Technické a softwarové prostriedky ochrany počítača v oblasti počítačovej kriminality

Technical and Software Resources for the Protection of Computers Criminality Field

Bc. Patrícia Ševčíková

Diplomová práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Patrícia ŠEVČÍKOVÁ**
Osobní číslo:	**A10341**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Technické a softwarové prostředky ochrany počítače v oblasti počítačové kriminality**

Zásady pro vypracování:

1. **Vypracujte literárnu rešerši k problematike počítačovej kriminality.**
2. **Popíšte obecné bezpečnostné riziká, ktoré súvisia s informačnou kriminalitou a naznačte legislatívne aspekty informačnej kriminality.**
3. **Zamerajte sa na vymedzenie potrieb ochrany dát (formulujte obecné závery vzťahujúce sa k téme), naznačte možné vývojové trendy v uvedenej oblasti pre budúce obdobie.**
4. **V základnom rozsahu identifikujte základné bezpečnostné riziká sociálnych sieti a naznačte možné spôsoby riešenia bezpečnostných problémov sociálnych sieti.**
5. **Zamerajte sa na konkrétny druh bezpečnostného incidentu a uveďte návrh prostriedkov, ktoré vedú k eliminácií dôsledkov a prevencií vzniku incidentu.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **ČANDÍK, Marek. Základy informační bezpečnosti. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004, 107 s. Učební texty vysokých škol (Univerzita Tomáše Bati ve Zlíně). ISBN 80-7318-218-1.**
2. **MATĚJKA, Michal. Počítačová kriminalita. Vyd. 1. Praha: Computer Press, 2002, 106 s. ISBN 80-7226-419-2.**
3. **POŽÁR, Josef. Informační bezpečnost. Vyd. 1. Plzeň: Aleš Čeněk, 2005, 311 s. Vysokoškolská učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-86898-38-5.**
4. **ČERVEŇ, Pavol. Cracking: a jak se proti němu bránit. Vyd. 2. Brno: Computer Press, 2003, 205 s. ISBN 80-7226-382-X.**
5. **REISCHL, Gerald. Sběratelé elektronických dat pod lupou. Vyd. 1. Překlad Alena Bezděková. Praha: Knižní klub, 2001, 254 s. ISBN 80-242-0514-9.**
6. **IVANKA, Ján, NAVRÁTIL, Petr. Digitální stopy a informační kriminalita .In: Security magazín. Roč.XVII, vyd.63, 5/2010, vyd.Familymedia, Praha, 2010 , s.41-43, ISSN 1210 - 8723.**

Vedoucí diplomové práce: **Ing. Ján Ivanka**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **24. února 2012**

Termín odevzdání diplomové práce: **15. května 2012**

Ve Zlíně dne 24. února 2012

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Predmetom predloženej diplomovej práce je zoznámenie sa s problematikou počítačovej kriminality, priblížiť čitateľom odbornej verejnosti základné bezpečnostné riziká, ktoré so sebou prináša Internet a sociálne siete. Zároveň teoretická časť práce obsahuje legislatívne aspekty, ktoré súvisia s danou problematikou v oblasti informačnej kriminality. V praktickej časti sú v základnom rozsahu uvedené možnosti ochrany a zabezpečenia osobného počítača a osobných dát, ktoré sú jeho obsahom. V neposlednom rade sa práca venuje konkrétnemu bezpečnostnému incidentu, v podobe infikovaného súboru, ktorý predstavuje vírus, vrátane vybraných spôsobov jeho detegovania a odstránenia. V konečnej fáze sa praktická časť zameriava na návrh preventívnych opatrení pred realizovaným bezpečnostným incidentom.

Kľúčová slova: počítačová kriminalita, malware, Internet, prevencia, sociálna sieť, ochrana počítača, ochrana dát

ABSTRACT

The aim of the given master thesis is to acquaint the reader with the problematic of computer criminality and to clarify the basic safety risks which are connected with Internet and social networks. The theoretical part includes legislative aspects, which are related to the given problematic in the field of informative criminality. In the practical part, there are given main possibilities of protection and security of computer and personal data. Last but not least problematic of this thesis is related to the concrete security incident in the form of attacked file that contains a virus with the given forms of detection and elimination. In the last phase, the practical part deals with the suggestion of forestallment against the realized security incident.

Keywords: computer criminality, malware, Internet, protection, social network, computer protection, data protection

Poďakovanie patrí predovšetkým vedúcemu mojej diplomovej práce, pánu Ing. Jánovi Ivankovi, za vedenie, odborné rady a cenné pripomienky pri spracovaní práce, bez ktorých by sa predložená diplomová práca nezaobišla. Zároveň by som chcela poďakovať svojej rodine za ich trpezlivosť, pomoc a podporu pri písaní diplomovej práce.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně ……

podpis diplomanta

OBSAH

ÚVOD

Úvod teoretickej časti diplomovej práce je zameraný na definovanie počítačovej kriminality, jej krátkej histórie a zároveň zobrazenie samotnej motivácie jej vzniku. Každý z nás si pod pojmom „počítačová kriminalita“ predstaví niečo iné. Jednotnou myšlienkou by mal byť charakteristický trestný čin, ktorý je páchaný pomocou počítača a iných informačných a komunikačných technológií.

S príchodom nových informačných technológií vznikajú aj nové druhy bezpečnostných incidentov. V diplomovej práci sú prezentované primárne bezpečnostné riziká, s ktorými sa môže bežný užívateľ Internetu stretnúť. V základnom rozsahu sú zobrazené legislatívne aspekty danej problematiky v rámci Slovenskej republiky. Pozornosť je venovaná aj sociálnym sieťam, so zameraním na Facebook, ktorý predstavuje určitý fenomén súčasnosti. Veľa užívateľov sociálnych sietí dôveruje samotnému „virtuálnemu prostrediu“ a zároveň ľudom, s ktorými uskutočňuje konverzáciu. Nie jedenkrát sa stalo, že si užívateľ sociálnej siete sám stiahol nebezpečný vírus. Prostredie sociálnych sietí môže predstavovať základný zdroj pre rozposielanie nebezpečných vírusov. Bezhlavé klikanie na rôzne odkazy a sťahovanie rozličných aplikácií, ktoré nám sociálne siete poskytujú môže mať vážne následky pre samotný počítač užívateľa a dáta, ktoré sú jeho obsahom.

Internet si v našom živote našiel nenahraditeľné miesto. No rovnako, akú veľkú pomoc pre nás predstavuje, môže byť zároveň veľmi nebezpečný. Vzhľadom na túto skutočnosť, je dôležitá užívateľova opatrnosť, prevencia, ochrana, bezpečnosť a v neposlednom rade informovanosť. Nebezpečné vírusy, s ktorými sa ako užívatelia Internetu môžeme stretnúť môžu pre nás predstavovať rozsiahle škody. Škody v podobe finančnej straty, prípadne samotnej straty dát alebo obmedzenie funkčnosti operačného systému, nám môže do rozsiahlej miery znepríjemniť život. Práve preto by sme nemali podceňovať ochranu v podobe firewallu a antivírusového programu. V prípade, ak sú pre nás niektoré dáta v našom počítači príliš citlivé a dôverné, je potrebné sa zamerať na ich ochranu v podobe ich zašifrovania. Zároveň je nutná neustála záloha dát pred možnou stratou alebo poškodením. Cieľom predloženej diplomovej práce je predstaviť čitateľom odbornej verejnosti, ktorých zaujala problematika počítačovej bezpečnosti informatívny materiál definujúci existenciu najznámejších hrozieb. Zároveň poskytnutie návrhu prevencie proti definovaným hrozbám, v podobe uvedenia možnosti ochrany operačného systému a osobných dát, ktoré sú jeho súčasťou.

I. TEORETICKÁ ČÁSŤ

1 POČITAČOVÁ KRIMINALITA

Formulovať presnú definíciu pojmu počítačová kriminalita nie je vôbec jednoduché. Zložitosť stanovenia definície je spojená s rôznosťou chápania samotného pojmu. Počítačová kriminalita predstavuje v súčasnosti závažnú trestnú činnosť. Vo všeobecnosti môžeme charakterizovať počítačová kriminalitu ako trestný čin zameraný na počítač a zároveň trestný čin páchaný prostredníctvom počítača.

Páchanie trestnej činnosti pomocou počítačov v sebe zahŕňa nasledujúce poznatky:

- trestný čin môže byť spáchaný pomocou informačných a komunikačných technológií v priebehu pár sekúnd, pričom nie je nutné aby sa páchateľ nachádzal na mieste páchania trestného činu a poškodená osoba zaznamenala jeho činnosť,
- páchateľ môže uskutočniť trestný čin na veľké vzdialenosti, pričom je schopný si zachovať úplnú identitu,
- ľahká dostupnosť získania vedomosti pre páchanie trestnej činnosti.

Trestná činnosť v oblasti počítačovej kriminality môže byť páchaná okrem počítača a na počítači tiež prostredníctvom počítačových sietí, zneužívanie dát uložených v počítačových systémoch, prípadne prenášaných komunikačnými sieťami. Každý trestný čin predstavuje určité finančné straty a mnohokrát siaha za hranice jedného štátu, čo z neho robí medzinárodnú trestnú činnosť. [1, 2, 3, 36]

1.1 Druhy počítačovej kriminality

Základné všeobecné delenie počítačovej kriminality je delenie na priamu a nepriamu počítačovú kriminalitu.

a) Priama počítačová kriminalita zahŕňa všetky útoky proti počítaču (počítač je terčom útoku). Príkladom priamej počítačovej kriminality môže byť softwarové pirátstvo. Pri tomto druhu počítačovej kriminality je jednoduchšie vyčísliť spôsobenú škodu, ako pri počítačovej kriminalite nepriamej, kedy sa skôr jedná o majetok nehmotný.

b) Nepriama počítačová kriminalita predstavuje trestné činy, ktoré sú páchané prostredníctvom výpočtovej techniky. Jedná sa napríklad o trestné činy ekonomickej povahy, trestné činy, ktoré útočia na súkromie osoby, trestné činy zamerané na zneužitie údajov a dát, útoky na databázu a počítačové programy.[1, 3]

1.2 História počítačovej kriminality

Začiatky samotnej počítačovej kriminality sú spojené so vznikom počítačov. Finančné obohatenie viedlo ku krádeži a zneužívaniu hardvérových a softwarových prvkov počítačov od začiatku ich realizácie. Každý nový vývoj produktov v oblasti komunikačných a informačných systémov prinášal so sebou aj vznik nových foriem kriminality. Kriminalita bola páchaná pomocou alebo prostredníctvom práve novovzniknutých produktov.

Počítačová kriminalita v šesťdesiatych a sedemdesiatych rokoch

Stanford Rearch Institute (SRI) v USA sa staral od roku 1958 až po rok 1978 o zber údajov o zneužití počítačov. V tomto období sa údaje rozdeľovali do štyroch kategórií:

- krádež majetku alebo informácií,
- vandalizmus, ktorý bol namierený proti počítačovému hardwaru,
- podvod realizovaný pomocou počítača alebo krádež peňazí,
- neprípustné použitie počítača alebo krádež a predaj počítačového času.

Významnosť zaznamenaných dát sa prejavila až v roku 1968, kedy bolo zachytených trinásť prípadov. Obdobie šesťdesiatych a sedemdesiatych rokov zahŕňa v sebe rôzne príklady podvodov. Ukážkou môže byť obvinenie viceprezidenta brokerskej spoločnosti z dierovania špeciálnych dátových štítkov, ktorý si previedol na svoj účet 250 tisíc dolárov v priebehu osem rokov. V roku 1977 vzrástol počet zaznamenaných prípadov až na osemdesiatpäť. V novinách s názvom Seed sa objavil článok, ktorý popisoval technológiu zničenia počítača. Predstavujú sa prípady magnetického vymazávania a elektronického monitorovania. V tomto období dochádzalo k rozsiahlej výmene počítačových programov, či dokonca nelegálnemu predaju takýchto nosičov medzi užívateľmi, čo sa považovalo sa pirátstvo.

Počítačová kriminalita v osemdesiatych rokoch

Medzi charakteristické zločiny tohto obdobia môžeme zaradiť krádeže databáz, šírenie vírusov, infiltrácia logických a časových bômb, k rozširovaniu a využívaniu pirátskeho softwaru. Do histórie určite patrí meno Robert Tappan Morris.

Jedná sa o dvadsaťtriročného študenta, ktorý bol tvorcom prvého internetového červa v histórií. Škodlivý vírus červ s názvom „worm“ predstavoval kategóriu škodlivých kódov. Hoci červ tvoril iba deväťdesiatdeväť riadkov programového kódu, dokázal atakovať približne šesťtisíc počítačov. Morrisova obhajoba spočívala v tom, že jeho cieľom bolo uskutočniť experiment, ktorý mal spočítať všetky počítače v rámci Internetu, jeho úmysel nebol spôsobiť škodu. Položme si však otázku, čo ho viedlo k zachovaniu anonymity, prečo červa vypustil z počítačov Massachusetts Institute of Technology, pričom bol študentom Cornell University. Vytvorenie wormu sa mu stalo osudným. R. T. Morris bol historicky prvým obvineným podľa zákona Computer Fraund and Abuse Act (Zákona proti počítačovému podvodu a zneužitia). Jeho trestnom na základe súdneho procesu bolo 400 hodín obecne prospešných prác, tri roky podmienka a 10 050 USD pokuty.

Kevin Mitnick prvý hacker je zaradení v zozname desiatich najhľadanejších osôb americkej FBI. Jeho “sláva“ bola postavená na prienikoch do systémov veľkých firiem ako sú Nokia, Fujitsu, Motorola alebo Sun Microsystems. Škoda firiem siahala na niekoľko stoviek miliónov dolárov, čo pre Kevina M. znamenalo päť rokov vo vezení.

Kevin Lee Poulsen, prezývaný Dark Dante mal prvé problémy zo zákonom už v období puberty. Ako osemnásťročnému sa mu podarilo napadnúť sieť Arpanet (v súčasnosti Internet). Dokázal prevziať kontrolu nad celou sieťou, nájdením chyby v architektúre siete. Niekoľkokrát bol odsúdený a tak si dal pokoj s hackerskou činnosťou. Bohužiaľ neodolal pokušeniu, keď rozhlasová stanica v Los Angeles vyhlásila súťaž o nový automobil Porsche 944S2. Výhra by pripadla súťažiacemu, ktorý by sa dovolal na určené telefónne číslo ako stodruhý volajúci. Poulsen napadol miestnu telefónnu ústredňu, ktorú modifikoval, tak, že v momente spustenia súťaže bolo práve pre neho vyhradené víťazné stodruhé miesto. Cenu dostal, ale FBI začala celú súťaž vyšetrovať. Poulsen bol zadržaný a obvinený zo siedmych trestných činov. Jeho trestom boli štyri roky väzenia, päťdesiatosemtisíc dolárová pokuta a tri roky dostal zákaz pracovať s počítačom.

Počítačová kriminalita v deväťdesiatych rokoch

Na základe štatistiky amerického Národného strediska pre údaje o počítačovom zločine počítačová kriminalita preniká do nasledujúcich oblastí:

- 44 % elektronická krádež peňazí,
- 16 % krádež programov alebo informácií,
- 16 % škody, ktoré boli spôsobené na software,
- 12 % zmena dát,
- 10 % krádež služieb,
- 2 % nedovolený vstup.

Dochádza k celosvetovému rozvoju Internetu. Internet sa stáva nástrojom pre šírenie pornografie, rasizmu, propagácií drog a k prezentácií extrémizmu. Prienik do systému predstavuje pre hackera intelektuálnu výzvu, hackeri sa stali profesionálmi. Cieľom sa pre útočníkov stávajú informácie, uchovávané v počítači.

Vladimir Levin predstavuje ďalšiu významnú osobu v histórií. Interpol ho zadržal vo Veľkej Británii na letisku Heathrow. Vladimir Levin sa vlámal do interných počítačových systémov Citybank, previedol si vyše desať miliónov dolárov na svoje súkromné účty v USA, Fínsku, Holandsku, Nemecku a Izraeli. Po odsúdení ho čakali dva roky nepodmienečného trestu a peňažná pokuta vo výške 240 014 dolárov. Peniaze, ktoré V. Levin odcudzil sa podarilo úradom získať späť skoro v plnej výške. [2, 36]

1.3 Motivácia počítačovej kriminality

Motivácie počítačovej kriminality sú rôzne. Medzi najčastejšie prípady patrí určite finančné obohatenie sa, podvody, popularita či rôzne ideologické dôvody. Páchateľmi často bývajú zamestnanci firmy, ktorí sa chcú pomstiť zamestnávateľovi. Uviedla som prehľad podľa útočníkovej motivácie na základe jeho počítačových znalostí a skúsenosti, podľa názoru Doc. Ing. R. Raka, Ph.D. a Ing. R. Kummera.

Novic

Je závislý na iných osobách, pretože nemá dostatočné znalosti a schopnosti. Novic využíva hackerské nástroje, ktoré sú jednoducho dostupné na Internete. V niektorých prípadoch nemá predstavu ako jednotlivé hackerské nástroje fungujú a čo všetko môžu napáchať. Chce sa zaradiť do skupiny hackerov. Cieľom je vzrušenie, pričiniť sa v hackerskej oblasti.

Kybernetický chuligán

V porovnaní s Novicom ma vyššiu úroveň počítačového vzdelania. Je schopný programovať a vytvárať vlastné programy. Príkladom jeho charakteristických aktivít môžu byť krádež čísel kreditných kariet, spam, telekomunikačné podvody. Cieľom je popularita, pozornosť, sláva. V súvislosti preslávіť sa, preniká do pozornosti štátnych orgánov.

Vnútorný nepriateľ

Do tejto skupiny môžem zaradiť zamestnancov firmy. Dôvody páchania trestnej činnosti môžu byť napríklad nevyhovujúci kariérny rast, nedocenenie, hnev na vedenie, ideologické dôvody. Veľakrát môže byť takýto pracovník IT špecialista, administrátor prípadne z oddelenia manažmentu. Má dostatočné počítačové a informačné znalosti. Cieľom je spôsobiť zamestnávateľovi stratu a pre seba určitý osobný zisk.

Malý zlodej

Cieľom malého zlodeja je finančné obohatenie sa s využívaním informačných a komunikačných technológií. Venuje sa samoštúdiu, pre získanie potrebných počítačových znalostí. Svoju pozornosť sústreďuje na internetové prostredie, elektronické bankovníctvo, obchodovanie, kreditné karty.

Stará garda

Nerešpektuje osobné vlastníctvo a autorské právo. Odbornosť počítačových znalostí a skúsenosti je na vysokej úrovni. Vytvára agresívne programy, napomáha ich šíreniu a používaniu ale v skutočnosti sami neútočia.

Autor vírusu

Jeho počítačové znalosti a skúsenosti sú na odbornej úrovni. Vytvorené vírusy spáchali po svete obrovské škody. Motivácia nie je úplne jasne špecifikovaná. Najčastejšie sa jedná o prekonávanie intelektuálnych výziev.

Profesionálny kriminálnik

Vysoká úroveň odborných počítačových znalostí, ktoré využíva a sústreďuje pre páchanie kriminálnych činnosti. Motiváciou je finančné obohatenie. Prioritou nie je sláva a pozornosť štátnych orgánov. [6, 7]

1.4 Softwarové pirátstvo

Softwarové pirátstvo predstavuje druh priamej počítačovej kriminality. Jedná sa o synonymické označenie pre neoprávnené používanie softwaru, ktorý podlieha ochrane autorským právom. Softwarové pirátstvo sa uskutočňuje pri nelegálnej distribúcií, neoprávnenom používaní, sťahovaní, kopírovaní, upravovaní, rozširovaní a predaju softwaru. Rozšírenou formou softwarového pirátstva je inštalácia kópií softwaru vo väčšej miere, ako je rámec kúpenej licencie do osobného či pracovného počítača. Pri zakúpení softwaru nedochádza ku kúpe vlastného programu (softwaru), kupuje sa iba licencia na používanie softwaru. Obsahom licencie je určenie, akým spôsobom je dovolené so softwarom manipulovať. Príkladom manipulácie, ktorá je obsahom licenčnej zmluvy, môže byť uvedené, koľkokrát je možné nainštalovať software. Softwarovým pirátom môžu byť označené právnické aj fyzické osoby, ktoré protiprávne zaobchádzajú so softwarom. [37]

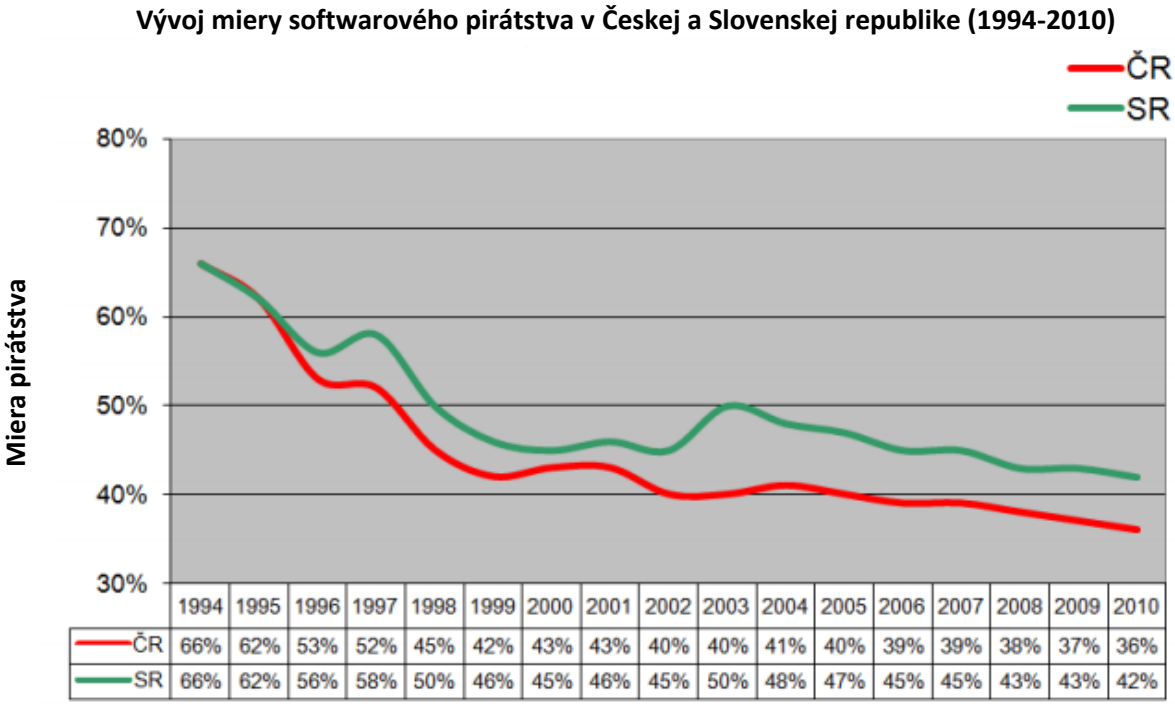
Miera softwarového pirátstva

Popredná organizácia Business Software Alliance (ďalej už iba BSA) je celosvetová organizácia, zaoberajúca sa presadzovaním digitálneho sveta, ktorý je bezpečný a hlavne legálny. Členmi BSA sú spoločnosti Acronis, Adobe, Altium, Apple, Asseco, Autodesk, AVEVA, AVG, Bentley Systems, SA Technologies, CNC Software, Compuware, Dassault Systemes SolidWorks Corporation, DBA Lab S.p.A., Intel, Intuit, McAfee, Microsoft, Minitab, NedGraphics, Progress Software, Siemens, PTC, Quest, Rosetta Stone, SAP, Symantec, Tekla a The MathWorks. BSA sa snaží dávať do popredia dôležitosť softwarového odvetvia pre ekonomický a sociálny rozvoj vo všetkých krajinách sveta. Každý rok jednotlivý členovia BSA uskutočňujú investície v podobe miliardy dolárov do ekonomík jednotlivých štátov. [37, 38]

Tab. 1. Softwarové pirátstvo v regiónoch v percentuálnom vyjadrení. [39]

	2009	2010
Stredná a Východná Európa	64%	64%
Latinská Amerika	63%	64%
Ázia - Pacifik	59%	60%
Stredná a Východná Afrika	59%	58%
Európska únia	35%	35%
Západná Európa	34%	33%
Severná Amerika	21%	21%
Celosvetovo	43%	42%

Miera pirátstva z globálneho hľadiska bola v roku 2010 na ústupe o celé jedno percento, v Európskej únii si svoje percentuálne vyjadrenie zachovala a miera softwarového pirátstva zostala rovnaká, a to 35 %. Podľa BSA je miera softwarového pirátstva v Slovenskej republike pre rok 2010 vyčíslená na 42 %. Vo všeobecnosti je Slovensko zaradené medzi tridsať krajín sveta, ktoré majú najnižšiu mieru softwarového pirátstva. Najrozšírenejšou formou softwarového pirátstva podľa BSA je kúpa jednej softwarovej licencie, ale program je inštalovaný do viacerých počítačov. Podľa tlačovej hovorkyne BSA Slávky Šikurovej boj proti softwarovému pirátstvu je na dobrej ceste i keď nie vo všetkých odvetviach. Úspešnosť sa prejavuje hlavne vo firemnom sektore. Podnikatelia si začínajú uvedomovať významnosť používania legálneho softwaru. So softwarovým pirátstvom je úzko spojená ekonomika celej Slovenskej republiky. Bohužiaľ v súkromnom domácom prostredí je pirátstvo stále problémom. Nové percentuálne vyjadrenie softwarového pirátstva pre rok 2011 by sa malo na stránkach BSA objaviť v máji tohto roku. [37, 38, 39, 40, 41, 42]



Obr. 1. Vývoj miery softwarového pirátstva v Českej a Slovenskej republike (1994 - 2010). [38]

Za softwarové pirátstvo môže dôjsť okrem vysokého finančného trestu aj k odňatiu slobody až na osem rokov. Z finančným trestom súvisí aj zaplatenie pokuty výrobcovi softwaru za spôsobenú škodu, kde táto úhrada môže predstavovať výšku až do sedemtisíc eur. [43]

1.5 Legislatívny rámec informačnej bezpečnosti v Slovenskej republike

Zákon alebo iná legislatívna norma venovaná osobitne počítačovej kriminalite nebola doposiaľ prijatá na území Slovenskej republiky. Legislatívny rámec informačnej bezpečnosti na území Slovenskej republiky je tvorení nasledujúcimi zákonmi:

- *„Zákon č. 22/2004 Z. z. o elektronickom obchode a o zmene a doplnení zákona č. 128/2002 Z. z. o štátnej kontrole vnútorného trhu vo veciach ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.*
- *Zákon č. 211/200 Z. z. o slobodnom prístupe k informáciám a zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov.*

- *Zákon č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.*
- *Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.*
- *Ústavný zákon č. 254/2006 Z. z. o zriadení a činnosti výboru Národnej rady Slovenskej republiky na preskúmavanie rozhodnutí Národného bezpečnostného úradu.*
- *Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.*
- *Zákon č. 300/2005 Z. z. trestný zákon v znení neskorších predpisov.*
- *Zákon č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov.*
- *Zákon č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov.*
- *Zákon č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.*
- *Zákon č. 540/2001 Z. z. o štátnej štatistike v znení neskorších predpisov.*
- *Zákon č. 610/2003 Z. z. o elektronických komunikáciách v znení neskorších predpisov.*
- *Zákon č. 618/2003 Z. z. o autorskom práve a právach súvisiacich s autorským právom v znení neskorších predpisov.*
- *Nariadenie vlády Slovenskej republiky č. 216/2004 Z. z., ktorým sa ustanovujú oblasti utajovaných skutočností.*
- *Metodické usmernenie Úseku bankového dohľadu Národnej banky Slovenska č. 7/2004 k overeniu bezpečnosti informačného systému banky a pobočky zahraničnej banky.*
- *Výnos Ministerstva financií Slovenskej republiky z 8. septembra 2008 č. MF/013261/2008-132 o štandardoch pre informačné systémy verejnej správy, ktorý obsahuje aj bezpečnostné štandardy.“* (35, s. 3, 4)

V nasledujúcich bodoch sú uvedené vyhlášky upravujúce ochranu utajovaných skutočností, ktoré vydáva Národný bezpečností úrad.

- *„Vyhláška Národného bezpečnostného úradu č. 325/2004 Z. z. o priemyselnej bezpečnosti.*
- *Vyhláška Národného bezpečnostného úradu č. 331/2004 Z. z. o personálnej bezpečnosti a o skúške bezpečnostného zamestnanca.*
- *Vyhláška Národného bezpečnostného úradu č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti v znení vyhlášky Národného bezpečnostného úradu č. 315/2006 Z. z.*
- *Vyhláška Národného bezpečnostného úradu č. 337/2004 Z. z., ktorou sa upravujú podrobnosti o certifikácii mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov a o ich používaní v znení vyhlášky Národného bezpečnostného úradu č. 314/2006 Z. z.*
- *Vyhláška Národného bezpečnostného úradu č. 339/2004 Z. z. o bezpečnosti technických prostriedkov.*
- *Vyhláška Národného bezpečnostného úradu č. 340/2004 Z. z., ktorou sa ustanovujú podrobnosti o šifrovej ochrane informácií.*
- *Vyhláška Národného bezpečnostného úradu č. 314/2006 Z. z., ktorou sa mení a dopĺňa vyhláška Národného bezpečnostného úradu č. 337/2004 Z. z., ktorou sa upravujú podrobnosti o certifikácii mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov a o ich používaní.*
- *Vyhláška Národného bezpečnostného úradu č. 315/2006 Z. z., ktorou sa mení a dopĺňa vyhláška Národného bezpečnostného úradu č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti.*
- *Vyhláška Národného bezpečnostného úradu č. 453/2007 Z. z. o administratívnej bezpečnosti“.* (35, s. 3, 4)

Medzi ďalšie právne akty, ktoré sú záväzné pre Slovenskú republiku z dôvodu členstva v Európskej únii, Organizácii pre ekonomickú spoluprácu a rozvoj, Organizácii Spojených národov a Organizácii Severoatlantickej zmluvy patria nasledujúce:

- *„Smernica Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov (Mimoriadne vydanie Ú. v. EÚ, kap.13/zv. 15), transponovaná do zákona č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov.*
- *Smernica Európskeho parlamentu a Rady 1999/93/ES z 13. decembra 1999 o rámci spoločenstva pre elektronické podpisy (Mimoriadne vydanie Ú. v. EÚ, kap.13/zv. 24), transponovaná do zákona č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.*
- *Smernica Európskeho parlamentu a Rady 2000/31/ES z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode (smernica o elektronickom obchode) (Mimoriadne vydanie Ú. v. EÚ, kap.13/zv. 25), transponovaná do zákona č. 22/2004 Z. z. o elektronickom obchode a o zmene a doplnení zákona č. 128/2002 Z. z. o štátnej kontrole vnútorného trhu vo veciach ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.*
- *Dohovor Rady Európy o počítačovej kriminalite z 23. novembra 2001, transponovaný do zákona č. 300/2005 Z. z. trestný zákon v znení neskorších predpisov; podpísali ho členské štáty Rady Európy a ďalšie účastnícke štáty a Slovenská republika ho podpísala a ratifikovala vo februári 2005.*
- *Nariadenie Komisie (ES) č. 831/2002 zo 17. mája 2002, ktorým sa vykonáva nariadenie Rady (ES) č. 322/97 o štatistike spoločenstva so zreteľom na prístup k dôverným údajom na výskumné účely (Mimoriadne vydanie Ú. v. EÚ, kap.1/zv.4).*
- *Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (Smernica o súkromí a elektronických komunikáciách) (Mimoriadne vydanie Ú. v. EÚ, kap.13/zv. 29), transponovaná do zákona č. 610/2003 Z. z. o elektronických komunikáciách v znení neskorších predpisov.*
- *Dodatkový protokol k Dohovoru o počítačovej kriminalite o kriminalizácii činov rasistickej a xenofóbnej povahy spáchaných prostredníctvom počítačových systémov z 28. januára 2003; Slovenská republika ho zatiaľ neratifikovala.*

- *Smernica Rady 2008/114/ES z 8. decembra 2008 o identifikácií a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu (Ú. v. EÚ L 345, 23. 12. 2008).*
- *Smernica Európskeho parlamentu a Rady 2009/136/ES z 25. novembra 2009, ktorou sa mení a dopĺňa smernica 2002/22/ES o univerzálnej službe a právach užívateľov týkajúcich sa elektronických komunikačných sietí a služieb, smernica v sektore elektronických komunikácií a nariadenie (ES) č. 2006/2004 o spolupráci medzi národnými orgánmi zodpovednými za vynucovanie právnych predpisov na ochranu spotrebiteľa (Ú. v. EÚ L 337, 18. 12. 2009); smernica bola v roku 2011 transponovaná do novely zákona č. 610/2003 Z. z. o elektronických komunikáciách v znení neskorších predpisov.*
- *Nariadenie Európskeho parlamentu a Rady (ES) č. 223/2009 z 11. marca 2009 o európskej štatistike a o zrušení nariadenia (ES, Euratom) č. 1101/2008 o prenose dôverných štatistických údajov Štatistickému úradu Európskych spoločenstiev, nariadenia Rady (ES) č. 322/97 o štatistike Spoločenstva a rozhodnutia Rady 89/382/EHS, Euratom o založení Výboru pre štatistické programy Európskych spoločenstiev (Ú. v. EÚ L 81, 31. 3. 2009).“* (35, s. 4, 5)

2 OBECNE NAJZNÁMEJŠIE BEZPEČNOSTNÉ RIZIKA

Internet má v súčasnosti v našom živote nezastupiteľné miesto. Jeho prínos je pre nás nenahraditeľný. Je potrebné si uvedomiť, že rovnako ako veľmi nám pomáha, môže byť zároveň nebezpečný. Práve preto je veľmi dôležitá ostražitosť, opatrnosť, ochrana, bezpečnosť a informovanosť. V nasledujúcej kapitole je definovaný základný a stručný prehľad najzákladnejších nebezpečenstiev, s ktorými sa môžeme stretnúť v praxi, ako používatelia počítača a Internetu. Počítačové vírusy a ostatné druhy malware sú dnes hrozbou, z ktorej určite majú používatelia Internetu strach. Nebezpečné vírusy, s ktorými sa môžeme stretnúť, predstavujú nebezpečenstvo, ktoré môže spôsobiť rozsiahle škody (v podobe finančného charakteru, straty a znehodnotenie údajov, poškodenie mena a značky alebo obmedzenie funkčnosti informačných systémov). Je dôležite im predchádzať a dostatočné chrániť svoje dôverné údaje.

2.1 Hacking

Hacking sa odvádza od slova hack, čo v doslovnom preklade z angličtiny predstavuje slovo rozseknúť. S týmto prekladom sa spája aj samotný význam hackerov. Hacker je v skutočnosti extatický programátor s rozsiahlymi vedomosťami, ktorý sa zameriava na rozoberanie, študovanie rozličných technológií, snaží sa zistiť a pochopiť, ako funguje systém. Dochádza k nesprávnemu spájaniu slova hacker s pojmom počítačový pirát. Informovaná verejnosť používa pre počítačových pirátov označenie napríklad attacker (útočník), cracker alebo spider (pavúk).

Hacker sa nesnaží o napadnutie užívateľa vo svoj prospech, jeho cieľom je riešenie a skúmanie, rozseknutie a prelúsknutie nevyriešiteľných záhad v počítačovom svete, ukazovať možnosti a postupy riešenia. Hacking dnes predstavuje určitý životný štýl, ktorý sa vyznačuje v obohatení seba samého, zvládnutí bariér a napredovaní v rôznych životných sférach. [3, 24, 25]

Existuje rozdelenie hackerov podľa farby klobúka. White hat (biely klobúk) označuje dobrých, etických hackerov, ktorých cieľom nie je spôsobiť škody užívateľa. Snažia sa poukázať administrátorom systému na možné problémy, nežiaduce chyby. Takýchto hackerov si často spoločnosti prenajímajú na testovanie ochrany svojich systémov, určenie miery zabezpečenia a prevencie.

Ďalšou kategóriu tvoria Grey hat (šedý klobúk), takýto hackeri surfujú v prostredí Internetu a snažia sa o prienik do počítačových systémov, nie so zlým úmyslom. Ich cieľom nie je vlastné finančné obohatenie, či spôsobiť škodu užívateľovi, snažia sa poukázať, prípadne informovať administrátora o úspešnosti prieniku do jeho systému alebo zistenia problému. Tretia kategória zahŕňa hackerov, nazývaných Black hats (čierne klobúky). Títo hackeri môžu byť samotnými tvorcami vírusov. Jedná so o hackerov, ktorý sa snažia o poškodzovanie systémov vo svoj prospech dokonca pre finančné obohatenie sa. V niektorých prípadov do tejto kategórie patria aj samotní crackeri (viz kapitola 2.2). Čierne klobúky sa neriadia etikou, ktorú používajú biele a šede klobúky. [3, 25]

2.1.1 Etika hackerov

Hackeri sa držia etiky, ktorá hovorí, že všetky informácie by mali byť slobodné a dostupné zadarmo. Prienik do systému a prístup do počítačov so zámerom pochopiť a naučiť sa ako funguje je prijateľné dovtedy, kým sa hacker nepokúša o krádež alebo poškodenie systému alebo počítača. Hackeri prejavujú skepticizmus voči autoritám, rasistickým a fašistickým hnutiam alebo organizáciám, ktorý sa zameriavajú na šírenie detskej pornografie. V neposlednom rade prejavujú nedôveru voči ľuďom, ktorí sa snažia dostať peniaze od obyčajných používateľov počítača za pochybné služby alebo výrobky, ktoré im ponúkajú. Počítač vie ľudom pomáhať, posúvať život dopredu k lepšiemu. Počítač by mal byť prostriedok pre tvorenie krásy a umenia súčasne. Hackeri by mali byť posudzovaní podľa svojich diel a nie podľa veku, národnosti, pohlavia, pozícií či spoločenskému postaveniu. [3, 24, 25]

2.1.2 Hnutie Anonymous

Hnutie Anonymous je nezávislé združenie hackerov, sieťových aktivistov a iných, ktorí majú radi výstredné žarty. Jedná sa o nehierarchické hnutie, ktoré nemá vytvorenú štruktúru vedenia ani cieľové zameranie. Hnutie Anonymous sa do popredia verejnosti dostalo práve hackerskými útokmi a preto sú vo všeobecnosti chápaní ako hackerské nezávislé hnutie, hoci hacking je iba jedna z mnohých činnosti, ktoré uskutočňujú. Ich cieľom je boj o to, aby bola na Internete sloboda. Členovia hnutia Anonymous reagujú na nové spoločenské problémy. [44, 45]

Maska na nasledujúcom obrázku zobrazuje symbol hnutia Anonymous, ktorým sa predstavujú členovia hnutia. Ako vzor pre svoj symbol (masku) si zvolili Guya Fawkesa, anglického vojaka s katolíckym vyznaním a tiež hrdinu z Mooreovho komiksu V for Vendetta (V ako Vendeta).

Obr. 2. Maska – symbol hnutia Anonymous. [46]

Hnutie Anonymous vyjadrilo svoj názor, presadzovalo svoje záujmy aj v Slovenskej republike, kedy zaútočilo na webovú stránku politickej strany 99% - občiansky hlas alebo pri preukázaní podpory pri proteste Gorila (akcia Gorila – odhalenie korupcie). Dňa 24. januára 2012 sa dve hodiny pred polnocou objavilo video na profile Anonymous, ktorý majú vytvorený na sociálnej sieti Facebook. Obsahom videa bol nasledujúci text. *„Vážení obyvatelia Slovenskej republiky, my sme Anonymous. 24. januára vo večerných hodinách sa uskutoční útok na stránku strany 99 %. Vykradli myšlienku hnutia Occupy a tento čin nesmie ostať nepotrestaný. Práve hnutie 99 % vie, že žiadna politická strana nám požadovanú zmenu neprinesie. My sme Anonymous. Sme légia. Neodpúšťame. Nezabúdame. Očakávajte nás.“(47)* Cieľom hnutia Anonymous bolo uskutočniť DDoS (Distributed Denial of Service) útok, ktorý preťaží internetové servery, čím sa stránka stane neprístupná. Rovnaký útok využili pri proteste Gorila. Zaútočili na internetové sídlo investičnej skupiny Penta a Ministerstvo spravodlivosti Slovenskej republiky. [47, 48, 49]

2.1.3 Legislatíva

Nasledujúca tabuľka obsahuje vyňaté paragrafy, zamerané na hacking, z Trestného zákona (zákon č. 300/2005 Z. z).

Tab. 2. Právna kvalifikácia hackingu vo vybraných paragrafoch Trestného zákona. [3, 13]

Paragraf	Klasifikácia
§ 196	Porušovanie tajomstva prepravovaných správ.
§ 198	Odpočúvanie informácií prenášaných prostredníctvom elektronickej komunikačnej služby.
§ 215	Neoprávnené užívanie cudzej veci.
§ 283	Porušovanie autorského práva

2.2 Cracking

Anglický preklad slova cracking znamená tvorenie prasklín alebo trhlín. Cracker sa snaží o vytvorenie praskliny v samotnom programovom vybavení, so zámerom zmeniť fungovanie programu a tým sa dostať k dátam. Okrem prelomenia ochrany počítača je v jeho snahe získať tajné bezpečnostné kódy alebo zašifrované informácie.

Cracker predstavuje schopného človeka, ktorého cieľom je prienik do systému za účelom škodiť. Zároveň sa snaží o získanie citlivých údajov alebo o finančné obohatenie pre seba, v niektorých prípadoch sa jedná iba o súťaž. Crackeri sa snažia odstrániť ochranu z programov, aby sa programy dali ďalej nelegálne šíriť.

V nasledujúcich bodoch sú zobrazené najpoužívanejšie prostriedky, ktoré crackeri používajú pri vykonávaní nelegálnej činnosti.

- Debugger predstavuje program, ktorý sa používa ako prostriedok na vyhľadávanie chýb v inom programe. *„Zobrazuje zdrojový kód odlaďovaného programu a prostredníctvom simulácie umožňuje nájsť miesto, kde vznikla chyba. Cracker ho používa pre pochopenie funkčnosti a chodu programu a následné odstránenie kódov zabezpečujúcich ochranu.“* (3, s. 40) Sú dva základné typy debuggerov. Prvý z nich je kernel mode debugger, ktorý umožňuje ladiť všetko, čo sa deje v počítači. Druhý s názvom user mode debugger predstavuje obyčajný program, ktorý niekedy nie je nutné ani inštalovať. V porovnaní s kernel mode debuggerom je o niečo slabší.

- Disassembler predstavuje program, ktorý prevádza kód aplikácie, ktorá bola naprogramovaná v hociktorom jazyku do assembleru (jazyk symbolických adries). Disassemblerom vygenerovaný kód nezahŕňa názvy premenných, programov, ani žiadne komentáre. *„Ak sa tento kód po spustení sám upravuje v RAM pamäti alebo ho upravuje iný proces, tak sa tieto zmeny vo výpise nezobrazia, čo predstavuje znaky ochranných prvkov, ktoré využíva cracker na ich odstránenie.“* (3, s. 40)

- Hexadecimálny editor upravuje program priamo v strojovom kóde. Pre lepšiu prehľadnosť sa kód vyjadruje v hexadecimálnej (šestnástkovej) sústave.

- Trasovacie programy zabezpečujú prístup k databáze registrov, ktorá je používaná v operačným systémom Windows. Obsahom databázy registrov sú konfiguračné dáta operačného systému a ostatných nainštalovaných programových vybavení. [2, 3, 15, 16]

2.2.1 Preventívne opatrenia

Registračné číslo (serial number), pre využitie tejto ochrany je potrebné zadať programu určité číslo, ktoré závisí od daných kritérií.
Poznáme niekoľko ochrán, ako môžeme registračné číslo využiť:

- registračné číslo je zakaždým rovnaké,
- registračné číslo môžeme meniť na základné zadaných údajov (meno, názov firmy apod.),
- registračné číslo sa mení podľa počítača užívateľa,
- kontrola registračného čísla sa uskutočňuje on-line prostredníctvom Internetu.

Registračný súbor (key file), býva najčastejšie umiestnený v adresári. Dochádza ku kontrole obsahu programom. Ak je obsah správny, správa sa ako registrovaný. V opačnom prípade je pasívny. Obsahom registračného súboru môžu byť napríklad informácie o užívateľovi.

Časové obmedzenie (time limit). Používanie uvedenej ochrany je veľmi časté. Cieľom autora programu bolo zabezpečenie svojho programu, aby ho nebolo možné ďalej požívať po uplynutí skúšobnej doby.

V nasledujúcich bodoch sú uvedené základné typy ochrany s časovým obmedzením:

- po zadaní správneho registračného čísla sa zruší časové obmedzenie,
- po nahraní registračného súboru dochádza k zrušeniu časového obmedzenia,
- časové obmedzenie sa nedá zrušiť, je možné zakúpiť si originálny program, ktorý je bez obmedzenia,
- časové obmedzenie je obmedzené počtom spustení.

Hardwarový kľúč (nazývaný tiež dongle), kedy nie je možné spustiť program bez hardwarového kľúča, prípadne má program iba obmedzené niektoré funkcie. Na port, kde má byť hardwarový kľúč pripojený, posiela program dáta a následne čaká na odozvu. Ak odozva nepríde, program nie je možné spustiť.

Šifrovanie. Šifrovacie programy spojené s ochranou dátového nosiča proti kopírovaniu predstavujú v súčasnosti využívanú ochranou proti crackingu. Obsahom nosiča sú informácie, ktoré je náročne skopírovať. Zašifrovanie chráneného programu, ktorý je obsahom nosiča, je realizované tak, aby bolo možné jeho spustenie bez potreby inštalácie dodatočného softwaru. Pre dešifrovanie sa používa práve informácia, ktorú nie je možné jednoducho skopírovať. Útok na chránený software opísaným spôsobom môže byť realizovaný vytvorením dôkladnou kópiou originálu. Iný spôsobom je dešifrovanie, pričom útočník musí mať rozsiahle skúsenosti. [15, 16]

2.2.2 Legislatíva

Nasledujúca tabuľka obsahuje vyňaté paragrafy, zamerané na cracking, z Trestného zákona (zákon č. 300/2005 Z. z).

Tab. 3. Právna kvalifikácia crackingu vo vybraných paragrafoch Trestného zákona. [3, 13]

Paragraf	Klasifikácia
§ 215	Neoprávnené užívanie cudzej veci.
§ 219	Neoprávnené vyrobenie a používanie elektronického platobného prostriedku a inej platobnej karty.
§ 226	Podvod.
§ 226	Neoprávnené obohatenie sa.
§ 247	Poškodenie a zneužitie záznamu na nosiči informácií.
§ 264	Ohrozenie obchodného, bankového, poštovného, telekomunikačného a daňového tajomstva.
§ 272	Výroba a držba falšovateľského náčinia, vrátanie programov.
§ 283	Porušovanie autorského práva.
§ 374	Neoprávnené nakladanie s osobnými údajmi.

2.3 Malware

Malware, malicious software preklad z angličtiny znamená zákerný/zlomyseľný software. Predstavuje rozsiahle, spoločné označenie škodlivého softwaru. Môžeme sem zahrnúť napríklad vírusy, trójske kone, spyware, adware apod..

2.3.1 Druhy malware

Počítačový vírus

Počítačový vírus predstavuje program alebo jeho časť, ktorý sa dokáže šíriť vlastným rozmnožovaním z počítača na počítač. Šírenie sa uskutočňuje pripojením ku hocijakému typu súboru alebo odlišnému programu (hostiteľ) bez vedomia užívateľa počítača. Aktivovanie počítačového vírusu sa realizuje spustením infikovaného programu. Cieľom počítačového vírusu je samotné napadnutie a infikovanie počítača a zároveň spôsobiť škodu užívateľovi počítača. Vírusy sa do počítača môžu dostať prostredníctvom bežných prenosových médií (disketa, CD, telefónna linka, pamäte, apod.) alebo tiež prostredníctvom spamu či Internetu. [2, 3, 15, 17, 18, 19]

Rozdelenie počítačových vírusov podľa motivácie:

a. **Deštruktívne vírusy** sa snažia o formátovanie pevného disku, prepisujú náhodne vybraté sektory, zameriavajú sa na zmenu obsahu súborov ich mazanie a šifrovanie dát.

b. **Nedeštruktívne vírusy** disponujú zväčša akustickým a vizuálnym prejavom (zobrazovanie rôznych textových správ).

Rozdelenie počítačových vírusov podľa lokalizácie v pamäti:

a. **Rezidentné vírusy**. Po skončení realizácie infikovaného programu aplikovaním mechanizmu TSR (terminate and stay resident) zostávajú trvalo v operačnej pamäti počítača, nainštalované na vhodné miesto.

b. **Nerezidentné vírusy**, nazývane tiež vírusy priamej akcie, nezostávajú trvalo v operačnej pamäti počítača. Po spustený infikovaného programu, konkrétneho súboru sa začne replikovať. Dochádza k nakazeniu zvyčajne niekoľko súborov v určitom adresári, následne ponechá riadenie infikovanému programu.

Rozdelenie počítačových vírusov podľa cieľa infekcie:

a. **Bootovacie vírusy** sa zameriavajú na systémové oblasti počítača. Ich cieľom je infikácia systémovej oblasti disku, ako napríklad navádzací sektor na začiatku disku, tzv. boot sector. Napadnutím uvedeného sektoru si boot vírus zabezpečí spustenie ešte pred inštalovaním samotného operačného systému.

b. **Súborové vírusy** sa zameriavajú na súbory. Cieľom sú súbory s príponami .exe, .com, .ovl, .bin, .sts, .scr, .obj, .dll. K aktivácií dochádza po spustení napadnutého súboru. Súborové vírusy môžeme ďalej rozdeliť nasledovne:

   - *Prepisujúce vírusy*, natrvalo prepisujú časť kódu súboru na začiatku. Infikovaný súbor prestáva fungovať, ak ho spustíme, dochádza iba k spusteniu kódu vírusu.

   - *Neprepisujúce vírusy,* pripájajú vlastný kód programu na koniec napadnutého súboru, z dôvodu zachovania všetkých informácií potrebných pre správny chod jeho činnosti. Pre okamžitú aktiváciu vírusu po spustení napadnutého súboru, musia na začiatok programu vložiť inštrukciu skoku na telo vírusu.

c. **Adresárové vírusy.** Ich cieľom je infikácia spustiteľných programov. Infikácia sa uskutočňuje nie zmenou kódu programu, ale zameriavajú sa na jeho ukazovateľ v adresárovej položke disku. Ak zobrazíme obsah adresára, všetko sa nám zdá v poriadku, no ak spustíme program, dochádza k spusteniu kódu vírusu.

d. **Duplicitné vírusy** sú ťažko detekovateľné. Vírus napadne súbor s príponou .exe, následne vytvára nový súbor s rovnakým menom, ale miesto prípony .exe použije príponu .com. Takto vytvorený súbor obsahuje telo vírusu. Takže ak otvoríme súbor, automatický sa otvorí ten s príponou .com. Prípona .com sa stáva nadradenou oproti pôvodnej prípone .exe.

e. **Multiparitné vírusy**, predstavujú vírusy, ktoré dokážu infikovať dve alebo viac komponentov počítača (napr. spustiteľné súbory a zároveň boot sektor). [2, 3, 15, 17, 18, 19]

Počítačový červ

Počítačový červ (worm) nepotrebuje hostiteľa. Červ je schopný šírenia samého seba pomocou počítačovej siete. Jeho cieľom je snaha o pripojenie na každý dosiahnuteľný počítač v počítačovej sieti, kde sa snaží využiť pre svoj prenos slabé miesto nedobre zabezpečeného počítača. Nedostatočné zabezpečenie počítača predstavujú hlavne slabiny v operačnom systéme, programového vybavenia nainštalovaného v počítači, ktoré poskytujú sieťové služby. Počítač, ktorý nie je relatívne dobre zabezpečený, poskytuje priestor, kde sa červ môže aktivovať a opäť sa pokúšať šíriť do iných počítačov. Najdôležitejšie proti napadnutiu červa je nepodceňovať zabezpečenie počítačovej siete. [2, 3, 12]

Trójsky kôň

Trójsky kôň predstavuje program alebo jeho časť, nebezpečný kód, ktorý môže byť súčasťou prospešného softwaru, ktorý sa na prvý pohľad zdá pomerne užitočný. Základný rozdiel od vírusov a červa spočíva v tom, že nedochádza k jeho ďalšiemu šíreniu, nachádza sa v napadnutom počítači iba v jednej kópií. Cieľom trójskeho koňa je podobne ako u vírusov napadnutie počítača pomocou škodlivých akcií (prepisovanie údajov, formátovanie pevného disku, diaľkové ovládanie počítača, posielanie prístupových hesiel). Dropper je považovaný za zákerný druh trójskych koňov. Princíp droppera spočíva v napadnutí systému, vypustením rôznych malware v určitých intervaloch. Ďalším nebezpečenstvom, akým môžu trójske kone škodiť, je otvorenie backdoor (zadné vrátka). Útočník (tvorca trójskeho koňa) je schopný sa do systému dostať cez zadné vrátka, pričom nemusí ani poznať prístupové zabezpečenie (meno a heslo). Veľa trójskych koňov sa skrýva v súboroch či programoch s koncovkami napríklad .exe, .bin, .com, .zip apod.. [2, 3, 12]

Spyware

Spyware je program, ktorý je ukrytý v počítači bez vedomia užívateľa. Jeho cieľom je zber citlivých údajov o počítači (software, hardware). Príkladom citlivých údajov môžu byť zoznamy o súboroch, ktoré užívateľ sťahuje z Internetu, užívateľské mená a heslá, e-mailové adresy, zoznam programov, ktoré má užívateľ počítača nainštalované vo svojom počítači, akú aktivitu vykonáva užívateľ na Internete. Zvyčajne nie je spyware programovaný ako samostatný program. Je riešení ako volaná vlastnosť či funkcia, ktorá je pridaná do iného programu navyše. [3, 12]

Adware

Slovné pomenovanie adware predstavuje program, ktorý sťahuje, zobrazuje, prehráva užívateľovi reklamné informácie, „plagáty“ z Internetu. Môže byť súčasťou aktivít reklamných agentúr alebo neraz ho využívajú firmy, ktorých cieľom je poskytovanie služieb druhu „zarábaj cez Internet.“ Obsahom takéhoto reklamného materiálu sú rôzne možnosti hrania hier, otváranie porno stránok, ponuka programov pre prácu s videom apod.. Adware predstavuje značné riziko hlavne v otravovaní užívateľa Internetu počítačovou reklamou. [3, 12]

Dialer

Dialer je slovné pomenovanie pre program, ktorý mení možnosť prístupu na Internet, použitím modemu. Zameriava sa na presmerovanie telefónneho čísla pre internetové pripojenie na čísla s vyššou tarifikáciou (rádovo desiatky centov za minútu). K dialeru sa môžeme dostať pri spustení určitých stránok, príkladom môžu byť rôzne pornografické stránky. V iných prípadoch to môže byť spustiteľný súbor s príponou .exe, ktorý sa ponúka užívateľovi k stiahnutiu bežným dialógom. [3, 18]

Hoax

V skutočnosti hoax nie je vírus, ale je definovaný, ako falošná správa, mystifikácia, podvod alebo žart, ktorý môže napríklad upozorňovať na nebezpečenstvo ohrozenia novým počítačovým vírusom alebo rôzne e-mailové petície, rôzne fámy a varovania apod.. Najvyskytovanejšou formou hoaxu sú nevyžiadané e-mailové správy, ktoré obsahujú falošné prosby o pomoc či rôzne reťazové správy šťastia. V iných prípadoch hoax reaguje na aktuálny stav diania v spoločnosti. Hoax je zaradený do kategórie vírusov práve preto, že vďaka hromadnému šíreniu takýchto správ môže byť v konečnom dôsledku rovnako nebezpečný ako samotný vírus. Najúčinnejšia ochrana pred hoaxom je zamyslieť sa nad samotným obsahom správy a uvedomiť si jeho reálnosť. Veľa známych hoaxov je zobrazených na stránke www.hoax.cz, kde si môžeme preštudovať databázu a porovnať si pravdivosť prijatej správy. Konkrétnym príkladom hoaxu môže byť fáma o spoplatnení sociálnej siete Facebook. Správa znela nasledovné: *„Prevádzkovateľ Facebooku ho zvažuje od 1.1.20011 spoplatniť! Nebude to za veľa, odhaduje sa cena asi 2 doláre, čo je v prepočte cca 1,50 EUR mesačne. Ale... Po celom svete vznikajú petície, ktoré sa proti tomu búria.“* [2, 12, 19, 71]

Makrovirus

Makrovírusy sa zameriavajú na dokumenty. Ich cieľom je vytvárať makra v textovom alebo tabuľkovom procese. Príkladom môžu byť makra uložené v balíku MS Office (MS Word, MS Excel, MS PowerPoint). Tieto makra môžu byť uložené v rovnakom dokumente ako text v MS Worde. Vírusy sa spúšťajú automaticky so spustením Wordu alebo napríklad otvorením dokumentu. Makrovírusy sú pomerne rozšírený druh vírusov, práve vďaka intenzívnej výmene dokumentov prostredníctvom elektronickej pošty. [2, 15]

Bomby

Bomby predstavujú programy, ktoré čakajú na aktivačný podnet po ich spustení. Takýmto podnetom môže byť napríklad aktuálny dátum, čas, zmena súboru alebo kľúč z klávesnice. [2, 17]

2.3.2 Preventívne opatrenia

Je dôležité si uvedomiť, že stopercentná ochrana dát, uložených v počítači, nie je možná. Najprioritnejším cieľom je minimalizácia rizika poškodenia, krádeže a následného zneužitia dát:

- dôležité je používanie antivírusového programu,
- zapnutie brány firewall,
- uskutočňovať na počítači pravidelné prehliadky so zameraním na vyhľadávanie vírusov,
- pravidelná aktualizácia antivírusového programu,
- nepodceňovať zálohu dát na výmenné média,
- v prípade firiem je dôležité vymedziť práva a zodpovednosť používateľov počítačov (bezpečnostná politika organizácia zameraná na ochranu pred počítačovými vírusmi),
- zabezpečenie svojej WiFi siete prístupovým heslom, ktoré bude kombináciou číslic a písmen (malých aj veľkých), neotvárajte neznáme prílohy a odkazy v e-mailovej správe od odosielateľa, ktorého nepoznáte,
- chránenie si svoje e-mailovej adresy,
- ochrana vstupu do počítača heslom,
- vypnúť automatické spúšťanie programov pri vložení média (USB disk, CD, DVD). [12, 28]

2.3.3 Legislatíva

Nasledujúca tabuľka obsahuje vyňaté paragrafy, zamerané na malware, z Trestného zákona (zákon č. 300/2005 Z. z).

Tab. 4. Právna kvalifikácia malware vo vybraných paragrafoch Trestného zákona. [3, 13]

Paragraf	Kvalifikácia
§ 198	Odpočúvanie informácií prenášaných prostredníctvom elektronickej komunikačnej služby.
§ 226	Neoprávnené obohatenie (zásahom do SW, HW počítača).
§ 284	Všeobecné ohrozenie.
§ 361	Šírenie poplašnej správy.
§ 369	Rozširovanie detskej pornografie.
§ 374	Neoprávnené nakladanie s osobnými údajmi.

2.4 Phishing

Samotný názov pochádza z anglického spojenia password fishing, doslovný preklad znamená rybárčenie hesiel. Cieľom útočníka je získať od užívateľa Internetu jeho heslá, identifikačné dáta a iné prístupové údaje. Klasickým a častým príkladom sú hesla používané napríklad k bankovému účtu. Phishing je zvyčajne uskutočňovaný založením novej webovej stránky útočníka. Nová webová stránka je presnou kópiou existujúcej dôveryhodnej stránky. Pri zadávaní mena a hesla do novej phishingovej stránky sa zadané údaje odošlú podvodníkovi, ktorý ich môže potom zneužiť. Inou formou phishingu je rozposielanie e-mailov s cieľom získať dôverné údaje. Obsahom takéhoto e-mailu je žiadosť na používateľa o zmenu hesla, prípadne jeho obnovenie. Phishing zneužíva neopatrnosť užívateľov Internetu. Princípom phishingu je privlastniť si identitu hodnovernej inštitúcie s cieľom získať osobné údaje zákazníkov. K najčastejším osobným a citlivým údajom obetí, ktoré sú cieľom podvodu s názvom phishing patrí napríklad, meno a priezvisko, kód alebo PIN (Personal Identification Number) platobnej karty, číslo bankového účtu, rodné číslo, čísla osobných dokladov, číslo zdravotného poistenia alebo sociálneho či dôchodkového zabezpečenia, prístupové heslá k internetovým službám. [3, 8]

Najúčinnejšia ochrana proti phishingu je opatrnosť pri používaní dôveryhodných webových stránok a e-mailu. Najdôležitejšie je informovanosť klienta od samotnej inštitúcie.

From: WEBMAIL ACCOUNT UNIT
To: undisclosed-recipients:;
Date: Friday, May 22, 2009, 4:19:53 PM
Subject: Overte svoj Slovenská technická univerzita Email ÚČET NA ZABRÁNENIE UZAVRETÍ

===8<==========Original message text==========
Vážení Slovenská technická univerzita webmailovej držiaky

Toto je správa z Slovenská technická univerzita WebMail ÚČTU správ
Centrum pre komunikáciu so všetkými našimi Slovenská technická
univerzita Webmail vlastníkov.

V súčasnosti pracujeme na našej databázy, e-mail V users.We sa
delecting všetky staré nevyužité E-mail Slovenská technická univerzita
Webmail účtu, pre viac priestoru pre nových používateľov.

Ak chcete zabrániť svojmu účtu nemožno delected
z našej databázy, mali by ste o potvrdenie Vašej Slovenská technická
univerzita webmailovej účte okamžite.

Podať informácie o vašom účte nižšie

Webová stránka .....
Užívateľ :.....
Heslo .....
Dátum narodenia: .....
Krajiny alebo územia: .....

Pozor! E-mail vlastníkov, ktorí sa odmietajú podrobiť
jeho / jej e-mailového konta informácií, a to do siedmich dní od tohto
dátumu prijatia bude stráca svoj účet Webmail permanetly.

Ďakujeme vám,

Slovenská technická univerzita Webmail Team

Odošlite e-mailový účet informácií na tento e-mail:
(wwebunitwebaccount2@live.com)

===8<==========End of original message text==========

Obr. 3. Phishing – príklad podvodnej e-mailovej správy. [72]

Na obrázku 3 je ukážka konkrétneho podvodného phishingového e-mailu, ktorý bol rozosielaný prostredníctvom elektronickej pošty v Slovenskej technickej univerzite v Bratislave. Odosielateľ sa snažil získať pod zámienkou aktualizácie účtu od pracovníkov univerzity heslá k účtom ich elektronickej pošty a iných osobných údajov, ako napríklad dátum narodenia. [72]

2.4.1 Preventívne opatrenia

K základným preventívnym opatreniam pred phishingom patria nasledujúce:

- v žiadnom prípade neodpovedajte na e-mail, ktorý obsahuje žiadosť na vaše dôverné a citlivé údaje,
- na webové stránky bánk, alebo iných dôveryhodných inštitúcií sa zásadne pripájajte zo zabezpečeného počítača, ku ktorému nie je voľný prístup alebo ktorý nie je zdieľaný s inými užívateľmi,
- neotvárajte odkazy, ktoré sú súčasťou e-mailov, uprednostňujte tradičnú adresu inštitúcie,
- nenahrávať osobné údaje priamo do formuláru, ktorý je obsahom e-mailovej správy,
- overte si bezpečnosť webovej stránky, skôr ako vkladáte svoje osobné údaje,
- prezývku (nick), pod ktorou budete vystupovať na internete, si zvoľte tak, aby nebolo jednoduché vás podľa nej stotožniť,
- svoje opodstatnenie má zložitosť hesiel, ktoré používate (minimálne 7 znakov, kombinácia písmen a číslic, kombinácia malých a veľkých znakov),
- s heslami je spojená aj ich odlišnosť, t.j. nepoužívať rovnaké heslo na všetkých stránkach,
- dôležitá je kontrola svojich bankových výpisov, každú nedôveryhodnú platbu je potrebné nahlásiť banke,
- používať antivírový program, antispyware, firewall a nezabúdať na ich pravidelnú aktualizáciu. [3, 8, 12]

2.4.2 Legislatíva

Nasledujúca tabuľka obsahuje vyňaté paragrafy, zamerané na phishing, z Trestného zákona (zákon č. 300/2005 Z. z).

Tab. 5. Právna kvalifikácia phishingu vo vybraných paragrafoch Trestného zákona. [3, 13]

Paragraf	Kvalifikácia
§ 215	Neoprávnené užívanie cudzej veci.
§ 221 - § 226	Podvod.
§ 226	Neoprávnené obohatenie sa.
§ 247	Poškodenie a zneužitie záznamu na nosiči informácií.
§ 264	Ohrozenie obchodného, bankového, poštovného, telekomunikačného a daňového tajomstva.
§ 272	Výroba a držba falšovateľského náčinia, vrátanie programov.
§ 283	Porušovanie autorského práva.
§ 374	Neoprávnené nakladanie s osobnými údajmi.

2.5 Spamming

Určite každého z nás obťažujú nevyžiadané správy, ktoré zahlcujú našu súkromnú či pracovnú e-mailovú schránku. Práve takáto nevyžiadaná, hromadné rozosielaná správa sa nazýva spam. Veľakrát sa stáva, že vďaka spamu nemusíme dostať správy, ktoré sú pre nás dôležité. V inom prípade si dokonca môžeme vymazať svoje dôležité správy pri odstraňovaní nežiaducich spamových správ. Spam je zvyčajne odosielaný z neexistujúcich adries. Obsahom môžu byť napríklad komerčné produkty, ale samozrejme tiež nebezpečné vírusy, ktorých cieľom je získať naše citlivé údaje.

Je dôležité chrániť svoju osobnú a pracovnú e-mailovú adresu. K tomu, aby spammer získal našu e-mailovú adresu, sa používajú počítačové roboty, ktoré prehľadávaním internetových stránok zhromažďujú e-mailové adresy. Takýmito stránkami môžu byť napríklad rôzne diskusné fóra, inzeráty, verejné chaty. Stratu ochrany a šírenie našej e-mailovej adresy môžu spôsobiť reťazové správy.

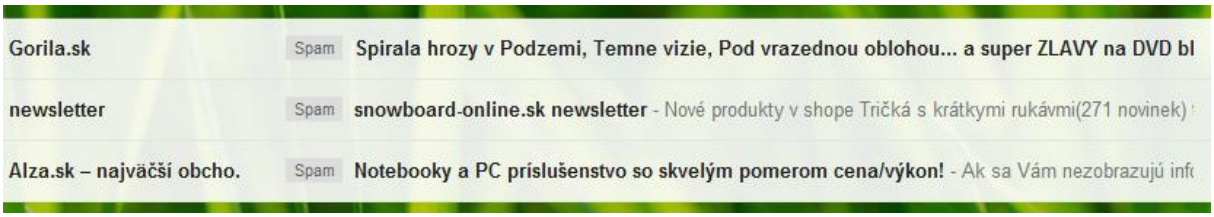
V prípade, ak posielame rôzne komické obrázky, nové hry alebo výstrahy, rozposielame svoju adresu veľkému počtu užívateľov. Čím viac sa jeden e-mail pošle viacerým adresátom, tým naberá na množstve rôznych e-mailových adries. V prípade, ak má jeden z adresátov zavírovaný počítač, môže dôjsť k zneužitiu našej e-mailovej adresy.

Spamy môžeme rozdeliť podľa obsahu na komerčné a nekomerčné. Komerčné spamy predstavujú nevyžiadané komerčné správy, väčšinou rovnakého obsahu, rozličné správy reklamného profilu. Nekomerčné správy, ktoré sú tiež pomenované ako hoax, predstavujú nevyžiadané e-maily s falošnou prosbou o pomoc, upozornenie alebo varovanie pred počítačovými vírusmi, rôzne žartovné a reťazové listy šťastia.

Ďalej spamy môžeme rozdeliť na základe formy šírenia správ. Najčastejšie to môže byť prostredníctvom e-mailu, priamo do súkromnej alebo pracovnej schránky užívateľov Internetu. Inou formou sú spamy šírené v diskusných fórach alebo rôznych komentároch v prostredí Internetu. RSS (Really Simple Syndication) spamy sú založené na využívaní RSS kanálov a nástrojov pre šírenie reklamy a propagáciu. Technológia RSS dáva užívateľovi Internetu možnosť k odberu noviniek z webu. Jedná sa o stránky, kde dochádza k častému pridávaniu či zmene obsahu, napríklad rôzne spravodajské servery. Spamy zneužívajú tiež mobilné telefónne zariadenia pri šírení rôznych reklamných správ.

Nevyžiadané správy sú prijímané formou SMS (Short Message Service) alebo MMS (Multimedia Messaging Service) správ. V neposlednom rade by sme si mali uvedomiť, že papierové letáky supermarketov a hypermárketov sú prakticky tiež považované za spam. V súčasnosti neútočia už iba na naše poštové schránky, ale vo veľkom počte sa stávajú súčasťou našej e-mailovej pošty. [2, 3, 9, 10, 11]

Konkrétnym príkladom z mojej e-mailovej schránky je spam od spoločnosti Gorila. Webová stránka Gorila predstavuje internetový predaj kníh, plagátov, DVD, CD a rôzneho podobného tovaru. Na uvedenú stránku som sa zaregistrovala pri kúpe knihy a odvtedy mi chodia spamy o rôznych novinkách, aktualizáciách, zľavnených kupónoch apod..



Obr. 4. Spam – konkrétny príklad.

Podobným príkladom sú spamové správy od spoločnosti Alza a Snowboard-online. Hoci som si nevybrala možnosť o informovaní noviniek a aktuálnej ponuky, chodia mi nevyžiadané správy. Okrem samotného filtrovania spamu používam dve rôzne e-mailové adresy, aby som osobnú e-mailovú schránku nemala zahltenú prevažne nevyžiadanou poštou.

2.5.1 Preventívne opatrenia

- Legislatívne opatrenie.
- Antispamový filter (nástroj, ktorý dokáže vyhodnotiť prijatú správu alebo sa jedná o spam alebo nie), ktorý by mal poskytovať priamo poskytovateľ mailových služieb na poštových serveroch.
- Vlastná ostražitosť pri zverejňovaní svojej e-mailovej adresy na verejných serveroch. Výhodou je si zriadiť aspoň dve vlastné e-mailové adresy.

Jednu z nich môžeme používať práve pri registrácií na verejných serveroch. Druhú adresu používať zásadne iba pre súkromné prípadne firemné účely.

- Svoje nezastupiteľné miesto pri ochrane proti spamu má osveta a informovanosť ľudí, ktorí začínajú používať e-mailové schránky. Zvyšovať informovanosť (školenie, prednášky, semináre) laickej verejnosti o samotnom spame a možnostiach, ako sa proti nemu brániť.
- Ak ste rozpoznali, že sa jedná o spam, takú správu nikdy neotvárajte, neodpisujte a dôležité je trvalé vymazanie spomínanej správy aj z koša. Väčšina poskytovateľov e-mailových služieb ponúka možnosť označiť takúto správu ako spam. V budúcnosti takáto správa príde automaticky do samostatného adresára.
- Pri výbere poskytovateľa e-mailových služieb si vyberte práve takého, ktorý poskytuje antispamový filter, ktorý presúva spam priamo do samostatného adresára.
- Pravidelná kontrola antispamových filtrov pre prípad, že obsahuje správu, ktorá nemusí byť spam.
- Vlastná inštalácia antispamového filtra, ak nie je súčasťou e-mailového klienta.
- Dôležitá je pravidelná aktualizácia databázy antispamového softvéru.
- V prípade odosielania jednej správy viacerým príjemcom je dôležité si nastaviť odosielanie tak, aby prijímatelia nedostali všetky e-mailové adresy.
- Zaobchádzajte so svojou e-mailovou adresou bezpečne a nezverejňujte ju na rôznych fórach, inzertných a diskusných stránkach. Utajenie svojej e-mailovej adresy je možné nahradením @ slovom „zavináč“, často sa využíva aj „(at)“.
- Čo sa týka samotnej ochrany v oblasti mobilnej komunikácie, je dôležite si utajiť svoje telefónne číslo. V žiadnom prípade neposkytujte svoje telefónne číslo neznámym osobám alebo inštitúciám.
- Účinnosť pred spamom predstavuje metóda blacklist (čierna listina), ktorý si udržuje vlastný zoznam IP adries a domén, z ktorých najčastejšie prichádza spam. V prípade, ak nám príde spam z novej adresy, môžeme pridať nový záznam do existujúceho zoznamu. Každá hlavička prichádzajúceho e-mailu obsahuje informácie o odosielateľovi.

Ak sa tieto informácie zhodujú s nejakou adresou v mojom blackliste, dochádza k automatickému zničeniu prichádzajúceho e-mailu. Nevýhodu predstavuje fakt, že spammeri každú chvíľu menia svoje IP adresy. [2, 3, 12, 14]

2.5.2 Legislatíva

Zákon o elektronickom obchode (zákon č. 22/2004 Z. z).

Zákon o ochrane spotrebiteľa pri finančných službách na diaľku (zákon č. 266/2005 Z. z).

Zákon o reklame (zákon č. 147/2001 Z. z).

Zákon o elektronických komunikáciách (zákon č. 610/2003 Z. z).

Nasledujúca tabuľka obsahuje vyňaté paragrafy, zamerané na spam, z Trestného zákona (zákon č. 300/2005 Z. z).

Tab. 6. Právna kvalifikácia spamu vo vybraných paragrafoch Trestného zákona. [3, 13]

Paragraf	Kvalifikácia
§ 196	Porušovanie tajomstva prepravovaných správ.
§ 198	Odpočúvanie informácií prenášaných prostredníctvom elektronickej komunikačnej služby.
§ 247	Poškodenie a zneužitie záznamu na nosiči informácií.
§ 265	Zneužívanie informácií v obchodnom styku.
§ 284	Všeobecné ohrozenie.
§ 361	Šírenie poplašnej správy.
§ 369	Rozširovanie detskej pornografie.
§ 371, § 372	Ohrozovanie mravnosti.
§ 374	Neoprávnené nakladanie s osobnými údajmi.
§ 423	Hanobenie národa, rasy a presvedčenia.
§ 424	Podnecovanie k národnostnej, etnickej a rasovej nenávisti.

2.6 Pharming

Cieľom pharmingu je získať citlivé údaje užívateľov Internetu, pre finančné obohatenie sa páchateľa. Jedná sa o falošné (totožné stránky, ktoré sú dokonalou kópiou originálu) webové stránky, na ktoré je užívateľ Internetu presmerovaný po prístupe na skutočnú webovú stránku, napríklad stránku banky. Rozdiel oproti phishingu spočíva v tom, že pri pharmingu je užívateľ Internetu presmerovaný na podvodnú stránku až po prístupe na pravú webovú stránku. Takto zneužitý užívateľ webovej stránky svojej banky sa stáva obeťou, bez toho, aby si to uvedomoval. Po pripojení na skutočnú webovú stránku sa po zobrazení identifikačnej stránky nachádza na falošnej, podvodnej webovej stránke. Pri zadávaní identifikačných údajov sa užívateľ stáva obeťou, útočník získava jeho prihlasovacie a zároveň osobné údaje, ktoré zneužíva pri vykonávaní finančných podvodov. Pharming využíva zraniteľnosť DNS (Domain Name Sytem). [3, 12]

2.6.1 Preventívne opatrenia

Medzi základné preventívne opatrenia proti pharmingu môžeme zaradiť nasledovné:

- informovanosť užívateľov Internetu,
- správnosť nastavenia a aktuálnosť antivírusového programu,
- inštalácia firewallu,
- používať software, ktorý chráni pred škodlivými kódmi,
- pravidelná aktualizácia softwaru,
- kontrola bezpečného internetového spojenia k webovým stránkam, na ktorej zadávame citlivé údaje, HTTPS (Hypertext Transfer Protocol Secure) predstavuje šifrovaný prenosový protokol pre zabezpečenie internetového spojenia,
- ochrana klienta banky informovaním SMS správy, ktorá obsahuje kód pre prihlásenie na konto užívateľa. [3, 20]

Obr. 5. Kontrola zabezpečeného spojenia proti pharmingu.

Pri používaní Internetbankingu je dôležité si všímať adresu samotnej stránky banky. Je dôležité, aby bol použitý protokol HTTPS (Hypertext Transfer Protocol Secure), ako je ukázané na obrázku číslo 5 a nie iba obyčajný http protokol.

2.6.2 Legislatíva

Nasledujúca tabuľka obsahuje vyňaté paragrafy, zamerané na pharming, z Trestného zákona (zákon č. 300/2005 Z. z).

Tab. 7. Právna kvalifikácia pharmingu vo vybraných paragrafoch Trestného zákona. [3, 13]

Paragraf	Kvalifikácia
§ 215	Neoprávnené užívanie cudzej veci.
§ 226	Neoprávnené obohatenie sa.
§ 221 - 226	Podvod.
§ 247	Poškodenie a zneužitie záznamu na nosiči informácií.
§ 264	Ohrozenie obchodného, bankového, poštovného, telekomunikačného a daňového tajomstva.
§ 272	Výroba a držba falšovateľského náčinia, vrátanie programov.
§ 283	Porušovanie autorského práva.
§ 374	Neoprávnené nakladanie s osobnými údajmi.

2.7 Sociálne inžinierstvo

Sociálne inžinierstvo je pomerne elegantná a niekedy jednoduchá forma získavania citlivých údajov alebo informácií. Pracuje na základe psychologického podtextu pre získanie dôverných informácií, ktoré môžu byť ďalej zneužité počítačovým pirátom pre spáchanie trestného činu. Sociálne inžinierstvo sa zameriava na najslabší článok informačnej bezpečnosti, ktorú predstavuje samotný človek. Útočník zneužíva ľudskú neopatrnosť, nevedomosť, ľahkovážnosť pri používaní Internetu, aby sa dostal k užívateľovým údajom, ktoré by mohol zneužiť vo svoj prospech. Základným prvkom sociálneho inžinierstva je manipulácia. Útočník sa vydáva za inštitúcie, spoločnosti alebo osoby, ktoré naozaj existujú. Útočník sociálneho inžinierstva musí byť veľmi šikovný hlavne po hereckej stránke, aby bol schopný zahrať na obeť divadlo. Mal by byť vytrvalý, pôsobiť dôveryhodne a vyžarovať určitú charizmu.

Najčastejšia a zároveň najjednoduchšia forma sociálneho inžinierstva sa uskutočňuje prostredníctvom telefónu. Cieľom je získať údaje od obete sociálneho inžinierstva. Útočník je schopný zozbierať voľne dostupné údaje o firme či osobe, na ktorú sa chystá zaútočiť. Pripraví si monológ, ktorý bude pôsobiť dôveryhodne a sebaisto. Najmenej využívanou formou sociálneho inžinierstva je osobný kontakt. Táto forma je náročná, pretože útočník musí byť maximálne pripravený aj po vizuálne stránke. Nesmie mu chýbať skoro dokonalý oblek, firemný preukaz a rôzne iné doplnky, ktoré sú potrebné aby mu obeť útoku uverila jeho identitu. Inými využívanými formami sú útoky sociálneho inžinierstva prostredníctvom Internetu alebo poštou. Cez Internet sa útočník hrá na databázového správcu, administrátora, technika údržby alebo iného špecialistu, ktorý sa snaží vylákať od obete útoku prístupové alebo iné dôverné heslá, aby mohol vykonať opravu alebo odstránenie chyby. Prostredníctvom pošty príde obeti útoku list. List obsahuje všetky náležitosti (meno, adresa, telefón, fax, e-mail, P.O.Box apod.) vymyslenej organizácie. Útočník sa snaží získať dôverné informácie a prihlasovacie heslá. Odpoveď na list si vo väčšine žiada zaslať na uvedený, v skutočnosti vymyslený P.O.Box. [3, 26]

Príklad útoku sociálneho inžinierstva prostredníctvom telefónu:

Obeť: Ševčíková, prosím?

Útočník: Dobrý deň, tu je Michal Novák z oddelenia bezpečnosti IT. Volám vám na základe bezpečnostnej poruchy systému v organizácií. Následne potrebujeme overiť užívateľské meno a heslo všetkých užívateľov systému.

Obeť: Rozumiem, ako vám môžem pomôcť?

Útočník: Potreboval by som vaše používateľské meno a heslo, aby som skúsil urobiť login a zistil tak, či je všetko v poriadku.

Obeť: V poriadku, môžeme to skúsiť.

Útočník: Nadiktujte mi prosím užívateľské meno, ktoré používate.

Obeť: „sevcikova“

Útočník: Ďakujem! Teraz Vás poprosím heslo, ktoré používate.

Obeť: Heslo, ktoré používam je „sobota04“

Útočník: Nemali ste v poslednej dobre problém s prihlásením do systému?

Obeť: Nie, do systému som sa prihlasovala normálne.

Útočník: OK, všetko je v poriadku, v systéme vás už vidím. Všetky by malo fungovať dobre. Ďakujem vám za váš čas a spoluprácu, prajem pekný deň. Dovidenia.

Obeť: Nie je za čo. Som rada, že som mohla pomôcť. Ďakujem, dovidenia. [3]

2.7.1 Preventívne opatrenia

Je potrebné si uvedomiť, že útočník, ktorý sa zameral na získanie našich dôverných dát, bude odhodlaný využiť rôzne formy útokov sociálneho inžinierstva a zároveň využívať ich kombinácie. V nasledujúcich bodoch sú uvedené základné možnosti ochrany pred sociálnym inžinierstvom:

- najdôležitejšie je neposkytovať dôverné informácie osobe, pri ktorej si neviete overiť identitu,
- overiť si skutočnú identitu osoby, ktorá sa snaží dostať k citlivým údajom. Žiadať od osoby preukázania úplných identifikačných údajov,

- firmy by sa mali snažiť o vytvorenie pravidiel, akými možnosťami je dovolené žiadať o dôverné informácie z vonkajšieho prostredia,
- inou formou ochrany organizácií je podrobná kontrola prístupu do budovy a priestorov organizácie. Okrem fyzickej prekážky sa môže využiť technická ochrana v podobe inštalovania kamier. [3, 26, 27]

2.7.2 Legislatíva

Nasledujúca tabuľka obsahuje vyňaté paragrafy, zamerané na sociálne inžinierstvo, z Trestného zákona (zákon č. 300/2005 Z. z).

Tab. 8. Právna kvalifikácia sociálneho inžinierstva vo vybraných paragrafoch Trestného zákona. [3, 13]

Paragraf	Kvalifikácia
§ 215	Neoprávnené užívanie cudzej veci.
§ 221 - 226	Podvod.
§ 226	Neoprávnené obohatenie sa.
§ 264	Ohrozenie obchodného, bankového, poštovného, telekomunikačného a daňového tajomstva.
§ 374	Neoprávnené nakladanie s osobnými údajmi.

2.8 Spoofing

Technika spoofing je využívaná útočníkmi na zmenu (falšovanie) totožnosti pri odosielaní správ. Spoofing nachádza uplatnenie ako základ pri využívaní rôznych druhov počítačovej kriminality. Na báze spoofingu sú páchané napríklad phishing, pharming, spamming.

K najznámejšie používaným metódam spoofingu patrí náhrada e-mailovej adresy pri odosielaní e-mailov, podvrhnutie IP adresy stránky a metóda MITM (man-in-the-middle, preklad: „muž v strede“). V prvom prípade sa jedná o doručenie falošnej správy napríklad klientovi banky. Falošná správa vyzerá, ako by ju odoslala banka, obsahom kolónky odosielateľa je skutočná adresa banky.

Opísaná metóda sa často využíva pri malware a spam. Podvrhnutie IP adresy stránky si nachádza využitie pri pharmingu. Cieľom sú stránky, kde dochádza k overovaniu totožnosti užívateľa, ktorý sa musí prihlásiť. Jedná sa o falošné webové stránky. Takouto podvodnou stránkou môže byť napríklad banka. Webová stránka banky má vo svojom záhlaví skutočnú URL alebo DNS adresu stránky samotnej finančnej inštitúcie, v skutočnosti je užívateľ pripojený na podvodnú stránku. Poslednou a pomerne nebezpečnou metódou spoofingu je metóda MITM. Princíp tejto metódy pozostáva v poškodení komunikácie medzi inštitúciou, konkrétnym príkladom môže byť banka a klient. Útočník sa snaží o narušenie šifrovacieho systému (používaný pri elektronickej komunikácií, na princípe verejného a súkromného kľúča). Aby útočník mohol použiť metódu MITM, musí získať kľúč banky, aby sa mu podarilo narušiť elektronickú komunikáciu medzi klientom a bankou. Banky a mnohé iné inštitúcie mnohokrát samotné kľúče menia pre ochranu svojich klientov. [3, 20]

2.8.1 Preventívne opatrenia

- Nezabúdať na zálohu údajov,
- nastavenie internetového prehliadača tak, aby bol schopný overiť platnosť certifikátu pri elektronickej komunikácií,
- pravidelná aktualizácia operačného systému,
- používanie firewall, ktorý zabezpečuje ochranný múr medzi počítačom a možnou hrozbou na Internete,
- zabezpečenie bezdrôtovej WiFi siete,
- ostražitosť pri prezeraní nezabezpečených webových stránok,
- ochrana súkromnej alebo pracovnej e-mailovej adresy,
- neotvárať neznáme prílohy v e-mailovej správe,
- aktualizácia antivírusového systému,
- ostražitosť pri zdieľaní priečinkov/súborov v sieti. [12, 20]

2.8.2 Legislatíva

Nasledujúca tabuľka obsahuje vyňaté paragrafy, zamerané na spoofing, z Trestného zákona (zákon č. 300/2005 Z. z).

Tab. 9. Právna kvalifikácia spoofingu vo vybraných paragrafoch Trestného zákona. [3, 13]

Paragraf	Kvalifikácia
§ 196	Porušenie tajomstva prepravovaných správ.
§ 198	Odpočúvanie informácií prenášaných prostredníctvom elektronickej komunikačnej služby.
§ 221 - 226	Podvod.
§ 226	Neoprávnené obohatenie sa.
§ 374	Neoprávnené nakladanie s osobnými údajmi.

2.9 Sniffing

Sniffing predstavuje odchytávanie nešifrovanej komunikácie v oblasti počítačovej siete. Odchytávanie komunikácie uskutočňuje páchateľ, ktorý nie je ani adresát ani odosielateľ komunikácie. Cieľom sniffingu je odpočúvanie linky, prostredníctvom ktorej sa prenášajú balíky (pakety) informácií, ktoré majú pre páchateľa príťažlivý význam. Obsahom prenášaných informácií môžu byť rôzne citlivé dáta (heslá, e-mailové správy) užívateľa počítačovej siete. Sniffer, okrem pomenovania páchateľa sniffingu, predstavuje tiež program alebo technické zariadenie (napríklad sieťovú kartu), ktoré slúžia k monitoringu nešifrovanej komunikácie. [3, 21]

2.9.1 Preventívne opatrenia

- najdôležitejšou ochranou proti sniffingu predstavuje šifrovanie komunikácie v počítačových sieťach,
- ochrana osobných citlivých údajov a súbor (zálohovanie),
- používaní silných hesiel.

2.9.2 Legislatíva

Nasledujúca tabuľka obsahuje vyňaté paragrafy, zamerané na sniffing, z Trestného zákona (zákon č. 300/2005 Z. z).

Tab. 10. Právna kvalifikácia sniffingu vo vybraných paragrafoch Trestného zákona. [3, 13]

Paragraf	Kvalifikácia
§ 196	Porušovanie tajomstva prepravovaných správ.
§ 198	Odpočúvanie informácií prenášaných prostredníctvom elektronickej komunikačnej služby.
§ 221-226	Podvod.
§ 226	Neoprávnené obohatenie sa.
§ 376	Neoprávnené nakladanie s osobnými údajmi.

2.10 Warezing

Warezing predstavuje nelegálne kopírovanie a šírenie autorsky chránených prác, najčastejšie v prostredí Internetu alebo prostredníctvom CD a DVD nosičov. Porušovanie autorského práva sa najčastejšie uskutočňuje kopírovaním produktov, ako sú napríklad filmová tvorba, hry, počítačové programy alebo hudobné skladby. Útočník (warezer) sa snaží o nelegálnu výrobu a následné šírenie kópií autorsky chráneného diela. Vo väčšine prípadov nepredstavuje páchateľa jednotlivec, ale môže ísť o nejakú organizovanú warezingovú skupinu. [3, 22]

2.10.1 Preventívne opatrenia

Zápas proti warezingu je pomerne náročný proces a presadzuje sa legislatívnou ochranou. Organizácie väčšinou vo filmovom či počítačovom priemysle, sa snažia presadzovať práva vlastníkov diel. Najznámejšie možnosti šírenia warezu predstavujú systémy FTP (File-Transfer-Protocol) a technológia P2P (peer-to-peer). FTP systém predstavuje nenáročný prenos dát medzi jednotlivými počítačmi, pričom prenos nie je obmedzený operačným systémom. Technológia P2P vznikala v čase, kedy došlo k nárastu užívateľov pripojených na internetové siete. P2P siete nie sú dnes efektívne, pretože je potrebná vysoká rýchlosť pripojenia užívateľa, ktorý zdieľa súbor. [3, 23]

2.10.2 Legislatíva

Zákon č. 618/2003 Z. z. o autorskom práve a právach súvisiacich s autorským právom (autorský zákon).

Nasledujúca tabuľka obsahuje vyňaté paragrafy, zamerané na warezing, z Trestného zákona (zákon č. 300/2005 Z. z).

Tab. 11. Právna kvalifikácia warezingu vo vybraných paragrafoch Trestného zákona. [3, 13]

Paragraf	Kvalifikácia
§ 215	Neoprávnené užívanie cudzej veci.
§ 221-226	Podvod.
§ 226	Neoprávnené obohatenie sa.
§ 247	Poškodenie a zneužitie záznamu na nosiči informácií.
§ 283	Porušovanie autorského práva.
§ 284	Všeobecné ohrozenie.
§ 369	Rozširovanie detskej pornografie.
§ 371, §372	Ohrozovanie mravnosti.
§ 423	Hanobenie národa, rasy a presvedčenia.
§ 424	Podnecovanie k národnostnej, etnickej a rasovej nenávisti.

3 SOCIÁLNE SIETE

Na základe výskumu „Inštitútu pre verejné otázky“ vzniká fakt, že v súčasnosti využíva sociálne siete 54 % slovenského obyvateľstva. Štvrtina populácie pozná, čo sociálna sieť je a ďalšia pätina populácie nemá ani predstavu, čo tento pojem predstavuje. Dominantné miesto v Slovenskej republike patrí sociálnej sieti Facebook. Najväčšiu pozornosť venujem práve tejto sociálnej sieti, ktorá sa v súčasnosti stála určitým fenoménom, pomerne rýchlo došlo k jej rozšíreniu, zároveň je dosť využívaná ako na Slovensku tak aj v Českej republike. Medzi ďalšie najznámejšie sociálne siete v Slovenskej republiky patrí Pokec, iné sú napríklad MySpace, Twitter, Google+ alebo Badoo. Často využívaným prostriedkom komunikácie predstavuje aj ICQ alebo Skype. Sociálnym sieťam prepadajú hlavne študenti, mladí ľudia, ľudia duševne pracujúci a často aj ženy na materskej dovolenke. Určite každého z nás láka predstava „virtuálneho sveta“, v ktorom si môže jedinec vytvoriť vlastnú identitu, podľa svojich predstáv. Takýto „virtuálny svet“ si môžeme vytvoriť prostredníctvom sociálnych sietí. Každá doba so sebou prináša nové príležitosti a možnosti. Sociálna sieť predstavuje komunitu, skupinu ľudí, ktorí sú poprepájaní rôznymi väzbami, napríklad v podobe spoločných záujmov, priateľov, rodinných vzťahov apod.. Prostredníctvom sociálnej siete si jednotlivci vytvárajú vlastné profily, obsahujúce určite údaje o nich. Na základe vložených informácií, údajoch o sebe a zároveň použitím fotografií dochádza k nadväzovaní vzťahov s inými užívateľmi. Súčasťou sociálnych sieti sú rôzne hry, testy, reklamy a iné doplnkové aplikácie, ktoré vedia osloviť svojich užívateľov. Okrem rizík v základnom rozsahu, ktorým sa venujem samostatne v závere tejto kapitoly, nám vo všeobecnosti sociálne siete prinášajú aj svetlú stránku v podobe možnosti komunikácie s priateľmi alebo rodinou, ktorí sú niekoľko tisícok kilometrov od nás vzdialení. Svoje súkromie by sme si mali však dostatočne chrániť a nezverejňovať o sebe na sociálnych sieťach údaje, ktoré by mohli ohroziť našu bezpečnosť a právo na súkromie. Smelo využívajme sociálne siete ako prostriedok pre komunikáciu a vyjadrenie svojich názorov ale skôr ako tak urobíme, by sme si mali premyslieť čo nás môže reálne ohroziť. Veľa ľudí si neuvedomuje do akej miery nám sociálne siete „hltajú“ čas. Mnoho z nás využíva sociálne siete aj vo svojom pracovnom čase, čo môže viesť k zníženiu intenzity práce, pracovnej morálky. Zároveň zvedavosť mladých ľudí vedieť „čo sa deje“, „čo sa stalo“, kto, s kým, aké nové fotky pribudli a mnohé iné uberajú čas, ktorý mohol byť využitý pre iné účely (napríklad školské povinnosti, osobný rozvoj). [66, 67, 68, 69]

3.1 Facebook

Facebook dnes predstavuje obľúbený komunikačný prostriedok, hoci pri jeho vzniku nebolo zakladateľovým cieľom nahradiť osobnú komunikáciu. Facebook vznikol ako vysokoškolský projekt devätnásťročného študenta druhého ročníka Harvardskej univerzity Marka Zuckerberga. V októbri 2003 zrealizoval program s názvom Facemash, čo bol akýsi predchodca Facebooku. Cieľom tohto programu bolo zistiť, ktorá osoba je v škole najpríťažlivejšia. Webovú stránku Facemash spustil 2. novembra popoludní zo svojho notebooku. Používatelia Facemashu porovnávali dve odlišné tváre rovnakého pohlavia a vyberali z nich tú, ktorá sa im zdala viac príťažlivá. V priebehu jedného dňa stránku navštívilo 450 študentov, ktorí stihli ohodnotiť 22 tisíc párov fotografií. Fotografie, ktoré boli v databáze na porovnávanie stiahol Zuckerberg nelegálne z univerzitných databáz. Práve preto oddelenie pre správu počítačovej siete na škole zakročili a vypli jeho prístup na web, pretože jeho stránka nezodpovedala základným podmienkam bezpečnosti dát, ochrane autorských práv a súkromia. Následne musel Mark Zuckerberg predstúpiť pred disciplinárnu komisiu, škola ho však nevylúčila. V roku 2004, 4. februára spustil zo svojej izby na internáte portál TheFacebook, ktorý bol zo začiatku prístupný iba pre harvardských študentov, aby pokryl potreby rozsiahlej verejnosti na Harvarde. TheFacebook mal byť prostriedok na vyhľadávanie ľudí na škole, pomôcka pre zistenie, kto zdieľa s vami rovnaké hodiny, vyhľadávanie priateľov prostredníctvom svojich priateľov apod.. V priebehu štyroch dní od spustenia sa prihlásilo 650 študentov. Ako spoluzakladateľ sa uvádza Eduard Saverin, ktorý Markovi poskytol prvý finančný vklad pre rozbehnutie projektu, čím získal 30 % spoločnosti. Facebook sa stál otvorený naozaj pre každého až 26. septembra v roku 2006, kedy si mohol konto založiť každý, kto spĺňal vek nad trinásť rokov a vlastnil platnú e-mailovú adresu. V roku 2010 dosiahol Facebook pol miliardy registrácií. S novým objemom užívateľov, prichádzali aj nové problémy zamerané na neuspokojivú úroveň ochrany súkromia a zneužívanie dát samotných užívateľov. Dnes už Facebook poskytuje možnosti nastavenia si svojho súkromia, čo by mal každý užívateľ urobiť hneď po registrácií do sociálnej siete. Je iba na nás, aké fotky a informácie sme ochotný o sebe zverejniť a s kým ich chceme zdieľať. V súčasnosti nie je Facebook už iba predmetom zábavy pre mladú populáciu ale dokáže meniť spôsoby komunikácie a vzájomného pôsobenia ľudí, marketingové stratégie, politické a vládne kampane. [69, 70]

3.2 Bezpečnostné riziká sociálnych sieti

3.2.1 Najväčšie bezpečnostné riziká

Medzi rozsiahle bezpečnostné riziká sociálnych sieti môžeme zaradiť nasledovné:

- ohrozovanie mladistvých,
- dôverčivosť mladistvých a s tým spojená hrozba pedofílie,
- fotografie na sociálnych sieťach ako základná informácia pre potenciálneho zamestnávateľa,
- status, ako prostriedok informácie pre potenciálneho zlodeja,
- strata súkromia a ohrozenie osobných údajov,
- sociálne siete ako prostredie pre šírenie malware.

Najväčšie riziká sociálnych sieti sú spojené s ohrozovaním mladistvých. Mladiství, ktorí si vytvárajú profily na sociálnych sieťach nemajú dostatočné vedomosti o rizikách spojených s ochranou súkromia. Väčšina z nich na Internete uvádza svoje pravé osobné údaje, ktoré môžu byť súčasťou Internetu naveky a ktokoľvek má k nim prístup. Uvádzajú pravdivé mená, adresu bydliska, adresu školy. Takto vytvorený virtuálny svet jedinca môže mať vážne následky v reálnom živote, kedy môže dochádzať k reálnym útokom alebo k obťažovaniu.

Reálnou hrozbou sociálnych sietí predstavuje aj pedofília, kde sa útočníci tvária ako vrstovníci, čím sa snažia získať dôveru od svojich naivných obetí, ktoré si neuvedomujú riziká sociálnych sieti.

Inou formou bezpečnostného rizika, ktoré so sebou sociálne siete prinášajú je zverejňovanie fotografií. V prípade hľadania nového zamestnania, môže budúci zamestnávateľ navštíviť stránky sociálnych sieti. Práve na základe fotiek, ktoré sú súčasťou sociálnych sieti si môže potenciálny zamestnávateľ urobiť svoj vlastný obraz a následne posúdenie uchádzača o zamestnanie.

Zároveň určité riziko predstavuje aj vytváranie statusov. Status je jeden z mnohých súčasti komunikácie prostredníctvom sociálnej siete Facebook. Užívateľ uverejňuje text, ktorý si následne môžu prečítať ostatní užívatelia, podľa úrovne zdieľania, ktorú si sami nastavia.

Status môže obsahovať maximálne štyristodvadsať znakov. Status môžu ostatný užívatelia komentovať, označovať tlačidlom „páči sa mi to“.

Nespočetnekrát sa stávajú obsahom týchto statusov užívateľove plány blízkej budúcnosti, ako napríklad balenie sa na dovolenku, s konkrétnym dátumom a dĺžke dovolenky. Takýto status môže byť jasnou a priamou informáciou pre zlodejov, ktorí neváhajú využiť príležitosť navštíviť užívateľovu domácnosť bez jeho súhlasu.

Nie každý užívateľ sociálnej siete uvádza pri registrácií svoje pravé osobné údaje, ako sú meno, priezvisko, rok a dátum narodenia a pod.. Veľa z nás sa chráni a prejavuje nedôveru voči sociálnym sieťam. No je veľa i takých, ktorí vypĺňajú všetky údaje, vytvárajú si kompletné profily, kde zverejňujú citlivé údaje o sebe. Veľa ľudí využíva sociálne siete iba ako prostriedok komunikácie s rodinou, ktorá je vzdialená tisícky kilometrov. Iní užívatelia sú zvedaví čo sa aktuálne deje v spoločnosti. Aké sú trendy alebo všeobecé dianie. Zaujímajú sa o súkromie svojich priateľov, ich život, prácu, záujmy o priateľov ich priateľov apod.. Strata súkromia a ohrozenie našich samotných citlivých údajov je možná iba do tej miery, ako si to užívateľ sám nastaví. Je pravda, že nátlak spoločnosti a samotná zvedavosť sú silnou motiváciou pre uskutočnenie registrácie do niektorých zo sociálnych sietí. Treba si však uvedomiť, že nikto nás predsa nenúti byť súčasťou sociálnej siete, zverejňovať o sebe fotografie a iné osobné údaje.

V neposlednom rade predstavujú sociálne siete terč pre šírenie vírusov, spamu a iného škodlivého malware, ohrozujúci samotný operačný systém a zároveň dochádza k ohrozeniu dôverných dát, ktoré sú obsahom počítača, ktorý sa stal obeťou útoku.

Existuje kampaň inštitúcií EÚ s názvom „Rozmýšľaj kým niečo zverejníš“, určená pre dôverčivých a nerozumných užívateľov sociálnych sietí. Cieľom kampane je zvýšiť vedomosti a informovanosť užívateľov o rizikách, ktoré zo sebou prinášajú sociálne siete a zdieľanie svojich osobných informácií s neznámymi osobami. [66, 67, 68, 69]

3.2.2 Možné spôsoby riešenia

Veľa z nás rozpráva o tom, ako je pre nich dôležité súkromie a sami si vyberáme cestu, ako o sebe zverejniť čo najviac informácií, či fotografií na sociálnych sieťach. Aj nevedomá informácia o nás, publikovaná inými je určitý zásah do súkromia. Takúto nevedomú informáciu môže predstavovať fotografia, ktorej súčasťou sú aj iní ľudia. Je dôležité si chrániť svoje súkromné a osobné údaje. Mali by sme si uvedomiť, že sociálne siete do určitej miery môžu byť prostredím pre tvorbu falošných priateľstiev. Práve preto je dôležité si uvedomiť, že prostredie sociálnych sieti nie je uzavreté a bezpečné. Hocičo čo o sebe zverejníme sami či niekto iný, zanecháva na Internetu určitú digitálnu stopu.

Prvé dva body prechádzajúcej kapitoly sú zamerané na mladistvých a ich pôsobenie na sociálnych sieťach. Veľa z nich si neuvedomuje riziko ohrozenia majetku či samých seba. Pedofília ma na sociálnych sieťach svoje početné zastúpenie. Treba sa zamyslieť a prísť na myšlienku, že štrnásťročná Kata môže byť v skutočnosti tridsaťdeväťročný pedofil. Ochrana by sa vzťahovala na samotných mladistvých užívateľov a ich rozsiahlu informovanosť, aké následky do budúcna môže mať ich nepremyslené konanie na sociálnej sieti. Zásah rodičov, kontrola súkromia mladistvých, poznanie ich hesla, je otázkou dôvery. Prvým krokom ochrany sú rodičia, ktorí by mali byť natoľko informatívne vzdelaní, aby mohli poskytnúť dostatočné informácie mladistvým o možných rizikách a hrozbách sociálnych sietí.

Je dôležité dávať pozor, čo o sebe píšeme, aké statusy zverejňujeme. Nemusí predsa každý vedieť, čo sme práve urobili a kde sa chystáme budúci týždeň na dovolenku. Zamyslime sa nad tým, či chceme mať databázu priateľov iba o určitej skupine ľudí, s ktorými sa stretávame. Ľudí, ktorých dobre poznáme a vieme, čo od nich môžeme čakať. Sociálna sieť nám v tomto prípade slúži ako komunikačný prostriedok pre rýchlu komunikáciu. Druhou možnosťou je databázu zahltiť neznámymi osobami, ktorých zaujímajú naše fotoalbumy, miesto štúdia alebo aktuálna adresa bydliska.

V neposlednom rade si chráňme svoj počítač a osobné dáta pred nebezpečenstvom v podobe vírusov alebo spamu. Nemali by sme zabúdať na pravidelné zálohovanie dát, pred poškodením alebo úplným zničením. S tým súvisí ochrana v podobe antivírusového programu, používanie brány firewall a hlavne ostražitosť pri klikaní rôznych odkazov a sťahovaní nebezpečných súborov z Internetu alebo e-mailových správ. [68, 69, 82]

II. PRAKTICKÁ ČÁSŤ

4 OCHRANA POČÍTAČA

Obsahom nasledujúcej kapitoly je v základom rozsahu zobrazená ochrana počítača, ktorú si užívateľ môže realizovať sám hneď po zapnutí počítača. Cieľom kapitoly je predstaviť užívateľovi základne možnosti ochrany počítača, ktoré má v ponuke v samotnom operačnom systéme. Ochrana počítača je vo všeobecnosti rozdelená na ochranu softwarovú a ochranu hardwarovú. Softwarová ochrana počítača je realizovaná prostredníctvom antivírusových programov, firewallov, ochranou heslom apod.. Hardwarová ochrana je realizovaná napríklad pomocou rozširujúcej karty.

4.1 Softwarové prostriedky

4.1.1 Antivírusový program

Antivírusový program slúži k vyhľadávaniu škodlivého a nebezpečného softwaru. Ak užívateľ nepoužíva žiadny antivírusový program, dochádza k ohrozeniu počítača nežiaducim softwarom, ktorý môže spôsobiť škody. Nastáva aj ohrozenie iných počítačov, pretože môže dôjsť k rozšíreniu vírusov.

V nasledujúcich troch skupinách som uviedla rozdelenie služieb, ktoré nám poskytujú antivírusové programy.

a) Konkrétne antivírusové techniky:
   - rezidentná ochrana,
   - hľadanie známych reťazcov.

b) Všeobecné antivírusové techniky:
   - porovnávací test,
   - heuristická analýza.

c) Preventívna ochrana. [2, 29, 30, 31]

Konkrétne antivírusové techniky vyhľadávajú vírusy, ktoré sú známe v súlade s vírusovou databázou (hľadanie známych reťazcov). Antivírusový program si vytvorí vlastnú vírusovú databázu, ktorá si vyžaduje pravidelnú aktualizáciu. Pri nájdení vírusu je možnosť tento vírus odstrániť zo súborov alebo z boot sektorov.

Odstránenie sa dá realizovať na základe informácií o víruse, ktorý daný súbor infikoval. Taktiež ak použijeme pôvodné informácie o súbore, ktoré opisujú, ako súbor vyzeral pred nakazením.

Rezidentná ochrana je účinnou metódou pri odhaľovaní vírusov v počítači. Prostredníctvom rezidentnej ochrany je možné vírusy, ktoré sú obsahom vírusovej databázy, vyhľadať v každom súbore, s ktorým pracujeme (otváranie, kopírovanie). Tiež vyhľadáva vírusy v zavádzacích sektoroch diskiet, ktoré vkladáme do počítača. Keď zapneme počítač, dochádza k spusteniu antivírusového programu. Antivírusový program má dohľad na miesta, ktoré sú náchylné na napadnutie a tiež stráži súbory, ktoré sa práve používajú.

Úlohou a cieľom všeobecných antivírusových techník je lokalizácia a následné odstránenie doposiaľ neodhalených vírusov. Jednou z metód je používanie porovnávacieho testu. Ak spustíme porovnávací test prvýkrát, program si zapíše rozhodujúce informácie o súbore, ako sú napríklad jeho veľkosť, dátum alebo čas. Pri opätovnom používaní testu dochádza k porovnaniu zapísaných informácií s aktuálnym stavom. V prípade, ak sa údaje zmenili, objavuje sa možnosť, že na počítač zaútočil vírus.

Ďalšou a známou metódou je heuristická analýza, ktorá je nezávislá na vírusovej databáze. Heuristická analýza sa sústreďuje na analýzu obsahu súborov, ktoré sa nachádzajú na pevnom disku. Pri vykonávaní analýzy vyhľadáva rôzne podozrivé konštrukcie, ako sú napríklad priamy zápis na disk alebo prevzatie kontroly nad operačným systémov apod.. Pri využívaní heuristickej analýzy sa zároveň vykonáva aj test na známe vírusy. V tomto prípade môže nastať prípad, kedy je súbor označený ako napadnutý, následne dochádza k prehľadávaniu vírusovej databázy a po identifikácií vírusu je meno vírusu vypísané. V prípade, ak sa vírus v databázy nenachádza, je označený ako neznámy. Poznáme tiež plnú heuristickú analýzu, nazývanú tiež heuristickou analýzou s emuláciou[1] kódu. Tu sa antivírusový program snaží o napodobenie činnosti počítača pri spustení programu. V praxi dochádza k častým falošným poplachom, kedy sú určité súbory označené ako infikované.

[1] Emulácia znamená schopnosť napodobniť jeden systém iným systémom.

Preventívne antivírusové techniky sa využívajú pred usadením vírusu v počítači. Ich cieľom je odhaliť a (ak je to možné) odstrániť nežiaduci vírus skôr, ako sa skopíruje do počítača. [2, 29, 30, 31]

4.1.1.1 Najznámejšie antivírusové programy

Medzi najznámejšie a zároveň najviac využívané antivírusové programy v Slovenskej a Českej republike môžeme zaradiť Eset, AVG, Aviru, Norton a Microsoft Security Essentials. Každý z uvedených antivírusových programov poskytuje v menšej či väčšej miere komplexnú ochranu počítača. Niektoré z nich sú vydávané tiež s rozšírenou verziou s firewallom, často sú označované ako „internet security". Je na jednotlivcovi, ktorý z antivírusových programov si vyberie. Rozhodnutie je individuálne na základe predchádzajúcich skúsenosti, odporúčaní či samotnej recenzie antivírusového programu rôznymi užívateľmi.

ESET NOD32 Antivirus

Pre rok 2012 prichádza Eset s piatou generáciu NOD32, s presným názvom ESET NOD32 Antivirus 5, ktorý poskytuje kompletnú ochranu, s jednoduchým rozhraním, pri minimálnom spomaľovaní systému. Jeho súčasťou sú najnovšie technológie detekcie zamerané na ochranu proti malware, adware či spyware. Chráni užívateľa na Internete pred možnými hrozbami v reálnom čase. Eset predstavuje pre užívateľa jednoduchú inštaláciu. Nová generácia ponúka užívateľovi rýchlejšie skenovanie pri nízkej záťaži systému. Eset je jeden z najvyužívanejších antivírusových programov, ktorý chráni užívateľa pri sťahovaní dát, komunikácií na sociálnych sieťach, výmene súborov prostredníctvom USB či iného prenosového média. [75, 76]

AVG Anti-Virus 2012

Nové funkcie, ktoré sú súčasťou antivírusového programu AVG sa zamerali aj na vylepšenie ochrany v oblasti sociálnych sietí. Zároveň poskytuje AVG vysokú ochranu pred najnovšími vírusmi, červami alebo trójskymi koňmi, zároveň ochranu pred malware, adware a spyware. Aj AVG je známy jednoduchou inštaláciou, ktorá si nevyžaduje reštart pre úspešnú inštaláciu. Poskytuje jednoduché rozhranie pre skenovanie a samotné odstránenie nájdenej infekcie. Samozrejme aj AVG uskutočňuje automatickú aktualizáciu svojej vírusovej databázy. [75]

Avira Antivir Premium 2012 Antivirus

Avira má tiež svoje vedúce postavenie na trhu v oblasti informačnej bezpečnosti. Svojmu užívateľovi môže poskytnúť kvalitnú funkciu skenovania a ochranu pred trójskymi koňmi, červami a iným škodlivým malware. Zároveň predstavuje aktívnu ochranu pred phishingom, ponúka detekciu neznámych vírusov na základe ich správania. Samozrejmosťou je ochrana pred hrozbami z rôznych webových stránok, pred sťahovaním alebo surfovaním na Internete. Inštalácia nie je náročná a spomalenie systému je minimálne. Ochrana v reálnom čase chráni počítač pred možnou nákazou. Aktualizácia sa uskutočňuje automaticky, ale zároveň je možná manuálna kontrola aktualizačného balíčka. [75]

Norton 2012

Vynikajúcu ochranu pred hrozbami v podobe vírusov či spyware, trójskymi koňmi, apod. predstavuje aj antivírusový program Norton. Poskytuje užívateľovi vysoký výkon, ktorý nespomaľuje počítač. Zabraňuje prístupu útočníkov do počítača a chráni informácie, ktoré sú jeho obsahom. Poskytuje bezpečné sťahovanie súborov, on-line bankové transakcie alebo bezpečné prezeranie webových stránok. Pri zistení nebezpečnej webovej stránky dochádza k automatickej blokácií. Rýchlo identifikuje a zastaví nové hrozby, ktoré môžu ohroziť počítač. Okamžite reaguje na prítomnosť vírusov, podozrivých odkazov, infikovaných príloh a iných nebezpečenstiev ešte pred ich otvorením či spustením. Poskytuje rodičovskú kontrolu riadenia (Norton Online Family), kde je možné sledovanie detí pri on-line aktivitách, čím rodičia môžu chrániť deti a zároveň počítač pred nebezpečenstvom z Internetu. Rovnako upozorňuje na podvodné webové stránky (phishing ochrana). [77]

Microsoft Security Essentials

Jedná sa o bezplatný antivírusový program, ktorý chráni počítač pred nebezpečnými vírusmi. Osobitnú pozornosť venujem uvedenému programu v kapitole 4.1.1.3.

4.1.1.2 Porovnanie antivírusových programov

Porovnaním sa v súčasnosti zaoberá niekoľko firiem, medzi najznámejšie z nich patria AV-Comparatives a AV-Test. Druha menovaná spracovala pre rok 2012 bodové hodnotenie vybraných produktov, kde výsledky sú obsahom tabuľky 12. Test antivírusových programov sa uskutočnil v mesiacoch január a február v operačnom systéme MS Windows XP.

Tab. 12. Test antivírusových programov pre rok 2012. [34]

Výrobca_Výrobok	Ochrana	Oprava	Použiteľnosť
AhnLab_V3 Internet Security 8.0	2.0	4.5	4.5
Avast_Free AntiVirus 6.0	4.5	4.5	5.0
AVG_Anti-Virus Free Edition 2012	4.5	4.0	5.5
AVG_Internet Security 2012	5.0	4.5	5.5
Avira_Internet Security 2012	4.5	4.5	4.5
BitDefender_Internet Security 2012	6.0	6.0	5.0
ESET_Smart Security 5.0	3.5	2.0	5.5
F-Secure_Internet Security 2012	5.5	4.5	5.5
G Data_Internet Security 2012	6.0	3.5	4.5
GFI_Vipre Antivirus Premium 2012	4.5	3.0	5.0
K7 Computing_Total Security 11.1	5.0	4.0	4.5
Kaspersky_Internet Security 2012	6.0	5.5	5.0
MCAfee_Total Protection 2012	5.0	3.5	4.5
Microsoft_Security Essentials 2.1	2.5	5.0	5.0
Norman_Security Suite Pro 9.0	4.5	4.5	5.5
Panda_Cloud Antivirus Free Edition 1.5.1	5.0	4.0	5.5
Panda_Internet Security 2012	5.5	4.5	4.5
PC Tools_Internet Security 2012	4.5	3.5	3.0
Qihoo_360 Antivirus 2.0 & 3.0	5.5	4.0	3.0
Symantec_Norton Internet Security 2012	6.0	4.5	4.5
Trend Micro_Titanium Maxim Security 2012	4.5	4.0	5.0
Webroot_Secure Anywhere Complete 8.0	5.5	4.0	5.0

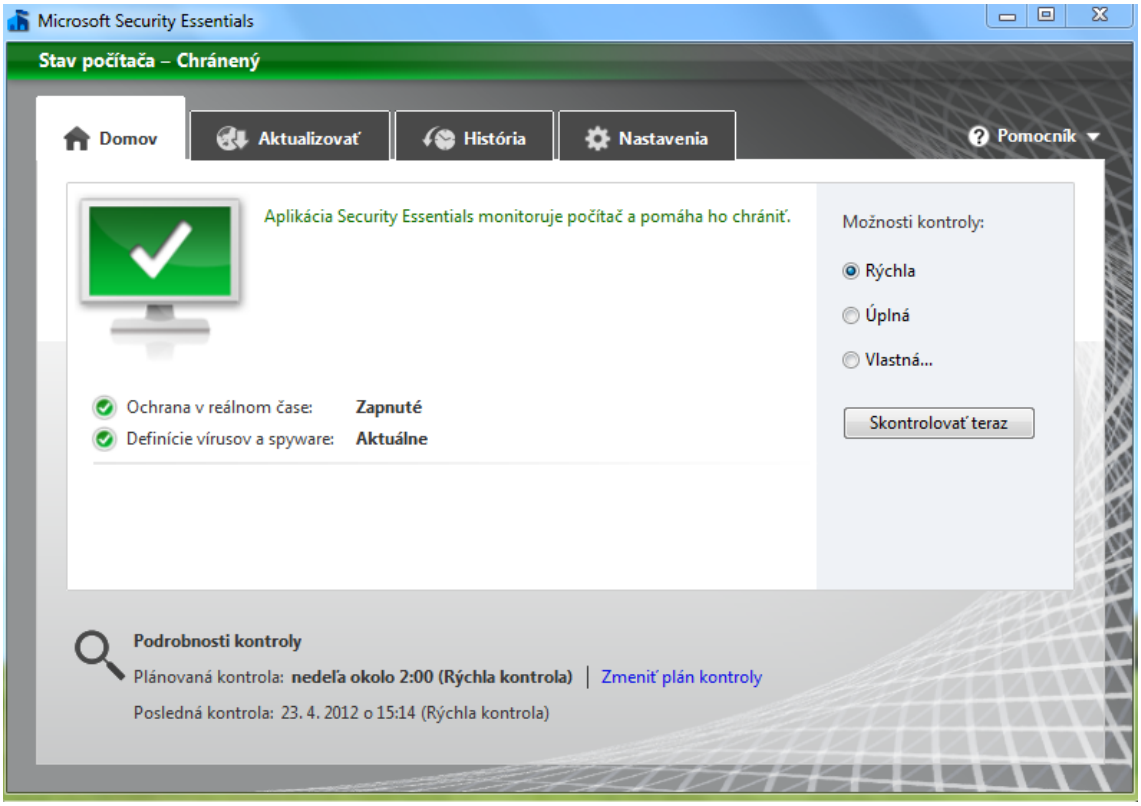
Tabuľka je zoradená podľa abecedy, nie podľa dosiahnutých výsledkov. Súčasťou tabuľky nie sú iba samostatné antivírusové programy ale tiež kompletné balíky, ktoré v sebe okrem antivírusu zahŕňajú aj ochranu v podobe firewallu.

Prvý stĺpec ružovej farby, s názvom ochrana (protection) testuje ochranný účinok bezpečnostných riešení systému, skúma, aká je reakcia na nebezpečné hrozby (malware). Takéto testovanie je vykonávané pomocou rôznych simulácií, scenárových útokov, ako sú napríklad potenciálna hrozba v prílohe e-mailovej správy alebo v infikovaných webových stránkach, ktoré sa mohli dostať do počítača z externých pamäťových zariadení. Druhý ružový stĺpec tabuľky s názvom oprava (repair) predstavuje analýzu systému, ktorý je už nakazený vírusom. Dochádza k hodnoteniu postoja programu pri odstraňovaní škodlivej nákazy (aktívny malware) a zároveň celkového správania systému. Posledný stĺpec tabuľky ružovej farby s názvom použiteľnosť (usability) sa zameriava na použiteľnosť bezpečnostného programu v operačnom systéme. Napríklad varovné správy, výskyt falošnej lokalizácie počas kontroly počítača, ako veľmi antivírusový program spomaľuje výkon počítača apod..

V roku 2010 bol na popredných priečkach antivírusový program Essentials Security od Microsoftu. V minulom roku sa víťazmi stali platené antivírusové programy. Prvé miesto v ochrane pred napadnutím vírusom patrilo BitDefender_Internet Security Suite 2011. [34]

4.1.1.3 Microsoft Security Essentials

Vo svojom osobnom počítači používam antivírusový program Microsoft Security Essentials, ktorý predstavuje bezplatnú aplikáciu (je potrebné mať platnú licenciu OS Windows), navrhnutú pre jednoduchú inštaláciu a používanie. Microsoft Security Essentials zabezpečuje ochranu pred vírusmi a iným škodlivým softwarom. Aplikácia je vhodná pre počítače používané v domácnosti alebo v malých organizáciách.

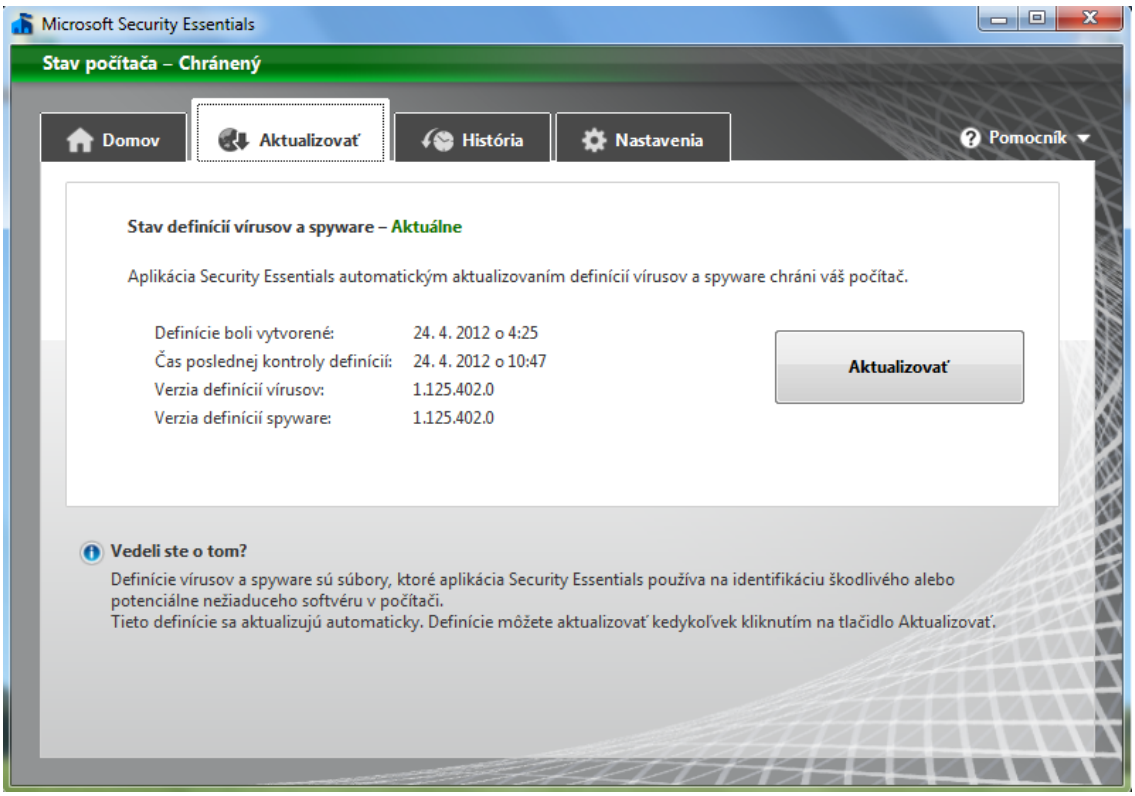


Obr. 6. Microsoft Security Essentials.

Microsoft Security Essentials poskytuje jednoduché menu pre užívateľa. Súčasťou je možnosť nastavenia kontroly počítača podľa vlastného uváženia. Pri rýchlej kontrole sa kontrolujú oblasti, na ktoré najčastejšie útočí škodlivý software.

Úplnej kontrole podliehajú všetky súbory na pevnom disku a všetky programy, ktoré sú práve spustené. Z praxe je možné, že pri výbere tejto kontroly môže čas kontrolovania presiahnuť jednu hodinu. Ak si užívateľ vyberie kontrolu „vlastnú“, dochádza ku kontrole umiestnení a súborov, ktoré si užívateľ sám vyberie.

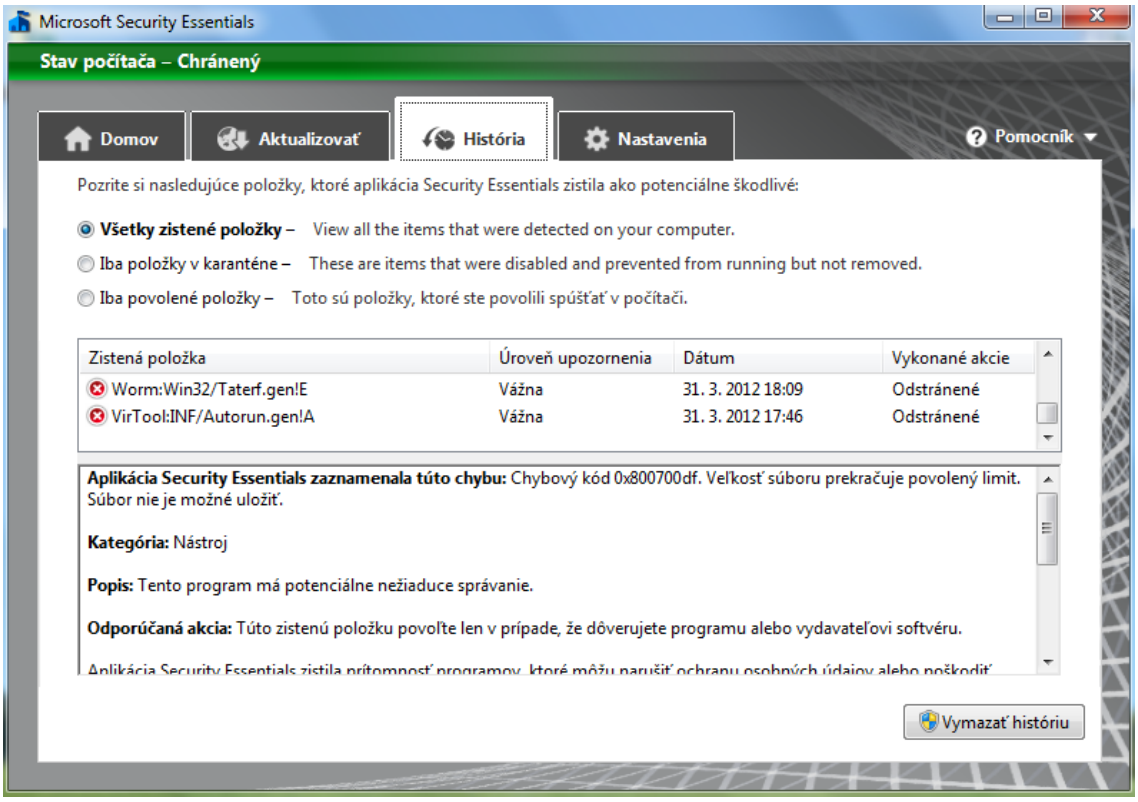
Aplikácia Microsoft Security Essentials poskytuje automatickú aktualizáciu definicií vírusov v databáze.



Obr. 7. Microsoft Security Essentials – aktualizácia vírusovej databázy.

V súčasnosti vznikajú stále nové vírusy a iné hrozby, ktoré môžu vážne ohroziť náš počítať a zároveň zneužiť naše citlivé dáta, ktoré sú jeho súčasťou. Je dôležité pravidelne aktualizovať svoj antivírusový program, aby bol počítač dostatočne chránený pred potenciálne nebezpečnými hrozbami.

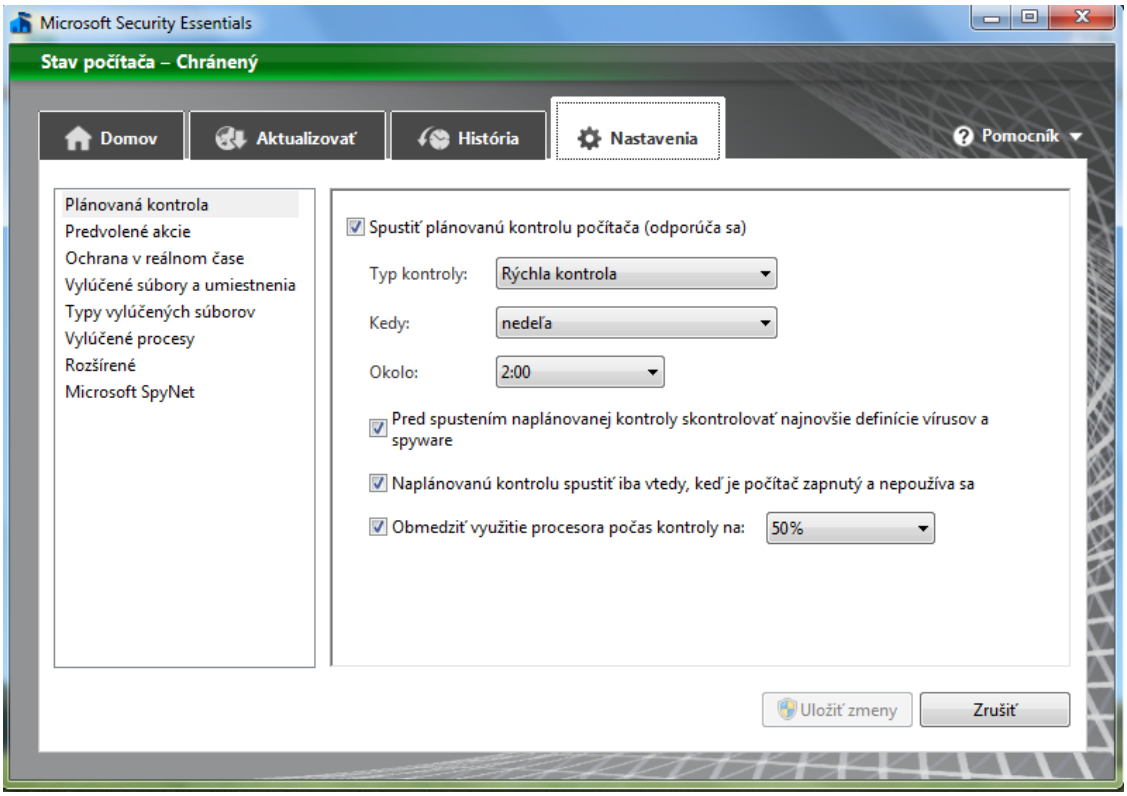
Súčasťou aplikácie Microsoft Security Essentials je história predchádzajúcich kontrol v počítači, viz nasledujúci obrázok.



Obr. 8. Microsoft Security Essentials – história kontroly počítača.

Aplikácia Microsoft Security Essentials poskytuje prehľadnú tabuľku nebezpečných vírusov, ktoré boli odhalené pri kontrole počítača. V tabuľke sú zobrazené údaje o závažnosti ohrozenia, ktoré samotný vírus predstavuje, tiež dátum odhalenia vírusu v počítači a následne vykonaná akcia užívateľom.

Poslednou záložkou aplikácie Microsoft Security Essentials sú rozšírené nastavenia, ktoré sú zobrazené na nasledujúcom obrázku.



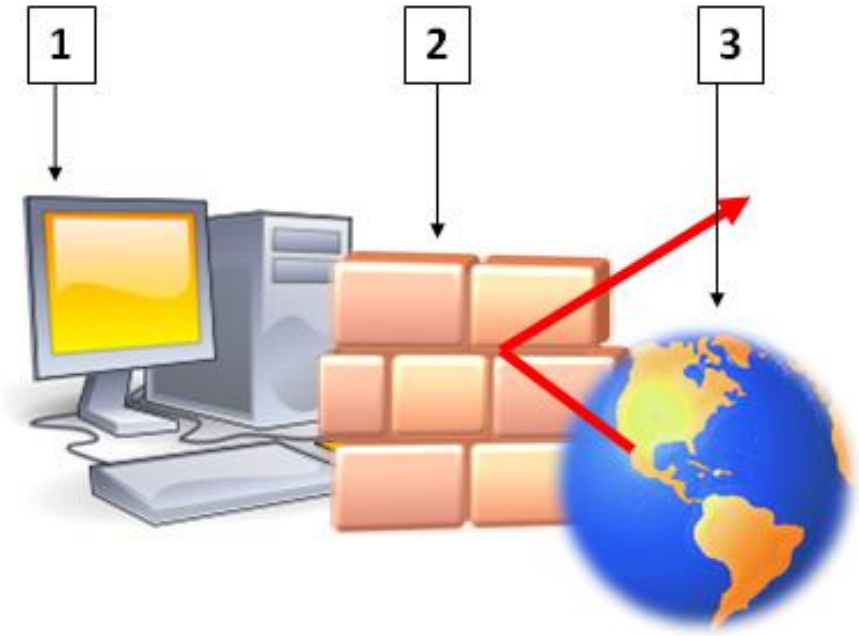
Obr. 9. Microsoft Security Essentials – rozšírené nastavenia.

V nastaveniach si môžeme naplánovať pravidelnú kontrolu počítača na konkrétny deň v týždni a konkrétnu hodinu. Svoje opodstatnenie má aj ochrana v reálnom čase, kde dochádza k upozorneniu užívateľa o víruse alebo inom nebezpečnom software, ktorý sa snaží nainštalovať sa do počítača. [31, 33]

4.1.2 Firewall

Firewall predstavuje software alebo hardware, ktorého cieľom je kontrola informácií prichádzajúcich z Internetu alebo Intranetu. Firewall sa snaží o vytvorenie ochrannej brány, bariéry medzi počítačom a potenciálnym nebezpečenstvom z prostredia Internetu. Chráni tak dáta v počítači pred hackermi a neoprávneným prístupom. Nastavenie brány firewallu umožňuje zablokovanie alebo umožnenie vstupu dátového toku.

Ak zamietne dátový tok, firewall prestane spracovávať prichádzajúci paket[2]. Firewall umožňuje zastaviť odosielanie škodlivého softwaru z jedného počítača do iných počítačov. Na nasledujúcom obrázku je zobrazený princíp, ako v skutočnosti brána firewall pracuje.

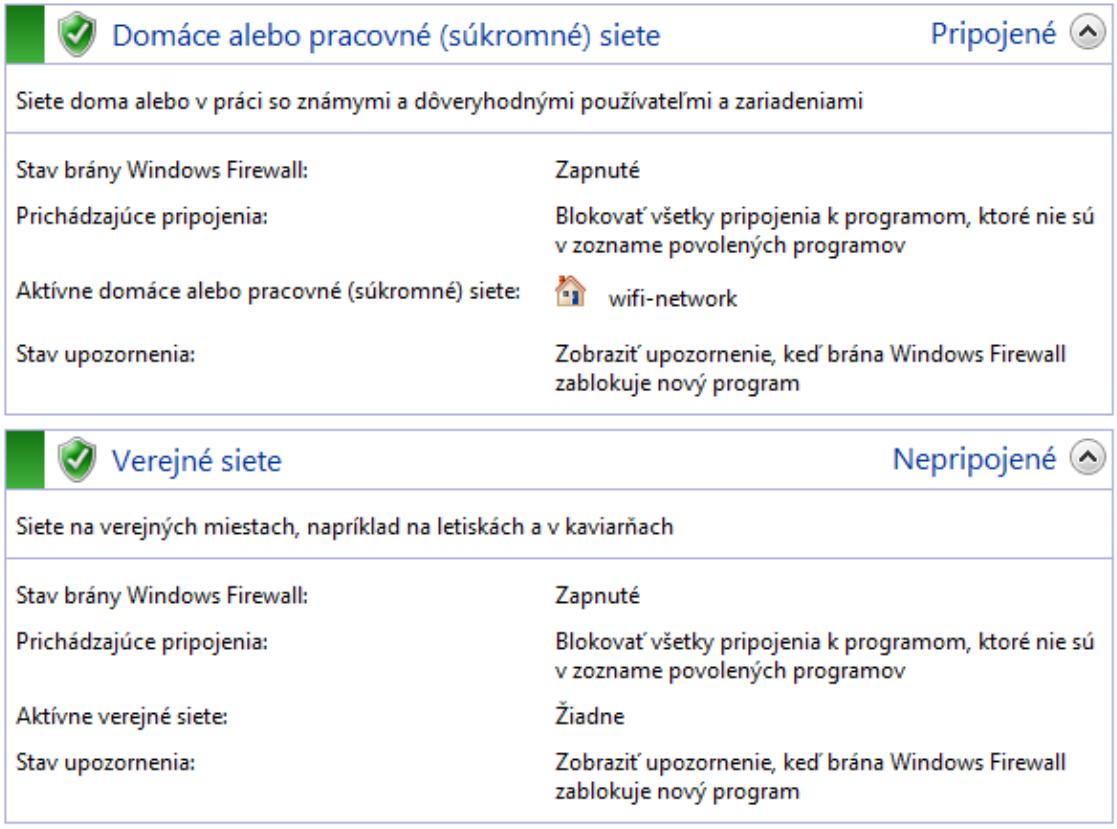


Obr. 10. Princíp činnosti brány firewall.

Na obrázku je zobrazený princíp činnosti brány fiewall, kde číselne označenie 1 určuje počítač, číslo 2 brána firewall a číslo 3 predstavuje Internet.

[2] Paket (z anglického prekladu balíček) predstavuje blok prenášaných dát.

Vo svojom počítači mám nainštalovaný operačný systém MS Windows 7. Ponukou operačného systému MS Windows 7 je prispôsobenie nastavenia firewallu samostatne pre každý typ siete (domáca sieť, pracovná sieť a sieť verejná). Na nasledujúcom obrázku je konkrétne nastavenie brány firewall v mojom osobnom počítači. Je výhodné používať pri pripojení do počítačovej siete buď „pracovná sieť“ alebo „verejná sieť“ lebo obmedzujú prístup do počítača po sieti. Domácu sieť je vhodné používať naozaj iba doma, ak je to možné.

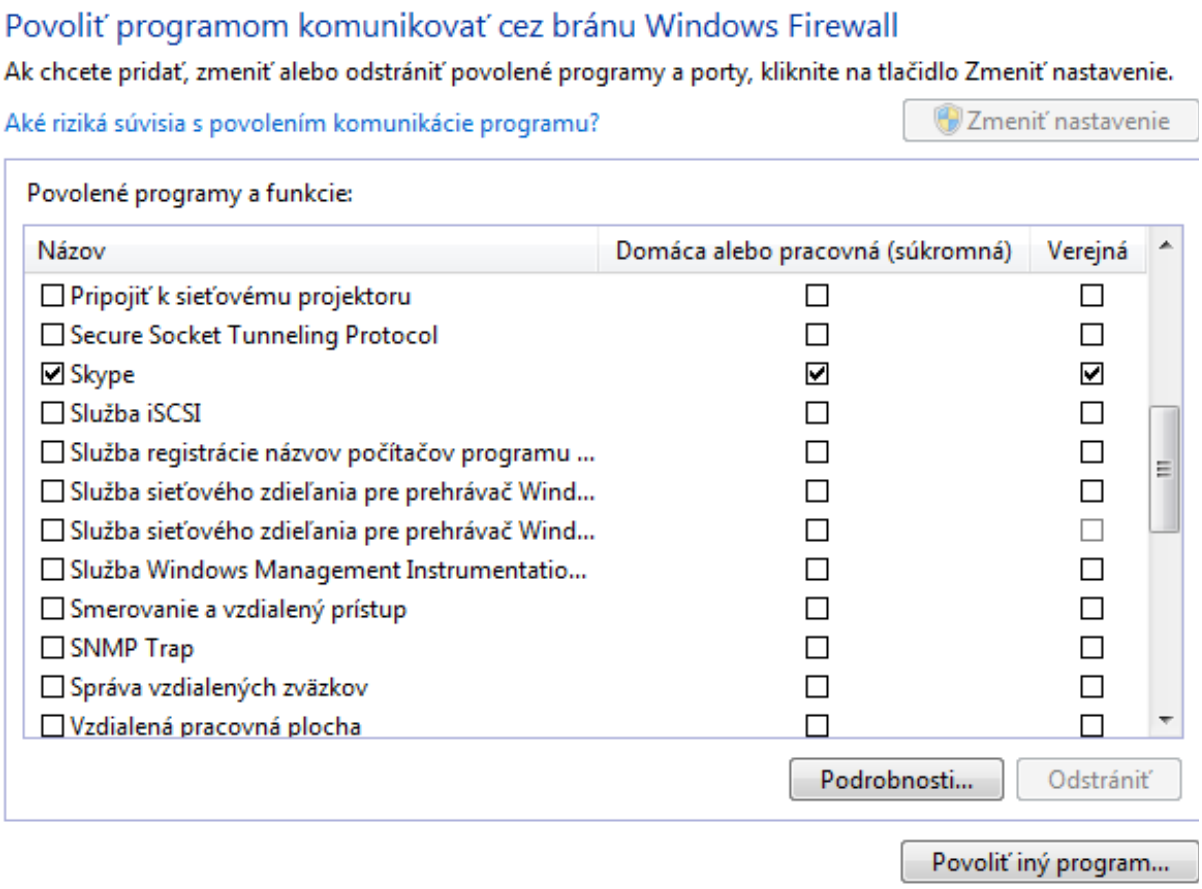


Obr. 11. Nastavenie brány Windows Firewall.

Nastavenie brány firewall v operačnom systéme MS Windows 7 (ďalej iba Windows Firewall) môžeme realizovať nasledovne:

Štart - Ovládací panel - Windows Firewall - Zapnúť alebo vypnúť bránu Firewall.

Windows Firewall poskytuje rozšírene nastavenia, kde si užívateľ sám riadi a zadáva, ktorý software môže a nemôže komunikovať prostredníctvom brány firewall.



Obr. 12. Povolenie programov komunikácie cez bránu Windows Firewall.

Nastavenie povolenia programom komunikovať cez bránu Windows Firewall môžeme realizovať nasledovne: Štart - Ovládací panel - Windows Firewall - Povoliť program alebo funkciu v bráne Windows Firewall. [2, 31, 32]

Samostatné programy s ochrannou funkciou firewall

Medzi iné programy, ktoré poskytujú ochrannú funkciu v podobe firewall patria nasledujúce:

Comodo Firewall

Comodo Firewall poskytuje užívateľovi počítača prevenciu ochrany voči vírusom a inému škodlivému malware a pred útokmi hackerov.

Medzi prioritnú ochranu môžeme zaradiť nasledujúce funkcie:

- zabraňuje inštalácií škodlivému softwaru,
- chráni počítač pred útokmi z Internetu,
- kontroluje spustené súbory a programy v počítači,
- poskytuje jednoduché a zrozumiteľné informačné upozornenia,
- je vhodný pre amatérov v počítačovej oblasti, pretože sa nevyskytujú žiadne zložité problémy s konfiguráciou,
- ponúka prijemné, príťažlivé grafické rozhranie pre užívateľa.

Firewall je jednou zo súčasti kompletného balíka ochrany počítača. Okrem ochrany v podobe firewallu poskytuje aj samotný antivírus. Ochrana prostredníctvom programu Comodo je vhodná pre laickú verejnosť ale zároveň pre odborníkov v oblasti informačných technológií, pretože poskytuje výber z niekoľkých režimov ochrany. Antivírus, ktorý poskytuje, však nie je kvalitný, odporúča sa využívať iba firewall, ktorý patrí k najvyužívanejším na trhu. [73]

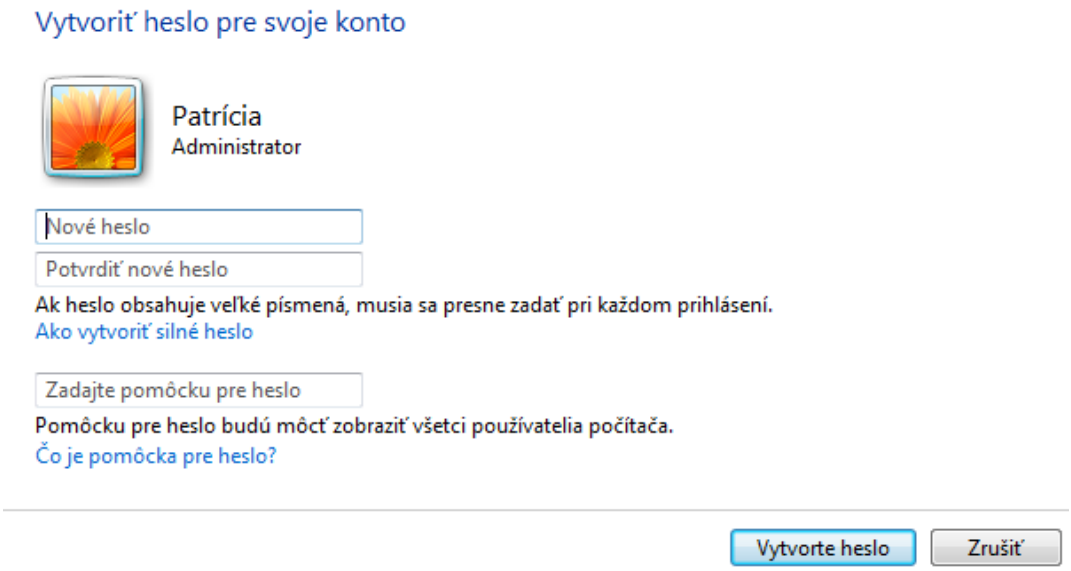
Kerio Control

Kerio Control predstavuje ochranu počítača v podobe úplnej kontroly informácií medzi jednotlivými počítačmi v rámci lokálnej siete a v prostredí Internetu. Dokáže vytvárať pravidlá pre prichádzajúcu a odchádzajúcu komunikáciu. Užívateľ si môže nastaviť pravidlá pre pakety, protokoly či samotné IP adresy, prípadne filtrovanie obsahu www. Je vhodný pre operačný systém Microsoft Windows, Linux, Mac OS. Kerio Control okrem samotného firewallu, poskytuje zároveň antivírusovú ochranu. Ochrana prostredníctvom Keria sa zameriava na firemnú oblasť. Vývoj verzie pre domácnosť bola zastavená pred štyrmi rokmi. [74]

4.1.3 Nastavenie hesla

Nastavenie hesla pre prístup do užívateľovho konta je prvou a základnou ochranou počítača a citlivých informácií, ktoré sa v ňom nachádzajú. Heslo má za úlohu zabezpečiť aby sa na užívateľove konto nedostala neoprávnená osoba, ktorá by mohla zneužiť uložené dáta. Ak nie je nastavené heslo pre prístup ku kontu v počítači, môže sa na počítač a k všetkým dôležitým dátam dostať akákoľvek osoba a to hneď po zapnutí počítača.

Nasledujúci obrázok ukazuje možnosť, ako si užívateľ môže nastaviť prístupové heslo pre svoje konto v operačnom systéme MS Windows 7.

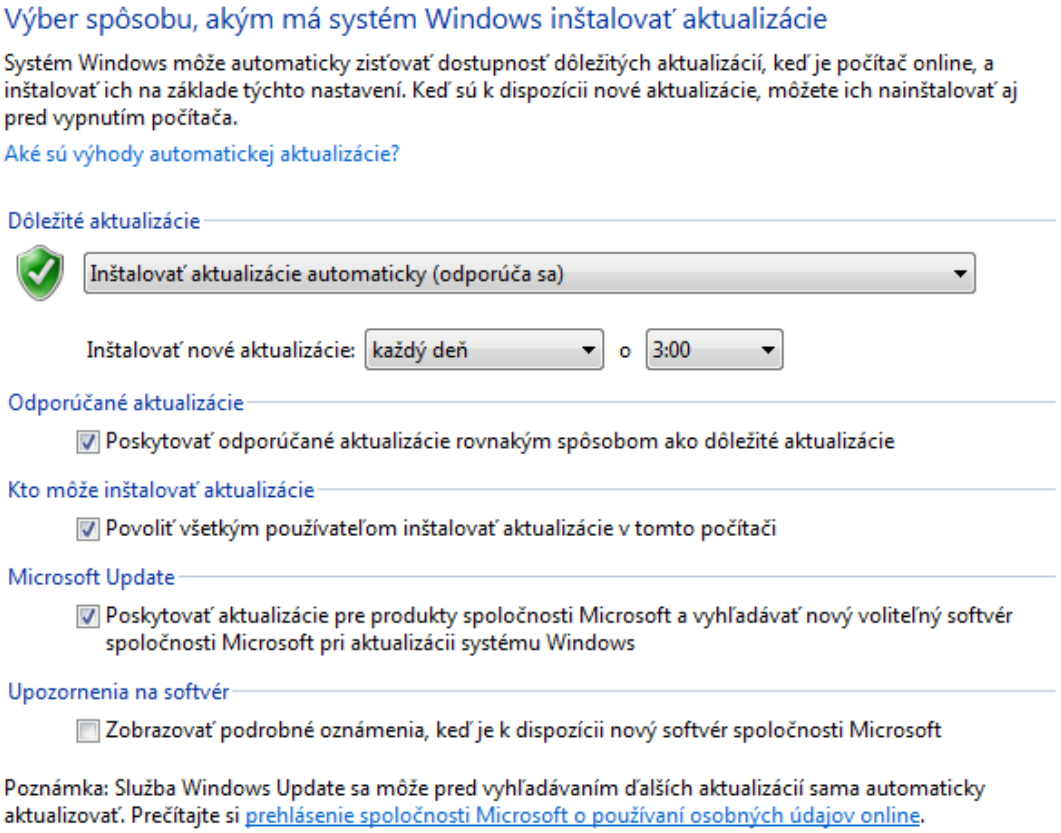


Obr. 13. Nastavenie hesla v OS MS Windows 7.

Nastavenie hesla v operačnom systéme MS Windows 7 môžeme realizovať nasledovne: Štart - Ovládací panel - Používateľské kontá - Vytvoriť heslo pre svoje konto. Je dôležité si zvoliť silné heslo, ktoré je kombináciou číslic a písmen. Odporúča sa heslo si chrániť a nikomu ho neprezrádzať. Heslo by sme mali vedieť, nie je praktické si ho zapisovať a už vôbec sa neodporúča si ho značiť niekde v blízkosti chráneného počítača. Ďalšou významnou ochranou samotného odhalenia hesla predstavuje fakt, že si užívateľ vytvorí vždy jedinečné heslo pri prihlásení rôznych prihlasovacích kont. [33]

4.1.4 Nastavenie automatickej aktualizácie OS MS Windows 7

Nastavenie automatickej aktualizácie v operačnom systéme MS Windows 7 je vhodné hlavne pre laických užívateľov počítača. Výhodou tohto nastavenia je, že aktualizácia systému sa uskutoční automaticky a systém si sám sťahuje potrebné aktualizácie, ktoré automatický zároveň nainštaluje. Počítač je takto chránený pred bezpečnostnými chybami v operačnom systéme, ktoré sa môžu objaviť. Práve pravidelnými aktualizáciami sa chyby odstraňujú.

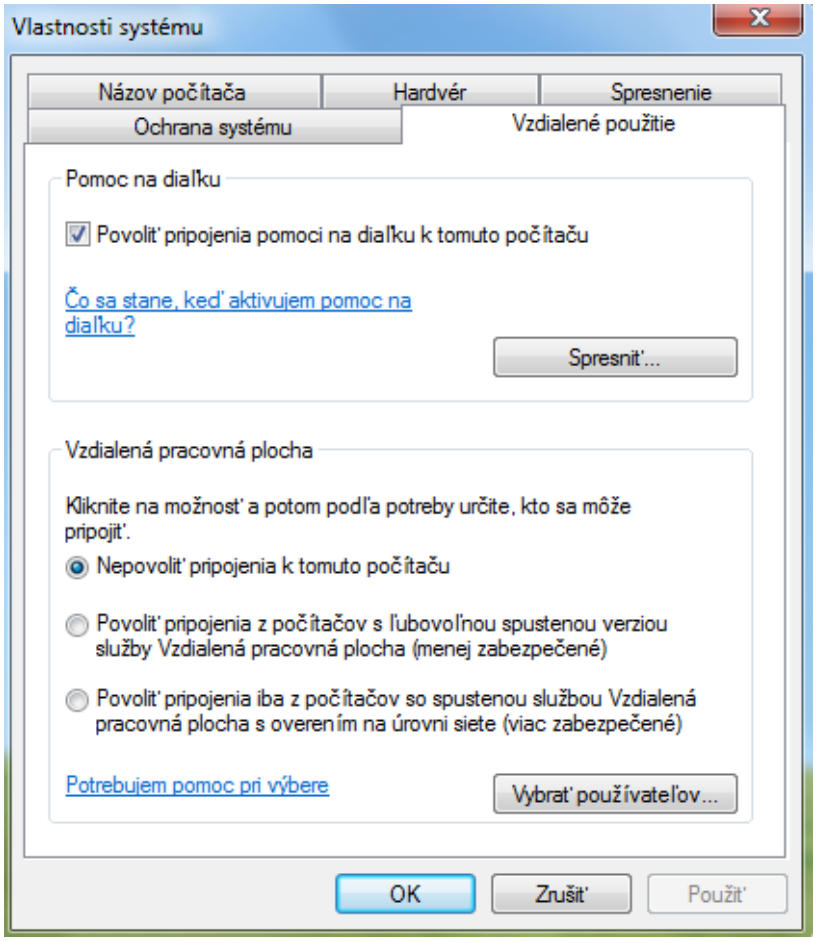


Obr. 14. Automatická inštalácia aktualizácií v OS MS Windows 7.

Nastavenie automatickej aktualizácie v operačnom systéme MS Windows 7 môžeme realizovať nasledovne: Štart - Ovládací panel - Windows Update - Zmeniť nastavenia. Následne je potrebné si vybrať z možnosti, odporúča sa vybrať možnosť inštalovať aktualizácie automaticky. [32]

4.1.5 Zákaz vzdialenej správy

Zákaz vzdialenej správy nám chráni počítač, aby nebolo možné sa v rámci siete pripojiť na diaľku k počítaču. Týmto zároveň zabránime prístupu k citlivým dátam. Nasledujúci obrázok ukazuje možnosť, ako si samy môžeme zakázať vzdialenú správu. [32]

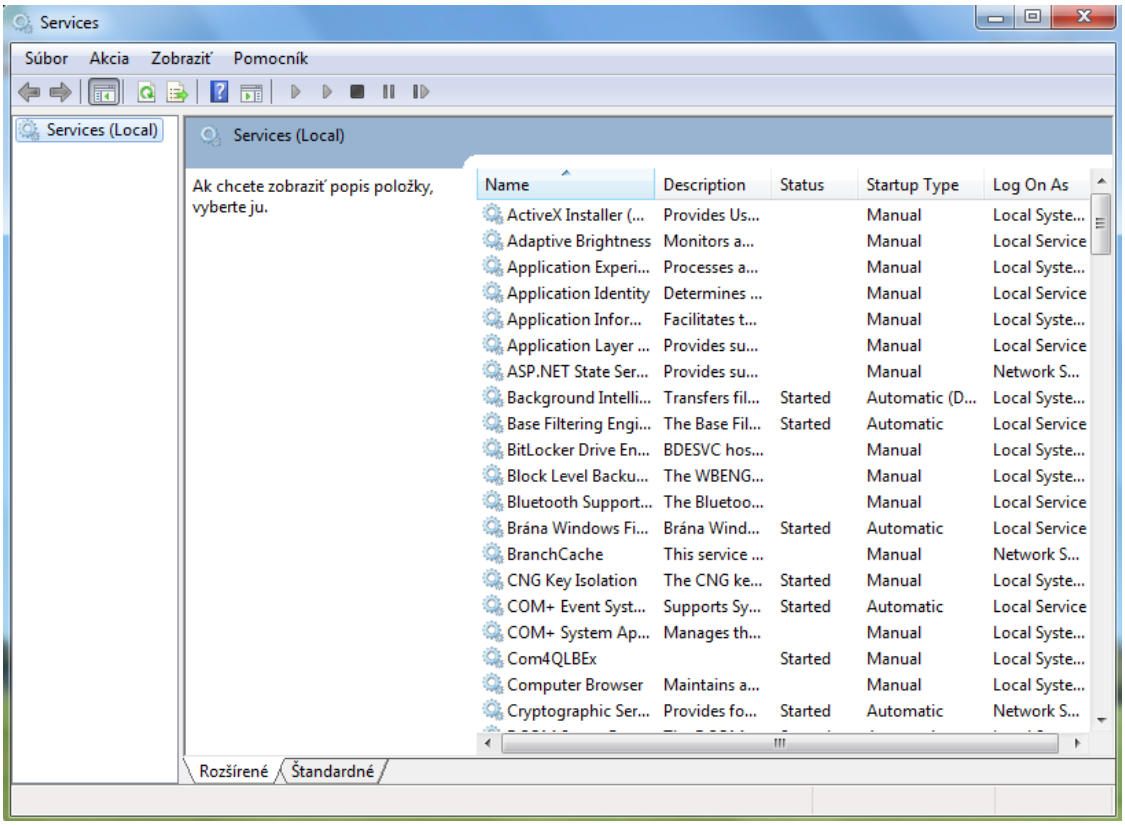


Obr. 15. Zákaz vzdialenej správy v OS MS Windows 7.

Zákaz vzdialenej správy v operačnom systéme MS Windows 7 môžeme realizovať nasledovne: Štart - Ovládací panel - Systém - Nastavenie vzdialeného prístupu.

4.1.6 Vypnutie potenciálne nebezpečných hrozieb

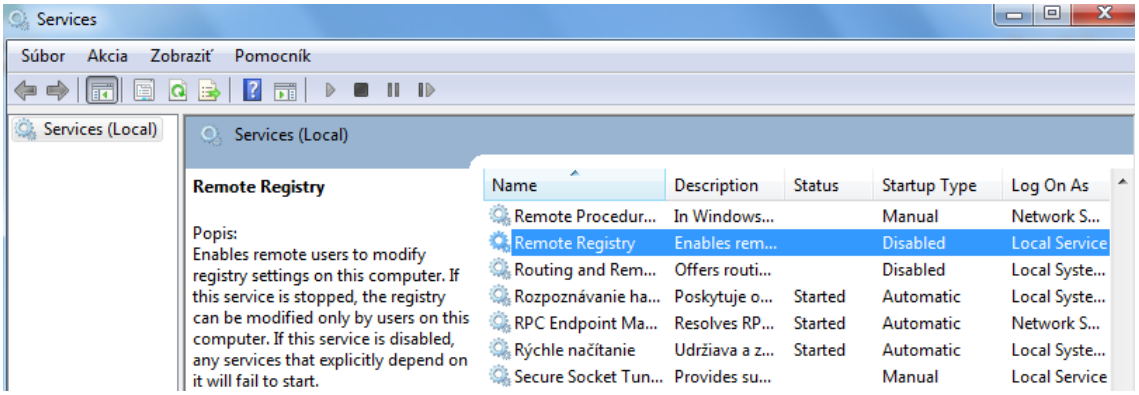
Vypnutie potenciálne nebezpečných hrozieb, prostredníctvom služieb, ktoré nájdeme v nástrojoch na správu, v operačnom systéme MS Windows 7 môžeme realizovať nasledovne: Štart - Ovládací panel - Nástroje na správu - Services (služby). V uvedenom prostredí môžeme prehľadne nastavovať služby. Užívateľ má prehľad, ktoré služby sú aktívne a ktoré zastavené. Spustenie služby sa realizuje buď automaticky (automatic), kedy sa služba spustí pri štarte systému a je stále aktívna. Ďalšie možnosti nastavenia je spustenie ručne (manual) nastavenie služby, kedy je spustená iba vtedy, ak je to potrebné. Posledný prípad predstavuje zakázanie služby (disabled).



Obr. 16. Services (služby).

4.1.6.1 *Vzdialený register (Remote Registry)*

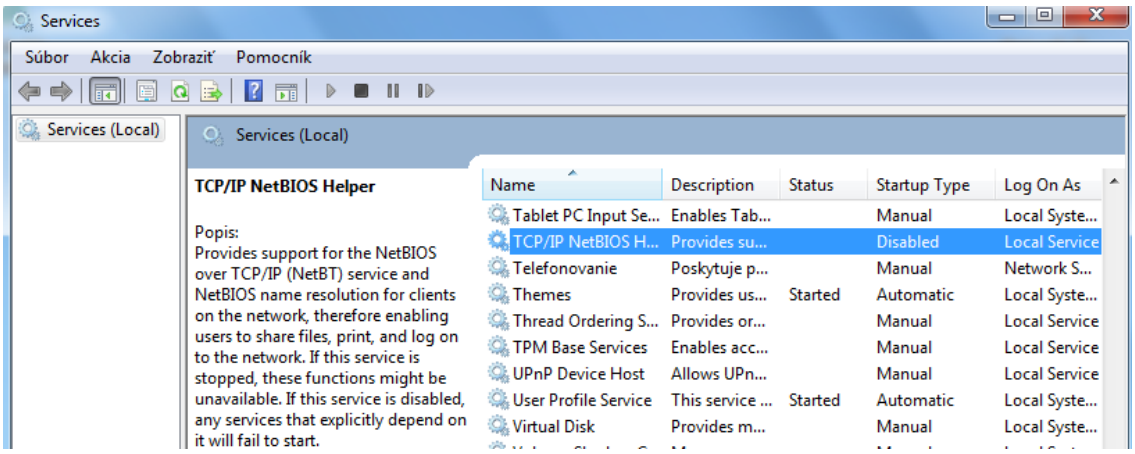
Službu Vzdialený register (Remote Registry) sa odporúča vypnúť pre ochranu počítača, ako je zobrazene na nasledujúcom obrázku. Uvedená služba umožňuje vzdialený prístup k databáze registra v OS Windows 7 a zároveň môže obmedziť prístup.



Obr. 17. Remote Registry (vzdálený register).

4.1.6.2 *TCP/IP NetBIOS Helper*

Podpora NetBios nad TCP/IP sa odporúča vypnúť v prípade, ak užívateľ nepoužíva zdieľanie súboru alebo zariadenia, pretože hrozí potenciálne nebezpečenstvo z Internetu. Uvedená služba poskytuje možnosť zdieľania súborov, tlačiarní medzi jednotlivý klientmi siete.



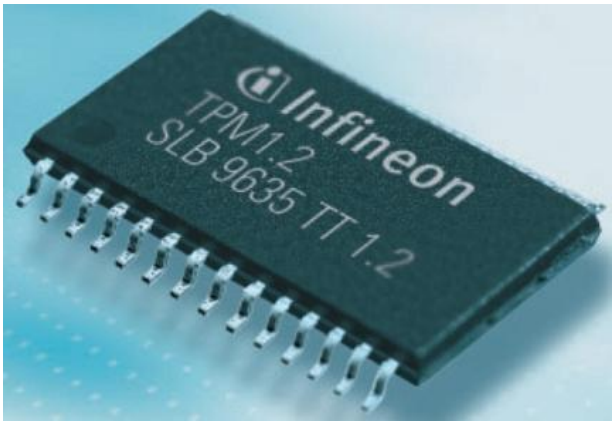
Obr. 18. TCP/IP NetBIOS Helper.

4.2 Hardwarové prostriedky

Jednou formou hardwarovej ochrany je realizácia pomocou rozširujúcej karty. Súčasťou rozširujúcej karty je ROM (Read Only Memory) pamäť spolu so špeciálnym softwarom, ktorá uchováva programy a dáta, ktoré sú stále spustené počas chodu počítača a nie je nutná ich zmena. V základnom rozsahu rozširujúca karta zabezpečuje bezpečnosť, ktorá je realizovaná vďaka niekoľkostupňovému ochrannému systému. Samotný prístup k počítaču je prostredníctvom hesla, ktoré je šifrované. Dochádza k monitorovaniu počítača, t.j. sledovanie samotnej prevádzky, registrácie a pokusov o neoprávnený prienik do systému. Súčasťou karty je batériou zálohovaná pamäť, v ktorej sú uložené nastavené parametre, vrátané prístupových práv. Samotnú kartu si užívateľ môže doplniť o rôzne moduly, ako napríklad pre zálohovanie či kódovanie. [2, 50]

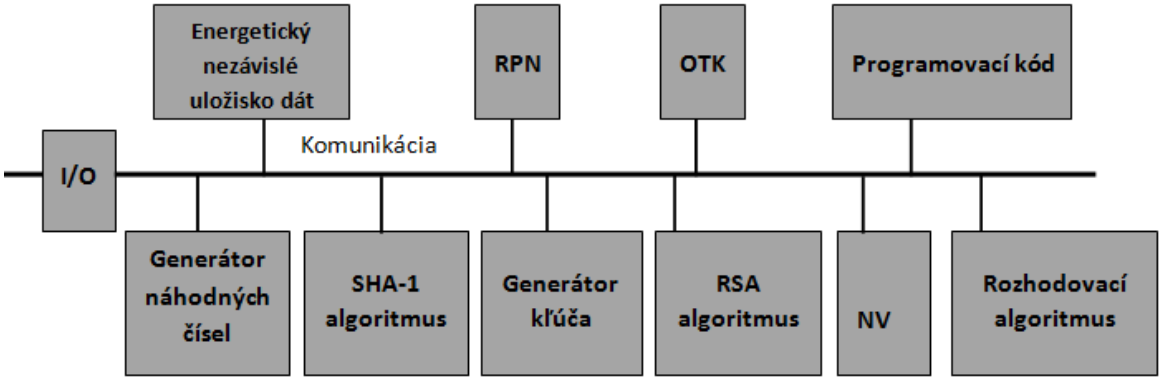
4.2.1 Modul TPM

Modul TPM (Trusted Platform Module) predstavuje mikročip (hardwarový modul), prostredníctvom ktorého získava počítať možnosť využitia rozšírených funkcií zabezpečenia. Samotný modul TPM môže byť už súčasťou počítačov novšieho typu, väčšinou je pripojený na základnú dosku počítača. V prípade, ak je súčasťou počítača, táto skutočnosť je uvedená v príslušnej dokumentácii, ktorá je dodaná spolu s počítačom. Každý modul TPM má vlastné nezrovnateľné číslo a dáta od výrobcu, čím sa stáva nesporne identifikovateľný. Na nasledujúcom obrázku je zobrazený modul TPM. [51, 52]



Obr. 19. Modul TPM (Trusted Platform Module). [52]

Modul TPM má široké využitie, neviaže sa iba na počítače ale svoje uplatnenie môže nájsť pri mobilných telefónoch či PDA (Personal Digital Assistant). Cieľom TPM je zabezpečiť dáta v každej chvíli. Nasledujúci obrázok vykresľuje logickú stavbu mikročipu TPM, kde RPN zobrazuje skratku pre register platformy nastavení, OTK je skratkou pre overenie totožnosti kľúčom a skratka NV znamená nastavenie vstupov. [51, 52]



Obr. 20. Schéma – logická stavba mikročipu TPM. [52]

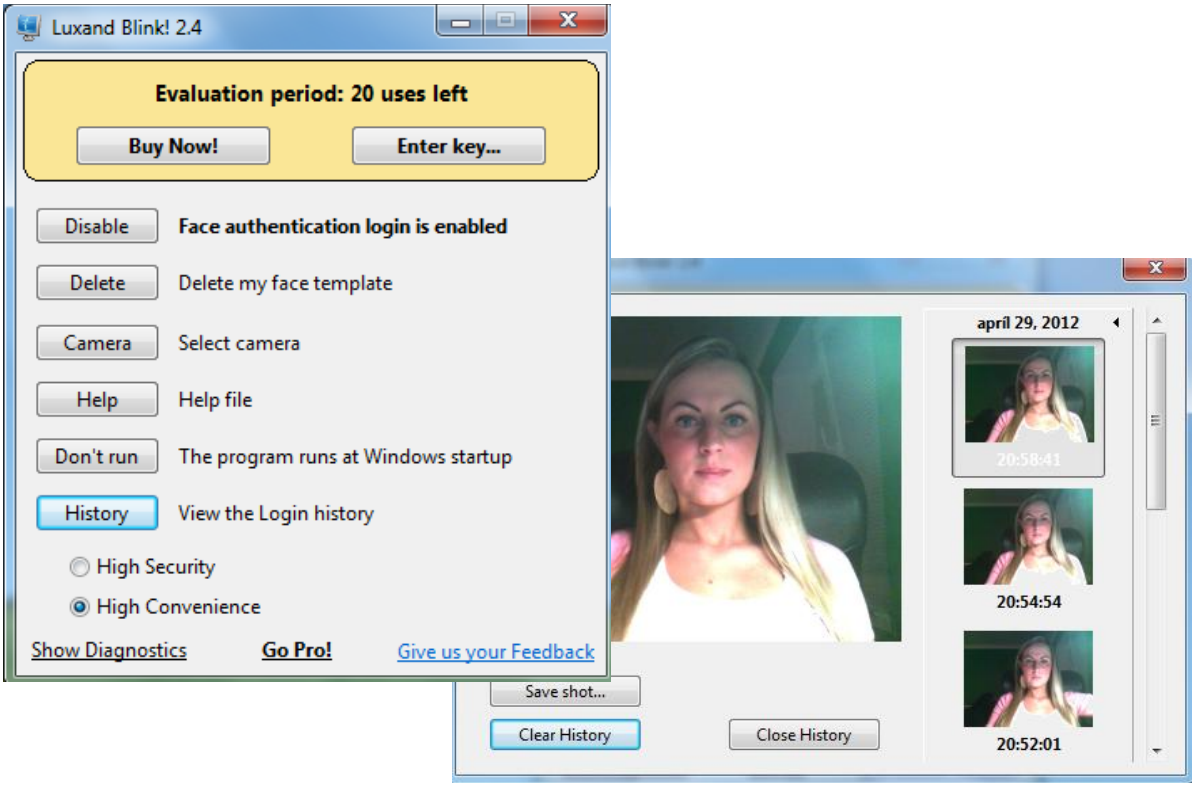
Počítač, ktorý obsahuje modul TPM dokáže vytvárať šifrovacie kľúče. Obsahom TPM je generátor náhodných čísel a dešifrovacie kľúče, ktoré majú dĺžku 2048 bitov. TPM vlastní svoju pamäť, čo poskytuje užívateľovi silnejšiu ochranu proti odhaleniu šifrovania. Pri prvom spustení modulu TPM dochádza k vytvoreniu hesla vlastníka modulu TPM, ktoré poskytuje zabezpečený prístup a samotnú správu modulu TPM. Modul TPM poskytuje možnosť pre prihlásenie aj biometrickou formou. [51, 52]

Obr. 21. Spolupráca modulu TPM a čítačkou odtlačkom prsta. [52]

4.2.2 Prihlasovanie do Windows pomocou webkamery

4.2.2.1 Luxand Blink

Samotná ochrana počítača a samozrejme osobných dát, ktoré sú jeho súčasťou, je pre užívateľa dôležitá. V súčasnosti okrem prihlasovania do systému pomocou prístupového hesla je možne aj prihlasovanie pomocou tváre alebo odtlačku prstu (ktorým je dnes už vybavených veľa notebookov), ako je zmienené na predchádzajúcej strane. Ak sa rozhodneme pre využitie webkamery ako prostriedku pre prihlásenie do systému, môžeme tak urobiť pomocou aplikácie Luxand Blink. Uvedená aplikácia udáva podporu pre operačný systém Windows Vista a Windows 7. Aplikácia je dostupná na Internete, cena je cca 40 EUR ale je možné si ju stiahnuť a vyskúšať po dobu 20 dní. [83]



Obr. 22. Program Luxand Blink.

Uvedená možnosť prihlásenia prostredníctvom rozpoznávania tváre je zaujímavá ale nie dokonalá. Technológia je prekonateľná pomocou digitálnej fotografie reálneho užívateľa počítača, na základe ktorej je možné technológiu prekonať, nerozlišuje rozdiel medzi skutočným obrazom a fotografiou. Dochádza k porovnaniu vybraných znakov aktuálneho obrazu z webkamery s fotkami registrovaných užívateľov. Táto možnosť je vhodná ako doplnková, pri klasickom prihlasovaní pomocou prístupového hesla. [83]

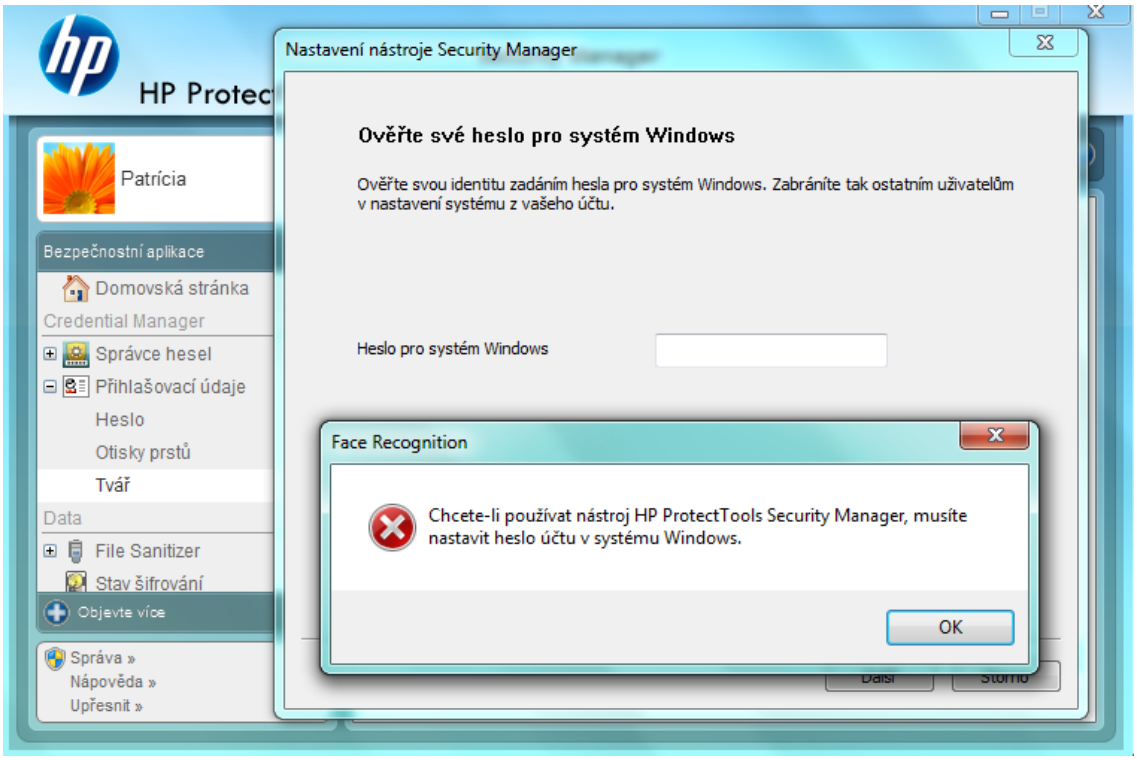
4.2.2.2 Program HP (Hewlett Packard) ProtectTools

Iným príkladom môže byť už vstavaný program v notebooku pre bezpečný pristúp do Windows.

Obr. 23. Správa možností prihlásenia programom HP ProtectTools.

Obr. 24. Zaregistrovanie scény tvárou.

Program HP ProtectTools je určený pre HP notebooky. V niektorých prípadoch môže byť program priamo vstavaný v operačnom systéme, zároveň je možnosť si program stiahnuť z webovej stránky HP. Súčasťou okrem prihlasovania sa do systému pomocou web kamery, poskytuje možnosť prihlásenia odtlačkom prstu.



Obr. 25. HP ProtectTools: demonštrácia previazanosti zabezpečovacích prvkov s prihlasovacím heslom.

Ak chce užívateľ využívať nástroje, ktoré mu HP Protectools Security Manager ponúka, je dôležité nastaviť prístupové heslo účtu k systému Windows.

4.2.3 Bezpečnostný zámok

V súčasnosti sú notebooky rozšírene viac ako stolné počítače. Ich výhoda spočíva v malých rozmeroch a celkovej hmotnosti počítača. Práve vďaka týmto vlastnostiam sa stávajú terčom pre zlodejov. Rovnako ako ku krádeži notebookov dochádza ku krádeži stolných počítačov. Okrem jasne vyčísliteľnej finančnej straty notebooku alebo stolného počítača dochádza k strate údajov, ktoré sú obsahom samotného počítača. Ochrana pred fyzickým odcudzením notebooku môže byť realizovaná pomocou bezpečnostného zámku alebo uzamykacou stanicou. Príkladom takejto ochrany notebooku môže byť zámok Kensington MicroSaver®ClickSafe od spoločnosti Kensington, ktorý je zobrazený na nasledujúcom obrázku. [54]

Obr. 26. Bezpečnostný zámok Kensington MicroSaver®ClickSafe. [53, 54]

Bezpečnostný zámok, ktorý je uvedený na obrázku poskytuje ochranu aj pre veľmi tenké notebooky. Hmotnosť tohto zámku je 0,207 kg a rozmery v milimetroch 160 x 30 x 210. Zamykací mechanizmus je s kruhovým kľúčom. Pripojenie k notebooku je realizované cez konektor pre zámok Kensington, ktorý v súčasnosti rozšírený. Cena zámku Kensington MicroSaver®ClickSafe je cca 72 EUR. [53, 54]

4.2.4 Uzamykacia stanica

Uzamykacia stanica chráni notebook pred krádežou. Notebook je bezpečne pripevnený k stolu. Spoločnosť Kensington ponúka uzamykaciu stanicu v dvoch prevedeniach a to buď v pohyblivom prevedení alebo v podobe pevného pripojenia. Uzamykacia stanica, ktorá je zobrazená na nasledujúcom obrázku od spoločnosti Kensington je určená pre notebooky, ktoré majú uhlopriečku displeja v rozmedzí od 13,3“ až do 17“, poskytuje jednoduchú inštaláciu na každom stole. [55]

Obr. 27. Uzamykacia stanica. [56]

Pri pevnom pripojení je nutné pripevniť uzamykaciu stanicu k stolu pomocou skrutiek. Pohyblivé riešenie predstavuje pripevnenie uzamykacej stanice k stolu pomocou lanka. Využitie uzamykacej stanice si nájde svoje uplatnenie pri používaní notebooku na verejných miestach (napríklad: bary, knižnice) ale zároveň vo väčších organizáciách. Cena uzamykacej stanice je cca 65 €. [55]

4.2.5 Hardwarový kľúč

Hardwarový kľúč (nazývaný tiež dongle) Guardant, ktorý je zobrazený na nasledujúcom obrázku je od spoločnosti Fineco. Slúži k ochrane softwaru pred počítačovým pirátstvom, pred ochranou sieťových a lokálnych aplikácií. HW kľúč môže byť v prevedení ako USB, ktorý je výhodný hlavne pre notebooky, alebo paralelný port pre stolové počítače. Pri obidvoch spôsoboch sa hardwarový kľúč pripája k počítaču. Hardwarový kľúč Guardant obsahuje vlastný procesor a vlastnú pamäť, ktorá môže poslúžiť pre uloženie dát. [57, 58]

Obr. 28. Hardwarový kluč Guardant. [58, 59]

Procesor, ktorý je súčasťou samotného hardwarového kľúča Guardant je schopný pracovať sám, čím si dokáže spracovať šifrovacie algoritmy samostatne. Blok dát sa odosiela z chránenej aplikácie na HW kľúč, tieto dáta sú prevádzané, buď sa jedná o šifrovanie alebo dešifrovanie pomocou algoritmu v hardwarovom kľúči. Je podporovaný operačným systémom Microsoft Windows, takže s inštaláciou by nemal byť problém. Cena takéhoto zariadenia je v rozmedzí od 16 až po 145 €. Ochrana a bezpečnosť softwarových produktov proti nelegálnemu šíreniu a využívaniu by sa nemalá podceňovať. [57, 58]

5 OCHRANA DÁT

Obsahom nasledujúcej kapitoly sú v základnom rozsahu zobrazené možnosti ochrany dát. Rozoznávame pojmy informácie a dáta, pri ktorých dochádza v praxi k častej zámene. Dáta, ktoré sa môžu nazývať tiež údaje, predstavujú pevné, nemenné fakty, ktoré sú časovo nezávislé (napríklad: písmená, čísla, slová, znaky, grafy, prípadne ich kombinácie). Dáta získavame meraním, výpočtami, kreslením apod.. Podstatou spracovania dát je tvorba výsledných informácií. Informácie sa nedajú zmeniť, pretože zobrazujú stav reality v danom okamihu. Je možné pracovať s novými dátami o realite v novom, odlišnom časovom okamihu. Vo všeobecnosti z bežného života vnímame pod pojmom informácie rôzne správy, s ktorými sa môžeme stretnúť v televízii, v novinách alebo prostredníctvom dialógu s inou osobou. Treba si preto uvedomiť, že všetky informácie sú tvorené z dát (údajov), ale zároveň akékoľvek vzniknuté a uložené dáta (údaje) sa vždy nemusia stať informáciou. [15]

5.1 Kryptografia

Kryptografia je náuka, ktorá predstavuje šifrovanie, šifrovacie metódy so zameraním na utajenie významu, obsahu odosielanej správy. Cieľom kryptografie je utajenie správy prostredníctvom kódu alebo šifry, čím sa správa stane utajenou a nečitateľnou pre nežiaducu osobu. Takto odosielané správy sú chránené odosielateľom pred neoprávneným čítaním cudzou osobou. Kryptografia nie je moderná vec, ale dnes si svoje využitie nachádza v bežnom živote v rozsiahlejšej miere ako v minulosti. Praktické využitie má kryptografia napríklad v bankách pri realizovaní finančných transakcií alebo pri šifrovaní tajných obchodných správ. V neposlednom rade nachádza kryptografia svoje miesto aj pri vojenských operáciách, kde sa dnes na utajenie správ, v niektorých prípadoch aj samotných operácií, kladú väčšie nároky, ako tomu bolo v minulosti. Prioritou a cieľom samotnej kryptografie je postarať sa o utajenie, chránenie a zaistenie dôveryhodnosti chránených dát. Dáta, ktoré sú chránené by sa nemali dostať do rúk neoprávnenej osobe. Kryptografiu na základe počtu používaných kľúčov rozlišujeme na šifrovanie symetrické a šifrovanie asymetrické. [15, 60]

5.1.1 Symetrické šifrovanie

Pri šifrovaní a dešifrovaní správy prostredníctvom symetrickej šifry sa používa iba jeden tajný kľúč. Ak chce odosielateľ pred odoslaním zašifrovať správu, urobí tak pomocou šifrovacieho kľúča. Zašifrovanú správu posiela prijímateľovi. Šifrovanie správy tvorí ochranu obsahu správy pred prečítaním neoprávnenej osoby. Príjemcovi prichádza zašifrovaná správa, ktorú si následne dešifruje rovnakým kľúčom ako ju odosielateľ zašifroval, následne sa mu zobrazí pôvodný utajený text správy. Dôležitým krokom pri symetrickej šifre musí byť použitý rovnaký tajný kľúč pre šifrovanie aj dešifrovanie, na ktorom sa musí odosielateľ vopred dohodnúť s prijímateľom

Obr. 29. Princíp symetrickej šifry.

Samotná zložitosť odhalenia tajného kľúča spočíva v jeho vlastnej dĺžke. Ak má kľúč dĺžku 8 bitov, tak vzniká možnosť existencie $2^8 = 256$ možných kľúčov. Pre zložitosť odhalenia tajného kľúča sa využíva veľkosť 128 bitov, ktorý nie je možné zistiť v krátkom čase. Medzi symetrické šifry patria šifry prúdové, pri ktorých sa jednotlivé znaky otvoreného textu šifrujú a dešifrujú po jednom bite. Medzi takéto šifry patria RC4 a FISH. Pri blokových šifrách sa šifrovanie a dešifrovanie realizuje po skupinách bitov (blokov). Bloky musia byť rovnako veľké, najčastejšie sa používajú 64 bitové, 128 bitové a 256 bitové. Medzi takéto šifry patria DES, 3DES, IDEA, AES, CAST. Výhoda symetrickej šifry spočíva v rýchlosti šifrovania a dešifrovania správy. Nevýhodou je odlišnosť kľúča pri rôznych prijímateľov a zároveň, že je šifrovacia technika závislá na dĺžke kľúča. [15, 60]

5.1.2 Asymetrické šifrovanie

Asymetrické šifrovanie, nazývané tiež šifrovanie pomoc verejného kľúča (angl. public key) predstavuje skupinu šifrovacích metód, ktoré pre šifrovanie a dešifrovanie správy využívajú rozličné kľúče. Šifrovanie správy pomocou asymetrickej šifry využíva dvojicu kľúčov, a to kľúč verejný a kľúč privátny (súkromný). Akýkoľvek odosielateľ a príjemca vlastní pár kľúčov, ktorý pozostáva z kľúča verejného a z kľúča súkromného. Každý z nich, kto chce dostať šifrovanú správu musí zverejniť svoj verejný kľúč, pričom súkromný kľúč zostava utajený. Odosielateľ správy šifruje správu pomocou verejného kľúča príjemcu, ktorý je voľne prístupný. Následne dešifrovanie správy si príjemca urobí prostredníctvom svojho súkromného kľúča.

Obr. 30. Princíp asymetrickej šifry.

Hlavná výhoda šifrovania prostredníctvom asymetrickej šifry spočíva v dvojici kľúčov. Nie je potrebné posielať nikomu svoj súkromný kľúč, a tak môže zostať naďalej utajený a zároveň verejný kľúč je možné sprístupniť každému. Nevýhodou je nižšia rýchlosť spracovania, s porovnaním so symetrickou šifrou. Najznámejšie algoritmy využívané v asymetrickom šifrovanú sú RSA, DSA, Diffie Hellman, EIGamal. [15, 60]

5.2 Elektronický podpis

Elektronický podpis je definovaný v paragrafe 3, Zákona 215/2002 Z. z o elektronickom podpise. Vyhotovenie elektronického podpisu (ďalej iba EP) sa uskutočňuje na základe súkromného kľúča, elektronického dokumentu a verejného kľúča. EP predstavuje informáciu, ktorá je pripojená alebo inak logicky spojená s elektronickým dokumentom. Túto informáciu je možné urobiť na základe súkromného kľúča a elektronického dokumentu. Vytvorená informácia spolu s verejným kľúčom, ktorý patrí k súkromnému kľúču, ktorý bol použitý pri vytvorení informácie, sú prostriedkom pre samotné overenie totožností elektronického dokumentu. Vyhotovenie elektronického podpisu uskutočňuje podpisovateľ elektronického dokumentu na základe vlastného súkromné kľúča a elektronického dokumentu, vzniká nový údaj, ktorý predstavuje elektronický podpis. Svoje využitie EP nachádza napríklad pri styku s orgánmi verejnej moci, v organizáciách sa môže využívať pri internej komunikácie, ako je šifrovanie e-mailovej komunikácie, fakturácia apod.. EP zaručuje jednorázovosť použitia, t.j. že nie je možné vziať podpis a preniesť na iný dokument. [15, 60, 61, 62]

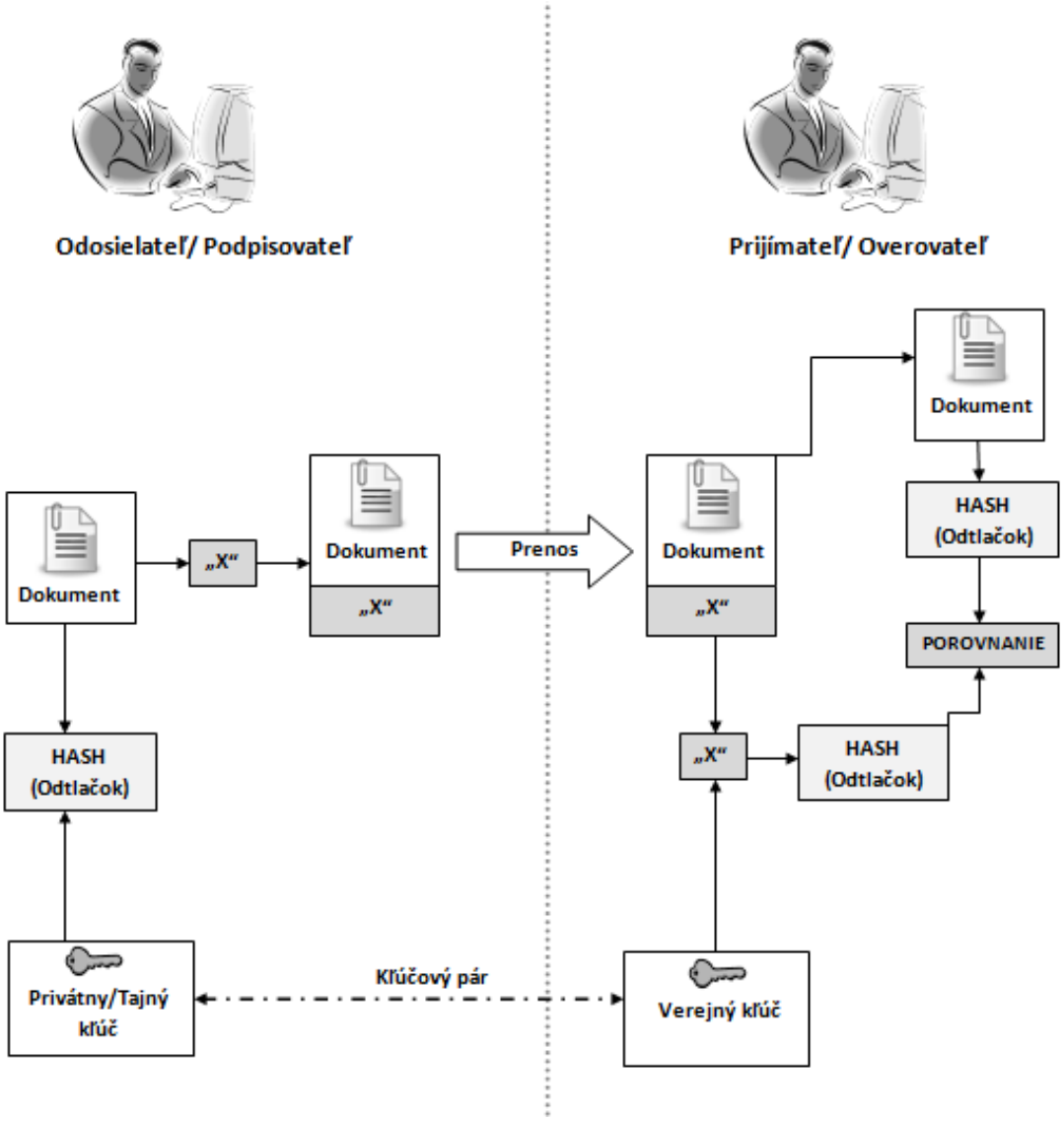
5.2.1 Zaručený elektronický podpis

Zaručený elektronický podpis je definovaný v paragrafe 4, Zákona 215/2002 Z. z o elektronickom podpise. Každému občanovi Slovenskej republiky sa poskytuje možnosť používania zaručeného elektronického podpisu (ďalej už iba ZEP). ZEP je rovnoprávny ako vlastnoručný podpis, ktorý je overený notárom. Rovnoprávnosť je v súlade so znením § 40 ods. 5 Občianskeho zákonníka. V prípade, ak sa občan Slovenskej republiky rozhodne pre používanie zaručeného elektronického podpisu, potrebuje pre elektronické podpisovanie určité nástroje. V prvom rade je potrebné navštíviť Akreditovanú certifikačnú autoritu (napríklad Prvú slovenskú certifikačnú autoritu, PSCA v Bratislave), kde je nutné získať kvalifikovaný certifikát a certifikované zaradenie pre uloženie podpisového kľúča. Pre získanie certifikátu je potrebné predložiť preukaz totožnosti a zároveň druhý osobný doklad (napríklad vodičské oprávnenie). Ďalej je potrebná kúpa softwaru pre podpisovanie dokumentov. Cena certifikátu na jeden rok je cca 40 EUR a cena potrebného softwaru predstavuje cca 84 EUR. Certifikát predstavuje elektronický dokument, ktorého obsahom je verejný kľúč držiteľa certifikátu.

Obsahom elektronického dokumentu sú identifikačné údaje samotného vydavateľa certifikátu, identifikačné údaje držiteľa certifikátu, identifikačné číslo certifikátu, platnosť certifikátu (dátum, čas začiatku a konca), verejný kľúč držiteľa certifikátu, identifikáciu algoritmov, pre ktoré je uvedený verejný kľúč určený a identifikáciu algoritmov používaných pri vyhotovení elektronického podpisu. Nevýhodou je, že pred blížiacim sa koncom platnosti nie je užívateľ nijak informovaný o vypršaní doby, preto je dôležité si sledovať dátumy platnosti. Samotné obnovenie a predĺženie platnosti certifikátu je možné stihnúť v intervale tridsať dní, pred skončením platnosti, prostredníctvom e-mailu alebo telefonicky. V prípade, ak si nepredĺžite platnosť certifikátu v danom intervale a jeho platnosť prepadne, je nutný rovnaký postup, ako keby sa certifikát vybavoval prvýkrát. Uplatnenie v praxi je napríklad pri elektronickom zasielaní dokumentov orgánom štátnej správy (daňový úrad). [61, 62, 63, 64]

5.2.2 Princíp elektronického podpisu a hash funkcia

Kľúčovým princípom vzniku elektronického podpisu je vypočítať „číslo“ z dokumentu, ktorý chce užívateľ podpísať. Číslo predstavuje hash, čo je vlastne ako keby odtlačok dokumentu. Výpočtový algoritmus zaisťuje, že neexistuje iný dokument, ktorý by mal rovnaký odtlačok (hash). Stačí aby sa dva dokumenty líšili iba v jednom znaku, tak už vznikajú rozličné hash. Zároveň z výstupného odtlačku nie je možné spätne vytvoriť pôvodný vstupný blok. Hash funkcia predstavuje matematický výpočet, ktorý premieňa vstupný blok binárnych údajov premennej dĺžky na odtlačok, ktorý má pevnú dĺžku. Elektronický podpis vzniká asymetrickým šifrovaním hash. Hash (odtlačok dokumentu) zašifruje odosielateľ tajným kľúčom a pripojí ho k dokumentu pre odoslanie, čím zašifrovaný hash predstavuje elektronický podpis. Odšifrovanie sa uskutočňuje prostredníctvom verejného kľúča. Prijímateľ si z prijatej správy vypočíta jej odtlačok, zároveň prostredníctvom verejného kľúča odšifruje hash (odtlačok dokumentu) od odosielateľa a nastáva porovnanie. V prípade, ak sa odtlačky zhodujú, nedošlo k zmene dokumentu od odosielateľa. Druhý prípad nastáva, ak nie sú odtlačky totožné, z čoho vyplýva, že pri prenose došlo k zmene dokumentu. [15, 60, 61, 64]



Obr. 31. Princíp elektronického podpisu.

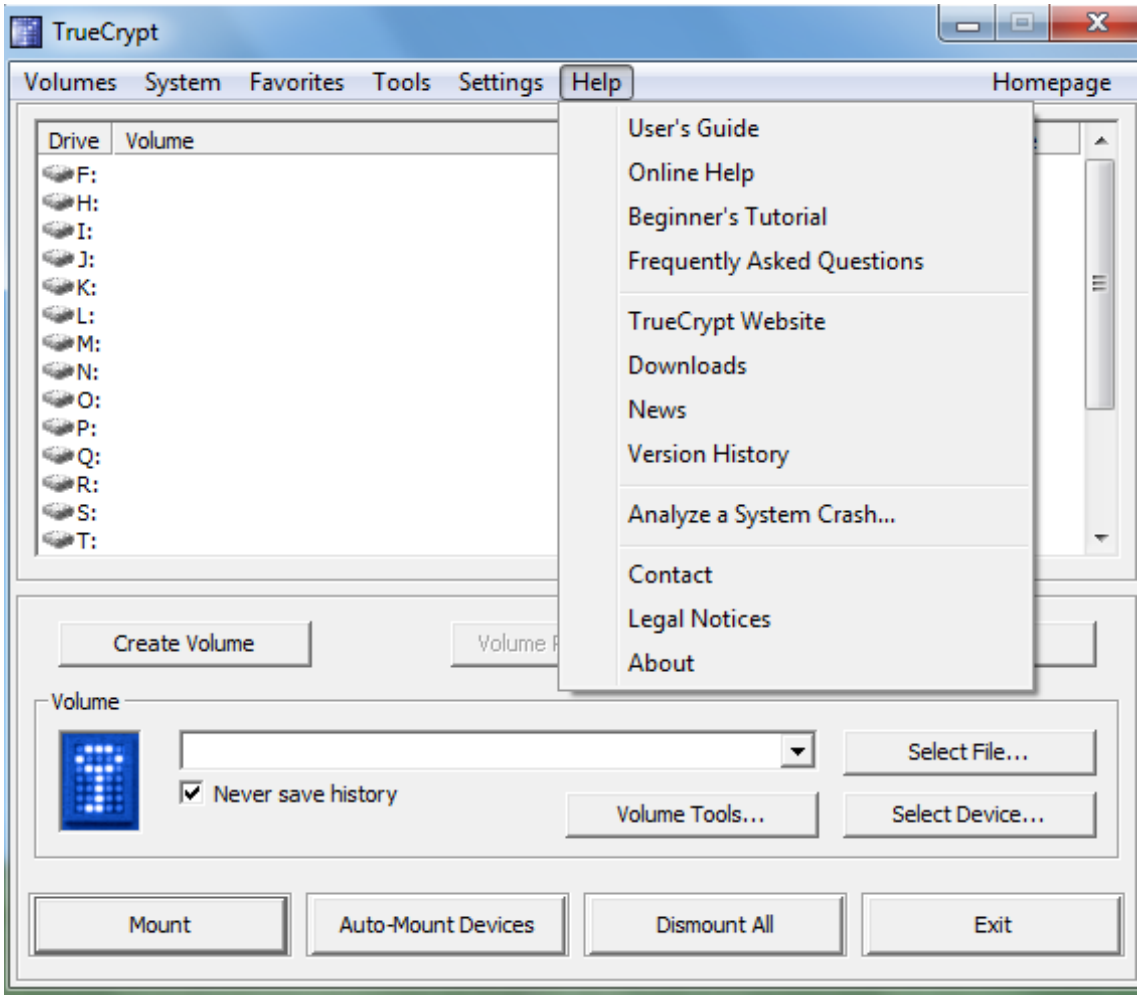
5.3 Protokol SSL

Protokol Secure Sockets Layer (ďalej už iba SSL) je štandardná bezpečnostná technológia pre vytvorenie šifrovaného spojenia medzi webovým serverom a prehliadačom. Najčastejšie je využívaný pre bezpečnú komunikáciu s internetovými servermi HTTPS (Hypertext Transfer Protocol Secure), kde HTTPS predstavuje zabezpečenú verziu protokolu HTTP. SSL zaisťuje, že všetky údaje zasielané medzi webovým serverom a prehliadačom, zostanú súkromné a zabezpečené. SSL spojenie funguje na základe asymetrickej šifry. Svoje využitie nachádza hlavne pri on-line transakciách medzi bankou a klientmi. [65]

5.4 Program TrueCrypt

Určite na každého z nás číha hrozba pred stratou, krádežou a následným zneužitím dát, ktoré sú obsahom našich počítačov. Práve program TrueCrypt nám poskytuje ochranu dát v prípade, ak sa staneme obeťou krádeže notebooku alebo straty USB kľúča.

TrueCrypt predstavuje šifrovací program pre ochranu dát v počítači. Výhodou, ktorý program poskytuje, je kompatibilita s rôznymi operačnými systémami (Windows, Linux, Mac OS). Ďalšou výhodou je otvorenosť zdrojového kódu. Práve tým, že je zdrojový kód otvorený, si môže užívateľ skontrolovať obsah programu. Šifrovací program TrueCrypt je možné si stiahnuť z webových stránok TrueCrypt (*http://www.truecrypt.org*) zdarma.



Obr. 32. TrueCrypt po spustení.

Po spustení programu TrueCrypt sa nám zobrazí zoznam voľných písmen od „F“ po „Z“ pre pripojenie diskových jednotiek, ako je zobrazené na obrázku 32. Vďaka tomu si užívateľ môže vytvoriť niekoľko rôznych virtuálnych šifrovaných diskov, pričom ich môže používať naraz. Pre bezpečnejšie používanie si môžeme zašifrovaný disk skryť.

Program dáva užívateľovi možnosť šifrovania diskov a vytváranie virtuálnych zabezpečených jednotiek, do ktorých môže následne ukladať svoje dáta, ktoré chce užívateľ chrániť. Užívateľ môže šifrovať buď skutočný disk v podobe pevného či externého disku alebo USB kľúča. Prípadne môže šifrovať špeciálny súbor, ktorý následne slúži ako úložisko, ktoré je pripojené pomocou virtuálnej diskovej jednotky. Tretou možnosťou je zašifrovanie diskového oddielu, kde je nainštalovaný operačný systém. Samotné šifrovanie sa uskutočňuje prostredníctvom troch algoritmov (AES, Twofish, Serpent) a ich možnou kombináciou. Pri pripojení k zašifrovanému textu je pomocou prihlasovacieho hesla. Program poskytuje aj možnosť kontroly hesla, ktoré si užívateľ zvolil prostredníctvom testovania rôznych kombinácií znakov.

Súčasťou programu je niekoľkostranová dokumentácia, predstavujúca manuál ako treba postupovať. Uvedený program však nie je určený pre začínajúceho užívateľa. [78, 79]

5.5 Zálohovanie dát

V súčasnosti veľa ľudí má svoje dáta uložené práve v elektronickej podobe a ich strata môže mať pre ich vlastníkov vážne až nenahraditeľné následky. Ďalšou možnosťou ako chrániť svoje dáta je ich zálohovanie. Zameriavam sa na osobné dáta bežných používateľov Internetu a počítača. Strata takých dát, ktoré sú významné pre veľké spoločnosti, môže mať fatálne následky v podobe ohrozenia samotnej existencie spoločnosti. Zároveň takýmito citlivými dátami sú údaje z oblasti bankového či zdravotného systému. Cieľom zálohovania dát je vytvoriť ich bezpečnostnú, zálohovú kópiu, ktorá je dostupná v prípade ich straty, znehodnotenia alebo úplného vymazania. Hrozbu v podobe straty dát môžu predstavovať rôzne vírusy, porucha hardwaru, chybou softwaru, samotné zlyhanie ľudského faktoru (užívateľ), prípadne ohrozenie v podobe rôznych prírodných katastrof (požiar, záplava). [2, 84]

Zálohovanie dát, musí spĺňať určité základné podmienky. V prvom rade sa musí zálohovanie uskutočňovať pravidelne a dôsledne. Najlepšie by bolo uložiť zálohované dáta fyzicky mimo pracovného počítača. Medzi najčastejšie metódy zálohovania dát užívateľov počítača môžeme zaradiť nasledujúce.

5.5.1 Záloha na vlastné pamäťové média

- externý disk,
- CD/DVD,
- flash disk (USB kľúč),
- pamäťová karta,
- magnetické pásky.

Zálohovanie na vonkajšie pamäťové média sa považuje za dôkladné zálohovanie dát. Takéto dáta môžu predstavovať dôležité údaje, ktorých strata alebo zničenie by malo vážne následky pre užívateľa. Zálohovanie dát na CD a DVD bolo veľmi rozšírené, kým sa ešte veľmi nevyužívali veľkokapacitné externé disky. Flash disk je vhodný skôr pre krátkodobé zálohovanie. Zameriava sa skôr na rýchly, krátkodobý prenos uložených dát. Pamäťová karta ponúka svoju výhodu v malých rozmeroch, vysokou spoľahlivosťou a zároveň rýchlym prístup k uloženým dátam. V súčasnosti si užívateľ volí vonkajšie pamäťové médium pre zálohovanie svojich dát na základe veľkosti kapacitného zariadenie a jeho náchylnosti na poškodenie a v neposlednom rade od cenovej ponuky. Magnetické pásky sú určené pre rozsiahlejší objem skladovaných dát.

Záloha na rovnaký pevný disk.

Zálohovanie na ten istý pevný disk predstavuje jednoduché a rýchle zálohovanie, kde si vytvoríme priečinok na rovnakom pevnom disku, kde sa ukladá napr. kópia textových dokumentov, s ktorými aktuálne pracujeme. Takáto forma zálohy je praktická pri náhodnom zmazaní súborov alebo dokumentov, v prípade zlyhania pevného disku dochádza k úplnej strate všetkých údajov. Jedna sa o najvyužívanejší spôsob zálohovania dát v priebehu vykonávanej práce. Využívanou metódu ochrany dát, v prípade zlyhania disku je metóda RAID (Redundant Array of Inexpensive/Independent Disks).

Predstavuje viacnásobné diskové pole lacných/nezávislých diskov, kde sa na dva disky rovnakých kapacít ukladajú totožné informácie. Jedná logická dátová jednotka (blokové zariadenie) zobrazuje prácu s dvomi alebo viacerými pevnými diskami. Užívateľovi sa tak poskytuje kompromis medzi odolnosťou proti výpadku jedného či viac diskov a zároveň medzi kapacitou a výkonom. Existuje veľa typov RAID, medzi najznámejšie a zároveň najjednoduchšie patrí RAID 1, kde sa na dva disky rovnakých kapacít ukladajú totožné informácie a pri výpadku jedného disku sa bez prerušenia pokračuje v činnosti. [84, 86]

5.5.2 Záloha on-line

On-line zálohu dát si užívateľ môže voliť práve vtedy, ak nemá finančné prostriedky do investovania vlastného zálohovacieho média. Takéto zálohovanie predstavuje službu na prenájom určitej diskovej kapacity pre užívateľove dáta. Tieto kapacity sa nachádzajú na serveroch konkrétneho poskytovateľa služby. Pri voľbe tejto formy zálohovania je potrebné si od poskytovateľa služby stiahnuť aplikáciu pre automatické zálohovanie súborov. Po úspešnej inštalácií aplikácie dochádza k výberu súborov, ktoré chce užívateľ zálohovať. Následne sa uskutočňuje samotná automatická záloha na servery poskytovateľa služby pomocou šifrovaného internetového spojenia. Strach a nedôvera užívateľa sa zameriava na obavu prečítania si jeho dát pri prenose. Preto je dôležité vybrať profesionálneho poskytovateľa tejto služby, ktorý zaručí vysokú úroveň zabezpečenia. Konkrétnym príkladom môže byť firma Backovery, alebo služba Dropdox (kapacita zdarma 2GB), pre zálohovanie a zdieľanie súborov. Ďalším príkladom môže byť program Mozy (kapacita zdarma 2 GB), SkyDrive (kapacita zdarma 25 GB), SugarSync (kapacita zdarma 5 GB), Box (kapacita zdarma 2 GB), iCloud (kapacita zdarma 5 GB). [84]

5.6 Obecné závery a možné vývojové trendy pre budúce obdobie

Zálohovanie na vonkajšie pamäťové média by mal poznať každý užívateľ Internetu a počítača. Jedná sa o základný princíp ochrany svojich dát, ktoré majú dôležité a nenahraditeľné zastúpenie v prípade ich straty, poškodenia alebo odcudzenia. Zálohovanie na rovnaký pevný disk nie je bezpečné.

Nevhodné na dlhodobé zálohovanie osobných dát sú tiež USB kľúče. Ich hlavné využitie je najmä pre krátkodobý prenos dát, prípadne krátkodobú zálohu.

Ďalšia možnosť je v podobe on-line zálohy dát, hoci niektorí užívatelia majú strach z ohrozenia dát pri prenose. Nemali by sme podceňovať výber dôveryhodného poskytovateľa služby. Je vhodné a bezpečné si vybrať poskytovateľa on-line zálohovania z danej krajiny, v ktorej žijeme. Tranzitný prenos nemusí byť bezpečný. Príkladom poskytovateľa uvedeného zálohovania môže byť firma Backovery, ktorá je dostupná na webovej stránke *http://www.backovery.sk/*.

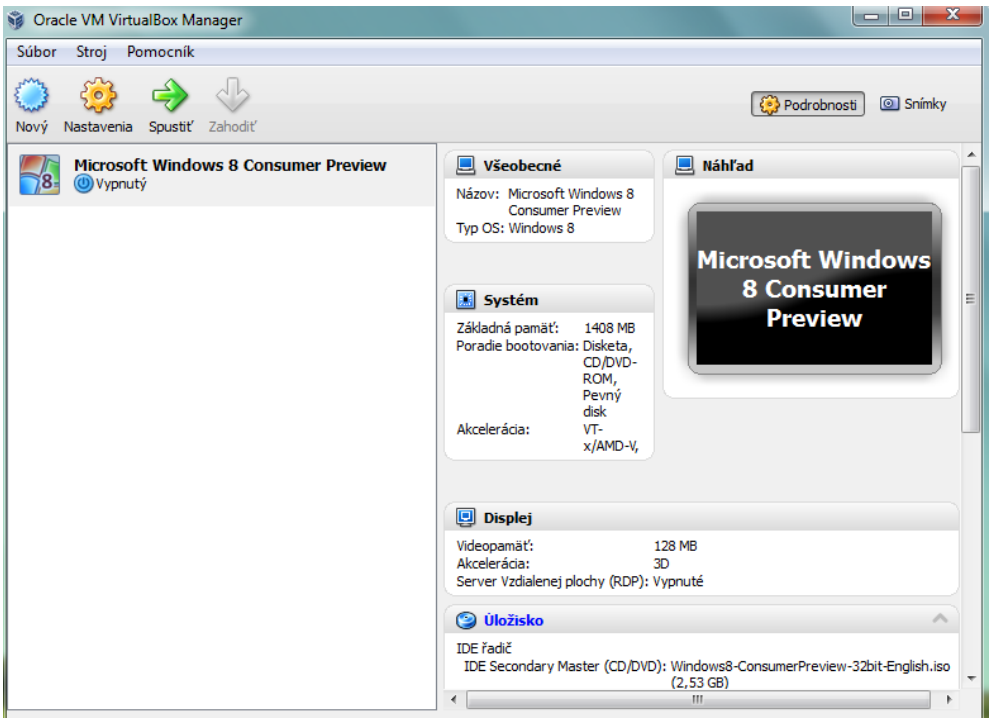
Píše sa rok 2012 a ľudia chcú všetko riadiť, vybavovať jednoducho a rýchlo. Ideálne by bolo pre užívateľa obsluhovať svoj život prostredníctvom mobilných aplikácií inteligentných telefónov či tabletov, jedným stlačením dotykového zariadenia. Do popredia sa dostavajú chytré smartfóny a tablety, ktoré pracujú s operačným systémom Android, oproti klasických počítačov a notebookov. Bankovníctvo a zdravotníctvo by sa malo v budúcom období zamerať na rozvoj technológií pre svojich klientov. Aplikácia v mobilnom telefóne, ktorá nahradí platobnú kartu pri nákupe alebo bezpečné zdravotné záznamy v elektronickej podobe. S príchodom nových možností, s rozvojom technológií je potrebné zamerať pozornosť na bezpečnú realizáciu prevádzky s ohľadom na ochranu dát. Určite sa aj v budúcom období nájdu útočníci, ktorých cieľom bude prekonať rôzne zabezpečenia a dostať sa tak k osobným údajom užívateľa. Práve preto sa budú užívatelia snažiť ochrániť svoje dáta pravidelným zálohovaním. Pozornosť bude v budúcnosti venovaná aj kryptografií, hlavne pri šifrovanom prenose súborov a dát. Štátne alebo súkromné organizácie, spoločnosti priemyslu komerčnej bezpečnosti budú vlastniť viac digitálnych dát a preto bude v ich záujme zabezpečiť ochranu svojich dôležitých dát. Významnú úlohu v budúcnosti môžu zohrávať šifrovacie zariadenia, pracujúce na báze kvantovej kryptografie (kvantové počítače). Kvantová kryptografia pracuje na základe zákonov fyziky (kvantové chovanie fotónov svetla), využíva poznatky kvantovej mechaniky odohrávajúce sa v Hilbertovom priestore. Do popredia sa dostavujú aj rôzne antivírusové programy pre mobilné telefóny a tablety, s cieľom zamerať sa na samotnú ochranu zariadenia a dát pred škodlivými vírusmi. [85]

6 BEZPEČNOSTNÝ INCIDENT

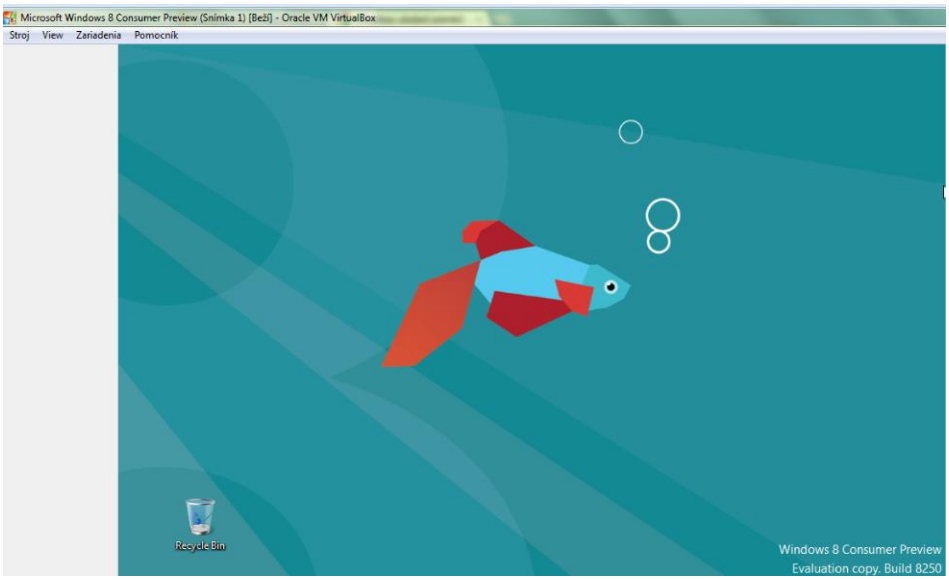
Bezpečnostný incident zobrazuje praktickú ukážku konkrétneho testovacieho vírusu EICAR, ktorý je voľne dostupný na webovej stránke *http://www.eicar.org/85-0-Download.html*. Cieľom praktickej ukážky je zobraziť jednu z mnohých hrozieb ohrozenia dát ako aj samotného operačného systému. Zároveň sa zameriavam na reálnu ochranu pred vírusom v podobne antivírusového programu Microsoft Security Essentials a on-line nástroja na skenovanie ESET Online Scanner. Pozornosť je venovaná aj v samotnej prevencií pred infikovaním počítača v podobe ostražitosti a opatrnosti užívateľa, pri používaní Internetu. Spracovaním praktickej ukážky bezpečnostného incidentu sa zaoberajú nasledujúce kapitoly.

6.1 Realizácia v prostredí VirtualBox

V prvom kroku som realizovala inštaláciu programu VirtualBox. Program VirtualBox, ktorý predstavuje bezpečné virtuálne prostredie, som si vybrala práve preto, aby som ochránila svoje dáta v reálnom operačnom systéme. Rozhodla som sa inštalovať do uvedeného programu operačný systém Microsoft Windows 8 Consumer Preview (ďalej iba Windows 8). Hoci spomenutý operačný systém by mal byť v predaji koncom októbra tohto roku, momentálne je dostupná jeho beta verzia na testovanie.



Obr. 33. VirtualBox Manager.



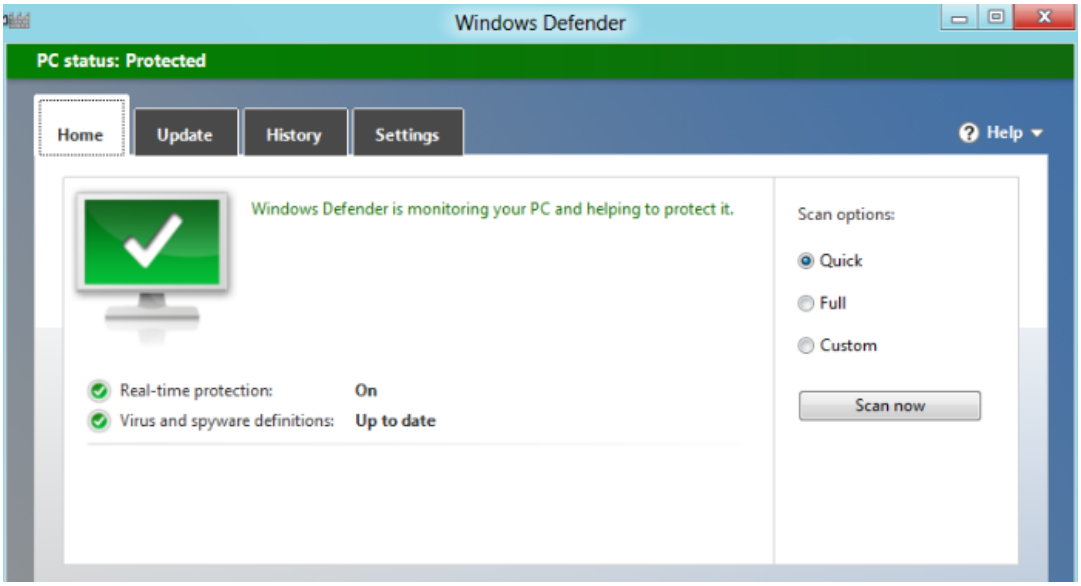
Obr. 34. Windows 8 vo virtuálnom prostredí VirtualBox.

Operačný systém Windows 8, 32 bitový (ktorý som si vybrala) a tiež 64 bitový sú voľne dostupné na webovej stránke *http://windows.microsoft.com/cs-CZ/windows-8/iso*.

6.2 Inštalácia antivírusové programu Microsoft Security Essentials

Následne v ďalšom kroku som prešla k samotnej inštalácií antivírusového programu Microsoft Security Essentials. Inštalácia však nebola nutná, pretože funkcie uvedeného antivírusového programu boli celkom integrované do predinštalovaného programu Windows Defender.

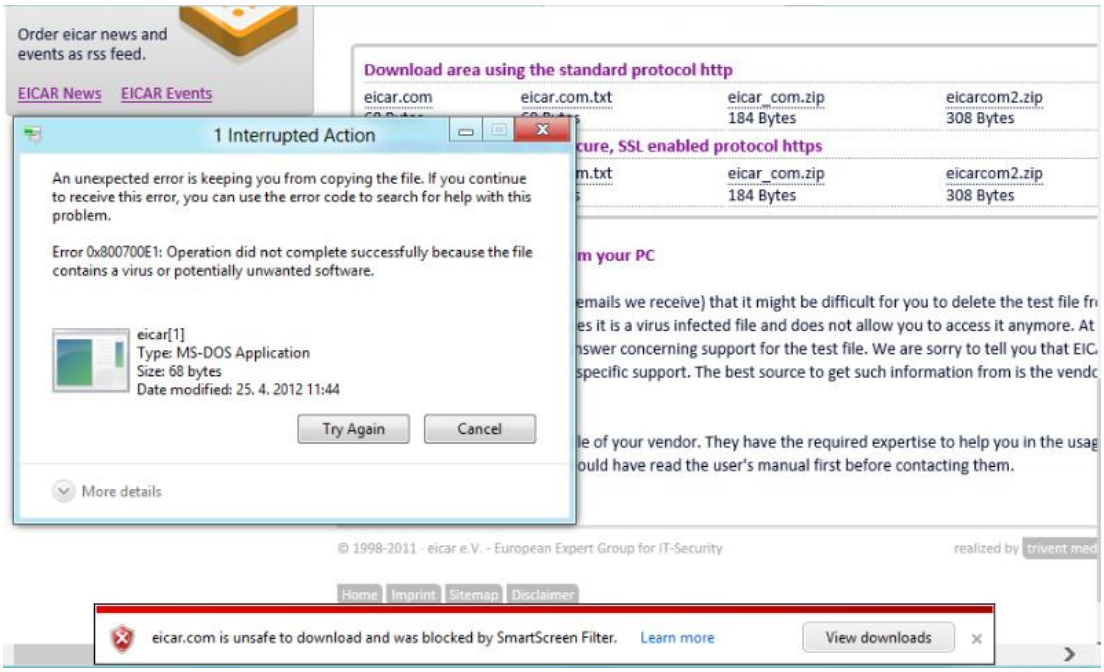
Obr. 35. Chyba pri inštalácií Microsoft Security Essentials.



Obr. 36. Windows Defender.

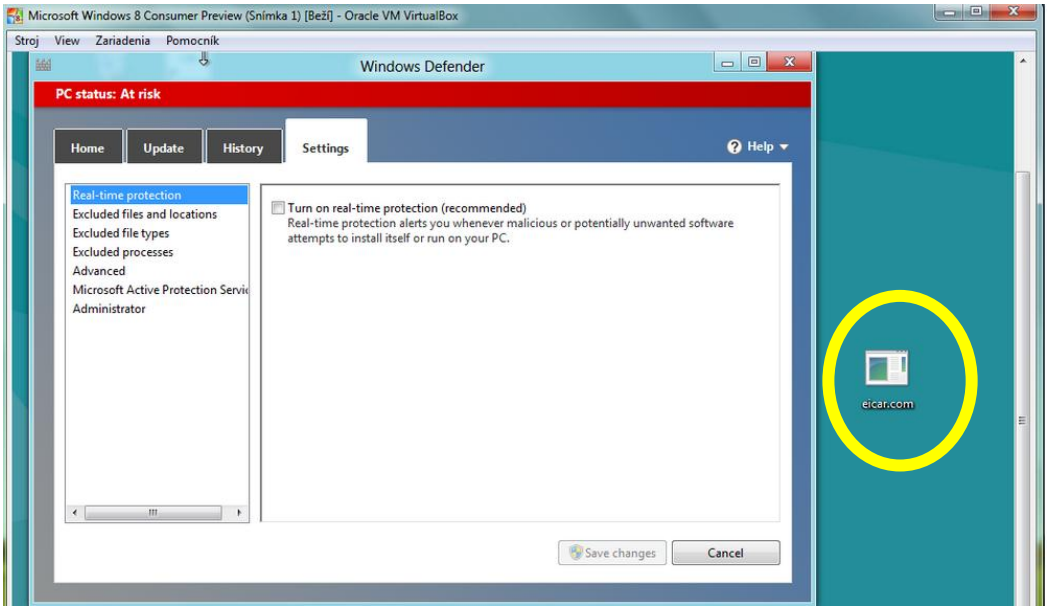
6.3 Aplikovanie infikovaného súboru

V ďalšom kroku som sa zamerala na aplikovanie už spomínaného vírusu EICAR na testovanie reakcie systému. Pri sťahovaní testovacieho vírusu ho Windows Defender hneď rozpoznal. Reakcia uvedeného antivírusového programu na aplikovaný vírus, pri aktívnej funkcií „Real-time protection“ je zobrazená na nasledujúcom obrázku.



Obr. 37. Reakcia antivírusové programu na aplikovaný vírus.

Aby sa dal vírus stiahnuť do virtuálneho operačného systému, bolo potrebné vypnúť ochranu aktívnej funkcie Real-time protection antivírusového programu. Po vypnutí uvedenej funkcie sa infikovaný súbor stiahol a uložil bez problémov, ako je zobrazené na nasledujúcom obrázku v žltom koliesku.

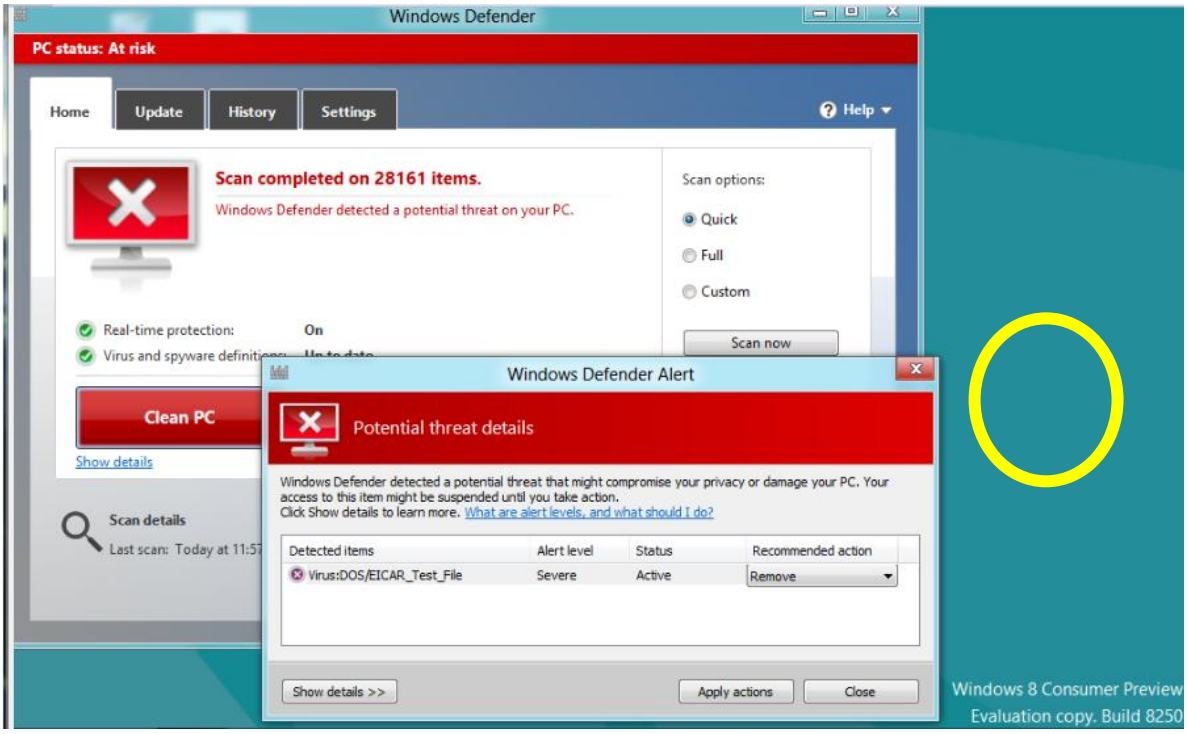


Obr. 38. Vypnutie funkcie Real-time protection.

6.4 Detekcia infikovaného súboru

6.4.1 Windows Defender (predtým Microsoft Security Essentials)

Po opätovnom zapnutí funkcie Real-time protection antivírusového programu nebol vírus detegovaný lebo v momente sťahovania infikovaného súboru sa antivírusový program nepoužíval, bol neaktívny. Až po následnom preskenovaní disku došlo k okamžitému rozpoznaniu vírusu a následne jeho vloženie do karantény. Automaticky bol odstránený infikovaný súbor s názvom eicar.com z pracovnej plochy, ako je zobrazené na obrázku 39.

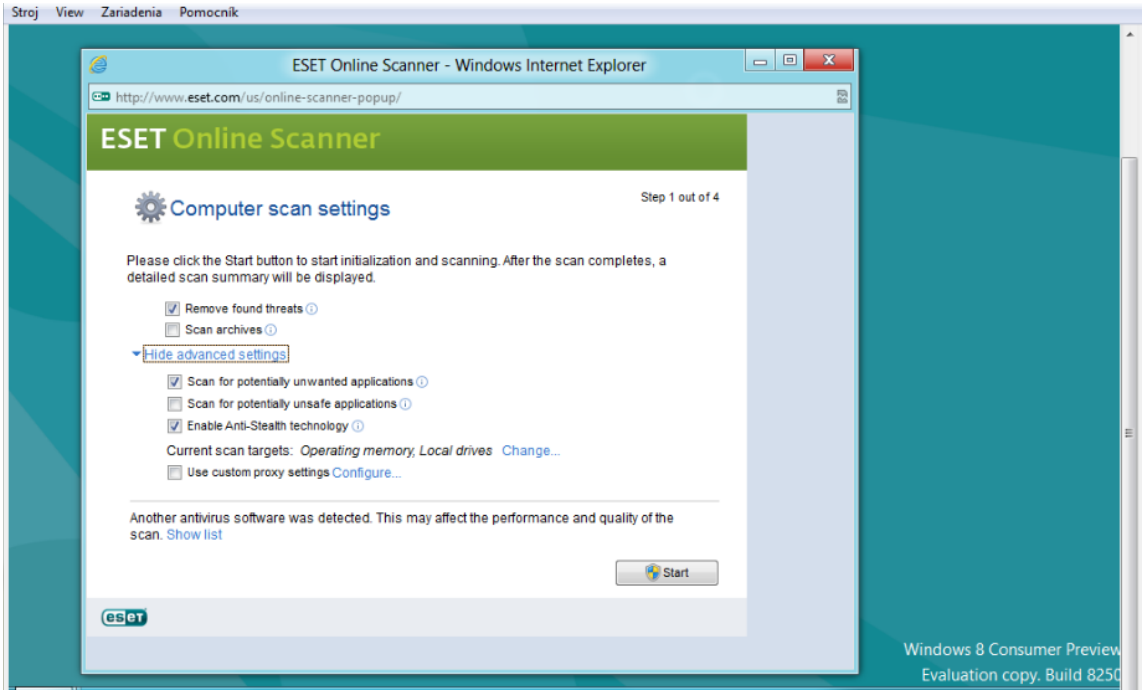


Obr. 39. Identifikácia vírusu a jeho vloženie do karantény.

6.4.2 ESET Online Scanner

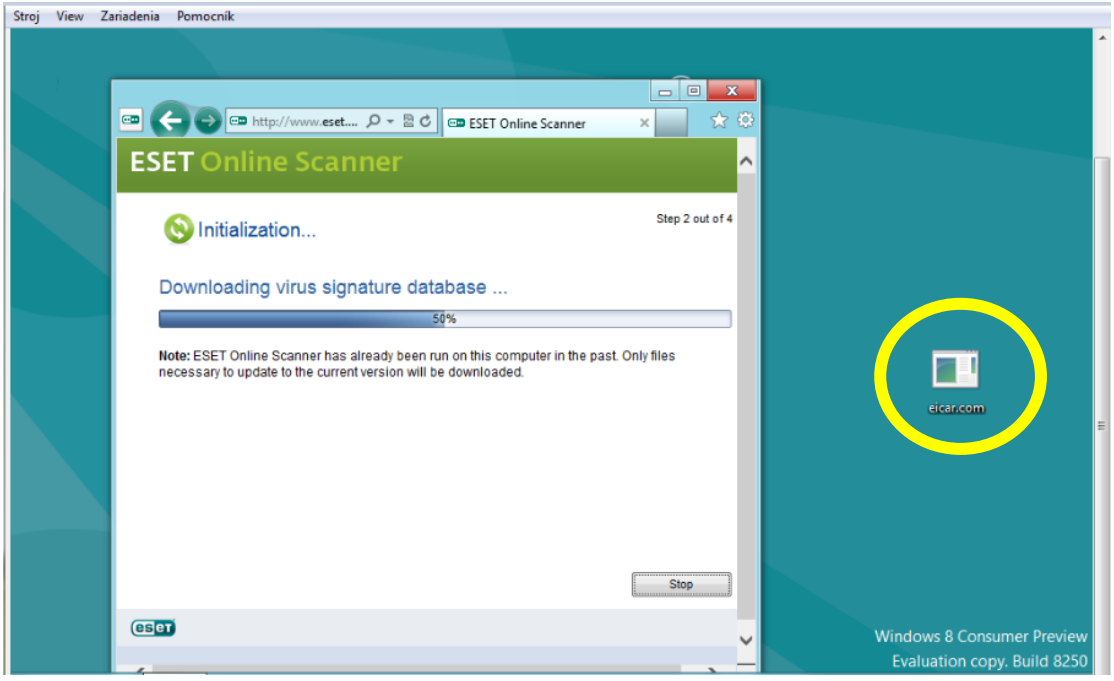
ESET Online Scanner prestavuje bezplatnú službu, ktorá poskytuje užívateľovi rýchlu a nenáročnú kontrolu operačného systému. Je schopný zachytiť a odstrániť všetky druhy počítačových hrozieb. Spúšťanie sa uskutočňuje priamo z internetového prehliadača. Využíva technológiu ThreatSence.Net[3], vďaka ktorej poskytuje aktuálnu vírusovú databázu. Pomocou ESET Online Scanneru som sa zamerala na rovnaký vírus (EICAR), ktorý bol odhalený antivírusovým programom Windows Defender. Celá detekcia sa odohráva v štyroch krokoch, ktoré sú zobrazené na nasledujúcich obrázkoch. [80]

[3] Systém spoločnosti ESET, prostredníctvom ktorého užívatelia zasielajú informácie a vzorky o aktuálnych druhoch infiltrácií, ktoré sa šíria.



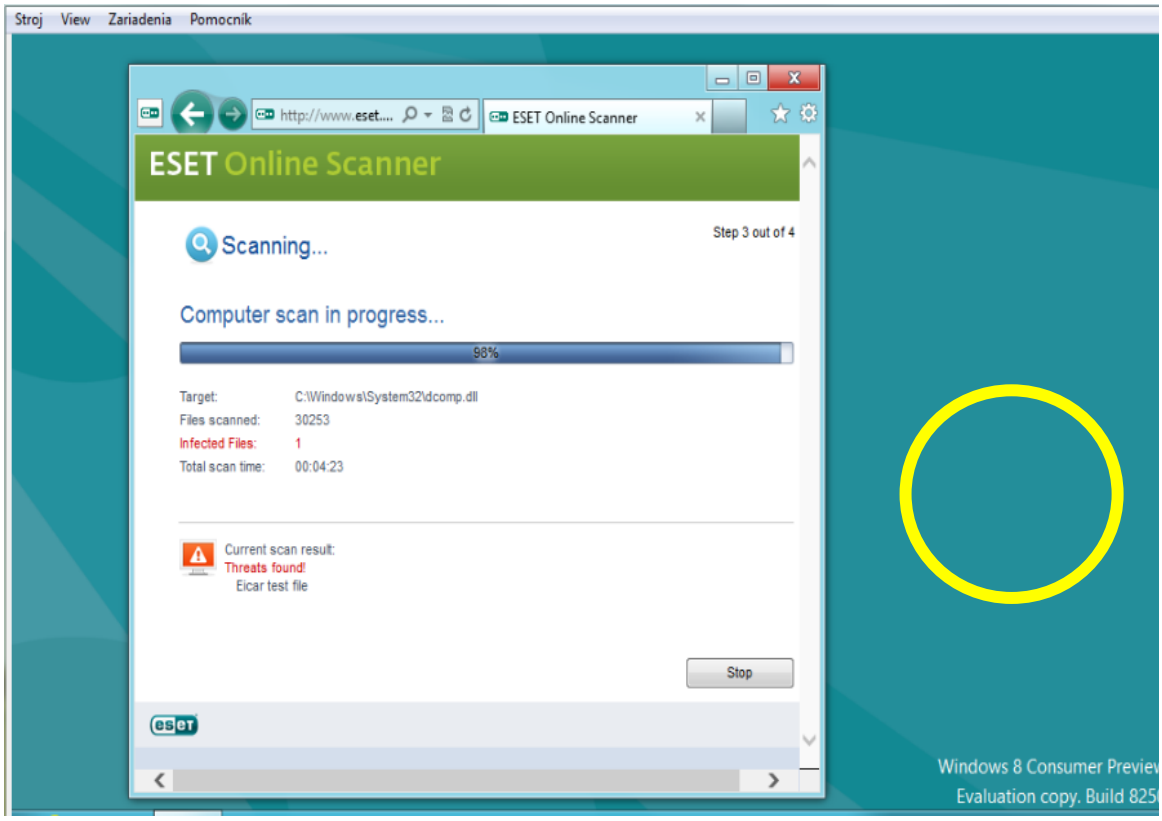
Obr. 40. ESET Online Scanner, prvý krok.

Obrázok 40 zobrazuje prvý krok po spustení bezplatnej služby ESET Online Scanner, kde sú zobrazené voľby možností, ktoré som si vybrala.

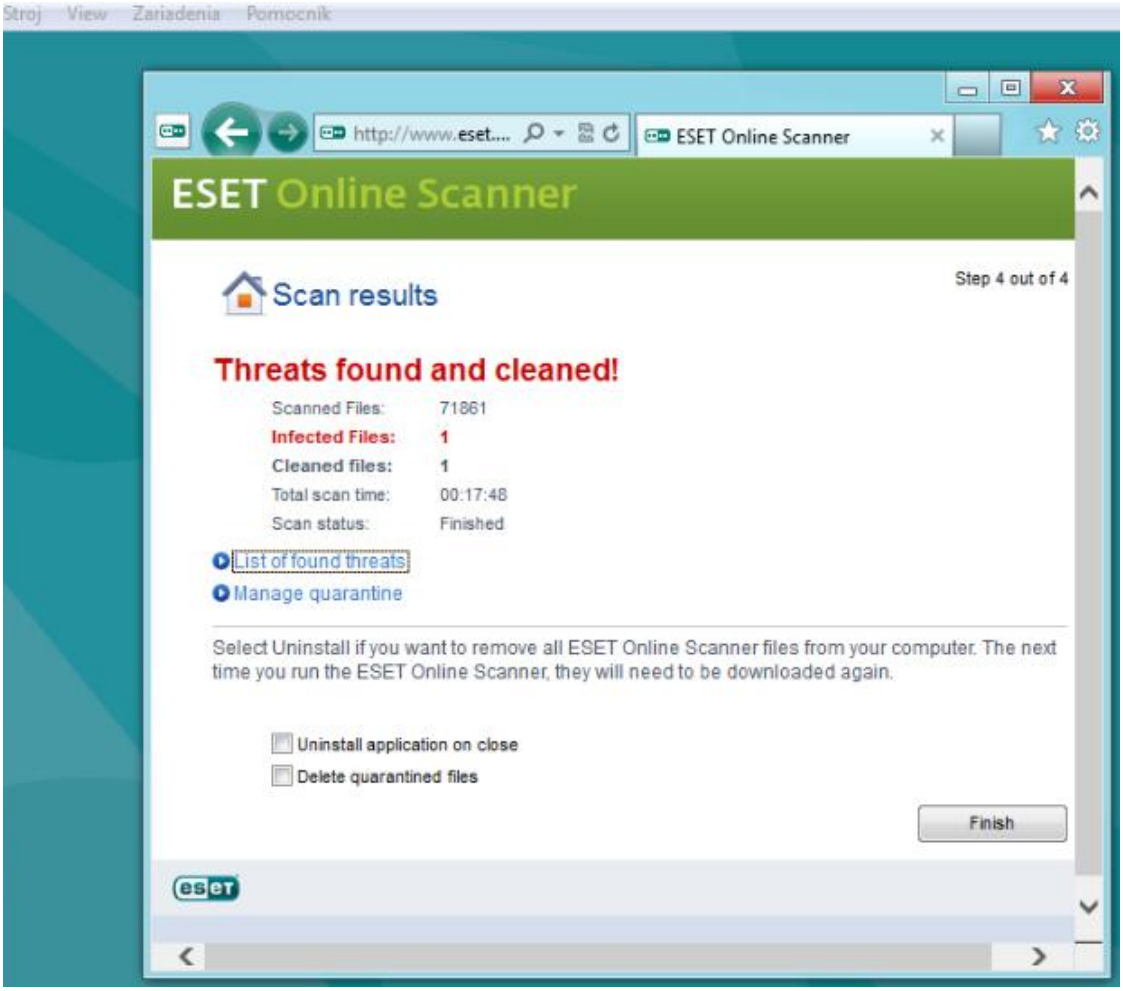


Obr. 41. ESET Online Scanner, druhý krok.

Na obrázku 41 je zobrazená inicializácia vírusovej databázy. Obrázok 42 zobrazuje priebeh skenovania počítača. Po spustení kontroly ESET Online Scannerom bol vírus opäť detegovaný a automatický presunutý do karantény, odkiaľ nepredstavuje ďalšie nebezpečenstvo pre počítač.



Obr. 42. ESET Online Scanner, tretí krok.



Obr. 43. ESET Online Scanner, štvrtý krok.

V poslednom štvrtom kroku je vyhodnotenie samotnej detekcie. Infikovaný súbor bol izolovaný do karantény a užívateľovi bola poskytnutá možnosť nenávratného zmazania súboru. Zároveň sa tu nachádza prehľad o počte skenovaných súborov, počet infikovaných súborov a zároveň počet súborov, ktoré bolo treba vyčistiť. Celkový čas skenovania je iba sedemnásť minút, pretože sa skenovanie realizovalo vo virtuálnom prostredí, kde neboli uložené žiadne dáta. V reálnom systéme môže trvať táto procedúra aj niekoľko hodín.

6.5 Zhodnotenie výsledkov

Vírusy dnes predstavujú každodenné ohrozenie bežného užívateľa Internetu a počítača a práve preto som si vybrala bezpečnostný incident v podobe vírusu. Môj názor sa odvíja od rozšírenosti veľkého počtu známych vírusov, ktoré môžu byť uložené na niektorých stránkach na Internete. Nasledujúca tabuľka obsahuje desať aktuálne najrozšírenejších vírusov, na základe on-line služby „ESET radar on-line“ za posledný týždeň (od 18. apríla do 24. apríla 2012).

Tab. 13. Najrozšírenejšie vírusy za posledný týždeň. [81]

VÍRUS	POČET	POMER INFEKCIE (%)	POMER INFEKCIE
1. Win32/TrojanDownloader.Agent.RAG trojan	3986	0.007 %	1/ 14.1 tis.
2. a variant of Win32/Kryptik.AEIP trojan	2437	0.004 %	1/ 23.1 tis.
3. Win32/Netsky.Q worm	1557	0.003 %	1/ 36.2 tis.
4. Win32/Netsky.C worm	1032	0.002 %	1/ 54.6 tis.
5. Win32/Zafi.B worm	619	0.001 %	1/ 91.0 tis.
6. Win32/Bagle.HE worm	433	0.001 %	1/ 130.1 tis.
7. Win32/Mydoom.Q worm	384	0.000 %	1/146.7 tis.
8. a variant of Win32/Kryptik.AEPB trojan	123	0.000 %	1/458.1 tis.
9. Win32/Merond.O worm	110	0.000 %	1/512.2 tis.
10. HTML/Phishing.Gen trojan	81	0.000 %	1/ 695.6 tis.

Testovací vírus, ktorý som aplikovala sa nazýva EICAR. Vznikol po dohovore výrobcov antivírusových programov. Uvedený vírus predstavuje nevinný bezpečný súbor, ktorý by nemal spôsobiť užívateľovi škodu, často sa používa práve pri samotnom testovaní antivírusových programov. Názornú ukážku som realizovala prostredníctvom testovacieho vírusu z dôvodu ochrany reálneho operačného systému a zároveň svojich dát. Ak by sa daný bezpečnostný incident realizoval pomocou skutočného vírusu, nebolo by to profesionálne, pretože by do vážnej miery mohlo dôjsť k ohrozeniu operačného systému. Takéto ohrozenie by sa mohlo prejaviť v podobe celkového spomalenia systému, pretože by došlo k uloženiu vírusu niekde do pamäti alebo na pevnom disku a následne by sa mohol začať vírus šíriť po celom pevnom disku, čo by stále viac spomaľovalo chod počítača. Zároveň by mohlo dôjsť k skutočnému ohrozeniu dát v podobe ich krádeže či nebezpečenstvo v podobe šifrovania, prípadne samotného zničenia alebo vymazania dát.

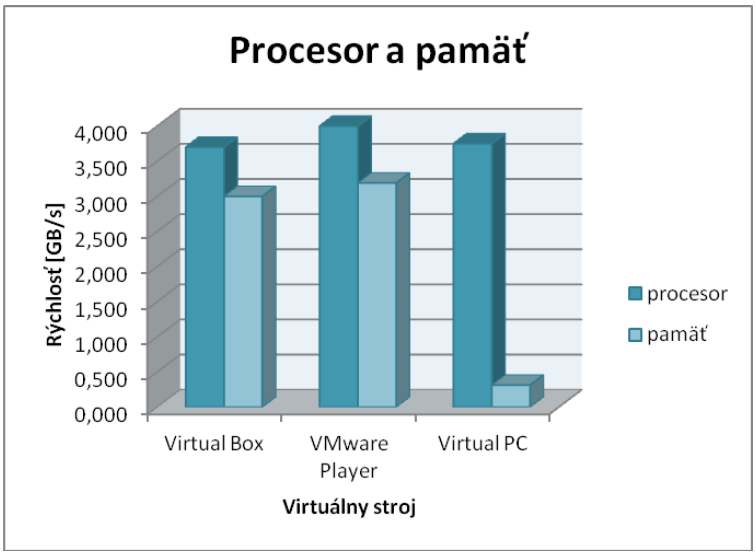
Výhodu pre čitateľa práce vidím v tom, že si môže prostredníctvom predstaveného vírusu otestovať svoj vlastný antivírusový program, ktorý aktuálne používa vo svojom počítači, čím zároveň zistí jeho schopnosť detekcie aplikovaného vírusu.

Zamerala som sa na testovanie a detekciu vírusu prostredníctvom antivírusového programu Microsoft Defender, pretože sama využívam jeho predchodcu Microsoft Internet Essentials a zároveň je pre bežných užívateľov Internetu dostupný zdarma, je ale potrebné mať platnú licenciu na OS Windows, ako som sa zmienila v kapitole 4.1.1.3, kde som ho čitateľom práce už predstavila. Zároveň bude Microsoft Defender už súčasťou Windwos 8, ktorý sa dostane na trh koncom októbra tohto roku.

Pre predstavenie, zaujímavého a názorného príkladu som sa zamerala na ESET Online Scanner, ktorý veľa užívateľov nepozná. Hlavnú výhodu vidím v jeho dostupnosti zdarma, bez nutnej inštalácie. Samotné spustenie programu je priamo prostredníctvom internetového prehliadača. Poskytuje rozšírenú podporu prehliadačov, medzi najpoužívanejšie patria Inernet Explorer, Mozilla Firefox, Opera, Chrome. Užívateľ si prostredníctvom uvedenej služby môže rýchlo a nenáročne urobiť kontrolu svojho operačného systému.

Súčasné počítače poskytujú vysoký výkon, aby bolo možné pracovať s dvomi operačnými systémami naraz. Hovoríme o virtualizácií, ktorá predstavuje súbežný beh viacerých izolovaných operačných systémov v jednom počítači. Takto vzniknuté operačné systémy sa delia o hardwarové prostriedky (procesor, pamäť, apod.), ale pritom sú od seba navzájom oddelené. Zároveň je dodržaná bezpečnosť každého operačného systému, pretože navzájom o sebe nevedia. Virtualizáciu je vhodné použiť napríklad pre skúšanie/testovanie nových programov. Preto som sa aj ja rozhodla použiť virtuálne prostredie pri aplikovaní infikovaného súboru, aby som ochránila svoj reálny operačný systém. Medzi najznámejšie a najviac využívanie virtuálne prostredia môžeme zaradiť VirtualBox, VMware a Virtual PC. Vo svojej praxi som sa stretla iba s prvými dvomi vymenovanými. VMware je dnes veľmi využívaný, vybrala som si však VirtualBox, ktorý je možné inštalovať v operačných systémoch Windows XP/Vista/7, MAC OS a Linux. Zároveň v programe VirtualBox môžeme virtualizovať širokú škálu operačných systémov, napríklad Solaris, rôzne distribúcie Linuxu, Mac OS X a samozrejme tiež najpoužívanejšie MS Windows.

Pre optimálny beh týchto operačných systémov zadávame do VirtualBoxu tiež patričnú verziu systému, pre MS Windows, máme na výber od verzie 3.1 až po najnovšiu verziu Windows 8 (vrátane 64 bit varianty). Pre jeho inštaláciu vo Windows 7 je potrebné mať minimálne 512 MB voľnej pamäte RAM. Keďže VMware ešte nie je takto prispôsobený pre beh Windows 8, nemôžem v ňom túto verziu zvoliť, vybrala som si radšej pre virtualizáciu práve VirtualBox.



Obr. 44. Procesor a pamäť.[88]

Obrázok 44 zobrazuje grafické spracovanie testovania rýchlosti virtuálneho procesora (pri aritmetických výpočtoch, uvedenú v miliónoch operácií za sekundu) a test priepustnosti pamäte RAM pre konkrétne virtuálne stroje (VirtualBox, VMware Player a Virtual PC). Test bol realizovaný v nástroji na testovanie rýchlosti diskov CrystalDiskMark 3. Výsledky ukazujú, že Virtual PC je obmedzený nízkou hodnotou priepustnosti pamäte a je pozadu s porovnaním s ostatnými uvedenými. Z testovaných virtuálnych nástrojov dopadol najlepšie VMware. [87, 88]

Finálna verzia operačného systému Windows 8 bude v ponuke koncom októbra tohto roku, v štyroch verziách (Windows 8, Windows 8 Pro, Windows 8 RT a Windows 8 Enterprise). Prvé dve menované sú zamerané na domáceho užívateľa. Dovtedy je možné si stiahnuť a skúšať testovaciu verziu z webovej stránky*: http://windows.microsoft.com/cs-CZ/windows-8/iso.*

Pre Windows 8 som sa rozhodla ako pre možnosť vyskúšať nové technológie, spôsob ovládania tohto operačného systému, zoznámenie sa s novým pracovným prostredím a tiež ako v ňom bude fungovať antivírusový program Microsoft Security Essentials.

Zároveň ma Windows 8 zaujal grafický, pretože obsahuje nové pracovné prostredie „Metro“, ktoré je veľmi podobne (prispôsobené) predovšetkým dotykovým obrazovkám tabletov a nových smartfónov (podobný operačnému systému Android). [89]

6.6 Návrh prevencie

Dôležitá prevencia voči vírusom je v samotnom užívateľovi. Je veľmi podstatná jeho ostražitosť, ochrana a informovanosť. Veľa vírusov si môžeme zaobstarať sami, pri klikaní na rôzne odkazy, sťahovaní nebezpečných príloh e-mailových správ (dnes rozšírená forma rozposielania vírusov od neznámych odosielateľov), prenášaní rôznych súborov alebo v ľahostajnom používaní flash diskov. Ako užívatelia Internetu by sme nemali byť príliš dôverčivý a nemali by sme všetkým a všetkému dôverovať. Skôr ako si niečo prinesieme a uložíme do svojho počítača, mal by sa daný súbor podrobiť kontrole. Predchádzajme nebezpečenstve v podobe vírusov hlavne zodpovedným prístupom pri komunikáciách na sociálnych sieťach alebo pri sťahovaní a výmene súborov z verejných počítačov (školská počítačová učebňa). Dôležitá je aj ostražitosť pri príchode e-mailov od neznámych odosielateľov. Zároveň používajme dôverných e-mailových klientov, kde automatické spúšťanie príloh nepovolíme. Mali by sme si uvedomiť, že stopercentná ochrana dát uložených v počítači nie je uskutočniteľná, prevencie však nikdy nie je dosť.

Práve preto by sme mali dbať na zmiernenie rizík poškodenia, krádeže, zneužitia alebo úplného odstránenia dát a nepodceňovať používanie antivírusového programu a firewallu, pravidelne sa zameriavať na prehliadky svojho počítača. V neposlednom rade je dôležité zálohovanie svojich dát a prípadne ich šifrovanie pre ochranu pred prístupom k nim nepovolenou osobou.

ZÁVER

Problematika počítačovej kriminality súčasnosti úzko súvisí so zdokonaľovaním informačných technológií. Pri dnešnom rozvoji a inováciách v oblasti informačných technológií sa stále viac kladie dôraz na bezpečnosť a ochranu dát. Samotná problematika ochrany dát v počítači sa dnes nevzťahuje iba na dáta v štátnych alebo súkromných organizáciách, spoločnostiach priemyslu komerčnej bezpečnosti ale pozornosť sa práve kladie aj na dáta, ktoré sú súčasťou nášho každodenného života v osobných počítačoch. S ochranou dát súvisí ich dôkladné zálohovanie, na ktoré by užívateľ nemal zabúdať. Praktická časť diplomovej práce v základnom rozsahu zobrazuje najvyužívanejšie možnosti zálohy dát a ich ochranu v podobe symetrického a asymetrického šifrovania. S ochranou dát úzko súvisí samotná ochrana počítača a jeho operačného systému. Práve preto je dôležité zameranie sa na možnosti ochrany, ktoré máme v ponuke hneď po spustení počítača. Nepodceňovať dôležitosť antivírusového programu a ochranu v podobe firewallu. Je praktické a bezpečné využívať a kombinovať viac prvkov bezpečného prihlásenia do systému.

V informačnom svete je najdôležitejšia informovanosť, práve preto je dôležité si definovať hrozby, čo všetko sa nám môže stať, čo nás môže ohroziť a následne sa k novým skutočnostiam postaviť. Okrem definovania existencie najznámejších hrozieb sa v predloženej práci zameriavam aj na bezpečnostné riziká sociálnych sietí, v podobe straty súkromia, ohrozenia osobných údajov, dôverčivosti mladistvých a s tým spojená hrozba pedofílie. Mali by sme s informáciami o sebe a ich zverejňovaním nakladať s dostatočnou obozretnosťou a opatrnosťou.

Posledná kapitola praktickej časti diplomovej práce venuje pozornosť ukážkovému spracovaniu bezpečnostného incidentu, infikovaného súboru predstavujúceho vírus. Vírusy znamenajú rozsiahle nebezpečenstvo súčasnosti. Z tohto záveru je dôležité poznať svoj antivírusový program a vedieť ako pracuje, aká je jeho reakcia pri infikovaní škodlivého súboru, aby sme dostatočne mohli ochrániť svoj počítač. Prevencia vzniku incidentu sa zameriava na samotného užívateľa Internetu, na jeho informovanosť, ostražitosť pri sťahovaní rôznych súborov a zároveň využívaní sociálnych sietí a s tým súvisiaca pripravenosť užívateľa na vznik možného ohrozenia. Práca obsahuje obecne definovanie bezpečnostných rizík súvisiacich s informačnou kriminalitou a s ňou spojené legislatívne aspekty. Pozornosť je venovaná dôležitosti ochrany dát a samotného počítača.

Pozornosť sa zameriava aj na sociálne siete a naznačenie bezpečnostných rizík, ktoré so sebou prinášajú. V neposlednom rade sú uvedené možné spôsoby riešenia bezpečnostných rizík sociálnych sietí. Praktické spracovanie identifikácie infikovaného súboru v operačnom systéme má poukázať na základnú ochranu a dôležitosť antivírusového programu a iného prostriedku, v podobe ľahko dostupného on-line skenera operačného systému pre odhalenia nebezpečenstva. Pracovníci štátnych alebo súkromných organizácií, spoločností alebo agentúr priemyslu komerčnej bezpečnosti pracujú s dôležitými dátami, využívajú Internet a tiež e-mailové adresy. Práve preto je strategicky správne poznať existenciu možného ohrozenia v oblasti informačných technológií. V taktom prípade sa kladie dôraz napríklad, ako bolo uvedené v práci, na zásadne oddelenie pracovnej a súkromnej e-mailovej adresy. Nevystavovať dôležité dáta možnému nebezpečenstvu je vo väčšej miere na pleciach užívateľa počítača a Internetu a preto by mal každý jedinec k tejto skutočnosti pristupovať zodpovedne, s dostatočnou obozretnosťou, predvídaním, informovanosťou a pripravením.

CONCLUSION

The problematic with the computer criminality is closely related to the improvement of information technologies. With a contemporary development and innovation of information technologies, the biggest emphasis is put on security and data protection. The problematic of data protection itself is nowadays not related only to data in the state-owned or private organizations or in the industrial companies but also the biggest emphasis is put on the data which are parts of our everyday work with personal computers. The user should not definitely forget about making a back up of his/her data since it is closely related to the protection of data itself. The practical part of the master thesis dealt in its basic extent with the most commonly used possibilities of making back up of data and its protection in the form of symmetrical and asymmetrical cryptography. The protection of the computer is another aspect closely related to the computer protection and its operational system. Therefore it is important to concentrate on the protection possibilities which are offered right after launching the computer. It is important not to underestimate the importance of antivirus program and the firewall protection. For the users it is practical and safe to combine more elements of secure enrolment in to the system.

In this informational world, information is the most important element and therefore it is really important to define the threats that may threaten our being in this world. The art is to know how to define it and react appropriately. Except for defining the best known forms of threats, the given thesis is oriented on the safety risks of social network like the loss of privacy, endangering the personal data, trustfulness of the youth and the threat of paedophilia closely connected with it. We should publish our personal data with the circumspection and carefulness.

The last chapter in the practical part of the master thesis is related to sample processing of the safety incident- contaminated file which represents a virus. Viruses are given as a potential threat in today's technological world. Therefore it is crucial to know your antivirus program and be able to use it and recognize its reaction while being contaminated by a virus. The protection of an incident formation is connected directly with the Internet user, his/her awareness while downloading various files and his alertness with potential threat while using social networks.

The thesis generally contains the definition of safety risks which are related to informational criminality and the legislative aspects. The attention is given to the importance of data protection and the computer itself. The other part of the thesis is aimed at the social networks and implying of the safety risks connected with it. Last but not least, there are stated possible methods of solutions to this safety risks at social networks. The practical identification processing of the file in the operating system should point out the basic protection and importance of the antivirus program and also it should point out the other means in the form of easily accessible online scanner of operating system for detecting the threat. Those working in state and private sector or in industrial agencies for commercial protection have been working with very important data. They have been using Internet and email addresses as well and therefore it is strategically useful to known the existence of potential threat in the field of information technologies. In this case the emphasis is put on the absolute separation of email address as stated in the thesis earlier. It is the matter of the Internet user not to expose the important data to potential threat and that's why each human being should deal with this problematic in a responsible manner, with circumspection, foresight, awareness and alertness.

ZOZNAM POUŽITEJ LITERATÚRY

[1] MATĚJKA, Michal. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002, 106 s. ISBN 80-722-6419-2.

[2] ČANDÍK, Marek. *Základy informační bezpečnosti*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004, 107 s. Učební texty vysokých škol (Univerzita Tomáše Bati ve Zlíně). ISBN 80-731-8218-1.

[3] KOSTRECOVÁ, Eva, Matúš JÓKAY a Matej KOSTREC. *Počítačová kriminalita*. Vyd. 1. Bratislava: Slovenská technická univerzita v Bratislave v Nakladateľstve STU, 2010, 128 s. ISBN 978-80-227-3410-3.

[4] PŘIBYL. Kapitoly z historie hackingu - [II] 10 útoků, které změnily svět. *Security Word* [online]. 2006, [cit. 2012-02-14]. Dostupné z: http://securityworld.cz/securityworld/kapitoly-z-historie-hackingu-ii-10-utoku-ktere-zmenily-svet-1104.

[5] CHOLEVA, Martin. *Počítačová kriminalita na Slovensku*. Žilina, 2007. Bakalárska práca. Žilinská univerzita. Vedoucí práce Ing. František Kaluža.

[6] RAK, Roman a Radek KUMMER. Motivace a znalosti pachatelů kybernetické trestné činnosti. *SecurityWorld* [online]. 2006, [cit. 2012-02-29]. Dostupné z: http://securityworld.cz/securityworld/motivace-a-znalosti-pachatelu-kyberneticke-trestne-cinnosti-1079.

[7] *Počítačová kriminalita a počítačová bezpečnosť*. Bratislava: Akadémia Policajného zboru SR, 1996. ISBN 80-88751-88-8.

[8] Phishing. In: *Wikipedia*: *the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2012 [cit. 2012-03-09]. Dostupné z: http://sk.wikipedia.org/wiki/Phishing.

[9] Čo je to spam a antispam. *Centrum holdings* [online]. © 2012 [cit. 2012-03-07]. Dostupné z: http://www.centrumholdings.sk/email/694401-co_je_to_spam_a_antispam.

[10] Spam. In: *Wikipedia*: *the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2012 [cit. 2012-03-09]. Dostupné z: http://sk.wikipedia.org/wiki/Spam.

[11] RSS (formát súboru). In: *Wikipedia*: *the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2012-03-09]. Dostupné z: Phishing. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2012 [cit. 2012-03-09]. Dostupné z: http://sk.wikipedia.org/wiki/Phishing.

[12] Prevencia. In: *Zodpovedne.sk* [online]. [cit. 2012-03-08]. Dostupné z: http://www.zodpovedne.sk/download/Prevencia.pdf.

[13] Trestný zákon. In: *Zbierka zákonov č. 300/2005*. 20. mája 2005.

[14] PALÁT, Michal. Boj proti spamu: súboj Dávida s Goliášom. *Živе* [online]. 2003 [cit. 2012-03-09]. Dostupné z: http://www.zive.sk/boj-proti-spamu-suboj-davida-s-goliasom/sc-3-a-256678/default.aspx.

[15] POŽÁR, Josef. *Informační bezpečnost*. Vyd. 1. Plzeň: Aleš Čeněk, 2005, 311 s. Vysokoškolská učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-86898-38-5.

[16] STREHOVSKÝ, Michal. Cracking a ochrana pred ním, 1. časť: pohľad crackera. *Živé* [online]. 2005 [cit. 2012-03-13]. Dostupné z: http://www.zive.sk/cracking-a-ochrana-pred-nim-1-cast-pohlad-crackera/sc-3-a-264533/default.aspx.

[17] Delenie počítačových vírusov. *Pcplusbeh.blog* [online]. 2010 [cit. 2012-03-15]. Dostupné z: http://pcplusbeh.blog.cz/1002/delenie-pocitacovych-virusov.

[18] *POČÍTAČOVÉ VÍRUSY*. 2012. Dostupné z: http://www.gt12.sk/predmety/inf/materialy/ucebnica/informacna_spolocnost/informacna_spolocnost.htm.

[19] Malware. In: *Wikipedia*: *the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2012 [cit. 2012-03-15]. Dostupné z: http://sk.wikipedia.org/wiki/Malware.

[20] B., Martin. Počítačová kriminalita. *Virusy.yw.sk* [online]. 2009 [cit. 2012-03-18]. Dostupné z: http://www.virusy.yw.sk/pckriminalita.html.

[21] ZADRAŽILOVÁ, Iva. *Nebezpečí zneužití osobních informací v době globálního monitoringu s přihlédnutím k možnostem ochrany soukromí*. Brno, 2009. Diplomová práca. MASARYKOVA UNIVERZITA.

[22] ŽEMLIČKA, Martin. *Trestněprávní úprava počítačové kriminality*. Brno, 2009. Bakalárska práca. Masaryková univerzita.

[23] ŠČUČINSKÝ, Pavel. *Fenomén počítačového pirátství*. Olomouc, 2011. Diplomová práca. Univerzita Palackého v Olomouci.

[24] Kto je hacker?. *Blackhole* [online]. 2004 [cit. 2012-03-21]. Dostupné z: http://blackhole.sk/topickto-je-hacker.

[25] Hacker. *Hacking & Programming* [online]. 26. 12. 2006 [cit. 2012-03-21]. Dostupné z: http://realhacking.wz.cz/articles/article11.php.

[26] HAVROŠ, RICHARD. Sociálne inžinierstvo: crackeri v oblekoch. In: *SME* [online]. 2002 [cit. 2012-03-21]. Dostupné z: http://pocitace.sme.sk/c/531255/socialne-inzinierstvo-crackeri-v-oblekoch.html.

[27] Informačná bezpečnosť. *CSIRT* [online]. 2010 [cit. 2012-03-21]. Dostupné z: http://www.csirt.gov.sk/informacna-bezpecnost/navody-a-odporucania/socialne-inzinierstvo-812.html.

[28] OSTER, Jaroslav. Protivírusová ochrana - Publikácie. *Vírusy* [online]. 2001 [cit. 2012-03-24]. Dostupné z: http://www.virusy.sk/clanok.ltc?ID=19.

[29] Počítačové vírusy. *Uniba* [online]. 2003 [cit. 2012-03-26]. Dostupné z: http://edi.fmph.uniba.sk/~winczer/SocialneAspekty/NovotnyVirusy.htm.

[30] Vírusy. *ZONES* [online]. 2008 [cit. 2012-03-26]. Dostupné z: http://www.zones.sk/studentske-prace/informatika/1126-virusy/.

[31] Antivírusová ochrana počítača. *Antivirus.vacau* [online]. 2012 [cit. 2012-03-26]. Dostupné z: http://antivirus.vacau.com/softwarova-ochrana/.

[32] Firewall. *Bezpečné PC* [online]. 2011 [cit. 2012-03-26]. Dostupné z: http://www.bezpecne-pc.estranky.sk/clanky/zakladne-nastavenia-pc/firewall.html.

[33] Microsoft Security Essentials. *Windows.microsoft* [online]. 2012 [cit. 2012-03-26]. Dostupné z: http://windows.microsoft.com/sk-SK/windows/products/security-essentials.

[34] The Independent IT-Security Insitute. *AV-Test* [online]. 2012 [cit. 2012-03-27]. Dostupné z: http://www.av-test.org/en/tests/test-reports/janfeb-2012/.

[35] Legislatívny zámer zákona o informačnej bezpečnosti. *Informatizácia* [online]. 2010 [cit. 2012-03-27]. Dostupné z: http://www.informatizacia.sk/vyhladavanie/1534s?page=2&stext=N%C3%A1vrh.

[36] MUSIL, Stanislav. *POČÍTAČOVÁ KRIMINALITA*. Praha, 2000, 299 s. ISBN 80-86008-80-0.

[37] Business Software Alliance. *BSA* [online]. 2000-2011 [cit. 2012-03-31]. Dostupné z: http://www.bsa.org/country/BSA%20and%20Members.aspx.

[38] *BSA* [online]. Praha, 2011 [cit. 2012-03-31]. Dostupné z: http://portal.bsa.org/globalpiracy2010/downloads/press/pr_czech_czech.pdf.

[39] KOVÁČ, Martin. Pirátskeho softvéru vlani u nás ubudlo, no nie v domácnostiach. *Živé*: *ako na počítač* [online]. 2011 [cit. 2012-03-31]. Dostupné z: http://anp.zive.sk/?q=node/4601.

[40] Pirátstvo na Slovensku je menšie. *PCSPACE* [online]. 2011 [cit. 2012-03-31]. Dostupné z: http://www.pcspace.sk/index.php/spravy/aktuality/4710-piratstvo-na-slovensku-je-menie.

[41] *BSA* [online]. Bratislava, 2010 [cit. 2012-03-31]. Dostupné z: http://portal.bsa.org/globalpiracy2009/pr/pr_slovakia.pdf.

[42] Veda a technika Počítače a internet: Miera softvérového pirátstva na Slovensku vlani klesla. *Webnoviny*[online]. 2011 [cit. 2012-03-31]. Dostupné z: http://www.webnoviny.sk/veda-a-technika/miera-softveroveho-piratstva-na-slove/348452-clanok.html?from=suggested_articles.

[43] PC: BSA rozbieha novú kampaň proti nelegálnemu softvéru. *Zoznam.sk* [online]. 2011 [cit. 2012-03-31]. Dostupné z: http://pc.zoznam.sk/novinka/bsa-rozbieha-novu-kampan-proti-nelegalnemu-softveru.

[44] Anonymous (skupina). In: *Wikipedia*: *the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2012-03-31]. Dostupné z: http://cs.wikipedia.org/wiki/Anonymous_(skupina).

[45] Hackeri Anonymous vyvolali internetovú vojnu: Čo sú vlastne zač?. *Topky.sk* [online]. 2012 [cit. 2012-03-31]. Dostupné z: http://www.topky.sk/cl/11/1296939/Hackeri-Anonymous-vyvolali-internetovu-vojnu--Co-su-vlastne-zac-.

[46] Hnutie Anonymous. *Google obrázky* [online]. 2012 [cit. 2012-03-31]. Dostupné z: http://www.google.sk/search?tbm=isch&hl=sk&source=hp&biw=1280&bih=699&q=hnutie+anonymous&gbv=2&oq=hnutie+a&aq=0S&aqi=g-S2&aql=&gs_l=img.1.0.0i24l2.35204l37263l0l39079l8l8l0l2l2l0l114l570l5j1l6l0.frgbld.

[47] Anonymous se chystají zaútočit na Slovensku. *Pirátské Noviny* [online]. 2012 [cit. 2012-03-31]. Dostupné z: http://www.piratskenoviny.cz/?c_id=33543.

[48] Anonymous deň pred voľbami zaútočí na weby politických strán. *TA3* [online]. 2012 [cit. 2012-03-31]. Dostupné z: http://www.ta3.com/clanok/10830/anonymous-den-pred-volbami-zautoci-na-weby-politickych-stran.html.

[49] Anonymous podporí protest Gorila útokom na weby MS SR a Penty. *TA3* [online]. 2012 [cit. 2012-03-31]. Dostupné z: http://www.ta3.com/clanok/9362/anonymous-podpori-protest-gorila-utokom-na-weby-ms-sr-a-penty.html.

[50] Ochrana počítača pred vírusmi. *Ekonomická Fakulta*: *Systém pre podporu vzdelávania* [online]. 2010 [cit. 2012-04-01]. Dostupné z: http://www2.ekf.tuke.sk/moodledata/4/moddata/assignment/2/4050/ochrana.html.

[51] Windows: Čo je zabezpečovací hardvér modulu TPM (Trusted Platform Module)?. *Windows.Microsoft* [online]. 2012 [cit. 2012-04-01]. Dostupné z: http://windows.microsoft.com/sk-SK/windows-vista/What-is-the-Trusted-Platform-Module-security-hardware.

[52] PAVLIS, Jakub. Notebooky Technologie: TPM - ochrana dat na všech úrovních. In: *Notebook.cz* [online]. 2006 [cit. 2012-04-01]. Dostupné z: http://notebook.cz/clanky/technologie/2006/TPM.

[53] Zámek MicroSaver® ClickSafe. *FUJITSU* [online]. Copyright 1995 - 2012 [cit. 2012-04-01]. Dostupné z: http://www.fujitsu.com/cz/products/computing/pc/accessories/security/kensington-locks/microsaver-clicksafe.html.

[54] Kensington zámok novej generácie ClickSafe TWIN Laptop Lock. *Shark.sk* [online]. 2012 [cit. 2012-04-01]. Dostupné z: http://www.shark.sk/notebooky/prislusenstvo/kensington-zamok-novej-generacie-clicksafe-twin-laptop-lock/.

[55] Uzamykacia stanica bezpečne pripevní ľubovoľný notebook k stolu. *DSL*: *Digitálny svet pod lupou* [online]. 2010 [cit. 2012-04-01]. Dostupné z: http://www.dsl.sk/article.php?article=9503.

[56] Kensington Laptop Locking devices kill some paranoia. *Newlaunches* [online]. 2010 [cit. 2012-04-01]. Dostupné z: http://www.newlaunches.com/archives/kensington_laptop_locking_devices_kill_some_paranoia.php.

[57] KASAL, Jaroslav. Hardwarová ochrana informací - Hardwarový klíč Guardant. In: *PCWorld* [online]. 2003 [cit. 2012-04-02]. Dostupné z: http://pcworld.cz/hardware/hardwarova-ochrana-informaci-hardwarovy-klic-guardant-13433.

[58] Technologies. *Guardant* [online]. 2012 [cit. 2012-04-02]. Dostupné z: http://www.guardant.com/technologies/hardware-encryption/.

[59] Hardwarové klíče Guardant. *MCU*: *web s informace o mikroelektronice* [online]. 2002 [cit. 2012-04-02]. Dostupné z: http://mcu.cz/print.php?news.179.

[60] RIGÁŇOVÁ, Lenka. *Kryptografická ochrana utajovaných informácií*. Zlín, 2010. 60 s. Bakalárska práca. UTB Zlín.

[61] Zákon 215/2002 Z.z.: o elektronickom podpise a o zmene a doplnení niektorých zákonov. 2002.

[62] Aký je rozdiel medzi ZEP a EP ?. *Zaručený elektronický podpis* [online]. 2010 [cit. 2012-04-07]. Dostupné z: http://zarucenyelektronickypodpis.eu/aky-je-rozdiel-medzi-zep-a-ep.

[63] KONRÁD, Roman. Ako som vybavoval zaručený elektronický podpis. In: *SME* [online]. 2009 [cit. 2012-04-07]. Dostupné z: http://romankonrad.blog.sme.sk/c/203566/Ako-som-vybavoval-zaruceny-elektronicky-podpis.html.

[64] Elektronický podpis. *Národný bezpečnostný úrad* [online]. 2011 [cit. 2012-04-07]. Dostupné z: http://www.nbusr.sk/sk/elektronicky-podpis/index.html.

[65] What is SSL?. *SSL.com* [online]. 2011 [cit. 2012-04-10]. Dostupné z: http://info.ssl.com/article.aspx?id=10241.

[66] Sociálne siete. In: *Bezpečný internet* [online]. 2012 [cit. 2012-04-11]. Dostupné z: http://www.bezpecnyinternet.sk/socialne-siete.

[67] Facebook a Pokec sú najpopulárnejšie sociálne siete na Slovensku. In: *EurActiv.sk* [online]. 2012 [cit. 2012-04-11]. Dostupné z: http://www.euractiv.sk/informacna-spolocnost/clanok/facebook-a-pokec-su-najpopularnejsie-socialne-siete-na-slovensku-018910.

[68] EÚ varuje: Sociálne siete ohrozujú mladistvých. In: *EurActiv.sk* [online]. 2010 [cit. 2012-04-11]. Dostupné z: http://www.euractiv.sk/informacna-spolocnost/clanok/eu-varuje-socialne-siete-ohrozuju-mladistvych-014498.

[69] KYŠKA, Roland. *Všetci sme nahí na facebooku*. Český Těšín: Těšinské papírny, s. r. o., 2010, 147 s. ISBN 978-80-89359-24-0.

[70] KIRKPATRICK, David. *Facebook efekt*: *Skutočný príbeh spoločnosti, ktorá spája svet*. Edita Horváthová. Bratislava: Eastone Books, 2011, 326 s. ISBN 970-80-8109-188-9. Z anglického originálu David Kirkpatrick: The Facebook Effect, vydaného vydavateľstvom Simon & Schuster v roku 2010.

[71] ZPOPLATNĚNÍ FACEBOOKU. *HOAX* [online]. 2011 [cit. 2012-04-18]. Dostupné z: http://www.hoax.cz/hoax/zpoplatneni-facebooku/.

[72] Phishingový e-mail. *Slovenská technická univerzita v Bratislave*: *Fakulta elektrotechniky a informatiky*[online]. 2009 [cit. 2012-04-18]. Dostupné z: http://www.fei.stuba.sk/generate_page.php?page_id=2591.

[73] Comodo Firewall. *COMODO* [online]. 2012 [cit. 2012-04-18]. Dostupné z: http://www.comodo.com.

[74] Kerio Control. *KERIO* [online]. 2012 [cit. 2012-04-18]. Dostupné z: http://www.kerio.cz/cz/control/utm.

[75] Najlepšie Antivirus 2012. *Best Antivirus 2012* [online]. 2012 [cit. 2012-04-20]. Dostupné z: http://www.bestantivirus2012.com/sk/.

[76] NOD32 Antivirus 5. *ESET* [online]. © 1992 – 2012 [cit. 2012-04-20]. Dostupné z: http://www.eset.com/sk/produkty/eset-nod32-antivirus/.

[77] Norton Internet Security: Antivirus, Antispam. *NORTON* [online]. ©1995 - 2012 [cit. 2012-04-20]. Dostupné z: http://us.norton.com/internet-security.

[78] TrueCrypt: šifrování pevných i přenosných disků. *EXTRA Windows* [online]. 2008 [cit. 2012-04-24]. Dostupné z: http://extrawindows.cnews.cz/truecrypt-sifrovani-pevnych-i-prenosnych-disku.

[79] Šifrujeme údaje na disku: TrueCrypt. *Inet*: *internetový denník* [online]. 2009 [cit. 2012-04-24]. Dostupné z: http://www.inet.sk/clanok/6978-sifrujeme-udaje-na-disku-truecrypt/.

[80] Free Antivirus Online Scanner. *ESET* [online]. Copyright © 1992-2011 [cit. 2012-04-25]. Dostupné z: http://www.eset.co.uk/Antivirus-Utilities/Online-Scanner.

[81] Virus radar on-line. *ESET* [online]. 2012 [cit. 2012-04-25]. Dostupné z: http://virovyradar.seznam.cz/index_c168h.html.

[82] ŠIMOVEC, Martin. Sociálna sieť môže ľuďom poriadne znepríjemniť život. *TRENČIANSKE NOVINY*. 2011, roč. 52, č. 10.

[83] Login to Your PC by Simply Looking at It!. *LUXAND* [online]. © 2005-2012 [cit. 2012-04-29]. Dostupné z: http://www.luxand.com/blink/.

[84] Záloha dát. *ZÁLOHA DÁT*: *Vaše údaje majú nenahraditeľnú hodnotu.* [online]. 2011 [cit. 2012-04-29]. Dostupné z: http://www.zaloha-dat.sk/.

[85] SAVITZ, Eric. 2012 Data Security Trends: A Look At The Risks Ahead. *Forbes* [online]. 2012 [cit. 2012-04-29]. Dostupné z: http://www.forbes.com/sites/ericsavitz/2012/01/16/2012-data-security-trends-a-look-at-the-risks-ahead/.

[86] Kam se systémem a daty? RAID. DOČEKAL, Michal. *Linuxexpres* [online]. 2009 [cit. 2012-04-29]. Dostupné z: http://www.linuxexpres.cz/praxe/sprava-linuxoveho-serveru-raid-teoreticky.

[87] BALÁŽ, Ondrej. Čo je to virtualizácia?. *V-PORTAL*: *Portál o virtualizácií a všetkom, čo s tým súvisí.* [online]. 2012 [cit. 2012-05-04]. Dostupné z: http://www.v-portal.sk/2011/01/co-je-to-virtualizacia/.

[88] VOJSOVIČ, Dušan. *Porovnanie výkonnosti virtualizačných softvérových produktov*. Trenčín, 2012. Bakalárska. Trenčianska Univerzita Alexandra Dubčeka v Trenčíne, Fakulta Mechatroniky.

[89] Windows 8 budou hotové první týden v červnu, potvrdil Microsoft. *Novinky* [online]. 2012 [cit. 2012-05-04]. Dostupné z: http://www.novinky.cz/internet-a-pc/software/266251-windows-8-budou-hotove-prvni-tyden-v-cervnu-potvrdil-microsoft.html.

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

BSA	Business Software Alliance.
CD	Compact Disc.
DDos	Distributed Denial of Service.
DNS	Domain Name System.
DVD	Digital Versatile Disc.
EP	Elektronický podpis.
EU	Európska únia.
FTP	File Transfer Protocol.
HP	Hewlett Packard.
HTTP	Hypertext Transfer Protocol.
HTTPS	Hypertext Transfer Protocol Secure.
HW	Hardware.
IP	Internet Protocol.
MITM	Mman-Nn-tThe-Middle.
MMS	Multimedia Message Service.
MS	Microsoft.
NV	Nastavenie vstupov.
OS	Operačný systém.
OTK	Overenie totožnosti kľúčom.
PDA	Personal Digital Assistant.
PIN	Personal Identification Number.
P2P	Peer-to-Peer.
RAM	Random Access Memory.
RPN	Register Platformy Nastavení.

RSS Really Simple Syndication.

SMS Short Message Service.

SRI Stanford Rearch Institute.

SSL Secure Sockets Layer.

SW Software.

TPM Trusted Platform Module.

TSR Terminate and Stay Resident.

USB Universal Serial Bus.

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK