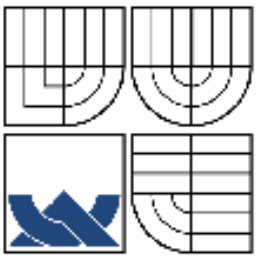
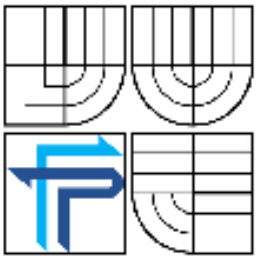


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA PODNIKATELSKÁ
ÚSTAV MANAGEMENTU

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF MANAGEMENT

BEZPEČNOSTNÍ RIZIKA ELEKTRONICKÉHO OBCHODOVÁNÍ

THE SECURITY RISKS OF E-COMMERCE

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. OLDŘICH BAUER
AUTHOR

VEDOUCÍ PRÁCE — prof. Ing. JIŘÍ DVOŘÁK, DrSc.
SUPERVISOR

BRNO 2009

Tato verze diplomové práce je zkrácená (dle Směrnice děkana č.4/2007). Neobsahuje identifikaci subjektu, u kterého byla diplomová práce vypracována (dále jen „dotčený subjekt“) a dále informace, které jsou dle rozhodnutí dotčeného subjektu jeho obchodním tajemstvím či utajovanými informacemi.

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2008/09
Ústav managementu

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bauer Oldřich, Bc.

Řízení a ekonomika podniku (6208T097)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává diplomovou práci s názvem:

Bezpečnostní rizika elektronického obchodování

v anglickém jazyce:

The Security Risks of E-commerce

Pokyny pro vypracování:

Úvod
Systémové vymezení problému
Cíl práce
Informační zdroje
Teoretická východiska práce
Analýza problému
Návrh řešení
Zdůvodnění návrhu
Závěr
Seznam použitých informačních zdrojů
Přílohy

Seznam odborné literatury:

DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. 1. vyd. Brno: Computer Press, 2006. 24 s. ISBN: 80-251-0106-1

JURMANOVÁ VOLEMANOVÁ, Věra. Digitální knihovny z pohledu autorského práva. 1. vydání. Brno: Masarykova univerzita, 2005. 66 s. ISBN 80 -210 -3646 -X.

FRIMMEL, Martin. Elektronický obchod: právní úprava. 1. vyd. Praha: Prospektrum, 2002. 312 s. ISBN 80-7175-114-6.

GRUBLOVÁ, Eva. Internetová ekonomika. Ostrava: Repronis, 2002. 88 s. ISBN 80-7329-000-6

RÁBOVÁ, Zdeňka. HANÁČEK, Petr. HRUBÝ, Martin: Prostředí pro modelování bezpečných systémů, In: Proceedings of NETSS06, Ostrava, CZ, MARQ, 2006, 39-42 s. ISBN 80-86840-06-9

Vedoucí diplomové práce: prof. Ing. Jiří Dvořák, DrSc.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2008/09.

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ Fakulta podnikatelská

L.S.

PhDr. Martina Rašticová, Ph.D.
Ředitel ústavu

doc. RNDr. Anna Putnová, Ph.D., MBA
Děkanka fakulty

V Brně, dne 25.3.2009

Abstrakt

Práce se zabývá bezpečnostními riziky ve firmě na nejmodernější úrovni a je zaměřená na rizika spojená s elektronickým obchodováním. Popisuje tyto technologie a podává ucelený pohled na bezpečnostní opatření, navrhovaná pro konkrétní firmu v praxi.

Abstract

This thesis is concerned with the security risks in company and it is oriented to risks connected with electronic commerce. It describes these technologies a gives comprehensive view to security risks, designed for concrete firm in practice.

Klíčová slova:

Elektronický podpis, šifrování, kryptologie, bezpečnostní rizika, elektronický dokument, internet, elektronický obchod, hrozby.

Key words:

Electronic signature, crypthology, encryption, electronic commerce, threats, internet, security risks, electronic document.

Bibliografický záznam

BAUER, O. *Bezpečnostní rizika elektronického obchodování.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2009. 108 s. Vedoucí diplomové práce prof. Ing. Jiří Dvořák, DrSc.

Čestné prohlášení

Prohlašuji, že jsem celou diplomovou práci zpracoval samostatně na základě uvedené literatury a pod vedením svého vedoucího diplomové práce. Prohlašuji, že citace použitých pramenů je úplná, a že jsem v práci neporušil autorská práva (ve smyslu zákona č. 121/2000 Sb. O právu autorském a o právech souvisejících s právem autorským)

V Brně dne 15.května 2009 . . . . . .

Bauer Oldřich

Poděkování

Tímto bych chtěl poděkovat **prof. Ing. Jiří Dvořákovi , DrSc.** za jeho věcné připomínky, rady a spolupráci na mojí diplomové práci.

Obsah

Úvod

Téma této diplomové práce jsem zvolil z několika důvodů. Jednak to byl můj zájem z oblasti informačních technologií, které se věnuji už několik let a kde vidím svoji budoucnost. Dále to bylo již dřívější zaměření na fakultě Podnikatelské, kde jsem se již v bakalářské práci věnoval okrajově i bezpečnosti elektronického obchodování.

Účelem této práce není přesně a technicky do nejmenších detailů popsat všechny možné technologie, které se využívají ve vztahu k bezpečnosti elektronického obchodování, ale je spíše úkolem popsat model jejich fungování a dále pak navrhnout jejich praktické využití. Mým záměrem bylo zasadit tyto technologie do kontextu s praxí ve firmě, kde jsem svoji diplomovou práci vypracovával. Dále je nutné zdůraznit, že na problematiku samotnou je pohlíženo manažersky, z pohledu řízení firmy. Všechny poznatky, ke kterým jsem se v průběhu zpracovávání této práce dostal byly a jsou nadále neustále konzultovány s majiteli firmy a i tímto je zaručena jejich praktická využitelnost.

1. Systémové vymezení problému

V dnešní vyspělé době se elektronické technologie používají doslova na každém kroku. Obklopují nás moderní elektronická média, používáme počítače ke své potřebě a k práci. Nakupujeme po internetu v elektronických obchodech a svoje peníze máme kdykoli po ruce v aplikaci pro internetové bankovnictví. Tyto všechny výše uvedené aspekty skýtají jedno velké mínus v podobě zabezpečení – bezpečnosti. Zabezpečení tvoří dnes velmi obsáhlou a velmi důležitou oblast elektronického obchodování. Zabezpečení je nutné na všech úrovních elektronického obchodování a při všech činnostech. Dále bude zřejmé, kde všude a proč je důležité zabezpečení. Nyní bych se rád na tuto problematiku zaměřil systémově. V dnešní době jsou z marketingových či výzkumných důvodů důležitá jakákoli data o koncovém uživateli či spotřebiteli. To je jeden z mnoha důvodů, proč chránit svoje soukromí a dbát na bezpečnost. Naším cílem je chránit naše osobní údaje, chránit naše soukromí, naše informace. Jak jsem již uvedl výše na pouhém jednom příkladu, marketingový výzkum placený obchodní značkou může být jedním z důvodů, proč se firma – nebo firmy – bude snažit získat informace o nás. Ty mají totiž dnes zcela zásadní význam. V tomto případě cílení reklamy na koncového zákazníka ze specifické cílové skupiny.

Dále se budu více zaměřovat na zabezpečení, které chrání nejen informace o nás, ale i samotné naše finance a budu hledat takový model zabezpečení, který umožní využívat naplno všechny možnosti, které dnešní doba nabízí a přitom mít jistotu, že náš elektronický obchod funguje bezchybně, že naše konto s firemními financemi je v bezpečí a že email, kterým komunikujeme s obchodními partnery nebude číst nikdo jiný.

Ve své práci popisuji problém na úrovni zabezpečení jednotlivých aplikací, které firma využívá ve svém elektronickém obchodování. Zaměřuji se na konkrétní hrozby a uvádím konkrétní opatření, která mají těmto hrozbám předejít.

2. Cíl práce

Cílem práce je identifikovat a popsat bezpečnostní rizika, která hrozí v oblasti elektronického obchodování malé firmy. Nedílnou součástí je pak stanovení jejich příčin a možných důsledků a navržení optimálního modelu zabezpečení, který těmto důsledkům v dostatečné míře předchází. Dílčím cílem je potom zhodnocení takových opatření jak z pohledu praktické využitelnosti v konkrétní firmě, tak z ekonomického hlediska.

3. Informační zdroje

3.1. Přehled norem pro řízení bezpečnosti

Zde uvádím výčet norem, které se vztahují k bezpečnosti a bezpečnostním rizikům.

- Metriky a indikátory pro vyhodnocování:
  ISO/IEC 27004 – Information security management measurements.

- Požadavky na management bezpečnosti informací:
  ISO/IEC 27001:2005 (BS 7799-2) Information security management systems

- Model bezpečnosti, části 1 až 4:
  ČSN ISO/IEC TR 13335-1:2004 Směrnice pro řízení bezpečnosti IT

- Hodnocení rizik informačních systémů:
  BS 7799-3:2006 Information security management systems – Part 3: Guidelines for information security risk management.

- Bezpečnost informačních technologií v bankovním sektoru:
  ISO/IEC TR 13569:2005 Banking and related financial services – Information security guidelines.

- Management bezpečnosti informací – soubor postupů:
  ČSN ISO/IEC 17799:2005 (ISO/IEC 27002) Informační technologie

3.2. Knižní publikace

Seznam knih a tištěných materiálů, které jsem využil ve své diplomové práci uvádím v příloze. Na tomto místě bych rád zmínil přínos knihy od autorů Pipera a Murphyho nazvané „**Kryptografie**“, která byla mým prvním krokem k základnímu poznání světa kryptografie a bezpečnosti obecně. Všem případným zájemcům ji mohu vřele doporučit.

3.3. Tištěné zdroje

Použité tištěné zdroje uvádím v kapitole Informační zdroje, následují pak i doporučené zdroje, ze kterých je možno čerpat další informace o této problematice.

3.4. Odborná periodika

Zde bych opět rád, kromě citovaných zdrojů v příloze, uvedl zdroj – internetové stránky Crypto-World: Novinky ze světa kryptologie, na stránkách http://crypto-world.info. Zde se každý může registrovat a následně jsou mu formou E-Zinu zasílány soubory ve formátu pdf na emailovou adresu. Jedná se o zaměření na bezpečnost, články jsou velice zajímavé i pro laika a velmi přínosné pro odbornou veřejnost.

3.5. Elektronické zdroje

Elektronické zdroje jsou dnes přirozeně nejvíce využívaným zdrojem. I přesto, podle mého názoru, je na jejich kvalitě co zlepšovat a stoupající počet čtenářů takových zdrojů by měl být výzvou pro každého z autorů. Obecně můžeme říct, že elektronické zdroje netrpí známým neduhem neaktuálnosti daného tématu či článku, problémem se však většinou stává jejich návaznost, nesrozumitelnost a také problematické citování takového zdroje, kdy je nutné údaje získávat složitými cestami.

3.5.1. Virtuální knihovny

Zde uvádím jen příklad velmi obsáhlých a zajímavých digitálních knihoven, další zdroje v této podobě jsou uvedeny v kapitole Informační zdroje.

- Národní knihovna ČR - dostupná z: http://www.nkp.cz.
- Městská zemská knihovna v Brně - dostupná z: http://www.mzk.cz.
- Síť knihoven a studoven VŠE - dostupná z: http://www.library.vse.cz.

3.5.2. Stránky zaměřené na bezpečnost, firemní stránky

- Informační systém veřejné správy
  http://www.isvs.cz/bezpecnost/

- Microsoft – Bezpečnostní technologické centrum
  http://technet.microsoft.com/en-us/security/default.aspx

- AVG – antivir, antispam, firewall
  http://www.grisoft.cz/

- McAfee, - antivir, anti-spam, firewall, šifrování
  http://www.mcafee.com

- CheckPoint– firewall, IDS, IPS, síťová řešení, VPN, řízení přístupu
  http://www.checkpoint.com

- PGP - softwarová ochrana dat, šifrování
  http://www.pgp.com/

4. Teoretická východiska práce

4.1 Kryptologie

4.1.1 Prostředí kryptologie pro obor e-commerce

Všechny technologie týkající se elektronického podpisu, elektronické podatelny a podobných stavějí svoje základní principy na technologii šifrování dat. Šifrování nějaké informace, nebo chceme-li nějakých dat využívá lidstvo již odnepaměti. Již odnepaměti se lidstvo snaží utajit nějaké zasílané či ukládané informace před zraky cizích lidí a zasadit se tak o svoji bezpečnost, v našem kontextu o bezpečnost svého podnikání. Jeden z největších rozmachů šifrování nastal během světových válek, kdy se většina velmocí snažila utajit strategické informace a kladla enormní důraz na vývoj metod, aplikovatelných v praxi, které by zaručily například přenos utajené zprávy, aniž by se o tom dozvěděli nepřátelé. Další obrovský boom v rozvoji šifrování nastal s rozvojem moderních technologií, které se začlenily do našeho každodenního života. [15]

S kryptologií těsně souvisí dva základní pojmy:

- **Autentizace** – je proces ověření identity
- **Autorizace** – udělení určitých práv a povolení aktivit.

Poznámka k dalšímu textu: jako šifrovaný text jsou dále uváděna i některá synonyma v odpovídajícím kontextu, jako například informace, zpráva, data, text, dokument. V každém případě je ale myšlena zašifrovaná informace, která má být tajná a neveřejná.

4.1.2. Kryptologie jako věda

Kryptologie se zformovala ve samostatný vědní obor. Někdy se označuje jako kryptografie a tyto dvě disciplíny je možné volně zaměnit. Obecně můžeme říci, že je to nauka o metodách, které se používají při utajování zpráv, v tomto smyslu při převodu do podoby, která je rozluštitelná za použití jistého algoritmu nebo s využitím speciálních znalostí.

Základním pojmem je zde tedy samotná šifra, v širším pojetí šifrovací algoritmus, který zprávu převede do zašifrované podoby a naopak. Je to matematická metoda, využívající šifrovacího klíče jako prostředku k „otevření“ zašifrované zprávy. Tento šifrovací klíč je v celém postupu poměrně zásadní, protože pouze s jeho pomocí je možné zjistit podobu zašifrované zprávy. Z výše uvedeného je patrné, že obě komunikující strany, v našem případě například obchodní partneři, musí mít daný klíč k dispozici, aby bylo možné zprácu či informaci správně zašifrovat a na druhé straně, aby adresát – příjemce – neměl problém s jejím přečtením. K této proceduře, dnes již značně automatizované, se využívají dva základní druhy šifrovacích algoritmů. [15]

Z výše uvedeného už lze vycítit důležitost této techniky nejen v oboru kryptografie, ale v celém systému bezpečnosti elektronické komunikace. Je to mnohaletý vývoj, který dal vzniknout velmi zajímavým a sofistikovaným metodám, které se dnes běžně v oblasti zabezpečení využívají. Na úvod bych zde rád také zmínil jednu zásadní, neoblíbenou, ale zcela jistě již ověřenou skutečnost: **žádná šifra není neprolomitelná, žádné zabezpečení není stoprocentní.** Jde jen o prosté vyčíslení sil a nákladů, které je nutné vynaložit k jejímu prolomení a potom už je na straně „hackera“ či podobné osoby, aby bilancoval. O tomto tématu a jeho významu v oblasti e-commerce se zmíním ještě v dalších kapitolách.

Důležitým poznatkem zde je, že šifrovaní se zabývá utajením, ochranou určitých informací před nepovolanými osobami, které by měly zájem tyto informace získat.

4.1.2.1. Symetrické šifrování

Jako první bych rád popsal technologii symetrického šifrování. Symetrická šifra, jednoduše řečeno, je taková šifra, kde se k jejímu zašifrování i rozšifrování používá stejný klíč. Základní schéma využití symetrického šifrování je vcelku jednoduché. Dvě strany, které spolu komunikují se rozhodnou, že předmětem jejich komunikace bude zašifrovaná zpráva, tedy například dokument, který nemá být veřejný. Důležité tady je, že není účelem utajit, že zpráva byla zaslána, ale utajit její obsah. Tyto dvě strany se tedy domluví na využití konkrétního šifrovacího klíče. Jedna strana komunikace – komunikant – tuto zprávu zašifruje pomocí šifrovacího klíče a stejně tak strana druhá, zprávu pomocí stejného klíče rozšifruje.

Tento postup je schématicky velmi jednoduchý. Základní a velmi důležitou skutečností zde je, že šifrovací klíč znají jen tyto dvě strany a nikdo jiný. Problematická se situace stává v případě, že do komunikace vstupuje více osob – subjektů. Zde platí, že všechny zúčastněné strany v komunikaci musí mít přístup k tomuto klíči. Tím se velmi podstatně zvyšuje riziko prozrazení šifrovacího klíče a komunikace se stává rázem nešifrovanou – veřejnou. Takovou komunikaci, kde selhala nějaká bezpečnostní opatření nazýváme také „otevřenou“. Symetrické šifrování obecně se často používají dohromady se šiframi asymetrickými, k dosažení vyšší efektivity. Symetrické šifry využívají ve většině případů dva základní postupy. Substituční a transpoziční. Jak už název napovídá, substituční spočívá v náhradě (záměně) znaků zprávy podle určitého systému – algoritmu. Tento algoritmus nazýváme také „tabulka šifrovacího klíče“. U transpozice dochází naproti tomu k záměně v pořadí jednotlivých znaků. V současné době známe velké množství různých algoritmů, kde mezi nejznámější patří algoritmy AES, DES, IDEA, CAST a BLOWFISH. Algoritmus DES byl vyvinut v USA v průběhu sedmdesátých let. Tento algoritmus se stal na několik let normou pro šifrování po celých USA. Díky moderním technologiím byl brzy prolomen a zůstal tak otevřený. Z tohoto důvodu byla vytvořena varianta 3DES, kde jsou data několikrát po sobě šifrována před odesláním, aby byl zaručen vysoký bezpečnostní standart. [16]

Z výše uvedeného začíná být patrné, že v extrémně rychle se vyvíjející době symetrické šifrování jednoduše nestačí pokrýt požadavky trhu a proto se začíná využívat šifrování asymetrické.

4.1.2.2. Asymetrické šifrování

V dobách rozvoje šifrování samotného museli inženýři dbát na jednoduchost a hardwarovou nenáročnost takových postupů. Symetrické šifrování vysvětlené výše bylo velmi jednoduché, ale zároveň velmi nespolehlivé a nedokázalo odolat nárokům na bezpečnost. Proto bylo vyvinuto šifrování asymetrické. U asymetrického šifrování je možnost prozrazení výrazně nižší, ale zase se zde zvyšuje náročnost na hardwarové a softwarové vybavení komunikujících stran a tím se proces šifrování zpomaluje.

Nyní charakterizuji samotný algoritmus asymetrického šifrování. Každá ze stran, zapojená do komunikace si vytvoří takzvaný šifrovací pár neboli klíčový pár. Tento klíč – pár – obsahuje dva klíče**: klíč veřejný a klíč soukromý**. Soukromý klíč je jednoznačným tajemstvím vlastníka a není určen pro nikoho jiného. Naproti tomu klíč veřejný, je veřejně přístupný a přístup k němu mají všechny zainteresované strany, které využívají šifrovaní například u některé z certifikačních autorit. (viz. dále) Při využití tohoto páru se postupuje tak, že se zpráva šifruje klíčem veřejným a dešifruje klíčem soukromým. Tohoto postupu se využívá zejména proto, že zašifrovaná zpráva se dešifruje pouze soukromým klíčem. Z toho vyplývá jedna základní vlastnost: nelze využít jednoho klíče k oběma operacím, jak by se nabízelo. Při šifrování se totiž využívá takových matematických postupů, které se nedají provést zpětně, respektive se nedá provést jejich reverze. V tomto smyslu je nejčastěji používaným algoritmem RSA a ECC. RSA podle autorů Rivesta, Shamira a Adlemana. U tohoto algoritmu je stupeň jeho bezpečnosti závislý na délce klíče, který byl využit. V elektronickém obchodování, při využití elektronického podpisu se běžně využívají **klíče s délkou 1024 bitů**. tento algoritmus vznikl v roce 1977. Prolomení spočívá ve schopnosti útočníka řešit matematické úlohy složitějších typů, konkrétně faktorizace velkých čísel. Ve srovnání s výše uvedenými RSA a DES algoritmy je ECC výrazně pomalejší, ale také výrazně

bezpečnější. Při softwarových operacích je to asi sto násobně a při hardwarových realizacích je to asi 1000 až 10 000 násobně. [16]

4.1.2.3. Hybridní – Kombinované šifry

Pokrok doby a technik hackerů a dalších útočníků si vyžádal další vývoj technik, využívaných pro šifrování. Začalo se tedy s kombinací obou zmiňovaných postupů. Byly vyvinuty takzvané hybridní neboli kombinované šifry. Logicky kombinují **symetrické a asymetrické šifrování**. Je nutné zmínit, že je to opět kompromisní řešení mezi bezpečností u šifrování asymetrického a mezi rychlostí u šifrování symetrického. Nedostatky jednoho typu doplňují přednosti druhého a naopak. Velká hardwarová náročnost asymetrického šifrování tento proces výrazně urychlila a vznikl následující postup: tajná zpráva se zašifruje jednodušším symetrickým šifrováním, které vytvoří svůj náhodný klíč. Tento byl nově vygenerován a je jedinečný pro každou novou operaci. Tento se posléze zašifruje pomalejším asymetrickým šifrováním a vše se uloží do jednoho datového balíčku. Celý tento balík – packet – se odešle příjemci, kde se rozšifruje symetrické klíč – tedy velmi rychle – a následně samotná tajná data – bezpečně. Tak byli splněny obě základní podmínky, které jsou na šifrování kladeny v praxi. Lze konstatovat, že tento postup využívá většina programů, které využívají asymetrické šifrování. [15]

4.1.2.4. Rozdělení šifrování

Na rozdělení šifrování lze pohlížet i z jiného úhlu. Jako jednosměrné šifrování označujeme postup, kdy se data zašifrují, bez možnosti tento stav zvrátit. Při tomto šifrování se nepoužívá žádného klíče. Tento se využívá například při otisku dat v databázi nebo při ukládání otisku dat kvůli ověření jejich pravosti. Jak je patrné, patří mezi hashovací funkce – vytváří se jednoznačný nezaměnitelný otisk, z kterého nelze zpětně získat původní data. Obousměrné šifrování naproti tomu označuje postup, kdy jsme schopni při znalosti správného klíče zprávu dešifrovat a získat tak původní zprávu. [62]

4.1.2.5. Hash algoritmus

Všeobecně je Hash algoritmus známá funkce, využívaná v souvislosti elektronickým obchodováním. Pracuje na matematickém principu, matematické funkci. Podstata spočívá v tom, že v jednom takzvaném přímém směru spočítáme funkci naprosto jednoduše, ale naopak, ve směru inverzním je tento výpočet prakticky nemožný. Výsledkem je 128 nebo 160 bitů dlouhá sekvence, která jednoznačně definuje vstupní data jako například dokument, textový soubor a podobně. Pokud by se v těchto původních datech změnil byť jen jeden jediný bit, jejich hash funkce se výrazně změní.

Nyní bych zde rád uvedl několik základních a nejpoužívanějších HASH funkcí:

- SHA-1 – oblíbená, ale již prolomená funkce. V únoru 2005 byl zveřejněn objev postupu, který umožňuje nalézt kolizi podstatně rychleji než pouze silou, na základě matematických výpočtů. Tento postup však vyžaduje velmi výkonný hardware a potom se zase uvažuje o bilancování mezi náklady a ziskem z prolomení.

- **SHA-2 –** rodina 4 hašovacích funkcí (SHA-256, SHA-384, SHA-512 a SHA-224), které jsou součástí standardu FIPS 180-2. U těchto do dnešní doby nebyly nalezeny žádné výrazné bezpečnostní slabiny.

- MD5 – oblíbená, ale již bezpečnostně prolomená funkce. Od srpna 2004 je veřejně znám postup pro nalezení kolizního páru zpráv, takže není možné ji využít v praxi. [31]

4.1.3. Kryptoanalýza

Kryptoanalýa je vědní obor, který se zabývá metodami, jak získat obsah šifrovaných zpráv, ale bez přístupu k utajovaný informacím, tedy k soukromému klíči, který je potřeba pro dešifrování. Obecně lze říci ,že kryptoanalýza je prolamování kódu a kryptografie tento kód naopak vytváří. Člověk zabývající se kryptoanalýzou je potom kryptoanalytik. Vývoj kryptoanalýzy jako samotné vědy vychází prakticky z vývoje kryptografie, kdy vzniká přirozená potřeba zašifrovaný text dešifrovat a to nejen svůj, ale také cizí, chceme-li soukromý. Logicky se dešifruje buď samotná zpráva nebo pouze soukromý klíč, který byl použit k jejímu zašifrování. Tento potom samozřejmě slouží stejně dobře k vyluštění samotné zprávy. Tento typ zneužití se obecně označuje jako **attack – útok** (na šifru, algoritmus). Firma se proti těmto technikám samozřejmě musí bránit a to cestami uvedenými v návrhové části práce.

Rozlišujeme několik typů útoků:

- Útok hrubou silou – jednoduché procházení všech možných šifrovacích klíčů a možností za pomocí vysoce výkonné techniky, jak již bylo zmíněno, vysoce hardwarově náročné.

- Dešifrování s pomocí šifrovaného textu, kdy se analyzuje několik zašifrovaných textů, které mají stejný klíč a šifrovací algoritmus, poměrně nepřesná metoda.

- Dešifrování za pomoci znalosti otevřeného textu, kdy se klíč získává z otevřených – nešifrovaných dokumentů.

- Dešifrování za přispění uživatele. Klíč je získáván násilím, nelegálními technikami nebo také přesvědčováním, špionáží. Tento postup v posledních několika letech získává opět na významu, protože mnoho lidí si zvyklo na vysoké zabezpečení v elektronickém světě, ale začali opomíjet nebezpečí bezprostřední. [1]

4.2. Elektronický podpis

4.2.1. Úvod do problematiky

Elektronický podpis je jedna z technologií, která by měla ulehčovat práci v dnešním trendu digitalizace současného světa. Jedná se zde nejen o firmy a instituce, ale i o problémy běžných občanů. Dnes se v elektronickém obchodování nebo v elektronické komunikaci vyžaduje několik standardů, které zabezpečují její využitelnost a bezpečí komunikujících stran. V mnoha případech je vyžadováno pevné svázání s jednou právnickou či fyzickou osobu. Elektronickým podpisem musí být jednoznačně zajištěno, aby tento dokument byl nepopiratelný, tedy musí být jednoznačně prokazatelné od koho pochází. Dále se vyžaduje pravdivost – v tomto smyslu myslíme, že to co je uvedeno v dokumentu nebylo změněno bez vědomí vlastníka. Tyto základní funkce využití elektronického podpisu se týkají především různých listin, které mají právní hodnotu. Dnes je velice důležité vyznat se ve spleti lidí a skupin, které útočí prostřednictvím internetu na naše soukromí a snažit se je tímto postupem identifikovat a zneškodnit, v horším případě alespoň výše uvedené listiny označit za upravené, zkopírované nebo neautentické. Elektronický podpis má proti sobě silně motivované chytré jedince, kteří se snaží nějakou cestou obohatit a proto je mu přikládán takový význam. Rád bych zde zmínil ještě několik dalších funkcí elektronického podpisu. [27]

Jedná se zejména o **identifikaci** (také označovanou jako autentifikace) **osoby**, která přikládá elektronický podpis, dále pak je to nepopiratelnost – osoba nemůže popřít, že podepsaný dokument odeslala. Jakmile je tedy dokument digitálně podepsán, jejím autorem je zcela jistě podepsaná osoba. Další vlastností je **integrita** – tato vlastnost nám říká, že dokument nebyl změněn ani v průběhu přenosu k příjemci. Poslední základní vlastností je právní **akceptovatelnost** – chceme-li elektronický podpis využívat, je nutné jej zakotvit v zákoně a upravit jeho používání příslušnými právními normami.

4.2.2. Technologie elektronického podpisu

4.2.2.1. Elektronický podpis

Elektronický podpis se v zásadě skládá ze dvou součástí: jednak je to hash funkce a dále pak asymetrická šifra. Hash algoritmus se používá na každý dokument samostatně a vždy je vypočítán jeho řetězec – v tomto smyslu jako sled po sobě jdoucích čísel. Tento hash algoritmus se asymetricky zašifruje soukromým klíčem, kdy dojde k naprostému zabezpečení a zároveň nám vznikne i digitální otisk dokumentu, zaručující všechny základní funkce popsané výše. Příjemce zprávy od nás dostane samotný dokument s elektronickým podpisem, který obsahuje kromě názvu a typu certifikační autority i zvolený asymetrický algoritmus. Po použití veřejného klíče a tohoto algoritmu vznikne takzvaný otisk. Následně dešifruje elektronický podpis a dostane náš hash. Dalším krokem je porovnání hash odesílatele a příjemce a pokud jsou tyto shodné, je patrné, že dokument nebyl na cestě změněn a že ho odeslal právě podepsaný člověk, kterému patří veřejný klíč. Pokud je však elektronický podpis založen bázi certifikátu, je tento zasílán s dokumentem příjemci, kde jsou uvedeny osobní údaje odesílatele a veřejný klíč – využívá se často v komunikaci s institucemi, kdy se tyto dvě strany „vzájemně neznají“. [43]

Zjednodušeně lze říci: nejdříve odesílatel chce odeslat dokument příjemci. Odesílatel jej opatří elektronickým podpisem a odešle. Ten, kdo ho dostane ověří, jestli elektronický podpis v něm uvedený náleží podepsanému odesílateli a také jestli text nebyl v průběhu změněn – jestli k sobě dokument a podpis opravdu patří. Toto vše během zlomku sekundy. Tento postup a všechny algoritmy ve skutečnosti provádí speciálně vyvinutý software, často implementovaný do prostředí internetu, webových rozhraní. Za pomocí toho softwaru je podepsání nebo přečtení podepsané zprávy úplně jednoduché a uživatelsky nenáročné.

4.2.2.2. Časové razítko

Časové razítko má jednu jedinou funkci, kterou elektronický podpis neoplývá a to je časové rozlišení. Pro přesné ověření platnosti a důvěryhodnosti jsou tyto informace velice důležité. Razítko poskytuje samo o sobě informaci kdy bylo vytvořeno a kdo jej vytvořil. Razítko vydává takzvaná časová autorita a razítko se běžně doplňuje k podepsané zprávě, resp. ke jejímu otisku. Časový údaj doplní autorita podle UTC – Světového koordinovaného času. Poté je dokument klasicky digitálně podepsán a odeslán příjemci, který zkontroluje digitální podpis a i časové razítko. Toto razítko lze však využít nejen jako příloha k digitálnímu podpisu, ale i k jakémukoli jinému souboru. [39]

4.2.2.3. Elektronická značka

Elektronická značka se velmi podobá elektronickému podpisu. Elektronická značka se naproti elektronickému podpisu využívá spíše v paušálním označování podepsaných dokumentů a využívají ji spíše instituce a úřady. jedná se o rychlejší, levnější a postačující řešení, například při rozesílání soudních obsílek apod. Dá se využít v soukromé praxi při rozesílání informací o reklamacích, kde jsou citlivá data dostatečně chráněna a také při rozesílání reklamních materiálů, ovšem nespamových typů. Využívá se především u velkého množství dokumentů, hlavně u e-podatelny, katastru nemovitostí nebo u soudních obsílek. Podstatný rozdíl je pouze v právní definici, kdy elektronický podpis vytváří soukromá – fyzická osoba, elektronickou značku vytváří právnická osoba a tato značka zde slouží podobně jako razítko ve fyzické podobě například na úřadě. [39]

4.2.3. Certifikáty

4.2.3.1. Certifikát

Certifikace, někdy označovaná jako ověřování, je proces, sloužící k zabránění získání veřejných klíčů ze strany útočníků, respektive do jejich databáze. Z tohoto důvodu jsou všechny veřejné klíče certifikačních autorit certifikovány a tak je potvrzena autentičnost těchto klíčů a tím se uživatel ujišťuje, že daný klíč patří skutečně uvedené certifikační autoritě, popřípadě konkrétní osobě. V této podobě získává elektronicky podepsaný dokument příjemce s přílohou, kde je uvedena certifikační autorita a také s ověřením, že tato autorita je důvěryhodná. [42]

Certifikáty se dělí podle druhu a obsahu a z toho je odvozen i jejich obsah.

Každý certifikát obsahuje minimálně tři části:

- podepsaný veřejný klíč.
- certifikační informace: identifikátor vlastníka veřejného klíče , dobu platnosti certifikátu, jméno certifikační autority.
- jeden nebo více elektronických podpisů certifikační autority. [42]

Nyní bych rád prakticky popsal získání certifikátu, k vytvoření elektronicky podepsaného dokumentu. Vycházíme z modelové situace, kdy tento certifikát chce získat běžný uživatel. Praxe ukázala, že získání elektronického podpisu ve firmě je principielně stejné. Uživatel si tedy v první řadě vytvoří dvojici soukromého a veřejného klíče. Následuje doručení veřejného klíče certifikační autoritě (v mém případě Česká pošta,s.p.) a tato autorita po ověření totožnosti vydá uživateli certifikát. Soukromý klíč naproti tomu zůstává neustále utajen a v rukou uživatele a dokonce ani certifikační autorita nezná jeho podobu. Vydaný certifikát ověřuje pouze sounáležitost veřejného a soukromého klíče, tedy že jej vytvořila jedna a ta samá osoba. Tento vztah se také nazývá veřejný klíč – identifikátor vlastníka. Bereme-li v úvahu více uživatelů

v uvedené skupině musí být tato identifikace dostatečně prokazatelná a k tomu slouží až znalost soukromého klíče, v tomto případě je to schopnost rozšifrovat zprácu pomocí veřejného/soukromého klíče. Vydaný certifikát jako jednu z důležitých bezpečnostních opatření obsahuje informaci o době platnosti a to i s možností okamžitého zrušení platnosti. Této možnosti uživatel využije, pokud je vyzrazen nebo prolomen jeho soukromý klíč. Tento úkon s nazývá **revokace**. Následuje informování komunikujících stran o jeho zneplatnění. [42]

Dva nejpoužívanější typy certifikátů a způsob jejich revokace:

1. Standard ITU-T se stará z hlediska jednotné mezinárodní normalizace o celou řadu oblastí komunikačních sítí. Standard ITU-T X.509 je částí série doporučení X.500 definujících adresářově vazby a na ně navazující služby. Jedná se zejména o databáze o uživatelích a jejich činnostech, kde lze získat marketingově důležitá a citlivá data, kam se mimo jiné ukládají i certifikáty. Podle normy X.500 jsou záznamy uspořádány do stromu odrážejícího organizační strukturu systému s tím, že certifikační autorita vydává pravidelně seznam podepsaných a revokovaných certifikátů. Každý certifikát je opatřen sériovým číslem, datem a číslem certifikace, popřípadě revokace. Uživatel potom automaticky ověřuje přítomnost využívaného certifikátu na seznamu revokovaných certifikátů. [42]

Ještě bych zde rád zmínil další specifikované technologie z hlediska jednotné mezinárodní normalizace:

- fax (T.2 - T.4, T.30, T.37, T.38),
- telefonní síť: číslovací plán
- paketová síť: X.25,
- bezpečnost: PKI (Public Key Infrastructure; X.509),
- multimédia: kódování obrazu (JPEG: řady T.80 a T.800), kódování zvuku (řady doporučení G.711 a G.72x), kódování videa (H.262/MPEG2-Video, H.264/AVC), VoIP (rodina kolem H.323),

- optická síť: SDH (G.707 - G.803) a pasivní optická síť (PON: G.983.1, G.984.1/2). [59]

2. Systém PGP (Pretty Good Privacy) sloužící pro autentizaci šifrování a emailové komunikace. Systém PGP využívá pouze asymetrické šifrování pro vytvoření elektronického podpisu zprávy nebo i pro utajení soukromého klíče. Využívá nejednotný model při autentifikaci veřejných klíčů, který nedůvěřuje obecně žádné certifikační autoritě. Každý uživatel v systému PGP může vystupovat jako certifikační autorita a potvrzovat jiné klíče podle svého uvážení. Každý uživatel si svobodně volí, komu důvěřuje a komu nikoli a následně tak vzniká zaručený systém označovaný jako **pavučina důvěry** (anglicky označovaný jako*: the web of trust*). [28]

4.2.3.2. Certifikační autorita

Certifikační autoritou rozumíme organizaci, vydávající elektronické certifikáty, které dále využívá druhá strana. Tato certifikační autorita, jak již jsem zmínil například v kapitole 4.2.3.1. to dělá za úplatu, k dosažení zisku. Předpokladem úspěchu takové autority je její důvěryhodnost. Certifikační autorita vlastní soukromý klíč, který utajuje a veřejný klíč, který zveřejňuje a je k nalezení například na webových stránkách takové autority. V případě firem, obchodujících nebo komunikujících převážně prostřednictvím elektronických obchodů jde ještě o vyšší typ zabezpečení, který nabízí takzvaný **kvalifikovaný certifikát.** Je to certifikát, pomocí kterého lze vytvořit zaručený elektronický podpis. Tento podpis je verifikován pouze v případě, že je v souladu se současnými zákonnými úpravami a s dalšími předpisy, které upravují tuto problematiku a opět musí být spojen s jednou jedinou osobou.

Nejvyšší zabezpečení nabízí akreditovaný poskytovatel certifikačních služeb. Ten vydává kvalifikované certifikáty, ale bezpečnější. Tyto certifikáty jsou podrobeny přísnějším kontrolám již při ukládání dat a vydávání. Vlastník takového certifikátu může podepsat úřední listinu a další dokumenty, jako by je podepsal fyzicky. Certifikační autorita tohoto typu však vyžaduje akreditaci státu a s touto akreditací teprve může digitálně podepisovat. [30]

V současné době v České republice působí tyto certifikační autority:

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

V České republice také působí 3 akreditované certifikační autority:

- Česká pošta s.p.
- eIdentity a.s.
- První certifikační autorita a.s. [55]

Každá firma nabízející certifikační služby nabízí i jiné produkty, které se dají s elektronickým podpisem zkombinovat a to nejen pro běžné uživatele, ale i firmy. Ještě zde bych rád zmínil, že legislativu týkající se elektronického podpisu ošetřuje v České republice Zákon č. 227/2000 Sb. O elektronickém podpisu a některé další právní úpravy. Upravuje podmínky pro jeho využití, nabízení, podmínky pro vydávání, uchovávání a nakládání s elektronickým podpisem samotným. Každé certifikační autoritě náleží jedna registrační autorita, prakticky část firmy, která má oprávnění kontrolovat a zjišťovat totožnost zájemců o elektronický podpis. [44]

Moje vlastní zkušenost se získáním svého osobnímu elektronického podpisu u certifikační autority. Jedná se o společnost 1. Certifikační autorita.

Na internetových stránkách jsem si vybral požadovaný certifikát, nainstaloval jsem si potřebné komponenty do počítače a stáhl další součásti.Vše probíhalo zatím automaticky. Většinou se jedná o komponenty prvků Active X a Kořenový certifikát 1. Certifikační autority (dále jen 1.CA). Na disku se vytvoří speciální adresář – složka – kam se automaticky instalují potřebné soubory. Původní nastavení je do :\Program Files\I.CA web komponenty. Následně nás systém registrace požádá o zadání všech osobních údajů a potvrzení žádosti o vytvoření soukromého klíče. Obratem po předběžném schválení žádosti systémem jej obdržíme potvrzený a tento klíč si zálohujeme na svém počítači. Následuje odeslání této žádosti kompletně na pobočku 1. Certifikační autority. Posledním krokem k získání je osobní přítomnost na jedné z poboček, kde nám při předložení dokladu totožnosti potvrdí, že registrovaná osoba jsme skutečně my a že zadané údaje souhlasí. Tímto krokem nabývá certifikát platnosti a uživatel ho může okamžitě využívat. Samozřejmostí, kterou jsem ani nezmiňoval je zaplacení. Většinou se jedná o položky do 500,-Kč. Neméně důležitým prvkem hotového díla je smlouva o využívaní certifikačních služeb, obsahující všechny potřebné údaje, stejně jako smluvní a všeobecné podmínky a podmínky pro využívání, ztrátu popřípadě generování certifikátů. Někdy se přikládá i takzvané bezpečností pole s PIN kódem, popřípadě s přihlašovacím jménem a PIN kódem. Důležité údaje jsou v části, kde se popisuje, jakým způsobem se uživatel musí zachovat, ztratí-li někde přihlašovací údaje, nebo je-li vyzrazen jeho soukromý klíč. (Musí vše samozřejmě nahlásit certifikační autoritě, která jej umístí na Seznam zneplatněných certifikátů – CRL – anglicky *Certificate Revocation List*)

4.2.3.3. Bezpečné uložení klíčů a certifikátů

Jak jsem již zmínil, ze systémového hlediska lze říci, že největším problémem, jak se v praxi ukázalo, není prolomení šifrování samotného nebo objevení či prolomení soukromého klíče, ale je to právě bezpečné uložení soukromých klíčů a certifikátů, které způsobuje obrovské bezpečnostní trhliny v bezpečnostní strategii firmy. Ve firmě, kde jsem zpracovával tuto diplomovou práci jsem zjistil, že jak zaměstnanci

v soukromí, tak ve firemním prostředí byly certifikáty a všechny soubory týkající se elektronického podpisu, volně na pevném disku a ještě k tomu umístěny v jednoduchém umístění, například přímo na ploše. Největší chybou je zaznamenávání samotných hesel nebo PIN kódů například do souboru ve formátu .txt přímo do složky, kde je umístěn soukromý klíč.

Jednou z osvědčených možností se ukazuje **šifrování souborů** přímo na disku, resp. přesun šifrovaných souborů například na flash disk. Jedním z programů sloužících k šifrování souborů je program BestCryp, který vytvoří transparentní vrstvu mezi programem a místem na disku. Tento přechod potom zajišťuje šifrování dat při zapisování a dešifrování při čtení. Program využívá virtuální disky, nazývané kontajner, fyzicky reprezentované souborem. Pokud se jedná o šifrování samotné, je zabezpečení na vynikající úrovni. Programy využívají čtyř známých algoritmů: GOST, TWOFISH a BLOWFISH a DES. GOST je nepříliš známý algoritmus užívaný v bývalém Sovětském svazu, TWOFISH a BLOWFISH jsou vynikající a známé algoritmy užívané i v jiných programech. DES je známá verze šifrovacího systému, která je však již dnes považovaná za méně nebezpečnou díky malé délce klíče – 56 bitů. [62]

Další programy, využívané pro šifrovaní souborů na počítači: X-key Lite (http://ese.asultsoft.info/uvod.php) , FileCryptor (http://filecryptor.boolean.cz/). Oba dva jsou použitelné jako freeware. Často využívanou možností je ještě využití programů jako například archivátor WinRar a tou jsou zaheslované RAR archivy. Jedná se však o nouzové řešení a doporučuje se využití dlouhých hesel a speciálních znaků proti použití tzv. crackerů (česky „louskáčků“), které zkouší na heslo aplikovat všechny možné kombinace. [62]

Nastínil jsem použití jedné z možností, **jak zabezpečit svůj soukromý klíč**, resp. elektronický podpis, proti jeho zneužití útočníkem. Další známou možností je využití speciálního hardwaru, instalovaného přímo do PC slotu. Tento bezpečnostní hardware však není tak bezpečný jako ostatní metody.

Nejefektivnější možností jak zabezpečit svoje data, jsou **speciální karty s čipem**, velmi podobným těm na všech SIM kartách v mobilních telefonech. Tyto karty při určité vzdálenosti nebo dotyku se snímačem indikují shodný kód a proto jsou i nejvíce bezpečné – je nutná fyzická přítomnost. Karty se dle použití dělí na dotykové – kontaktní – kde karta přichází přímo do styku se snímačem a bezdotykové, kde se využívá elektromagnetických vln na dálku. Existuje i varianta kombinující oba způsoby – karty duální. Karta je běžně chráněna PIN kódem, ochraňujícím kartu při krádeži. Pokud k tomu dojde, karta je zabezpečena tím, že PIN kód lze zadat pouze n-krát, přičemž číslo n si volí uživatel nebo vydavatel karty a označuje počet odmítnutých pokusů. Tím se uživatel chrání proti zkoušení „všech“ možných kombinací. Většinou bývá číslo n na staveno na hodnotu 3, tedy pokud útočník zadá PIN kód třikrát špatně, systém kartu zablokuje. [61]

Aby byl výčet možností úplný, uvádím ještě příklad využití takzvaných **tokenů.** Na tomto tokenu (zařízení podobné flash disku – viz. obrázek.) jsou uložena tato citlivá data. Token se připojuje k PC pomocí USB sběrnice. Jedná se o identifikační předměty, určené také pro jednoduchou autentizaci uživatelů. Zabezpečují přístup do počítačových či VPN sítí, intranetu, k elektronickým podpisům a PKI. Stejně jako výše uvedené karty využívají PIN kódy, ale nabízí kryptografické funkce – hardwarovou podporu bezpečnostním algoritmům MD5 a RSA s délkou až 1024 bitů. Disponují většinou pamětí 32 kB. Důležitým faktorem zde je, že privátní klíč nelze z tokenu exportovat do jiného zařízení. [21]

V předchozích kapitolách jsem tedy nastínil možnosti jak zabezpečit svůj soukromý klíč nebo obecně počítač před útokem. Při vypracovávání diplomové práce jsem zjistil, že je to právě poslední možnost – využití USB tokenu – kterou firma využívá. O konkrétním řešení v dané firmě se však zmíním v dalších částech svojí práce.

Obrázek 1: USB Token
Zdroj: www. linuxexpress.cz

4.2.4. Elektronický podpis a legislativa

4.2.4.1. Elektronický podpis v České republice

Již od roku 2000 je u nás platný Zákon o elektronickém podpisu (227/2000 Sb. O elektronickém podpisu). Elektronický podpis spadá do kompetencí Úřadu pro ochranu osobních údajů, který k tomuto zákonu vydává i prováděcí vyhlášky. Jednou z nich je například prováděcí vyhláška č. 366/2001 Sb., kde jsou specifikovány požadavky pro vytvoření a vydávání elektronického certifikátu a dále požadavky na nástroje o elektronickém podpisu, to vše se zaměřením na subjekty, které chtějí získat akreditaci pro vydávání kvalifikovaných certifikátů. Jako první získala akreditaci firma První certifikační autorita a.s. Od ledna 2003 dostalo elektronický podpis na starosti ministerstvo informatiky. To také akreditovalo Českou poštu k vydávání kvalifikovaných certifikátů a kvalifikovaných systémových certifikátů. [37], [26]

4.2.4.2. Digitální podpis v Evropské unii

První zemí v Evropské Unii, která schválila zákon o elektronickém podpisu bylo Německo a následně další země Evropské unie. Evropskou komisí byla schválena 30.11.1999 direktiva Evropské Unie o elektronickém podpisu, která se zabývala jeho platností, technologiemi a poskytovatelem certifikačních služeb. Na základě těchto dohod byla nastavena kritéria a zavedeny takové postupy, které umožňovaly další zavedení e-podpisu v praxi. Důležitým kritériem zde byla technologická neutralita, rozumí se tím, že technologických postupů je možné využít i do budoucna s trvající invencí. Dalším důležitým bodem bylo rozpoznání a jasné definování elektronického podpisu, aniž by nastaly pochybnosti o jeho platnosti nebo autenticitě. Samozřejmě se v těchto počátcích objevily v zákonech Evropské unie vážné právní trhliny. Jednou ze základních bylo ignorování faktu, že počet a kvalita certifikačních autorit musí být omezena, na což se ale nemyslelo. [34]

4.2.4.3. Elektronický podpis v praxi

Jako u každého teoretického pojmu i zde se snažíme o praktické využití. Elektronický podpis samotný se od začátku potýkal s mnohými problémy a to především v legislativní oblasti. Od svého zavedení jako právního pojmu, byl již několikrát novelizován a toto kopíruje přirozený vývoj požadavků a potřeb trhu. Statistiky nám ukazují, že elektronický podpis se obecně uchytil hlavně ve **státní administrativě** a při komunikací s ní. Zákonné úpravy většiny států dnes umožňují podání velkého množství dokumentů elektronicky a počet těchto možností neustále roste, ovšem stejně tak rostou bezpečností rizika a požadavky.

Zde bych rád zmínil některé služby, kde se elektronický podpis využívá nejvíce. V první řadě je to podání daňového přiznání – DPH, silniční daň a daň z příjmu. Dále je možné také elektronický podpis využít pro vydání občanského průkazu. Velmi širokou oblastí, kde elektronický podpis nalezl uplatnění je **elektronické obchodování**. Zde se využívá jak mezi dodavateli a obchodníky, kteří si navzájem ověřují faktury a data, ale i objednávky a pohledávky.

Poslední, ale neméně důležitou je oblast bankovnictví, kde je zabezpečení snad na nejvyšší úrovni. Online banking jak bývají transakce a přístup k účtům přes internet označovány, je velice **diskrétní, moderní, rychlý a flexibilní způsob jak ovládat svůj účet** z pohodlí domácího počítače. Rád bych zde zdůraznil onu mobilnost, protože tou se budu zabývat i později. Svůj elektronický certifikát si totiž můžete například na flash disku přenést na kterýkoli počítač a zde plně využívat služeb svojí banky. Je také ale nutné zmínit zvýšené riziko napadení takového účtu ze strany hackera a také nedostupnost aplikace v případu energetické havárie a následného výpadku proudu. Elektronický podpis v případech uvedených výše v každém případě znamená pohodlí a úsporu času a energie. [29]

Další oblasti využití elektronického podpisu v podmínkách České republiky:

1. Státní správa – portál v veřejné správy, elektronické podání dokumentů

- **Česká správa sociálního zabezpečení** – evidenční listy důchodového pojištění, přihlášky a odhlášky zaměstnanců k nemocenskému pojištění . Přehled o příjmech a výdajích OSVČ za rok 2005

- **Zdravotnictví** – v České republice měla být zavedena takzvaná zdravotní knížka společností IZIP (Internetový přístup ke zdravotním informacím pacienta), kdy zabezpečení mělo probíhat na principu čipové karty a biometrických údajů. Na kartě by byla nahrána část údajů o pacientovi a např. otisk jeho prstu, který by se dále ověřoval. Pacient by potom vložil kartu do čtečky a na snímací pole přiložil prst, čímž by byla provedena jeho autentizace.

- **Ministerstvo financí –** prostřednictvím e-podpisu lze přiznat:
    - Daň z přidané hodnoty
    - Daň z příjmů fyzických a právnických osob
    - Daň z nemovitostí
    - Silniční daň

▪ Bankovnictví – vedení kompletního bankovnictví přes internet, u některých operací v součinnosti s ověřováním přes mobilní telefon. Výrazná úspora nákladů.

▪ Elektronický obchod - vyjádření solidarity a bezpečí při obchodování zajištěném elektronickým podpisem. Využívá výhody při nepřetržitém provozu, využití služeb zásilkové služby. Zaručuje také fyzickou existenci druhé strany.

▪ Digitální fotografie – zde časové razítko a elektronický podpis ochraňují fotografie před falšováním, nelegálním kopírováním a falešným autorstvím. Je

možné také využít formou metadat vložených do informací o fotografii (EXIF) nebo jako vodoznak upravující přímo samotnou fotografii.

▪ Digitální knihovny – podobné využití jako u digitální fotografie. [36]

4.3. Elektronická podatelna

4.3.1. Systémová charakteristika

Ze systémového hlediska se jedná o stejný princip jako u podatelny klasické – fyzické. Elektronická podatelna zprávy a dokumenty přijímá, potvrzuje jejich přijetí, třídí je a ukládá. Při elektronickém podání uživatel po zaregistrování a přihlášení k webovému rozhraní přiloží ke svým údajům elektronický podpis, ověřený některou z certifikačních autorit. Následné fyzické podání se odehrává buď přes webové formuláře nebo pomocí emailové služby. Formulář nebo email se doplní o nezbytné údaje, jako je elektronický podpis a časové razítko a podatelna podá uživateli zprávu, zda byl takový dokument přijat. Všechny údaje a transakce jsou ukládány do archivu pro případ dalšího využití, například u reklamací. Podatelna takovou zprávu zpracuje a po ověření elektronického podpisu a časového razítka ji zařadí k dalšímu zpracování, které už provádí fyzická osoba na úřadě. Data potom převede do samostatného protokolu, který se uloží do archivu. Tento systém autentizace zprávy, ověření úředníka (digitální certifikát pro ověření komunikujících stran) a zašifrovaného kanálu se uskutečňuje dle vysokých bezpečnostních požadavků a je velice efektivní.

4.3.2. Technologie podatelny

První součástí s kterou uživatel přijde do styku je webové rozhraní, na které si zaregistruje certifikát a nadále sleduje průběh požadovaných akcí. Toto rozhraní bývá navrženo jako velmi přehledné a uživatelsky nenáročné s tím, že musí být

technologicky na vysoké úrovni vzhledem k potřebě zabezpečení. Jde o dotyk poměrně vyspělé technologie s lidským faktorem. Součástí každé elektronické podatelny je její databáze (ORACLE, MySQL), kde se data ukládají a archivují a odkud jsou pomocí dotazů získávána zpět pro případné využití.

Další komponentou z pohledu z druhé strany je aplikace nebo webová stránka, která slouží pro přístup úředníkům a poslední částí je speciální software, kterým se podatelna ovládá. [23]

4.3.3. Legislativa

V současné době v České republice platí v této oblasti důležitá vyhláška č. 496/2004 Sb., která se zabývá právě e-podatelnou (Zákon o elektronický podatelnách), která tak navazuje na nařízení vlády č. 495/2004 Sb. O elektronických podatelnách. Výše uvedené zákony upravují a vymezují prostor pro elektronické podatelny, přijímaní a odesílání zpráv prostřednictvím elektronické podatelny a upravují také povinnost úřadů zřídit a provozovat elektronickou podatelnu, souběžně s podatelnou klasickou. Znění vyhlášky upravuje především komunikaci mezi občanem a státem. Nejdříve měla jako elektronická podatelna sloužit emailová adresa Ministerstva informatiky. Orgán dozorující elektronickou podatelnu je povinen zveřejnit provozní řád, podle kterého se další jednání řídí. Orgány jsou také povinny aktualizovat svoje databáze, v tomto případě seznamy certifikačních autorit a to hlavně organizací Česká pošta, s.p. a eIdentity, a.s.. Také jsou povinny pravidelně aktualizovat kořenový certifikát. [58]

Další právní předpisy týkající se problematiky e-podatelny:

- Zákon č. 500/2004 Sb., správní řád
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy
- Zákon č. 337/1992 Sb., o správě daní a poplatků
- Zákon č. 106/1999 Sb., o svobodném přístupu k informacím
- Zákon č. 227/2000 Sb., o elektronickém podpisu
- Zákon č. 71/1967 Sb., o správním řízení (správní řád)

- Zařízení vlády č. 495/2004 k provedení zákona o elektronickém podpisu
- Zákon č. 634/2004 Sb., o správních poplatcích [38]

4.3.4. Praxe v České republice

Při zavádění elektronických podatelen se ukázalo, že jejich zřízení je velmi nákladné. Projevilo se to u nákupu speciálního bezpečnostního a ovládacího softwaru či také speciálního hardwaru. Další náklady vznikaly při rekvalifikaci pracovníků úřadů, protože bylo nutné zaručit, aby lidské zdroje nenapáchaly více škody než užitku. Nutnou součástí bylo také získání elektronických podpisů od akreditovaného poskytovatele certifikačních služeb. Dnes už můžeme říci, že v cestě za zřízením elektronické podatelny náklady nejsou větším problémem, i když menší obce se s tím potýkají. Mohou také ale využít možnosti zřídit elektronickou podatelnu u jiného úřadu a tam přesměrovat zájemce o elektronické podání. To se většinou děje, je-li objem elektronické komunikace úměrně malý. Potom už je zcela na obci, zda je výhodné elektronickou podatelnu zřizovat. [46]

4.4. Digitální knihovny

4.4.1. Charakteristika digitálních knihoven

Digitální knihovny (anglicky Digital libraries, také DL´s) někdy také označované jako virtuální nebo elektronické se začaly rozvíjet v devadesátých letech v USA. Samotné digitální knihovny vznikly z prosté potřeby ušetřit místo a minimalizovat objem tištěných informací. Také bylo nutné všechny informace reorganizovat a dodat jim určitý řád, k dosažení přehledného uložiště. Můžeme tvrdit, že celý internet je teoreticky jedna velká digitální knihovna, i když několik odlišností

zde najdeme. Informace na internetu totiž nejsou nijak uspořádány, což je hlavní atribut každé digitální knihovny.

Velmi důležitá je také vlastnost, kdy rychle a přesně najdeme nějakou informaci a právě tu informaci, kterou jsme vyhledávali. Označujeme ji jako relevantnost takové informace. Každý uživatel v ideálním případě vyžaduje, aby po vyhledání hesla např. „kolo“ dostal zpět právě význam, který hledá. Dnes to může být bicykl jindy kolo u auta. V digitálních knihovnách jsou informace uspořádány a vytříděny, aby bylo možné v nich jednoduše vyhledávat. Z důvodů bezpečnosti se také data archivují a zálohují. Obecně lze říci, že digitální knihovna označuje spíše souhrn všech činností, postupů, lidí a technologií, které zabezpečují elektronické uložení nějakých dat. Může to být celá organizace, která nějakým způsobem pracuje s informacemi nebo tyto informace vlastní. V digitálním archivu se mohou nacházet všechny možné materiály převedené z textové podoby jako například knihy, noviny, letáky a časopisy nebo i umění převedené do obrazů, audio a video záznamy apod. Tyto archivní materiály se nejdříve převedou do digitální podoby, nejčastěji pomocí scanneru a následně se vytřídí, uspořádají dle určitého systému a uloží do digitální knihovny, kde je možné s nimi dále pracovat.

Výhody digitálních knihoven:

- přístup je možný non stop
- materiály jsou zpracovány digitálně – snažší manipulace a vyhledávání
- ovládání z domova a úspora nákladů
- materiál neztrácí na hodnotě jako tomu je například u knih
- není potřeba obrovských skladovacích prostor a archivů
- zapůjčením uživatel data neblokuje pro ostatní

4.4.2 Technologie digitálních knihoven

K základním prvkům každé digitální knihovny tedy patří samotné digitální objekty, které tak tvoří obsah knihovny (data a metadata), jako základní součást. Dále pak je to vyhledávací a identifikační systém, správa a služby uživatelům.

Rád bych zde uvedl několik projektů, které se zabývají digitální knihovnou ve větším měřítku:

▪ DSpace vyvíjený firmou Hewlett-Packard, který dnes vyvíjí skupina odborníků po celém světě. Na rozdíl od jiných systémů jej není třeba upravovat a je připraven k použití. Je vyvíjen i samotnými uživateli a zvládá výborně kódování různých jazyků.Je to velmi univerzální a rychlý systém.

▪ Fedora (anglicky Flexible Extensible Digital Object and Repository Architecture), který absolutně nezávislý na místních podmínkách a lokalizaci. Služba je tvořena pomocí webového rozhraní a umožňuje exportování dat systémem METS (anglicky Metadata Encoding and Transmission Standard).

▪ Greenstone (Greenstone Digital Library Software) z Nového Zélandu.

▪ CD Sware vytvářený pro CERN (anglicky European Organization for Nuclear Research), který však není dopracován.

▪ EPrints, který je určen pro vědeckou obec a kde je webové rozhraní generováno dopředu a nemění se tak. Tento systém se hodně využívá v praxi.

V podmínkách České republiky se nejlépe osvědčil systém Greenstone, vzhledem k optimální lokalizaci. [47]

4.4.2.1. Digitální dokumenty

V oblasti digitálních médií, u dokumentů v digitální knihovně rozlišujeme, zda již byly vytvořeny digitálně nebo jestli do této podoby byly převedeny. Prvně zmiňované se označují jako born digital (česky digitálně narozené) a ty nejsou nikde ve fyzické podobě, ale pouze v digitální. Na druhou stranu, existují i dokumenty, které jsou v klasické fyzické podobě a my je převádíme do digitální podoby. V poslední době se

toto týká zejména a nejvíce oblasti fotografie, kde se pouze pomocí scanneru vyhneme jejich stárnutí a tím devalvaci. Příkladem takového dokumentu může být i tato diplomová práce. Nejdříve bude v podobě digitální, následně vytištěna a potom opět digitalizována a uložena v nějaké databázi školy. Samotná digitalizace také označovaná jako digitální workflow (česky průběh) a zahrnuje mimo jiné i výběr titulů a materiálů, které mají být digitalizovány, grafické úpravy před scannováním a po scannování, ukládání metadat, zpřístupnění uživatelům a archivace. Dnes jsou elektronické dokumenty nedílnou součástí každodenního života, zvláště na akademické půdě. Všichni je denně upravujeme, posíláme, kopírujeme a také v nich vyhledáváme a získáváme informace. Metadaty vybavené dokumenty lze jednoduše a efektivně uspořádat. Nejznámější standardy metadat jsou XML, DC a MERC. [48]

4.4.2.2. Identifikační systém

Identifikační systém patří jednoznačně k základním atributům kvalitní digitální knihovny. V minulosti využívané systémy se potýkají s několika problémy, jako je například vyčerpaná kombinace využívaných míst, nejednotnost a geografická nezávislost. Jsou to ale právě tyto atributy, které jej činí použitelným. Jejich bezproblémové fungování zaručuje především jejich použitelnost a platnost po celém světě – např. ISBN (anglicky International Standard Book Number, v překladu mezinárodní standardní číslování knih) – dále je to jejich jednoznačnost – identifikace. V současnosti žádný s využívaných systémů tyto podmínky nesplňuje a hledají se další cesty, které identifikační systémy využívají, aby bylo možné je využívat po celém světě, byly jednotné a nedocházelo k vyčerpání možných kombinací. Začaly vznikat nové systémy jako např. DOI (anglicky Digital Object Identifer), PURL (anglicky Persistent Uniform Resource Locator), URN (anglicky Uniform Resource Name), které jsou adaptovány pro prostředí rozsáhlých sítí v digitálním prostředí. [49]

4.4.2.3. Administrace

Elektronickému dokumentu v repozitáři jsou přidělena metadata, která kvalifikují vlastnosti tohoto dokumentu a záznamy o transakcích. Repozitář umožňuje různé operace s takovými dokumenty. Digitální knihovna může sloužit jako archiv, ale velkým problémem se stává trvalé řešení – trvalé uchování elektronického dokumentu. Fakt je, že s dokumentem uloženým v elektronické podobě se snadno manipuluje, fakticky není možné jej ztratit, vše je uloženo ve stejné kvalitě. Tento problém nastává, jakmile se změní technologie či postup. Při změně technologie např. vytváření nebo ukládání fotografií je totiž nutné změnit i technologii pro jejich čtení a tím změnit systém celého archivu, což je velmi náročné. Dokument, který by neprošel touto úpravou by mohl být nečitelný, nepoužitelný a proto vznikl projekt Rossetský disk, inspirovaný Rossetskými deskami, kde se jedná a speciální archiv, aplikovatelný na digitální knihovnu. Tento projekt by vyřešil, v e svém ideálním případě, problémy se změnami technologií. [49]

4.4.2.4. Služby digitálních knihoven

Nyní se podíváme na služby elektronické knihovny z jiného hlediska – z uživatelského hlediska, kdy neposuzujeme systémově funkce jako byly archivace a vyhledávání, ale samotný přístup ke službám digitálních knihoven. Algoritmus je poměrně jednoduchý, ale ze strany knihovny vyžaduje nemalé prostředky k dodržení především bezpečnostních standardů. Uživatel si po přístupu na nějaké stránky digitální knihovny musí nejdřív zařídit svoje konto, jako obvykle vyplnit registrační údaje, kde důležitou podmínkou je odsouhlasení licenční smlouvy a provozního řádu. Služby digitálních knihoven jsou většinou placené a to je další prvek takové aplikace – online platby. Ve většině případů se dokonce platí předem stanovená záloha za využívání služeb knihovny. Následně obdrží uživatelské jméno a heslo a tím přístup do samotné knihovny. Díky databázi je možné sledovat stav objednávek, historii zakoupených nebo prohlížených dokumentů, objednávat dokumenty, sledovat stav konta a k tomu je mu ještě k dispozici technická podpora ze strany knihovny k řešení případných problémů. Díky tomuto kontu a s tím spojeným zadáváním údajů je také vyřešena autorská

ochrana elektronických dokumentů v knihovně, protože ve většině případů se zadané údaje ověřují a je nutné dojít s dokladem totožnosti na nějaké místo, kde se spojí uživatel – login s fyzickou osobou. Všechny dokumenty v digitální knihovně jsou zařazeny a uspořádány v katalogovém systému, podle katalogových čísel. V tomto katalogu pak uživatel vyhledává podle tohoto čísla a nebo podle jiných parametrů, která jsou u dokumentu uvedena (například velikost). Důležitý je zde časový limit nastavený pro danou operaci, který opakuje nebo stornuje operaci je-li překročen. Pokud však nedojde k překročení limitu a dokument je podle nastavených parametrů vyhledán, uživatel jej může vytisknout a při tom neporuší autorský zákon. Jednou z možností, která se především dříve využívala (u pomalých připojení k internetu) byla služba DDS (anglicky Document Delivery Service), která zabezpečovala dodání dokumentu buď klasickou nebo elektronickou poštou. Výše jsem uvedl, že uživatel se identifikuje pomocí hesla. Toto heslo bývá někdy nahrazeno digitálním podpisem, kde digitální knihovna podpis a certifikát nejdříve ověřuje a tím je zaručena autorizace uživatele.

V praxi vyvstává problém, v jakém formátu pracovat s uloženými daty. V praxi se ukazuje, že nejbezproblémovějším formátem se zdá být formát PDF (Portable Document Format). Tento formát vyvíjí řadu let firma Adobe a ta stejná firma k tomuto účelu sama vyvíjí a dává k dispozici zdarma i univerzální program k práci s PDF - Adobe Reader. Důvodů k jeho využívání je více, ale jeho základní předností je jeho nezávislost na hostitelském počítači, v praxi jinak řečeno se ukazuje na každém počítači stejně. Tím se zaručuje vzhled, struktura a další nastavení dokumentu. Důležitým prvkem vyplývajícím z použití formátu PDF je jeho zabezpečení a to jak pro úpravu, tak i pro čtení, kopírování, mazání nebo i tisk.
Důležité je také ale zmínit, že tato zabezpečení fungují jen na omezené úrovni a dnes není nijak složité toto prolomit pomocí běžně dostupných nástrojů. [20]

Další výhody PDF:

- vkládání vodoznaku (obrázek nebo text)
- pokročilá optimalizace obrázků
- převzorkování obrázků

- šifrování a ochrana dokumentů
- možnost zabezpečení PDF proti zápisu
- možnost zašifrování PDF dokumentu
- ochrana vlastním elektronickým podpisem

Elektronický podpis se však bohužel v digitálních knihovnách zatím moc nevyužívá z důvodu jeho poměrně vysokých nákladů na pořízení pro knihovnu, administraci. [50]

4.4.3. Ochrana digitálních knihoven

Ochrana digitálních knihoven je stejně důležitá jako sama kvalita digitální knihovny. Jak jsem již zmiňoval, uživatel v rozmezí digitální knihovny zadává svoje osobní údaje, někdy včetně rodného čísla, heslo, provádí online platby a spravuje svůj účet. Toto jsou velmi citlivá data z pohledu zneužití a je nutné zabezpečit technicky knihovnu před různými druhy útoků. Na druhé straně je to ochrana autorského práva, kde správné zabezpečení brání zneužití všech dokumentů podléhajících autorským zákonům. Zavedení digitální knihovny tedy bude balancování na hranici mezi pohodlím uživatele a požadavky bezpečnostních inženýrů, kteří budou zabezpečení projektovat a zdokonalovat. Také je nutné brát na vědomí Zákon na ochranu osobních údajů a související právní předpisy a těmito se řídit při nakládání s takovými daty.

4.4.3.1. Ochrana autorského práva

V otázkách ochrany autorského práva v podmínkách České republiky narážíme na kolizi mezi dvěma zájmy. Na jedné straně stojí autoři uchovávaných děl a tvůrci elektronických dokumentů a na druhé straně stojí uživatelé, tedy široká veřejnost. V prvním případě jsou zájmy jasně dané: autoři chtějí ochranu svých dokumentů a jsou ochotni je půjčovat nebo prodávat za úplatu, chtějí zisk. Na druhé straně stojí uživatelé, kteří by naopak byli rádi, kdyby dokumenty byly volně dostupné, požadují neomezený přístup k informacím. Digitální knihovna v každém případě musí vycházet

z kompromisu mezi těmito dvěma zájmy, protože bez jednoho nemá smysl existence druhého. Knihovna tedy musí zabezpečit svobodný přístup k informacím, elektronické dokumenty a za to autorům bude poskytovat finanční ohodnocení. Mezi klasickou a digitální knihovnou zde nacházíme zásadní rozdíl: v prostředí klasické knihovny si půjčíme originální dílo, které si někdy za úplatu můžeme zkopírovat, ale v podmínkách elektronické podoby knihovny je situace složitější. Neplatí zde vyjímka z ochrany autorských práv pro volné užití díla, která se vztahuje na klasické knihovny. Pokud je totiž dokument uložen v digitální podobě, je fakticky zkopírován a vzniká tak jeho kopie. Podle § 37/1 Autorského zákona pak může být takový dokument užit pouze k archivačním účelům. V tomto případě se také setkáváme se dvěma pojmy: volné dílo, kde autor souhlasí s využitím díla v tomto směru a nebo již vypršela lhůta autorské ochrany a potom licencované dílo, které bylo již vydáno v digitální podobě. To autorský zákon ošetřuje pomocí pojmu sdělování veřejnosti – posílání po internetu a kopírování. V licenční smlouvě jsou potom konkrétní podmínky pro otevření, čtení, tisk a rozmnožování takového díla.

Situace v Evropské unii je poněkud odlišná. Autorské zákony zde ošetřuje hlavně směrnice Evropského parlamentu a Rady č. 2001/29/ES. V EU se projevuje snaha zákony sjednocovat a odstranit odlišnosti jednotlivých právních systémů z různých zemí. Trend je nyní takový, že pomocí různých projektů a analýz těchto odlišností se sjednocují pravidla pro užití licencovaných děl a tyto pravidla se následně aplikují v podmínkách celé Evropské unie.

4.4.3.2. Ochrana uživatele

Poslední podkapitolou je ochrana uživatele, na kterou se velice často zapomíná. Uživatel, stejně jako digitální knihovna, má některé práva a povinnosti. Knihovna v tomto případě už ze zákona ručí, že všechna data budou pečlivě uložena a zabezpečena proti zneužití a že nedojde jejich zjištění ani zneužití třetí osobou. Další podmínkou je možnost vymazání všech údajů na přání uživatele. Uživatel ale také sám musí dbát obezřetnosti a opatrnosti při nakládání s těmito údaji, především s přístupovým heslem ke svému účtu zvláště tam, kde se zavádějí placená konta. [2]

4.5. Elektronické obchodování

4.5.1. Úvod

V této části bude nejdříve nutné popsat některé, již dlouhá léta zavedené, termíny. Je to především z toho důvodu, aby nedocházelo k mylným přiřazením významů některého z termínů. K všeobecnému úvodu bych rád uvedl samotný pojem internet.

Internet z technického hlediska je síť rozprostřená po celém světě. Je to tedy síť počítačová, spojující jednotlivé počítače mezi sebou. Propojuje však nejen počítače, ale i menší sítě a to pomocí sady IP protokolů. IP protokol (anglicky Internet Protocol) je datový protokol, využívaný pro přenos dat přes paketové sítě. Počítačová síť obecně, označuje technické prostředky, které realizují spojení a tok informací mezi jednotlivými počítači.

Historie sítí sahá do šedesátých let dvacátého století, kdy se datují první spojení počítačů. Následně byly vyvinuty mnohé technologie, ale nejvýznamnější pro nás je síť internet, využívající sadu protokolů TCP/IP (Transmission Control Protocol/Internet Protocol - česky primární transportní protokol – TCP / protokol síťové vrstvy – IP)
Architektura protokolu TCP/IP rozložena do jednotlivých vrstev a to s ohledem na složitost celé problematiky. Vrstvy reprezentují hierarchii činností, kde samotná výměna mezi vrstvami je definována zcela přesně.
Komunikace mezi dvěma stejnými vrstvami dvou systémů je však řízena komunikačním protokolem a to bez ohledu a nebo vlivu na vrstvy ostatní. [53]

Členění architektury TCP/IP:

- síťová vrstva
- aplikační vrstva
- vrstva síťového rozhraní
- transportní vrstva

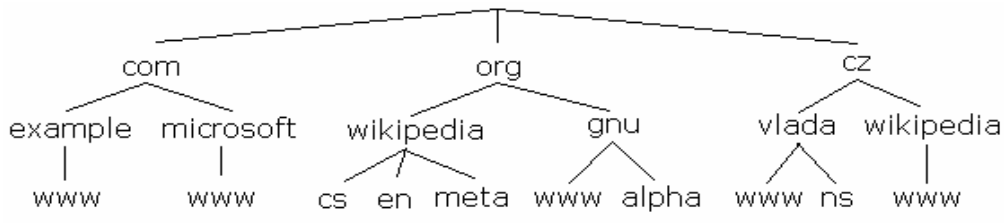
Název slova internet pochází z anglického slova síť – tedy *network* a latinského slova *inter* – mezi. Tím je dán i jeho význam – propojuje nějaké celky „mezi sebou“. Internet v širším významu má za sebou spoustu služeb, které v dnešní době využíváme v plné míře. Rád bych zde zmínil služby jako elektronická pošta, vyhledávací servery, blogy uživatelů, komunikační, seznamovací a informační servery, samotné webové stránky a webové prezentace, neuvěřitelné množství kompletních elektronických obchodů, hraní on-line her, chatovací služby a mnoho dalších. [54]

4.5.2. Identifikace počítačů v síti Internet

Každý počítač připojený k síti internet má svoji unikátní IP adresu, tvořenou 32bitovým číslem. Jsou to čtyři desítková čísla v intervalu od 0 do 255, oddělené vždy tečkou. Celkový počet IP adres se odhaduje na 4 294 967 296.
Již jsem zmínil architekturu TCP/IP a k tomu je nutné ještě zmínit internetové domény. Ty vznikly z prostého důvodu – identifikace počítače pomocí IP adres je velmi nesnadná a nepraktická – uživatel si těžko bude pamatovat několik IP adres svých oblíbených stránek. Domény proto převádějí IP adresy na srozumitelné a zapamatovatelné názvy. Jedná se o takzvané DNS (anglicky Domain Name System) domény, tvořené hierarchickým systémem. Tuto hierarchii realizují DNS servery. Jejich hlavním účelem je výše zmíněná transformace IP adresy na domény a naopak.

Domény mají také určitá pravidla pro přidělování:

- národní – například: .cz, .sk, .de, .au
- obecné (generické) – například: .com, .org, .edu, .net



Obrázek 2: DNS strom
Zdroj: http://cs.wikipedia.org/wiki/Soubor:DNS_strom.png

Obrázek 3: Doménový strom
Zdroj: http://www.nic.cz/page/312/o-domenach-a-dns/

Ve velmi zjednodušené formě jsem tedy popsal podstatu fungování internetu, propojení a komunikaci počítačů mezi sebou a některé vlastnosti, využívaných při práci s internetem. Aby byl tento úvod kompletní, je třeba ještě zmínit, jak se vlastně počítač k takové síti fyzicky připojí a některá další fakta. [53]

4.5.3. Připojení počítače k síti internet

V dnešní době jsou některá připojení již minulostí, výčet by bez nich ale nebyl úplný. Připojení tedy lze realizovat pomocí:

▪ klasického telefonního vytáčeného spojení, za využití analogového dial-up modemu. Rychlost je zde omezena na 56 kB/s. Jde o jeden z nejstarších způsobů, který se dnes snad již nevyužívá a který s sebou přináší mnohá omezení a limitující faktory – rychlost je tím nejzávažnějším a pro dnešní účely se již absolutně nehodí.

▪ ADSL (anglicky Asymetric Digital Subscriber Line) – nevyužívanější typ DSL připojení. Jedná se o asymetrické připojení – to znamená, že rychlost příchozích a odchozích dat je různá. Rychlost dat přicházejících k uživateli je větší než rychlost dat odesílaných. Toto by ještě nebyl problém. Problém nastává, kdy jsou využívány náročné technologie jako jsou video konferenční hovory a kapacita tohoto připojení už nestačí. V praxi se dále ukázalo, že každé vytáčené připojení je méně stabilní.

K připojení počítače k internetu pomocí ADSL je nutné mít ADSL modem, který se k počítači se připojuje buď přes USB, Ethernet (RJ-45) nebo ve formě PCI karty. Modem samotný nedokáže poskytovat připojení více než jednomu počítači.

- ISDN (anglicky Integrated Services Digital Network, česky Digitální síť integrovaných služeb) - nabízí plně digitální přenos a převod signálu se odehrává v ISDN modemu. Jde o multimediální komunikaci, neboť tato technologie umožňuje přenos hlasu, textu, obrazu a to i několik činností zároveň. V Evropě byl zaveden standard Euro ISDN, který implementuje všechny typy ISDN. Rychlost je omezena na 64kb/s.

- Mobilní telefon – poměrně pomalé připojení, ale skýtající jednu obrovskou výhodu – ve spojení s notebookem je možné se připojit, kdekoli kde má operátor signál. Tuto výhodu využívá čím dál více uživatelů a pro firmy má velký praktický přínos. Využívá technologií GPRS (anglicky General Packet Radio Service) – jedná se tedy o mobilní datovou službu, pro uživatele GSM telefonů, která se pohybuje na rozhraní mezi 2G a 3G telefony – a EDGE (anglicky Enhanced Data rates for Global Evolution, nebo také Enhanced Data rates for GSM Evolution) což je další vývojový stupeň v technologii .
Technologii připojení přes mobilní telefon dnes ale ovládají novější: CDMA u operátorů O2, UMTS (operátor O2, rychlost 384kb/s – označován jako 3G) a Internet 4G u T-Mobile.

- Připojení pomocí kabelové televize - dnes asi nejvyužívanější připojení, umožňující dosahování vysokých rychlostí připojení. Závislé je pouze na pokrytí sítí kabelů. Klasickým poskytovatelem je například společnost UPC Česká republika. K připojení je nutné vlastnit síťovou kartu a speciální-kabelový modem.

- WI-FI připojení (anglicky Wireless Fidelity) - jedná se o nejznámější technologii připojení k internetu – standard pro bezdrátové sítě (IEEE 802.11a), který využívá mikrovln pro přenos informací. Pohubuje se v rozmezí rychlostí 11 a 54Mb/s.

Využívané frekvence:

- 2,4 GHz
- 3,5 GHz
- 5 GHz
- 10 GHz

Nejvyužívanější je frekvence 2,4 GHz.

Technologie WI-FI připojení se začíná i v ČR neustále rozšiřovat jako cesta k připojení k internetu. Její výhody jako je mobilita a fakt, že není potřeba fyzického spojení se sítí využívají čím dál širší vrstvy uživatelů, v první řadě lidé v manažerských funkcích, kteří často cestují a potřebují spojení s internetem. Poskytovatel vybuduje vždy síť přístupových bodů (AP - access point), které však musejí být v přímém dosahu připojované stanice. Notebook má dnes už běžně zabudovanou – interní – WI-FI anténu, kterou již tedy není nutno externě připojovat. WI-FI připojení využila efektivně i firma, kde jsem zpracovával diplomovou práci. Jednak k připojení právě na služebních cestách a jednáních a jednak i jako řešení připojení jednotlivých stanic k internetu po firmě. Došlo zde nepřímo i k optimalizaci cable managementu v síti.

▪ Připojení pomocí optických systému – zde však vysoké náklady a vysoké přenosové rychlosti (155 Mb/s, 622Mb/s nebo 10Gb/s, 40Gb/s nebo i více) předurčují tyto technologie pro vybudování páteřních síti internetu. [57]

4.5.4. Historie

Zde bych rád velice stručný přehled vývoje internetu a TCP/IP protokolu:

- 1962 - Vzniká projekt počítačového výzkumu agentury DARPA.
- 1969 - Vytvořena experimentální síť ARPANET.
- 1972 - ARPANET rozšířena na cca 20 směrovačů a 50 počítačů.
- 1973 - Zveřejněn TCP (Transmission Control Protocol).
- 1980 - Experimentální provoz TCP/IP v síti ARPANET.

- 1984 - Vyvinut DNS (Domain Name System).
- 1985 - Zahájen program NSFNET, sponzoruje rozvoj sítě ve výši 200 mil. dolarů, první komerční služby.
- 1987 - Vzniká pojem „Internet“.
- 1987 - V síti je propojeno 27 000 počítačů.
- 1989 - Tim Berners-Lee publikuje návrh vývoje WWW .
- 1993 - Marc Andreessen vyvíjí Mosaic, první WWW prohlížeč.
- 1994 - Vyvinut prohlížeč Netscape Navigátor.
- 1996 - 55 milionů uživatelů.
- 1999 - Rozšiřuje se Napster.
- 2000 - 250 milionů uživatelů.
- 2005 - 900 milionů uživatelů.
- 2006 - více než miliarda uživatelů. [54]

4.5.5. Elektronický obchod

Při popisování modelu zabezpečení se nevyhnu popisu i elektronického obchodu obecně. Zde bych rád uvedl jen stručné údaje se zaměřením na méně známá fakta. Dnes už po tolika letech vývoje elektronického obchodu vyvstává otázka samotné definice, protože elektronický obchod se vyvinul v mnoha směrech a transformoval do mnoha podob, o kterých se zmíním v následujícím textu. Největší rozvoj nastal během devadesátých let, elektronický obchod se začal označovat jako e-business a jako takový býval často omezen na pojem e-commerce. E-commerce je obecně podnikání za využití elektronických prostředků, to znamená elektronický obchod v užším pojetí. E-commerce se zabývá především podporou podnikání pomocí informačních technologií a jejího softwarového vybavení. Toto podnikání se tedy odehrává v mírně změněné podobě než podnikání klasické, protože využívá elektronickém prostředky. Musíme sem také zahrnout řízení vztahu se zákazníky - CRM systémy, řízení dodavatelských řetězců – SCM systémy a také řízení znalostí – KM. Na druhé straně tedy pojem e-business označuje samostatné elektronické obchodování, kde pomocí internetu uzavíráme obchod a to s přispěním moderních technologií, typicky pomocí

internetu. Moderní tendence ukazují, že zanedlouho se pojmy e-commerce a e-business stanou ekvivalentními termíny pro obchod, nákup a další, bez formálního „e“. Elektronický obchod chápeme jako na dálku realizovanou obchodní činnost, pomocí internetu, speciálního software a hardware. Je důležité zmínit, že z právního hlediska dochází k uzavření smlouvy tak, že zákazník projeví vůli a pomocí některého z programů provede jasný krok k uzavření smlouvy. V praxi se toto děje pomocí „odsouhlasení“ smlouvy jediným kliknutím zákazníka. Další možností jak realizovat elektronický obchod je aktivní vyhledávání zákazníků například pomocí emailu, kde dochází k jejich přímému oslovení, zaslání nabídky a dalších kroků a následné zpětné interakci. Zboží v elektronickém obchodu může být hmotné i nehmotné a může mít i podobu služby. Elektronický obchod zahrnuje i veškeré činnosti, které s ním souvisí jako je například reklama, uzavírání smluv, podpora zákazníků a služeb. [13]

Ze začátku elektronického obchodování se lidé potýkali především se zažitým postupem si věc vyzkoušet, „ohmatat“ a potom ji teprve koupit. V dnešní době je zcela běžná praxe, že zákazník jde nejdříve do kamenné prodejny, kde si zboží vyzkouší a následně si to stejné objedná na internetu, což je zcela fatální pro kamenné obchody, které nemohou konkurovat cenou, vzhledem k vysokým nákladům na provoz. Je potřeba také říci, že moderní uživatel již běžně obchoduje po internetu – označujeme jako třetí generaci uživatelů, kteří již kvůli úspoře času a finančních prostředků do kamenného obchodu prakticky nechodí. Typy elektronických obchodů můžeme shrnout v následující tabulce:

	Obchodník – **B**usiness	Spotřebitel – **C**onsumer	Vláda, instituce - **G**overnment
Obchodník – **B**usiness	B2B - velkoobchod	C2B – elektronické systémy, spotřební zboží	B2G – nabídka zboží a služeb
Spotřebitel – **C**onsumer	B2C - zákazníkům	C2C – obchod typu e-Bay	C2G – daňová přiznání, volby
Vláda, instituce - **G**overnment	G2B – veřejné zakázky	G2C – informace o veřejné správě	G2G – koordinace samosprávy a vlády

Tabulka 1: Typy elektronických obchodů
Zdroj: vlastní

Nyní se stručně zmíním o základních formách elektronického obchodování.

4.5.5.1. Business - to - Business

Jak názvy napovídají u všech typů se dá odhadnout čeho se týkají. Uvedená dvojka vznikla z anglické výslovnosti čísla 2 a slovíčka *„to“*, které zde označuje pomyslný směr obchodování. Je to tedy jen zkrácení. B2B je tedy označení pro obchodování mezi většinou velkými firmami, obchodními společnostmi. Jedná se většinou o velkoobchodní vztahy a firmy neoslovují koncové spotřebitele. Velmi důležitou roli zde hrají informační technologie, konkrétně využití nějaké typu databáze, kde firma uchovává všechna data a do níž zákazník přistupuje. Tento typ je podobný elektronickému obchodu, jak jej známe i my. V případě B2B obchodu se však uplatňují některé zvyky, například výrazné slevy pro často odebírající firmy nebo podmínka minimálního odebraného množství. Výhodou pro obchodní firmu je právě toto využití moderních technologií, které jsou schopné například automaticky objednávat zboží, upozorňovat na zboží na skladě, na zboží nejčastěji prodávané a dalších spoustu činností. Všechny tyto výhody vedou k jedinému cíli a tím je snížení nákladů. Ideální je případ, kdy se všechny činnosti s objednaným zbožím provedou automaticky a my, jako vlastníci takového velkoskladu, jen celou transakci dozorujeme. Může se jednat nejdříve o vytvoření zakázky, vyskladnění objednaného zboží, popřípadě okamžitého objednání chybějícího zboží, expedice, přijetí platby, vystavení dokumentů. Naše činnost by v tomto případě byla jen fyzicky přemístit zboží z našeho skladu, tyto aktivity zaznamenat a popřípadě zase zboží naskladnit, vše samozřejmě metodou just-in-time. Je však zřejmé, že to je idealizace.

4.5.5.2. Business - to - Consumer

B2C označuje vztah mezi obchodníkem a koncovým zákazníkem, opět za využití informačních technologií. V dnešní době je velice obtížné tento typ obchodu provozovat, resp. úspěšně konkurovat mezi tak silnou konkurencí. Spektrum oborů, nabízejících služby nebo výrobky na internetu je, dovolím si říci, vyčerpáno. Proto je velice obtížné konkurovat na tak nasyceném trhu. Je to však možné. Je nutné využít

osvědčené marketingové metody (například viral marketing v reklamě – označuje způsob šíření povědomí o našem produktu nebo značce a přirovnává jej k šíření viru.)
, kam patří například šíření reklamy nebo nabídky formou emailu (nyní nemyslíme spam). Po krátkém hledání na internetu snadno najdeme obrovské množství E-Shopů. Některém fungují skvěle, jiné méně, ale jejich množství je ohromné. Podle mých zkušeností z praxe potom platí, že čím větší množství e-shopů v daném odvětví existuje, tím menší je množství obchodů kvalitních s odpovídajícími službami. Na druhou stranu lze vycházet z předpokladu, že tzv. „neviditelná ruka trhu“ sama tyto nekvalitní e-shopy odstraní. V praxi se tak lze setkat s pozdními dodáními, vysokými cenami, technicky špatně řešenými a dalšími e-shopy a na druhou stranu s nesmírně kvalitně provedenými a designově pěknými obchody, které plně využívají kapacit a příležitostí pro nakupování na internetu.

Pro orientaci mezi elektronickými obchody dnes slouží zvláštní stránky, které se dají velmi dobře využít**.**

Rád bych zde uvedl několik příkladů:

www.iobchody.com

www.i-shopy.cz

www.centrumobchodu.net

Výhodou těchto stránek je možnost najít si i zkušenosti uživatelů.

4.5.5.3. Consumer - to – Business

C2B j zvláštní typ obchodu, kdy si spotřebitel sám vyhledává prodejce a sám si zjistí nabídku a další parametry podle sebe a sám iniciuje nákup. Jedná se většinou o velmi specifické zboží (parní turbíny) nebo zboží, kde hraje velkou roli firemní značka (doutníky apod.)

4.5.5.4. Consumer – to - Consumer

Typ C2C je takovou zvláštností mezi typy obchodů. Jde o velmi dobře známé obchody typu E-Bay, kde obchodují spotřebitelé mezi sebou. V mnoha případech je to formou aukce se vším všudy (jako například na české aukci aukro.cz). Zvláštností je, že zde lze nejen kupovat za peníze, ale i směňovat zboží za zboží a také že zde lze sehnat naprosto cokoli.

4.5.5.5. Další formy

- elektronický obchod – e-shop
- elektronický obchodní dům – e-mall – několik obchodů v jednom
- elektronická burza – e–procurement
- elektronická aukce [13]

4.5.5.6. Legislativa

V této kapitole nebudu popisovat celou právní úpravu, ale zmíním zde jen jednu problematiku a tou je fyzické umístění serverů. Je zřejmé, že daňové zákony a právní úpravy se vztahují pouze na území, kde je server fyzicky umístěn a proto je neustále v kurzu umístění serverů do tzv. daňových rájů, ale jejich praktické provozování jinde.

Je nutné zmínit, že právo Evropské Unie (Směrnice 2000/31/ES o elektronickém obchodu) pojem e-shop nezná, ale zavádí pojem „služby informačních společností“ (information society services). [3]

4.5.6. Podoba elektronického obchodování

Elektronické obchodování, jak již bylo zmíněno, může nabírat mnoho podob. Není úkolem této práce je všechny bezezbytku popsat, ale spíše shrnout nejdůležitější fakta, která jsou nebo přímo byla využita při vypracovávání praktické části ve firmě.

Důležitým atributem potom bude, u každé podoby – formy – zmínit riziko z pohledu bezpečnosti, které s sebou nese.

4.5.6.1. GSM banking

Jde o jednu z nevyužívanějších forem e-bankingu, která v posledních letech zažívá nespoutaný rozvoj. GSM banking je u nás prakticky zcela závislý na GSM sítích a tedy i mobilních operátorech, kteří zprostředkovávají tuto službu. U klasického GSM bankingu nelze využít pevnou linku, je nutné používat klasický mobilní telefon, kde jednou ze zásadních vlastností je jeho identifikace podle jedinečného GSM čísla, vydávaného operátorem, které lze registrovat jedné osobě. GSM banking se často využívá k převodním příkazům, informacím o účtu a podobně. Pomocí funkce GSM Toolkit, kterou má již dnes zabudovanou většina mobilních telefonů, lze po aktivování v příslušné bance rozšířit telefon o řadu funkcí, které se týkají bankovního účtu a velmi pohodlně jej lze také ovládat. Riziko spočívá potom v uvedené identifikaci, kdy zcizený telefon může k informativním účelům využít kdokoli, ale pro ostatní operace (platební příkazy) je však nutné zadat většinou heslo, PIN nebo kombinaci obojího a to přímo telefonnímu operátorovi. Pokud je telefon rozšířen o funkce telefonního bankovnictví přímo v menu, je toto menu chráněno pomocí BPIN a BPUK kódů.

4.5.6.2. Internetové bankovnictví – homebanking

Homebanking je dnes také zcela běžná forma ovládání svého účtu přes internet. Zásadní nevýhodou zde je jistá imobilita, protože k využití služby je nutný přístup jednak k PC a jednak k internetu. Klasický postup při požadavku využívaní techto služeb je následující: klient si u své banky přes internet po zadaní všech údajů vytvoří elektronickou identifikaci a vygeneruje šifrovaný tvar elektronického klíče. Nainstaluje si také potřebné aplikace, které mu banka nabídne ke stažení a následně si vytiskne elektronický klíč, se kterým jeho cesta vede na přepážku svojí banky, kde se elektronicky ověří, že klíč vygenerovaný a vytištěný klientem souhlasí s tím uloženým v databázi banky a zároveň, že se vším souhlasí osobní údaje kontrolované podle OP.

uživatel následně zvolí heslo a vytvoří si a stáhne certifikát, který si uloží na bezpečné místo do počítače, v podobě, kterou ukazuje následující obrázek.

Obrázek 4: Příklad soubrou certifikátu v PC
Zdroj: www.mojebanka.cz

Následně při každém přihlášení do aplikace internetového bankovnictví vybere cestu k uložení tohoto souboru a zadá svoje heslo a tím dojde k autorizaci a aplikace mu umožní vstup do webového rozhraní svého účtu, kde již lze provádět všechny klasické transakce, doplněné o další služby – například možnost dobití telefonu či zaplacení faktury. Každá transakce je pak v moderních systémech chráněna ještě právě za využití GSM bankingu a to tak, že při zadaní například platebního příkazu, uživatel zadá nejen heslo, ale i v SMS obdržený autorizační kód a teprve po jeho zadání je platba připravena k provedení.

Obrázek 5: Aplikace internetového bankovnictví
Zdroj: www. mojebanka.cz

4.5.6.3. Platební karty

Původním účelem platebních karet bylo jejich využití při bezhotovostním styku, zejména v maloobchodní síti a dále pak jejich využití při vybírání hotovosti z bankomatů. Karta samotná je doklad, který popisuje norma ISO 3554. Karta je pokaždé majetkem banky, která ji vydala nikoli uživatele, který ji používá. Karty můžeme rozdělit na několik typů – kreditní, co-branded, charge debetní karty. Poslední zmíněné se využívají jako zdroj financí při běžných platbách, kde ale na běžném účtu jde klient banky do mínusu a tato služba je přirozeně zpoplatněna v podobě vyšších úroků. U Charge karet dochází k zaplacení se zpožděním, podobně jako u faktury, ale výhodou je, že klient nevyužívá úvěr. Pro můj pohled – bezpečnostní – jsou ale důležité ochranné prvky a další zabezpečení karet. Důležitým termínem je zde „embosovaná karta“, která je chráněna jednak magnetickým proužkem, jednak údaji o majiteli a klasicky číslem karty. tyto údaje jsou ale vyobrazeny plasticky a je velmi obtížné takové karty zkopírovat.

4.5.6.4. Elektronické platební systémy

Elektronické platební systémy se začaly vyvíjet již v devadesátých letech. Jejich tehdejší hlavní výhodou bylo, že se neřídily hranicemi států a platby bylo možné provést jen v závislosti na rychlosti IS/IT systémů. Elektronických platebních systémů je několik druhů a mezi nimi několik odlišností, kde se zaměřím především na oblast bezpečnosti. Všechny druhy ale mají stejného jmenovatele a tím jsou elektronické peníze – tedy předmět těchto plateb.

4.5.6.5. Elektronická výměna dat

Elektronická výměna dat (EDI – anglicky Electronic Data Interchange) – jsou specifické metody, které se využívají při výměně zpráv mezi počítači, jako mezinárodní standardy. EDI jsou pořád nejpoužívanějším datovým formátem pro elektronické obchodování, rozšířené po celém světě. Jde o zprávy přesně strukturované, kde mezi

sebou komunikují dvě aplikace. Tyto zprávy bývají generovány automaticky na základě nějaké činnosti bez přispění lidského faktoru. Nejčastěji se jedná o faktury nebo elektronické objednávky. Největší přínos lze spatřit v non-stop provozu takových systémů a nahrazení klasických papírových dokumentů. Z našeho pohledu se lze s EDI setkat především při běžném nakupování v elektronickém obchodu, kde se automaticky generují objednávkové listy, často zasílané na emailovou adresu, dále pak záruční listy, faktury a nebo nabídky podobného zboží. [52]

4.6. Bezpečnost informačních systémů

Ve firmě, kde jsem zpracovával tuto diplomovou práci, se v první fázi projektu nedbalo na bezpečnost nebo „bezpečí“ žádným z uvedených způsobů. Proto prvním krokem, před praktickou částí bude zmapování rizik, která ohrožují informační systémy obecně a především toho, jak se takových rizik vyvarovat. Je logické, že jako u většiny firem, nejdůležitější není software nebo hardware, ale jsou to právě informace – data, která je nutné pečlivě chránit a zabezpečovat.

Na náš informační systém z pohledu zabezpečení se lze dívat ze dvou pohledů, dvěma směry. Jednak z pohledu vnějšího, kdy zkoumáme rizika uvnitř firmy a z pohledu vnitřního, kde nás zajímají rizika, ohrožující firmu z vnějšku. Podle tohoto rozdělení potom rozlišujeme hrozby na externí a interní. *„Ze statistik vyplývá, že téměř největší procento zneužití dat mají na svědomí pracovníci vlastní organizace, před kterými se dá také chránit nejhůře.“* [1]

Ve firemní praxi se ukazuje, že není možné řešit pouze bezpečnost informačního systému samostatně, ale v souladu s dalšími zabezpečeními, která se dotýkají celém organizace. Je to třeba již zabezpečení firmy před vniknutím cizí osoby. Z manažerského pohledu je potom nutné zvolit rozumnou alternativu mezi stupněm zabezpečení firmy a mezi požadavky na provoz. Tyto dvě odvětví si často odporují, protože extrémně vysoké zabezpečení firmy znemožňuje bezproblémový chod firmy a

[1] KOCH, Miloš, DOVRTĚL, Jan. *Management informačních systémů*. 1.vyd. 2006.174s. ISBN 80-214-3262-4.

naopak. Analýza rizik firmy, která by měla předcházet všem opatřením zahrnuje několik kroků. Prvním krokem je studie bezpečnosti, kde jsou definovány jasné postupy, aktuální stav a možné hrozby. Dále je to bezpečnostní politika firmy, kde si firma jasně zvolí, jakým směrem se bude v této oblasti ubírat a jakého stupně zabezpečení, jaké úrovně chce dosáhnout. Definuje zde tedy strategická opatření. Posledním krokem je bezpečnostní projekt, kde se již konkrétně stanoví postupy, které vedou k dosažení vytyčeného cíle. Rizika, která nám vyplynou ze zmíněné studie jsou potom na pomyslném průsečíku mezi velmi pravděpodobným a velmi ničivým rizikem, kde velmi pravděpodobné a velmi ničivé riziko je nutné řešit nejdříve.

Při stanovování bezpečnostní politiky je nutné si analyzovat několik základních témat:

- co je předmětem ochrany
- kdo nese odpovědnost za tuto ochranu
- stav, ve kterém je ochrana efektivní
- pokyny a požadavky, kterými toho dosáhneme
- časový plán a způsob realizace

Bezpečnostní politika firmy jako celek je potom souhrn návrhů, řešení, požadavků, technických a organizačních opatření. Naproti tomu projekt samotný musí obsahovat i požadavky bezpečnostního manažera, který stanoví normy, směrnice a postupy k dosažení bezpečnosti. Ve větších firmách se často využívá služeb externích poradců nebo konzultantů z hlediska vyšší časové náročnosti a vysoké odbornosti takových činností. Při stanovování těchto postupů je nutné zahrnout celou škálu dalších segmentů, které zaručují správné využití všech bezpečnostních opatření. Jedná se o administrativní úroveň (v konkrétní firmě v externí podobě, která může upozornit na různé formy podvodů), personální úroveň (zejména útoky uvnitř firmy), IS/IT oddělení (nejdůležitější, je nutný vysoký stupeň důvěry), technická úroveň (fyzické zabezpečení). pro všechny typy událostí nebo útoků má potom firma definované jasné postupy, jak takové incidenty řešit.

Vycházíme-li z výše uvedených faktů, je nutné si uvědomit, že bezpečnost ve firmě je prakticky nikdy nekončící proces, nejedná se tedy jen o jednorázová opatření. Je také nutné, aby někdo z vedoucích pracovníků měl zabezpečení firmy na starosti, aby byl za ni někdo odpovědný a tento pracovník si musí uvědomit, že i když jsou některé zabezpečení velice nákladná, škody, kterým mohou zabránit, jsou zpravidla násobně větší.

Informační systém a jeho bezpečnostní prvky jsou základním prvkem každého bezpečnostního projektu. **Mezi základní bezpečnostní prvky řadíme:**

- fyzickou bezpečnost – technické zajištění firmy. Jedná se o prvky aktivní ochrany, mříže, tvrzená skla, alarmové a kamerové systémy, požární systémy, trezory a další. Jejich původní účel je však zabránění vniknutí do objektu, jejich sekundární účel je tedy fyzická ochrana bezpečnostního systému.

- záložní zdroje – UPS (anglicky ***U**ninterruptible **P**ower **S**upply* – nepřerušitelný zdroj energie) – systémy zajišťující neustálou a nepřerušovanou dodávku elektrické energie v případě:

- Ztráty napájení (blackout) - úplná ztráta napájecího napětí
- Krátkodobého poklesu - velmi krátkodobý pokles napětí o 15-20%
- Dlouhodobého podpětí (brownout)
- Dlouhodobého přepětí - dlouhá linie vysokého napětí- způsobuje poškození a rychlé opotřebování spotřebičů.
- Změny frekvence - odchylka od standardní frekvence (50Hz, způsobuje např. změnu rychlosti motorů, „spadnutí“ počítače
- Napěťového rázu - okamžiková špička až 20 000V.
- Harmonického zkreslení - Harmonické zkreslení sinusového průběhu.

- přístupová práva – administrace hesel a jejich uživatelů, úschova, zneplatnění, vydávání a všechny podobné činnosti.

- firewall – hardwarové nebo softwarové zařízení – aplikace – sloužící k zajištění bezpečnosti počítače připojeného do sítě – k internetu. Soubor opatření týkajících se firewallu se běžně označuje jako *bezpečnostní politika firewallu*. Jde zde o pravidla komunikace mezi sítěmi, jak jsem je zmínil už dříve, ale také o různorodá globální nastavení nebo překlady adres nebo o šifrovaná spojení mezi branami – takzvané VPN sítě (VPN – anglicky Virtual Private Networks)

- antivirové programy – dnes již běžně rozšířené aplikace sloužící k ochraně PC před útokem zvenčí. Jedná se o jedno z největších rizik a antivirový program je jeden z nejúčinnějších nástrojů proti. Dnes je běžné nastavení na každodenní aktualizaci, resp. aktualizaci na požadavek serveru, odkud antivirový program pochází a také neustále zapnutá rezidentní ochrana. Ve firmě je využíván antivirový program Nod32, ale o tomto se zmíním až dále.

- zálohování dat – je jeden ze základních prvků ochrany informačního systému. Pokud jsou data pravidelně a poctivě zálohována, tak jakákoli škoda způsobená například na hardwarovém vybavení je zanedbatelná, pokud naše data zůstala zachována. Jedná se tedy o pasivní ochranu, která neumožňuje jejich zneužití.

Záloha dat umožňuje napravit chyby způsobené:

- chybami pevných disků, napájecího zdroje a dalších komponent
- chybami software
- přírodními katastrofami – požár, zatopení
- lidskými chybami – náhodnými nebo úmyslnými – pravděpodobně největší oblast.

4.6.1. Počítačové viry

Obecně hovoříme o úmyslně napsaném programu – spustitelném kódu – který se dokáže sám nebo na pokyn útočníka šířit nebo spustit bez vědomí uživatele. Pro toto množení se umí vložit do jiných spustitelných souborů nebo programů. proto je označován jako vir – analogicky navazuje na biologický vir – tomuto šíření viru se proto někdy říká infekce a napadenému souboru či počítači potom hostitel. Viry jsou jedním z druhů malware – zákeřný software. Některé viry mohou být záměrně sestrojeny k ničení souborů, jiné napadený systém neničí, ale pouze získávají data nebo jen obtěžují uživatele. Nejničivější dopad má však samotná replikace viru, který zatěžuje počítačové systémy. Proti virům obecně se bráníme antivirovými programy. V každé firmě dnes již je takový program samozřejmostí a i v mojí praxi jsem se s těmito útoky setkal a v návrhové části jsem popsal obranu proti těmto útokům.

Počítačové viry můžeme rozdělit na několik základních typů, značně odlišných, proti kterým potom stanovujeme různé typy obrany v podobě antivirových programů:

1. **Klasické viry** – výše zmíněný typ, kdy vir je schopen sebereplikace na hostitelském PC, ke kterému je připojený. Jako hostitel bývá využíván buď přímo pevný disk nebo program a nebo jen skripty – specifické aplikace. Jakmile je kód viru spuštěn, vir se aktivuje a dochází k dalšímu nakažení a proběhne samotná ničivá činnost, ke které byl daný vir konstruován.

2. **Trojské koně** – tento druh viru není schopen samovolného šíření. Trojský kůň bývá ukryt v neškodném programu, který má uživateli sloužit, ale v jádru uživateli škodí. Jedná se například o key-loggery (programy zaznamenávající údery klávesnice a tím získání přístupových hesel a všech informací, které uživatel zadává). Některé trojské koně fungují jako „backdoor“ aplikace, které umožňují přístup do systému dalším – podstatně škodlivějším – programům.

3. **Červi** – šíří se ve formě síťových paketů, které jsou šířeny od nakažených systému k dalším, neinfikovaným, běžně prostřednictvím internetu. Pokud červ narazí na systém s bezpečnostní trhlinou, usadí se zde a využívá tento systém jako domovský k šíření. Dochází ve výsledku k datovému zahlcení sítě nebo internetu obecně.

4. **Makroviry** – viry, které jsou kódovány v některém z makrojazyků a bývají například součástí souborů vytvořených v programu MS Excel.

5. **Stealth viry** – viry tající svoji činnost nebo i přítomnost před antivirovými programy.

6. **Polymorfní viry** – schopné měnit svůj kód tak, aby nebyly odhaleny. Dokáží se velice účinně přizpůsobit vyhledávacím sekvencím antivirových programů.

7. **Spyware** – programy, které využívají hostitelský systém k odesílání důvěrných informací bez vědomí uživatele. Většinou se však jedná o informativní údaje, které slouží útočníkům k marketingovým účelům. Bývají to například informace o navštívených stránkách, čase stráveném na internetu s přehledem činností apod.

8. **Ad-ware** (advertising-supported software) – produkty znepříjemňující nebo někdy i znemožňující práci s aplikací pomocí cílené reklamy. Ad-ware programy mají různé stupně a formy – od menších bannerů po „neuzavíratelná“ pop-up okna a změny v nastavení domovských stránek prohlížečů.

Mezi další bezpečnostní hrozby ještě můžeme zařadit phishing a pharming – pojmy, které se na scéně objevily teprve nedávno.

1. **Phishing** – je podvodná technika sloužící k získání citlivých údajů uživatele (hesla), fungující na principu rozesílání emailů, které na první pohled vypadají jako by je odeslala oficiální instituce – nejčastěji banka. Tyto emaily většinou upozorňují na končící platnost hesla nebo karty a nabádají klienta k jejich zadání do aplikace nebo přímo k zaslání tohoto hesla na uvedený email. Uživatel po kliknutí na odkaz uvedený v emailu uvidí věrnou kopii stránek své banky a pokusí se o přihlášení do aplikace internetového bankovnictví. Stránky jsou samozřejmě jen kopií a útočník tak získá nejen heslo, ale i certifikát uživatele, který uživatel nechtěně uploaduje. V České republice je známo už několik takových aktivit. (například se s těmito typy útoků potýkala Komerční banka)

2. **Pharming** – jedná se podobný typ útoků jako je uveden výše, jen v jiné formě. Útočník využívá změněné IP adresy a překladu jména serveru k útokům na DNS. Potom už analogicky postupuje jako v v případě phishingu. [12]

4.7. Shrnutí

V předchozích kapitolách (4.1. – 4.6.) jsem uvedl informace o kryptologii, elektronickém podpisu, elektronické podatelně, digitálních knihovnách, elektronickém obchodování a bezpečnosti informačních systémů. Všechny tyto informaci mi poslouží v návrhové části k vytvoření modelu bezpečnosti, který jsem si stanovil v kapitole 2 – Cíle práce. Na první pohled se řada informací může jevit jako informace nesouvisející, ale v následujících částech práce ukážu, že tomu tak není. Při vytváření bezpečnostní politiky firmy je nutné se o tyto znalosti opírat a vycházet z nich. V řadě případů jsem tyto témata vybral a popsal právě na základě praktických zkušeností z působení ve firmě a u mnoha kapitol na toto odkazuji. Není cílem této práce všechny tyto technologie dopodrobna popsat, ale využít základní znalosti o nich k vytvoření návrhové části.

5.Analýza problému

5.1. Informace o firmě

Utajeno dle přání dotčeného subjektu.

5.1.1. Obecná charakteristika

Utajeno dle přání dotčeného subjektu.

5.2. SWOT analýza firmy

Utajeno dle přání dotčeného subjektu.

5.3. Analýza trhu

Utajeno dle přání dotčeného subjektu.

Analýza nedostatků

Utajeno dle přání dotčeného subjektu.

6. Návrh řešení

Utajeno dle přání dotčeného subjektu.

6.1. Stanovení bezpečnostní politiky

Utajeno dle přání dotčeného subjektu.

6.2. Informační systém

Utajeno dle přání dotčeného subjektu.

6.3. Model zabezpečení

Utajeno dle přání dotčeného subjektu.

7. Zdůvodnění návrhu

Utajeno dle přání dotčeného subjektu.

7.1 Ekonomické zhodnocení návrhů

Utajeno dle přání dotčeného subjektu.

8. Závěr

Utajeno dle přání dotčeného subjektu.

Seznam použitých informačních zdrojů

Knihy a tištěné materiály

[1] DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. 1. vyd. Brno : Computer Press, 2006. 24 s. ISBN: 80-251-0106-1

[2] JURMANOVÁ VOLEMANOVÁ, Věra. Digitální knihovny z pohledu autorského práva. 1. vydání. Brno : Masarykova univerzita, 2005. 66 s. ISBN 80 -210-3646-X.

[3] FRIMMEL, Martin. Elektronický obchod : právní úprava. 1. vyd. Praha : Prospektrum, 2002. 312 s. ISBN 80-7175-114-6.

[4] GRUBLOVÁ, Eva. Internetová ekonomika. Ostrava : Repronis, 2002. 88 s. ISBN 80-7329-000-6

[5] MLÝNEK,J.: *Zabezpečení obchodních informací*. 1.vyd. Brno: Computer Press, 2007. 154s. ISBN: 978-80-251-1511-4.

[6] KOSIUR, D. Elektronická komerce, principy a praxe. 1.vyd. Praha: Computer Press, 1999. 267s. ISBN 80-7226-097-9.

[7] RÁBOVÁ, Zdeňka. HANÁČEK, Petr. HRUBÝ, Martin. Prostředí pro modelování bezpečných systémů, In: Proceedings of NETSS06, Ostrava, CZ, MARQ, 2006, s. 39-42, ISBN 80-86840-06-9

[8] SMEJKAL, V. a kolektiv. Právo informačních a telekomunikačních systémů. 2. vyd. Praha: C. H. Beck, 2004. Str. 343., ISBN 80-7179-765-0

[9] SVOBODA, P. a kolektiv. Právní a daňové aspekty e-obchodu. 1. vyd. Praha: Linde, 2001. Str. 59, ISBN 80-7201-311-4

[10] DIEPOLT, J. Využití Internetu ve firmách vyžaduje analýzu bezpečnostních rizik. Business World, 2000, č. 5. ISSN 1213-1709.

[11] POUR, J. a kol. Informační systémy a elektronické podnikání. Praha: VŠE, 2001. 221 s. ISBN 80-245-0227-5.

[12] KOCH, Miloš, DOVRTĚL, Jan. Management informačních systémů. 1. vyd. 2006. 174 s. ISBN 80-214-3262-4.

[13] DVOŘÁK, J. Elektronický obchod 1. vyd. Brno: Vysoké učení technické v Brně, 2004. 78 s. ISBN 80-214-2600-4.

[14] PUŽMANOVÁ, Rita: Doporučení řady X, LANcom, 102 s., 1996, ISBN 80-902251-0-1

[15] PIPER, Fred, MURPHY, Sean. *Kryptografie*. [s.l.] : [s.n.], 2006. 160 s. ISBN 80-7363-074-5.

Internetové zdroje

[16] PETR , Nádeníček. Pravdy o elektronickém podpisu a šifrování (1-10). *Svět sítí & Infinity* [online]. 2003, roč. 5 [cit. 2009-04-12]. Dostupný z WWW:<http://www.svetsiti.cz/view.asp?rubrika=Technologie&clanekID=220>.

[17] Teorie a principy [online]. 1.CA, 2006 [cit. 2009-03-07]. Dostupný z WWW: <http://www.ica.cz/home_cs/?acc=teorie_a_principy>.

[18] NÁPRAVNÍK , Jiří. Starostové nechtějí elektronický podpis?. *Mesec.cz* [online]. 2005 [cit. 2009-04-18]. Dostupný z WWW: <http://www.mesec.cz/clanky/starostove-nechteji-elektronicky-podpis/>.

[19] HRAZDILA, Z. *Jak budovat a rozvíjet e-shop.* [online]. 16. 12. 2003. Dostupné z WWW:< http://interval.cz/clanky/jak-budovat-a-rozvijet-e-shop/>.

[20] NÁPRAVNÍK , Jiří. Elektronickým podpisem vydělal na cestu do vesmíru. Mesec.cz [online]. 2005 [cit. 2009-04-18]. Dostupný z WWW:<http://www.mesec.cz/clanky/elektronickym-podpisem-vydelal-na-cestu-do-vesmiru//>.

[21] PETR , Nádeníček. Pravdy o elektronickém podpisu a šifrování – Čipové karty a USB tokeny, aneb bezpečnější autentizace a šifrování - bezpečnostní požadavky na tokeny V. *Svět sítí & Infinity* [online]. 2003, roč. 5 [cit. 2009-03-12]. Dostupný z WWW: <http://www.svetsiti.cz/view.asp?rubrika=Technologie&clanekID=245>.

[22] *Komunikace : Komunikační desatero* [online]. Agora, 2007 [cit. 2009-02-15]. Www.agora-praha.cz. Dostupný z WWW: <http://www.agora-praha.cz/page-komunikace.html>.

[23] NÁPRAVNÍK , Jiří. Elektronická podatelna: Prostor pro kšeft?. *Mesec.cz* [online]. 2005, č. 8 [cit. 2009-04-12]. Dostupný z WWW: <elektronicka-podatelna-prostor-pro-kseft/>.

[24] *Digitální podpis a získání certifikátu* [online]. 2007 [cit. 2009-03-12]. Dostupný z WWW: <http://www.zoner.cz/photo-studio/digitalni-podpis.asp?vypis=vlastnosti>.

[25] KOUŘIL, Daniel. Certifikáty veřejných klíčů. *Zpravodaj ÚVT MU* [online]. 2005, roč. 9, č. 4 [cit. 2009-04-16], s. 5-9. Dostupný z WWW: <http://www.ics.muni.cz/zpravodaj/articles/181.html>. ISSN 1212-0901.

[26] KOUŘIL, Daniel. Správa soukromých klíčů pomocí hardwarových tokenů. *Zpravodaj ÚVT MU* [online]. 2005 [cit. 2009-04-11], s. 12-16. Dostupný z WWW: <http://www.ics.muni.cz/zpravodaj/articles/335.html>.ISSN 1212-090.

[27] *Elektronický podpis a jeho využití* [online]. 2006 , 3.10.2006 [cit. 2009-03-13]. HTML. Dostupný z WWW: <http://businessinfo.cz/cz/clanek/it-telekomunikace/elektronicky-podpis-a-jeho-vyuziti/1000473/2984/>.

[28] *Jak PGP pracuje* [online]. Skynet, s.s. , 2007 [cit. 2009-03-06]. Dostupný z WWW: <http://www.pgp.cz/index.php?l=cz&p=7&r=4>.

[29] VÍCHA, Květoslav. E-podpis za lidovku?. *Interval.cz* [online]. 2004, č. 12 [cit. 2009-04-16]. Dostupný z WWW: <http://interval.cz/clanky/e-podpis-za-lidovku/>.

[30] DOLEŽAL, Dušan. Jak si vybrat certifikační autoritu. *Interval.cz* [online]. 2003, č. 3 [cit. 2009-04-15]. Dostupný z WWW: <http://interval.cz/clanky/jak-si-vybrat-certifikacni-autoritu/>.

[31] *Hashovací funkce* [online]. Wikipedia, 2004 , 7.4.2007 [cit. 2009-04-06]. Dostupný z WWW: <http://encyklopedie.seznam.cz/heslo/443073-md5>.

[32] KNESCHKE, Jana. Netiketa - pravidla obchodních e-mailů. *Marketingové noviny : marketingovenoviny.cz* [online]. 2006 [cit. 2009-04-13]. Dostupný z WWW:<http://www.marketingovenoviny.cz/index.php3?Action=View&ARTICLE_ID=4175>.

[33] SATRAPA, Pavel. Netiketa. *Lupa.cz* [online]. 2005, č. 3. [cit. 2009-03-10]. Dostupný z WWW: <http://www.lupa.cz/clanky/netiketa/>.

[34] *Ochrana údajů (Evropská Unie)* [online]. 2005 [cit. 2009-03-17]. Dostupný z WWW: <http://ec.europa.eu/youreurope/nav/en/citizens/services/eu-guide/data-protection/index_cs.html>.

[35] INKLÁT, Václav. Šifrovací token iKey 3000. *www.linuxexpres.cz* [online]. 2006, č. 5 [cit. 2009-03-01]. Dostupný z WWW: <http://www.linuxexpres.cz/hardware/sifrovaci-token-ikey-3000>.

[36] NÁDENÍČEK, Petr. Pravdy o elektronickém podpisu a šifrování (12) - USB tokeny. *Www.svetsiti.cz* [online]. 2003 [cit. 2009-04-08]. Dostupný z WWW: <http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&temaID=244&clanekID=257>.

[37] Zákon o elektronickém podpisu: business.center.cz [online]. Business.center.cz, 2006 [cit. 2009-03-16]. Dostupný z WWW: <http://business.center.cz/business/pravo/zakony/epodpis/cast1.aspx>. ISSN 1213-723.

[38] KOMÁREK, Petr. Slavíme tři roky zákona o elektronickém podpisu. *Interval.cz* [online]. 2003 [cit. 2009-04-13]. Dostupný z WWW: <http://interval.cz/clanky/slavime-tri-roky-zakona-o-elektronickem-podpisu/>.

[39] VRABEC, Vladimír. Elektronické časové razítko, doplněk elektronického podpisu. *Interval.cz* [online]. 2003, č. 6 [cit. 2009-04-18]. Dostupný z WWW: <http://interval.cz/clanky/elektronicke-casove-razitko-doplnek-elektronickeho-podpisu/>.

[40] VÍCHA, Květoslav. E-podpis aneb testujeme digitální certifikáty. *Interval.cz* [online]. 2003, č. 3 [cit. 2009-03-22]. Dostupný z WWW: <http://interval.cz/clanky/e-podpis-aneb-testujeme-digitalni-certifikaty/>.

[41] DOLEŽAL, Dušan. Jak si vybrat certifikační autoritu. *Interval.cz* [online]. 2003 [cit. 2009-03-23]. Dostupný z WWW: <http://interval.cz/clanky/jak-si-vybrat-certifikacni-autoritu/>.

[42] DOLEŽAL, Dušan. Co to je digitální certifikát. *Interval.cz* [online]. 2003 [cit. 2009-04-10]. Dostupný z WWW: <http://interval.cz/clanky/co-to-je-digitalni-certifikat/>.

[43] PINKAVA, Jaroslav. Elektronický podpis. *Crypto-world.info* [online]. 2004 [cit. 2009-04-06]. Dostupný z WWW: <http://crypto-world.info/pinkava/prezentace/epodpis.ppt>.

[44] *Vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb* [online]. Www.micr.cz, 2006 [cit. 2009-03-12]. PDF. Dostupný z WWW: <http://www.micr.cz/scripts/detail.php?id=3630>.

[45] ARMS, William Y. . Key Concepts in the Architecture of the Digital Library. *D-lib magazine* [online]. 2006 [cit. 2009-03-12]. Dostupný z WWW: <http://www.dlib.org/dlib/July95/07arms.html>.

[46] BARTOŠEK, Miroslav. Digitální knihovny – teorie a praxe. *Ústav výpočetní techniky, Masarykova universita* [online]. 2004, roč. 15, č. 4 [cit. 2009-03-17], s. 233-254. Dostupný z WWW: <http://knihovna.nkp.cz/NKKR0404/0404233.html>. ISSN 1214-0678.

[47] TKAČÍKOVÁ, Daniela. Když se řekne digitální knihovna. *Ikaros.cz* [online]. 2003 [cit. 2009-04-17]. Dostupný z WWW: <http://www.ikaros.cz/node/1035>. ISSN 1212-5075.

[48] REJČÍŘ, Vlastimil. Systémy pro tvorbu digitálních knihoven. *Ikaros.cz* [online]. 2006, roč. 10, č. 5 [cit. 2009-03-21]. Dostupný z WWW: <http://www.ikaros.cz/node/3457>. ISSN 1212-5075.

[49] VOJNAR, Martin. Nové standardy digitálních knihoven pro dlouhodobou ochranu. *Vědecká knihovna v Olomouci* [online]. 2005 [cit. 2009-03-15]. Dostupný z WWW: <http://knihovna.nkp.cz/pdf/0502/050245.pdf>.

[50] DVOŘÁK, Jakub. PDF nemusí být vždy nedobytné. *IDnes.cz* [online]. 2006, roč. 9 [cit. 2009-03-15]. Dostupný z WWW: <http://technet.idnes.cz/pdf-nemusi-byt-vzdy-nedobytne-dkj-/software.asp?c=A060906_205656_software_dvr>.

[51] CZ.NIC – Statistiky [online] 2009 [cit. 2009-04-15]. Dostupný z WWW: <http://www.nic.cz/stats/?stat_type=1&zone=-1&time_step=month&from_year=2008&from_month=1&from_day=1&to_year=2009&to_month=5&to_day=13&submit=1>

[52] Elektronický obchod – BusinessInfo.cz [online]. 2007 [cit. 2009-04-14]. Dostupné z WWW: <http://www.businessinfo.cz/cz/rubrika/elektronickyobchod/1000819/>.

[53] *Envyklopedie seznam : Interenet* [online]. 2007 [cit. 2009-03-08]. Dostupný z WWW: <http://encyklopedie.seznam.cz/heslo/132239-internet>.

[54] Historie Internetu [online]. 2006 [cit. 2009-04-10]. Dostupný z WWW: <http://www.webdesign.paysoft.cz/clanky/2006/historie-internetu/>

[55] Ministerstvo vnitra ČR : Přehled kvalifikovaných poskytovatelů certifikačních služeb a jejich kvalifikovaných služeb [online]. 2007 [cit. 2009-05-04].

Dostupný z WWW:<http://www.mvcr.cz/clanek/prehled-kvalifikovanych-poskytovatelu-certifikacnich-sluzeb-a-jejich-kvalifikovanych-sluzeb.aspx>.

[56] Komunikační cesty internetu: E-mail | DSL.cz [online] 2005 [cit. 2009-01-21]. Dostupný z WWW: <http://www.dsl.cz/clanky-dsl/clanek-285/komunikacnicesty-internetu-e-mail>

[57] HRUBÝ, J. *Internet, připojení k němu a možný rozvoj*. [online] 2006 [cit. 2009-02-11]. Dostupné z: <http://www.internetprovsechny.cz/clanek.php?cid=167>

[58] VONDRUŠKA, P. *Crypto-World*. [online]. 2001 [cit. 2009-03-18].. Dostupné z:<http://platba.cz/cryptoworld/casop3/Crypto04_01.pdf>

[59] *Envyklopedie seznam : Kryptografie* [online]. 2007 , 23.12.2007 [cit. 2009-04-14]. Dostupný z WWW: <http://encyklopedie.seznam.cz/heslo/187096-kryptologie>.

[60] DOLEŽAL, Dušan. *Interval.cz* [online]. 2003 [cit. 2009-04-18]. Dostupný z WWW: <http://interval.cz/clanky/jak-si-vybrat-certifikacni-autoritu/>.

[61] *Root.cz : Šifrování souborů snadno a rychle* [online]. 2007 [cit. 2009-05-02]. Dostupný z WWW: <http://www.root.cz/clanky/sifrovani-souboru-snadno-a-rychle/>.

[62] *Šifrování.ic.cz : Šifrování* [online]. 2006 [cit. 2009-05-08]. Dostupný z WWW: <http://sifrovani.ic.cz/sifrovani-souboru>.

Přílohy

Seznam obrázků

Seznam tabulek

Utajeno dle přání dotčeného subjektu.

Další informační zdroje

Stránky městské části Brno – Žabovřesky:
http://www.brno.cz/zabovresky/o-zabovreskach/

Internetové stránky

http://www.ebiz.cz
http://www.rpa.cz
http://www.spir.cz
http://www.zive.cz
http://www.centrumeo.cz
http://www.e-commerce-magazin.de
http://www.spis.cz
http://www.ecommercebenchmarking.com/
http://www.interval.cz
http://www.e-commerce.cz
http://www.computerworld.cz
http://www.itaa.org
http://www.systemonline.cz
http://www.apek.cz
http://www.centrum.cz
http://www.ibusiness.de
http://www.isdn.cz
http://www.brezen.cz
http://www.cssi.cz
http://www.lupa.cz
http://www.itpravo.cz
http://www.shopfinder.cz
http://www.witsa.org
http://www.businessworld.cz

Vyhledávací portály

http://www.google.com
http://www.seznam.cz
http://www.centrum.cz
http://www.atlas.cz
http://www.yahoo.com
http://www.altavista.com
http://www.zbozi.cz
http://www.goto.com
http://www.quick.cz
http://www.excite.com
http://www.cent.cz
http://www.lycos.com

Skripta vysokých škol, vysokoškolské práce

JAROŠ, P. Model elektronického obchodu. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2006. 76s. Vedoucí diplomové práce prof. Ing. Jiří Dvořák, DrSc.

DVOŘÁK, J. Návrh internetové prezentace firmy. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2007. 65 s. Vedoucí bakalářské práce prof. Ing. Jiří Dvořák, DrSc.

FOURNÍK, R. *Elektronický obchod.* [online]. 2000. Dostupné z: http://home.zf.jcu.cz/~froula/e-commerce/html.1.html

PLEYER, J. *Transformace drobného a středního podnikání v podmínkách elektronické komerce.* [online]. 2001. Dostupné z: http://www.pleyer.cz/diplomka

VUČKA, J. *Vybrané právní aspekty elektronického obchodu.* [online]. 2001. Dostupné z: http://mujweb.cz/www/cyberlaw/aspects.htm

PODOBA, Tomáš. Modelovací postupy pro trojrozměrnou vizualizaci. 2005. 68 s. Univerzita Tomáše Bati ve Zlíně. Vedoucí bakalářské práce Ing. Pavel Pokorný, Ph.D. CERM, 2005. 161 s. ISBN 80-214-2803-1.

Digitální knihovny

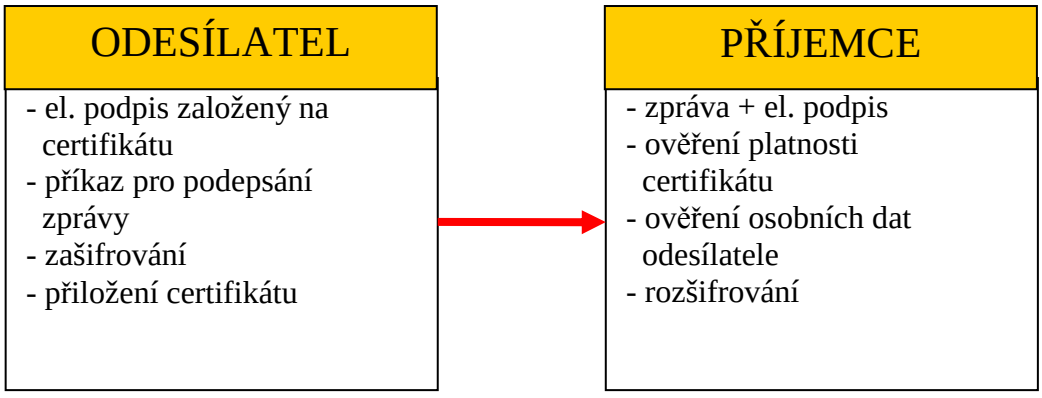
VPK	http://www.vpk.cz
EDD CVUT	http://edd.cvut.cz/edd/readme.php
Document Delivery NK ČR	http://doc.nkp.cz/php/bridge.php?con=start
VŠE a Cerge	http://ciks.vse.cz/veda-vyzkum/edd.asp
EDD SVK HK	http://sukhk.cz/zobraz.asp?id=112
EODD	http://knihovna.vsb.cz/eodd/index.html
British Library Centre	http://www.bl.uk/services/document/dsc.html
Library TU Delft	http://www.library.tudelft.ul
SUBITO	http://www.subito-doc.de
JASON	http://ub.uni-bielefeld.de/english/databases/jason
UNCOVER	http://www.ingenta.com
Digitální knihovna VŠ prací	http://www1.cuni.cz/~brt/dvk/dvk3.htm
Seznamy digitálních knihoven	http://www1.cuni.cz/~brt/dk/dk2.htm
Digitální knihovna historických fondů	http://dig.vkol.cz
Česká elektronická knihovna	http://www.ucl.cas.cz/ek/index.php?pg=about
Digitální knihovna plnotextových dokumentů	http://www.cuni.cz/~brt/dk/dk.htm
Česko-slovenská knihovna parlamentních spisů	http://www.psp.cz/kps/knih/elknih.htm
Digitální knihovny v medicíně	http://www.sweb.cz/hnemeskalova/dk.htm
E-LIB	http://www.ukoln.ac.uk/services/elib
Vascoda	http://www.vascoda.de
The Australian Subject Gateways Forum	http://www.nla.gov.au/initiatives/sg/gateways.html
Gellica	http://gallica.bnf.fr/
American Memory	http://memory.loc.gov/ammem/index.html
Digital Library of Canada	http://www.collectionscanada.ca/index-e.html
National Diet Library	http://www.ndl.go.jp/en/index.html

E-podatelny

- ProIT, a.s. http://www.proit.cz
- PVT, a.s. http://www.pvt.cz
- AEC, spol. s r.o. http://www.aec.cz
- INFIMA Software, s.r.o. http://www.infima.cz
- Triada, spol s r.o. http://www.triada.cz
- GORDIC, spol. s r.o. http://www.p-ji-ext.gordic.cz
- DIGNITA, s.r.o. http://www.dignita.cz
- Software602, a.s. http://www.602.cz

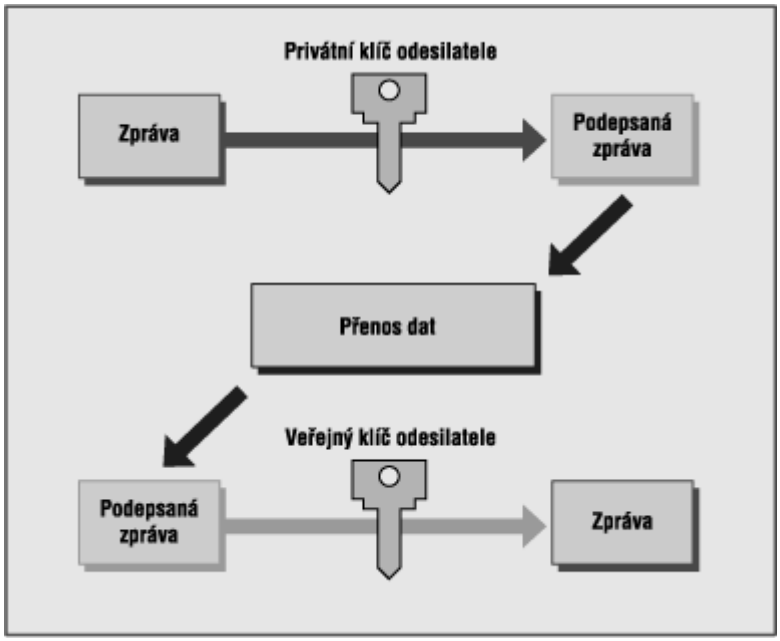
Seznam příloh

Příloha č. 1: Jednoduché schéma odesílání a přijímání digitálně podepsaných zpráv



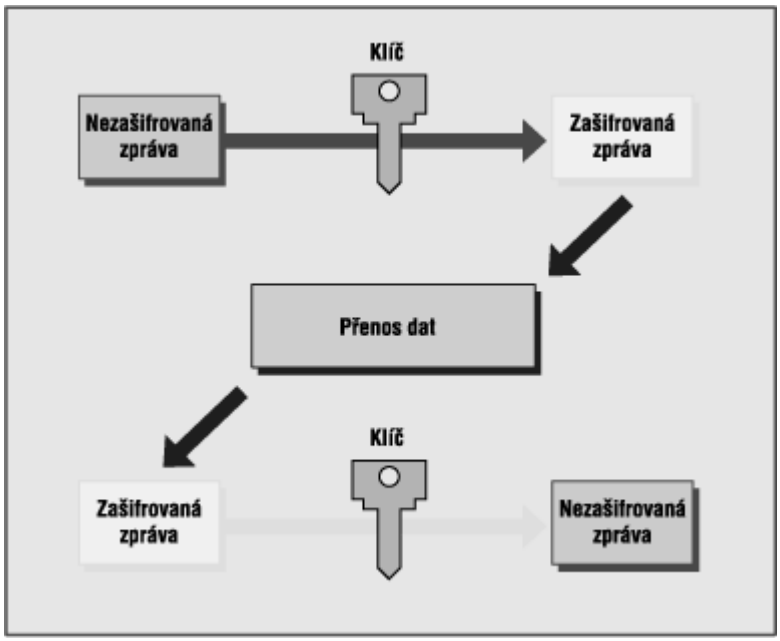
Zdroj:
http://www.ica.cz/home_cs/?acc=teorie_a_principy

Příloha č. 2: Asymetrické šifrování



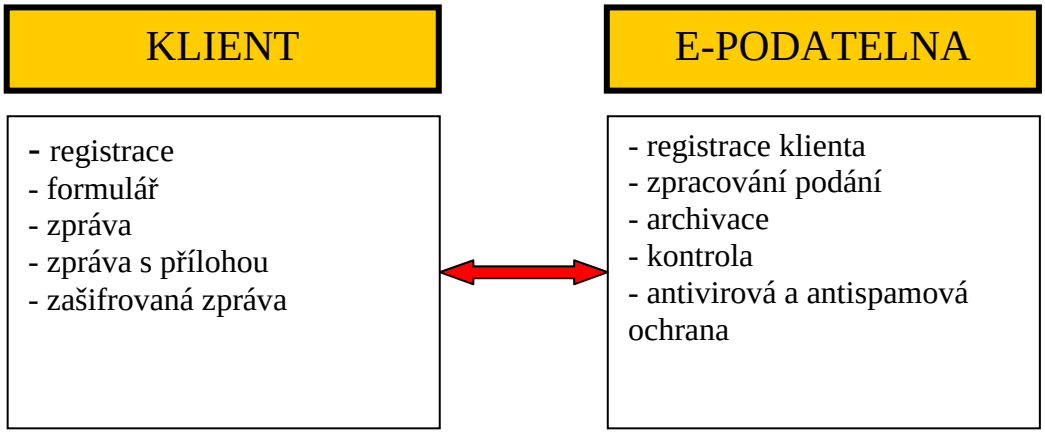
Zdroj:
http://www.ica.cz/home_cs/?acc=teorie_symetricke_a_asymetricke_kryptografie

Příloha č. 3: Symetrické šifrování



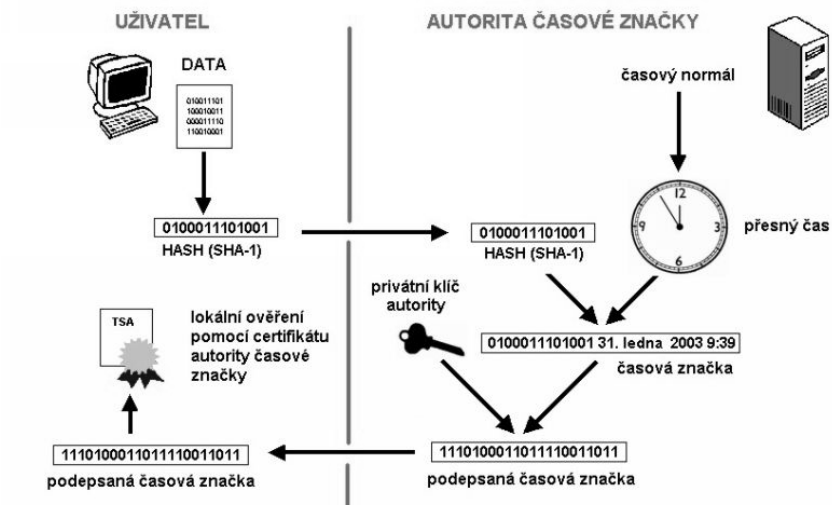
Zdroj:
http://www.ica.cz/home_cs/?acc=teorie_symetricke_a_asymetricke_kryptografie

Příloha č. 4: Jednoduché schéma e-podatelny



Zdroj:
http://www.ica.cz/home_cs/?acc=teorie_a_principy

Příloha č. 5: Schéma funkce časového razítka



Zdroj:
http://www.trustport.cz/images/TSA_cz.jpg

Slovník pojmů a použitých zkratek

SMTP / Simple Mail Transfer Protocol - elektronická pošta, e-mail.

FTP / File Transfer Protocol - přenos vzdálených souborů.

Telnet - virtuální terminál, vzdálený přístup.

NFS / Network File System - sdílení vzdálených souborů.

DHCP / Dynamic Host Configuration Protocol - dynamická konfigurace síťové stanice

SNMP / Simple Network Management Protocol - jednoduchý protokol pro správu sítě

HTTP / Hypertext Transfer Protocol, World Wide Web

DNS / Domain Name System - překlad doménových jmen

Akceptace rizika - rozhodnutí přijmout existující úroveň rizika.

Analýza rizik - proces, který slouží k odhadu ztrát, jež mohou vzniknout působením hrozeb na systém.

Autentizace - poskytnutí záruky týkající se identity subjektu.

Autorizovaný uživatel - uživatel, který má určité právo nebo povolení pracovat v IS.

Bezpečnost informací - vlastnost nebo stav ochrany informací proti ztrátám.

Bezpečnost IS - ochrana IS a informací, které jsou v nich uchovávány a zpracovávány.

Bezpečnostní cíle - stav bezpečnosti, který má daný systém nebo produkt dosáhnout.

Bezpečnostní funkce - funkce provádějící požadovanou činnost, zajišťující realizaci bezpečnostních požadavků.

Bezpečnostní manažer - zaměstnanecká role pro výkon odpovědnosti

Bezpečnostní opatření - souhrn prostředků a opatření, kterými je prosazována bezpečnostní politika s cílem navodit požadovaný stupeň bezpečnosti.

Bezpečnostní politika IS - celkový záměr vedení a směr řízení bezpečnosti informací se stanovením kriterií pro hodnocení rizik.

Bezpečnostní událost - identifikovaný stav systému, ukazující na možnost porušení bezpečnostní politiky nebo selhání bezpečnostních opatření.

Citlivá data -chráněná data mající pro chod organizace zásadní význam.

Důvěrnost - zajištění, že informace jsou přístupné pouze tomu, kdo je k jejich přístupu oprávněn.

Firewall - bezpečnostní prvek ochrany sítě.

Hrozba - potenciálně ničivá fyzikální událost.

HW / Hardware - technické vybavení.

ID / Identification - identifikátor uživatele.

Informační bezpečnost - bezpečnost při manipulaci s informacemi, především vzhledem k požadavkům na důvěrnost, integritu a dostupnost informací.

Integrita - zajištění správnosti, úplnosti a aktuálnosti informací a softwaru k jejich zpracování.

ISMS / Information Security Management System - Systém řízení bezpečnosti informací. Součást řízení organizace, zaměřená na řízení rizik a zlepšování bezpečnosti IS organizace.

ISO / International Organization for Standardization - Mezinárodní organizace pro normalizaci

LAN / Local Area Network - lokální počítačová síť.

OS - operační systém.

Produkt - softwarový nebo hardwarový výrobek IT zabezpečující funkce, navržené pro přímé využití nebo k začlenění do různých systémů.

Přístupové právo - uživateli nebo subjektu přidělené oprávnění uskutečňovat typ přístupu.

Server - uzlový počítač sítě.

SW / Software - programové vybavení.

UPS / Uninterruptible Power Supply - nepřerušitelný zdroj napájení.

Uživatel / User - Součást systému, která v rozsahu přidělených pravomocí využívá informace systému, zajišťuje vstupní informace potřebné pro identifikaci objektu nebo prostředku.

VPN / Virtual Private Network - virtuální privátní síť.