovém prohlížeči je v pravém horním rohu ikona tří teček, která rozbalí nové menu, kde klikněte na možnost Nové anonymní okno.



Obrázek 18: Vytvoření anonymního okna

6. Otevře se nové anonymní okno, ve kterém můžete prohlížet internet stejně jako ve všech ostatních internetových prohlížečích s tím rozdílem, že v prohlížeči nezůstane uložená historie prohlížení, cookies soubory a žádná data vložená do formulářů, o čemž jste informováni hned při otevření anonymního okna.

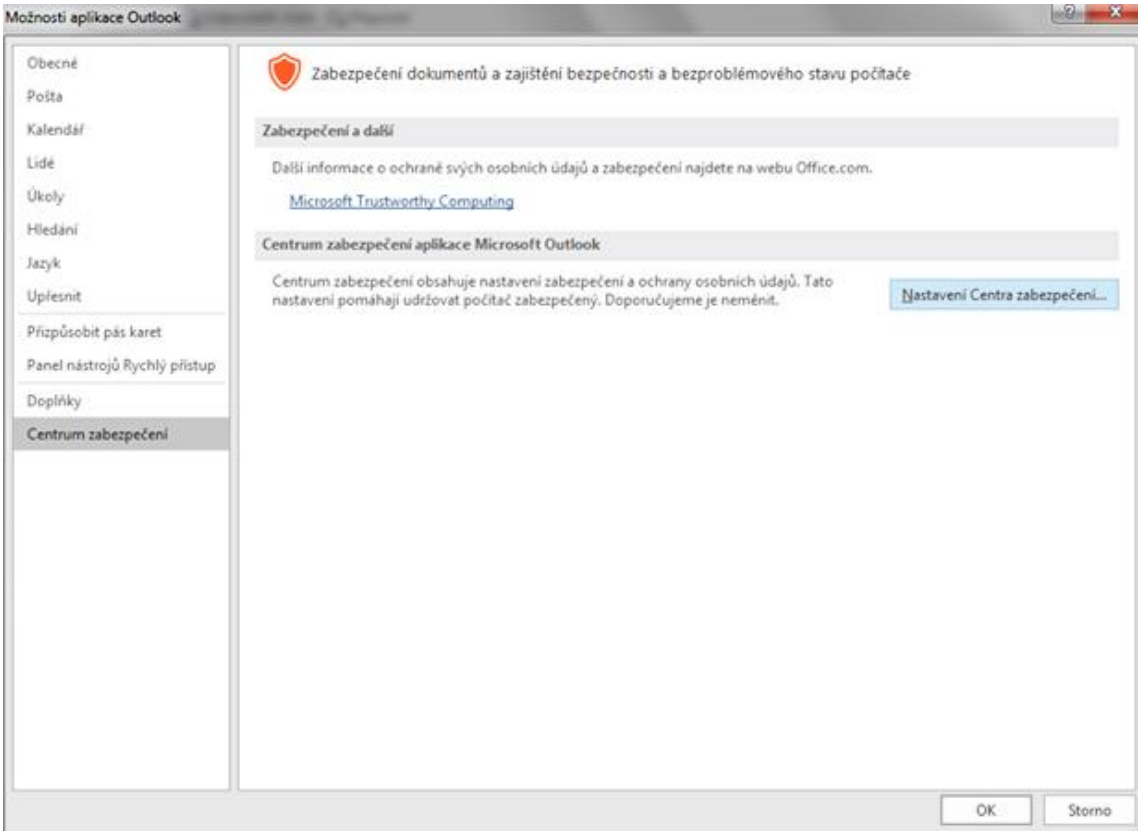


Obrázek 19: Anonymní režim

3.10 Šifrování mailů

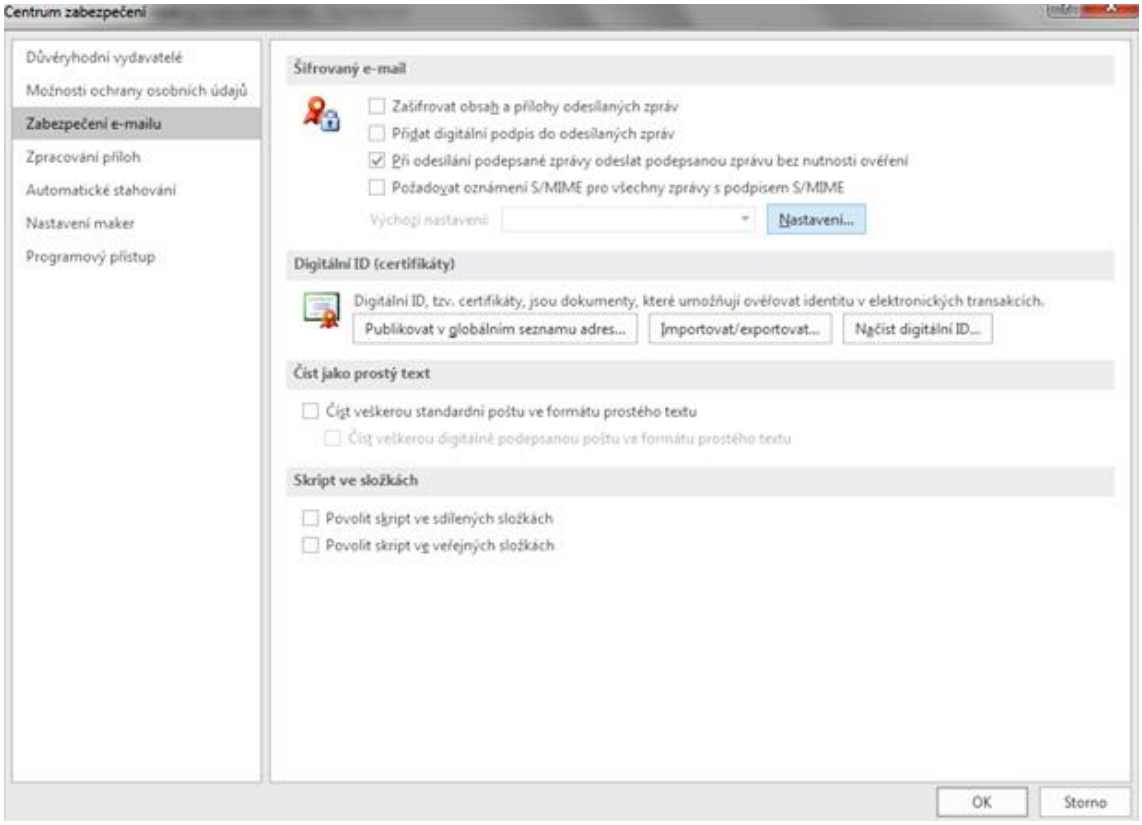
V této úloze se pokusíte zašifrovat všechny odchozí e-maily pomocí programu Microsoft Office Outlook.

1. Na ploše najděte program Virtual box a spusťte ho.
2. Najděte počítač Win7 Šifrování a spusťte ho.
3. Přihlaste se
    a. Uživatelské jméno: root
    b. Heslo: root.
4. Na ploše najděte program Outlook 2016 a spusťte ho.
5. V tomto programu klikněte na možnost Soubor a v novém menu na Možnosti.
6. V novém okně klikněte na Centrum zabezpečení a poté na Nastavení centra zabezpečení.



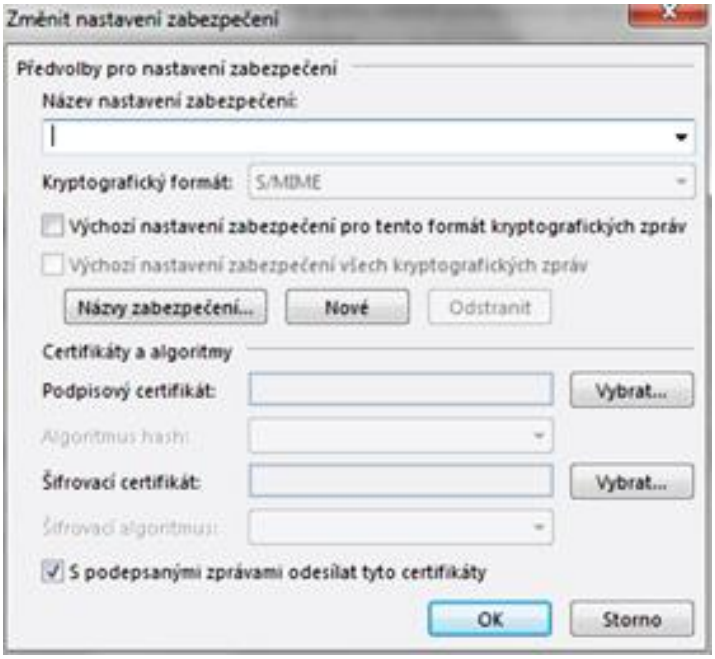
Obrázek 20: Nastavení centra zabezpečení

7. V dalším okně zvolte možnost Zabezpečení e-mailu a poté Nastavení.



Obrázek 21: Zabezpečení e-mailu

8. V posledním okně vyberete Váš podpisový a šifrovací certifikát a kliknete na možnost OK a tímto jste zašifrovali veškerou odchozí poštu.



Obrázek 22: Změna nastavení

4 Diskuse

Byl vytvořen výukový materiál, v němž jsou vytvořeny a vyzkoušeny popsané úlohy. Tyto úlohy mohou posloužit jako výukový materiál pro další studenty z ČVUT a také pro lékařský personál.

Velkou výhodou práce v takové laboratoři je to, že při zkoušení úloh nedojde k porušení zákonů, což by se v reálném prostředí mohlo stát. Dále nemůže dojít k poškození reálných dat či porušení bezpečnosti skutečného systému.

Tato bakalářská práce by mohla posloužit jako předloha pro další rozvoj laboratoře a psaní návazných bakalářských, popřípadě diplomových prací. Mladší studenti oboru biomedicínská informatika by mohli laboratoř dále rozvíjet a vytvořit další navazující úlohy a přispět tím k obecnému vzdělávání lékařského personálu z hlediska bezpečnosti v IT.

5 Závěr

Cílem této bakalářské práce bylo rozšířit virtuální laboratoř v prostorách fakulty a to tím, že v laboratoři budou vyzkoušeny a nasimulovány úlohy na vytvoření hesla, ověření síly hesla, zjištění digitální stopy v prohlížeči a na internetu, smazání a obnovení dat a zašifrovat e-mail.

Tento cíl byl úspěšně splněn a po vyzkoušení a sepsání návodů, jak úlohy v laboratoři provést si myslím, že si tyto úlohy může úspěšně vyzkoušet i naprostý laik. Tato bakalářská práce by měla být přínosem nejen pro studenty FBMI ČVUT, ale také pro lékaře a další zdravotnický personál, který by se po vyzkoušení vytvořených úloh mohl jednoduše vyhnout základním a často se vyskytujícím chybám v praxi.

Seznam použité literatury

[1] *Nejčastější hesla roku 2015: 123456 stále kraluje* [online]. Praha: Svět Androida, 2016 [cit. 2017-08-16]. Dostupné z: https://www.svetandroida.cz/hesla-rok-2015-201601

[2] *Typy virů* [online]. Praha: Robert Havlíček, 2006 [cit. 2017-08-16]. Dostupné z: http://pcviry.wz.cz/list/typyviru.html#trojske

[3] *Antivirový program* [online]. Nový Jičín: Antivirové centrum, 2017 [cit. 2017-08-16]. Dostupné z: https://www.antivirovecentrum.cz/antiviry.aspx

[4] Moderní počítačové viry. *Viry.cz* [online]. Hradec Králové: Igor Hák, 2005 [cit. 2017-08-16]. Dostupné z: https://viry.cz/download/kniha.pdf

[5] 25 nejpoužívanějších hesel za rok 2014 – žádné překvapení. *SW Mág* [online]. Ostrava: Ondřej Dostál, 2015 [cit. 2017-08-16]. Dostupné z: http://www.swmag.cz/novinka/2840/25-nejpouzivanejsich-hesel-za-rok-2014-zadne-prekvapeni/

[6] Poradíme vám, jak prolomit zapomenutá hesla. *Technet.cz* [online]. Praha: Radek Kubeš, 2007 [cit. 2017-08-16]. Dostupné z: http://technet.idnes.cz/poradime-vam-jak-prolomit-zapomenuta-hesla-fkj-/software.aspx?c=A071110_225046_software_vse

[7] Jak na šifrování dat a ochranu systému - 2. díl. *PCWorld* [online]. Praha: IDG Czech Republic, 2013 [cit. 2017-08-16]. Dostupné z: http://pcworld.cz/software/jak-na-sifrovani-dat-a-ochranu-systemu-2-dil-46280

[8] Odebrání skrytých dat a osobních údajů kontrolou dokumentů. *Microsoft Office* [online]. Praha: Microsoft, 2017 [cit. 2017-08-16]. Dostupné z: https://support.office.com/cs-cz/article/Odebr%C3%A1n%C3%AD-skryt%C3%BDch-dat-a-osobn%C3%ADch-%C3%BAdaj%C5%AF-kontrolou-dokument%C5%AF-356b7b5d-77af-44fe-a07f-9aa4d085966f

[9] Šifrování hesel. *Technet Microsoft* [online]. Praha: Microsoft, 2017 [cit. 2017-08-16]. Dostupné z: https://technet.microsoft.com/cs-cz/library/cc733036(v=ws.11).aspx

[10] Hesla a šifrování. *Lupa* [online]. Praha: Lupa, 2017 [cit. 2017-08-16]. Dostupné z: https://www.lupa.cz/specialy/jak-zabezpecit-pocitac-s-windows/hesla-a-sifrovani/

[11] Autentizace, ověření, identifikace. *ManagementMania* [online]. Plzeň: ManagementMania, 2017 [cit. 2017-08-16]. Dostupné z: https://managementmania.com/cs/autentizace-identifikace

[12] KOLOUCH, Jan. *CyberCrime* [online]. Praha: CZ.NIC, z.s.p.o., 2016 [cit. 2017-08-16]. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf

[13] Vymazat se z internetu není možné, velkou část osobního obsahu však odstranit můžete. *Živě.cz* [online]. Praha: CN Invest, 2016 [cit. 2017-08-16]. Dostupné z: https://www.zive.cz/clanky/vymazat-se-z-internetu-neni-mozne-velkou-cast-osobniho-obsahu-vsak-odstranit-muzete/sc-3-a-184259/default.aspx

[14] Po světě se rapidně šíří nový ransomware. Zasáhl sto zemí včetně Česka. *Technet.cz* [online]. Praha: MAFRA, a. s., 2017 [cit. 2017-08-16]. Dostupné z: http://technet.idnes.cz/ransomware-wannacry-wcry-wanncrypt0r-ransomware-f7q-/sw_internet.aspx?c=A170513_070537_sw_internet_vse

[15] Informační bezpečnost. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005, s. 201-214. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-86898-38-5.

[16] Bezpečí na internetu. *Bezpečí na internetu: pro všechny*. Liberec: Dialog, 2014, s. 125-130. Tajemství (Dialog). ISBN 978-80-7424-066-9.

[17] STUCHLÍK, David. *Bezpečnost osobního počítače v ordinaci lékaře zejména z hlediska síťových útoků*. Kladno: ČVUT, 2016. Bakalářská práce, ČVUT, Fakulta biomedicínského inženýrství. Katedra biomedicínské techniky.

[18] Bezpečné mazání dat: žádný problém. *Chip* [online]. Praha: Chip, 2013 [cit. 2017-08-16]. Dostupné z: http://www.chip.cz/casopis-chip/earchiv/rubriky/technika/bezpecne-mazani/

Seznam obrázků

Seznam příloh

Přílohy na CD

Příloha 1 Abstrakt česky (Abstrakt_CJ.pdf)

Příloha 2 Abstrakt anglicky (Abstrakt_AJ.pdf)

Příloha 3 Naskenované zadání BP (Zadani_BP.pdf)

Příloha 4 Bakalářská práce (BP.pdf)