ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA EKONOMICKÁ

Bakalářská práce

Vývoj a užití kryptografie a kryptoanalýzy v elektronickém podnikání

Development and application of cryptography and cryptoanalysis in the electronical business

Marek Dyršmíd

PLZEŇ 2014

Čestné prohlášení

Prohlašuji, že jsem bakalářskou práci na téma

„Vývoj a užití kryptografie a kryptoanalýzy v elektronickém podnikání“

vypracoval samostatně pod odborným dohledem vedoucího bakalářské práce za použití pramenů uvedených v přiložené bibliografii.

V Plzni, dne 22.04.2014

.....

Marek Dyršmíd

Poděkování

Děkuji vedoucímu bakalářské práce RNDr. Mikuláši Gangurovi, Ph.D., za jeho cenné připomínky a čas, který mi při řešení dané problematiky věnoval.

Obsah

Úvod

Elektronické podnikání v dnešní době neznamená pouze nákup a prodej zboží a služeb přes internet. Tento obor čítá mnohá další zaměření, bez kterých by dnes velké korporace, firmy i jednotliví živnostníci nebyli schopni na trhu fungovat. Jelikož elektronické podnikání probíhá ve formě elektronického přenosu informací po různých druzích sítí a internetu, je také vystaveno bezpečnostním rizikům, která tyto sítě přinášejí. Tato rizika dala prostor propojení elektronického podnikání s oblastmi zabezpečení elektronických přenosů informací a sítí obecně.

Cílem této bakalářské práce je poskytnutí informací o bezpečnostních hrozbách elektronického podnikání, bezpečnostních hrozbách provozu na síti a možnostech zabezpečení tohoto provozu; dále pak zjištění míry povědomí o možnostech zabezpečení provozu na síti mezi běžnými uživateli. Dílčími cíli práce jsou:

- popis historie a vývoje kryptografie a kryptoanalýzy
- popis bezpečnostních hrozeb a rizik provozu na síti
- vytvoření uceleného přehledu možností zabezpečení provozu běžných uživatelů na síti
- zpracování výzkumu zaměřeného na úroveň povědomí běžných uživatelů sítě o možnostech jejich zabezpečení
- vyhodnocení výzkumu a prezentace výsledků

Z cílů práce je patrné, že se autor zaměřuje hlavně na obecné uživatele sítě, nikoli firmy a korporace. Získání informací o zabezpečení provozu na síti z podniků je možné pouze při vypracovávání BP pro účely podniku. Z tohoto důvodu se autor práce rozhodl zaměřit na běžné uživatele sítě, internetu, kteří jsou samozřejmě do koloběhu elektronického podnikání také začleněni a jsou klíčovou cílovou skupinou z hlediska elektronicky realizovaných obchodů. V jistých případech i oni provozují vlastní druhy elektronické komerce na internetu. Častěji však tito uživatelé využívají webové stránky korporací, firem a různých poskytovatelů zboží a služeb na internetu, e-shopy, kterým poskytují své osobní a další citlivé údaje. Samozřejmě také hojně komunikují. Povaha jejich komunikace může být jak soukromá, tak i pracovní a v těchto chvílích se vystavují bezpečnostním rizikům na síti.

Práce je rozdělena do osmi samostatných kapitol. První kapitola poskytuje obecné informace o elektronickém podnikání, vymezuje přesně jeho součásti a poukazuje na důležitost definování Nové ekonomiky. Druhá kapitola se zaměřuje na historii a vývoj kryptografie a kryptoanalýzy. Pojednává o historických milnících těchto oborů a definuje důležité pojmy pro pochopení dalších částí práce. Ve třetí kapitole jsou popsány moderní šifrovací algoritmy. Především je zde popsán zásadní rozdíl mezi symetrickým a asymetrickým šifrovacím systém. Čtvrtá kapitola již pojednává o konkrétních způsobech využití kryptografie v elektronickém podnikání. Popisuje elektronický podpis, elektronický certifikát a možnosti získání certifikátů od certifikačních autorit. V následující páté kapitole jsou popsány hlavní bezpečnostní rizika provozu na nezabezpečené síti a internetu. Jsou zde hlouběji popsány typy útoků na uživatelské stanice a také škodlivý software. Šestá kapitola zobrazuje možnosti zabezpečení provozu na síti pro běžné uživatele. Obsahuje hlavní bezpečnostní zásady chování, které by měli uživatelé počítačů na síti dodržovat, a dále popisuje softwarové možnosti zabezpečení počítače. Sedmá kapitola je již zaměřena úzce na možnost zašifrování e-mailové komunikace mezi dvěma uživateli. Konkrétně je zde uveden i dostupný software pro toto využití a rámcově je popsána jeho funkcionalita. V kapitole je poté odkaz na velmi podrobný a přehledný manuál pro zašifrování e-mailové komunikace. Závěrečná osmá kapitola je popisem dotazníkového šetření, jehož hlavním účelem je zjistit míru povědomí běžných uživatelů počítačů o možnostech zabezpečení jejich provozu a úroveň již využívaného zabezpečení. Jsou zde k dispozici přehledné grafy s legendami ke všem otázkám šetření a popsány možné závislosti mezi nimi.

1 Elektronické podnikání

1.1 Úvod, definice elektronického podnikání (e-business) a elektronického obchodování (e-commerce)

Obor elektronického podnikání (e-business) prošel velmi rychlým vývojem, obzvlášť v posledních 15 letech. Nejprve byl chápán pouze jako internetové obchody, různé rezervační systémy apod., tedy části, které jsou dnes označovány jako elektronické obchodování (e-commerce). E-business již čítá mnohá další odvětví, jejichž cílem je

zejména zvýšení a podpora efektivity podnikových interních a externích procesů. (Suchánek, 2012, s. 9)

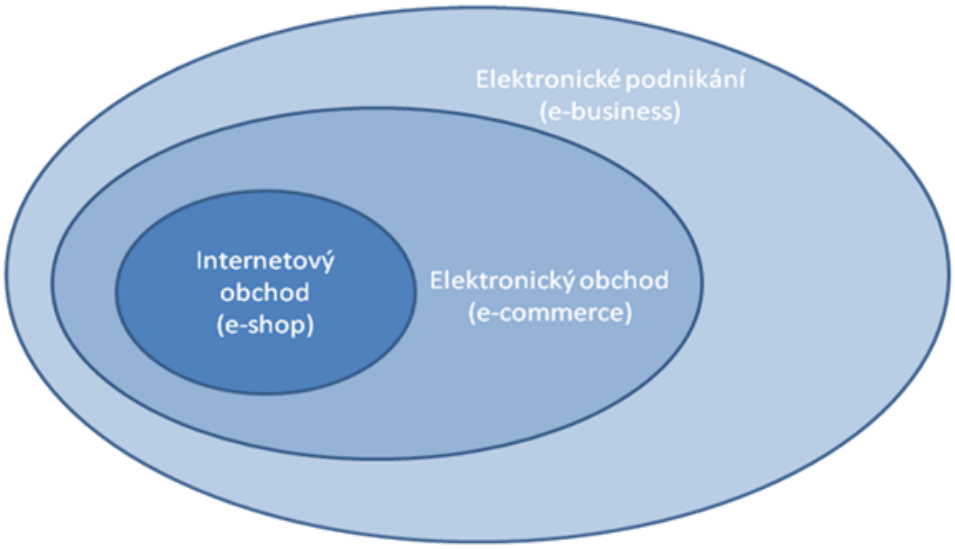
E-business staví na stejnou úroveň jak podniky a firmy, tak i běžné uživatele. Běžní uživatelé jsou velmi významnou cílovou skupinou v elektronicky realizovaných obchodech. Na druhé straně využívají Internet také ke vzdělávacím účelům, zábavě a pracovním potřebám.

Elektronické podnikání můžeme definovat následovně: „Elektronické podnikání znamená využití informačních a komunikačních technologií (ICT) ke zvýšení efektivnosti vztahů mezi podniky i mezi jednotlivými uživateli.“ (Suchánek, 2008, s. 26)

Elektronické obchodování můžeme definovat následovně: „Elektronický obchod je obchodem, při kterém komunikace mezi jeho účastníky probíhá zčásti nebo zcela pomocí počítačových sítí, jejich příslušenství a telekomunikací (elektronických informačních a komunikačních technologií)“. (Suchánek, 2008, s. 26)

Je tedy zřejmé, že e-business je vrcholem pomyslné hierarchie podnikatelských aktivit realizovaných s využitím ICT. Vezmeme-li pouze obchodní aktivity, hovoříme již výhradně o e-commerce, v rámci kterého jsou jedním z hlavních komunikačních rozhraní internetové obchody (e-shopy) reprezentované již přesnými webovými aplikacemi.

Obr. č. 1: *Části elektronického podnikání*



Pramen: Suchánek, 2012

Shrnutím uvedených skutečností můžeme konstatovat, že e-business obsahuje veškeré výrobní a obchodní aktivity včetně všech provozních a technicko-správních činností a e-commerce zahrnuje aktivity orientované na nákup/prodej zboží nebo služeb jednotlivými kupujícími/prodávajícími v rámci dodavatelsko-odběratelského řetězce.

1.2 Druhy elektronického podnikání podle subjektů

Základní druhy e-business rozlišujeme podle vzájemných vztahů mezi jednotlivými subjekty. Těmi mohou být firmy a podniky, zákazníci (široká veřejnost) nebo orgány státní správy.

Podle vzájemných vztahů mezi subjekty rozeznáváme následující druhy elektronického podnikání:

- B2C (Business to Customer) – obchodování mezi firmou a konečným zákazníkem (koncovým spotřebitelem)
    - Obsahuje přímý prodej koncovým zákazníkům. Službou B2C je snaha informovat o produktech, webové prezentace zde plní funkci papírových letáků a katalogů. Nejvyšším stupněm B2C je samotný e-shop, který splní funkci prezentační a realizuje i obchodní transakci s možností zaplacení za zboží či služby.

- B2B (Business to Business) – obchodování mezi dvěma firmami, například mezi firmou a jejím dodavatelem a odběratelem, kterým je také firma
    - B2B vztahy fungují většinou na principu elektronické výměny dat, jako jsou například objednávky, faktury, reklamační protokoly apod. Složitější B2B systémy zvládají i regulaci již nastavených obchodních vztahů, řízení kvality dodávek a standardizaci formátu předávaných dat s mezinárodní použitelností.
- B2G (Business to Government) – obchodní a komunikační vztahy s úřady a orgány státní správy
    - B2G vztahy zahrnují nabídky produktů institucím státní správy a také veškerou komunikaci s úřady. Příkladem je již fungující možnost podání daňového přiznání s využitím elektronického podpisu nebo používání datové schránky pro podnikatele.
- B2E (Business to Employe) – vztahy mezi podnikající firmou a jejími zaměstnanci
    - B2E vztahy zahrnují přenos například sdílených informací pro zaměstnance (rozvrh směn, potřebná příprava na určitou činnost apod.) Dále mohou zahrnovat třeba firemní sdělení o úpravě pracovních podmínek, zveřejňování firemních novin apod.
- B2R (Business to Sales Representative) – obchodní vztahy a komunikace mezi firmou a jejími obchodními zástupci
    - B2R zahrnuje většinou vzájemnou výměnu strukturovaných dat. Využívají se zejména různé formy extranetu.
- C2C (Customer to Customer) – vztahy mezi spotřebiteli navzájem
    - Obchodní operace na internetu, jako například inzertní služby, aukční portály, bazary apod. V tomto vztahu nevystupuje jako prodávající podnik, proto C2C nebývá považováno za druh elektronického podnikání. Avšak pro účely této práce je důležité tento vztah znát.

(Zdroj: upraveno a doplněno (Chromý, 2013, s. 120, 121)

1.3 Nová ekonomika

E-business se začal hlouběji rozvíjet hlavně díky potřebám tzv. nové ekonomiky. Nová ekonomika je také nazývána ekonomikou znalostí, kde základním prvkem tvorby nových příležitostí a zvýšení životní úrovně jsou inovativní nápady, technologie integrovaná do výrobků a služeb a kde je kladen důraz především na celoživotní vzdělávání a osobní rozvoj, a to v co nejvíce oblastech.

1.3.1 Hlavní rozdíly staré a nové ekonomiky

Stará ekonomika poskytuje možnost relativně snadného předvídání vývoje a určitou stabilitu práce a podnikání. Nová ekonomika se vyznačuje značnou nestabilitou práce a podnikání, jelikož je založena na schopnostech inovovat a neustále zdokonalovat.

Následující tabulka zobrazuje rozdíly mezi starou a novou ekonomikou v různých pohledech.

Tabulka č. 1: *Přehled nejdůležitějších odlišností staré a nové ekonomiky*

Oblast	Stará ekonomika	Nová ekonomika
Ekonomické charakteristiky		
Trhy	Stabilní	Dynamické
Konkurence	Národní	Globální
Forma organizace	Hierarchická, byrokratická	Propojená, síťová
Průmysl		
Organizace výroby	Masová výroba	Flexibilní produkce
Klíčové motory růstu	Kapitál/práce	Inovace/znalosti
Klíčová technologie	Mechanizace	Digitalizace
Zdroj konkurenční výhody	Snižování nákladů formou úspor z rozsahu	Inovace, kvalita, doba dodání na trh, náklady
Význam výzkumu/inovací	Nízký-střední	Vysoký
Vztahy s ostatními firmami	Jít za cílem sám	Aliance a spolupráce
Pracovní síla		
Cíl politiky	Plná zaměstnanost	Vyšší skutečné mzdy
Schopnosti	Odvozené od povolání	Široce orientované, napříč odvětvím
Požadované vzdělání	Vyučení nebo VŠ titul	Celoživotní vzdělávání
Vztahy – zaměstnanci-management	Odporující si	Spolupráce
Povaha zaměstnání	Stabilní	Poznamenaná rizikem a příležitostmi
Vláda		
Vztahy firmy-vláda	Uvalení požadavků	Podporovat příležitosti růstu
Regulace	Přikazuj a kontroluj	Tržní nástroje, flexibilita

Pramen: Atkinson, 1998

Současné informační systémy a technologie jsou tedy základem tzv. nové ekonomiky, kde informační produkty a služby se stávají rozhodujícím obchodním artiklem. Zásadní změny ekonomického a společenského prostředí nové ekonomiky vytvářejí tlak na změny informačních systémů a principů elektronického podnikání. Hlavní rozvoj elektronického podnikání přišel se změnami ekonomického prostředí do nové ekonomiky.

2 Historie a vývoj kryptografie a kryptoanalýzy

2.1 Úvod do kryptologie

Kryptologie je samostatná vědní disciplína, která se dělí na kryptografii a kryptoanalýzu a někdy se také uvádí, že zahrnuje steganografii (skrývání zpráv). Je vědou o informační celistvosti a zahrnuje tvorbu kryptografických technik (kryptografických algoritmů, kryptografických protokolů, hashovacích funkcí, kryptoanalytických útoků apod.), určení podmínek jejich praktického využívání a zkoumání odolnosti kryptografických algoritmů proti kryptoanalytickým útokům. Vychází z rozsáhlého matematického aparátu, propracované teorie informací, teorie složitosti, teorie čísel a teorie pravděpodobnosti. Je to věda velice stará, avšak významné a pro dnešní dobu přínosné algoritmy jsou produktem teprve 20. a 21. století. Kryptologie má širokou oblast využití, vedle klasických využití ve vojenství, diplomacii a špionáži se s jejími produkty setkáváme velice často v civilním prostředí. Příkladem mohou být elektronické bankovní převody, komprimace a zašifrování souborů, ochrana dat na síti, ochrana firemních tajemství, zabezpečení elektronických zpráv atd. (Zelenka, Čapek, Francek, Janáková, 2003, s. 12)

Kryptologie je vědou neustálého pokroku, již od jejích počátků se vede neustálý boj mezi kryptografy, kteří se snaží stále vylepšovat šifrovací algoritmy a učinit je tak neprolomitelnými a mezi kryptoanalytiky, kteří se neustále snaží ony algoritmy napadat a znehodnocovat. Každý šifrovací algoritmus má smysl pouze do té doby, nežli je účinným útokem prolomen. V takovém případě ho již nemá smysl využívat, častěji se z něj ale vyvine nová zlepšená varianta, proti které účinný útok zatím neexistuje.

2.2 Kryptografie a kryptoanalýza

2.2.1 Starověká kryptografie

Historie vědy o tvorbě šifer sahá hluboko do historie lidstva. Zpočátku bylo šifrování doménou pouze diplomatických kruhů, vojenských a špionážních služeb a sloužilo tak při rozhodování v mimořádně důležitých věcech.

První pokusy o utajení obsahu zpráv jsou již ze starověkého Egypta, Mezopotámie a Indie. Jednalo se o základní úpravy tehdejšího „písma“ přidáváním různých znaků známých pouze určitým osobám nebo tzv. pečetní válečky pro ověřování pravosti zpráv.

V této době se spíše využívalo skrývání zpráv (steganografie), nežli účinného šifrování. Římané prokazatelně zavedli vojenskou kryptografii kolem roku 0 našeho letopočtu. Zprávy mezi legiemi byly rozesílány pomocí záměny otevřeného textu za šifrovaný text. Každé písmeno zprávy bylo zaměněno za písmeno, které leželo o 3 místa dále v abecedě, tzv. jednoduchá Césarova šifra. (Zelenka, Čapek, Francek, Janáková, 2003, s. 21)

2.2.2 Středověká kryptografie a kryptoanalýza

Kryptografie systematicky rozvíjená se základy v matematických vědách vznikla hlavně díky vynikajícím arabským matematikům. Abú Bakr Ahmad roku 855 našeho letopočtu ve své práci popsal různé substituční šifrovací systémy. Právě jedna z popisovaných metod se v arabském světě používala beze změny ještě v roce 1775. Na práce arabských matematiků navázali představitelé kryptografie středověké Evropy. Významným představitelem byl benediktinský opat Johanes Trittheim. Ten kolem roku 1500 napsal první významnější evropskou knihu o šifrování. Zabýval se z velké části hlavně substitučními systémy, ve kterých byly náhodně vloženy znaky do textu za účelem ztížení statistického rozboru. I proto jej panovnické rody, které využívaly této šifry běžně pro komunikaci, označily za čarodějníka. Bály se, že jeho kniha vyzradila příliš mnoho detailů o substituční šifře. (Zelenka, Čapek, Francek, Janáková, 2003, s. 22)

Počátkem 16. století se také objevili první slavní kryptoanalytici. Jedním z nejslavnějších byl francouzský právník a matematik Francois Viete, který luštil zašifrované depeše španělského krále a předával je francouzskému panovníkovi Jindřichu IV. Navvarskému. Úspěšná kryptoanalýza (ale naopak i kvalitní neprolomené kryptografické šifry) pak začala stále více ovlivňovat dějiny. (Zelenka, Čapek, Francek, Janáková, 2003, s. 22)

2.2.3 Kryptografie a kryptoanalýza dvacátého století

Dynamický rozvoj kryptografie a různých šifrovacích strojů nastal počátkem 20. století v první světové válce a byl způsoben zavedením telegrafu. Telegrafická komunikace měla vlastnost snadného odposlechu, a proto bylo nutné vyvíjet jednoduché a bezpečné systémy šifrování. (Dobda, 1998, s. 198)

V tomto období se ukázala naplno veliká síla kryptoanalytiků. USA po vstupu do války vyluštily obsah šifrovaného telegramu – dnes známého jako tzv. Zimmermannův

telegram. První světová válka dala vyniknout také prvního velikána kryptologie dvacátého století – Williama Frederica Friedmana. Jeho čtyřsvazkové dílo „Základy kryptoanalýzy“ z roku 1923 se stalo opravdovou biblí všech kryptologů první poloviny dvacátého století. Tato kniha zásadně ovlivnila rozvoj kryptologie mezi dvěma světovými válkami ve všech zemích světa. S nadsázkou se dá říci, že díky této knize se znalosti na všech frontách vyrovnaly. Záhy vývoj kryptologie doplnil rozvoj techniky a začaly vznikat mechanické šifrovací stroje. Ten světu naprosto nejznámější vznikl ve 30. letech v Německu. Je jím mechanické šifrovací zařízení Enigma. (Zelenka, Čapek, Francek, Janáková, 2003, s. 23)

I ostatní země chystající se na druhou světovou válku vynakládaly značné množství prostředků na tvorbu šifrovacích zařízení. Druhá světová válka prověřila kvalitu přichystaných šifrovacích mechanizmů a ukázala, že většinu z nich se protistranám podařilo rozluštit. V tomto období měli navrch kryptoanalytici nad kryptografy.

Pro luštění šifer sestrojil Alan Turing jeden z prvních elektronických počítačů zvaný Colossus. Byl sestrojen pouze pro kryptoanalýzu Enigmy. Do konce druhé světové války patřila kryptografie k nejvíce střeženým státním tajemstvím na celém světě. Využívaly ji jen diplomatické a špionážní služby a armáda. Tato situace se začala zásadně měnit s příchodem informačních technologií a elektronické komunikace. Kryptografie se stává veřejně dostupnou službou, která zajišťuje důvěru k informacím. Vznikla řada šifer pro využití v bankovním sektoru, průmyslu a v informačních systémech. Společnost IBM na konci sedmdesátých let vyvinula dnes nejznámější symetrický šifrovací algoritmus DES *(Data Encryption Standard)*. Zásadním mezníkem, který přenesl šifrování do veřejné sféry, byl objev kryptosystému s veřejným klíčem, uskutečněný Diffiem a Hellmanem v roce 1976. Od tohoto okamžiku se začínají kryptosystémy dělit na symetrické a asymetrické. (Dobda, 1998, s. 198)

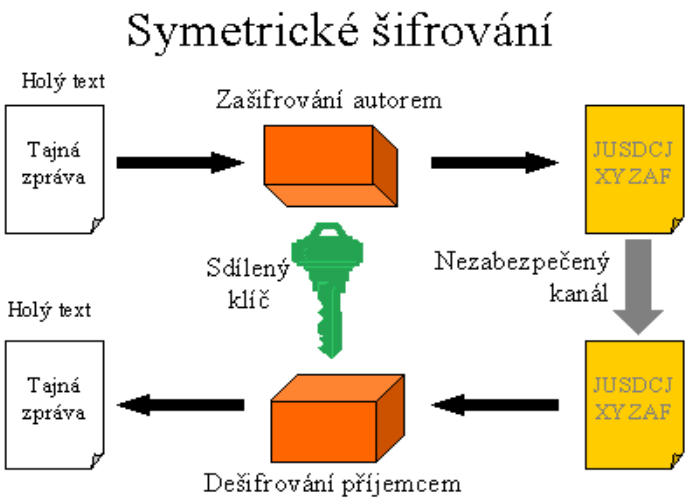
3 Moderní šifrovací algoritmy

Moderní šifrovací algoritmy využívají velké množství matematických postupů a přístupů. Volba konkrétního postupu souvisí nejčastěji s účelem, pro který je šifrovací algoritmus používán, s aspekty požadovaného stupně bezpečnosti, rychlosti komunikace a šifrování a s různými právními aspekty (patentové ochrany apod.). (Zelenka, Čapek, Francek, Janáková, 2003, s. 63)

3.1 Symetrický šifrovací systém

Symetrický se tento systém nazývá proto, že stejný šifrovací klíč používá k šifrování i dešifrování informace. Odesílatel i příjemce tedy mají shodný klíč. Zde nastává problém v přenosu tajného klíče k příjemci zprávy, jelikož se musí doručit bezpečně. V opačném případě se může stát, že padne do nepovolaných rukou a komunikace bude rozluštěna. Při delší době využívání tohoto systému se stále stejným klíčem se zvyšuje riziko, že tento klíč bude odhalen. Z tohoto důvodu se symetrické klíče často obměňují a také proto se nazývají „klíče pro sezení“ *(session)*. Oproti algoritmu nesymetrickému je výrazně rychlejší a používá se proto na velké objemy dat. Nejběžněji používané symetrické šifrovací algoritmy jsou Data Encryption Standard (DES), Rivest Cipher 4 (RC4), International Data Encryption Algorithm (IDEA), Skipjack a další. (Dobda, 1998, s. 207)

Obr. č. 2: *Schéma symetrického šifrovacího systému*



Pramen: http://www.svetsiti.cz/technologie/2003/Krypto/symetrik.gif

3.2 Asymetrický šifrovací systém

Oproti symetrickému šifrovacímu systému se zde využívá dvojice klíčů, kterou si uživatel vygeneruje za pomoci některých z veřejně dostupných aplikací a stane se tak jediným majitelem jednoho z klíčů - soukromého. V případě kdy nelze odvodit jeden klíč z druhého, je asymetrický šifrovací systém nazýván šifrovacím systémem s veřejným klíčem. Systém veřejného klíče je charakteristický tím, že data šifrovaná jedním z klíčů lze v určitém čase dešifrovat pouze se znalostí druhého z dvojice klíčů. První z dvojice klíčů – soukromý klíč (tajný) – je bezpečně ukryt majitelem, zatímco druhý klíč je věrohodně zveřejněn nebo přidělen, odtud název veřejný klíč. (Zelenka, Čapek, Francek, Janáková, 2003, s. 91)

Systém veřejného a soukromého klíče umožňuje v praxi dvě využití:

1) Přenos nešifrované, ale podepsané zprávy

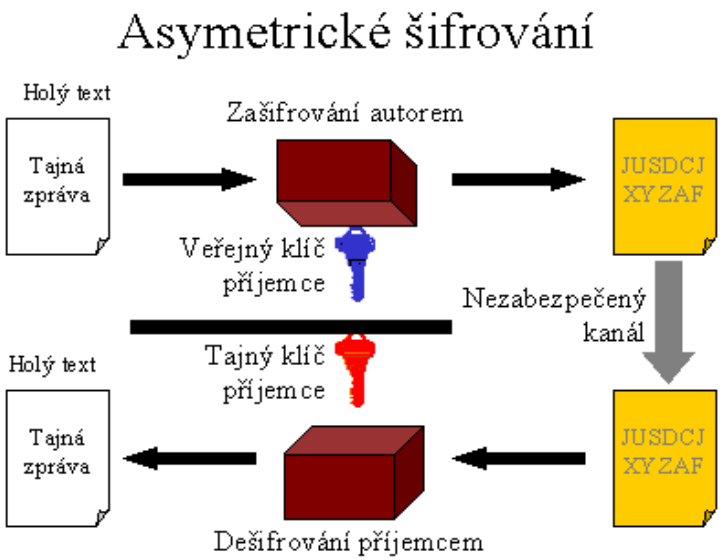
V této variantě využití systému veřejného a soukromého klíče se původní odesílaná zpráva zašifruje soukromým klíčem odesilatele. Zprávu potom dešifruje kdokoli se znalostí veřejného klíče odesilatele, který je však běžně dostupný. Tímto vznikne vlastně nezabezpečená zpráva s možností volného dešifrování, avšak se zárukou, že odesilatel je právě vlastník soukromého klíče. Libovolný příjemce takovéto zprávy tedy snadno ověří pravost jejího odesilatele. Tímto mechanismem se dá zařídit neodmítnutelnost odpovědnosti na straně odesilatele a pokud příjemce odešle podepsané potvrzení o přijetí, tak také na straně příjemce.

2) Přenos šifrované a podepsané zprávy

V tomto způsobu je na odesílanou zprávu použit veřejný klíč příjemce. Příjemce provede dešifrování svým vlastním soukromým klíčem, který zajistí nemožnost přečtení zprávy kýmkoli jiným. Veřejným klíčem příjemce může zašifrovat kdokoli a cokoli, nicméně obsah bude poté srozumitelný pouze vlastníkovi soukromého klíče, patřícího ke klíči veřejnému. Zpráva zašifrovaná veřejným klíčem příjemce je při případném odchycení škůdcem nesrozumitelná a nečitelná. Tento způsob šifrování používají zejména bezpečnostní protokoly (např. SSL - Secure Sockets Layer) v počáteční fázi komunikace, kdy se vyměňují identifikační údaje obou komunikujících stran a probíhají dohody o kryptografickém systému, který bude použit pro celou komunikaci.

Oba tyto způsoby je také možné zkombinovat, což vede k využití komplexního systému pro utajení i podepsání zprávy. Je tak zajištěna důvěryhodnost informací, autentizace odesílatele a neodmítnutelnost odpovědnosti odesílatele. (Zelenka, Čapek, Francek, Janáková, 2003, s. 93)

Obr. č. 3: *Schéma asymetrického šifrovacího systému*



Pramen: http://www.svetsiti.cz/technologie/2003/Krypto/asymetrik.gif

Nejznámějšími a nejpoužívanějšími kryptografické systémy s veřejným klíčem jsou RSA, DSA (Digital Signature Algorithm), ECDSA, D-H (Diffie, Hellman), El Gamal a Pohlig- Hellman.

Nevýhodou kryptografických systémů s veřejným klíčem je jejich výpočetní náročnost a tudíž velmi malá rychlost. Uvádí se, že asymetrické šifrovací systémy jsou obvykle až 1000krát pomalejší než symetrické. V praxi je tedy vhodné tyto dva systémy kombinovat a vytvořit tak hybridní kryptosystém využívající výhod obou podsystémů. V takovém případě se velmi často využívá následující kombinace: Pro zašifrování samotného obsahu zprávy se využije symetrického šifrovacího systému, hlavně pro jeho rychlost. Problém bezpečného přenosu shodného klíče k příjemci zprávy se odstraní použitím asymetrického systému – ten vytvoří jakýsi bezpečně šifrovaný kanál pro přenos klíče symetrického systému. (Zelenka, Čapek, Francek, Janáková, 2003, s. 95)

4 Způsoby použití kryptografie v elektronickém podnikání

Kryptografie v e-business představuje jednu z hlavních a důležitých vlastností jeho zabezpečení. „Bezpečnost je klíčovým prvkem, bez kterého by bylo elektronické podnikání úplně ztraceno, jelikož by nemělo potřebnou důvěru. Bezpečnost se odvíjí nejen od zajištění bezpečného přenosu informací, ale i například od zajištění autentizace uživatelů.“ (Suchánek, 2008, s. 157)

4.1 Elektronický podpis

Elektronický podpis je dnes zcela nezbytným prvkem mnoha systémů. V roce 2000 došlo k vytvoření právní podpory, kdy v platnost vešel zákon č. 227/2000 Sb. O elektronickém podpisu. Dle tohoto zákona je elektronický podpis definován následovně: „Elektronickým podpisem se rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě.“. (Suchánek, 2008, s. 166)

Největším problémem je ověřitelnost elektronického podpisu. Z tohoto důvodu vznikl tzv. digitální podpis, který umožňuje přesnou identifikaci podepsané osoby. Digitální podpis je spojení elektronického podpisu a certifikátu, který je spjat pouze s jeho vlastníkem. K zajištění plné důvěryhodnosti digitálního podpisu je nutné, aby certifikát ověřila nezávislá třetí strana, tzv. certifikační autorita. Princip certifikátů a certifikačních autorit bude vysvětlen v následující kapitole.

Princip elektronického podpisu

Na straně odesílatele se zprvu ze zprávy vytvoří pomocí tzv. hash funkce (transformační funkce – jednosměrný algoritmus) digitální vzorek zprávy (digiset). Jedná se o kryptografický kontrolní součet, který je zhuštěnou reprezentací podepisované informace. Použitý algoritmus musí zajistit, že je výpočetně nezvládnutelné nalézt k danému kontrolnímu součtu odpovídající zprávu nebo nalézt dvě zprávy, které mají stejný kontrolní součet. Nejčastěji se využívá algoritmů MD5 a SHS. (Zelenka, Čapek, Francek, Janáková, 2003, s. 152)

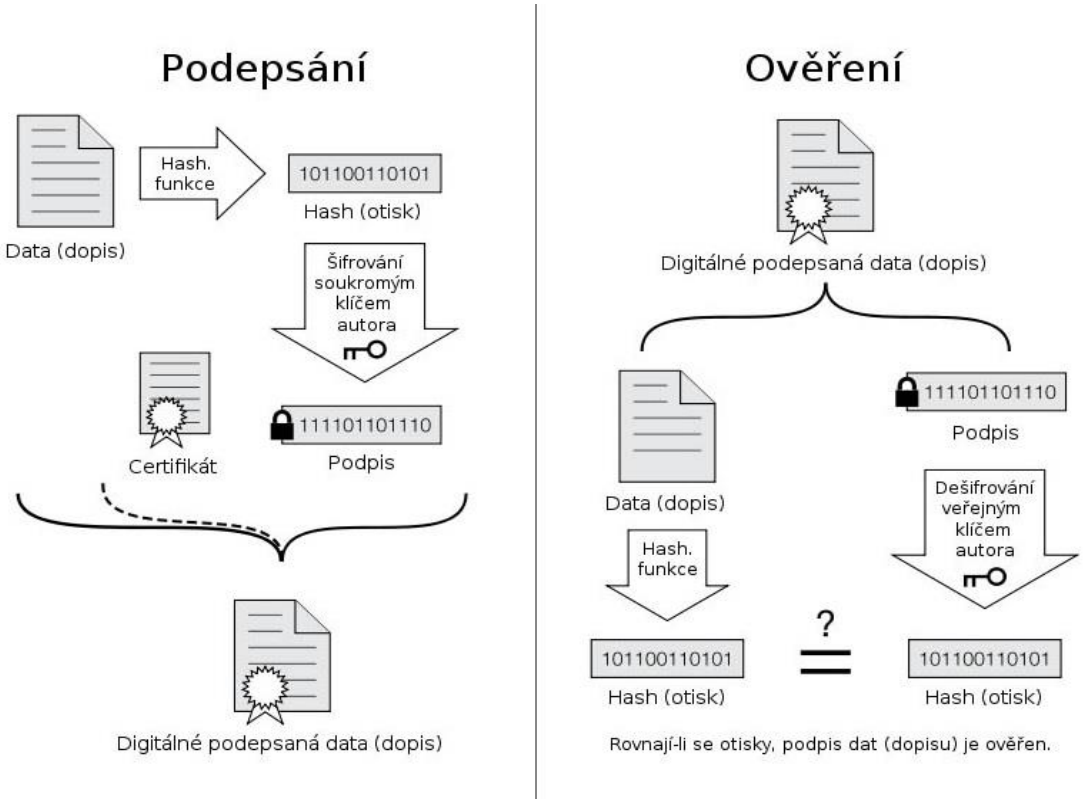
Digiset je pro každou zprávu jednoznačný a nezaměnitelný. Tento vzorek je zašifrován (podepsán) soukromým klíčem odesílatele a přiložen ke zprávě. Dále můžeme zašifrovat celou tuto zprávu veřejným klíčem příjemce a zajistit tak její bezpečný

přenos po síti. Příjemce dešifruje zprávu svým soukromým klíčem a získá obsah zprávy plus její digiset. Ze zprávy vytvoří pomocí stejné hash funkce kontrolní vzorek a ten doručený dešifruje pomocí veřejného klíče odesílatele. Pokud nastane shoda obou kontrolních vzorků, poskytne elektronický podpis příjemci následující:

- *autentizaci*: příjemce dokumentu bezpečně ví, kdo je jeho autorem
- *integritu*: příjemce má jistotu, že obsah zprávy nebyl během přenosu nebo zpracování změněn
- *nepopiratelnost autorství*: autor dokumentu nemůže popřít autorství ani jeho obsah

Digitální podpis je využitelný pro všechny typy dokumentů. Má velký význam například pro firmy a jejich výměnu dat (B2B), také pro živnostníky v komunikaci s úřady státní samosprávy apod. (Suchánek, 2008, s. 170)

Obr. č. 4: *Schéma podepsání a ověření zprávy elektronickým podpisem*



Pramen:http://www.mirecekp.net/wp-content/uploads/2010/08/800px
Digital_Signature_diagram_cs.jpg

Možný problém digitálního podpisu

Možný problém s používáním zaručeného elektronického podpisu je především v tom, že běžný uživatel nemusí mít pro jeho tvorbu prostředky přesně pod svou kontrolou, jak to vyžaduje zákon o elektronickém podpisu. Běžný uživatel obvykle není schopen se svými znalostmi a schopnostmi udržet svůj počítač v takové konfiguraci a úrovni zabezpečení, aby si mohl být jist, že ho má výhradně pod svou kontrolou. Z tohoto hlediska je nutné neustále zvyšovat odbornou způsobilost všech uživatelů výpočetní techniky, jelikož se dá předpokládat, že budou častěji chtít využívat elektronického podpisu jak pro soukromé, tak profesní potřeby. (Suchánek, 2008, s. 172)

4.2 Certifikační autorita

Certifikační autorita (CA) vystupuje při vzájemné komunikaci dvou subjektů jako třetí nezávislý důvěryhodný subjekt, který prostřednictvím jím vydaného certifikátu nevylučitelně sváže identifikaci subjektu s jeho dvojicí klíčů, tedy s elektronickým podpisem. Bez CA bychom mohli tedy získat veřejný klíč podepisovatele zprávy, nicméně bychom mohli být snadno oklamáni a odesílatel by se mohl vydávat za někoho jiného. Elektronický podpis by tedy pozbyl své hlavní podstaty. (Zelenka, Čapek, Francek, Janáková, 2003, s. 154)

Činnost certifikační autority se dá srovnat s činností notáře při ověřování klasického podpisu. Je zde ovšem jedna zásadní odlišnost – zatímco notář musí ověřit každý jednotlivý podpis, certifikační autorita neověřuje samotný fyzický podpis, nýbrž data pro vytvoření digitálního podpisu. Skutečných podpisů potom můžeme pomocí těchto dat vytvořit libovolné množství. CA musí zajistit, že žadatel o certifikát je opravdu vlastníkem dvojice klíčů, ke kterým bude certifikát přiřazen.

Protože digitální podpis se dá pomocí certifikátu vytvářet opakovaně po celou dobu platnosti certifikátu, zakládá se mezi držitelem certifikátu a certifikační autoritou obchodní vztah, který je obvykle opatřen smlouvou. Z této smlouvy vyplývají pro obě strany jisté povinnosti. CA poskytuje na základě smlouvy další servis, jako je například zneplatňování certifikátů a zveřejňování jejich seznamů, vydávání následných certifikátů apod. Držitel certifikátu musí poskytnout certifikační autoritě přesné a pravdivé informace, informovat ji o případných změnách těchto informací, chránit

svůj soukromý klíč a v případě jeho kompromitace požádat CA o zneplatnění certifikátu. (Suchánek, 2008, s. 172)

4.2.1 Struktury certifikačních autorit

Ve světě existují 3 typy certifikačních autorit. Záleží vždy na tom, jakým způsobem je ověřen veřejný klíč dané CA.

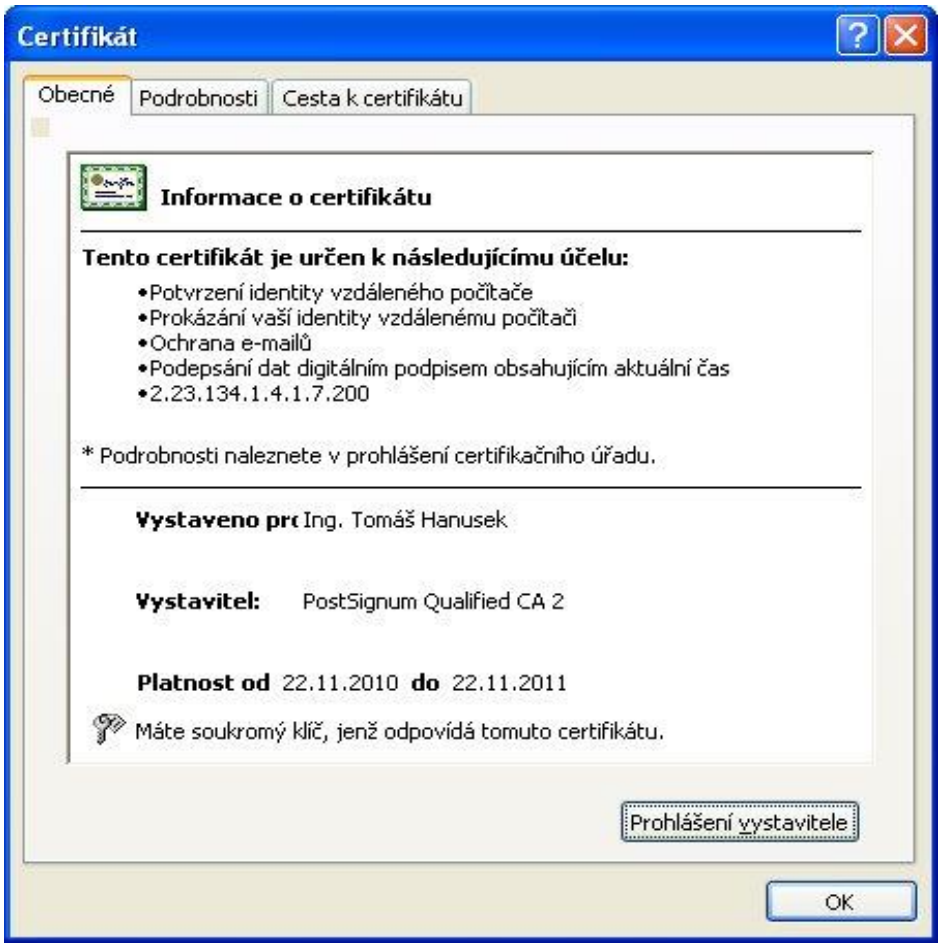
- Samocertifikující se (pseudokořenové) CA – certifikát si tato autorita vydala sama a sama si ho také podepsala. V takovém případě pak musí být veřejný klíč autority ověřitelný z jiného důvěryhodného zdroje (Úřad pro elektronický podpis, publikace ve Zlatých stránkách, bezpečný web státní instituce apod.).
- Křížový certifikát – v tomto případě si dvě CA podepíší své certifikáty navzájem. Stávají se tak navzájem jedna nadřazena druhé a tudíž rovnocenné. Křížový certifikát je výhodný hlavně ve spolupráci dvou firem, kdy zaměstnanci jedné firmy věří své CA a navíc prostřednictvím křížového certifikátu mohou věřit i certifikátům zaměstnanců druhé firmy (obě firmy se na tomto mohou dohodnout i smluvně).
- Třetí možností je, že veřejný klíč jedné certifikační autority podepíše jiná CA. Tato se stává „nadřízenou“ CA a i jí může certifikát podepsat další nadřízená autorita atd. Vzniká tak jakási certifikační cesta nebo strom, který končí u tzv. kořenové autority. Certifikát kořenové autority poté musí být opět ověřitelný podobně, jak bylo popsáno u pseoudokořenové CA. (Zelenka, Čapek, Francek, Janáková, 2003, s. 157)

4.2.2 Proces získání certifikátu od CA

V této podkapitole je popsán celý proces od podání žádosti o certifikát až po jeho vystavení. Uvedený proces se týká nejpoužívanějšího typu certifikátu – osobního. Žadatel o certifikát si nejprve musí vygenerovat dvojici klíčů a vytvořit elektronickou žádost. Generování klíčů je poměrně snadným úkonem. Dají se využít veřejně dostupné softwarové nástroje např. Kleopatra key management tool nebo využít webových aplikací dané CA. Ve značném množství případů poskytují certifikační autority možnost vygenerovat dvojici klíčů skrze jejich webové stránky. Po vygenerování klíčů a odeslání žádosti následuje nejdůležitější fáze - a sice ověření totožnosti žadatele. V některých případech musí žadatel za tímto účelem osobně navštívit sídlo CA nebo síť speciálních

poboček, takzvaných registračních autorit. Registrační autority nevystavují certifikáty, pouze provádějí ověření totožnosti žadatele. Existují i CA, které zvolily jiný přístup k ověřování totožnosti žadatele – po zaregistrování elektronické žádosti o certifikát vystaví písemnou smlouvu, kterou odešlou žadateli. Součástí smlouvy je požadavek o notářské ověření totožnosti žadatele a poté se smlouva odešla zpět certifikační autoritě. Samotný certifikát se po vystavení předává např. elektronickou poštou, fyzicky na přenosném datovém médiu, případně je ke stažení z webu CA. (Suchánek, 2008, s. 174)

Obr. č. 5: *Ukázka digitálního certifikátu*



Pramen: http://www.openoffice.cz/uploads/gallery/full/2360.jpg

4.2.3 Významné české certifikační autority

Zde jsou uvedeny některé významné české certifikační autority, jako jsou:

- Certifikační autorita Czechia
- Certifikační autorita TrustPort

- Certifikační autorita Globe Internet
- Certifikační autorita KPNQwest Czechia
- První certifikační autorita

Některé CA poskytují možnost vyzkoušení si fungování digitálního podpisu, tzv. testovací certifikáty. Pro nezkušené uživatele je to jistě vhodná cesta, jak získat dostatek zkušeností s používáním digitálního podpisu, než si zajistí oficiální verzi.

5 Bezpečnostní rizika provozu na síti

S rychlým vývojem digitálních technologii a přesunem důležitých služeb do prostředí počítačů se stává zabezpečení provozu na síti nedílnou součástí elektronické výměny dat. Uživatelé denně využívají internet k platebnímu styku, nákupu zboží všeho druhu a mnoha dalším službám, kde se využívá nejen jejich peněz, ale také osobních údajů. Dnešní fenomén být „on-line“ kdekoli a kdykoli se týká samozřejmě i velkých společností, pro které je strategie připojení k internetu kritickou částí, zaručující úspěšnost ve světě obchodu.

Označení síťová bezpečnost je v dnešní době již velmi široký pojem. V dřívějších dobách postačovalo, pokud měl administrátor obecný přehled o bezpečnostních rizicích, aby úspěšně ochránil síť. Dnes je situace diametrálně odlišná. Zakládají se komunity a organizace profesionálů, kteří vytváří předpoklady pro zajištění odpovídající bezpečnosti.

Firmy a podniky vytvářejí speciální oddělení pouze pro odborníky přes počítačovou bezpečnost, kteří neustále sledují nové trendy a možnosti a upravují zabezpečení firemních systémů a sítí. Jejich cílem je vždy být o krok napřed před nebezpečím, kterým uživatelé vědomě či nevědomě jsou. (Petrovič, Kostěnec, 2012)

5.1 Druhy útoků

Obecně lze síťové útoky klasifikovat na:

- útoky mapující síťové prostředí
- snahu o získání přístupu do systému
- útoky odmítnutí služby

Konkrétněji se jedná o viry, červy, trojské koně, dále o různé techniky sociálního inženýrství, útoky přes webové stránky a další. Většinou spolu souvisejí a to tak, že jeden předchází druhému do té doby, dokud útočník nedocílí svého původního záměru.

5.1.1 Průzkum sítě

Tento typ útoku slouží k neautorizovanému sbírání informací, mapování zařízení, systémů, služeb a všech potenciálně zranitelných míst v síti. Útočník nejprve zjišťuje, které IP adresy jsou dostupné, a následně hledá otevřené porty. V konečné fázi zjišťuje,

jaké služby naslouchají na otevřených portech a zda je jejich verze potenciálně zranitelná. V případě, kdy je průzkumný útok veden správně, je velmi složité jej odhalit. Pro jeho provedení se používá následujících nástrojů:

- **hromadné použití systémové utility ping (ping sweeps)**

  Tento nástroj je nejjednodušší technikou jak zjistit, které počítače jsou v síti aktivní. Hromadně se spustí příkaz ping a útočník tak může zmapovat potenciální cíle útoku. Účinnou obranou proti tomuto mechanismu je zákaz odpovědi na příkaz ping na firewallu (tento nástroj bude popsán později). Pokud můžeme na firewallu vybírat z akcí aplikovaných na kontrolovaný provoz, musíme rozlišit akce REJECT a DROP. Akce REJECT sice zapříčiní zahození paketu, nicméně odešle zprávu o nedostupnosti. Akce DROP paket také zahodí, nicméně oproti REJECT nezasílá útočníkovi informaci o nedostupnosti služby.

- **odchytávání paketů (packet sniffer)**

  Pro odchytávání paketů se používají programy, které využívají síťové karty v režimu, kdy posílají všechny přijaté pakety aplikaci na zpravování, včetně těch, které ji nejsou určené. Některé protokoly posílají hesla v nezabezpečené formě a je tedy velmi snadné je odchytit. Mezi nejznámější nástroje patří Wireshark, Tcpdump, Dsniff a další.

- **skenování portů (port scanners)**

  Tato metoda zjišťuje otevřené porty na vzdáleném počítači v síti a jejím cílem je zjistit seznam služeb, které jsou na daném počítači a otevřeném portu spuštěny. Existují desítky nástrojů na skenování portů. Jedním z nejznámějších je Nmap.

- **získávání informací zadaných při registraci IP podsítí, zařízení apod. (Internet information queries)**

  Díky těmto informacím může útočník získat přehled o tom, kdo server poskytuje, jaký má adresní rozsah, jaká je adresa DNS serveru a velké množství dalších informací. Aplikace zprostředkující tento obsah z veřejné databáze je dostupná i přes web a nazývá se Whois. (Petrovič, Kostěnec, 2012)

5.1.2 Získání přístupu

Získáním přístupu k zařízení může útočník získat citlivá data a také zařízení využít k dalším potenciálním útokům nebo šíření nevyžádaných zpráv. Nejčastější metodou získání přístupu je útok na heslo. Provádí se několika způsoby a to například tradičním útokem hrubou silou, použitím škodlivého softwaru nebo odchytnutí hesla v nezabezpečené podobě (POP3, Telnet, webové ověřování).

Lámání přístupového hesla je omezeno rychlostí interakce vzdáleného napadaného systému. Systémy lze chránit proti těmto útokům například prodloužením časového intervalu mezi špatně vloženými hesly nebo dočasným uzamknutím účtu uživatele. V první fázi tohoto útoku se zkouší slovník slov nebo nejpopulárnějších hesel daného jazyka. V případě neúspěchu musí útočník zkoušet všechny možné kombinace, což je v praxi při dodržení zásad bezpečných hesel takřka nemožné. (Petrovič, Kostěnec, 2012)

5.1.3 Využití důvěryhodnosti

V tomto případě útočník nenapadá přímo vybraný počítač, ale kompromituje jinou důvěryhodnou stanici, které je povolen přístup do sítě. Pokud je síť chráněna firewallem a důvěryhodné stanici je přístup do sítě povolen, je možné zařízení v chráněné síti napadnout právě prostřednictvím důvěryhodné stanice. (Petrovič, Kostěnec, 2012)

5.1.4 Man In The Middle (MITM)

Dle názvu je patrné, že útočník pronikne do komunikace mezi dvěma komunikujícími stranami a stane se prostředníkem komunikace. V tom případě má možnost komunikaci snadno odposlouchávat a také modifikovat. Tento druh útoku je velmi nebezpečný. Všechny techniky tohoto útoku mají stejnou podstatu. Původní komunikace mezi dvěma stranami je rozdělena na dvě části – jeden komunikační kanál je tvořen od strany A k útočníkovi a druhý od útočníka ke straně B. Přitom obě strany si stále myslí, že spolu komunikují jedním přímým kanálem. Existuji programy, které dokážou při útoku MITM přerušit SSL spojení, vyvolávající ve většině uživatelů pocit bezpečí. Jedním z nich je SSLSTRIP. Pokud přijme požadavek na zabezpečené spojení, nahradí jej směrem od útočníka za klasické HTTP, nikoli HTTPS. Uživatel může vidět pouze jeden patrný rozdíl a tím je začátek URL pouze http:// a ne https://, čehož si nezkušený

uživatel nemusí všimnout. Mezi obvyklé techniky provedení MITM patří podstrčení falešného DHCP serveru a podvrhování ARP záznamů. (Petrovič, Kostěnec, 2012)

5.1.5 Přetečení zásobníku

V programu nastává situace přetečení zásobníku ve chvíli, kdy zapíše data na zásobník mimo alokovanou oblast, většinou do zásobníku pevné délky, mající menší velikost než zapisovaná data. Takřka vždy takováto data pozmění obsah jiných proměnných a způsobí neočekávanou funkčnost aplikace nebo její pád. V případě, kdy takováto aplikace běží s oprávněním vysoké úrovně, činí celý systém zranitelným a vhodným k útoku. Jestliže si je útočník vědom této bezpečnostní díry v aplikaci, může se pokusit vložit do neošetřených uživatelských dat spustitelný strojový kód, který mu dovolí získat kontrolu nad procesem. Hlavním cílem útočníka je vložit škodlivý kód, který způsobí přetečení neošetřeného zásobníku a přepíše návratovou adresu tak, aby ukazovala na škodlivý kód. Výsledkem přetečení tedy není návrat k původní funkci, nýbrž spuštění onoho škodlivého kódu s oprávněním původního programu. Útočník tedy může získat nadvládu nad celým systémem, ovšem za předpokladu, že původní program měl nejvyšší oprávnění. Jedná se o jednu z nejstarších a nejúčinnějších forem počítačového útoku. (Petrovič, Kostěnec, 2012)

5.1.6 Phishing

Phishing je podvodná technika založená na sociálním inženýrství. Jde o falešné e-mailové zprávy, které vypadají téměř shodně, jako když je odešle uživatelova banka, pojišťovna nebo jiná podobná instituce. Ve většině případů se jedná o žádosti o potvrzení osobních a citlivých údajů, přístupových hesel, čísel platebních karet apod. Falešné zprávy vykazují velmi často podobné znaky, jako jsou gramatické chyby, nefunkčnost hypertextových odkazů, části v jiném jazyce nebo obsahují spustitelné přílohy apod. (Petrovič, Kostěnec, 2012)

5.1.7 Pharming

Pharming je technika, která se podobně jako Phishing, užívá na internetu k vylákání osobních údajů od uživatelů. Není však založena na rozesílání podvodných e-mailů, ale na manipulaci s DNS záznamy. V dnešní době je útok tak známý, že většina antivirových programů zamyká přístup k potřebným souborům. Útočníkovi tedy zbyde

pouze možnost napadnout samotný DNS server a to je spíše na poli teoretickém. (Petrovič, Kostěnec, 2012)

5.1.8 Denial of service (DoS) a Distributed DoS

Základem těchto útoků je omezení přístupu až úplné znepřístupnění určité služby, počítače nebo dokonce celé sítě. Útočník má za cíl zahltit oběť požadavky, které způsobí postupné vyčerpání výpočetního výkonu, zpomalení funkcionalit a následný pád. Konkrétními cíli těchto útoků bývají většinou důležité servery velkých firem, pro které je i dočasný výpadek služeb kritický. Může se jednat o banky, pojišťovny, burzy, pošty nebo důležité servery z hlediska fungování internetu, např. kořenové DNS servery. (Petrovič, Kostěnec, 2012)

Distributed DoS

S vývojem a neustálým zlepšováním hardwarových parametrů počítačů, a to hlavně těch serverových, se klasický DoS útok modifikoval na tzv. distribuovaný DoS, tedy DDoS. Principiálně se jedná o stejný typ útoku, avšak je veden z velkého množství stanic najednou. Dnešní počítače jsou schopny výpočetně odolat takovému útoku i z více stanic. DDos útok funguje většinou tak, že útočník napadne stovky až tisíce počítačů trojským koněm a ty poté na jeho pokyn, v jeden čas, začnou zahlcovat cílový server. Druhou variantou je například domluva mezi určitou komunitou uživatelů internetu, že dobrovolně v jeden čas začnou přistupovat na cílový server a ten nedokáže obsloužit jejich požadavky, až spadne. Proti takto vedeným útokům se téměř nelze bránit. (Petrovič, Kostěnec, 2012)

5.2 Nebezpečné programy

Nebezpečné programy, také škodlivý software, dnes nejsou již jen počítačové viry. Tímto slovním spojením se označují veškeré programy, které škodí uživatelům elektronických zařízení a sítí. V základě je můžeme rozčlenit na počítačové viry, trojské koně a červy. Podrobněji jsou popsány dále.

5.2.1 Počítačové viry

Označení bylo zvoleno kvůli nezaměnitelné podobnosti s biologickými viry. I virus počítačový potřebuje k životu a šíření hostitele. Ve valné většině případů se jedná o spustitelný soubor nebo soubor, který obsahuje alespoň z části spustitelný kód.

Při spuštění napadených souborů se spustí kód viru a poté až samotný program. Viry nemusí být ve všech případech destruktivní (mazání dat z disku, modifikace systémových registrů apod.). Existují i viry, které jsou spíše obtěžujícího charakteru a mohou zobrazovat nechtěné zprávy na obrazovce, sbírat adresy oblíbených stránek uživatelů a zobrazovat jim kontextovou reklamu apod. Ve většině případů však viry ovlivňují výkon a stabilitu systému. K infikování systému je třeba interakce uživatele (otevření emailové přílohy, přenesení infikovaného souboru na flash paměti, poslání po síti). V dnešní době jsou viry spíše na ústupu a jsou nahrazovány sofistikovanějšími způsoby napadání systémů. Hlavním důvodem je skutečnost, že vir jako takový se nestará o své šíření, napadne soubor a čeká, až ho uživatel přenese na jiný počítač nebo jakkoli jinak rozšíří dále. (Doseděl, 2004)

5.2.2 Červy

Červ je druh nebezpečného programu, který se oproti viru dokáže sám masově šířit. Ke svému šíření může používat řadu cest. Nejčastěji se jedná o chyby v programech systémem přetečení zásobníku a také o emailovou komunikaci. V poštovních klientech se červ sám rozešle na kontakty z adresáře uživatele a v mnoha případech dokáže i čerpat z uložených adresářů jiných programů (ICQ, Skype, Mirranda apod.). Samotné spuštění červa je velice jednoduché, stejně jako u viru a do značné míry spoléhá na neznalost a neopatrnost uživatelů. Velice známým příkladem je červ s obrázkem slavné tenistky Anny Kurnikovové. Jednalo se o obrázek, který byl doplněn spustitelným kódem. Červ nahraný do kódu systémem přetečení zásobníku může ovládnout síťové rozhraní počítače a neomezeně se tak rozšířit do všech stanic v síti. Princip útoku na přetečení zásobníku byl již popsán výše v samostatném odstavci. Vedlejším efektem šíření červů je zahlcování síťových linek a to vede ke snížení rychlosti připojení k internetu. Napadení červem způsobuje nemalé finanční škody hlavně firmám, které musí zaplatit nákladné čištění všech stanic a mají problém poskytovat stoprocentně své služby. Asi nejznámější masově rozšířené červy jsou Blaster, SQL Slammer a Code Red. (Doseděl, 2004)

5.2.3 Trojské koně

Již samotný název tohoto škodlivého softwaru evokuje analogii s Trojským koněm z řecké mytologie. I počítačový trojský kůň se tváří jako užitečný nástroj např. hra,

spořič obrazovky nebo jako program na odstraňování škodlivých souborů z počítače. Pokud uživatelé stahují nelegální software, setkávají se s trojskými koňmi nejčastěji v generátorech sériových čísel. Ty sice poskytnou uživateli sériové číslo, nicméně mohou útočníkovi také poskytnout nežádoucí přístup. Trojský kůň může být také přidán do funkční verze stávající aplikace a poté šířen nedůvěryhodnými cestami pro zamaskování původu. Mezi tyto způsoby šíření patří warez servery, P2P (peer to peer) sítě nebo torrenty. Trojské koně se nedokáží obvykle sami šířit a infikovat další aplikace na disku. Existují však červi, které nesou koně jako náklad anebo dokáží přidáním kódu vytvořit trojské koně z legitimních aplikací. (Petrovič, Kostěnec, 2012)

6 Zásady bezpečného provozu komunikace na síti a užívání počítače

V této kapitole je zprvu nutné rozdělit bezpečnostní hrozby na ty, proti kterým se běžný uživatel dokáže bránit a preventivně se na ně připravit a na ty, které ovlivní jen velice složitě.

Z výčtu typů bezpečnostních hrozeb na síti, které jsou popsané v předešlé kapitole, běžný uživatel jistě nedokáže zabránit útokům DoS a DDoS a využití důvěryhodnosti. O tyto bezpečnostní hrozby se musí postarat správci systémového firewallu nebo systému celého.

Zbylým typům se více či méně může běžný uživatel bránit správným chováním na síti, využitím dostupného softwaru a vzděláváním se v oboru informačních technologií.

6.1 Obecné zásady používání počítače v prostředí nezabezpečené sítě

Tato podkapitola se zaměřuje na možnosti nastavení počítače a obecné doporučené prvky chování na síti a internetu. Softwarové vybavení zůstává jako nadstavba těmto pravidlům do další samostatné podkapitoly.

Hlavními zásadami tedy jsou:

- **Používat různá a silná hesla** – použitím silných hesel se značně snižuje možnost odcizení přístupu k online účtům a zabrání se tak ztrátě dat v podobě e-mailů, různých úložišť online dokumentů, zneužití identity apod. Také není příliš vhodné používat pouze jedno heslo ke všem účtům, byť silné. Uživatel svou neopatrností může heslo někde vyzradit a ohrozí tak sám sebe na spoustě míst najednou.

  Silné heslo má obsahovat minimálně 8 znaků, zahrnující malá a velká písmena abecedy, číslice a náhodné znaky. Důležité je se vyvarovat použití běžných slov, která jsou dohledatelná ve slovníku. Útočník velice snadno hrubou silou zjistí heslo nebo jeho velkou část.

  Častou chybou uživatelů je, že byť silná hesla uchovávají na nevhodných místech (peněženka, nalepené papírky na monitoru apod.). Hesla by se měla uchovávat nejlépe pouze v paměti uživatele a doporučeno je využívat maximálně nápovědu ke vzpomenutí si na daná hesla.

- **Nepoužívat účet administrátora** – pro připojování k nezabezpečené síti a internetu je vhodné využívat standardní uživatelský účet operačního systému, nikoli účet administrator (Windows) nebo root (Linux). Účty pro administraci operačního systému mají neomezená práva a jsou zde mnohem větší rizika při napadení systému. Pokud se útočníkovi povede zavést škodlivý program do systému pod účtem administrátora, může získat neomezená práva k jeho řízení.

  V případě, kdy jednu stanici (jeden počítač) využívá více uživatelů, je vhodné vytvořit pro každého zvláštní uživatelský účet s omezenými právy.

- **Aktualizovat systém a aplikace** – operační systém počítače by měl být vždy plně aktualizovaný. Nové aktualizace doplňují systém o tzv. záplaty právě proti možnostem napadení a zneužití. Toto je spjaté s neustálým vývojem počítačových útoků a nutností reakce ze strany softwarových firem.

  Stejně se může toto pravidlo aplikovat i na doplňkové aplikace v operačním systému. Veškerý software, který není delší dobu aktualizován, přináší větší riziko z pohledu útoku právě skrze neaktuální aplikaci.

- **Instalovat jen potřebný a prověřený software –** uživatelé by měli na svoje počítače instalovat pouze aplikace, které opravdu potřebují a pouze z prověřených zdrojů – nejlépe aplikace oficiální a legální. Různé verze softwaru dostupné nelegálně v podobě warezu mohou obsahovat škodlivý kód a navíc jejich používáním uživatelé porušují autorský zákon.

- **Neotvírat všechny přílohy bez rozmyslu –** přílohy k elektronickým zprávám jsou velmi oblíbeným nástrojem využívaným ze strany útočníků. Příloha se zajímavým názvem, či obrázkem nebo ikonou, vybízí neopatrné uživatele k otevření. Poté, aniž by uživatel cokoli poznal, se do počítače zkopíruje škodlivý kód a útočník zvítězil. Přílohy k elektronickým zprávám by se měly otevírat s rozmyslem. Obecně vzato, o přijetí přílohy by uživatel měl předem vědět nebo musí pocházet z opravdu důvěryhodného zdroje. V opačném případě se doporučuje přílohy ignorovat.

- **Komunikovat přes zabezpečené protokoly –** při navštěvování webových stránek, které vyžadují přihlášení uživatelským jménem a heslem, by si uživatel měl ověřit, zda se k přenosu HTML stránky využívá zabezpečená varianta http

protokolu, tedy https. Protokol https využívá speciální vrstvu, protokol SSL, který vytvoří zašifrovaný kanál mezi počítačem a serverem a zabrání tak odposlechu. Uživatel toto využití pozná v podobě URL adresy stránky a některé prohlížeče navíc v těchto místech zobrazují obrázek zámku či jiného symbolu zabezpečení.

- **Zveřejňovat své osobní údaje s rozmyslem –** toto pravidlo se týká hlavně různých sociálních sítí, chatů, seznamek a dalších portálů, které přímo slouží ke zviditelnění své osoby. Uživatelé by si měli nejprve řádně rozmyslet, co všechno o sobě zveřejní. V dnešní době již existují skupiny kriminálníků - jak počítačových, tak i ostatních - kteří se přímo zaměřují na analyzování informací z podobných serverů. Příkladem může být zveřejněná informace o cestě do zahraničí a starost o to, zda doma přežijí těch 14 dní květiny bez vody – ve chvíli kdy na profilu uživatele bude zveřejněna adresa bydliště, stává se tato informace velice zajímavou pro zloděje.

(Petrovič, Kostěnec, 2012)

6.2 Softwarové nástroje pro zabezpečení provozu na síti

Tato podkapitola pojednává o rozšíření základních zásad používání počítače na internetu v podobě přídavného softwaru. Software pro zabezpečení počítače je v dnešní době již velice různorodý a uživatel má nepřeberné množství možností. Níže uvedený přehled by měl sloužit pro uvedení uživatelů do dané problematiky, nikoli jako návod jak tento software používat. Předpokládá se, že nezkušený uživatel pro získání a nastavení bezpečnostního softwaru využije rad nebo služeb odborníka.

6.2.1 Antivirový software

Antivirový software je nejrozšířenějším nástrojem pro obranu uživatelských systémů před hrozbami souvisejícími se zlomyslným a škodlivým softwarem, označovaným někdy souhrnně jako *malware*. Těmito hrozbami jsou především počítačové viry přenášené v infikovaných souborech, červy, které se šíří po síti autonomně, a také lidé, kteří zneužívají škodlivý software pro dálkové ovládání napadeného systému.

Antivirové programy zpravidla provádějí detekci infikace při sledování spouštěcího sektoru, paměti a souborového systému počítače. Vyhledávají projevy neboli signatury známého malwaru, a to i v běžících aplikacích v reálném čase. Správně provozovaný

antivirový software je velmi silným nástrojem v obraně proti infikaci systému. (Northcutt, Zeltser, Winters, Frederic, Ritchey, 2005, s. 238)

Antivirové programy jsou dostupné ve volně šiřitelných bezplatných verzích, ale také v placených verzích s časově omezenou licencí. Bezplatné varianty slouží zpravidla pouze k osobnímu využití a mají omezenou funkcionalitu oproti placeným verzím.

Nejznámější a nejpoužívanější antivirové programy:

- Microsoft Security Essential – bezplatný
- AVG Free – bezplatný v omezené funkcionalitě
- Avast Personal – bezplatný v omezené funkcionalitě
- Ad-Aware free antivirus – bezplatný v omezené funkcionalitě
- Eset Nod32 – placený s omezenou licencí
- Norton antivirus – placený s omezenou licencí

a další.

Stejně jako každý jiný obranný mechanismus má i antivirový software své silné a slabé stránky, o kterých je třeba získat povědomí.

Silné stránky antivirového softwaru

- Dokáže vzdorovat velkému množství vzorků známého škodlivého softwaru. Výrobci a tvůrci antivirových aplikací investují nemalé peněžní prostředky do výzkumu a dnes již umí analyzovat škodlivý software poměrně rychle, a vytvořit tak konkrétní signaturu viru, červu nebo trojského koně.
- Svého uživatele téměř neobtěžuje, po správném nastavení nevyžaduje téměř žádnou kooperaci uživatele pro svou činnost. To je dáno i tím, že má poměrně malé procento falešných poplachů (falešné pozitivní nálezy). I v režimu ochrany v reálném čase pracuje na pozadí a jen výjimečně vyžaduje zásah uživatele systému.
- Je cenově dostupný i v placených variantách pro profesionální využití. (Northcutt, Zeltser, Winters, Frederic, Ritchey, 2005, s. 239)

Slabé stránky antivirového softwaru

- Účinnost antivirového softwaru je především závislá na velikosti dostupné databáze projevů (signatur) škodlivého softwaru. Škůdci se může podařit masově rozšířit ještě dříve, než výrobce antivirového softwaru vytvoří signaturu a aktualizuje databázi. V nastavení antiviru se doporučuje zapnout automatické aktualizace virové databáze.
- Nízká účinnost při detekci zmutovaných variant škodlivého softwaru. Nebezpečný kód stačí jednoduše upravit bez zásadních změn funkcionality kódu a pro antivirový software vznikne problém při jeho detekci. (Northcutt, Zeltser, Winters, Frederic, Ritchey, 2005, s. 240)

Antivirový software by měl být součástí každého systému.

6.2.2 Personální Firewally

Firewall je zjednodušeně řečeno zařízení nebo software oddělující provoz mezi dvěma sítěmi (většinou privátní a internetem). Obsahuje sady pravidel, která mají za cíl propojení dvou nebo více sítí s různou úrovní důvěryhodnosti tak, že sníží předem definovaná rizika vyplývající pro chráněné sítě z tohoto propojení. V koncových uživatelských systémech běžně vystačíme se softwarovou variantou firewallu. Pravidla nastavená ve firewallu umožňují získat dohled nad vstupem paketů do systému a výstupem paketů ze systému. Personální firewally posilují obranu systému, protože dokáží odrazit řadu hrozeb, proti nimž jsou antivirové produkty krátké:

- Neomezený přístup ke sdíleným adresářům v systému
- Anonymní přístup k systému
- Nedetekovaný škodlivý kód
- Prohledávání (scan) portů a další typy průzkumu sítě
- Zranitelné síťové služby běžící v systému

Po první instalaci personálního firewallu se obvykle zablokuje veškerý přístup počítače na síť i ze sítě na počítač. Při každém uskutečněném pokusu o připojení z libovolného směru se firewall zeptá, zda je připojení pro uživatele důvěryhodné a má pro něj vytvořit do budoucna pravidlo. Drtivá většina personálních firewallů pro počítače s Windows umí stanovit omezující pravidla přístupu podle lokální aplikace, která se

pokouší o odeslání či příjem paketů. Než firewall povolí aplikaci požadované spojení, podívá se do množiny přípustných pravidel a v případě neshody spojení zakáže. Při prvotním použití firewallu mohou být velmi časté dotazy na pokusy o připojení znepokojující a otravné, nicméně po určitém čase si firewall zapamatuje nejčastější aktivitu uživatele a na cokoli jiného – podezřelého ho včas upozorní.

Zde nastává zásadní problém, kvůli kterému nejsou personální firewally dostatečně rozšířené mezi koncovými uživateli. Podstatná část těchto uživatelů není vyzbrojena nutnou dávkou trpělivosti odpovídat na dotazy firewallu několik dnů až týdnů nebo na ně jednoduše odpovědět neumí a firewall odstraní dříve, než mohl být pro systém užitečný.

Z tohoto důvodu někteří tvůrci poskytují k personálním firewallům skupiny předdefinovaných pravidel a tím zmírňují intenzitu dodatečných dotazů. Nicméně každý systém a každý uživatel mají své specifické požadavky na připojení, a tak je tato cesta spíše cestou „lepší něco než nic“.

Tvůrci firewallu ZoneAlarm zvolili jakousi střední cestu – uživateli odpovídání na dotazy ulehčuje vytvoření dvou skupin (zón) externích serverů, a sice důvěryhodné (lokální) a nedůvěryhodné (vnější internet). Pro každou tuto zónu platí samostatný soubor přístupových omezení a konkrétní zóna je definovaná kategorií vzdáleného hostitelského systému. Uživatel tak netvoří samotné skupiny oprávnění, pouze určí kam nebo odkud je daný pokus o připojení. (Northcutt, Zeltser, Winters, Frederic, Ritchey, 2005, s. 242)

Zde jsou některé z rozšířených osobních firewallů:

- ZoneAlarm (http://www.zonelabs.com/)
- Norton Personal Firewall (http://www.symantec.com/)
- Tiny Personal Firewall (http://www.tinysoftware.com/)
- Kerio Personal Firewall (http://www.kerio.cz/)
- Sygate Personal Firewall (http://www.sygate.com/)

Mnohé firewally jsou pro nekomerční použití zcela zdarma a jsou tak snadno dostupným nástrojem ochrany počítače pro každého uživatele.

7 Zabezpečení e-mailové komunikace (šifrování)

Tato samostatná kapitola pojednává o možnosti zabezpečení e-mailové komunikace pro všechny uživatele, kteří si chtějí nebo potřebují zajistit 100% soukromí při komunikaci elektronickou poštou. Jsou zde uvedeny konkrétní příklady softwarových nástrojů, pomocí kterých lze tohoto dosáhnout. Veškerý uvedený software je volně šiřitelný, a tedy zdarma. Možností pro dosažení šifrované e-mailové komunikace je samozřejmě více. Kapitola využívá informací uvedených v předešlých částech práce.

Šifrovaná e-mailová komunikace staví na principu asymetrického šifrování, tedy šifrování s veřejným klíčem. To znamená, že dva komunikující uživatelé musí vygenerovat svou dvojici klíčů – veřejný a soukromý. Své veřejné klíče si poté vymění a s jejich pomocí budou šifrovat zprávy pro majitele veřejného klíče, který obdrželi. Ten příchozí zprávu dešifruje pomocí svého soukromého klíče a komunikace proběhne v zabezpečené formě.

Obr. č. 6: *Ukázka veřejného klíče*

Pramen: http://www.evropsky-rozhled.eu/wp-content/uploads/gpg4win_36.JPG

K tomuto předpokladu je nutné mít nainstalované potřebné softwarové vybavení. Uživatelé začátečníci vystačí s jediným balíkem, který se jmenuje GPGforWin. Z názvu je patrné, že se jedná o verzi určenou pro operační systémy Windows. Obdobná varianta

existuje i pro operační systémy Linux. Tento softwarový balík obsahuje aplikaci pro tvorbu a správu klíčů Kleopatra a e-mailového klienta Claws Mail, který umí pracovat se šifrovanou elektronickou poštou. Obecně lze využít veškeré e-mailové klienty, které podporují šifrování zpráv.

Pomocí nástroje Kleopatra uživatel vygeneruje dvojici klíčů OpenPGP key pair a vytvoří si jejich zálohu. Svůj veřejný klíč poskytne všem, od kterých chce přijímat šifrované zprávy. Následně je nutné nastavit e-mailového klienta Claws Mail na nějakou již existující e-mailovou schránku a doplnit do něj modul, který zpracuje PGP klíče. Poté se do klienta pouze zavedou veřejné klíče komunikačních partnerů a při odesílání e-mailu se zvolí varianta šifrování, vybere se veřejný klíč adresáta a zpráva se odešle v zašifrované formě.

Obr. č. 7: *Ukázka zašifrované e-mailové zprávy*

From: vit [redacted] <vit@[redacted].net>
To: Ingrid Romancová <romancova@evropsky-rozhled.eu>
Subject: Re: Ahoj
Date: Sat, 8 Oct 2011 13:44:59 +0200
Sender: vit.[redacted]@gmail.com

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.11 (GNU/Linux)

hQEMA26oGd3aEkDlAQf/Uw97d5l4suOKnfRVIRTaKleZEJpXSljMwxelQwdNqwzX
o8lcLxs+el6p4FTQZ0aC60IMe7ucG94oxxozZQHXoo53kmcCN9whmGO4+MdN+lZm
OJWPqx/48U/4jx0EmZl8CemK5T94LDKODCud8+nzWwemzIWM69M+9En4na958cgb
/odiufbs5r4uoIZnH0UlMcLAnMIJjClHXlviyQ9sZ/iD02l3Fzl07aP+6MBq7IuX
mmSjcYPUm+Ee49Kdo2NNkVgCYZTi0YZaZLRVVIhrWSVJBzkDKF55Cb3dch0oazge
+4M4EPmysDKQJfj4O2XrwGSROxs30JIw3ByQUe9MmtLpASz5qmcoHOQA5XaQRlqU
LzdpplU7klfmFzeIKD+uylGXVL7cF04qOM7yPq+Rh6ZD8DYUjYi7yLhieejFulxy
DsXcgUi/dXn0AOgKVxqfCBWT4zPzqsVm5+F5X/MIHG0896gMfh6Jb/PB/H7Go79Y
3T0nu+ek4+TzqUL3oXDoJ+eJ/q7wljNCBFcWSuIVDlTMo4JRNMaiiK6DjIQvv43c
JI4C48sSg/NFH4uJzqtu3C0YNcPbUitvrkcI8ik025oyuGkxqZ07R+F+/ycA4xt/
oHiD6Z4JE7f7YlHZAOE0VU4q9Xvt9AtUXiv7R8eolWFqvFQjtSntKT6Umyzf4MTz
CRaW52op8oTkzHqzRlxOx+/WHurmuzOGXTQQEoU/FpswiAo3EcCxJ2P/XLK1kO6C
DlKzKpeupzFMa0J2wtnaycRAieUNPLUiCfdl4N0D63ifGln/rpKLcpjz6VVgSNDc
H2P7TRZxIAZSYLIB+ZvAxmXN9d48eXFcjxO6VE2eNenWuP6s0wkMWagbo58razPY
bLMQ9V4glmyh+arvqfLDNyceVzwesdkrY5FLaKqo4/0rZBVJuZVYbRZoQNCwwYfU
GOqvuWQhbxnJ3CevAL52+wfSfbT8vpvXWgMXkojG6dF3uulwVN4FBAWJeOkwqoTb
iPnWljzvx7yeg0TFKe7YPUeATH8F6bJZnGcNpXl/4PHvv/FEzjDk/h7TyCpcChlf
U3sAHatCu8nBMeOBtOXj8iWI2Qxr2Mx27lJeen+pl/HA4dMDKUNIs83fWJJgGo0g
6UvAYp8De6ZhMHuqvIHDNSJhnvkIDHhUuFxYJG6GdXVt3MEy625J+lPzBdi/93Gv
jCQ=
=lp9d
-----END PGP MESSAGE-----
```

Pramen: http://www.evropsky-rozhled.eu/wp-content/uploads/gpg4win_58.JPG

Podrobný online manuál na zprovoznění šifrované e-mailové komunikaci pomocí nástroje GPGforWin poskytuje server Evropský rozhled na následující adrese: http://www.evropsky-rozhled.eu/sifrovani-e-mailu-pro-uplne-zacatecniky-gpg4win/.

8 Dotazníkové šetření

Výzkumná část práce je realizována pomocí elektronického dotazníku na serveru Vyplnto.cz. Šetření probíhalo v období 5.3.2014 až 4.4.2014. Dotazník vyplnilo 232 respondentů různých věkových kategorií.

Jednotlivé otázky dotazníku jsou podrobně rozebrány v následujících částech kapitoly. Ke každé otázce je zpracován přehledný graf s procentuálním rozložením odpovědí. V závěru kapitoly jsou popsány různé hypotézy závislostí jednotlivých otázek a jejich odpovědí.

8.1 Cíl dotazníkového šetření

Cílem dotazníkové šetření je zjistit míru povědomí běžných uživatelů internetu o možnostech zabezpečení jejich provozu. Předpokladem pro vypracování práce je, že tato míra povědomí není na vysoké úrovni.

8.2 Cílová skupina oslovených respondentů

Cílová skupina je stanovena na běžné uživatele sítě a internetu. Není tedy nijak striktně omezena a šetření se zúčastnili uživatelé obou pohlaví a různých věkových skupin. Souhrnně dotazník vyplnilo 232 respondentů, kteří byli vybíráni převážně náhodně. Nicméně snahou bylo rozšířit dotazník do různých věkových skupin.

8.3 Vyhodnocení jednotlivých otázek

Dotazník obsahuje 15 dílčích otázek a v této podkapitole je jejich podrobný grafický přehled a popis.

Otázka č. 1: Jak často komunikujete prostřednictvím sítě/internetu?

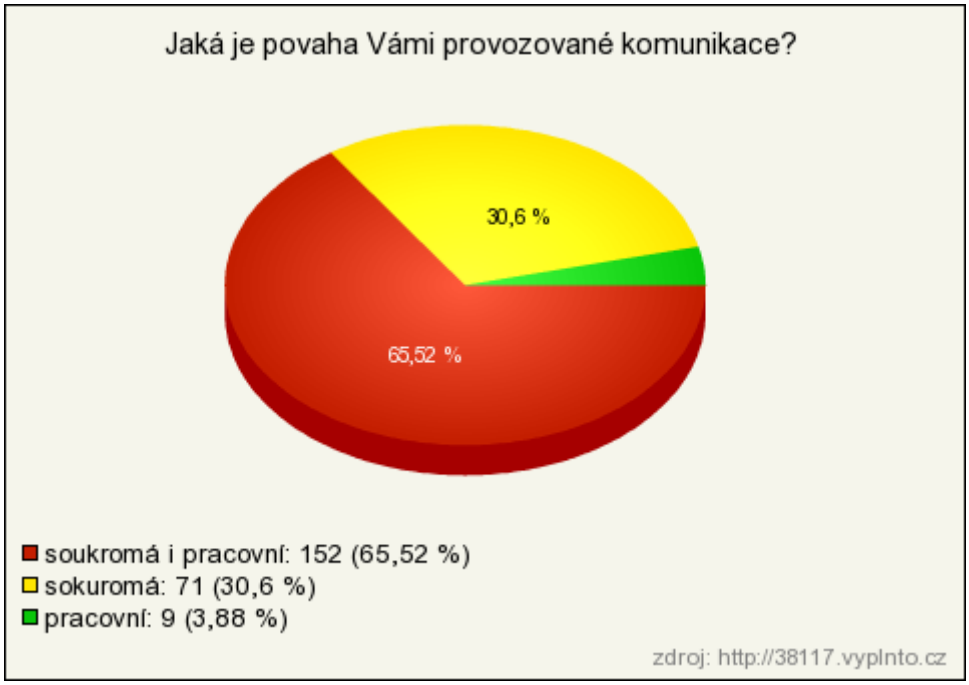
Tato otázka je velmi zásadní pro celý zbývající obsah dotazníku. Grafické zpracování odpovědí jasně ukazuje, že drtivá většina respondentů (téměř 90%) využívá internet ke komunikaci několikrát denně. Z tohoto hlediska by měla míra povědomí o zabezpečení provozu na internetu dosahovat vysoké úrovně.

Graf č. 1: *Grafické rozložení odpovědí na otázku č. 1*

Otázka č. 2: Jaká je povaha Vámi provozované komunikace?

Hlavním záměrem této otázky bylo zjistit, zda uživatelé používají internetovou komunikaci pouze k osobním účelům nebo i k pracovním. Z odpovědí je možné stanovit určitý poměr mezi komunikací osobního charakteru a pracovního charakteru. Zvláště pak v případě pracovní komunikace by uživatelé měli dbát bezpečnostních zásad.

Graf č. 2: *Grafické rozložení odpovědí na otázku č. 2*



Otázka č. 3: Využíváte ke svým internetovým účtům silná hesla z hlediska zabezpečení?

Uživatele, kteří odpověděli záporně nebo dokonce, že nevědí, o co se jedná, by měla otázka přimět k zamyšlení o nastudování problematiky bezpečných a silných hesel. Graf ukazuje skutečnost, že velké části uživatelů (78%) je toto základní pravidlo zabezpečení známé a využívají ho.

Graf č. 3: *Grafické rozložení odpovědí na otázku č. 3*

Otázka č. 4: Slyšeli jste již někdy o možnosti bezpečné komunikace na internetu?

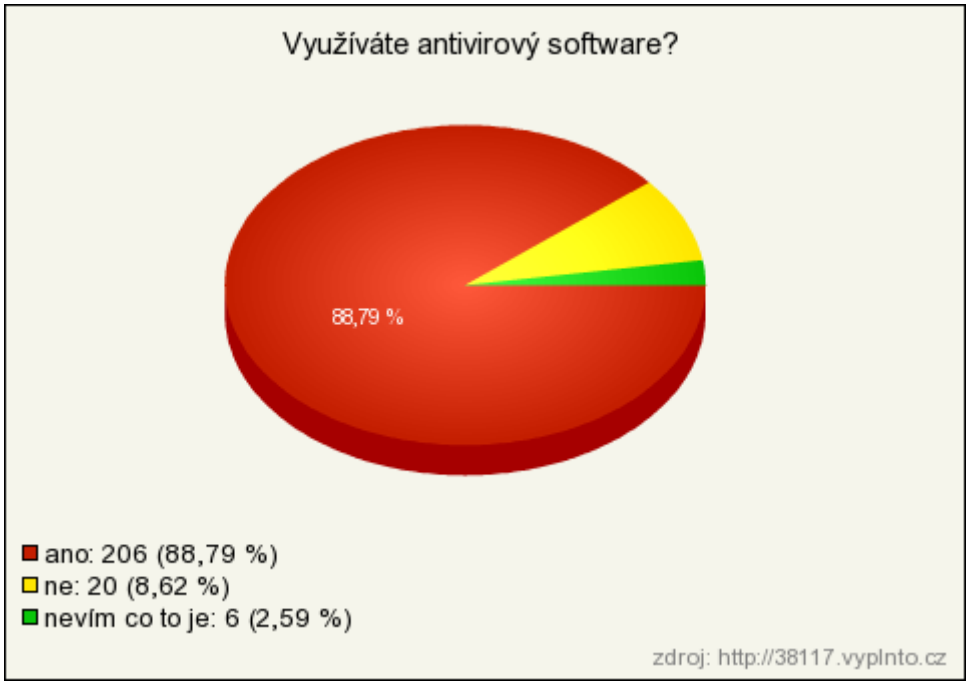
Z procentuálního rozložení odpovědí na tuto otázku je vidět, že téměř 40% respondentů odpovědělo záporně. To znamená, že doposud nikdy ani neuvažovali o rizicích spojených s komunikací po internetu, natož pak o možnostech jak jim předejít. Toto zjištění je poměrně alarmující, teoreticky totiž znamená, že 40% uživatelů může být snadným terčem virtuálních útočníků.

Graf č. 4: *Grafické rozložení odpovědí na otázku č. 4*

Otázka č. 5: Využíváte antivirový software?

Na tuto otázku odpověděla většina respondentů (88%) kladně, pouhá 2,5% odpověděla, že neví co to antivirový software je. Vysoké procento kladných odpovědí by se dalo přisoudit tomu, že je v dnešní době běžná situace, kdy antivirový software nabízí většina prodejců rovnou k zakoupenému počítači nebo operačnímu systému (OS). Prodej nových zařízení a OS je spjat s mnohdy výraznými slevami na antivirový software, a tak je pro uživatele takto dostupnější. Navíc se propagace společností vytvářejících antivirový software dostala hojně i do masovějších médií jako je televizní vysílání, billboardy apod.

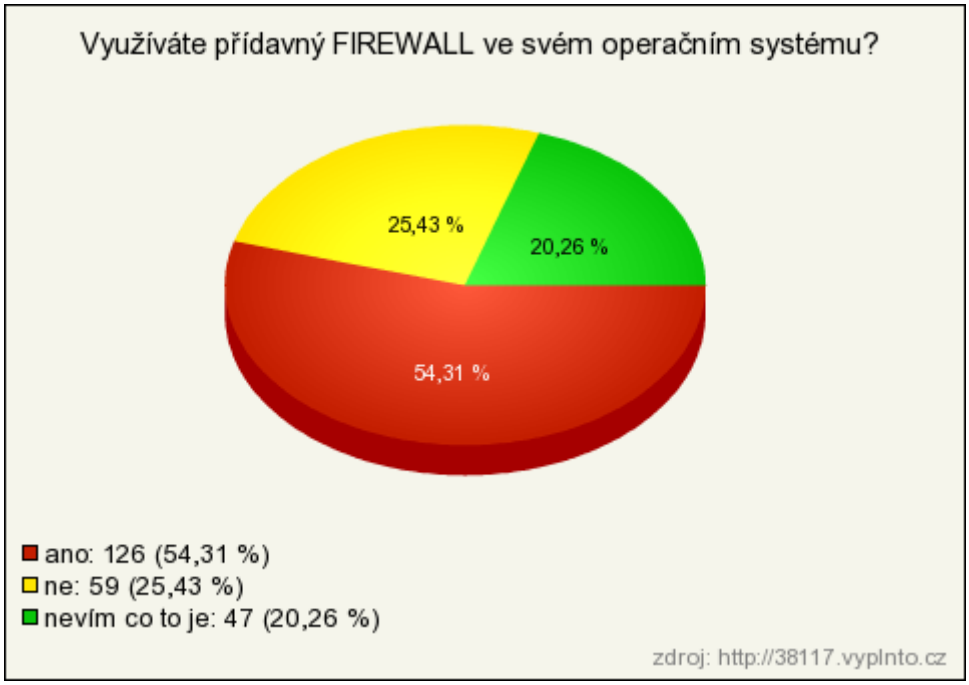
Graf č. 5: *Grafické rozložení odpovědí na otázku č. 5*



Otázka č. 6: Využíváte přídavný firewall ve svém operačním systému?

U šesté otázky týkající se využití přídavného firewallu již není situace tak jednoznačná jako v předešlé otázce. Zde nadpoloviční většina respondentů (54%) odpověděla kladně, nicméně celá ¼ respondentů odpověděla záporně a dokonce 20% uvedlo, že neví co to je firewall. Uživatelům je k dispozici značné množství tohoto bezpečnostního softwaru zdarma, a tak by se dalo očekávat, že výsledky budou příznivější.

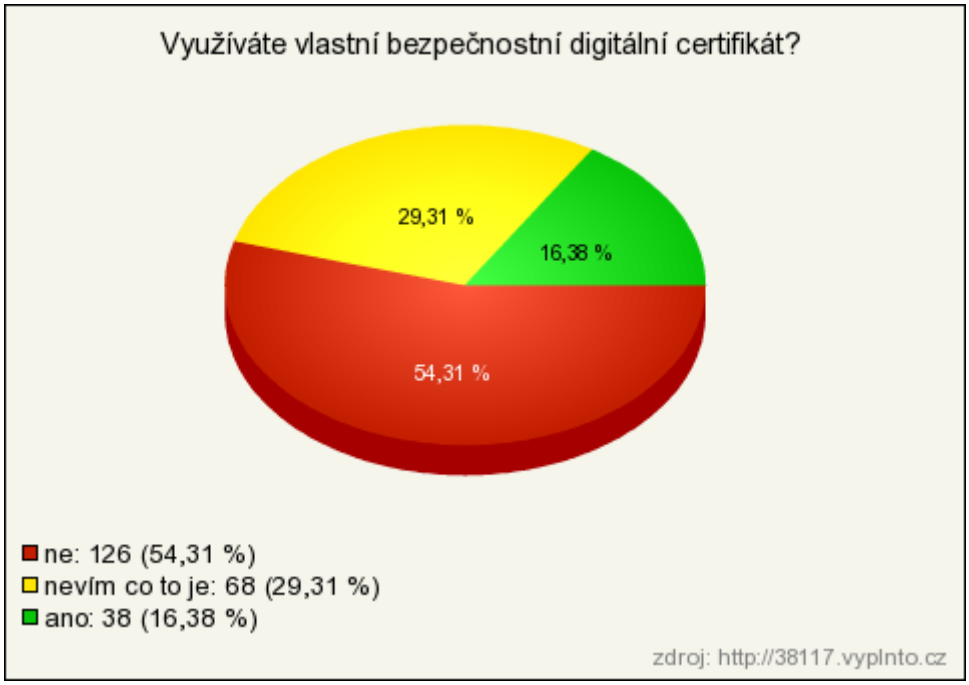
Graf č. 6: *Grafické rozložení odpovědí na otázku č. 6*



Otázka č. 7: Využíváte vlastní bezpečnostní digitální certifikát?

U této otázky již zaznamenávají odpovědi opačný trend. Více než polovina dotazovaných (54%) odpověděla záporně, k tomu téměř celá 1/3 odpověděla, že neví, co to je a 16% tázaných odpovědělo, že certifikát využívá. Je vidět, že metody šifrování nejsou mezi běžnými uživateli natolik rozšířené.

Graf č. 7: *Grafické rozložení odpovědí na otázku č. 7*



Otázka č. 8: Využíváte vlastního elektronického podpisu?

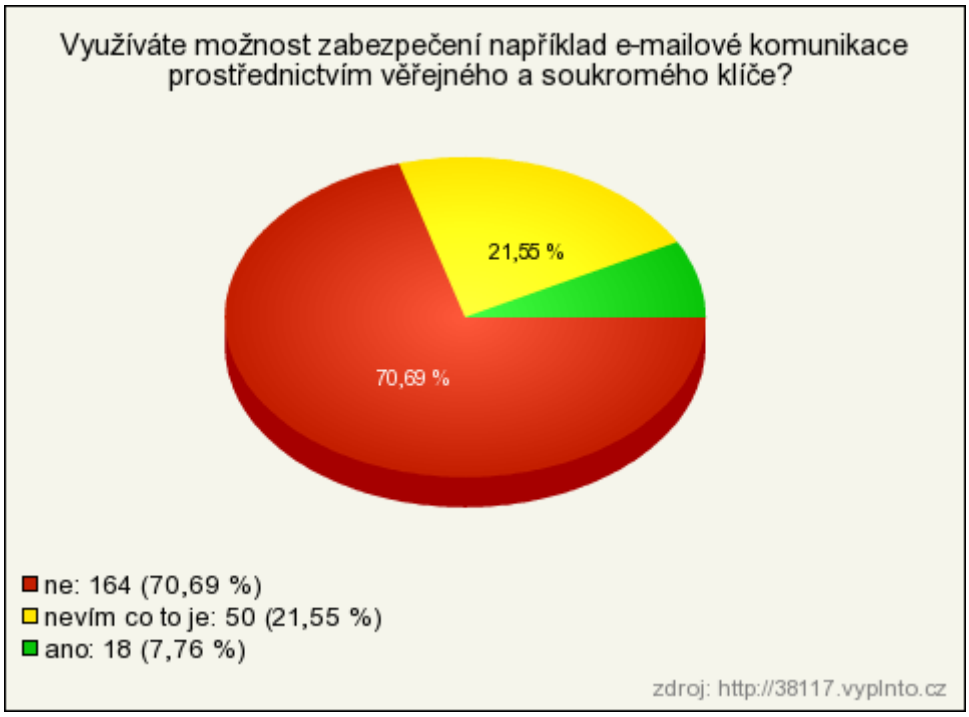
V této otázce se již drtivá většina dotazovaných vyjádřila záporně (88%), dalších necelých 5% odpovědělo, že neví, co to je a přibližně 8% odpovědělo kladně.

Graf č. 8: *Grafické rozložení odpovědí na otázku č. 8*

Otázka č. 9: Využíváte možnost zabezpečení, například e-mailové komunikace, prostřednictvím veřejného a soukromého klíče?

Šifrovanou e-mailovou komunikaci využívá z dotázaných pouze necelých 8%. Dalších 70% respondentů odpovědělo záporně a celých 21%, že neví, co to je. Z těchto výsledků je patrné, že míra povědomí uživatelů o možnosti zabezpečení e-mailové komunikace, kterou všichni jistě hojně využívají, je minimální.

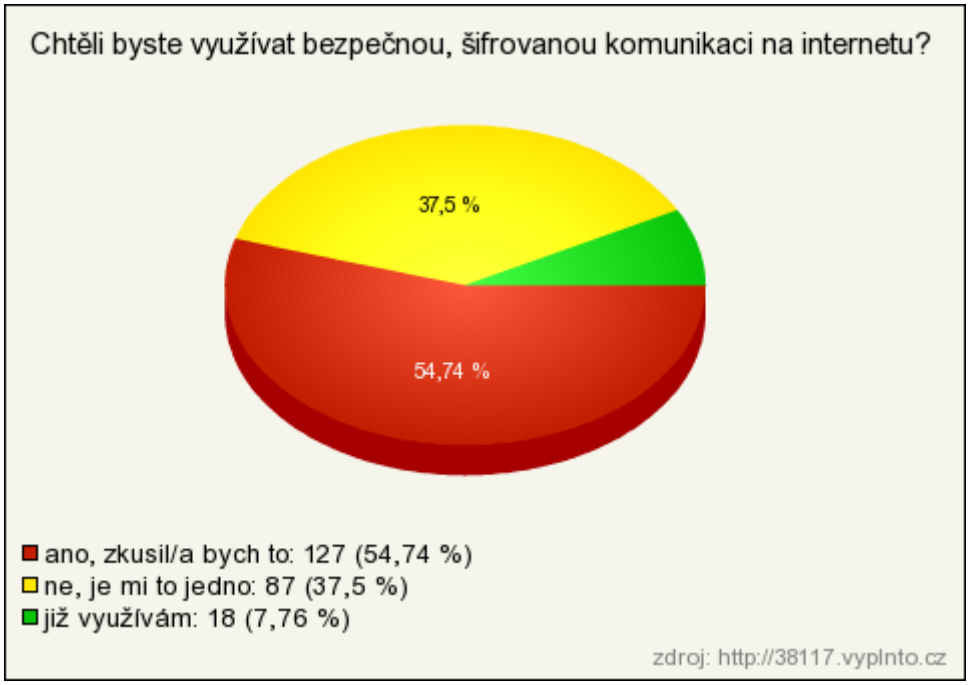
Graf č. 9: *Grafické rozložení odpovědí na otázku č. 9*



Otázka č. 10: Chtěli byste využívat bezpečnou, šifrovanou komunikaci na internetu?

Nadpoloviční většina respondentů (54%) odpověděla na tuto otázku, že by chtěli tuto možnost vyzkoušet. Celých 37,7% respondentů odpovědělo ve smyslu, že je jim tato situace lhostejná. Zbylá část dotázaných, v návaznosti na předešlou otázku, odpověděla, že již tuto možnost využívá.

Graf č. 10: *Grafické rozložení odpovědí na otázku č. 10*



Otázka č. 11: Provozujete vlastní e-shop nebo jinou formu elektronického obchodování?

Otázka byla položena hlavně z důvodu, aby bylo zjištěno, v případě kladné odpovědi, jakým způsobem vlastníci malých e-shopů řeší zabezpečení klientských a přístupových dat. Bohužel v daném vzorku respondentů odpovědělo kladně pouhých 13 jedinců, z toho 8 jich zabezpečení nechává na zhotoviteli e-shopu, který zakoupili. Zbylých 5 si e.shop vytvořilo individuálně a o zabezpečení se starají osobně.

Graf č. 11: *Grafické rozložení odpovědí na otázku č. 11*

Otázka č. 12: Kdo se stará o zabezpečení dat uživatelů Vašeho e-obchodu a zabezpečení vzájemné komunikace?

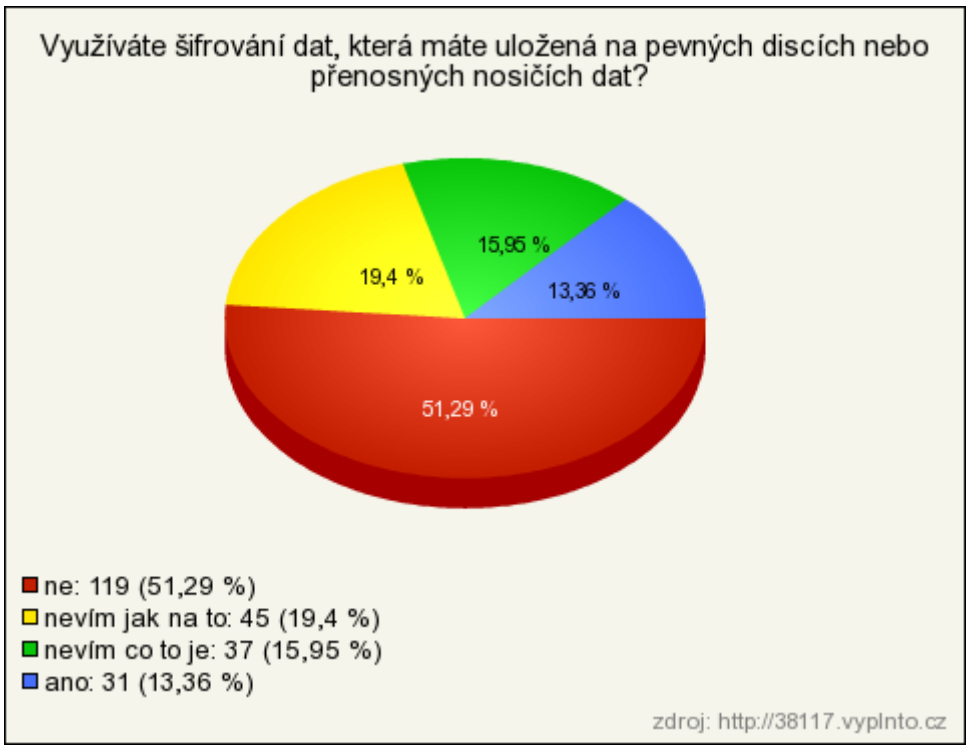
Tato otázka přímo navazuje na otázku předešlou a pouze zobrazuje rozložení odpovědí shrnutých výše.

Graf č. 12: *Grafické rozložení odpovědí na otázku č. 12*

Otázka č. 13: Využíváte šifrování dat, která máte uložená na pevných discích nebo přenosných nosičích dat?

Tato otázka byla do dotazníku vložena pouze za účelem zjistit, zda uživatelé využívají i například šifrování dat, která mají na svých úložištích. I tímto způsobem se mohou uživatelé bránit neoprávněnému zobrazení jejich obsahu, přestože se útočníkovi povede se dat zmocnit. Téměř 14% respondentů odpovědělo, že tuto možnost již využívá, což není úplně zanedbatelná část. Záporně odpověděla nadpoloviční většina (51%). Dalších dohromady 35% tázaných odpovědělo, že neví jak na to nebo neví co to je.

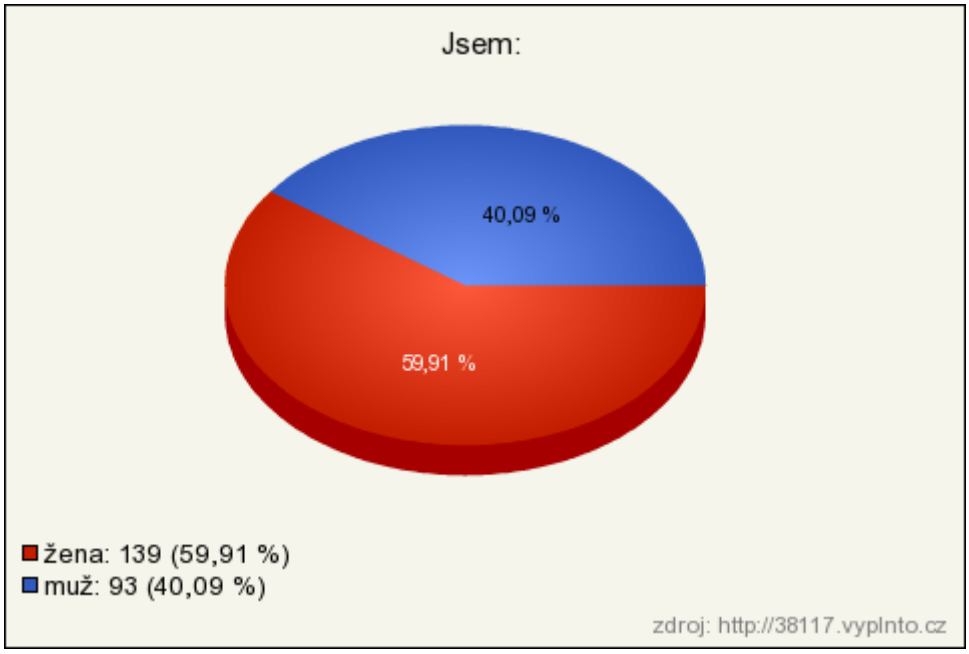
Graf č. 13: *Grafické rozložení odpovědí na otázku č. 13*



Otázka č. 14: Jaké je Vaše pohlaví?

Z celkového počtu 232 respondentů je 139 žen (59,91%) a 93 mužů (40,09%).

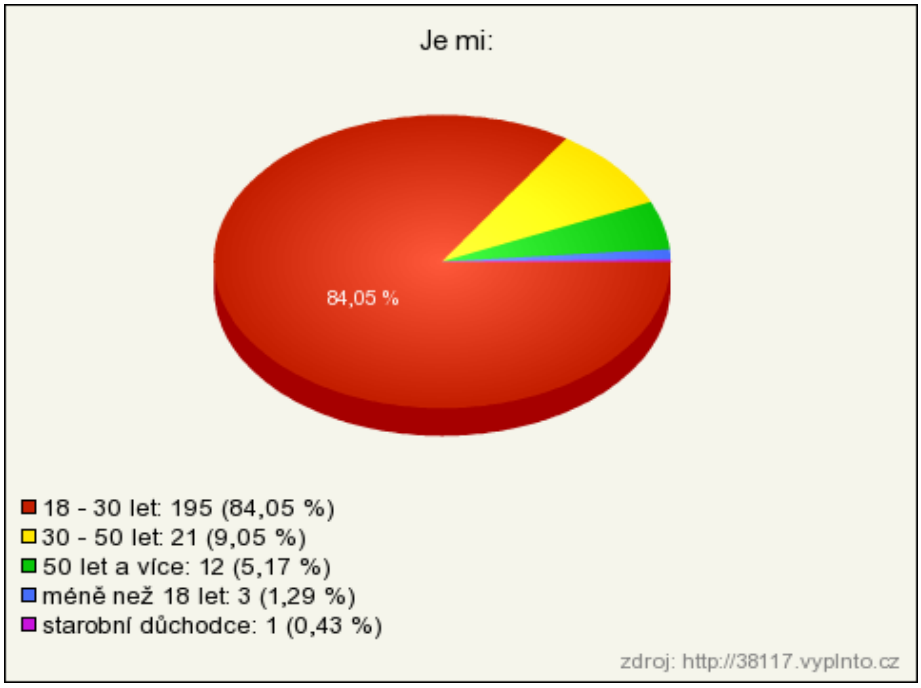
Graf č. 14: *Grafické rozložení odpovědí na otázku č. 14*



Otázka č. 15: Jaký je Váš věk?

V celém vzorku respondentů zaujímají majoritní postavení lidé mezi 18 až 30 lety věku (celých 84%). Zajímavostí je, že dotazníkového šetření se zúčastnil i jeden starobní důchodce. Z tohoto pohledu lze hovořit o vychýleném výběru vzorku respondentů. Prvotní předpoklad, že se podaří dotazník rozšířit rovnoměrněji mezi zvolené věkové skupiny, se z velké části nenaplnil. Dá se předpokládat, že při účasti více respondentů z dalších věkových skupin, by byly výsledky průzkumu značně odlišné.

Graf č. 15: *Grafické rozložení odpovědí na otázku č. 15*



Získávání respondentů probíhalo pomocí sdílení dotazníku na sociálních sítích, rozesílání e-mailem a ze zdrojů serveru Vyplnto.cz.

8.4 Testování hypotéz

V následující části se autor práce zaměřil na formulování a otestování 4 hypotéz souvisejících s dotazníkovým šetřením. Testování proběhlo metodou testu dobré shody (Pearsonův chí-kvadrát test).

K testování hypotéz je zapotřebí stanovit vždy dvě protichůdná tvrzení, tedy hypotézu H_0 (stanovena jako negativní ke skutečnosti, kterou se snažíme prokázat) a hypotézu H_1 potvrzující prvotní myšlenku.

1) Autor práce předpokládá, že využívání silných přístupových hesel k internetovým účtům mezi uživateli je závislé na pohlaví respondentů průzkumu. Stanoveny jsou následující hypotézy:

H_0: Používání silných hesel k internetovým účtům není závislé na pohlaví respondentů.

H_1: Používání silných hesel k internetovým účtům je závislé na pohlaví respondentů.

Kritická hodnota kritéria chí-kvadrátu (X^2) pro dva stupně volnosti (počet možných odpovědí) je $X^2_{0,95}$=5,99 s 5% pravděpodobností chyby 1. druhu.

Hodnota kritéria pro odpovědi ženského pohlaví byla stanovena na X^2=3,094.

Hodnota kritéria pro odpovědi mužského pohlaví byla stanovena na X^2= 4.575.

Z výsledků je patrné, že hodnoty kritérií obou pohlaví nepřesáhly kritickou hodnotu $X^2_{0,95}$. Závěrem tedy je, že se nepodařilo prokázat hypotézu H_1 - není statisticky prokazatelné, že využívání silných přístupových hesel je závislé na pohlaví respondentů.

2) Autor práce předpokládá, že využívání přídavného firewallu v operačním systému mezi uživateli je závislé na pohlaví respondentů průzkumu. Stanoveny jsou následující hypotézy:

H_0: Používání přídavného firewallu v operačním systému není závislé na pohlaví respondentů.

H_1: Používání přídavného firewallu v operačním systému je závislé na pohlaví respondentů.

Kritická hodnota kritéria chí-kvadrátu (X^2) pro tři stupně volnosti (počet možných odpovědí) je $X^2_{0,95}$=7,815 s 5% pravděpodobností chyby 1. druhu.

Hodnota kritéria pro odpovědi ženského pohlaví byla stanovena na X^2=7,99.

Hodnota kritéria pro odpovědi mužského pohlaví byla stanovena na X^2= 11,122.

Z výsledků je patrné, že hodnoty kritérií obou pohlaví přesáhly kritickou hodnotu $X^2_{0,95}$. Závěrem tedy je, že se podařilo statisticky prokázat hypotézu H_1 – je statisticky prokazatelné, že využívání přídavného firewallu v operačním systému je závislé na pohlaví respondentů.

3) Autor práce předpokládá, že využívání přídavného firewallu v operačním systému mezi uživateli je závislé na povaze provozované komunikace respondentů průzkumu (soukromá vs. pracovní). Stanoveny jsou následující hypotézy:

H_0: Používání přídavného firewallu v operačním systému není závislé na povaze komunikace respondentů.

H_1: Používání přídavného firewallu v operačním systému je závislé na povaze komunikace respondentů.

Kritická hodnota kritéria chí-kvadrátu (X^2) pro tři stupně volnosti (počet možných odpovědí) je $X^2_{0,95}$=7,815 s 5% pravděpodobností chyby 1. druhu.

Hodnota kritéria pro odpovědi s povahou komunikace soukromé byla stanovena na X^2=0,374.

Hodnota kritéria pro odpovědi s povahou pracovní komunikace byla stanovena na X^2= 0,337.

Z výsledků je patrné, že hodnoty kritérií u obou povah komunikace zdaleka nepřesáhly kritickou hodnotu $X^2_{0,95}$. Závěrem tedy je, že se nepodařilo prokázat hypotézu H_1 - není statisticky prokazatelné, že využívání přídavného firewallu je závislé na povaze provozované komunikace respondentů na internetu.

4) Autor práce předpokládá, že využívání silných přístupových hesel k internetovým účtům je závislé na povaze provozované komunikace respondentů průzkumu (soukromá vs. pracovní). Stanoveny jsou následující hypotézy:

H_0: Používání silných přístupových hesel k internetovým účtům není závislé na povaze komunikace respondentů.

H_1: Používání silných přístupových hesel k internetovým účtům je závislé na povaze komunikace respondentů.

Kritická hodnota kritéria chí-kvadrátu (X^2) pro dva stupně volnosti (počet možných odpovědí) je $X^2_{0,95}$=5,991 s 5% pravděpodobností chyby 1. druhu.

Hodnota kritéria pro odpovědi s povahou komunikace soukromé byla stanovena na X^2=2,455.

Hodnota kritéria pro odpovědi s povahou pracovní komunikace byla stanovena na X^2= 1,77.

Z výsledků je patrné, že hodnoty kritérií u obou povah komunikace nepřesáhly kritickou hodnotu $X^2_{0,95}$. Závěrem tedy je, že se nepodařilo prokázat hypotézu H_1 - není statisticky prokazatelné, že využívání silných přístupových hesel je závislé na povaze provozované komunikace respondentů na internetu.

Závěr

Hlavním cílem práce bylo zhodnotit míru povědomí běžných uživatelů sítě a internetu o možnostech zabezpečení jejich provozu a seznámit je se zásadami bezpečného chování u počítače. Práce seznamuje čtenáře i s problematikou elektronického podnikání a detailněji osvětluje tento obor, jakožto i jeho části, kterými nejsou pouhé elektronické obchody. V návaznosti na to je v práci popsána historie a vývoj kryptografie a kryptoanalýzy, od prvotních náznaků šifrování, až po dnešní sofistikované kryptografické systémy. Účelem práce nebylo vytvořit pro neznalé uživatele obsáhlý manuál pro zabezpečení provozu na internetu, jelikož dostupných možností a vybavení je celá řada. Obecně se předpokládá, že uživatel začátečník přenechá tuto činnost specialistovi v oboru, nicméně měl by disponovat alespoň základními znalostmi problematiky.

Dotazníkové šetření bylo provedeno na celkovém počtu 232 dotazovaných. Mezi respondenty převažovaly mírně ženy a zároveň byli nejčastějšími odpovídajícími lidé ve věku mezi 18 a 30 lety. Výsledky dotazníkového šetření jasně ukazují, že ani mezi mladými lidmi není úroveň povědomí a využívání zabezpečeného provozu na internetu na vysoké úrovni. Bohužel se pak tito uživatelé stávají snadnými terči pro počítačové zločince a jsou velmi často obtěžováni nevyžádanou reklamou. Za naprosto alarmující se dá považovat situace, kdy více než 10% respondentů dotazníkového šetření odpovědělo záporně na otázku, zda využívají antivirový software. Následující otázky dotazníku již zaznamenávají mnohem vyšší procenta záporných odpovědí ve smyslu využívání dalších bezpečnostních prostředků. Odpovědi na každou otázku jsou zpracovány do přehledných grafů a doplněny o komentáře.

Práce má napomoci čtenářům získat základní povědomí o bezpečnostních hrozbách na internetu, osvětlit problematiku elektronického podnikání včetně využívaných prostředků zabezpečení a poskytnout ucelený přehled o možnostech zabezpečení jejich provozu na síti a internetu.

Hlavním předpokladem pro vypracování práce bylo, že ono povědomí uživatelů o bezpečném provozu na internetu je nízké. Tento předpoklad se zcela jistě naplnil.

Dotazníkové šetření je zakončeno podkapitolou Testování hypotéz, kde autor formuloval 4 hypotézy týkající se závislostí odpovědí na dotazník. Závislost hypotéz byla otestována testem dobré shody a následně byla zformulována hodnocení.

Seznam obrázků a tabulek

Seznam tabulek

Seznam grafů

Seznam použité literatury

Odborná literatura

PETROVIČ, Michal; KOSTĚNEC, Michal. *Bezpečnost počítačových sítí*. Plzeň: Západočeská univerzita v Plzni, 214 s., 2012. ISBN 978-80-261-0117-8

SUCHÁNEK, Petr. *Podnikání a obchodování na internetu.* Opava: Slezská univerzita v Opavě, 223 s., 2008. ISBN 970-80-7248-458-4

SUCHÁNEK, Petr. *Elektronické podnikání a koncepce elektronického obchodování*. Praha: Ekopress, s.r.o., 144 s., 2012. ISBN 978-80-86929-84-2

ZELENKA, Josef; ČAPEK, Jan; FRANCEK, Jiří; JANÁKOVÁ, Hana. *Ochrana dat. Kryptologie*. Hradec Králové: Gaudeamus, 198 s., 2003. ISBN 80-7041-737-4.

KOISUR, David. *Elektronická komerce. Principy a praxe*. Praha: Computer Press, 267 s., 1998. ISBN 80-7226-097-9

DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Brno: Computer Press, 198 s., 2004. ISBN 80-251-0106-1

DOBDA, Luboš. *Ochrana dat v informačních systémech*. Praha: Grada Publishing, 286 s., 1998. ISBN 80-7169-479-7

SINGH, Simon. *Kniha kódů a šifer: Utajování od starého Egypta po kvantovou kryptografii*. Praha: Dokořán, 382 s., 2009. ISBN 978-80-7363-268-7

NORTHCUTT, Stephen; ZELTSER, Lenny; WINTERS, Scott; FREDERIC, Karen; RITCHEY, Ronald. *Bezpečnost počítačových sítí.* Brno: CP Books a.s., 589 s., 2005. ISBN 80-251-0697-7

BURDA, Karel. *Aplikovaná kryptografie*. Brno: Vutium, 255 s., 2013. ISBN 978-80-214-4612

CHROMÝ, Jan. *Elektronické podnikání: informace, komunikace, příležitosti*. Praha: Extrasystem, 263 s., 2013. ISBN 978-80-87570-10-4

Elektronické zdroje

ČERMÁK, Miroslav; ČERMÁKOVÁ, Dagmar. *CleverAndSmart*. [online]. [cit. 2014-04-01]. Dostupné na WWW: <http://www.cleverandsmart.cz >.

ROMANCOVÁ, Ingrid. *Šifrování e-mailů pro úplné začátečníky – Gpg4win*. [online]. [cit. 2014-04-01]. Dostupné na WWW: <http://www.evropsky-rozhled.eu/sifrovani-e-mailu-pro-uplne-zacatecniky-gpg4win/>.

Bezpečný internet. *Rizika on-line komunikace*. [online]. [cit. 2014-04-01]. Dostupné na WWW: < http://www.bezpecnyinternet.cz/zacatecnik/on-line-komunikace/rizika.aspx>.

ŠANDERA, Vladimír. *Odvirování počítače.* [online]. [cit. 2014-04-01]. Dostupné na WWW: <http://www.servisnaklik.cz/blog/odvirovani-pocitace/>.

Svět sítí & Infinity a. s. *Pravdy o elektronickém podpisu a šifrování.* [online]. [cit. 2014-04-01]. Dostupné na WWW: <http://www.svetsiti.cz/rubrika.asp?rid=17&tid=244>.

DEMČÁK, Marek. *Vyplňto.* [online]. [cit. 2014-04-01]. Dostupné na WWW: <http://www.vyplnto.cz/>.

Seznam příloh

Příloha A: Dotazník (Míra povědomí a užívání bezpečnostních prostředků na síti)

Příloha A: Dotazník (Míra povědomí a užívání bezpečnostních prostředků na síti)

1. Jak často komunikujete prostřednictvím sítě/internetu?

- ☐ několikrát denně
- ☐ několikrát týdně
- ☐ několikrát měsíčně
- ☐ téměř nikdy

2. Jaká je povaha Vámi provozované komunikace?

- ☐ soukromá
- ☐ soukromá i pracovní
- ☐ pracovní

3. Využíváte ke svým internetovým účtům silná hesla z hlediska zabezpečení?

(heslo neobsahuje běžná slova, obsahuje malá a velká písmena, číslice a ostatní znaky)

- ☐ ano
- ☐ ne

4. Slyšeli jste již někdy o možnosti bezpečné komunikace na internetu?

- ☐ ano
- ☐ ne

5. Využíváte antivirový software?

- ☐ ano
- ☐ ne
- ☐ nevím co to je

6. Využíváte přídavný FIREWALL ve svém operačním systému?

- ☐ ano
- ☐ ne
- ☐ nevím co to je

7. Využíváte vlastní bezpečnostní digitální certifikát?

- ☐ ano
- ☐ ne
- ☐ nevím co to je

8. Využíváte vlastního elektornického podpisu?

- ☐ ano
- ☐ ne
- ☐ nevím co to je

9. Využíváte možnost zabezpečení například e-mailové komunikace prostřednictvím veřejného a soukromého klíče?

(Slouží k tomu například veřejně dostupné nastroje jako jsou GPG4Win, Kleopatra, Enigmail a další)

- ☐ ano
- ☐ ne
- ☐ nevím co to je

10. Chtěli byste využívat bezpečnou, šifrovanou komunikaci na internetu?

- ☐ ano, zkusil/a bych to
- ☐ již využívám

☐ ne, je mi to jedno

11. Provozujete vlastní e-shop nebo jinou formu eletronického obchodování?

☐ ano

☐ ne

12. Kdo se stará o zabezpečení dat uživatelů Vašeho e-obchodu a zabezpečení vzájemné komunikace?

☐ nemám e-shop

☐ zřizovatel e-shopu, koupil jsem ho již hotový

☐ já sám, e-shop jsem si vytvořil

13. Využíváte šifrování dat, která máte uložená na pevných discích nebo přenosných nosičích dat?

(šifrovací nástroje jako je např. TrueCrypt)

☐ ano

☐ ne

☐ nevím co to je

☐ nevím jak na to

14. Jsem:

☐ muž

☐ žena

15. Je mi:

☐ 18 - 30 let

☐ 30 - 50 let

- ☐ 50 let a více
- ☐ méně než 18 let
- ☐ starobní důchodce

Zdroj: vlastní zpracování, 2014

Abstrakt

DYRŠMÍD, M. *Vývoj a užití kryptografie a kryptoanalýzy v elektronickém podnikání.* Bakalářská práce. Plzeň: Fakulta ekonomická ZČU v Plzni, 62 s., 2014

Klíčová slova: elektronické podnikání, kryptografie, kryptoanalýza, šifrování, internet, algoritmus, počítačová síť, bezpečnostní hrozby

Předložená práce je zaměřena na zabezpečení elektronického podnikání a provozu běžných uživatelů na síti a internetu. V první části práce jsou základní informace o elektronickém podnikání. Jsou zde uvedeny jeho součásti, jakožto rozsáhlého oboru. Dále jsou zde popsány návaznosti na tzv. novou ekonomiku. Další část práce se zaměřuje na historii a vývoj kryptografie a kryptoanalýzy, od daleké minulosti po současné kryptografické systémy. Pojednává také o konkrétním využití kryptografie v elektronickém podnikání. Poslední teoretická část práce se zaměřuje na popis bezpečnostních rizik provozu na síti a internetu. Zahrnuje přehled běžných hrozeb, kterým je vystaven každý uživatel počítače přistupujícího na internet. Přehled obsahuje popis škodlivého softwaru a také různé typy hackerských útoků. Praktická část obsahuje ucelený přehled možností, jak zabezpečit provoz uživatelů na internetu a obecná pravidla, jak se bezpečně chovat u počítače. Na tuto část navazuje průzkum, který zjišťuje míru povědomí běžných uživatelů internetu o možnostech zabezpečení jejich provozu.

Abstract

DYRŠMÍD, M. *Development and application of cryptography and cryptoanalysis in the electronical business.* Bachelor thesis. Pilsen: Faculty of economics, University of West Bohemia in Pilsen, 62 p., 2014

Keywords: electronical business, cryptography, cryptoanalysis, internet, algorithm, computer net, security threats

The submitted work focuses on securing of electronical business and operating of common users of computer net and the internet. The part one of the work contains the basic data about electronical business. As a wide branch, its parts, as well as descriptions of relationships to, so called, new economics, are included here. The part two deals with the history and development of cryptography and cryptoanalysis from its earliest history up to the cryptographical systems of the present time. It also deals with direct usage of cryptography in electronical business. The last theoretic part of the work aims to describe security threats of being on computer net and the internet. It includes a list of common threats for every user of PC connected to the internet. The list includes a description of malware and also different types of hackers attakcs.