INFORMACE

V CESTOVNÍM RUCHU

OBCHODOVÁNÍ NA INTERNETU, BANKOVNÍ SLUŽBY, ELEKTRONICKÁ CERTIFIKACE, DIGITÁLNÍ PODPISY A DALŠÍ NOVÉ TRENDY ICT

www.vzdelavanivcr.cz

esf evropský sociální fond v ČR

MPSV

MINISTERSTVO PRO MÍSTNÍ ROZVOJ

OBCHODOVÁNÍ NA INTERNETU, BANKOVNÍ SLUŽBY, ELEKTRONICKÁ CERTIFIKACE, DIGITÁLNÍ PODPISY A DALŠÍ NOVÉ TRENDY ICT

RNDr. Bohumír Štědroň, CSc.

Singular Czech, s.r.o.

Praha 2007

Obchodování na internetu, bankovní služby, elektronická certifikace, digitální podpisy a další nové trendy ICT

Vydalo: Ministerstvo pro místní rozvoj ČR, Praha, 2007.
Staroměstské náměstí 6, 110 15 Praha 1, www.mmr.cz

Tato skripta byla vytvořena pro projekt „Informace v cestovním ruchu“
CZ.04.1.03/4.2.00.1/0007 Operační program Rozvoj lidských zdrojů (OP RLZ), Opatření 4.2., Specifické vzdělávání.

Tento vzdělávací program je spolufinancován Evropským sociálním fondem (ESF)
a státním rozpočtem ČR.

1 Obsah

2 Předmluva:

Rychlý vývoj informačních a telekomunikačních technologií (ICT) vyžaduje i inovaci znalostí a postupů všech segmentů ekonomiky od cestovních kanceláří až po bankovní služby. Na tyto požadavky reaguje předkládaná publikace, která se zabývá novými trendy v segmentu ICT jako e-banking, RFID, elektronický podpis a mnoho dalších.
Autor děkuje recenzentům prof.ing.J.Daňhelovi,CSc. z VŠE, ing.Petru Budišovi,Ph.D. CEO ICA , generálnímu řediteli firmy Singular Czech Efstathios Amoutzasovi a výkonnému řediteli Asociace pro elektronickou komerci Bc.Janu Vetyškovi za náměty i kritické připomínky, které byly do textu zapracovány. Autor dále děkuje Mgr.V.Zvánovcovi z Úřadu pro ochranu osobních údajů za připomínky k částem , týkajícím se ochrany osobních údajů a elektronického podpisu.

RNDr.Bohumír Štědroň,CSc.
soudní znalec v oboru kybernetika

3 Úvod

Když se 17.prosince 1903 Orvillu Wrightovi podařil v USA první úspěšný let letadlem, vytvořil nový dopravní prostředek. Dnes po více než sto letech změnil tento vynález civilizaci: povrch celé planety je protkán sítí letišť a infrastrukturou leteckých, servisních a cestovních společností. Mnohem podstatněji však změnil tvář civilizace objev počítače, který je spojován v polovině minulého století se jmény K.Zuse, S.Williams, G.Stibitz, J.Atanasoff, C.Berry a mnoha dalšími.

Vývoj technologických komponent počítačů probíhal podle tzv. Moorova zákona (přibližně každého 1.5 roku se počet tranzistorů na čipu zdvojnásobí a totéž platí o dalších hardwarových komponentách jako je kapacita disků, rychlost aj.) a bylo zřejmé, že bez počítače je nepřestavitelná existence úspěšné strategické obrany i útoku každé velmoci. Na ruský náskok v raketové technice, demonstrovaný první umělou družicí Země v roce 1957, reagovala americká vláda rovněž založením Advanced Research Projects Agency (ARPA) zabývající se speciálním výzkumem. V šedesátých letech americká armáda řešila obranný úkol, jak zajistit, aby armádní počítače rozmístěné po celém území USA mohly spolu bez problému komunikovat, a to i v případě, že část této sítě bude vyřazena z provozu. Pracovníci RAND Corporation přišli s unikátním řešením - vybudování sítě bez centrálního uzlu: Informace bude vedena k příjemci jinou trasou, pokud bude některá linka zničena.

O dvacet let později v roce 1989 vymyslel Tim Berners-Lee nový způsob komunikace: hypertextové dokumenty. Texty, které obsahují odkazy na další dokumenty, mohou být umístěny na jiném počítači, třeba na druhém konci světa. V důsledku jednoduchého ovládání se tento způsob komunikace rozšířil i mimo CERN a dnes jej známe pod jménem World Wide Web. Masové rozšíření osobních počítačů zapříčinilo, že miliony nových uživatelů Internetu začaly využívat jednoduchou komunikaci prostřednictvím www-stránek. Komerční provoz na internetu se datuje od roku 1992, kdy National Science Foundation, která do této doby byla odpovědná za páteřní síť internetu, umožnila připojení i komerčním subjektům. Rokem 1993 začal Internet v USA prožívat nebývalý rozmach, k Internetu je připojen Bílý dům. Od roku 1993 do roku 1995 se zdvojnásobil počet připojených počítačů k Internetu. V roce 1995 je již v USA k Internetu připojeno na dva milióny počítačů. Souhrnné odhady v roce 1995 mluví o 20 miliónech uživatelů Internetu, později v roce 2000 je přes 300 miliónů uživatelů Internetu.

Komerční využívání Internetu se rychle rozvijí. V nedávné době byl Internet využíván čistě pro informační a reklamní účely. Jednotlivé společnosti zveřejňovaly svoje Internetové adresy, na kterých byly více či méně přehledné či více či méně komplexní informace o firmě.

Dnes už je situace jiná, většina lidí se zajímá o nabízené zboží a služby a předpokládá a očekává, že se o nich dozví rychle a přehledně právě na Internetu. O tom ostatně jasně hovoří i přehledné statistiky, uvedené v úvodní kapitole této knihy.

Nejpoužívanější cestou k získání informací je využití služeb takzvaných vyhledávačů. S jejich pomocí je možné najít na Internetu téměř cokoliv. Informace o jejich používání a přehledné statistiky jejich využívání uživateli Internetu jsou uvedeny ve druhé kapitole této knihy, Webové služby. Internet se stává i zajímavým podnikatelským prostředím, o čemž mimo jiné svědčí i ekonomické parametry společností, nabízejících elektronické služby.

Chceme-li Internet využívat pro obchodní účely, je nutné zajistit tomuto prostředí dostatečnou bezpečnost a legislativní oporu. Jedním z klíčových, opěrných bodů této publikace je proto téma elektronického podpisu. Zákon č. 227/2000 Sb., o elektronickém podpisu položil základ bezpečné elektronické komunikaci a většina kvalitních komerčních aplikací je na této technologii založena.

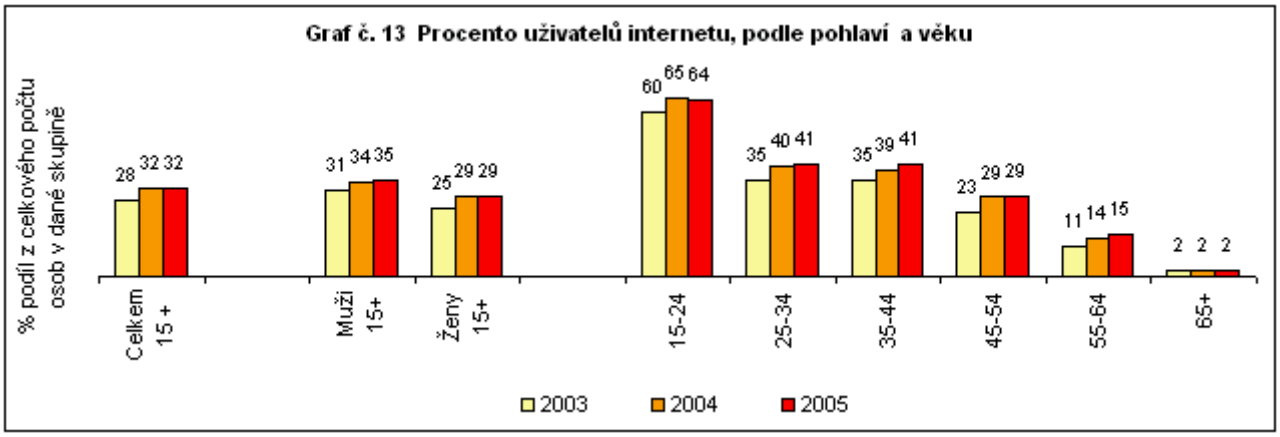
Mezi průkopníky bezpečnostních technologií a elektronického podpisu jsou z pochopitelných důvodů na prvním místě banky. Ty rychle pochopily přednosti komerčního využívání Internetu, ale i jeho nedostatky, dané nízkou bezpečností tohoto síťového prostředí. Proto do bezpečnosti investují nemalé prostředky. I přesto se množí různé formy útoků na klienty bank a jsou až překvapivě úspěšné. V kapitole E-kriminalita jsou některé publikované útoky popsány a rozebírány.

Mnozí z nás užívají některý z kanálů elektronického bankovnictví. Jejich využití je v podstatě dvojí. Jednak je to ovládání a vlastní zpráva našeho bankovního účtu a dále také je to nový platební nástroj. V případě, že chceme prostřednictvím Internetu získat nějakou službu, obvykle nastává problém s placením, a právě zde můžeme využít některé kanály elektronického bankovnictví. Více se dozvíte v kapitole věnované elektronickému bankovnictví a obchodování na Internetu.

4 Fenomén Internet

Formální připojení tehdejší ČSFR k internetu se slavnostně uskutečnilo 13. února 1992. Internet byl tedy dostupný v Praze na ČVUT, ale postupně se rozšířil na všechny vysoké školy z celé republiky. Již předtím, v prosinci 1991, schválilo České ministerstvo školství projekt předložený akademickou obcí a v červnu 1992 uvolnilo 20 miliónů korun pro sítě spojující univerzitní města. Po rozdělení ČSFR vznikl CESNET a SANET. V listopadu 1992 byly pevnou linkou propojeny Praha a Brno - dva hlavní uzly sítě CESNET - a v březnu 1993 bylo připojeno dalších 9 měst.

O 14 let později je již situace zcela změněna: pokud za uživatele internetu je považován jednotlivec, který použil internet v posledních 3 měsících, podle údajů ČSÚ a mezinárodních statistik je možno konstatovat, že v roce 2005 37% populace ČR ve věku 15 let a více někdy použilo internet. Uživatelů internetu bylo v roce 2005 32% populace ve věku 15 let a více. Uživatelů internetu je více mezi muži než ženami a více mezi mladšími než staršími. Stejně jako v případě použití počítače, také internet je nejvíce používán studenty, mladými lidmi ve věku 15–24 let a jednotlivci s vysokoškolským vzděláním. Nejméně internet používají jednotlivci ve věku 65 a více let. Nezanedbatelný vliv na počet uživatelů internetu má i lokalita, kde jednotlivec žije. Ve městech je podíl uživatelů internetu na celkové populaci výrazně vyšší než je tomu na venkově.

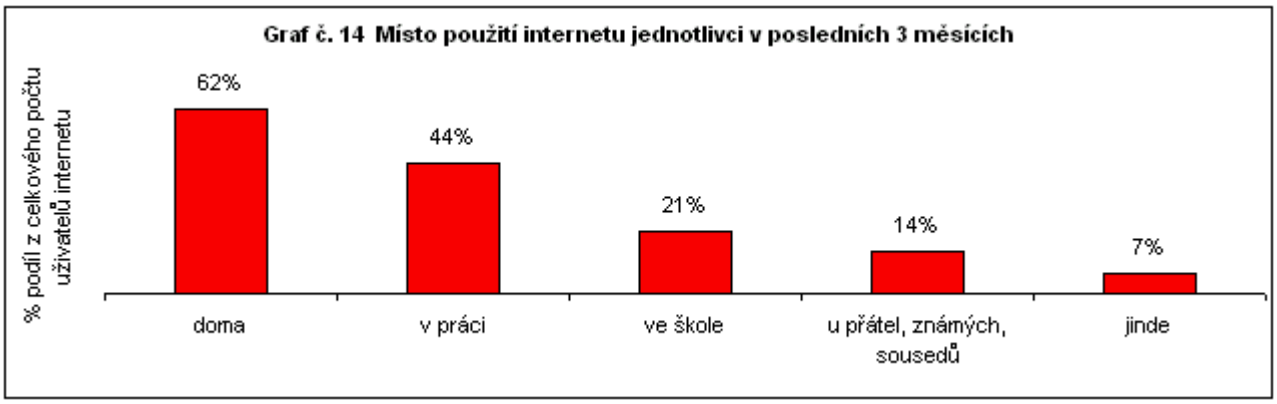


Šetření za rok 2003 proběhlo ve 4.čtvrtletí 2003, za rok 2004 ve 4.čtvrtletí 2004, za rok 2005 v 1.čtvrtletí 2005 Zdroj: ČSÚ, 2005

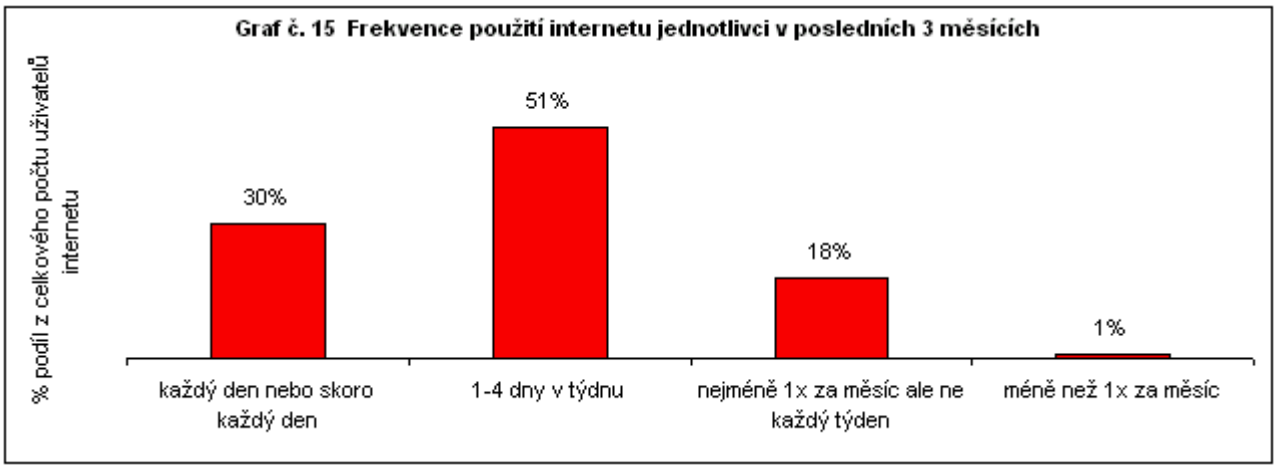
Podrobnější výsledky za rok 2005

Z uživatelů internetu (jednotlivců, kteří použili internet v posledních 3 měsících) se nejvíce osob připojilo k internetu z domova (62%), dále z práce (44%) a ze školy (21%). Od přátel, známých nebo sousedů se připojilo 14% uživatelů a z jiného místa (knihovna, internetová kavárna, atd.) 7% uživatelů (graf č. 14).

Přibližně polovina (51%) uživatelů použila internet 1 až 4 dny v týdnu, téměř třetina (30%) každý den nebo skoro každý den a přibližně pětina (19%) nejméně 1x za měsíc a méně často (graf č. 15).



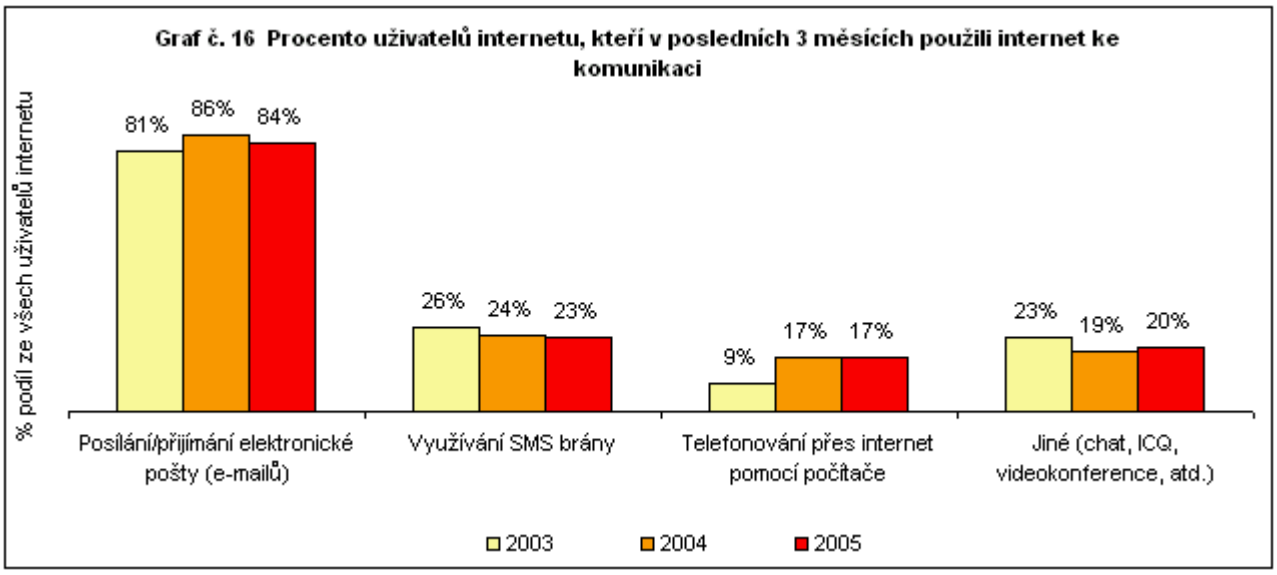
Šetření proběhlo v 1.čtvrtletí 2005 Zdroj: ČSÚ, 2005



Šetření proběhlo v 1.čtvrtletí 2005 Zdroj: ČSÚ, 2005

Komunikace přes internet

Nejpopulárnější ze všech činností je internetová komunikace. Uživatelé internetu nejvíce využívají posílání a příjímání elektronické pošty (e-mailů). V posledních 3 měsících použilo elektronickou poštu 84% uživatelů internetu. Stále populárnější se stává využívání internetu k telefonování, kde došlo k nárůstu podílu uživatelů internetu využívajících internet k telefonování z 9% v roce 2003 na 17% v roce 2005.



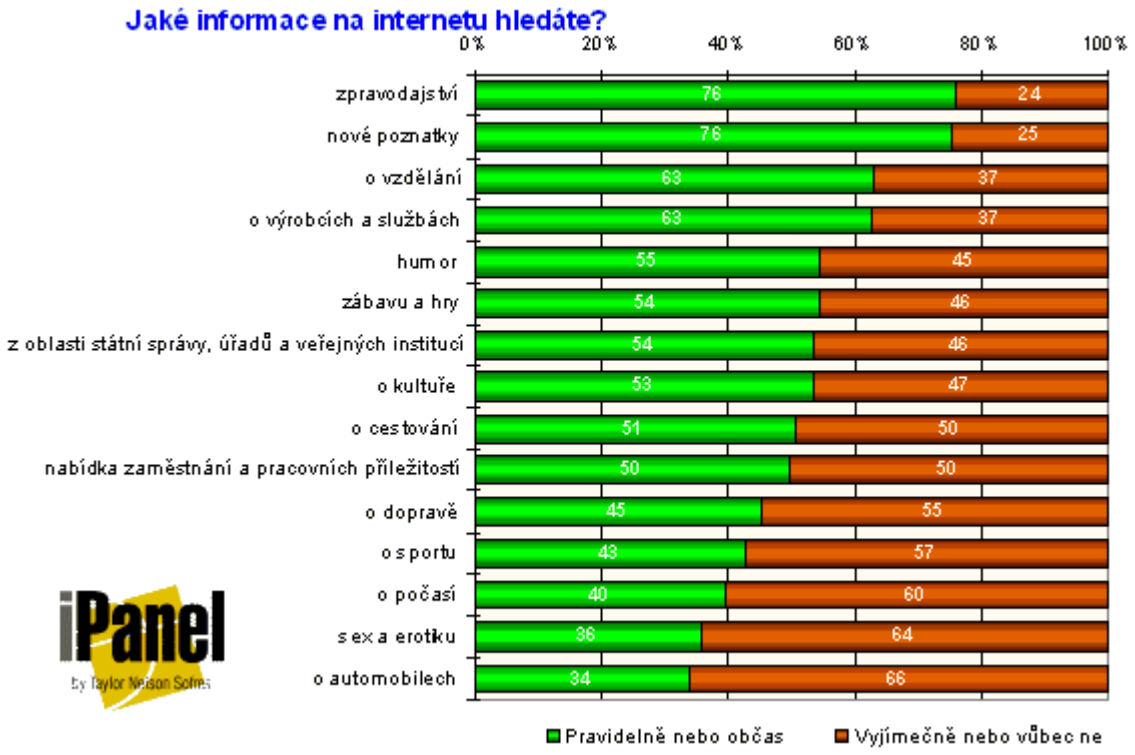
Šetření za rok 2003 proběhlo ve 4.čtvrtletí 2003, za rok 2004 ve 4.čtvrtletí 2004, za rok 2005 v 1.čtvrtletí 2005 Zdroj: ČSÚ, 2005

Vyhledávání bezplatných informací a on-line služeb – v roce 2005

Vyhledávání bezplatných informací a on-line služeb je nejčastější aktivita zájemců o internet. K nejpopulárnějším činnostem na internetu patří vyhledávání informací o zboží a službách (v posledních 3 měsících využilo 62% uživatelů internetu), vyhledávání a stahování odborných textů (54%), vyhledávání služeb týkajících se cestování a ubytování (38%), prohlížení a stahování on-line novin a časopisů (36%) a hraní a stahování počítačových her a hudby (28%). Zajímavé jsou bezesporu následující tabulky:

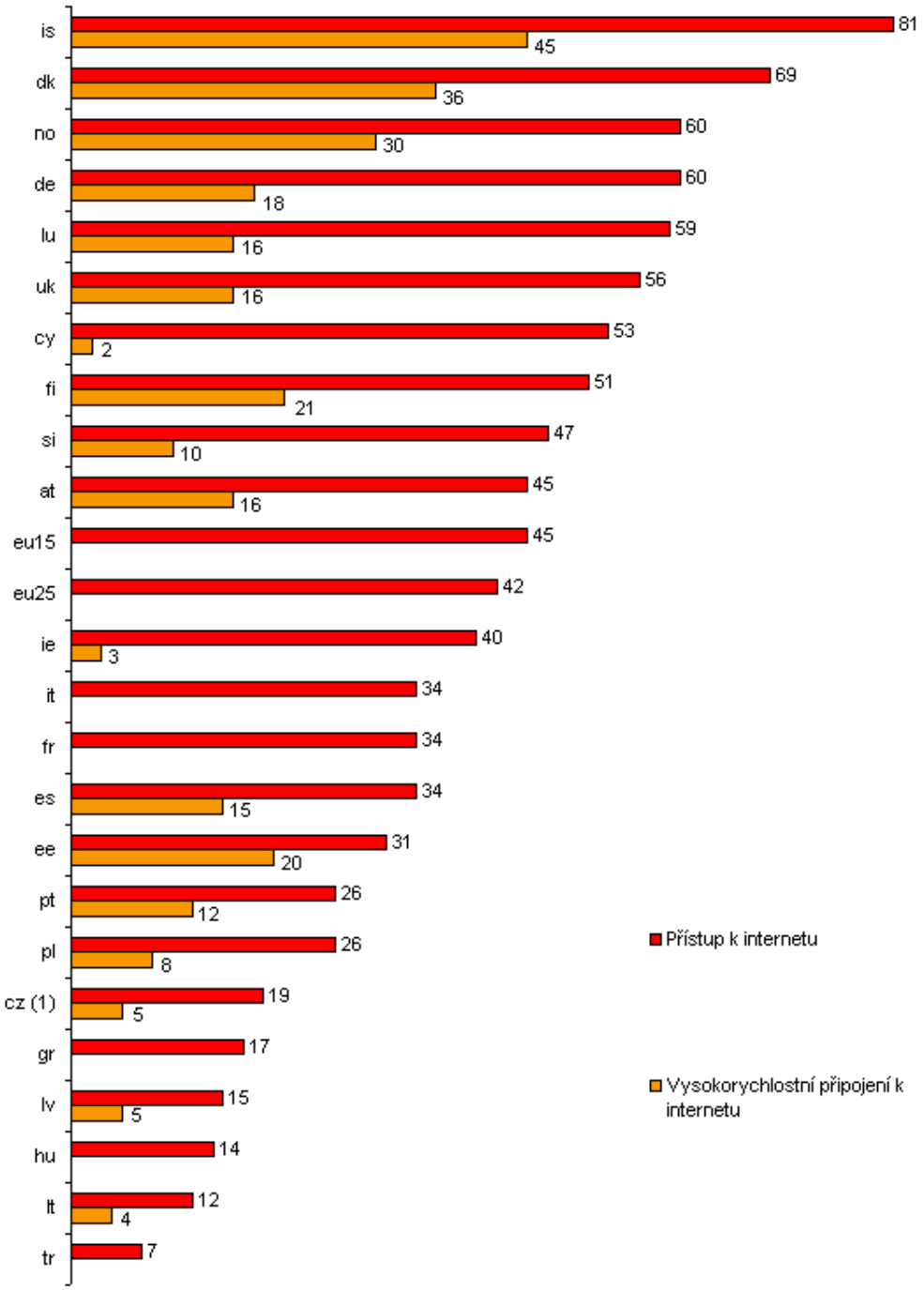
Šetření proběhlo v 1.čtvrtletí 2005 Zdroj: ČSÚ, 2005

Jaké informace na internetu hledáte?



2. Stav internetu, porovnání s Evropou

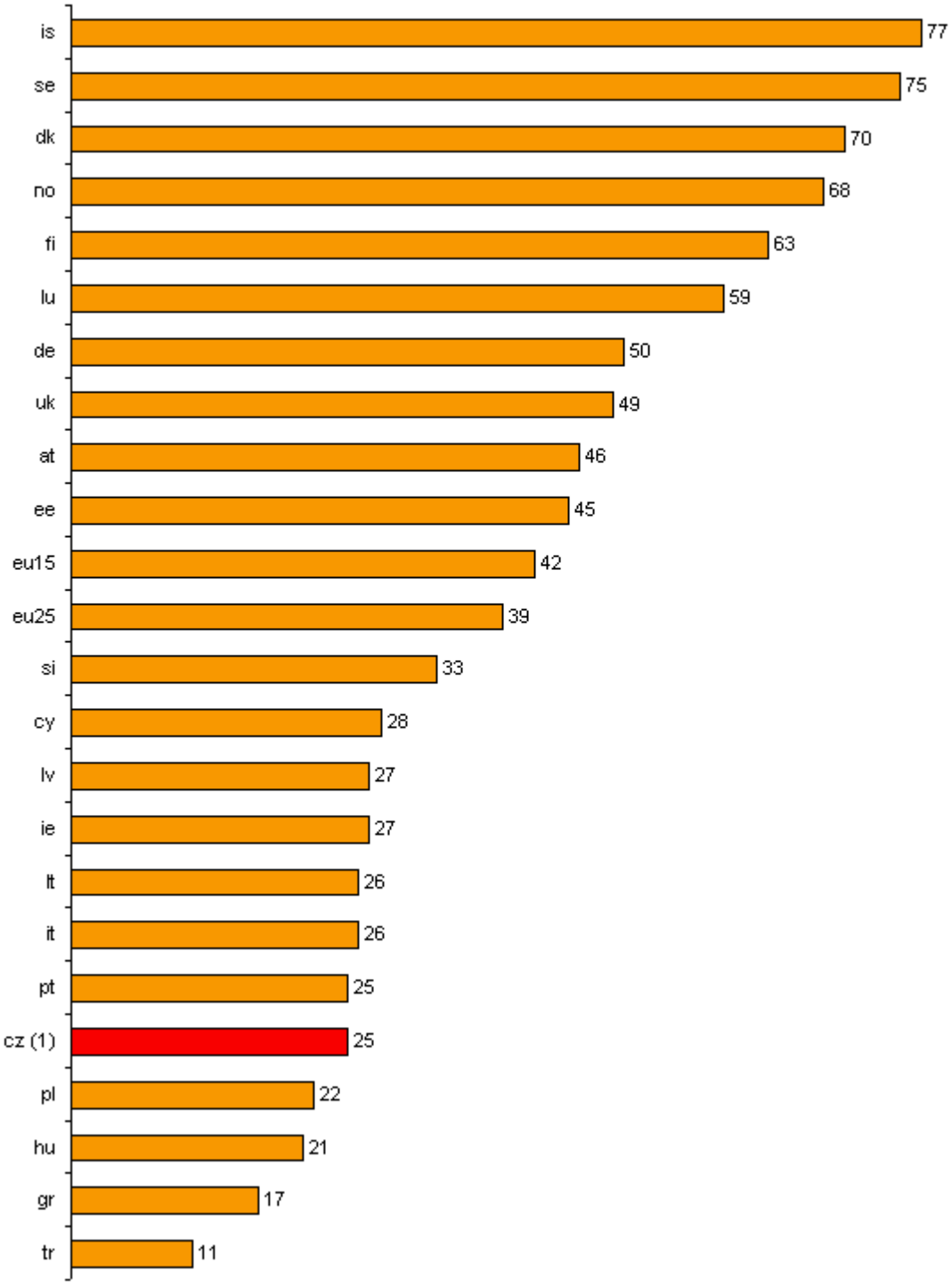
Graf č. 20 Procento domácností* s přístupem k internetu v 1.čtvrtletí 2004



*

Podíl na celkovém počtu domácností
(1) 4.čtvrtletí 2004
Zdroj: Eurostat, Community Household survey on ICT usage 2004
Šetření o využívání ICT v domácnostech a mezi jednotlivci v roce 2004, ČSÚ

Graf č. 21 Procento jednotlivců* , kteří v posledních 3 měsících pravidelně (alespoň jednou týdně) používali internet (údaje za r. 2004)

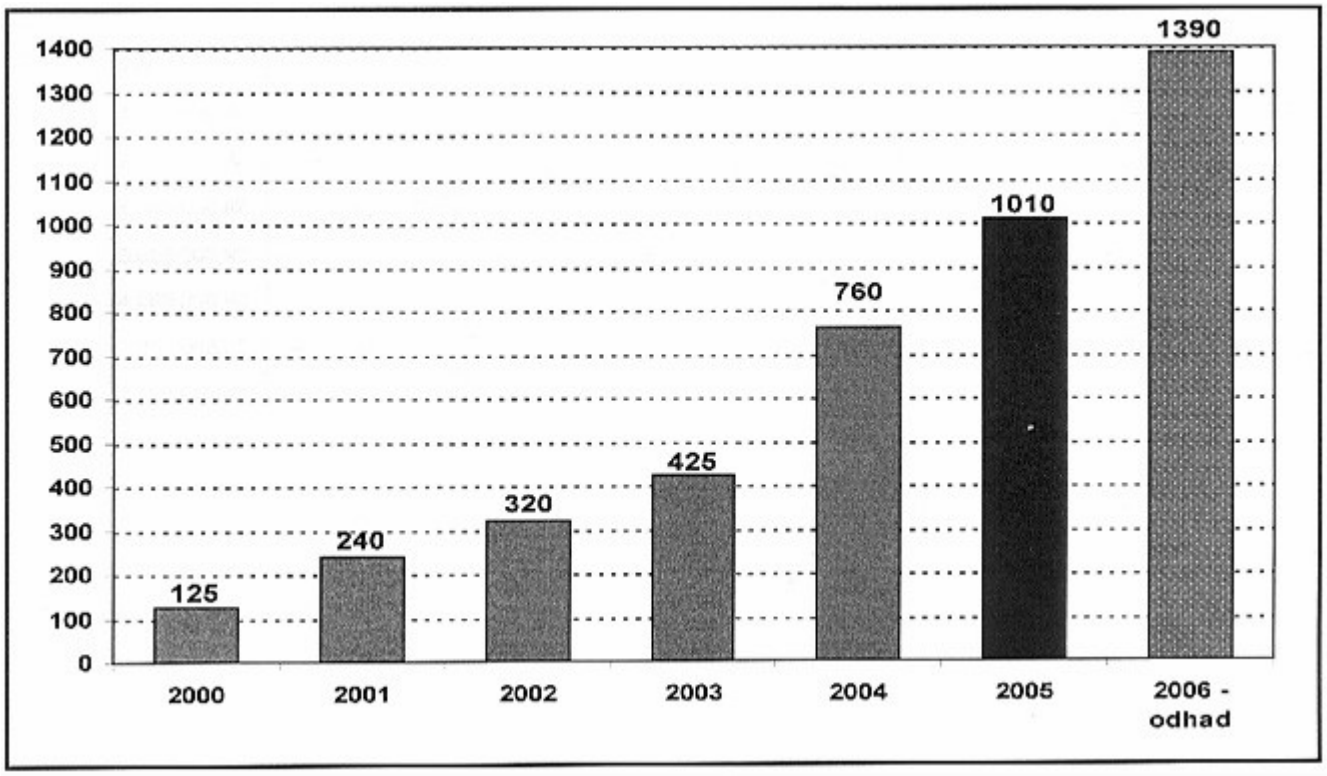


* Podíl na celkovém počtu jednotlivců ve věku 16 až 74 let (ČR – osoby ve věku 15 let a více)
Pozn.: šetření proběhlo v 1.čtvrtletí 2004

šetření proběhlo ve 4.čtvrtletí 2004

Zdroj: Eurostat, Community Household Survey on ICT Usage 2004;
Šetření o využívání ICT v domácnostech a mezi jednotlivci v roce 2004, ČSÚ

Objem internetové reklamy v letech 2000 – 2006 (v mil. Kč, rok 2006 – odhad)



Zdroj: SVIT (Sekce vydavatelů internetových titulů)

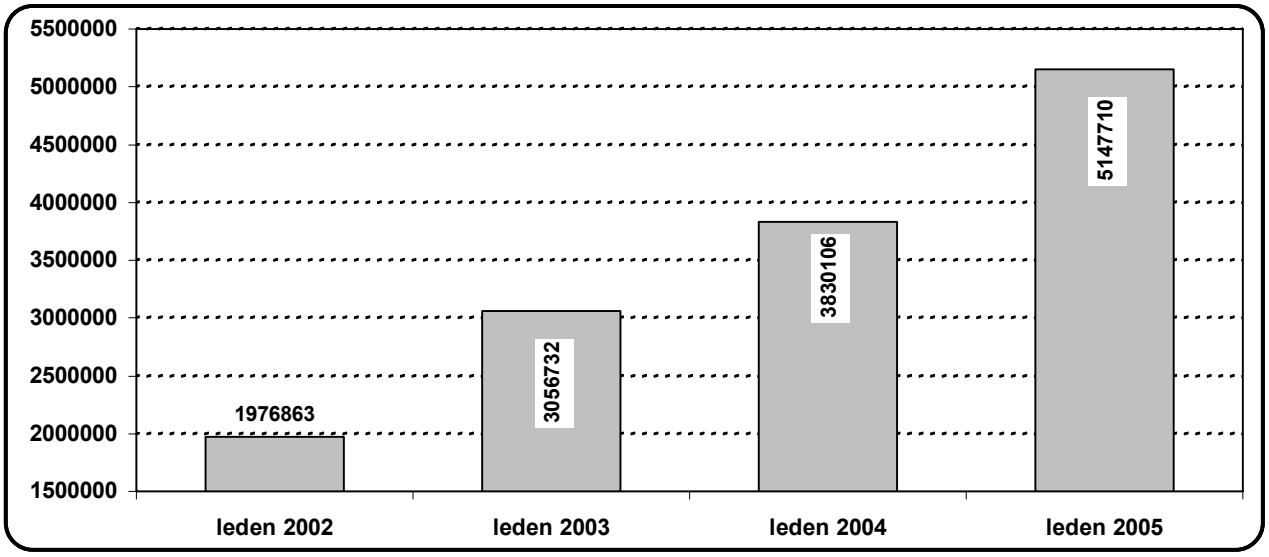
Pro rok 2005 SVIT na základě předpokladů účastníku průzkumu odhadoval nárůst o 36%. Předpokládal tak, že hrubý obrat internetové reklamy v roce 2005 dosáhne hodnoty 1,034 miliardy Kč. Odhadované tempo růstu je v roce 2005 nižší, než skutečné tempo dosažené v roce 2004, což je dáno tím, že nelze očekávat souhru tolika příznivých faktorů, jako v roce 2004. I tak ale bude internet stále nejdynamičtěji se rozvíjejícím reklamním mediem.

Je třeba konstatovat, že odhad tempa růstu internetové reklamy, který SVIT pro rok 2004 vydal v únoru roku 2004, se ukázal jako příliš restriktivní. Původně odhadovaný nárůst o 25% byl nakonec více jak trojnásobnou skutečností překonán. Ukázalo se, že pozitivní vliv vstupu komodity rychloobrátkového zboží do internetové reklamy, o kterém sekce před rokem uvažovala jako o hlavním faktoru růstu, se projevil nakonec ještě intenzivněji, než se předpokládalo. Navíc byl tento hlavní růstový moment podpořen ještě dalšími pozitivními činiteli, ze kterých je třeba upozornit především na vliv vstupu České republiky do EU, který posílil zájem o internet a také rostoucí počet uživatelů internetu vyplývající z výsledků iAuditu (viz tabulka), přičemž tento zájem se soustřeďuje zejména na obchodně nejvýznamnější servery a servery s kvalitním specializovaným obsahem. Prudký nárůst reklamních příjmů internetu v důsledku neočekávaně příznivých okolností potvrzují pro rok 2004 i některé další odhady renomovaných agentur.

Hrubý reklamní obrat je souhrnem hrubých reklamních obratů s přímými klienty, reklamními agenturami, mediálními agenturami, mediálními zastupitelstvími. Nezapočítávají se do něj bannerové bartery.

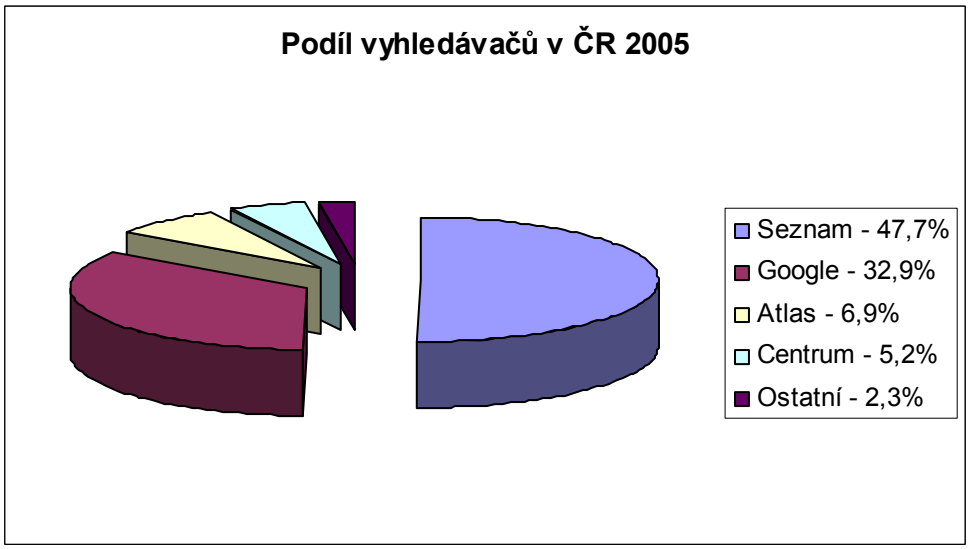
Počet uživatelů internetu v ČR v letech 2002 – 2005

Zdroj: iAudit International leden 2002 až leden 2005, www.iaudit.info



Uvedené údaje www.iaudit.info zahrnují i zahraničí; podle ČSÚ byl počet uživatelů internetu v ČR v roce 2005 vyjádřen číslem 3.54 milionu uživatelů (podobná čísla prezentuje i SPIR a NetMonitor).

Mezi základními službami, které Internet nabízí, dominuje možnost vyhledávání informací. Na českém Internetu převažují v oblasti vyhledávání až na jednu výjimku zaběhnuté portály. Pokud přicházejí zájemci na web z vyhledávače, pravděpodobně je jím Seznam, který svou dlouhodobě dominantní pozici drží okolo poloviční podílu, letošní měření mu přisoudilo 47,70 procenta. Na druhém místě figuruje zahraniční vyhledávač Google, který v součtu svých jazykových platforem dosáhl rekordních 32,90 procenta. Poslední vývoj na českém internetu ukazuje, že Google stahuje velký náskok portálu Seznam, ten je ale stále nejmocnějším vyhledávačem na českém Internetu, když drží téměř poloviční podíl na trhu.



Zdroj: toplist.cz

Zajímavé informace přináší následující tabulka:

Table 1. Top 5 Search Engines and Latest Share of Searches, June & October 2005

Provider	Jun-05 Searches (000)	Oct-05 Searches (000)	June to Oct. Growth	Oct-05 Share of Searches
Total	4,447,406	5,134,713	15%	--
Google	2,032,222	2,449,396	21%	47.7%
Yahoo!	965,642	1,118,429	16%	21.8%
MSN	540,686	582,702	8%	11.3%
AOL	358,667	368,130	3%	7.2%
Ask Jeeves	75,808	133,932	77%	2.6%

Source: Nielsen//NetRatings MegaView Search, December 2005

Table 2. Breakdown of Search by Vertical, June & October 2005

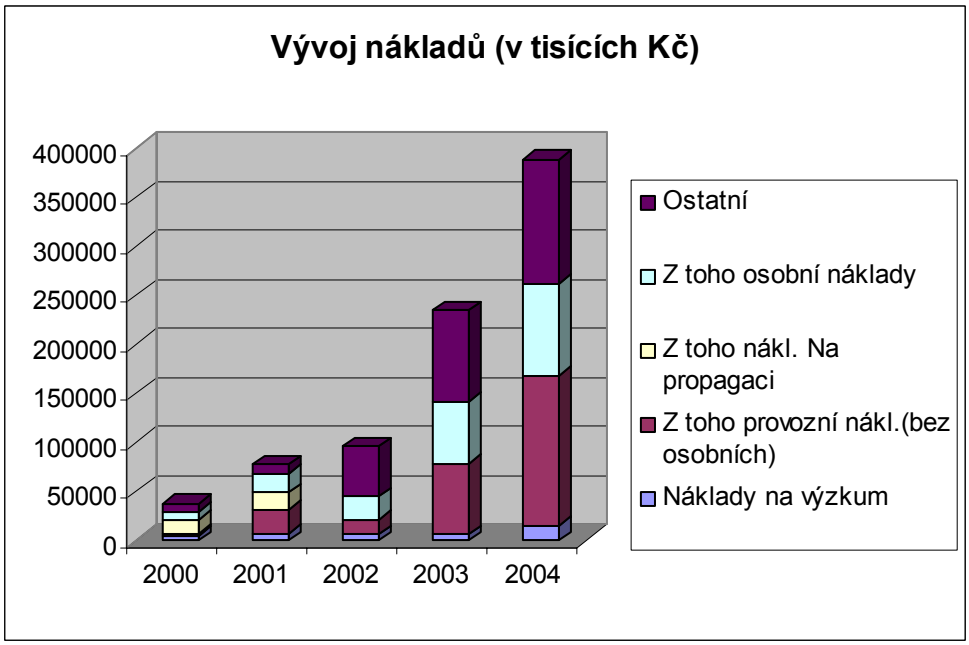
Search Verticals	Jun-05 Searches (000)	Oct-05 Searches (000)	June to Oct. Growth
Image	240,393	328,275	36.6%
Local	148,907	177,494	19.2%
Web	3,951,107	4,511,808	14.2%
News	31,706	35,721	12.7%
Shopping	70,351	77,270	9.8%

Source: Nielsen//NetRatings MegaView Search, December 2005

V globalizovaném světě podle společnosti Nielsen//Net Ratings celosvětově vede v počtu vyřízených dotazů v říjnu jasně Google (47,7 procenta), druhé je Yahoo (21,8 procenta), třetí MSN (11,3 procenta), čtvrté AOL (7,2 procenta), pátý Ask Jeeves (2,6 procenta). Nejrychleji rostoucí službou je vyhledávání v obrázcích, říká analýza [PDF, 81 kB]

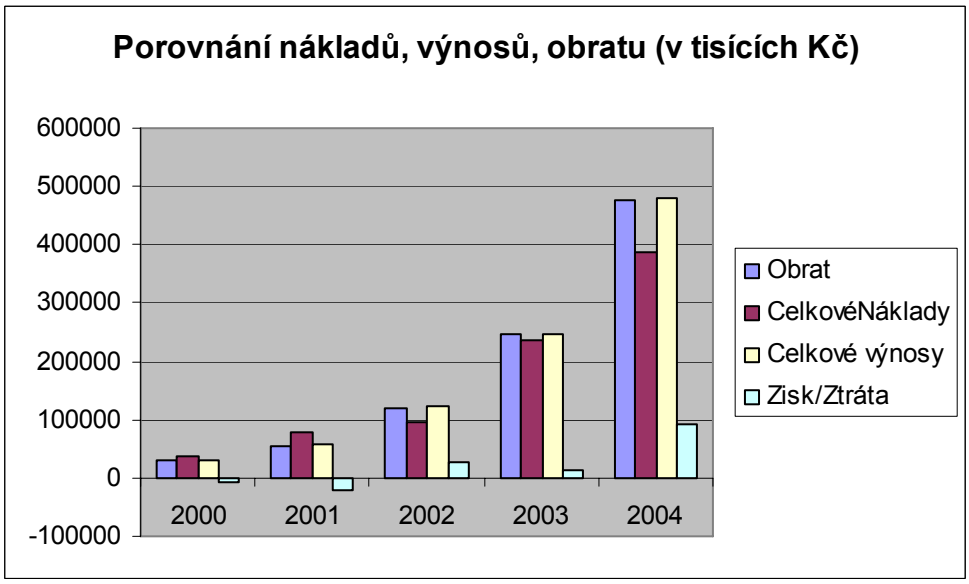
Pokud jde o ekonomické parametry portálů:

Seznam.cz

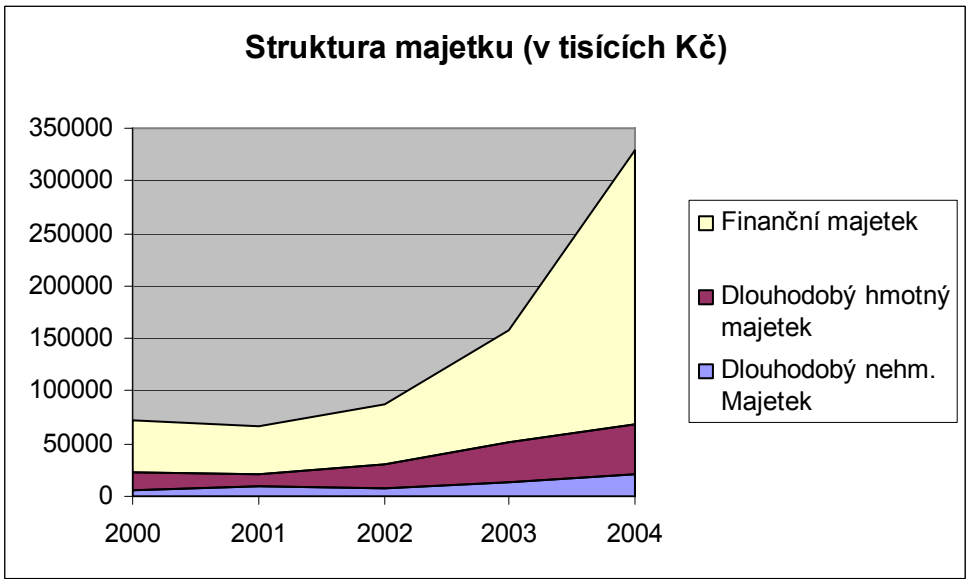


Údaj náklady na propagaci je získán pouze v roce 2000 a 2001, v ostatních letech je započítán do položky ostatní.

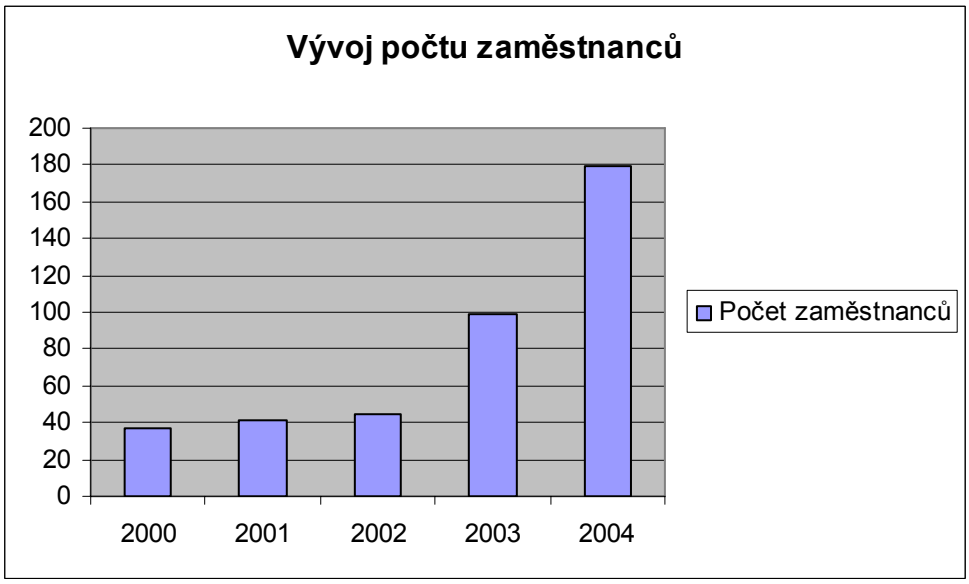
V roce 2000 tvořily největší část nákladů náklady na reklamu, v r. 2001 to byly provozní náklady, 2002 osobní, 2003 a 2004 provozní.



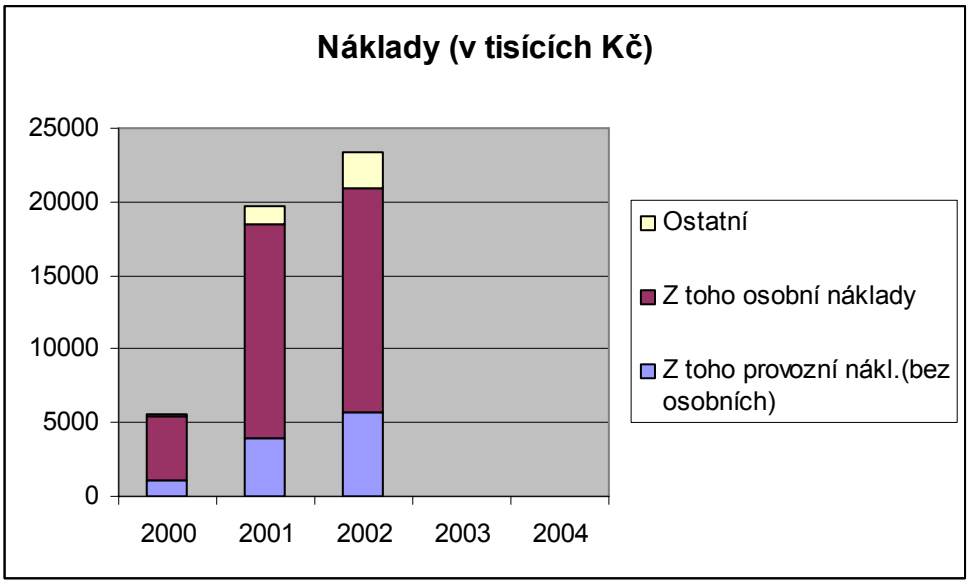
V roce 2000 a 2001 se Seznam ocitl ve ztrátě -7954 a -20427tis. Kč. Proto hledal strategického investora, kterým se v r. 1999 stal Lycos – majitel spray se nejprve s 1% podílem na vlastnictví, v roce 2000 pak 30%.



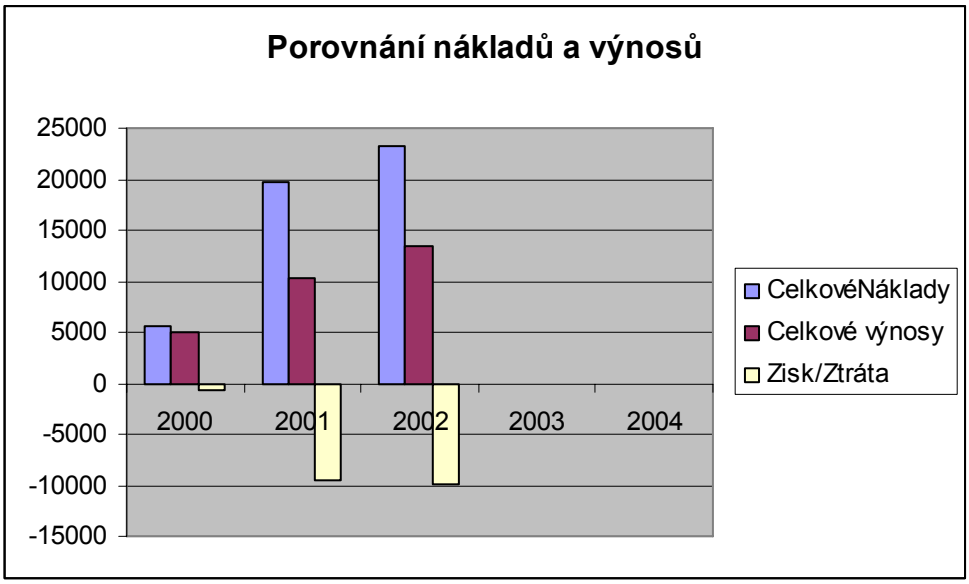
Největší podíl majetku má Seznam.cz na finančních účtech a to téměř 261 miliónů Kč, hodnota úroků z finančního majetku činí okolo 750tisíc Kč měsíčně.



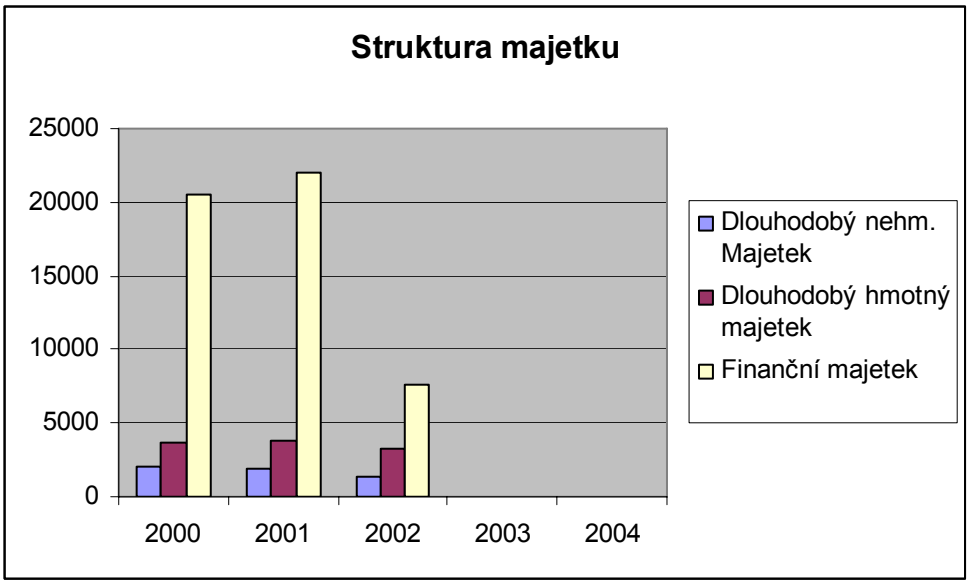
Centrum.cz



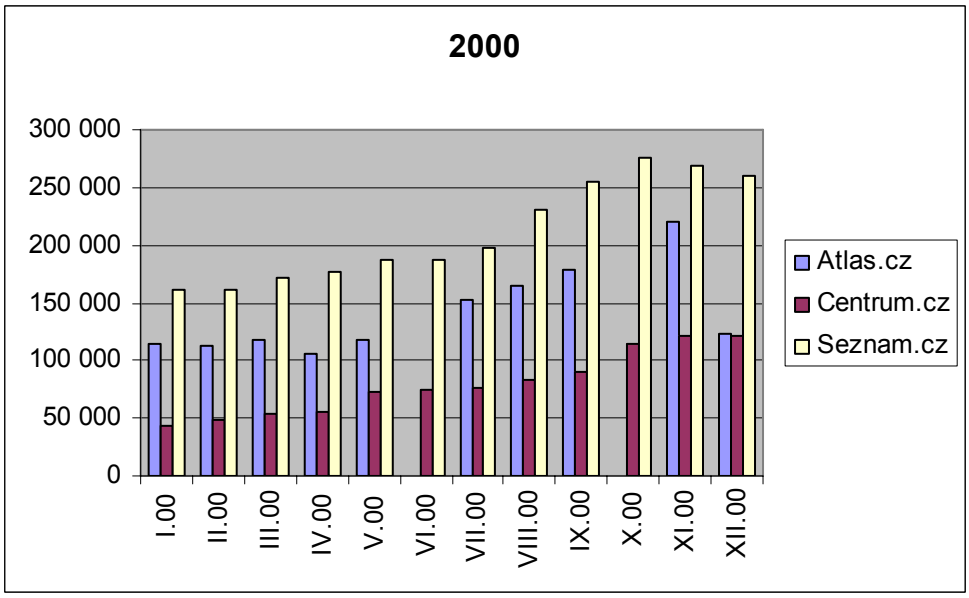
Největší složku nákladů tvoří v letech 200 – 2002 náklady osobní.

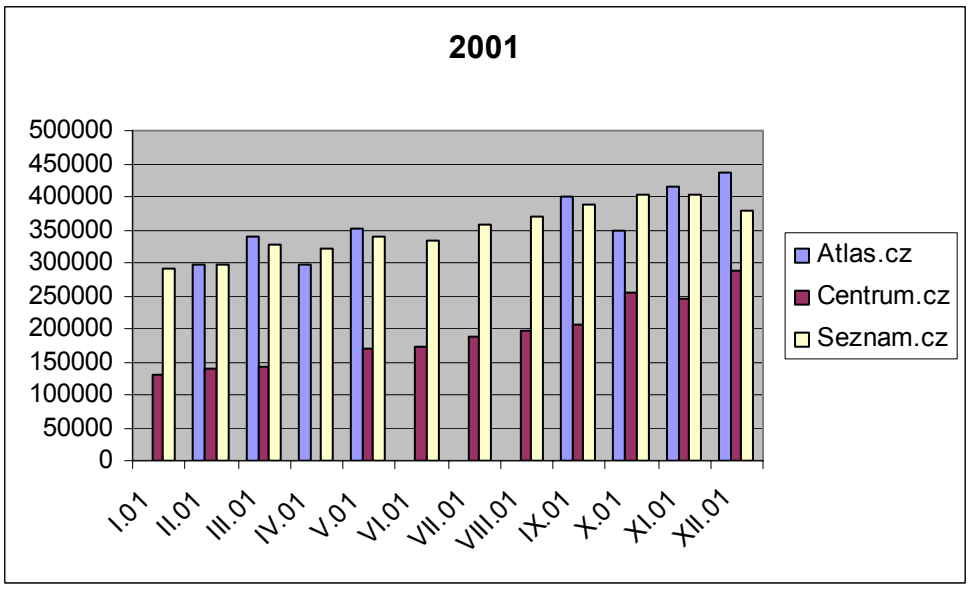


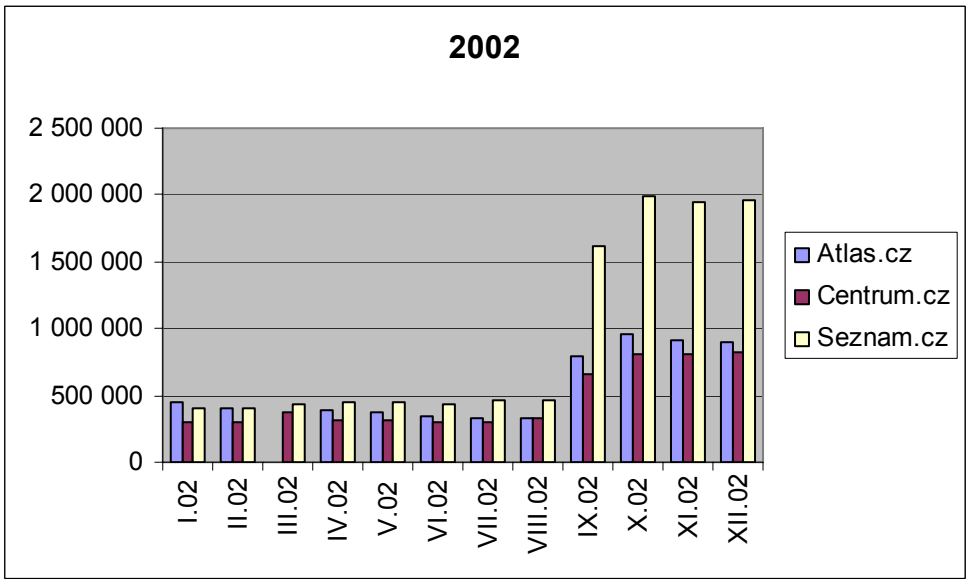
Společnost NetCentrum je za sledované období jednoznačně ve ztrátě. Vstup strategického investora v roce 2000. Náklady téměř o ½ převyšují výnosy (v letech 2001 a 2002).

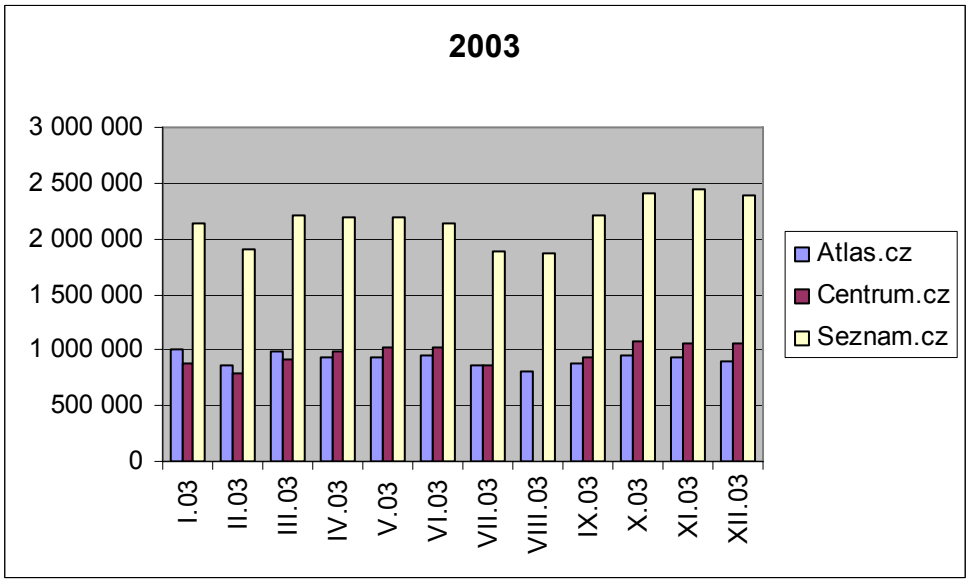


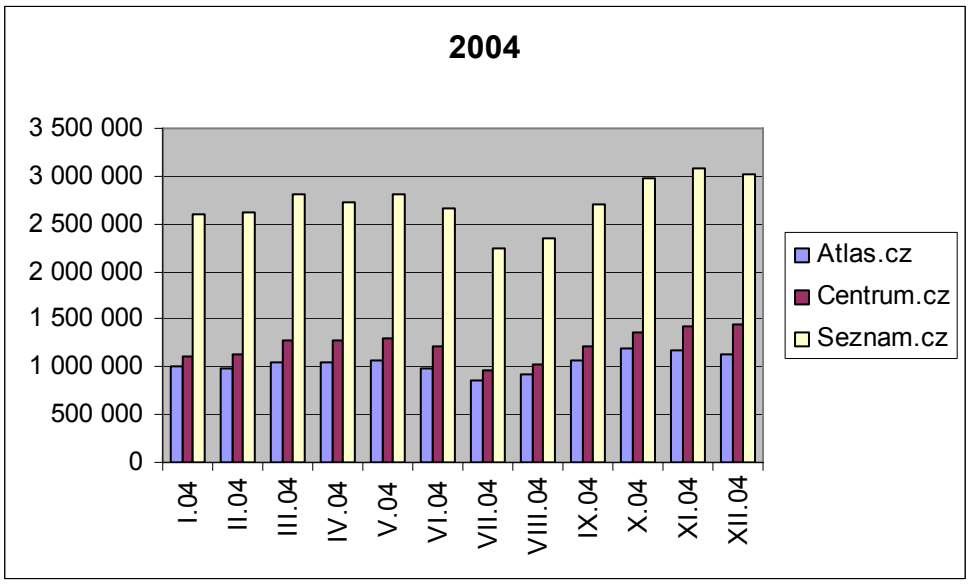
Na závěr uveďme informace, týkající se návštěvnosti portálů:

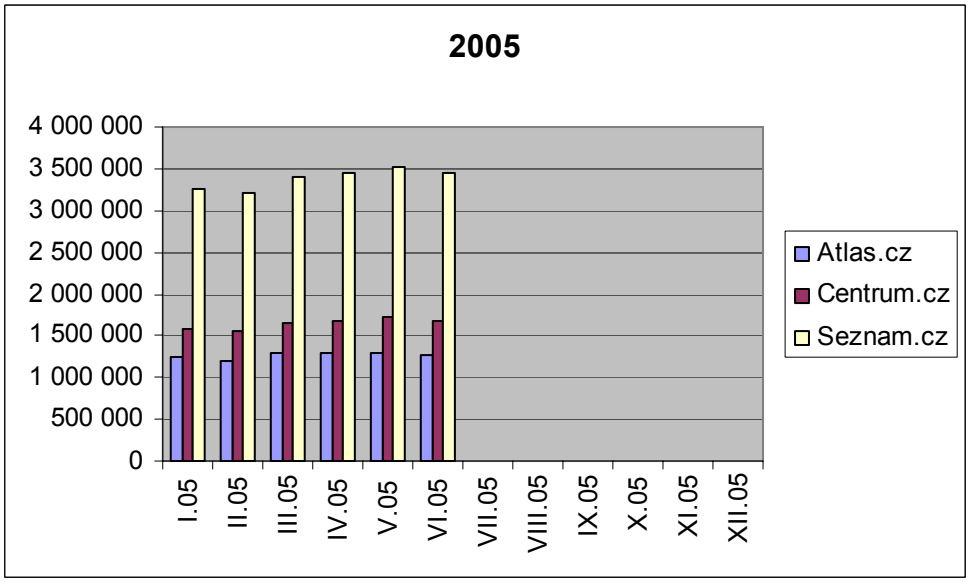





2002
2 500 000
2 000 000
1 500 000
1 000 000
500 000
0
I.02
II.02
III.02
IV.02
V.02
VI.02
VII.02
VIII.02
IX.02
X.02
XI.02
XII.02
Atlas.cz
Centrum.cz
Seznam.cz


2003
3 000 000
2 500 000
2 000 000
1 500 000
1 000 000
500 000
0
I.03
II.03
III.03
IV.03
V.03
VI.03
VII.03
VIII.03
IX.03
X.03
XI.03
XII.03
Atlas.cz
Centrum.cz
Seznam.cz


2004
3 500 000
3 000 000
2 500 000
2 000 000
1 500 000
1 000 000
500 000
0
I.04
II.04
III.04
IV.04
V.04
VI.04
VII.04
VIII.04
IX.04
X.04
XI.04
XII.04
Atlas.cz
Centrum.cz
Seznam.cz


2005
4 000 000
3 500 000
3 000 000
2 500 000
2 000 000
1 500 000
1 000 000
500 000
0
I.05
II.05
III.05
IV.05
V.05
VI.05
VII.05
VIII.05
IX.05
X.05
XI.05
XII.05
Atlas.cz
Centrum.cz
Seznam.cz

Otázky a úkoly ke kapitole I.:

1. Na www.obchodnirejstrik.cz najděte aktuální ekonomické ukazatele firem seznam.cz, centrum.cz a atlas.cz .

2. Na základě ekonomických údajů za posledních pět let odhadněte vývoj a ekonomické výsledky firem seznam.cz, centrum.cz a atlas.cz v aktuálním roce.
3. Na základě informací z internetu zpracujte vlastní studii „historie internetu“.

4. Zjistěte aktuální ekonomické informace firem www.google.com a www.yahoo.com pomocí U.S. Securities and Exchange Commission (www.sec.gov)**:** na této stránce lze nalézt množství užitečných informací o kapitálovém trhu v USA. V databázi EDGAR (http://www.sec.gov/edgar/searchedgar/webusers.htm) jsou pak k dispozici archivy výročních zpráv, zpráv o sloučení společností a účetní výkazy prakticky všech amerických společností obchodovaných na burze.
Další velmi užitečnou stránkou je Damodaran Online (www.damodaran.com)**,** kde lze nalézt množství informací pro oceňování společností a jiné finační aplikace, které lze jinak nalézt jen v placených databázích. Jedná se o beta koeficienty, tržní prémie za riziko pro jednotlivé země, historické bezrizikové úrokové míry, hlavní finanční ukazatele amerických i světových společností za posledních několik let a další.

5. Pomocí http://www.sec.gov zjistěte aktuální ekonomické informace známých IT firem v USA (IBM, Microsoft aj.).

Klíčová slova: internet, webové služby

5 Elektronické bankovnictví

Nové sofistikované technologie nabízejí přímou komunikaci klienta a banky, aniž je nutná návštěva na příslušném útvaru banky a mezi tyto služby patří: Telebanking, GSM banking, WAP banking, Internet banking, Home banking a nově se objevující forma přímého bankovnictví PDA banking.

K nejdůležitějším rozdílům mezi specializovanou elektronickou bankou a tradiční bankou "kamennou" patří:

1. *Odlišný způsob komunikace mezi klientem a bankou*

   - tradiční banky kladou důraz na osobní kontakt mezi zákazníkem a bankou, u přímého bankovnictví komunikace probíhá prostřednictvím komunikačních kanálů (počítač, Internet, telefon, fax …)

2. *Snížení nákladů na provoz banky*

   - internetová banka nepotřebuje rozsáhlou síť obchodních míst, zpravidla vystačí s minimálním počtem center, která poskytují služby spíše informačního a podpůrného charakteru

3. *Kvalita a dostupnost služeb*

   - díky moderní technice mohou být služby přímého bankovnictví klientům k dispozici 24 hodin denně, v tuzemsku i zahraničí

4. *Nové typy bankovních produktů a služeb*

   - úzké propojení bankovních IS a komunikačních kanálů umožňuje bankám převádět na Internet nejen standardní ale vytvářet i zcela nové typy produktů a služeb (TV a běžné účty, spoření a platební styk,...)

Elektronické bankovnictví ve své současné podobě vzniká v druhé polovině devadesátých let jako přirozená reakce na rozvoj informačních technologií, které se stávají běžnou (a poměrně levnou) součástí firemního i osobního života. Situace ve vyspělých zemích na západ od našich hranic se přitom příliš neliší od české reality, neboť ani v zahraničí nedosáhlo elektronické bankovnictví většího rozkvětu dříve než ve druhé polovině devadesátých let. Můžeme naopak říci, že Česká republika zde drží krok se světovými trendy.

Pro úplnost je potřeba poznamenat, že i dříve existovala zejména pro velké firmy možnost komunikovat s bankou elektronickou formou. Dokonce i u nás byly vybrané společnosti v osmdesátých letech napojeny na Státní banku československou elektronicky, nicméně provoz těchto systémů byl technicky nedokonalý a tudíž značně poruchový, nehledě na finanční náročnost. Existují dva hlavní důvody, proč banky začaly nabízet služby elektronického bankovnictví (a klienti tyto služby vyžadovat a používat). Oba souvisejí s již zmíněným rozvojem informačních technologií.

1) **zatraktivnění služeb**

- Ve finančním sektoru začínají působit subjekty, které se stávají vážnou konkurencí tradičních bank.
- Rychlost a komfortnost služeb je pro zejména finančně dobře zajištěné zákazníky významným faktorem při rozhodování.

Které subjekty a v jaké oblasti tradičním bankovním domům konkurují?

- firmy nabízející úvěrové produkty ve formě kreditních karet nebo splátkového prodeje. (Tyto společnosti často spolupracují s řetězci obchodních domů a hypermarketů a společně například nabízejí co-branded karty, které spojují platební funkci bankovní karty s věrnostní kartou partnera. Jedna karta tak nese jak logo banky a slouží jako klasická kreditní či debetní karta, tak logo partnera, což zakládá nárok na slevy v jeho prodejnách, a má tedy i významnou marketingovou úlohu.)

Příklad: *Komerční banka vydává co-branded karty ve spolupráci s cestovní kanceláří Fischer, což držiteli takové karty umožňuje jak čerpat výhody Fischer Card, tak používat klasickou platební kartu EC/MC.*

- dalšími konkurenty bank jsou dnes bezesporu otevřené podílové fondy (v mnoha zemích podpořené daňovým zvýhodněním)
- pro investování má dnes člověk možnost využít také produktů pojišťoven (u nás je za určitých podmínek daňově zvýhodněno životní pojištění) či penzijního fondu.

2) **úspora nákladů**

- dlouhodobý proces v horizontu spíše let než měsíců
- Elektronické bankovnictví umožňuje bance především snížit variabilní náklady na jednu transakci, vyžaduje však na začátku značné investice, které naopak zvýší fixní náklady.
- Nutností jsou výrazné investice do informačních technologií, jejichž využívání se bude zvyšovat pomalu a postupně. Není totiž většinou možné ihned po zavedení služeb elektronického bankovnictví propustit zaměstnance (mnohdy je spíše potřeba najmout nové, kvalifikovanější a tedy lépe placené) nebo zavřít alespoň část poboček. Tento krok by měl za následek ztrátu klientely, která dosud striktně vyžaduje osobní kontakt s bankou a o služby elektronického bankovnictví nemá zájem.

5.1 Důvody rozvoje elektronického bankovnictví

- vznikají internetové banky (v EU např. first-e, Egg a další), a dále kamenné banky hledají další prostor pro snižování nákladů na obsluhu svých zákazníků a zvýšení prodeje dalších služeb (půjčky, hypotéky atd.) těmto zákazníkům.
- získání části trhu, který byl dříve uzavřen vysokými vstupními náklady (zejména na budování poboček).
- přednosti kompletní on-line obsluhy zákazníka (tedy "absolutně" internetová banka bez poboček) vyvažují některé problémy: budování image a důvěryhodnosti u zákazníků, nastavení a především udržení úrovně obsluhy zákazníků, dostatek kvalitních produktů. Samozřejmě, že velkou roli hraje i "virtualita" internetových bank subjektivně podrývající jejich důvěryhodnost (zkušenosti nejen z českého trhu ukazují, že secesní

budovy nezajišťují prosperitu banky). Dlouhodobě se navíc ukazuje, že klíčem k výběru banky je podstatně více než jen vybraný obslužný kanál (byť s nesporně nenapodobitelnými kvalitami), zvláště ve chvíli, kdy jej nabízí více než jeden hráč na trhu. Důležitější je celkový "marketingový mix" a kvalita vlastních produktů -- a tady, především v Evropě, silné širokospektrální finanční skupiny mají rozhodně před jakoukoli internetovou bankou značný náskok.

- čistě internetové banky zaznamenávají menší počet transakcí než jejích větší a starší sourozenci (což znamená také menší příjmy). Důvodem je, že internetová banka většinou slouží jen pro některé operace zákazníka, který na ní nespoléhá zcela, a tudíž jsou jeho operace u těchto institucí omezenější než u "mateřské" banky.

- v EU naráží čistě internetová banka na příliš geograficky, jazykově, kulturně i právně fragmentovaný trh, který ji v podstatě nutí alespoň částečně chovat se jako banka klasická -- tedy vytvářet lokální pobočky, které jsou schopny poskytovat potřebnou zákaznickou podporu.

Na závěr pár čísel: největší evropská banka s on-line zákazníky je severská Nordea s 2,4 miliónu uživatelů jejího elektronického bankovnictví, největší internetová banka Egg má potom poloviční počet zákazníků, ale pouze desetinový počet transakcí vůči Nordee.

- omezená pracovní doba peněžních ústavů a stále časově náročnější zaměstnání jsou hlavními důvody, které rozhodují o tom, že čím dál tím více lidí začíná pociťovat potřebu provádět platební styk podstatně efektivněji a úsporněji, než aby kvůli každému příkazu navštěvovali svoji banku.

5.2 Výhody služeb přímého bankovnictví

Úspora času

- Za hlavní přednost elektronického bankovnictví je možné považovat časově neomezený přístup klienta ke svému účtu. Platební transakci je možné odkudkoliv a kdykoliv vyřídit jen za několik málo minut, a to znamená obrovskou úsporu času proti návštěvám pobočky.
- Většina služeb, které získá klient na pobočce, je u přímého bankovnictví k dispozici i elektronickou cestou. Z toho důvodu již vůbec není nutné ztrácet čas v nekonečných frontách na přepážkách pošt či bankovních domů s cílem zaplatit složenku či fakturu, ale velmi efektivně a pohodlně je možné tuto operaci provést z domova.

Úspora peněz

- Vedle časové úspory přináší využívání služeb přímého bankovnictví také nižší poplatky za platební transakce. Elektronický komunikační kanál je pro všechny banky podstatně levnější než klasická cesta podávání platebních příkazů na papírovém nosiči na pobočce. Proto také banky tuto formu platebního styku poplatkově zvýhodňují, aby klienty motivovaly přímé bankovnictví co nejvíce využívat. Naopak lidé, kteří stále dávají přednost zadávání platebních příkazů na pobočce, zaplatí výrazně více. Rozdíl mezi poplatkem za elektronický a papírový příkaz dosahuje až několika desítek korun.

Bezpečnost

- Zabezpečení služeb přímého bankovnictví je na takové úrovni, že pravděpodobnost prolomení systému je zanedbatelně nízká. Kde ale číhá pro uživatele těchto aplikací největší nebezpečí, je selhání lidského faktoru. Stupeň zabezpečení může být sebevyšší, ale pokud sám klient nedodržuje zásady bezpečnosti, ke zneužití může dojít. Vina pak není na straně systému, ale klienta, že kupříkladu zapomněl v cizím počítači disketu se svým elektronickým klíčem a ještě zde měl poznamenaný vstupní PIN.
Vstupní heslo a elektronický klíč u přímého bankovnictví jsou branou k penězům na účtu. Proto je nutné být na tyto bezpečnostní prvky velmi opatrný a při využívání služby dodržovat všechny bankou doporučené zásady.

Dokonalý přehled o všech pohybech na kontě

Elektronické bankovnictví umožňuje zjišťování aktuálního stavu na svém účtu, provádění platebních příkazů k převodu a inkasu, zakládání terminovaných vkladů, dobíjení mobilních telefonů a mít tak dokonalý přehled o všech transakcích.

5.3 Komunikační kanály a jejich vývoj

- Elektronické bankovnictví v masové formě se začalo rozvíjet na principu telefonního bankovnictví.

5.3.1 Klasické telefonní bankovnictví (telebanking, phonebaking)

- USA a VB – již od 80. let

- Služba phone banking nabízí svým uživatelům možnost komunikovat s bankou prostřednictvím telefonu. Klient tak může operovat se svým účtem 24 hodin denně, 7 dní v týdnu z celého světa. Phone banking lze používat pouze pomocí telefonního přístroje s tónovou volbou (včetně mobilního).

- princip: Klient zavolá na linku telefonního bankovnictví (u většiny bank je toto číslo bezplatné a lze na ně volat i z mobilního telefonu), kde se prokáže svým identifikačním číslem a číslem PIN.

2 modifikace:

1) Komunikuje s automatickým hlasovým systémem, který klientovi podá kompletní informace o produktech či aktuálním zůstatku. Dále je zde možné zadávat příkazy k úhradě či inkasu, trvalé příkazy, provádět konverzi měn.

2) Komunikace s telefonním bankéřem, který poskytuje stejné služby jako pracovník na přepážce od zadávání příkazů po zakládání termínovaných vkladů.

   - forma komunikace mnohdy umožňuje úsporu času a nákladů na straně klienta, pro banku neznamená téměř žádný nákladový přínos.

- dnes je jasné, že telefonní bankovnictví, kdy klient komunikuje s živým zaměstnancem banky a vyřizuje běžné záležitosti (zjištění zůstatku, příkaz k úhradě apod.), je zcela přežitkem a na ústupu

- tendence automatických telefonních systémů a živých telefonních bankéřů používat pouze pro řešení nestandardních situací, jako jsou například reklamace či ještě lépe objednávky nových služeb.

- automatické systémy nejsou a nikdy vzhledem ke své povaze pro klienta nebudou uživatelsky příjemné => budou vytlačeny technologiemi zejména na bázi internetu.

5.4 GSM banking

- umožňuje ovládat běžný účet prostřednictvím mobilního telefonu GSM. Klient tak může vyřídit některé transakce na běžném účtu kdykoliv a kdekoliv na světě, aniž by musel navštívit pobočku své banky. Pro zadávání platebních příkazů pak stačí mít jen dostupný signál svého mobilního operátora.
- spolu s internetovým bankovnictvím lze této oblasti prorokovat největší rozvoj a dynamiku (mobilní telefon má dnes ve vyspělých státech více než polovina obyvatelstva, u segmentu firemních klientů a středně a výše příjmově postavených fyzických osob se toto číslo blíží stu procentům).
- GSM Banking je bankovní služba, jejíž vznik a vývoj je úzce spjat s rozšířením mobilních telefonů.
- je hodně pravděpodobné, že mobilní operátoři se časem stanou nejen zprostředkovateli bankovních služeb, ale založí si (nebo koupí) vlastní banku. Jedná se totiž o služby s výraznou přidanou hodnotou, které tak generují zisk. A proč by se mobilní operátor měl o zisk dělit s bankou?
- SIM toolkit - dnes nejpoužívanější standard bankovních služeb v mobilních sítích GSM.
- banka do vašeho mobilního telefonu (na SIM kartu) nahraje vlastní bankovní aplikaci, která se objeví v menu vašeho telefonu. Potom vám tedy stačí nalistovat v menu aplikace správnou položku a vybrat některou ze základních služeb (např. zjišťování zůstatku na účtu, přehled historie pohybů na účtu, přehled kursů, zadávání příkazů, atd.). Na závěr obdržíte informaci o vámi vybrané službě a to buď formou textové zprávy na mobilní telefon, nebo formou e-mailu do vaší e-mailové předem nadefinované schránky.

Bezpečnost GSM banking

Při nahrávání aplikace je SIM karta zašifrovaná a nelze z ní získat žádné údaje (v případě, že se váš telefon dostane do nepovolaných rukou). Současně je přístup k této aplikaci chráněn zvláštním bankovním PIN kódem, tzv. BPIN.

5.5 SMS banking

- další varianta služby GSM je **SMS banking**, jehož výhodou je použitelnost u všech mobilních telefonů, bez ohledu na operátora.
- komunikace mezi klientem a bankou probíhá pouze prostřednictvím SMS zpráv.
- na první pohled to nevypadá příliš bezpečně, ale banka i k této aplikaci může vydávat tzv. autentizační kalkulátor, s jehož pomocí si vygenerujete speciální kód, který vložíte do struktury SMS zprávy.
- Nevýhodou je složitější manipulace, protože SMS zprávy musíte posílat přesně ve formátu daném bankou. Např. U částka účet_debet účet_kredit splatnost [Vvar_symbol] [Kkonst_symbol] [Sspec_symbol] [MAC]. Zadávání tedy vyžaduje velkou pozornost, abyste se nepřepsali.
- spolu s internetovým bankovnictvím lze této oblasti totiž prorokovat největší rozvoj a dynamiku.

5.6 WAP banking

- WAP (Wireless Application Protocol) jako technologie nacházející se na rozmezí mezi internetovým a GSM bankovnictvím se dosud příliš neprosadila.
- Důvody nejsou jednoznačné, ale zcela určitě mezi ně patří malá rozšířenost mobilních telefonů podporujících WAP. Není to ale vůbec jediný a hlavní důvod. - I tehdy, pokud banka nabízí přístup prostřednictvím WAP a klient má telefon podporující tuto technologii, většinou této možnosti nevyužívá. Proč?
- Existují jiné komunikační kanály, ve srovnání s kterými je WAP pomalý, nákladný a komplikovaný. Pokud můj operátor a banka zároveň podporují GSM SIM Toolkit, je pro mě jeho použití mnohem výhodnější než WAP.

5.7 Internetbanking

- Internetové bankovnictví umožňuje klientovi přístup ke svému účtu z jakéhokoli počítače připojeného do sítě internet.
- Služby poskytované prostřednictvím internetu se vyznačují největším komfortem a jsou pro zákazníky nejméně nákladné.
- První banky specializující se na přímé bankovnictví s využitím Internetu vznikly **počátkem devadesátých let v USA**. Byly schopny založit svému klientovi nový bankovní účet bez toho, aby musel opustit svoji pracovnu.
- Zpočátku velice pomalu rozvíjející se oblast, otázky bezpečnosti a zneužitelnosti. Dnes je situace opačná – každý, kdo dosud internetbanking nenabízí, usilovně deklaruje připravenost a prorokuje mu skvělou budoucnost.
- rozvoj internetového bankovnictví samozřejmě souvisí s masovější využívaností internetu samotného.

- Internetové bankovnictví ve velmi blízké budoucnosti zcela vytlačí zastaralé, zbytečně robustní, zcela nepružné a velice drahé homebankingové systémy
- Internetové bankovnictví zachová všechny výhody homebankingu, jako je hromadné zpracování tisíců platebních příkazů, napojení na ekonomický informační systém (účetnictví) firmy apod. a nabídne přístup odkudkoli ze světa, z jakéhokoli počítače připojeného k internetu.

5.7.1 Hlavní výhody internetového bankovnictví

- Možnost přístupu ke svému účtu 24 hodin denně z jakéhokoli počítače připojeného k síti internet
- Další důležitou výhodou je skutečnost, že klient má vždy aktuální přehled o dění na svém kontě a nemusí čekat na časově zpožděné papírové výpisy z účtu zasílané bankou.
- Důležitá je i úspora peněz za poplatky.
- Pomocí internetového bankovnictví lze nejenom sledovat aktuální zůstatek a platební historii na účtu a zadávat jednorázové platební příkazy, ale také zadávat, měnit a rušit trvalé příkazy k platbě či inkasu, sledovat poskytnuté úvěrové produkty, zakládat termínované vklady, zjišťovat informace o úrokových sazbách a měnových kurzech a také například systém internetového bankovnictví umožňuje dobíjení předplacených telefonních karet.

5.8 Home-banking

- Produkt umožňuje obsluhovat účet pomocí počítače připojeného k internetu a softwaru, který je dodán bankou (obvykle na instalačním CD).
- Tím se home banking odlišuje od internetového bankovnictví, kde stačí mít pouze přístup k Internetu.
- Tato forma přímého bankovnictví umožňuje zadávat platební příkazy k úhradě v domácích i cizích měnách včetně hromadných a trvalých příkazů, kontrolu příkazů, získávat informace o zůstatcích, obratech, vývoji plateb a příjmů na účtu, informace o neprovedených transakcích.
- Homebankingových systémů existuje velké množství a liší se v technickém řešení, množství realizovatelných operací i použitém zabezpečení. Některé samozřejmě nemusí pracovat v plném on-line režimu, ale využívají tzv. semi on-line (údaje jsou aktualizovány několikrát denně, například každou hodinu).
- Výhodou těchto produktů je kompatibilita s účetními a ekonomickými programy. Naopak nevýhodou je, že lze používat pouze počítač, na kterém je program nainstalován.

5.9 PDA banking

- Zatím nejmladší typ přímého bankovnictví , kterou nabízí v ČR E-banka (již od začátku března 2003).
- Jde o bankovní aplikaci, kde klient se svým kontem komunikuje prostřednictvím kapesního PDA počítače.
- Je přirozeně nezbytné, aby přenosný počítač byl připojen k internetu:

1) Prostřednictvím datových přenosů mobilního telefonu (nejčastější způsob)

2) Lze použít synchronizační kolébku, která spojí PDA s běžným počítačem připojeným na internet, a připojení tak pro PDA zprostředkovat. Tento způsob však postrádá největší výhodu PDA zařízení, a to mobilnost.

3) Další možností, kterou podporují jen nejnovější PDA zařízení, je možnost připojení k internetu pomocí tzv. hotspotů (technologie bezdrátových sítí s vysokou přenosovou rychlostí) - klient se ovšem musí pohybovat v oblasti, která je nějakým hot spotem pokryta.

Další požadavky na PDA banking

- Pro zprovoznění služby nemusíte na svém účtu nic nastavovat, nemusíte instalovat žádný speciální program - stačí vám pouze vlastnit kapesní počítač s připojením k internetu.
- Kapesní počítač musí obsahovat internetový prohlížeč, který podporuje SSL protokol.
- Dále si aktivujete připojení k internetu a vyhledáte si stránku http://pda.ebanka.cz/ (v anglické verzi pda.ebanka.com).
- K autentizaci a certifikaci budete potřebovat mobilní nebo osobní elektronický klíč.
- Operace prováděné pomocí osobního elektronického klíče jsou bezpečnější, jejich provedení je ovšem poněkud zdlouhavější; přístup k účtu prostřednictvím tohoto klíče stojí klienta 89 Kč/měsíc, zatímco prostřednictvím klíče mobilního je zdarma.
- PDA bankovnictví je plně funkční také na kapesním počítači s mobilním telefonem T-Mobile MDA.

-V žádném případě se operační funkčnost nedá srovnat s bankovnictvím internetovým.

Nejdůležitější služby jsou pokryty, další jsou buď to pro PDA nevhodné (např. z důvodu velikosti formuláře), nebo nejsou klienty podle sdělení představitelů banky pro PDA zařízení požadovány.

Shrneme-li celkově obsah této kapitoly je zřejmé, že dnes nabízejí služby elektronického bankovnictví prakticky všechny banky s malými rozdíly mezi nabízenými produkty.

Otázky a úkoly ke kapitole II.:

1.Zpracujte studii o nabízených produktech ČSOB v oblasti elektronického bankovnictví.

2.Zpracujte studii o nabízených produktech České spořitelny v oblasti elektronického bankovnictví.

3.Zpracujte studii o nabízených produktech Komerční banky v oblasti elektronického bankovnictví.

4.Zpracujte žebříček bank, operujících na území ČR podle ročního obratu.

5.Porovnejte služby v oblasti elektronického bankovnictví u konkurenčních bank.

Klíčová slova: elektronické bankovnictví, bankovní produkty, homebanking

6 Elektronický podpis v praxi, certifikáty

Zákon o elektronickém podpisu byl schválen v roce 2000 a upravuje v souladu s právem Evropských společenství používání elektronického podpisu, elektronické značky, poskytování certifikačních služeb a souvisejících služeb poskytovateli usazenými na území České republiky, kontrolu povinností stanovených tímto zákonem a sankce za porušení povinností stanovených tímto zákonem. Zákon 227/2000 Sb. vymezuje základní pojmy způsobem uvedeným v příloze.

V návaznosti na uvedený zákon o elektronickém podpisu, Ministerstvo informatiky udělilo zatím (stav v roce 2006) akreditaci třem firmám:

První certifikační autorita, a. s.,
identifikační číslo 26 43 93 95,
Podvinný mlýn 2178/6,
PSČ 190 00 Praha 9

Česká pošta, s. p.
identifikační číslo 47 11 49 83,
Olšanská 38/9,
PSČ 225 99 Praha 3

eIdentity a. s.,
identifikační číslo 27 11 24 89,
Vinohradská 184/2396,
PSČ 130 00 Praha 3

Výměna informací v elektronické podobě je trendem dnešní doby. Ne každá informace je však určená očím a uším každého. Jinak řečeno, data je často třeba chránit. Máme-li pak na mysli komunikaci ve sféře státní správy, financí, zdravotnictví, obchodu, dopravy a služeb aj. je nutné aby byly stejně důvěryhodné jako klasické procedury prováděné na základě osobního styku, tedy zejména s využitím ověření totožnosti, vlastnoručních podpisů či archivaci dokumentů. Na základě této úvahy lze v souladu s mezinárodními normami definovat základní bezpečnostní cíle, jejichž plnění by měl důvěryhodný systém zajistit.

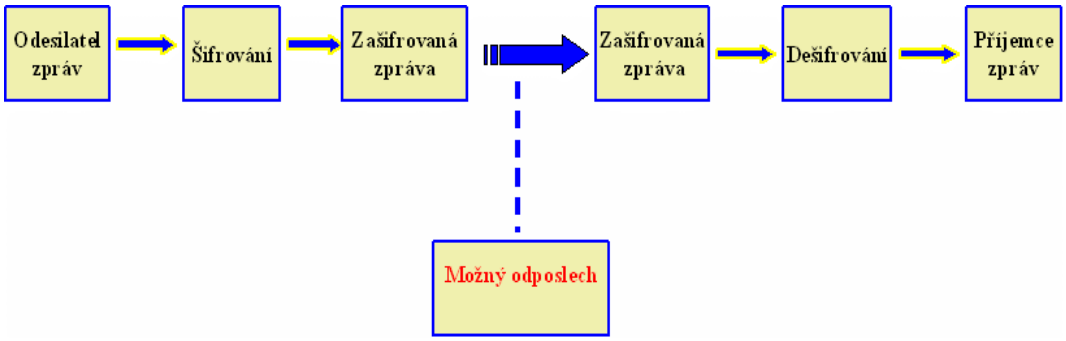
- ***důvěrnost informací*** - systém musí zabezpečit, že přístup k důvěrným informacím mají pouze autorizované subjekty
- ***integrita*** - systém musí zabezpečit informace proti modifikaci
- ***neodmítnutelnost odpovědnosti*** - systém musí mít schopnost přesvědčit třetí nezávislou stranu o přímé odpovědnosti subjektu za autorství, vlastnictví,odeslání, případně přijetí zprávy.

Ochranu informací lze rozdělit do dvou základních oblastí. Tou první je ochrana dat u správce či uživatele. V této fázi jsou nebo mohou být data pod výhradní kontrolou jediného subjektu. Tomu odpovídají i požadavky na zabezpečení, které může být řešeno jak fyzickou a organizační ochranou, tak i ochranou logickou, aplikací kryptografie. Pod fyzickou ochranou je možné si představit i počítač oddělený od dostupných komunikačních prostředků a sítí, ke kterém má přístup pouze jeho vlastník Ochrana uložených dat tímto způsobem není nosným předmětem popisované kapitoly. Těžištěm našeho zájmu je komunikační bezpečnost a aplikace kryptografie. Kryptografii je v této knize věnována samostatná kapitola, a proto jsou naším

cílem spíše popisy postupů a principů.

Fyzická ochrana přenosu je často náročná, většinou však nemožná. Nelze si představit ochranu byť jen několik kilometrů dlouhé linky tak, aby z ní nebylo možné signál odposlechnout. Často se navíc využívá komutované linky, která na každém uzlu k odposlechu přímo vybízí. Jistou bezpečnost snad nabízí spojení pomocí optického kabelu, ale ani v tomto případě nelze mluvit o vysokém stupni ochrany.

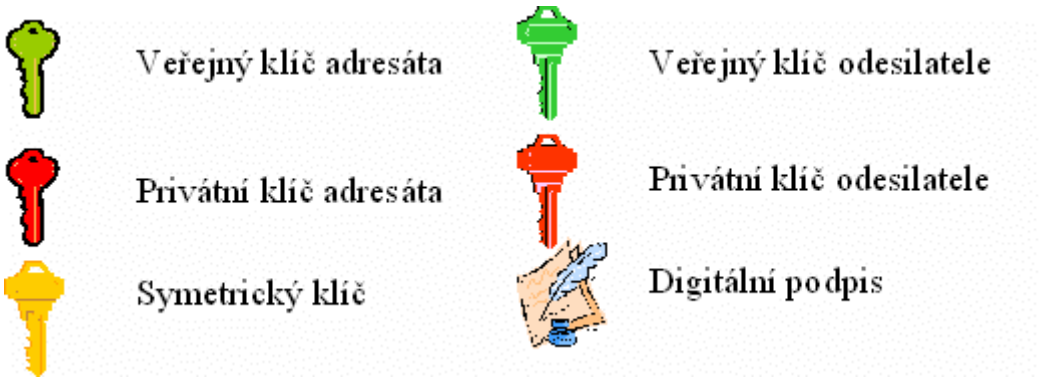
Nabízí se tedy možnost logické ochrany dat, konkrétně šifrování. Znamená to zašifrovat data na straně odesilatele, odeslat je a na straně příjemce zase dešifrovat.



obr. 1

Přenos zpráv šifrovaným kanálem.

Legenda k níže uvedeným obrázkům:



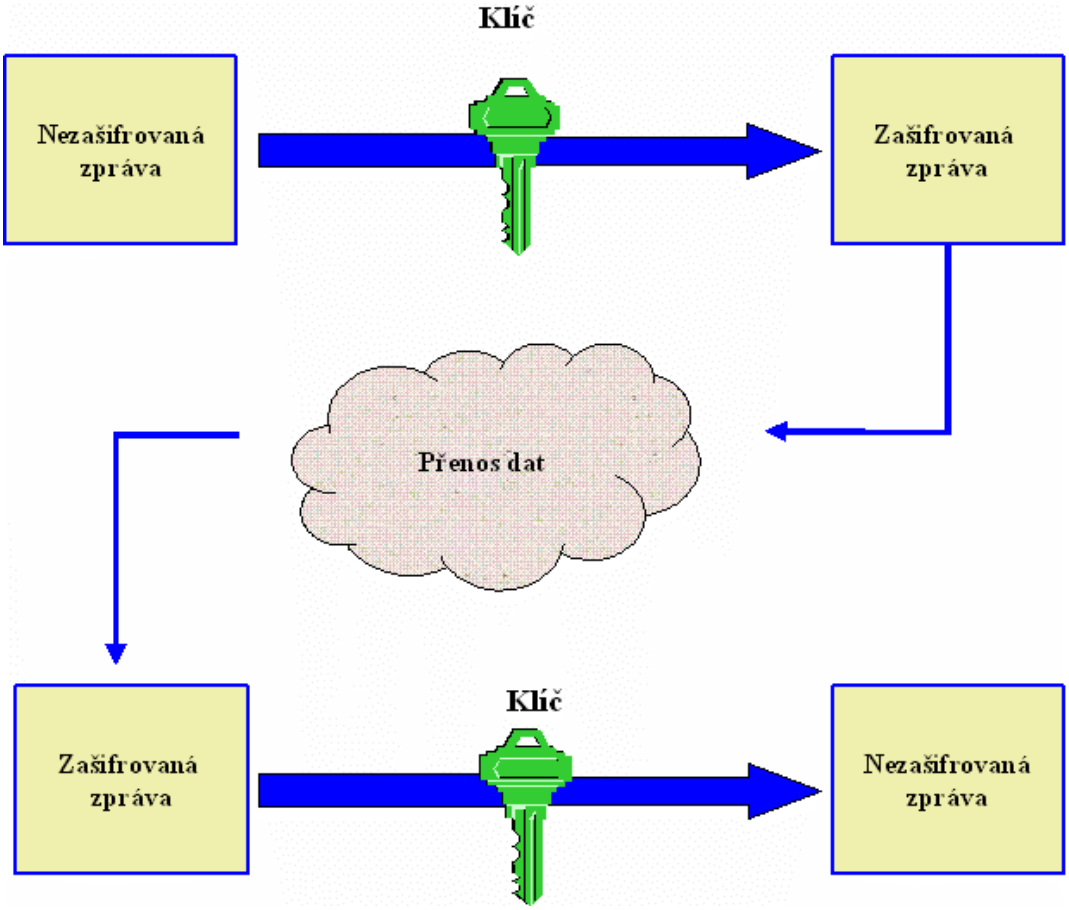
Kvalita ochrany zprávy je dána šifrovací metodou, typem užitého algoritmu, jeho aplikací, a délkou šifrovacího klíče.

Šifrovací metody

V zásadě rozlišujeme dvě šifrovací metody.

Symetrická kryptografie

První z nich je metoda symetrické šifry. Znamená to, že stejný klíč, který byl užit k zašifrování zprávy na straně odesilatele bude užit i na straně příjemce pro dešifrování zprávy. Tento klíč musí být samozřejmě udržován v tajnosti. Z toho vyplývá nutnost před začátkem komunikace předat důvěryhodným kanálem šifrovací klíč spolu s dalšími údaji (konkrétní typ algoritmu) druhé straně.



obr. 2
Šifrování zpráv symetrickou šifrou.

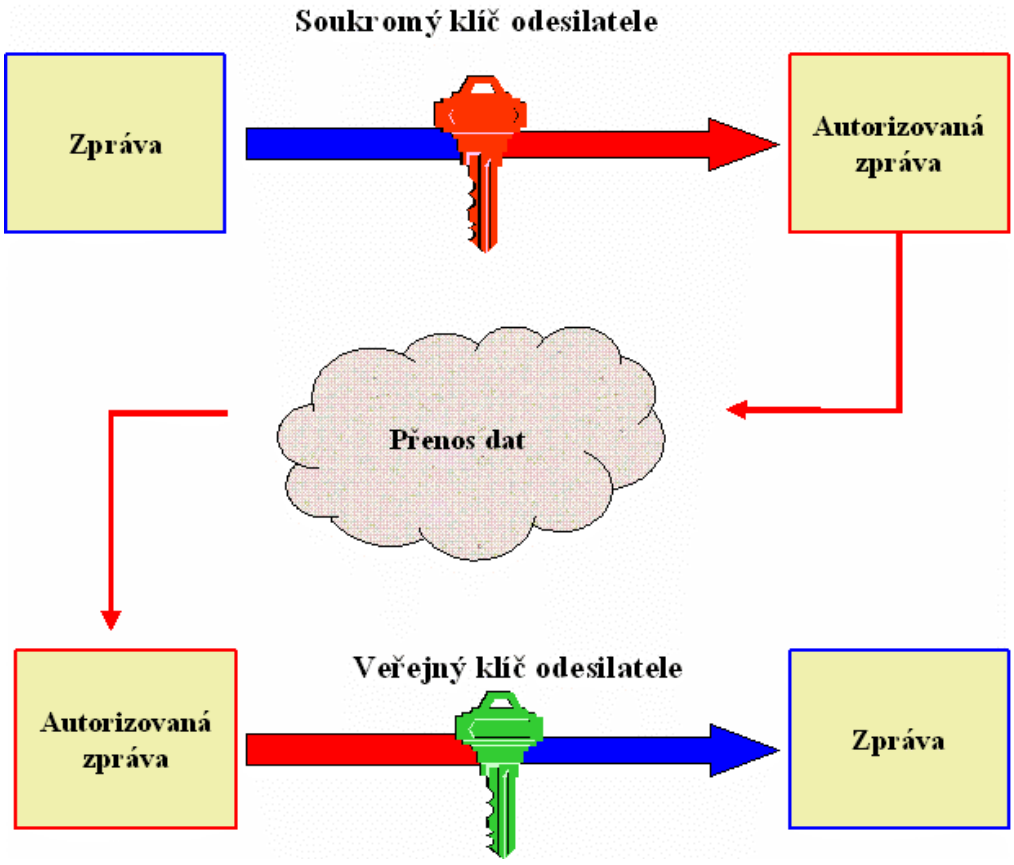
Současná komerčně dostupná výpočetní technika aplikuje tyto algoritmy (např. DES, TRIPLEDES, IDEA) téměř v reálnem čase. Na druhé straně i nejmodernější výpočetní technika je schopna dešifrovat (resp. luštit) data bez znalosti příslušných klíčů jen za relativně dlouhé časové období a s velkými finančními náklady. Pomocí matematických metod lze poměrně přesně vyčíslit náklady a čas potřebný k dešifrování dat, které jsou šifrovány definovaným algoritmem. Volbou délky klíče lze navíc tento výsledek výrazně ovlivnit.

Podrobný popis principů kryptografie je uveden v jiné kapitole této knihy.

Použití symetrických algoritmů představuje způsob, jak zabezpečit důvěrnost transakcí definovaným způsobem s možností přesného stanovení hrozeb, kterým toto zabezpečení odolává.Stěžejní nevýhodou je obtížná distribuce klíčů v rozsáhlých sítí, složitá logistika klíčů.

Asymetrická kryptografie

Oproti symetrické kryptografii se zde užívá jednoznačně daná dvojice klíčů. Tuto dvojici klíčů si vygeneruje uživatel pomocí některého z běžně dostupných SW produktů a stává se tak jejich jediným majitelem. Princip spočívá v tom, že data šifrovaná jedním z klíčů lze v rozumném čase dešifrovat pouze se znalostí druhého z dvojice klíčů a naopak. Jeden z nich, takzvaný privátní klíč je s maximální bezpečností ukrýván majitelem (čipové karty, disketa v trezoru, ...), zatímco druhý klíč je zveřejněn. Byla-li zpráva šifrována (autorizována) za použití privátního klíče a mi známe vlastníka veřejného klíče, kterým jsme zprávu dešifrovali, známe odesilatele. Protože je veřejný klíč obecně znám všem, nelze zprávu zašifrovanou (autorizovanou) podle výše popsaného postupu považovat za zašifrovanou v plném smyslu slova (důvěrnou), ale pouze za autorizovanou.



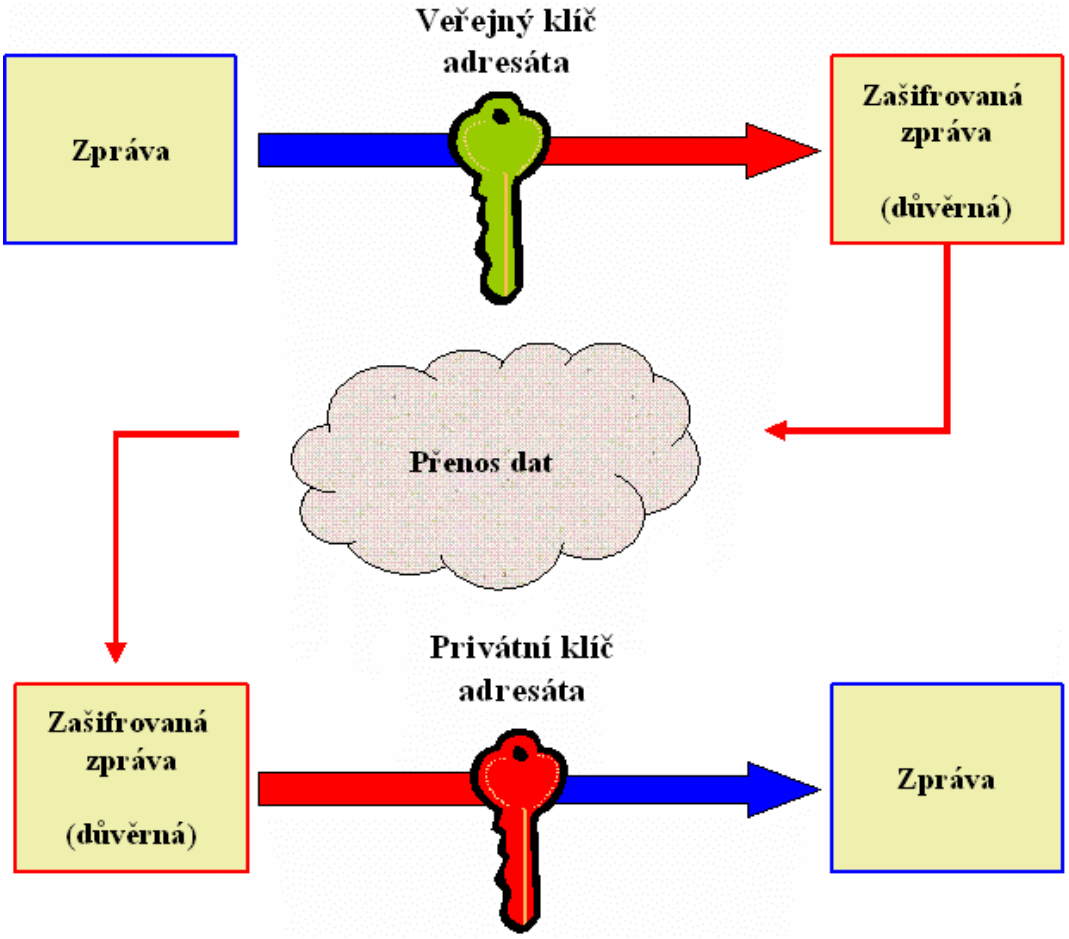
obr. 3a

Přenos neadresované, nezašifrované (veřejné), ale podepsané (principálně) i autorizované zprávy.

Tímto způsobem lze za pomocí asymetrické kryptografie řešit integritu dat a neodmítnutelnost odpovědnosti na straně odesilatele. Jestliže příjemce pošle autorizované potvrzení o přijetí zprávy, je zajištěna neodmítnutelnost odpovědnosti i ze strany příjemce,

který nebude moci popřít, že zprávu přijal.

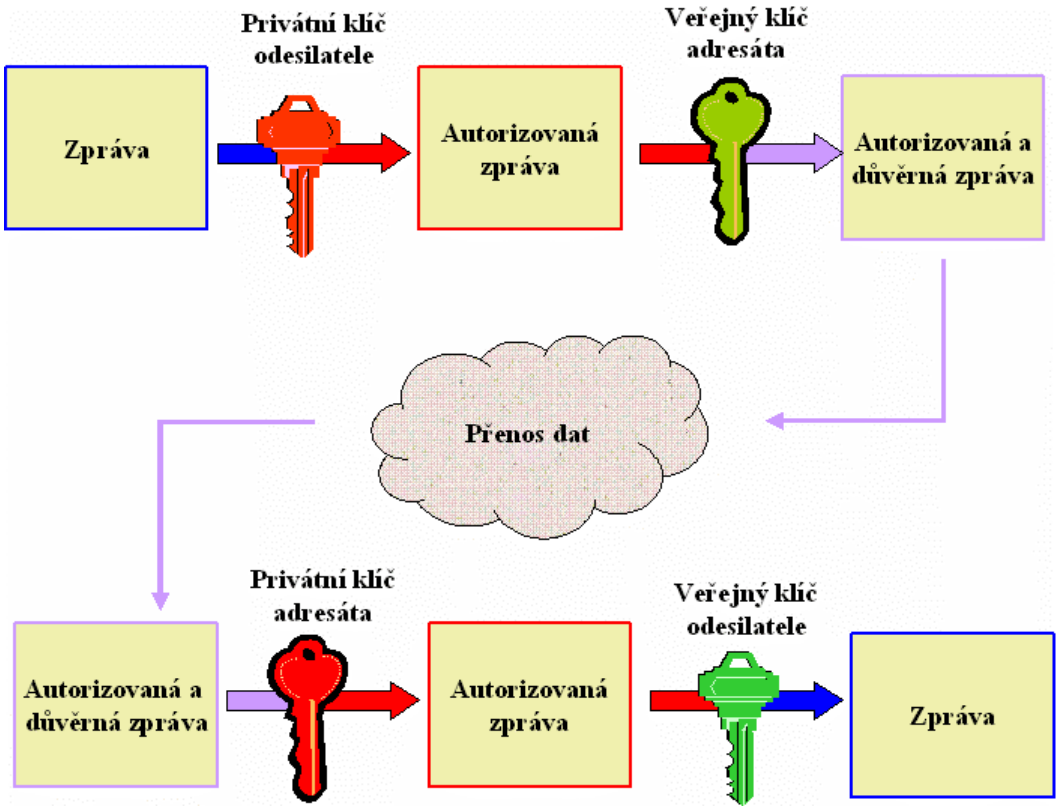
Výše popsaný postup neřeší požadavek důvěrnosti zpráv, tedy nečitelnosti pro neautorizované subjekty. K tomu lze využít šifrování zpráv pomocí veřejného klíče adresáta. Při zašifrování zprávy tímto klíčem máme jistotu, že ji přečte pouze adresát se svým privátním klíčem. Situace je znázorněna na obrázku 3b.



obr. 3b

Přenos adresované, zašifrované (důvěrné), ale neautorizované zprávy.

Celý systém pro šifrování a podepisování zpráv pomocí asymetrické kryptografie pracuje tedy následujícím způsobem. Zpráva je obvykle na straně odesilatele nejprve autorizována, autorizován je čitelný text zprávy, a potom šifrována. Na straně příjemce je zpráva nejprve dešifrována privátním klíčem příjemce, čímž je zajištěna adresnost zprávy a teprve potom je pomocí veřejného klíče ověřena identifikace odesilatele. Situaci zobrazuje obrázek 3c.



obr. 3c

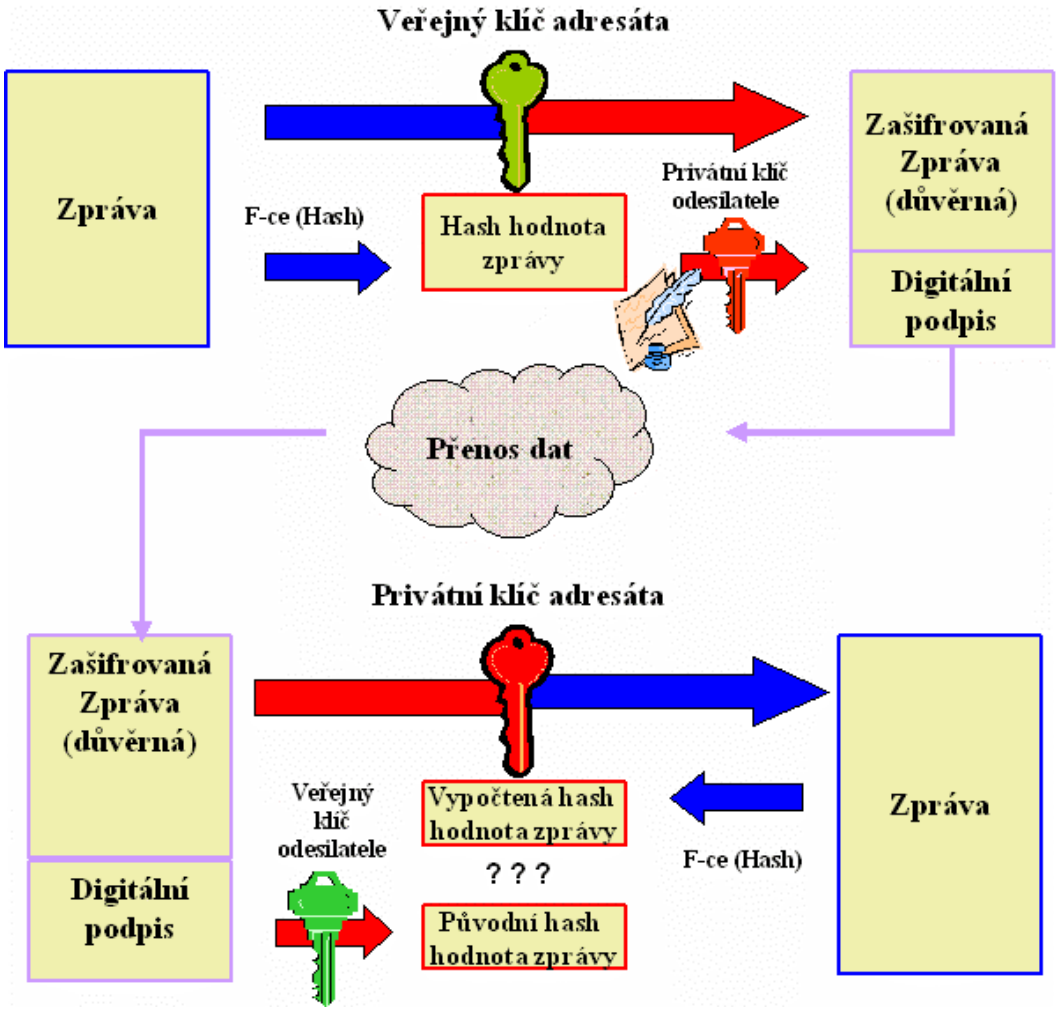
Přenos adresované, zašifrované (důvěrné) a autorizované zprávy.

Praktické využití

Aplikace asymetrických algoritmů je výrazně pomalejší než užití algoritmů symetrických. Je to dáno matematickou podstatou asymetrických algoritmů. I proto se zpravidla při tvorbě podpisu nešifruje privátním klíčem odesilatele celá zpráva, ale nejprve se na data použije takzvaná hash funkce. Hash funkce je jednosměrná transformace, která z variabilních vstupních veličin vytvoří jednoznačnou hodnotu (textový řetězec) pevné délky, který se nazývá hash hodnota. Hash hodnota představuje zhuštěnou hodnotu dlouhé zprávy ze které byla vypočtená, ve významu „digitálního otisku prstu“ (nebo „vzorku“) velkého dokumentu. Opačný proces je nemožný – díky jednosměrnosti hash funkce. Výpočet hash hodnoty zprávy je velmi rychlý. Nejprve se při podpisu zprávy vypočte hash hodnota zprávy, která bývá výrazně kratší než podepisovaná zpráva, a ta se zašifruje některým asymetrickým algoritmem s použitím privátního klíče, v této souvislosti též nazývaným „data pro vytváření elektronického podpisu“. Výsledkem je takzvaný digitální podpis. Ten je potom odeslán jako příloha zprávy nebo v samostatném bloku. Výhodou digitálního podpisu je, že splňuje stejná bezpečnostní kritéria jako autorizace celého dokumentu, provedení však trvá nesrovnatelně kratší dobu.

Kontrola digitálního podpisu zprávy u příjemce probíhá tak, že ke zprávě je podle dohodnutého algoritmu samostatně dopočítána nová hash hodnota a ta je potom srovnávána

s dešifrovanou (pomocí veřejného klíče předpokládaného odesilatele) hash hodnotou obsaženou v dodatku zprávy. Obě hodnoty si musí být rovny.



obr 4a.

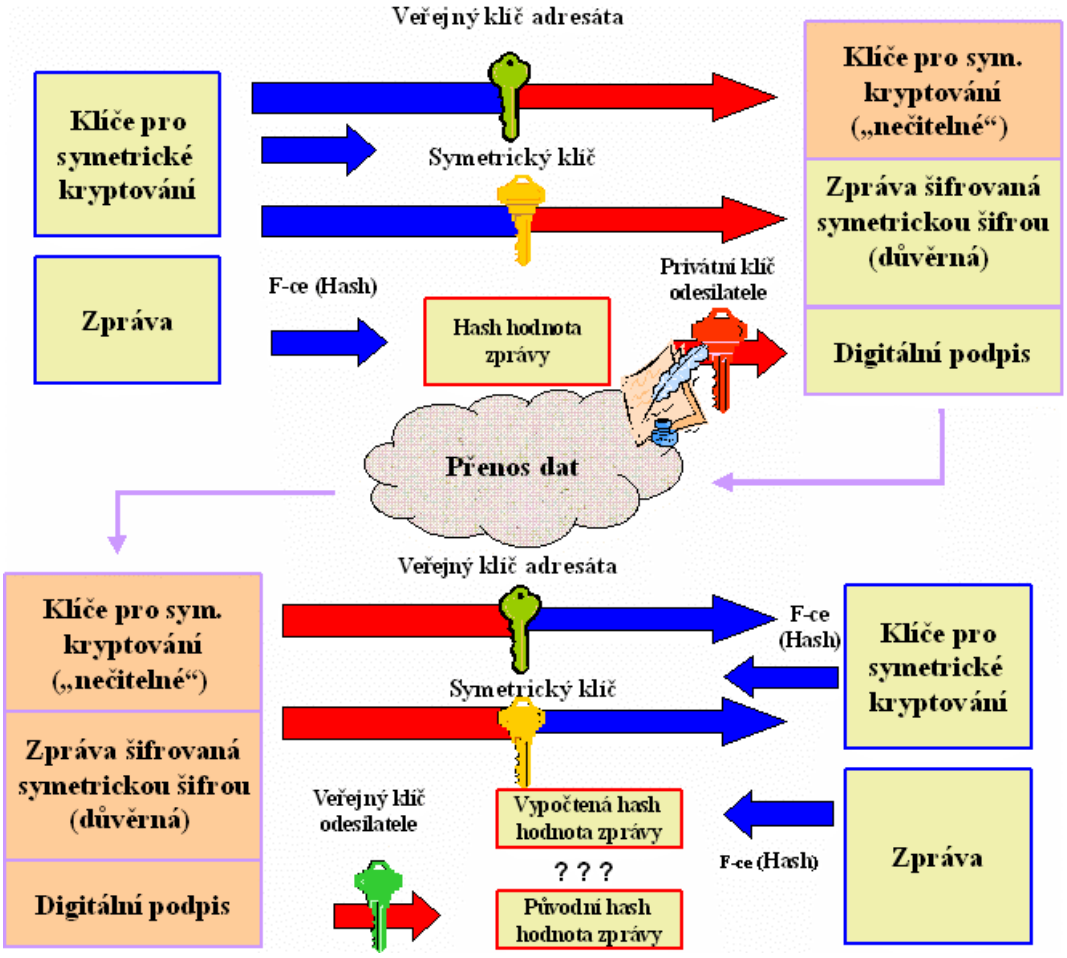
Bezpečná komunikace s využitím digitálního podpisu

K vytvoření digitálně podepsané a zašifrované zprávy můžeme použít níže popsaný postup. Odesilatel zprávy nejprve vypočte hash hodnotu zprávy a tu zašifruje svým privátním klíčem čímž vznikne digitální podpis zprávy. Potom zprávu zašifruje veřejným klíčem adresáta („znečitelní“ pro neautorizované subjekty). Takto upravená zpráva je spolu s digitálním podpisem předána (zaslána po síti, předána na disketě, ...) adresátovi. Ten nejprve zprávu dešifruje za pomocí svého privátního klíče a tím se zpráva stane čitelná. Podpis ověří výpočtem hash hodnoty zprávy a jejím srovnáním s dešifrovanou hash hodnotou z digitálního podpisu. V případě, že jsou srovnávané hash hodnoty shodné je zřejmé, že elektronický podpis vytvořila uvažovaná osoba a zpráva navíc nebyla po jejím podepsání změněna.

Tímto způsobem lze splnit kritéria bezpečnosti z úvodu. Protože je však při tomto postupu třeba jednou zašifrovat celou zprávu pomocí asymetrického algoritmu („znečitelnění“ zprávy), což by v případě delších zpráv trvalo na obou komunikujících stranách neúměrně dlouho, není toto užití v bezpečné komunikaci typické. Častěji se k šifrování zpráv používá model, ve kterém je asymetrická kryptografie použita pouze ke tvorbě digitálního podpisu a

bezpečné výměně klíčů pro symetrickou kryptografii, která je užita k vlastnímu šifrování přenášených dat. Tato komunikace vyžaduje dohodu o formátu přenášených dat a systému jejich šifrování. Pro každou přenášenou zprávu může odesilatel vygenerovat symetrický klíč, který bude použit k zašifrování (znečitelnění) zprávy. Samotný klíč je poté šifrován veřejným klíčem adresáta, čímž je zaručeno, že se k tomuto klíči dostane pouze adresát, který ho užije k dešifrování zprávy.

Příklad jednoduché, avšak prakticky užívané komunikace je zobrazen na obrázku 4b.



obr 4b.

Bezpečná komunikace s využitím digitálního podpisu a šifrováním zprávy symetrickou šifrou

Správa klíčů

Zřejmě nejproblematičtějším bodem bezpečné komunikace je správa a uchování klíčů. Při užití symetrické kryptografie je třeba s maximální možnou mírou bezpečnosti uchovávat klíče se seznamem příslušných komunikačních partnerů. Tento požadavek je však v rozporu s nutností poměrně časté změny klíče v souvislosti s dobou potenciálního prolomení těchto algoritmů. Jednodušší situace je při užití asymetrické kryptografie. Ani v tomto případě však nestačí chránit pouze soukromý klíč. Je také nutné uchovávat veřejné klíče všech komunikujících účastníků a k nim jednoznačnou identifikaci vlastníků těchto klíčů. Předání klíčů je před začátkem vůbec první vzájemné komunikace bezpečným kanálem je nezbytnou nutností. Při větším počtu vzájemně komunikujících subjektů to může být problém dosti závažný. Uchování těchto informací se tak stává nejslabším článkem bezpečné komunikace a může zcela znehodnotit snahy o vysoké zabezpečení přenášených dat.

Certifikáty

Certifikační autorita a certifikáty

Řešením problému zprávy, distribuce a uchování klíčů je využití služeb poskytovatele certifikačních služeb (PCS), častěji je v praxi užíván název certifikační autorita (CA). V textu dále bude zpravidla, až na výjimky používán pojem certifikační autorita. Certifikační autorita vystupuje při vzájemné komunikaci dvou subjektů jako třetí nezávislý důvěryhodný subjekt, který prostřednictvím jím vydaného certifikátu jednoznačně svazuje identifikaci subjektu s jeho dvojicí klíčů respektive s jeho digitálním podpisem. Certifikát se tak stává jakýmsi elektronickým průkazem totožnosti. Certifikáty obsahují ve své nejjednodušší formě veřejný klíč, jméno a další údaje zajišťující nezaměnitelnost subjektů. Běžně používané certifikáty též obsahují datum počátku platnosti, datum ukončení platnosti, jméno certifikační autority, která certifikát vydala, sériové číslo a některé další informace. Certifikační autorita garantuje jedinečnost subjektů podle užité identifikace subjektu. To je zajištěno legislativními a technickými pravidly provozu instituce certifikační autority. Splnění těchto požadavků potvrdí CA podpisem dokumentu svým privátním klíčem a následným vydáním tohoto certifikátu.

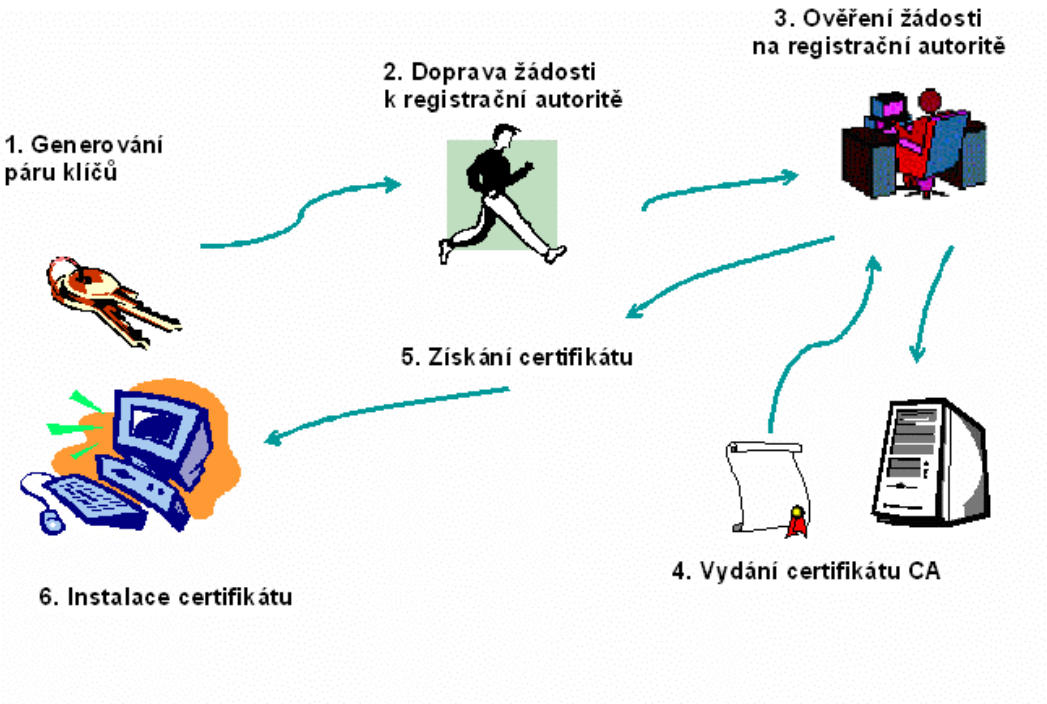
obr 5.
Certifikát

Znamená to, že certifikát je podepsaným dokumentem se všemi důsledky z toho plynoucími, tedy zejména autorizace (certifikační autorita jako garant pravosti dokumentu) a integrity dat (nelze zaměnit klíč nebo identitu klienta). Tím , že CA zaručuje správnost jí vydaného certifikátu , odstraňuje nutnost smluvní důvěryhodné výměny klíčů mezi dvěma subjekty navzájem a jejich dohoda spočívá pouze v domluvě o společně uznávané CA. Příklad běžného certifikátu vydaného fiktivnímu klientovi a certifikátu certifikační autority je v příloze. Důležité je, že se utajovaná data na straně klienta redukují pouze na bezpečné uchovávání privátního klíče, protože ostatní je řešeno certifikáty. Ty si můžeme kdykoliv ověřit se znalostí veřejného klíče certifikační autority, respektive jejího certifikátu. Existence CA také umožňuje důvěryhodnou komunikaci i subjektů, jenž se navzájem fyzicky nikdy nepotkali nebo neabsolvovali složitou proceduru vzájemné důvěryhodné výměny svých klíčů.

Tvorba a životnost certifikátů

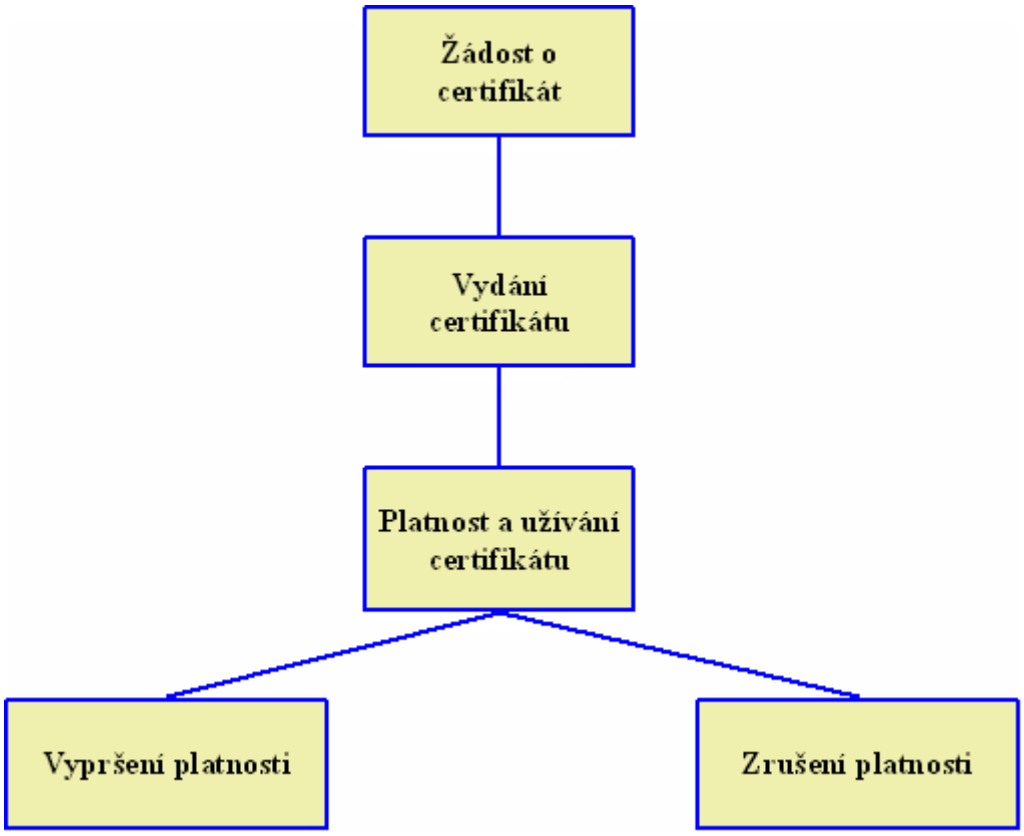
Tvorba certifikátu má 6 kroků:

1. Generování klíčů. Každý potenciální žadatel o certifikát si nejprve sám pomocí dostupného SW vybavení vygeneruje dvojici klíčů pro použití v asymetrické kryptografii. Pro tento účel není nutné počítat s nákupem nového softwaru, protože PC vybavené pro komunikaci na Internetu nutný software s největší pravděpodobností má již nainstalován. Procedura generace klíčů je zpravidla automatická nebo poloautomatická a probíhá v počítači. Aktivace procesu generace je možná buď spuštěním programu přímo na PC nebo je možné i vzdálené spuštění, například pomocí web serveru. Druhá varianta je často užívána, a to zejména pro to, že je rychlá a uživatelsky přívětivá.
2. Příprava identifikačních dat a žádosti o certifikát. Žadatel o certifikát shromáždí podle požadavků certifikační autority osobní identifikační materiály nutné pro vydání certifikátu, jako IČO, DIČ, resp. číslo OP, rodné číslo a podobně. Následuje vyplnění formuláře, ve kterém mohou být kromě standardních údajů, jako je například jméno a příjmení i údaje další, doplňkové. V žádosti o certifikát a následně i v certifikátu bývá často uvedena firma, pracovní zařazení, adresa atd.
3. Předání žádosti o certifikát autoritě. Certifikační autority, které nabízí své služby veřejnosti mají zpravidla kontaktní místa oddělena od centrálního systému. Důvodem není pouze vyšší bezpečnost, ale především nutnost mít kontaktní místa v mnoha lokalitách, blízko klientům. Kontaktní místa CA se nazývají registrační autority (RA). Žadatel předá na RA data nutná pro vydání certifikátu spolu s doklady o jejich pravosti. U CA vyšší úrovně bezpečnosti jsou údaje uvedené z žádosti následně kontrolovány na RA a proto je nutné, aby bylo možné jednotlivé položky žádosti doložit příslušnými doklady a ověřit.
4. Ověření informací. Certifikační autorita si na příslušných místech ověří, že může vydat žadateli certifikát. Při ověření žádosti o certifikát je možné ověřit nejen doklady žadatele a informace z dostupných registrů a ostatních datových zdrojů, ale je možné ověřit i konzistenci šifrovacích klíčů a jejich jedinečnost v rámci konkrétní CA.
5. Tvorba certifikátu. Certifikační autorita vytvoří digitální dokument příslušného formátu a ten poté podepíše svým privátním klíčem. U CA s vyšší úrovní bezpečnosti je certifikát vydáván off-line. Důvodem je především bezpečnost, která spočívá ve vícestupňové kontrole a možnosti oddělení centrálního systému od okolí.
6. Předání certifikátu. Podle dohody je certifikát žadateli předán (disketa), zaslán, nebo zveřejněn. Nezveřejnění certifikátu poskytuje pouze minimální ochranu, proto jsou certifikáty zpravidla u veřejných CA zveřejňovány. V rámci zveřejnění certifikátů CA informuje i o jeho platnosti a stavu, což naopak přispívá ke zvyšování bezpečnosti a důvěry.



Doba platnosti certifikátů je omezená a je uvedena v každém certifikátu. Tato veličina je velmi důležitá. Pokrok ve zvyšování výkonnosti výpočetní techniky a možnost objevení mezer v protokolech nebo algoritmech by ve velkém časovém horizontu mohl způsobit, že by se certifikáty staly nespolehlivé. Běžné certifikáty jsou proto vydávány s platností 6 měsíců nebo 1 rok. I během této doby je možné zrušit platnost certifikátu. Důvodem pro toto opatření může být například vyzrazení privátního klíče. I tuto situaci je možné přirovnat ke ztrátě osobních dokladů a následných procedur s tím spojených.

V praxi je možné o zneplatnění certifikátu požádat několika způsoby. Je však nutné brát v úvahu nutnost identifikace žadatele. Tím nejběžnějším způsobem zneplatnění certifikátu je osobní návštěva na RA. Zneplatnit certifikát je však často nutné i mimo pracovní dobu nebo v době a místě, kde jsou RA nedostupná. V tom případě nastupuje elektronická komunikace. K tomuto účelu umožňuje CA podat žádost o zneplatnění pomocí mailu či webu. Identifikace žadatele je řešena alternativně elektronickým podpisem nebo jiným identifikačním prostředkem, zpravidla jednorázovým heslem.



obr 6.
Životní cyklus certifikátu.

Zrušený certifikát je zařazen do seznamu zneplatněných certifikátu (CRL). Seznam zneplatněných certifikátů je tedy jakási černá listina, na které jsou uvedeny neplatné certifikáty, jejichž doba platnosti ještě nevypršela Tento seznam je obdobou případu seznamu zrušených kreditních karet. Banka nemůže donutit klienta aby neužíval svou kreditní kartu, stejně jako certifikační autorita nemůže zabránit klientovi v užívání certifikátu. Při každé transakci pomocí certifikátů je možné si pomocí této listiny certifikát ověřit.. Seznam zneplatněných certifikátů je veřejně přístupná listina podepsaná certifikační autoritou a chráněná tedy stejně jako certifikát.

Funkce CA

V předchozí kapitole byly popsány obě základní funkce CA z hlediska plnění potřeb zákazníka, tedy vydávání certifikátů a seznamu zneplatněných certifikátů. Certifikační autority však umožňují a zpravidla vykonávají i další úkony. Funkce CA lze rozdělit do čtyř základních kategorií:

1. *Autentikace a registrace ostatních certifikačních autorit a uživatelů.*

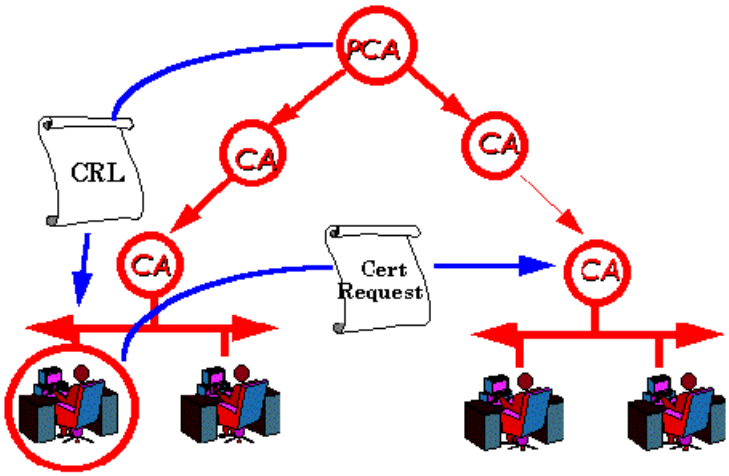
2. *Uložení a distribuce identifikačních informací.*

3. *Certifikace a certifikačně správní funkce.*

4. *Notářské funkce.*

Bod 1. poukazuje na autentizační, identifikační a registrační funkce Certifikační autority.

CA nemusí existovat samostatně, jak je typické u lokálních sítí typu intranetu, kde se zpravidla jedná o účelové certifikační autority. Ve velkých sítích, je míněn zejména internet, může existovat i systém propojených CA. Každý uživatel se může registrovat u CA, kterou si sám vybere, což je výhodné s ohledem na množství uživatelů, různorodé požadavky, jejich topologii a úroveň zabezpečení. Jednoduchý systém propojených CA je na následujícím obrázku.



obr.7
Stromová struktura certifikátu

Při zařazení nové CA do stromu nebo síťové struktury CA je třeba vzájemná autentizace a registrace CA. Zpravidla stačí, jestliže nová CA vydá certifikát a tak projeví důvěru k certifikační autoritě ve struktuře uvedené bezprostředně nad ní, případně certifikační autoritě uvedené bezprostředně pod ní. Nadřízená i podřízená certifikační autorita pak naopak vydají

certifikáty této nové CA (křížová certifikace). Při ověřování podpisu komunikačního partnera je třeba vytvořit certifikační cestu. To v praxi znamená, že první certifikát v řetězci certifikuje veřejný klíč certifikátu, který jej předcházel. Veřejný klíč posledního certifikátu náleží CA, které důvěřuje ověřovatel. Při velké složitosti stromu CA je možné vydání certifikátů i mezi nezvětvenými CA. To výrazně zjednodušuje uživateli ověřování důvěryhodnosti certifikátu komunikačního partnera, certifikovaného u vzdáleného CA, zkrácením certifikační cesty.

Autentizace a registrace jednotlivých uživatelů je problém důvěryhodnosti certifikátů. Různé kvality ověřování identity uživatele určují mimo jiné i důvěru v jeho certifikát. V nejjednodušší formě zajišťuje CA pouze jedinečnost jména subjektu a nikoliv jeho identitu. Ve vyšším stupni autentizace uživatelů je nutné již zmiňované ověření totožnosti podle osobních dokladů realizované prostřednictvím registračních autorit. Vzájemná komunikace mezi RA a CA musí probíhat po bezpečném kanále (např. bezpečný e-mail).

Při chodu CA vzniká velké množství dat, které je nutno odpovídajícím způsobem zveřejnit a uchovat. CA zpravidla pro tuto činnost vyžívají adresářové služby. Uložení dat CA bývá zálohováno spolehlivým způsobem.

Certifikační autorita i uživatelé uchovávají i data privátního charakteru. Jsou to především privátní šifrovací klíče a certifikát nadřízené (kořenové) CA. Tyto data je třeba s ohledem na důležitost a cenu těchto informací chránit před zneužitím nebo dokonce odcizením. Nejjednodušší ochranou je uložení soukromích dat na disku v zašifrované podobě chráněné přístupovým heslem. Obdobně lze tyto data uchovávat na disketě, kterou po ukončení práce uložíme na bezpečném místě. V poslední době se stále více užívá k uchování citlivých dat čipová karta chráněná PINem. Odpadá pamatování složitých hesel a jediná karta může umožňovat přístup k několika zařízením. Čipová karta má navíc inteligentní logickou ochranu. Ani tato moderní technologie však zejména u CA s vysokou úrovní bezpečnosti často nestačí. Zde se užívá bezpečné řešení, které odolává jak logickým, tak i fyzickým útokům.

Obsahem bodu 3. je certifikace a certifikačně správní funkce. Certifikační autorita z hlediska uživatele pracuje jako server, který na definovaný formát žádosti odpovídá standardní odpovědí. Při žádosti o službu vydání standardního certifikátu žádá uživatel zpravidla žádostí dle formátu PKCS #7. Nezbytnou součástí žádosti je identifikace žadatele a jeho veřejný klíč. Z bezpečnostních důvodů je žádost podepsaná privátním klíčem, čímž je potvrzena pravost klíče. Opovědí CA na tuto žádost je po nezbytných procedurách vydání standardního certifikátu (X.509, EDI). Kromě standardních certifikátů umožňuje CA i vydávání tzv. rozšířených certifikátů, definovaných v X.509 v.3 resp. PKCS #6, které mimo standardní položky obsahují navíc například položku účelu vydání certifikátu, certifikační politiku, alternativní jména a podobně.

Žádost o zneplatnění certifikátu je možné podat několika způsoby a jejich specifikace je přesne specifikována v příslušných dokumentech (zpravidla Certifikační politice) konkrétní CA. Opovědí na žádost o zneplatnění certifikátu je zneplatnění a vydání nového CRL, případně Delta CRL (X.509 v.3), což je seznam pouze nově zneplatněných certifikátů. Obdobně jako u certifikátů i u CRL je možné vydávat rozšířené CRL, které pak obsahuje například i důvod zneplatnění, datum a podobně.

Vydávání certifikátů se řídí tzv. Certifikační politikou. Ta určuje, za jakých podmínek bude kladně vyřízena žádost o certifikát. Certifikační politika je nedílnou součástí tzv. Bezpečnostní politiky CA, která je určující pro bezpečnost a tím i důvěryhodnost dané CA.

Poslední 4. funkcí CA je plnění notářských funkcí. Certifikační autorita může vystupovat ve funkci elektronického notáře při ověřování podpisu dokumentů, časového

cejchování, případně potvrzování celých transakcí.

Bezpečnost CA.

Celá kapitola pojednává především o bezpečné komunikaci. Bezpečnost CA, která je součástí komunikačního řetězce stejně jako komunikující strany je velmi důležitá. Nejde však pouze o ochranu privátních dat CA, jako jsou například privátní klíče, ale o celkovou bezpečnost celého systému certifikační autority. Tento problém je složitý, a vzhledem k výše uvedeným funkcím i rozsáhlý. Vysoká úroveň bezpečnosti je na jedné straně tedy žádoucí, na straně druhé však omezuje uživatele CA restriktivními opatřeními. Úkol tedy spočívá v nalezení kompromisu.
Proto, abychom byli schopni posoudit zda konkrétní CA vyhovuje požadavkům na zabezpečení certifikátů pro vybraný systém, je třeba detailně prostudovat bezpečnostní dokumentaci CA. V souladu s vyhláškou Úřadu pro ochranu osobních údajů k zákonu o elektronickém podpisu lze definovat základní dokumenty, které by měla mít každá CA. Pokud CA nemá níže popsané dokumenty, měla by mít jejich obdobu.

- certifikační politika
- certifikační prováděcí směrnice
- celková bezpečnostní politika
- systémová bezpečnostní politika
- plán zvládání krizových situací a plán obnovy

Je zřejmé, že ne všechny dokumenty nutné pro činnost CA jsou veřejné. Zveřejněny musí být právě dokumenty, které nám, uživatelům, umožní rozhodnout o přijatelnosti CA pro náš účel. Mezi takové dokumenty rozhodně patří certifikační politika. Popis obsahu jednotlivých dokumentů je rozebrán v kapitole věnované legislativě. Pro první posouzení vhodnosti CA je možné vycházet i z dále popsaných kritérií, které vám umožní v krátkosti posoudit některé klíčové body hodnocení.

Deset pohledů na bezpečnost a důvěryhodnost certifikační autority

Tato kritéria jsou použita k popsání některých technických řešení, provozních procedur a úrovně důvěry pro generaci, distribuci, ověřování a použití certifikátů certifikační autority.

1. Postupy vytváření jednoznačných jmen pro certifikační autority a uživatele

Zjednodušeně řečeno, certifikát spojuje fyzickou totožnost subjektu s totožností elektronickou. Co to však v tomto případě je fyzická totožnost? Běžně užívané certifikáty (X.509) mají definovánu základní sadu identifikačních položek, jako například jméno, organizace, organizační jednotka, a dále rozšířené položky, jejichž použití je zpravidla nepovinné. Tyto položky se však přesně nekryjí s položkami občanského průkazu nebo obchodního rejstříku. Proto je třeba určit postup, podle kterého budou údaje z průkazů totožnosti transformovány do certifikátů tak, aby v rámci možností poskytovaly jednoznačné údaje identifikující konkrétní subjekt, včetně takových zdánlivých detailů, jako je například transkripce jmen s diakritikou.
Certifikát je jednoznačně identifikován vydavatelem a číslem certifikátu. Vydavatelem certifikátu je certifikační autorita. Ta určuje postupy tvorby jednoznačných jmen svých klientů. Zákon o elektronickém podpisu popisuje dva druhy certifikátů, a to certifikát a kvalifikovaný

certifikát. Certifikát jako takový není ve vztahu ke konkrétním položkám jednoznačného jména zmiňován, pouze spojuje data pro ověření podpisu s podepisující osobou a umožňuje ověřit její totožnost. Zákon popisuje minimální požadavky na jednoznačné jméno uvedené v kvalifikovaném certifikátu, jméno a příjmení podepisující osoby nebo její pseudonym, případně zvláštní znaky podepisující osoby.
Zvláštní kapitolou je postup vzniku jednoznačného jména certifikační autority, zejména té s obecnou působností. Jednoznačná jména certifikačních autorit bude třeba koordinovat, aby nedošlo k duplicitám, ať již úmyslným nebo náhodným. Tato situace je potenciálním bezpečnostním incidentem.
Obecně je postup vytváření jednoznačných jmen popsán v dokumentu nazývaném zpravidla certifikační politika.

2. Pravidla pro ověřování jednoznačných jmen certifikačních autorit a uživatelů

Certifikáty lze rozdělit na dvě základní skupiny. V té první budou certifikáty, jejichž jednoznačné jméno nepodléhá žádné kontrole a ověření. To jsou především certifikáty pro testovací účely a nemají přílišného praktického využití. Nicméně někdy člověka potěší nechat si vydat certifikát na Microsoft. Výhodou těchto certifikátů je, že jejich vydání je zpravidla rychlé, bezproblémové, bez procedur s ověřováním položek, nemusí se nikam chodit a v neposlední řadě je to většinou zadarmo.
Druhou skupinou jsou certifikáty, jejichž položky podléhají kontrole. Tady jsou pravidla pro jednoznačná jména striktně daná. Certifikační autorita zpravidla prostřednictvím svých registračních autorit (RA) kontroluje platnost a pravdivost položek uvedených v žádosti o certifikát. Liší se však, a to mnohdy podstatně, kvalita ověřovací procedury. Mám na mysli zejména požadované doklady nutné k registraci a způsob jejich ověřování. Úroveň kontroly může být různá, od totální benevolence, až k obtěžování.
Vhodná úroveň tohoto atributu závisí především na účelu, ke kterému certifikáty potřebujeme. V každém případě však důvěryhodná CA musí zajistit možnost určení totožnosti vlastníka certifikátu.

3. Ověření platnosti žádosti o certifikát

Procedura vydání certifikátu začíná tvorbou žádosti o certifikát, potom následuje předání žádosti na vybranou certifikační autoritu. Ta žádost zpravidla ověřuje. A nejedná se pouze o ověřování položek jednoznačného jména. Je vhodné provádět pro ochranu žadatele celou řadu kontrol.
Většina CA vyžaduje formát, který má obsah žádosti podepsán příslušným privátním klíčem (PKCS# 10). Tato kontrola zajistí, že žadatel má k příslušnému veřejnému klíči i klíč privátní. Je velmi důležitá a eliminuje značná bezpečnostní rizika. Příkladem dalšího typu kontroly je ověřování, je-li klíč uvedený v žádosti o certifikát jedinečný. Pravděpodobnost, že bude ať již náhodou, či úmyslně vygenerována stejná dvojice kryptografických klíčů, je minimální, přesto některé CA z důvodů vyšší bezpečnosti tuto kontrolu provádějí.
Některé certifikační autority navíc zajišťují jedinečnost použitého jednoznačného jména. To sebou samozřejmě nese další kontrolu při podání žádosti a navíc potenciální obtíže při řešení a kontrole obnovovaných certifikátů.
Všechny kontroly žádostí o certifikát se odráží v bezpečnostní politice CA a zárukách, které nám konkrétní CA poskytuje.

4. Postup podepisování certifikátu a ochrana privátního klíče CA a uživatelů

Po ověření žádosti na všech možných i nemožných kontrolách následuje samotný akt tvorby certifikátu. To v podstatě znamená podepsat privátním klíčem CA položky získané během registrační procedury, a tím stvrdit platnost předchozích kroků. Pro CA je tento krok z bezpečnostního pohledu velice citlivý, protože znamená použití privátního klíče CA, tedy nejlépe střežených dat CA. Ztráta kontroly nad privátním klíčem je největším bezpečnostním incidentem, jaký může nastat. Proto je ochraně privátních dat CA věnována maximální pozornost.
Postup tvorby certifikátů je možný ve dvou módech. Za prvé off-line. Žádost o certifikát je pozastavena na CA a operátor musí dát souhlas k vytvoření certifikátu. Operátor aktivuje privátní klíč CA. Tento postup je obvyklý u CA vyšší úrovně zabezpečení. Jako hardwaru je použito minimálně čipových karet, častěji však zařízení vyšší bezpečnosti (black box). Privátní klíč toto zařízení nikdy neopustí a procedura podpisu probíhá přímo uvnitř tohoto zařízení. Off-line přístup sebou nese problémy v oblasti on-line služeb CA, jako například automatizované tvorby seznamu zneplatněných certifikátů (CRL) nebo služeb, jako je časové razítko.
On-line služby jsou procedurálně jednodušší, a proto bývají používány zejména na jednodušších CA.

Ochrana privátního klíče u uživatele je zpravidla zcela v kompetenci jeho samotného. Uložení privátního klíče na pevném disku není příliš bezpečné, i když jsou zpravidla uloženy v zašifrované podobě (pomocí symetrické kryptografie). Podstatně bezpečnějším řešením je použití čipové karty se čtečkou nebo podobný systém. Takové řešení není finančně nijak náročné a rozdíl v bezpečnosti privátního klíče je diametrální. Ponecháme-li stranou uzavřené systémy, CA nemá zpravidla prostředky ke kontrole nakládání klienta se soukromým klíčem, tuto otázku však řeší svými ustanoveními přímo Zákon o elektronickém podpisu.

5. Zneplatnění certifikátů a ověřování certifikátů

Při potenciálním nebezpečí zneužití privátního klíče nebo i z jiných důvodů je někdy třeba, obdobně jako u platebních karet, zrušit platnost certifikátu. To se děje zpravidla on-line procedurou různými komunikačními kanály. V takovém případě je využívána identifikace heslem, které je dohodnuto již při vzniku certifikátu. Je nedostatečné požadovat pouze elektronicky podepsanou žádost, protože právě ztráta privátního klíče je často důvodem k zneplatnění certifikátu. Jestliže CA akceptuje žádost o zneplatnění, je certifikát zařazen do seznamu zneplatněných certifikátů. Ten je zveřejňován zpravidla nejméně jednou denně. Při každé transakci s použitím certifikátu bychom tedy měli zjišťovat mimo jiné i to, jestli není certifikát našeho komunikačního partnera zneplatněn a nejedná-li se tedy o potenciální útok.
Kontrolu platnosti certifikátu je možné provádět dvěma způsoby. Buď kontrolujeme platnost certifikátu proti CRL a pokud tam certifikát není uveden, považujeme ho za platný, nebo se CA přímo dotazujeme na platnost konkrétního certifikátu. Oba způsoby mají své výhody i nevýhody.

6. Ochrana báze dat a software certifikační autority

Certifikační autorita je z určitého pohledu softwarový produkt. Po implementaci je třeba zajistit jeho bezproblémovou funkci především stabilizací jednotlivých komponent. Vzhledem k charakteru CA je důležitá minimalizace změn v primárních SW modulech, zejména v operacích s privátním klíčem CA. Případné upgrade nebo rozšíření modulů musí být

upraveno vnitřními předpisy. Platí obecná bezpečnostní zásada oddělení implementace od provozu.
Certifikační autorita musí uchovávat poměrně značný objem dat a dokumentů. Tato data musí předepsanou formou zveřejňovat, mnohdy po dlouhou dobu. Proto musí být základní dokumenty, jako smlouvy s klienty, identifikační údaje klientů, certifikáty, CRL a podobně chráněny nejen proti modifikaci, ale i proti ztrátě, kvalitním archivačním systémem.
Pro akreditované certifikační autority je zákonem stanovena doba archivace na 10 let. Data v působnosti CA mají často charakter osobních údajů a jsou tedy navíc chráněna i dalšími zákony.

7. Kontrola certifikačních autorit

Největší hodnotou certifikační autority je její důvěryhodnost. Ta se těžko získává, ale velice lehce ztrácí. CA v začátku svého fungování veřejně vyhlásí podmínky, které nabízí svým klientům ve smluvním nebo mimosmluvním vztahu. To se děje zpravidla prostřednictvím certifikační politiky, vzorových smluv a podobně. Tyto dokumenty jsou poté pro CA závazné. Jejich dodržování není nikým kontrolováno, vše funguje na bázi důvěry. Velká změna však přichází se zákonem o elektronickém podpisu. Z dikce zákona je kontrolou CA dle jednotlivých bodů definovaných zákonem nebo prováděcími předpisy u akreditovaných vydavatelů kvalifikovaných certifikátů pověřen přímo Úřad pro ochranu osobních údajů. Neakreditovaný vydavatel kvalifikovaných certifikátů podléhá kontrole nepřímo, protože je povinen nahlásit splnění podmínek vydávání kvalifikovaných certifikátů. Případné neplnění zmíněných podmínek by potom bylo porušení zákona a taková CA může být potrestána pokutou až do výše 20 mil. Kč. Ještě horší než pokuta, by byla ztráta dobrého jména, což v této branži znamená prakticky konec.

8. Směrnice pro uživatele a systémové administrátory certifikační autority

Součástí dokumentace CA jsou i směrnice a příručky pro uživatele i vnitřní potřebu CA. Dokumentace pro uživatele obsahuje především příručky týkající se tvorby žádosti o certifikát a operací s certifikátem obecně. Zpravidla jsou také k dispozici příručky pro instalaci certifikátu do různých prostředí. Pro bezchybné fungování CA většího rozsahu je nezbytné vytvořit kompletní dokumentaci pro operátory RA, operátory samotné CA a systémové pracovníky. Příručky jsou nezbytné i pro určení pravomocí a povinností pracovníků CA, určení odpovědnosti konkrétních pracovníků za jednotlivé operace CA. Příručky musí být přesné a detailní. Je třeba si uvědomit, že jde v neposlední řadě i o bezpečnostní atribut, protože až 80% útoků na systém je vedeno přímo z vnitřku organizace. Směrnice a příručky pro pracovníky CA jsou neveřejné.

9. Notářské úkony certifikační autority

Certifikační autorita může kromě svého hlavního poslání, tedy vydávání certifikátů a funkcí s tím spojených fungovat jako elektronický notář. Do těchto funkcí lze zařadit i například vydání časového razítka. CA tímto úkonem potvrzuje přesný čas konkrétní operace, například podpisu smlouvy nebo převodu peněz. CA také může nabízet služby důvěryhodné archivace citlivých elektronických dokumentů a podobně. Mnohé z těchto notářských úkonů jsou téměř nezbytné pro bezpečné využívání elektronického oběhu dokumentů v praxi. Zákon o elektronickém podpisu se o notářských funkcích CA nezmiňuje.

10. Přístupnost služeb certifikační autority

Dostupnost certifikační autority je jednou z veřejně deklarovaných hodnot. Nejedná se pouze o dostupnost a otevírací dobu RA, ale především o dostupnost CA jako důvěryhodného elektronického zdroje informací. Jde zejména o seznam vydaných a zneplatněných certifikátů. Tyto funkce CA mohou být pro některé operace kritické. Proto je požadována maximální, optimálně nepřetržitá dostupnost.
Některé z těchto služeb jsou pro CA vydávající kvalifikované certifikáty přímo předepsány zákonem. Jedná se především o možnost „neprodleně" ukončit platnost certifikátu a dále pak o již zmiňované zveřejnění CRL.
Uvedená kritéria nejsou v žádném případě vyčerpávajícím a detailním obrazem funkcí a bezpečnosti CA. Je pouze jakýmsi pohledem do problematiky.
Při případném výběru konkrétní CA, ať již akreditované nebo neakreditované, vydávající kvalifikované certifikáty nebo jiné, je třeba vidět i ostatní atributy. Zajímavým atributem je počet vydaných certifikátů, počet registračních autorit nebo délka provozu CA. I tyto dílčí údaje mohou poskytnout důležité informace o celkovém postavení firmy na dynamickém trhu ICT.
Z webových stránek http://www.ica.cz pochází i následující otázky a odpovědi:

1. **Co je to certifikát?**
   Certifikát je datová zpráva, která je vydána jakýmkoliv poskytovatelem certifikačních služeb (CA). Certifikát spojuje data pro ověřování podpisů s podepisující osobou a umožňuje ověřit její totožnost. Vyšší formou certifikátu je kvalifikovaný certifikát. Pro snadnější odlišení certifikátu od kvalifikovaného certifikátu se někdy pro certifikát používá označení komerční certifikát.

2. **Co je to kvalifikovaný certifikát?**
   Kvalifikovaný certifikát je certifikát, jehož náležitosti jsou definovány zákonem 227 Sb. O elektronickém podpisu. Kvalifikovaný certifikát musí být především označen jako kvalifikovaný dle zmiňovaného zákona, musí přesně identifikovat podepisující osobu i vydavatele certifikátu, musí mít vyznačenu dobu platnosti a další náležitosti.

3. **Co je to akreditace?**
   Akreditace je osvědčení, že poskytovatel certifikačních služeb splňuje podmínky stanovené ZoEP pro výkon takové činnosti. Akreditaci uděluje Úřad pro ochranu osobních údajů. Akreditovaný poskytovatel certifikačních služeb je oprávněn vydávat kvalifikované certifikáty, může však vydávat i certifikáty komerční.

4. **Co je to zákon o elektronickém podpisu (ZoEP)?**
   Zákon o elektronickém podpisu je zákon 227/2000 Sb. O elektronickém podpisu a o změně některých dalších zákonů.

5. **Co je elektronická podatelna?**
   Elektronická podatelna je pracoviště orgánů veřejné moci určené pro příjem a odesílání datových zpráv. Elektronická podatelna přijímá i zprávy (podání) podepsané zaručeným elektronickým podpisem a ty dále zpracovává.

6. **Jaké dokumenty mám získat od CA při vydávání certifikátu?**
   Při vydávání certifikátu předává CA žadateli různé dokumenty různé právní váhy. V té nejjednodušší podobě nemusí být klientovi předány žádné dokumenty, což zpravidla indikuje minimální záruky ze strany CA. Na druhé straně stojí akreditovaný poskytovatel certifikačních služeb, kde jsou ZoEP přesně definovány dokumenty, které mají být klientovi předány.

7. **Co je to CRL**
   CRL je zkratka pro Certification Revocation List, neboli seznam zneplatněných certifikátů.

8. **Co je certifikační autorita (CA)?**
   Certifikační autorita je jiný, často užívaný název pro poskytovatele certifikačních služeb**.**

9. **Jaké identifikační položky jsou uvedeny v certifikátu?**

10. **Co znamená pojem „následný" certifikát?**
    Následný certifikát je certifikát, který je vydán klientovi po uplynutí doby platnosti certifikátu prvotního. Následný certifikát je vydán pouze v případě, že klient nepožaduje změnu položek předchozího certifikátu. Pokud ji požaduje, nejedná se o certifikát následný, ale prvotní. Při vydávání následného certifikátu před vypršením platnosti předchozího certifikátu již není nutná přítomnost zákazníka na registrační autoritě I.CA. Klient pouze zašle s využitím platného certifikátu elektronicky podepsanou žádost o vydání následného certifikátu ve standardizované elektronické podobě

11. **Co je to registrační autorita?**
    Je to kontaktní pracoviště sloužící ke komunikaci s klienty. Zajišťuje zejména přijímání žádostí o certifikáty a jejich následné předávání klientům. Tato pracoviště provádějí ověření totožnosti žadatele o certifikát a shodu žádosti s předloženými doklady. Registrační autority nevydávají certifikáty, pouze o ně žádají na centrálním pracovišti I.CA.

12. **Co je to mobilní registrační autorita ?**
    Standardní pracoviště registrační autority, u kterého je zajištěna mobilita. Je tedy možné, aby bylo k dispozici na místě určeném klientem. Jeho výhodou je, že klient je obsloužen přímo v místě, které si určí (nejčastěji sídlo společnosti).

    I.CA provozuje službu „Výjezd mobilní registrační autority" což je služba určená především pro jednorázové vydání většího počtu certifikátů v jednom místě pro potřeby např. konference, výjezdního zasedání či uspokojení požadavku menší firmy, která chce službu zajistit jednorázově pro své zaměstnance.

13. **Co je to veřejná registrační autorita ?**
    Je to kontaktní pracoviště sloužící ke komunikaci s klienty, v tomto případě široké

veřejnosti. Zajišťuje zejména přijímání žádostí o certifikáty a následné předávání certifikátů klientům. Tato pracoviště provádějí ověření totožnosti žadatele o certifikát a shodu žádosti s předloženými doklady. Registrační autority nevydávají certifikáty, pouze o ně žádají na centrálním pracovišti I.CA.
V současné době jsou umístěny veřejné registrační autority na pracovištích Středisek služeb PVT, a.s. a jejich seznam lze naleznout zde.

14. Co je to klientská registrační autorita ?

Je to kontaktní pracoviště sloužící ke komunikaci s klienty, v tomto případě zřízené přímo v místě určeném klientem. Zajišťuje zejména přijímání žádostí o certifikáty a následné předávání certifikátů klientům. Tato pracoviště provádějí ověření totožnosti žadatele o certifikát a shodu žádosti s předloženými doklady. Registrační autority nevydávají certifikáty, pouze o ně žádají na centrálním pracovišti I.CA.
Zřízením takového pracoviště je vhodné pro větší firmy, které vydávají certifikáty svým zaměstnancům nebo klientům.

15. Co je to doba platnosti certifikátu?

Každý certifikát je vydáván na dobu určitou. Doba, po kterou je certifikát platný, je uvedena v každém certifikátu. Určení délky platnosti je vždy v moci poskytovatele certifikačních služeb a stanovení doby je úzce spojeno s použitou technologií a deklarovanou bezpečností. Klient má zpravidla možnost výběru délky platnosti dle možností nabízených poskytovatelem.
Během doby platnosti certifikátu je možné zrušit jeho platnost. Důvodem pro toto opatření může být například podezření na bezpečnostní incident.

16. Co znamená pojem „zneplatnění" certifikátu?

Zneplatnění certifikátu je úkon, který zajistí ukončení platnosti certifikátu dříve než bylo na certifikátu deklarováno. Důvod pro předčasné ukončení platnosti certifikátu může být např. odcizení PC s daty pro tvorbu elektronického podpisu.
Žádost o zneplatnění certifikátu podává klient prostřednictvím libovolné veřejné registrační autority, nebo prostřednictvím webových stránek. Zneplatněný certifikát je zařazen do seznamu zneplatněných certifikátu, které byly zneplatněny (CRL).

17. Co je důvěrnost, integrita, dostupnost a nepopiratelnost ?

Jde o základní vlastnosti v oblasti počítačové bezpečnosti. Důvěrnost znamená skutečnost, že data nebo informace nejsou předávány nebo prozrazovány neoprávněným stranám. Integrita znamená skutečnost, že data nebo informace nemohly být změněny neoprávněným způsobem. Dostupnost znamená skutečnost, že žádané zdroje jsou přístupné a použitelné v příhodnou dobu a požadovaným způsobem. Nepopiratelnost představuje vlastnost získanou na základě kryptografických metod, kdy je jednotlivým stranám zabráněno popřít, že uskutečnily určitou akci týkající se dat (jako například mechanismy k zabránění popření autorství, k dokázání povinnosti, záměru nebo závazku nebo dokazování vlastnictví).

18. Je podepsaná zpráva současně zašifrovaná ?

Není. Elektronický podpis zprávy zajišťuje především nepopiratelnost projevu vůle podepisující osoby vůči podepsané zprávě. Vzhledem k použité technologii realizace elektronického podpisu je zajištěna i integrita podepsané zprávy. Šifrování je technologie zajišťující primárně důvěrnost.

19. Co to jsou párová data?

V případě elektronického podpisu podle Zákona č. 227/2000 Sb. o elektronickém podpisu, jsou to data pro vytváření elektronického podpisu spolu s odpovídajícími daty pro ověřování elektronického podpisu. V případě digitálního podpisu se používá termín dvojice klíčů - veřejný a soukromý (privátní) klíč.

20. Co to je počítačová transakce?

Elektronická výměna počítačových dat mezi dvěma subjekty s využitím výpočetní techniky.

21. Co to je zablokování certifikátu?

Stav, ve kterém se certifikát nachází od doby, kdy jej I.CA zneplatnila, do doby, kdy I.CA zveřejnila seznam certifikátů, které byly zneplatněny, ve kterém je tento certifikát poprvé zařazen.

22. Co to je testovací certifikát ?

Certifikát sloužící k ověření funkčnosti této technologie. K jeho vydání dochází prakticky okamžitě po odeslání řádně vyplněné žádosti na I.CA. Fyzické ověření totožnosti žadatele o certifikát není v tomto případě požadováno. Platnost testovacího certifikátu je 14 dní, po uplynutí této lhůty je automaticky ukončena jeho platnost. Tyto certifikáty jsou neveřejné a jsou vydávány vždy zdarma.

23. Co to je komerční certifikát standard?

Certifikáty standard představují osobní certifikáty vhodné pro běžné využití. Jsou vydávány fyzickým nebo právnickým osobám na základě řádně vyplněné žádosti o certifikát předané kontaktnímu pracovišti I.CA, současně s předložením požadovaných dokladů pro nezbytné ověření totožnosti žadatele. Délka platnosti těchto certifikátu je vždy závislá na délce použitého kryptografického klíče.

24. Co to je komerční certifikát comfort?

Certifikáty comfort představují osobní certifikáty, jejichž hlavní odlišností od certifikátů standard je čipová karta, která je součástí této služby. Slouží jako médium k bezpečnému uložení dat pro tvorbu elektronického podpisu a bezpečnému vytváření elektronického podpisu. Tato služba je určena především pro firemní účely, je však poskytována pro fyzické i právnické osoby.

25. Co to je komerční certifikát pro server ?

Certifikáty pro servery jsou určeny pro bezpečnou komunikaci serverů. Jsou vydávány pro fyzické nebo právnické osoby na základě řádně vyplněné žádosti o certifikát, kterou žadatel pro ověření fyzické totožnosti předloží společně s požadovanými doklady totožnosti na kontaktním pracovišti I.CA. Délka platnosti certifikátu pro server je vždy závislá na délce použitého kryptografického klíče.

26. Mohu generovat žádost o certifikát na jiném počítači, než na kterém ho chci mít?

Ano, ale po vydání certifikátu příslušného k párovým datům je nutné realizovat export a následně import na požadované PC. Především je nutné z PC, kde párová data vznikla, tato odstranit. Z bezpečnostního hlediska však tento postup není příliš vhodný, neboť je zde řada možných rizik.

27. Liší se certifikáty komerční a kvalifikované ?

Z hlediska použité technologie se neliší. Liší se zejména účelem použití a tím, kdo může být podepisujícím subjektem. Vytváření, správa a použití se řídí odlišnými certifikačními politikami. Kvalifikovaný certifikát je striktně řízen zákonem č. 227/2000 Sb. a slouží výhradně pro oblast elektronického podpisu. Komerční certifikát je použitelný i pro oblast digitálních podpisů (viz otázka 23).

28. Mohu mít na jednom počítači více certifikátů (třeba ostatních členů rodiny)

Ano.

29. Jaký je rozdíl mezi zašifrovanou a podepsanou zprávou?

Primárním účelem podpisu je zajištění nepopiratelnostních funkcí. Primárním účelem zašifrování je zajištění důvěrnostních funkcí. Podle použitých technologií podpisu respektive šifrování může být sekundárně zajištěna i integrita.

30. Co se starým certifikátem?

Přesnější znění otázky by mohlo být - co se starými (vlastními) párovými daty, a co se starými (cizími) certifikáty. Pojmem " starý " rozumíme certifikát s prošlou platností nebo řádně zneplatněný. Pokud již v systému nemáte zprávy nebo data, které byly podepsány privátním klíčem příslušným k danému certifikátu (vlastnímu či cizímu), není nutné ho v systému udržovat. Pokud je tomu naopak, slouží v systému k ověřování. Privátní klíč sloužící k podepisování by jste měli ve vlastním zájmu vždy zničit po ukončení jeho platnosti, aby se snížila možnost jeho kompromitace dlouhodobým skladováním Naprosto jiná situace je u privátního klíče, který sloužil pro šifrovací funkce. Jeho zničením by jste si v prostředí nejběžnějšího poštovního klienta MS Outlooku znepřístupnili veškerou vámi zašifrovanou poštu. Zde je vidět, proč je z bezpečnostního hlediska velmi rizikové používat jedna párová data (populárně řečeno jeden certifikát) jak na podepisování tak na šifrování.

31. K čemu je certifikát certifikační autority?

Certifikát Certifikační autority má několik funkcí:
Jeho instalací na své PC uživatel systému deklaruje důvěru v takovou certifikační autoritu. V praxi to znamená, že pokud uživateli přijde zpráva, která je elektronicky podepsána certifikátem vydaným právě touto certifikační autoritou, je systémem chápán jako důvěryhodný. V ostatních případech se zpráva jeví jako nedůvěryhodná.
Instalace v systému umožňuje, aby uživatel výběrem důvěryhodných certifikačních autorit (a následnou instalací certifikátu certifikační autority) zajistil, že v případě, že obdrží elektronicky podepsanou zprávu, jejíž podpis byl učiněn s využitím certifikátu, který uživatel nepovažuje za důvěryhodný, bude na tuto skutečnost okamžitě upozorněn.

32. Jsou " Elektronický podpis " a Digitální podpis " dva výrazy pro stejnou věc ?

Ne, pokud budeme používat definici elektronického podpisu (dále též EP) uvedenou v platném českém Zákoně o elektronickém podpisu (č. 227/2000 Sb. dále též ZoEP). Definice EP a ZoEP je v § 2 písmeno a) :

Elektronický podpis jsou údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které umožňují ověření totožnosti podepsané osoby ve vztahu k podepsané zprávě.

Z této definice vyplývají zejména tyto skutečnosti :

- účel EP : elektronický podpis je určen k zajištění nepopiratelnosti projevu vůle podepsané (živé) osoby ve vztahu k obsahu podepsaných dat.

- zákon nespecifikuje technologii vytváření EP. Dnes se v praxi převážně používají technologie asymetrických šifer, ale je možné použít i jiné technologie jako např. biometrické metody.

- podpisovatel musí být (obdobně jako u ručního podpisu) pouze živý člověk.

Digitální podpis (dále též DP) v ZoEP definován není, nicméně můžeme jej definovat takto :

Digitální podpis je zobrazení, které datovému souboru pomocí kryptografických algoritmů přiřadí (vypočítá) jiný datový soubor.

Tato definice je maximálně obecná. V reálné (současné) praxi se většinou chápe digitální podpis konkrétněji. Tak pod kryptografickými algoritmy se rozumí některé konkrétní asymetrické šifrovací algoritmy (např. RSA, DSA aj.) většinou ve spolupráci s funkcemi vytvářejícími ze vstupního souboru tzv. otisk (hashovací funkce). Výstupnímu datovému souboru, se také dost často říká digitální podpis. Takto vypočtený výstupní soubor (pro účely této odpovědi jej nazveme DSO jako Digital Signature Output). DSO má (v závislosti na použitých algoritmech) různé užitečné vlastnosti, které jsou za určitých specifikovaných podmínek využitelné i v oblasti elektronického podpisu podle ZoEP.

Pro DP platí :

- účel DP : kromě nepopiratelností služby, které chrání proti tomu, aby podepisující subjekt neprávem popřel některou svou aktivitu se používá i v dalších případech jako je autentizace subjektu, zajištění integrity vstupního souboru, zašifrování vstupního souboru, zašifrování klíče pro jinou šifru, bezpečnou distribuci šifrových klíčů atd.

- DP je spojen s kryptografickými algoritmy asymetrických šifer.

- subjekt vytvářející DP (= podpisovatel) může být kromě fyzické osoby i právnická osoba, počítač (většinou se rozumí server), počítačová aplikace či jiný automat.

Z uvedeného je vidět, že DP a EP se liší v účelu použití, v technologiích i v tom, jaký subjekt je může používat. DP jako technologie může být využit pro vytváření EP (v současnosti je nejpoužívanější technologií pro EP). Rozhodně ovšem termíny EP a DP nejsou synonyma.

Klíčová slova: elektronický podpis, certifikační autorita, důvěrnost, integrita, dostupnost, nepopiratelnost

7 e- kriminalita

7.1 Popis phishingu a jeho kořeny

Phishing reprezentuje krádež citlivé, privátní informace patřící jedinci, jako jsou kompletní údaje o platební kartě (to je nejčastější) nebo odcizení přístupového jména a hesla, s jejichž pomocí lze na dálku manipulovat s financemi. Hlavním problémem phishingu je, že proti němu vlastně *neexistuje univerzální ochrana,* neboť je prováděn s pomocí e-mailů, které vypadají naprosto legitimně a v pořádku – správná adresa odesílatele (na první pohled), veškeré formální náležitosti také splněny, a obsah, který také nevypadá podezřele.

Slovo phishing vzniklo kombinací z fishing (rybaření) a phreaking (= phone hacking, využívání elektroniky k napadení telefonů a získání hovorů zdarma). Česky se někdy překládá jako Rhybaření. Nejtypičtějším současným phishingem je falešný e-mail, tvářící se jako odeslaný z vaší banky v němž banka žádá o ověření totožnosti. Po kliknutí na odkaz je uživatel zaveden na falešnou stránku (která se ovšem tváří, že je v pořádku), kde odevzdá své údaje a následně přijde o peníze.

7.2 Tři cesty Phishingu

V zásadě jsou k rhybaření používány následující tři cesty. První z nich je *varianta sociálního inženýrství*, kdy oběť je nějakou cestou "přesvědčena", aby vydala své logovací údaje (jméno a heslo). Obvykle již přímo v e-mailu je oběť nasměrována, aby se kliknutím na odkaz dostala na podvodnou webovou stránku.

Pojem sociální inženýrství: *Samotný pojem sociálního inženýrství prochází v posledních létech vývojem a v literatuře jsou uváděny různé definice, například* sociální inženýrství je lidská stránka průniku do podnikové sítě. *Pro hackera (útočníka) je často mnohem jednodušší věnovat se lidským slabinám, než se potýkat s technickými aspekty průniku. Sociální inženýrství, slouží-li k získání citlivých informací či neoprávněnému přístupu, se opírá o vytvoření vztahu důvěry s podváděnou stranou. Také Bruce Schneier ve své knize (Secrets & Lies: Digital Security in a Networked World) hovoří o sociálním inženýrství (neboli v jeho pojetí o* sociálně technických útocích*) jako o aspektu souvisejícím výhradně s člověkem a týkajícím se otázek důvěry. Tato důvěra je samozřejmě falešná. Kevin Mitnick (The Art of Deception) jde dále a objasňuje toto chování člověka jeho přirozenou snahu pomoci (a bohužel na tomto základě být snadno podveden). Lidé, nikoli technologie, jsou nejslabším článkem bezpečnostního řetězce.*

Útoky na bázi sociálního inženýrství mohou být prováděny bud přímo osobně nebo telefonicky anebo on-line, tedy libovolným komunikačním prostředkem. V posledních letech navíc fyzické hranice zemí přestávají být v tomto ohledu zábranou. Techniky sociálního inženýrství jsou jednoduché, snadné a velice efektivní. Jejich konkrétní podoby mohou být velice různorodé.

Některé příklady - podvodník se vydává za někoho jiného, podváděná stran je uvedena v omyl, pokud se týká hodnocení aktuální situace a samozřejmě řada technik pro rhybaření. A patří sem i populární Google hacking (http://interval.cz/clanky/google-hacking/). Mnoho lidí si stále neuvědomuje, jaké informace nechávají "viset" na síti a k čemu by mohly být zneužity. Dokonce v tomto směru i obsah odpadkových košů může přinést hodnotné informace. (Kolikrát jste ve filmech viděli, že hrdina se dostal na správnou stopu právě díky odpadkům?)

Druhá využívaná metoda se opírá o *keyloggery*, což jsou programy, které mapují vaše stisky klávesnice a odesílají tyto informace útočníkovi (pochopitelně bez vašeho vědomí). Jak se dostal keylogger na váš počítač? Obvykle pomocí trojského koně, který jste si stáhli z nějakého podezřelého webu, nebo s nějakým "unikátním" softwarem.

Třetí variantou je klasický útok *Man-in-the-Middle*. Útočník funguje jako prostředník mezi vámi a bankou a ani jedna strana netuší nic o jeho přítomnosti. Pokud oprávněný uživatel skončí se svým připojením k bance, podvodník v něm pokračuje a samozřejmě ho využije ke svým cílům. (Pokud se k přesměrování používá hacknuté DNS, hovoříme o pharmaření **pharming**).

Proč toto vše může na internetu fungovat? Vyplývá to z obtížnosti řešení autentizace na internetu. Zatímco postavit z cihel fyzickou napodobeninu banky určitě nebude jednoduchou záležitostí, vybudování falešné internetové identity banky již tak náročné (alespoň v současnosti) zdaleka není.

Je také třeba vzít do úvahy možný rozsah takovéhoto útoku. Podvodník svou falešnou e-mailovou zprávou může díky internetu velice snadno současně oslovit tisíce potenciálních obětí a, bohužel, pár se jich prostě chytí na vějičku. Podle údajů v některých odborných článcích se hovoří o pěti procentech napálených (u některých typů útoků), někde je popisováno dokonce vyšší procento. Například podle výsledků analytické společnosti Gartner z roku 2004 (Litan, A.: Phishing Attack Victims lakely Targets for Identity Theft) v roce 2003 vyústilo předání dat dvou miliónů (!) podvedených uživatelů na falešné webové stránky ve finanční ztrátu o velikosti 1,2 miliardy dolarů.

Lukrativita rhybaření pak pochopitelně vyplývá z profitu, který přináší iniciátorům podvodu. Doba, kdy hackeři na internetu experimentovali převážně jen proto, aby ukázali své dovednosti, jsou již nenávratně pryč. Skutečným motivem je výlučně finanční zisk.

7.2.1 Typy Phishingu

7.2.1.1 Spear phishing

Termín spear phishing (cílený phishing) označuje jakýkoli cílený útok pomocí podvodné nevyžádané pošty. Tvůrci cílené podvodné pošty odešlou zdánlivě pravý e-mail všem zaměstnancům nebo členům v rámci určité společnosti, vládního úřadu nebo jiné skupiny. Zpráva například vypadá, že pochází od vašeho zaměstnavatele nebo od kolegy, který by mohl odeslat e-mail všem osobám v rámci dané společnosti (např. osoba, která spravuje počítačové systémy). Tato zpráva může obsahovat žádost o poskytnutí uživatelských jmen nebo hesel.

Ve skutečnosti jsou však údaje o odesílateli e-mailu zfalšované nebo podvržené. Zatímco klasická podvodná pošta je určena ke krádeži informací od jedinců, cílem podvodů typu spear phishing je získat přístup k celému počítačovému systému určité společnosti. Pokud v odpovědi poskytnete své uživatelské jméno nebo heslo, klepnete na odkazy nebo otevřete přílohy v podvodném e-mailu, automaticky otevíraném okně nebo na webu, můžete se stát obětí krádeže identity a můžete vystavit riziku svého zaměstnavatele nebo danou skupinu.

Označení cílený phishing (spear phishing) lze použít také pro podvody, které se zaměřují na uživatele určitého produktu nebo webu. Autoři nevyžádané pošty se tuto poštu snaží pomocí konkrétních informací co nejvíce přizpůsobit specifické skupině.

7.2.1.2 Mophophishing

Jedna novější varianta rhybaření týkající se uživatelů mobilních telefonů. Jedná se o typ rhybaření, kdy hackeři pošlou falešnou bankovní aplikaci na mobilní telefon klienta banky. Uživatel poté vyplní důvěrné informace pod dojmem, že se přihlašuje ke svému účtu, ale ve skutečnosti zasílá informace hackerovi, který je posléze zneužije ke svému prospěchu.

Jedná se o závažnější variantu phishingu, poněvadž oproti phishingu emailovému zde není možné nahlédnout do zdrojového kódu stránky a ověřit si tak autentičnost odkazů i internetové domény.

7.2.1.3 Google hacking

Google hacking je termín používaný pro nalezení napadnutelné oběti a citlivých dat přes internetový vyhledávač. Google Hacking Database (GHDB) je databáze s dotazy, které na vašem webu odhalí citlivá data. Přestože google blokuje některé známější dotazy používané pro Google hacking, nic nezastaví hackera před procházením vašich stránek a spouštěním dotazů z Google Hacking Databáze přímo na prohledávaný obsah.

Příklad: Na stránce, která byla věrnou kopií stránky Google, podvodníci umístili slib výhry 400 dolarů - jen zašlete detaily vaší kreditní karty...

7.2.1.4 Smart redirection

Jako odpověď na sílící ochranu uživatelů před rhybařením (identifikace a vzápětí likvidace podvodných webů) vymysleli rhybáři nový trik. Útočí pomocí takzvaného rychlého přesměrování, kdy existuje řada podobných podvodných webů a URL ve falešném e-mailu nasměruje klamaného uživatele na speciální IP adresu. Zde umístěný redirektor rychle otestuje, který z podvodných webů ještě funguje, a uživatele tam přesměruje.

Trik byl použit i u "českého" phishingu – útok na City Bank.

7.2.1.5 Phishing bez emailové intervence

Hackeři umístí skript přímo na servery s Microsoft Internet Information Services - skript pak přesměruje zákazníky na podvrženou stránku. Zákazník se standardně přihlásí a dostane se na falešnou stránku, odkud je následně odeslán na jinou stránku, která již požaduje

jeho osobní údaje.

7.2.1.6 VoIP phishing

V poslední době se rozmáhá i takzvaný **VoIP phishing**. Podvodník vám místo e-mailu zatelefonuje, samozřejmě se vydává za zástupce vaší finanční instituce, a nějakou cestou se snaží z vás příslušná data dostat.

Příklad: *Konkrétní příkladem může být například SKY TV. Podvodník orientovaný na předplatitele Sky TV (Velká Británie) se telefonicky vydává za zaměstnance společnosti a tvrdí, že nemáte zaplaceno a vaše předplatné bude zrušeno.*

7.2.2 Ukázky Phishingu

1)


citibank

Serial EM202-16

Vážený kliente Citibank Online®,

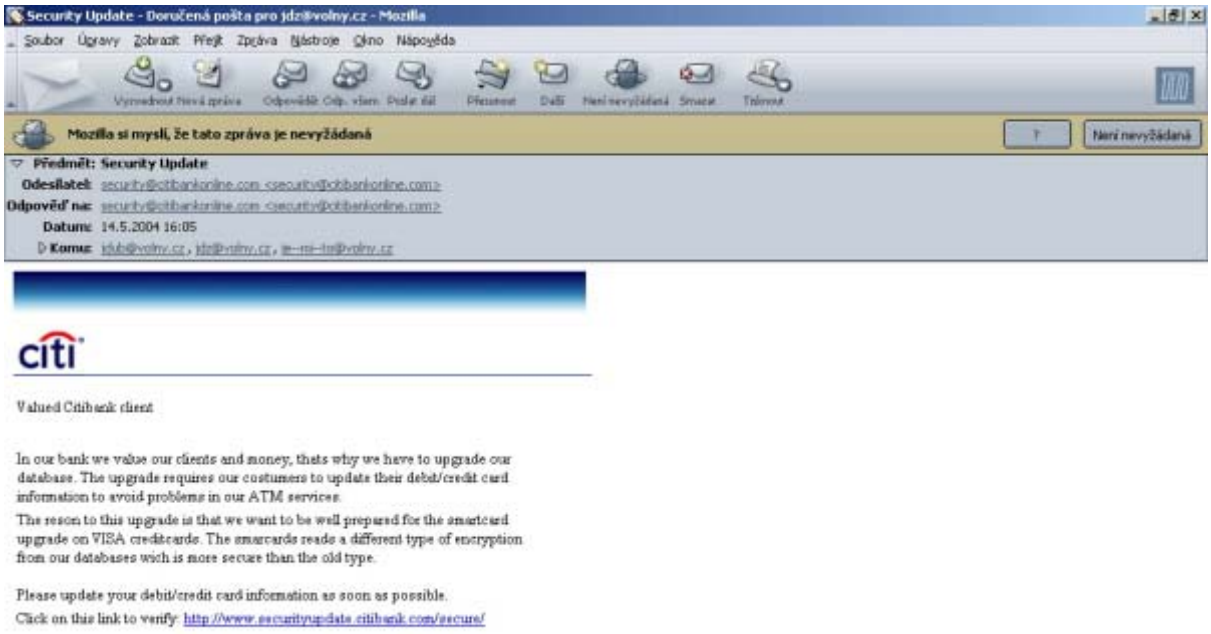
03/02/2006 na Váš běžný účet byl přijat převod v cizí měně na částku ve výši Ł 2000 . Se shodou s *spotřebitelským souhlasem CitiBank® online*, je potřeba potvrdit tento převod pro jeho úspěšné zařazení na Váš běžný účet. **Pro potvrzení platby** Vás prosím o návštěvu programu ovládání Vaším účtem CitiBank® online a dále postupujte podle předloženého návodu. V případě neprijetí potvrzení v průběhu 48 hodin, bude částka vracena odesilateli.

Pro vstup do programu CitiBank® online, **kliknčtc sem** >>>

S pozdravem
Služba CitiBank® Alerting Service

Obrázek 1 Ukázka podvodného emailu

2)



Obrázek 2 Ukázka podvodného emailu

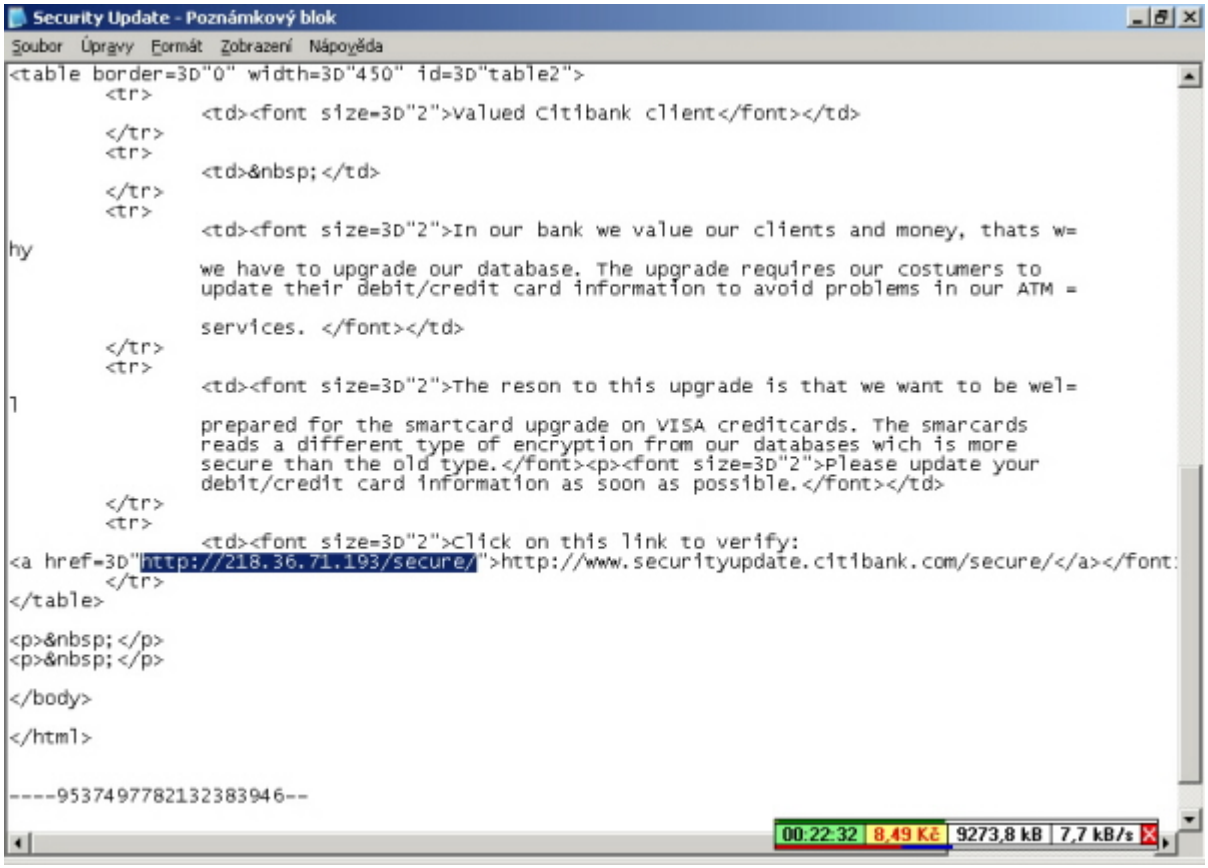
7.3 Analýza podvodu (City bank)

V současné době je již stránka podvodníků zrušena, ale před zrušením stránek se povedlo odborníkům provést dokumentaci celého podvodu a ukázat celý princip podvodu, který je následující:

1) V podvodné zprávě je využito sociální inženýrství, kdy je uživateli vysvětleno, že banka připravuje vylepšení systému a aby se vyhnul případným problémům při použití bankomatu, je dobré bance sdělit určité údaje. Přestože je tato žádost nesmyslná, najde několik důvěřivců, kteří se nachytají - různé statistiky uvádějí 5-8%.

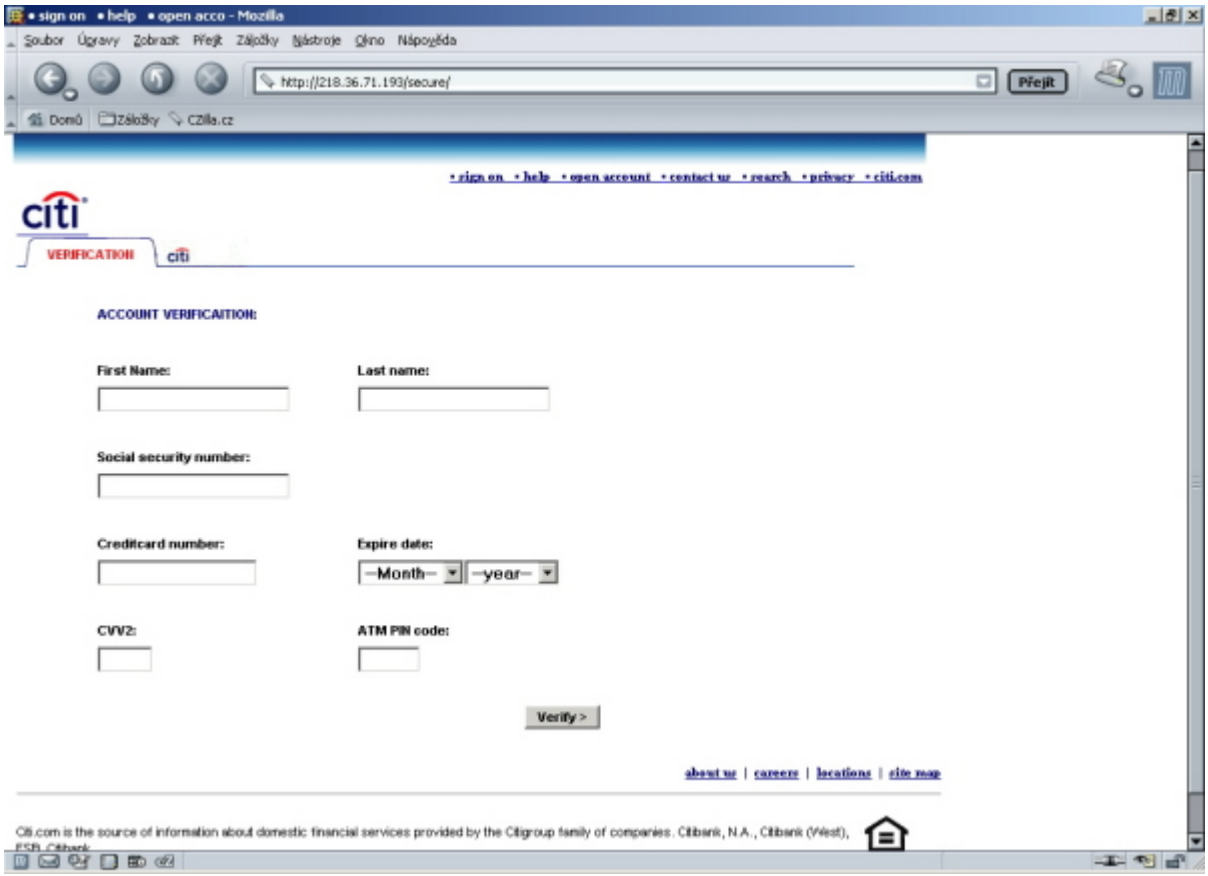
2) V e-mailu je uveden odkaz, na který se má kliknout a tím by měl uživatel vstoupit na stránku banky. Přestože text odkazu v e-mailu vypadá, že uživatel bude přesměrován na server banky, skutečné přesměrování bude provedeno jinam, jak se můžete podívat níže na obrázku. Skutečný (pro uživatele na první pohled neviditelný) příkaz je jiný než odkaz zobrazený v emailu. To samo ještě nic neznamená, protože oba zápisy mohou být správné.

Ale **v tomto případě IP adresa (číselný kód) je jiná než skutečná IP adresa serveru CITIBANK.COM!**

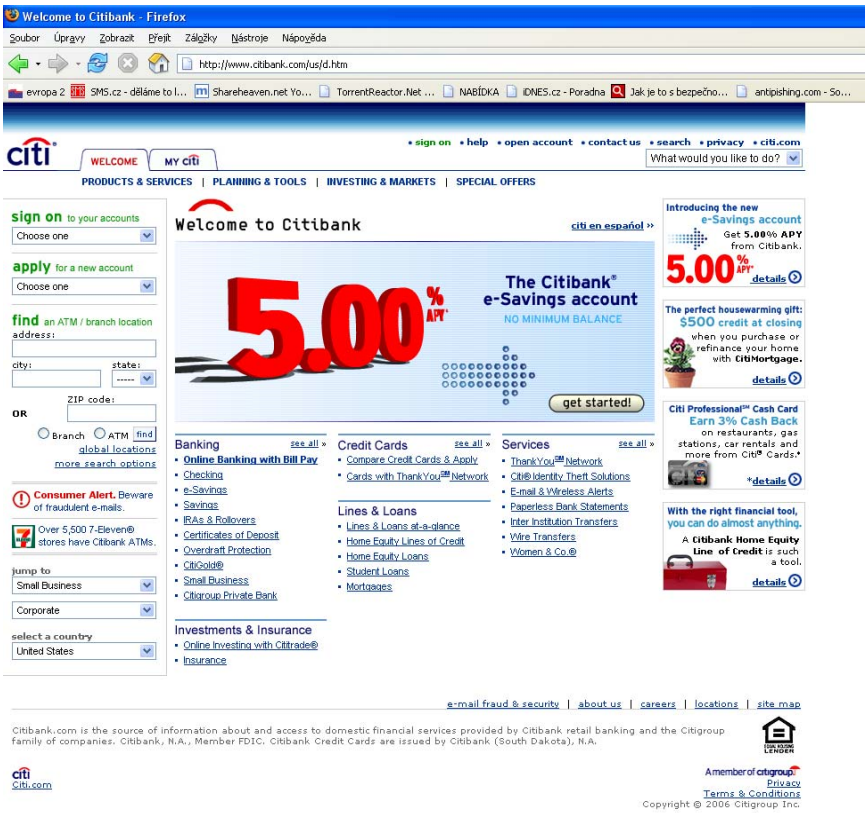


Obrázek 3 Analýza zdrojového kódu

3) Odkaz v e-mailu přesměruje na stránku podvodníků (jej již zrušena). Styl stránky se nápadně podobá originální stránce banky (viz. porovnání níže), proto nepozorný návštěvník si ani nemusí uvědomit, že je na cizím serveru. Po uživateli bylo požadováno, aby ve formuláři vyplnil důvěrné informace o jeho platební kartě. Pak už by podvodníkům nebránilo nic v její zneužití. Někteří si možná všimli, že spojení se serverem je pomocí protokolu http a ne https, jak je u důvěrných informací obvyklé.

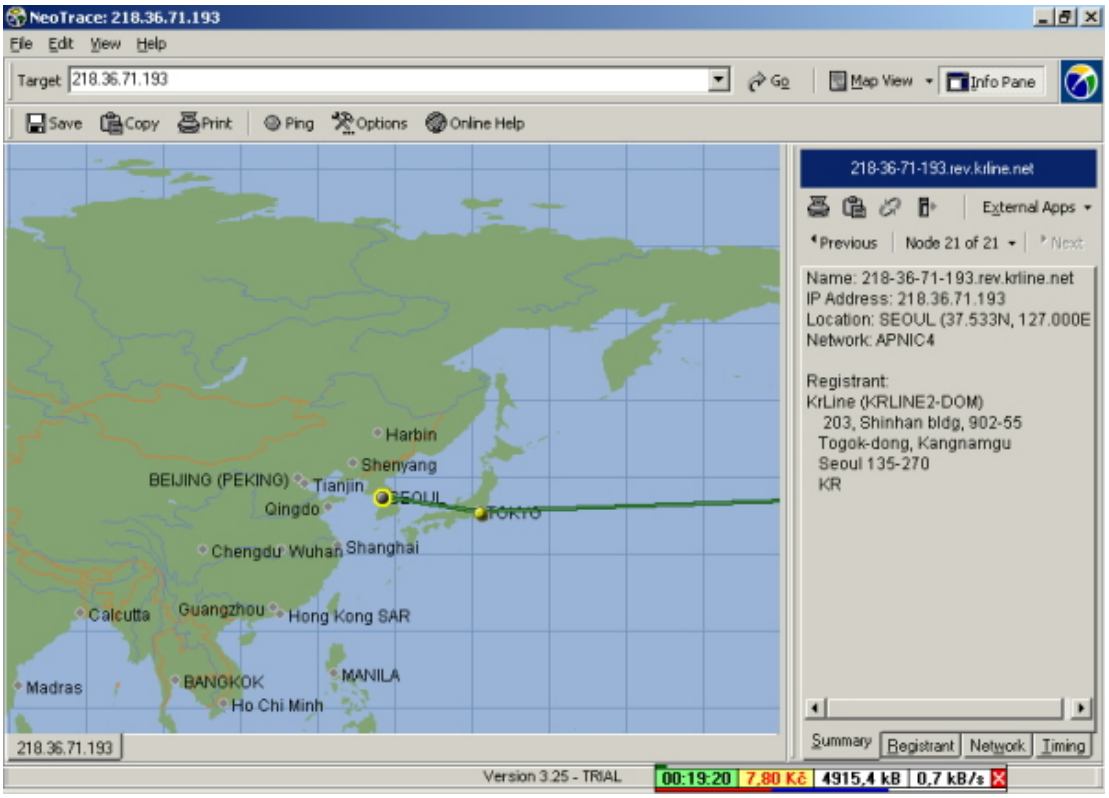


Obrázek 4 Falešná stránka

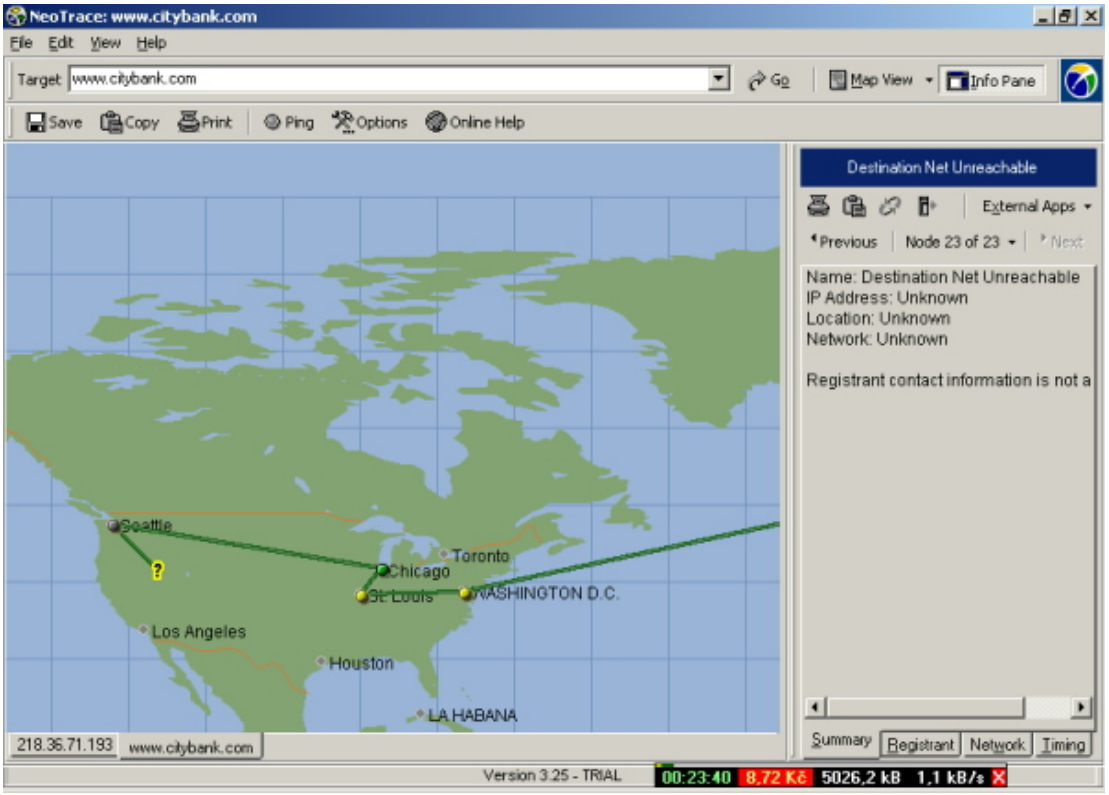


Obrázek 5 Originální stránka banky

4) Pomocí programu Traceroute je možné zjistit umístění obou serverů. Zatímco pravý server CITYBANK.COM se nachází v USA, stránky, kde byly požadovány důvěrné informace byly umístěny na serveru v Koreji.



Obrázek 6 Umístění serveru v Koreji



Obrázek 7 Správný odkaz na citibank.com do USA

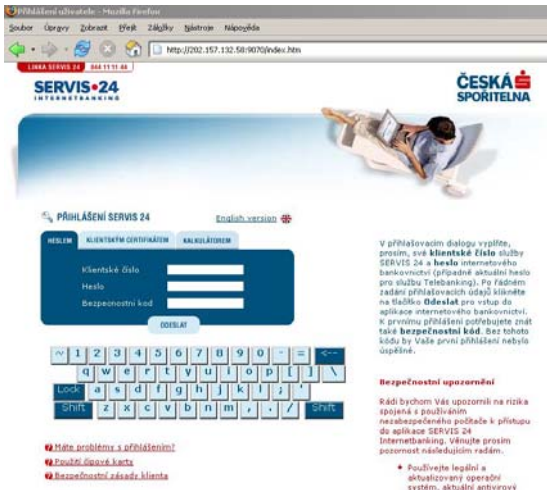
7.4 Analýza podvodu (Česká spořitelna)

http://www.mesec.cz/clanky/klienti-ceske-sporitelny-v-ohrozeni/

10. října 2006 se objevil další český phishing tentokrát útočící na největší českou retailovou banku Českou spořitelnu. Jednalo se o email, kde se odesílatel vydával za zástupce banky a vyzýval k aktivaci nového zabezpečení. Email klienty pobízel k zadání uživatelských jmen a hesel a přihlášení do online aplikace Servis24, kam byl klient přesměrován po kliknutí na odkaz uvedený v emailu.

Odkaz ovšem přesměroval klienty na falešné stránky, které byly velmi vydařenou kopií stránek České spořitelny. Na první pohled tak klient může nabýt dojmu, že je na správné adrese a že se tedy nemá čeho obávat. Přesto lze odhalit řadu rozdílů, podle nichž přesměrování snadno zjistíme:

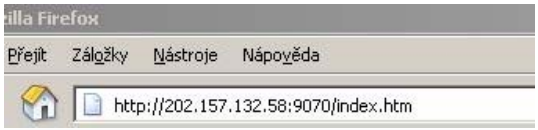
Falešné stránky



Originální stránky

1) Pravé stránky ukazují jméno serveru servis24.cz, falešné jsou nahrazeny číselným odkazem. Za povšimnutí stojí i to, že podvodná adresa běží na nezabezpečeném protokolu http, kdežto pravá adresa na zabezpečeném kanálu https.

Podvodné stránky



Originální stránky

2) Druhý rozdíl je ve funkčnosti. Klienti, kteří využívají virtuální klávesnici, zjistí, že ani tato nefunguje.

3) Nefunguje ani většina odkazů vedoucích ze stránky.

4) Nejdůležitější rozdíl - a zásadní - je v certifikátu stránky. Každá banka má své stránky podepsané certifikátem, ověřeným některou certifikační autoritou (české banky nejčastěji VeriSign - případ i České spořitelny, nebo ICA). Podvodné stránky certifikát nemají žádný.

Poznámka: Některé podvodné stránky si mohou také nechat vystavit certifikát. Proto je u nich důležité zkontrolovat organizaci, pro kterou byl vydán, organizaci, která certifikát vydala, a datum platnosti certifikátu.

7.5 Phishing v praxi

Zajímavé je použití technik „phishermanů“. Aby uspěli, musí odeslat obrovské množství falešných mailů (spamů), což už dnes není příliš snadné, protože velké přijímací (SMTP) servery už dokáží mnoho masových mailingů blokovat. Phisheři nejdříve zavirují tisíce běžných počítačů připojených k internetu; může mezi nimi být i ten váš. Virus, který umí rozesílat maily z daného stroje, zatím spí, a je probuzen právě v okamžiku, kdy phisherman zavelí k masovému mailingu a odešle si svou dávku e-mailů.

Těmto počítačům se říká „botnets“ a počítači, který je hostuje, „zombie machine“. Výhoda botnetu pro útočníka je, že je v tom nevinně – i kdyby jej agenti FBI vypátrali a vyslali zásahovou jednotku, najdou naprosto nevinného člověka, který jen klikl na něco, na co neměl.

Při zadávání osobních údajů je nejobtížnějším problémem pro hackery, jak si poradit s internetovou (webovou) adresou, neboť tu zatím, na rozdíl od e-mailové adresy, nelze padělat. Stále nejčastější postup je, že se padělaná část adresy vyskytuje v levé části URL, tj. např. „www.citibank.com“, a za ní je nepřehledná a dlouhá spleť znaků, přičemž skutečná adresa (nejčastěji jen IP číslo) je až úplně vpravo, kam zrak tak často nezavítá.

To je ale dnes už poněkud naivní trik, na který jen tak někdo neskočí: nejnovější vynález je ale opravdu rafinovaný. Spočívá ve vytvoření malého javascriptového okénka, které nenápadně na stránce vyskočí, zakryje řádku s URL a nahradí ji falešným textem, který už nemůže vzbudit žádné podezření, protože se jedná o „správně napsanou“ adresu. Jedinou obranou uživatele je pak vypnout JavaScript – ale to dělá jen málo osob.

Co se děje s vašimi daty

V okamžiku, kdy má gang vaše údaje, může postupovat několika způsoby. Třeba zkusí po troškách vytáhnout peníze z vaší platební karty – naúčtuje vám neexistující nákupy v

internetových obchodních domech a vaše banka může povolit transfer peněz. Problémem ovšem je, že zde zločinec musí vystoupit z temnot: musí mít účet, na který peníze poputují, musí mít smlouvu s kartářskou společností jako prodejce (*merchant*). Zatímco vlastní phishing se dá provést odkudkoli ze světa.

Toto už dnes prakticky nejde provést se zemí, kde nefungují zákony, protože banky nepřevedou peníze na účty při online nákupech do těchto částí světa. Zločinecký gang, který má v ruce tisíce čísel od platebních karet, musí volit rafinovanější postupy jak tyto peníze vyluxovat, vyprat a odtransportovat.

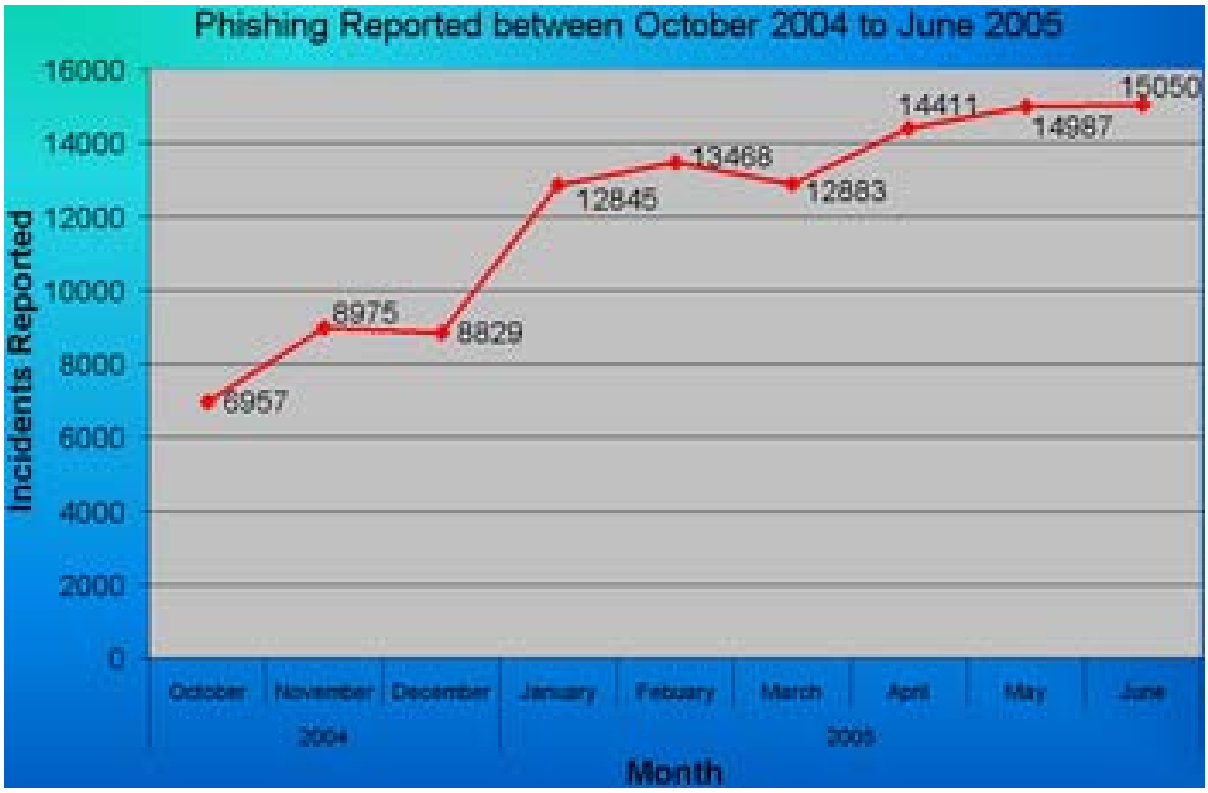
FBI udává, že většina gangů pochází z východní Evropy a zejména z Ruska; ti pak nastrčí své „bílé koně“ do civilizovaných zemí, kde si otevřou řádné účty a internetové obchody, vyinkasují peníze, převedou je a zmizí do podzemí.

Až neuvěřitelně vysoká čísla účinnosti svědčí o tom, v jak masovém měřítku se „phishermanům“ daří klamat lidi. Studie tvrdí, že se na phishing chytne *každý dvacátý oslovený uživatel,* tedy jedná se o pětiprocentní účinnost.

Organizace zabývající se phishingem pak říkají, že se každý den rodí *několik desítek* nových variant útoků – nových pastiček, které někde šikovní psychologové placení kriminálními gangy vymýšlejí. (Řada typických případů je uvedena na www.antipishing.com.) Zatím jde nejčastěji o předstírání identity největších amerických bank (Citibank, Bank One, Fleet atd.), kartářských společností (MasterCard, VISA, AmEx) nebo největších internetových obchodů a platebních služeb (Amazon, eBay, PayPal). Ušetřen nezůstal ani Microsoft. Postupně ale zločinci pokračují k méně známým obchodům a službám, což je nebezpečnější – pokud se uživatel trošku zorientuje, budou mu e-maily od velkých bank a obchodů s žádostí o „ověření osobních informací“ brzy podezřelé, ale maily od specializovaných služeb budou působit věrohodněji.

7.6 Statistické údaje

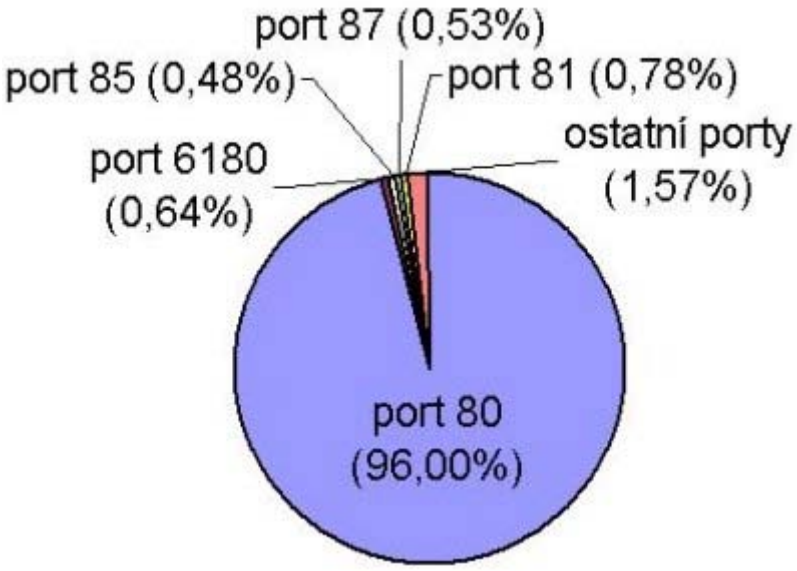
Podle serveru Antiphishing je úspěšnost rhybhářů znepokojivě vysoká – podvést se nechá kolem pěti procent oslovených, přičemž počet rhybholovů rychle stoupá. Zatímco v listopadu loňského roku bylo zaznamenáno necelých 30 unikátních útoků touto metodou, letos v březnu už jich bylo 420 (z toho 110 cílených na eBay, 98 na Citibank a 63 na Paypal).



Obrázek 8 Zvyšování phishing zpráv z října 2004 k červnu 2005.

Počet nahlášených aktivních phishing stránek v březnu 2004	**2870**
Průměrný měsíční nárůst phishing stránek od července 2004 do března 2005	**28 %**
Stát s nejvíce podvrženými phishing stránkami	**USA**
Průměrný počet dní online stavu podvodné stránky	**5,8**
Nejdelší doba online stavu podvodné stránky (dny)	**31**
Počet lidí, kteří se setkali s online phishingem v USA (v milionech)	**57**

Nejčastěji používaným portem, na kterém phishingový server naslouchá, je podle očekávání standardní HTTP port číslo 80, celkově byla procenta rozložena takto:



Oblíbeným cílům útoků s přehledem vévodil finanční sektor, na nějž směřovalo 81 procent všech pokusů o podvod. Jak již první tabulka naznačila, nejvíce podvržených stránek pochází ze Spojených států (více než 34 procent), druhé místo si s dvanácti procenty vysloužila Čína a pomyslná bronzová příčka patří Jižní Koreji (devět procent). Během března bylo zaznamenáno 66 různých zemí s podvrženými stránkami.

7.7 Obrana proti phishingu

http://www.microsoft.com/cze/athome/security/online/phishing_filter.mspx#EQB

Klíčovým nástrojem na ochranu před phishingem je zdravý rozum. Dokonale účinná softwarová ochrana před ním neexistuje a asi ani existovat nemůže. Nicméně jako podpůrný prostředek si můžete nainstalovat například EarthLink Toolbar (www.earthlink.net), který vás mimo jiné upozorní, když vstoupíte na server, který je znám jako podvodný. Ovšem tato ochrana pochopitelně funguje jen na provařené případy, nepomůže u nových útoků.

Dalším obranným nástrojem proti phishingu je použití software Microsoft Phishing Filter, který poskytuje dynamickou ochranu proti phishingu při návštěvě webů dvěma způsoby. Kontroluje a identifikuje podezřelé weby a poskytuje aktualizace a hlášení o známých podvodných serverech. Nástroj Microsoft Phishing Filter je zdarma k dispozici jako doplněk k panelu MSN Search Toolbar a bude také dostupný v příštím prohlížeči Windows Internet Explorer 7.

Tento nástroj Microsoft Phishing Filter spojuje dvě technologie ochrany před podvody typu phishing:

1) **Zabudovaný filtr**, který v navštěvovaných adresách URL a webech kontroluje určité charakteristiky vážící se k phishingu.
2) 2) **Služba online**, která nabízí informace o ohlášených podvodných webech v reálném čase. (Podvodné weby se objevují a mizí v rámci 24 – 48 hodin, proto je důležité aktualizovat informace každou hodinu.)

A jak tento programu pozorní uživatele na výskyt phishingu?

Po instalaci doplňku Microsoft Phishing Filter do panelu MSN Search Toolbar, bude každý navštívený web ověřen a zkontrolován, zda nemá podezřelé vlastnosti, a bude automaticky ověřeno, zda se nejedná o známý podvodný web.

Pokud přejdete na podezřelý web, který by mohl být podvodný, zobrazí se žluté upozornění.

Když se pokusíte navštívit známý podvodný web, zobrazí se červené upozornění a dojde ke znemožnění zadání jakýchkoliv informací do jakéhokoliv formuláře na webu.

Pokud vám i přes použití těchto či jakýchkoliv jiných programů chránících proti phishingu nějaký podobný email přijde, doporučuje se postupovat následovně:

Na nic neklikat! Odkazy v podvodných e-mailových zprávách vás často zavedou přímo na falešné weby, kde můžete bezděčně předat podvodníkům své osobní nebo finanční údaje. Neklepejte na odkazy v e-mailové zprávě, pokud si nejste jisti cílovou adresou.

1. Přemýšlet! Posoudit reálnost popisované situace, všímat si případných odchylek od vzhledu či obsahových prvků, které dopisy od dané instituce obvykle mívají.

2. Pokud máme pocit, že by dopis mohl být reálný, podívat se do rhybhařského archivu (www.antiphishing.org) jestli tam dotyčný dopis již není zdokumentován.

3. Pokud máme ještě pořád pocit, že by dopis mohl být reálný, ověřit si jej u instituce, která jej údajně odeslala. Samozřejmě nepoužívat žádné kontaktní informace uvedené v dopise, ale obrátit se na kontakt, který pro komunikaci s dotyčnou institucí obvykle používáme a máme ověřen.

Uživatel musí být opatrný a nejlépe *odmítat jakýkoli e-mail, který jej nutí na něco kliknout.* Samozřejmostí je kvalitní antivirus, neboť jednou z dalších variant phishingu je instalace programu (viru), který zaznamenává a odesílá vše, co napíšete na klávesnici (tedy i čísla karet a hesla). Přes veškerou a zlepšující se snahu policie i napadaných institucí se dnes jako jediná téměř absolutní ochrana jeví zavedení systému, který bude *ověřovat pravost obdrženého e-mailu.* Vestavba v e-mailovém klientovi nalezne v e-mailu ověřovací kód, bude kontaktovat zdroj a provede ověření; následně uživateli sdělí, zda je odesílatel (uvedený v hlavičce) pravdivý nebo ne a vypíše jeho jméno.
Experti se shodují v tom, že zavedení takovéhoto systému by současný phishing prakticky zlikvidovalo. Je ale náročné, vyžaduje vytvoření a schválení standardů i technickou realizaci systému a následně pak ochotnou a dobrovolnou spolupráci milionů uživatelů. Vytvoření a zavedení tohoto systému je tedy pracné po všech stránkách a zavede do práce s e-mailem další proceduru, ale experti se shodují, že je to zřejmě nevyhnutelné a jediné účinné řešení.

7.8 Pharming

Termín „pharming“ označuje činnost, kterou kriminální hackeři přesměrovávají internetovou komunikaci z jedné webové stránky na jinou, stejně vypadající stránku s cílem oklamat vás tak, abyste zadali své uživatelské jméno a heslo do databáze na jejich falešné stránce. Častými cíly těchto útoků jsou bankovní a finanční stránky. Zde se zločinci snaží získat osobní informace, aby měli přístup k vašemu bankovnímu účtu, mohli ukrást vaši identitu nebo provést jiné druhy podvodů pod vaším jménem.

Pharming, používání falešných webových stránek, může vypadat podobně jako podvod zvaný phishing, ale pharming je mnohem zákeřnější, protože můžete být přesměrováni na falešnou stránku bez jakékoliv vaší účasti nebo vědomí.

7.8.1 Principy pharmingu

Namísto toho, aby útočník čekal, než nepozorný uživatel klikne na odkaz v e-mailové zprávě, pokouší se zaútočit přímo na internetový prohlížeč či DNS záznamy. Jestliže si i zadáme do prohlížeče správnou adresu, trójsky kůň, „červ“ nebo jiný „nástroj“ přesměruje náš požadavek na server, kde může zachytit citlivé informace - jméno, heslo, číslo kreditní karty a podobně. Jinou možností, jak se útočníkovi podaří stejný výsledek, je útok na DNS.

Pharming využívá ke své činnosti překladu jména serveru na odpovídající IP adresu, útočí tedy na DNS (Domain Name System). Pokud pak uživatel ve svém internetovém prohlížeči zadá adresu například www.inetbanka.cz, nedojde k překladu na odpovídající IP adresu, nýbrž na nějakou jinou, podvrženou. Pokud se útočníkovi podaří změnit DNS záznam výše zmiňované imaginární banky www.inetbanka.com, přesměruje se komunikace na jiný stroj, jiné stránky, které však na první pohled nelze rozpoznat od originálu. Nic netušící uživatel tedy zadá požadované přihlašovací údaje a bez větších překážek jimi obdaruje útočníka.

Pharming lze s trochou "štěstí" provést také lokálně modifikací souboru hosts a případným vytvořením podvržené WWW stránky. Zmiňovaný soubor hosts můžete pod operačním systémem Windows nalézt v adresáři C:\WINDIR\system32driversetc, kde \WINDIR\ je instalační adresář Windows. Hosts může obsahovat například tyto údaje:

IP adresa	název
127.0.0.1	localhost
81.31.5.18	www.lupa.cz

Pokud uživatel zadá ve svém webovém prohlížeči URL www.lupa.cz, pak bude přesně podle údaje v souboru hosts kontaktován stroj s adresou 81.31.5.18. Pharming spočívající v modifikaci souboru hosts by pak mohl vypadat takto:

1. Útočník si vytvoří na první pohled identickou kopii stránek www.inetbanka.com, díky které bude po nic netušícím uživateli požadovat zadání citlivých údajů o jeho osobě.

2. Tyto podvodné stránky umístí například na stroj s IP adresou 111.222.33.44.

3. Přidá do souboru hosts na vybraném počítači řádek s falešnou IP adresou a doménou:

IP adresa	název
127.0.0.1	localhost
81.31.5.18	www.lupa.cz
111.222.33.44.	www.inetbanka.com

4. Čeká, až se oběť přihlásí ke "svému" účtu na adrese www.inetbanka.com.

Přístup do souboru hosts na vzdáleném počítači může útočník získat například použitím trojského koně, kterého předtím uživateli podstrčil.

7.8.2 Příklady pharmingu

Příkladem mohou být nedávné incidenty , když se objevili první náznaky nových útoků. Uživatelé serverů Google a Amazon stěžovali na neustále přesměrováni na „Med Network“ – online obchod s léčivy. Postižení byli uživatelé na různých platformách - operačních systémech: Windows, Mac OS, UNIX či prohlížečích: Internet Explorer, Netscape, Firefox a Opera. Na napadených počítačích se nenašli žádné viry, ani spyware.

Jiným příkladem je červ Banker AJ, který se pokoušel ukradnout přihlašovací informace na bankovních portálech. Na začátku tohoto roku se objevil útok na server internetového providera Panix.com, kdy došlo k přepisu DNS záznamů a vlastnictví domény panix bylo bez vědomí jeho vlastníka přesunuté do Austrálie, DNS záznam do Velké Británie a emaily přesměrované na jinou společnost v Kanadě. Panix v souvislosti s tímto incidentem vydal varování pro svoje zákazníky, že pachatelé mohli zachytit jejich přihlašovací údaje. Podobně MasterCard International taktéž uvádí na svých stránkách informace o více než deseti útocích za poslední měsíce.

7.8.3 Obrana proti pharmingu

I přesto, že náš počítač je vybavený nejnovějším antivirovým programem, firewallem a nástrojem proti spyware, těžko se ubráníme přesměrování na falešnou webovou adresu, pokud bude například napadený DNS záznam. Jestliže bychom ale měli informaci o tom, že stránka, na které se nacházíme, má IP adresu registrovanou v „podezřelé krajině“, případně dostali informaci od jiných uživatelů, že daná stránka je zneužitá na kriminální činnost, mohli bychom se účinněji bránit. Nástroj, který nám takovéto informace může poskytnout, je například Netcraft Toolbar. Při použití této aplikace se u každé zobrazované stránky vypíší doplňující informace - např. země, do které navštívená adresa náleží, nebo hodnocení jiných uživatelů. S Netcraft Toolbar se zvyšují vaše šance na odhalení snah o phishing a pharming, případně rovnou můžete nějaký nově odhalený podvodnický server udat. Pomoci v ochraně proti pharmingu by nám měli také samotní výrobci software a poskytovatelé webových služeb. Ochrana by měla spočívat v lepším zabezpečení internetových prohlížečů, vývoji nových autentifikačních protokolů, či použitím tzv. „multi-faktor“ autentifikace. Proti tomuto způsobu se můžete bránit kvalitním antivirovým systémem a jeho pravidelnou aktualizací. Cestu za úspěchem útočníkovi dále může ztížit správně nakonfigurovaný firewall, nicméně obrana proti

pharmingu není v globále vůbec jednoduchá. Jako reakci na sofistikované bankovní podvody připravily všechny banky novinky (2006) pro zvýšení zabezpečení internetového bankovnictví. Následující tabulka uvádí novinky 5 největších bank, operujících na českém trhu:

Zabezpečení internetového bankovnictví pěti největších bank

GRAFIKA: HN, HOTO: HN - ALEŠ MASNER ZDROJ: BANKY

zdroj: www.ihned.cz

8 Obchodování na Internetu

Význam fenoménu e-business lze demonstrovat na společném prohlášení EU a USA o elektronickém obchodu z 5. října 1997, které obsahuje nové přístupy:

- Globální elektronický obchod se stane významným motorem světového hospodářství v 21. století.
- E-commerce nabídne nová pracovní místa a nové příležitosti pro podniky ve všech částech světa.
- Malé a střední firmy budou schopné bez značných nákladů podnikat v celosvětovém měřítku s širokým sortimentem zboží a služeb.
- E-commerce zvýší produktivitu ve všech sektorech ekonomiky, vzniknou nové sektory, nové formy marketinku a prodeje.
- Vyšší míra globální konkurence (tj. s firmami různé velikosti, při vynaložení malých nákladů) přinese větší výběr spotřebitelům a tak povzbudí hospodářskou aktivitu a inovace
-

Zadáme-li do portálů seznam.cz nebo google.com heslo *elektronický obchod,* dostaneme řádově tisíce firem, které nabízení nejrůznější zboží , služby a technologie k elektronickému obchodování. Souvisí to se skutečností, že internetové obchody mají v současné době druhý největší obrat v ČR po řetězcích hypermarketů a ČR je součástí globálních sítí.

K výhodám nakupování na Internetu patří:

- nižší ceny než v "kamenných obchodech" a nakupování z pohodlí domova nebo kanceláře
- 24 hodin denně
- variantní možnosti platby: bankou, na dobírku, hotově při dodávce kurýrem, na splátky
- dovoz zboží až do domu nebo kanceláře často bezplatně
- aktuální slevy akce a výprodeje
- anonymita podle přání zákazníka

V současné době **není elektronický obchod** jako takový **upraven** žádnou **právní normou**. Nové a připravované zákony s obchodním stykem v elektronické podobě počítají; zatím neexistuje ucelená právní norma, která by upravovala na jednom místě práva a povinnosti spojené s elektronických obchodem. Odborníci na legislativu diskutují vlastní právní podstatu internetu. **Internet** není **ani hmotným předmětem**, **ani** čistě **nehmotným statkem**, tj. právem nebo jinou majetkovou hodnotou. Proto také podřazení určitých na internetu uskutečněných jednání pod některou "klasickým právem" definovanou oblast bývá někdy značně obtížné. Obecně však lze říci, že k zajištění náležité ochrany subjektivních práv a zákonem chráněných zájmů ve většině případů postačí důsledně a jednotně aplikovat stávající právní předpisy. Jediným problémem v takovýchto případech může být dosud chybějící rozhodovací pravomoc soudů, která by do jisté míry stanovila standardizované řešení na internetu vznikajících modelových situací.

Komise OSN pro mezinárodní obchodní právo (**UNCITRAL**) připravila tzv. **modelový zákon o elektronickém obchodu**; tento modelový zákon zatím není závaznou právní normou.

Jedna z možných klasifikací elektronického obchodu je segmentace na

A) B2B - Business to Business

Tento druh elektronického obchodování se používá v distribučních a prodejních sítích, ve kterých mohou mezi sebou komunikovat výrobci, pobočky, distributoři, velkoobchody, dealeři nebo obchodní zástupci. Základní rozdíl mezi tímto druhem elektronického obchodu a internetovým obchodem typu B2C (business-to-consumer) je v tom, že **prodávající** (výrobce, distributor, velkoobchod, apod.) **zná předem nakupujícího**. Většinou se jedná o partnera, který má předem stanoveny obchodní podmínky, za kterých může nakupovat. Klasickým příklade elektronického obchodu B2B jsou elektronická tržiště, na která mají přístup pouze registrovaní účastníci. Někteří velcí odběratelé organizují takováto tržiště formou dražby, kdy za minimálních nákladů se během relativně krátkého času shromáždí velké množství nabídek.

B) B2C - Business to Consumer

Tento druh elektronického obchodování je zaměřen na prodej koncovým zákazníkům - spotřebitelům. Je to vlastně obdoba klasického "kamenného" obchodu na Internetu. Internetový obchod disponuje oproti klasickému obchodu řadou výhod . Je známé jméno každého nakupujícího včetně jeho adresy - to je pro běžný obchod obrovský průlom s důsledky pro koncipování nabídky a marketingu a individuálního přístupu ke každému zákazníkovi.

Ke standardním modelům pro elektronické obchodování patří:

Elektronický obchod (e-shop)

- online marketing firmy nebo obchodu
- v prvním případě jde o marketing organizace a jejího zboží nebo služeb s možností objednávat, příp. i platit (často kombinováno s tradičními marketingovými kanály)
- prvotním cílem je zvýšit poptávku, mezi další cíle patří redukce nákladů na prodej a marketing, je to levná cesta k prezentaci na globálním trhu
- zisky se očekávají ze snížených nákladů, zvýšení obratu, příp. z reklamy

Elektronická burza (e-procurement)

- online nabídky a zprostředkování zboží a služeb
- typicky provozované velkými podniky nebo veřejnými institucemi
- hledání dalších dodavatelů a redukce nákladů na nabídku (např. specifikace nabídek mohou být stahovány dodavateli na místo zasílání poštou), může být rozšířeno o online formu vyjednávání, uzavření smlouvy a spolupráci prostřednictvím online média
- jako hlavní zdroj zisku se očekává snížení nákladů (na zpracování nabídek a na získání lepších nabídek za minimálně srovnatelné náklady)

Elektronické obchodní centrum (e-mall)

- soustava elektronických obchodů pod společným zastřešením např. zavedené značky
- může být rozšířeno o obecně garantovanou metodu online placení

- při specializaci na určitý segment trhu se pak takové obchodní centrum stává centrem pro celé odvětví
- přidanou hodnotou mohou být služby nebo vlastnosti virtuálního společenství (diskusní fóra, uzavřené uživatelské skupiny, FAQ - seznam často kladených otázek apod.)
- příjmy se očekávají ze členských poplatků, z reklamy, příp. z provize za transakci (pokud jsou platby prováděny prostřednictvím obchodního centra)

Trh třetí strany (3rd party marketplace)

- rozvíjející se model vhodný pro organizace, které dávají přednost outsourcingu online marketingových operací (jako doplněk k tradičním marketingovým kanálům)
- ve své základní podobě se jedná o uživatelské rozhraní ke katalogu produktů nebo služeb, které může být dále rozšířeno o speciální služby typu propagace obchodní značky, online platby, logistiku, objednávky, příp. komplexní službu zahrnující i bezpečné transakce
- příkladem představujícím obchodní vztah firma-koncový zákazník může být marketing jedné akce (např. konference) zaštítěný dobře známou firmou v daném oboru, poskytovatelé připojení mohou použít tento model pro obchodní vztahy firma-firma a využít tak schopnosti tvorby WWW služeb
- příjmy mohou být generovány na základě členských poplatků, poplatků za služby nebo provizí z hodnoty uskutečněné transakce

Virtuální společenství (virtual communities)

- základní hodnota je vytvářena členy daného společenství (zákazníky nebo partnery), kteří přidávají svoje informace do základního prostředí, které garantuje poskytovatel
- příjmy mohou plynout ze členských poplatků nebo z reklamy
- virtuální společenství může být důležitým doplňkem ostatním marketingovým aktivitám v rámci budování důvěry u zákazníků a zajišťování zpětné vazby

Poskytovatel služeb hodnotového řetězce (value chain service provider)

- specializace na některou z funkcí hodnotového řetězce (např. platby nebo logistika) se záměrem získat tímto odlišením konkurenční výhodu
- klasickým příkladem byly vždy banky, které mohou nyní nalézt nové příležitosti
- nové přístupy se objevují v řízení výroby nebo ve skladovém hospodářství
- zisky mohou být založeny na poplatcích nebo procentním podílu

Integrátor hodnotového řetězce (value chain integrator)

- zaměřuje se na integraci více kroků hodnotového řetězce a na potenciál zhodnocení informačních toků mezi těmito kroky jako další přidanou hodnotu
- zisky mohou plynout z poplatků za konzultační činnost nebo za transakci

Kooperativní prostředí (collaboration platform)

- soustava nástrojů a informační prostředí pro kooperaci mezi firmami

- může být zaměřeno na určité funkce, jako je např. společné navrhování nebo projektování
- obchodní příležitosti lze najít v managementu celé služby (za členské nebo uživatelské poplatky) a v prodeji (licencí) speciálních nástrojů (např. pro návrh, workflow, řízení oběhu dokumentů aj.)

Informační broker a další služby (informationbrokerage and other services)

- objevuje se celá řada nových služeb přidávající hodnotu k množství dat, které se nacházejí na otevřených sítích nebo které pocházejí z integrovaných obchodních operací, jako je sestavování profilu zákazníka, burza obchodních příležitostí, investiční poradenství apod.
- informace a poradenství musejí být obvykle placené přímo buď na základě "předplacení" nebo platby za užití, další možností je využití reklamy
- zvláštní kategorií jsou služby poskytované certifikačními autoritami a elektronickými notáři nebo jinou důvěryhodnou třetí stranou
- zdrojem příjmu mohou být předplatitelské poplatky kombinované platbou za užití nebo prodej software či konzultační činnost

Celý segment je regulován v ČR mj. následujícími právními normami:

- Vyhláška č. 442/2006 Sb., kterou se stanoví struktura informací zveřejňovaných o povinném subjektu způsobem umožňujícím dálkový přístup
- Vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb
- Vyhláška č. 326/2006 Sb., o atestačním řízení pro elektronické nástroje
- Nařízení vlády č. 173/2006 Sb., o zásadách stanovení úhrad a licenčních odměn za poskytování informací podle zákona o svobodném přístupu k informacím
- Zákon č. 106/1999 Sb., o svobodném přístupu k informacím
- Zákon č. 127/2005 Sb. o elektronických komunikacích
- Nařízení vlády č. 100/2005, kterým se mění nařízení vlády č. 140/2000 Sb. a č. 469/2000 Sb.
- Zákon č. 480/2004 Sb., o některých službách informační společnosti
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy
- Zákon č. 95/2005 Sb., kterým se mění zákon č. 29/2000 Sb., o poštovních službách
- Zákon č. 29/2000 Sb., o poštovních službách
- Poštovní podmínky České pošty, s.p.
- Novela zákona č. 227/2000 Sb., o elektronickém podpisu
- Nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb., o

elektronickém podpisu a o změně některých dalších zákonů

- Vyhláška č. 496/2004 Sb. k elektronickým podatelnám
- Novela Nařízení vlády o Obchodním věstníku

Novou organizací je v tomto segmentu Asociace pro elektronickou komerci (APEK).

V době založení APEK byla internetová ekonomika v ČR obecně neznámým pojmem, a proto byla Asociace v roce 1998 založena za účelem podpory e-komerčních aktivit v prostředí českého Internetu a to formou standardizační, popularizační a výchovné činnosti, s jejíž pomocí měla napomáhat kultivovat a rozvíjet tuto novou oblast podnikání.
Cíle, které si Asociace pro elektronickou komerci na počátku svého vzniku určila, naplňuje především, jako nezisková organizace, veřejnými projekty.

V oblasti standardizace je úspěšně provozován projekt certifikace **APEK Certifikovaný obchod** *(původní název do roku 2004 Nákup bez obav). Tento jeden z nejstarších projektů Asociace je součástí vládního programu Česká kvalita, který podporuje poskytování kvalitních služeb v České republice. Cílem projektu certifikace je zvýšit důvěryhodnost elektronických obchodů v očích spotřebitelů, zároveň poskytnout zpětnou vazbu obchodníkům, a pochopitelně aplikovat nová zákonná ustanovení v podmínkách internetového trhu.*

Samotný certifikační proces je prováděn na základě exaktně stanovených Certifikačních pravidel, která jsou vytvořena Asociací, základem pro stanovení těchto pravidel se staly platné zákony – zejména Směrnice Evropského parlamentu a Rady o elektronickém obchodu, Směrnice o prodej na dálku, občanský zákoník, zákon o ochraně spotřebitele – stávající pravidla APEK a certifikační pravidla zemí EU.
Tento projekt na sebe upoutal pozornost českých i zahraničních médií, zároveň značně zvýšil zájem o členství v APEK a aktivní účast podnikatelských subjektů na rozvoji a zkvalitňování e-komerce v ČR.

Dalším neméně zajímavým projektem je ***Bezpecnynakup.cz*** , který od března 2005 prezentuje způsoby bezpečného nakupování a placení na Internetu. Jedná se o výukový projekt, který zábavnou formou učí uživatele internetu, jak bezpečně a bez obav nakupovat na internetu. Výukový server provádí návštěvníky nákupem v internetovém obchodě v jednotlivých fázích a popisuje základní pravidla, která platí při nákupu na internetu. Tento projekt se v březnu 2005, kdy byl zahájen, setkal s unikátním ohlasem 50 000 návštěvníků v tomto měsíci. Server je i nadále provozován a je jedním z nástrojů edukační činnosti Asociace.

Projektem, který se zaměřuje pouze na členy Asociace a odbornou veřejnost, tedy nikoli na koncové zákazníky, je E-business Fórum. Do tohoto projektu pořádaným Tuesday Business Network se APEK zapojil v roce 2006. Jedna se o série diskuzních večerů s vybranými osobnostmi nad tématy elektronického obchodu. Účastníci setkání si při těchto příležitostech vyměňují zkušenosti a prezentují úspěšné i neúspěšné příklady z praxe.

Na počátcích vzniku Asociace tvořilo členskou základnu pár internetových obchodníků a firem, které podnikaly na internetu. Postupem času se členy staly i subjekty obdobného zaměření, které mají za cíl podílet se na rozvoji elektronického nakupování, jedná se především o softwarové společnosti a finanční instituce.

V současné době mezi členy Asociace patří největší české internetové obchody, přední softwarové společnosti a finanční instituce.

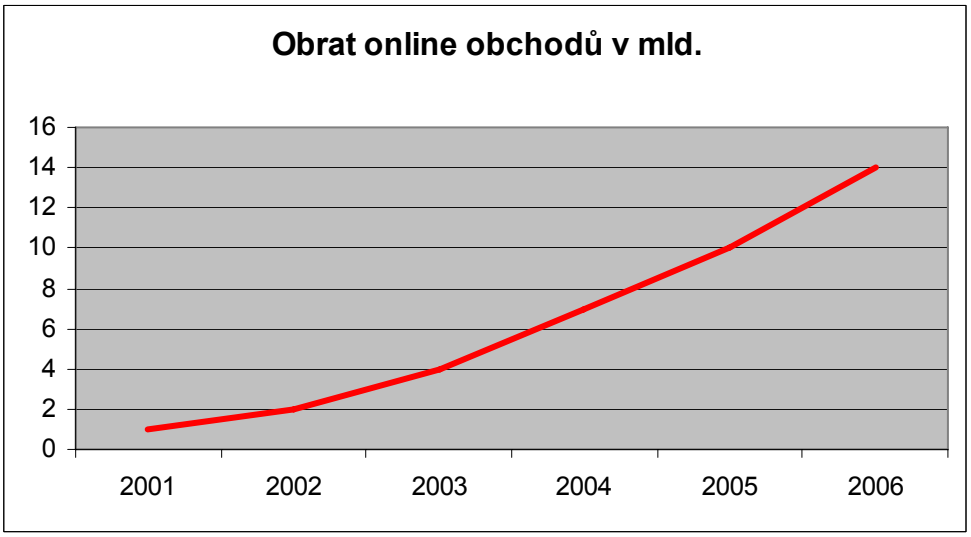
Podle názorů analytiků celý segment elektronické komerce zažívá nebývalou konjunkturu. Agentura Forrester Research signalizuje, že v roce 2006 obrat obchodů přes internet překročí v Evropě sto miliard Euro. V České republice podle dalších údajů Asociace pro elektronickou komerci v roce 2006 v Internetu proběhnou transakce za 14 miliard korun, což představuje nárůst v porovnání s předešlým rokem o čtyřicet procent. K největším hráčům na českém trhu patří firmy Internet Mall (v roce 2006 očekává tržby výrazně přes miliardu CZK), Vltava Stores, Eurocomm Group, Internetshops a Quelle.

Internet Mall je nákupní galerie, sdružující pod jednou střechou specializované obchody, které kromě vlastního prodeje nabízejí svým zákazníkům i kompetentní odborné poradenství a široký repertoár doplňkových služeb.
Internet Mall a obchody bilezbozi.cz, mp3store.cz, fotoexpert.cz, audioexpert.cz, videoexpert.cz, pcexpert.cz, pneuexpert.cz, mobilka.cz, showpark.cz, sekacky.cz, hobbyexpert.cz, ostrovpokladu.cz, zařízeno.cz, bartsport.cz, levnastavba.cz, gameson.cz, last.cz, happyanimals.cz, mimina.cz, joy.cz, cykloexpert.cz a chrono.cz jsou provozovány společností Internet Mall, a.s.
Společnost Vltava Stores, a.s. je provozovatelem předních českých internetových obchodů Cybex.cz, Vltava.cz, ElectroHall.cz, MusicKatalog.cz a aukčního serveru Aukce.cz. Zároveň je jediným společníkem slovenské společnosti CP Internet, s.r.o., provozujícím jeden z největších internetových obchodů na Slovensku - Dunaj.sk.
Ve svých obchodech společnost nabízí nejširší nabídku zboží a služeb - knihy, hudbu, film, elektroniku, domácí spotřebiče, počítačovou techniku, digitální fotoaparáty, mobilní telefony, programové vybavení, hry a hračky, potřeby pro kutily, zahrádkáře a chovatele zvířat, produkty pro zdraví a kondici nebo také zájezdy a rekreační pobyty. Vltava Stores vyvíjí stálé úsilí o další zkvalitňování a rozšiřování nabídky. V současné době obsahuje nabídka zboží a služeb víc jak milion položek. V roce 2005 společnost dosáhla obratu 417 milionů korun a zaznamenala meziroční nárůst obratu 52%. Tím se zařazuje mezi obchodníky s největší dynamikou na českém retailovém trhu vůbec. Obchody Vltava Stores registrují v součtu cca 420 tisíc zákazníků, průměrný měsíční přírůstek nových zákazníků je cca 9 tisíc.
Cílem společnosti je vybudování stabilní a dominantní značky Vltava Stores na českém internetovém trhu. Základním posláním je být tradičním, solidním a důvěryhodným partnerem pro své zákazníky a obchodní přátele a napomáhat tak dalšímu rozvoji internetového obchodování na českém trhu.
Opírá se přitom o své zkušenosti - 10 let tradice a stability nejstaršího internetového obchodu na českém trhu Vltava.cz, dynamiku vývoje – obchod Cybex zaznamenal v roce 2005 meziroční nárůst 77%, širokou nabídku zboží a služeb a také o nový kapitál, který do společnosti vstoupil s investičními fondy v roce 2005.

Zakoupené zboží mohou zákazníci do čtrnácti dnů bez udání důvodů vrátit. I když způsob platby na dobírku v ČR zatím dominuje, je rovněž možné platit bankovním převodem,on-line kreditní kartou či přímo na pobočkách prodejců.
V roce 2005 tvořil internetový obchod 1,7 % z celkového maloobchodního prodeje v ČR (údaje bez započítaní prodeje aut do maloobchodu). Český trh má ve střední Evropě značný náskok oproti ostatním zemím (Slovensko, Maďarsko, Polsko, Pobaltí, atd.). Lze tedy předpokládat, že silné české obchody se budou snažit získat i tyto trhy, případně částečný podíl na trhu

v západní Evropě, odkud je možno za zajímavých podmínek dovážet část sortimentu. Obecně pak je možné říci, že stále více zákazníků bude nakupovat po internetu stále širší sortiment zboží. Internetovému nakupování v podstatě nahrává přirozený vývoj internetu, který se stává normální součástí života většiny obyvatel. Celkově vzato trh se vyvíjí směrem, kde i klasické kamenné obchody spouští internetové obchody jako doplňky svých poboček (příklady budiž Electroworld a Datart v posledním roce). To samé platí ovšem i například o malých obchodnících nebo živnostnících, nabízejí-li jakýkoliv produkt či službu, snaží se svou nabídku prezentovat i na Internetu. Stále se jedná o nejlevnější formu propagace s nízkými náklady.
Ve výhodách nakupování je také mnohem širší sortiment na Internetu, než v kamenných obchodech, e-shopy nabízejí na jednom místě až desetitisíce položek, což v kamenném obchodě není technicky možné.
Zajímavý pohled nabízí následující tabulka:

Obchodování na Internetu



	2005 (v miliónech Kč)
Internet Mall	1010
Eurocomm (Kasa.cz)	470
VltavaStores	420

Otázky a úkoly:

1. Co obsahuje internetová adresa www.apek.cz ?
2. Najděte na http://www.obchodnirejstrik.cz ekonomické údaje firem Internet Mall, Kasa.cz, VltavaStores a dalších, operujících na českém trhu
3. Najděte na http://www.google.com a http://www.yahoo.com vyznané firmy, operující v oblasti elektronického obchodu ve světovém měřítku
4. Najděte na http://www.yahoo.de firmy, podnikající na německém teritoriu v segmentu elektronického obchodu
5. Najděte na internetu analýzy poradenských společností Forrester Research a Gartner, které se týkají elektronického obchodu.V čem se liší ?

Klíčová slova: elektronický obchod, UNCITRAL

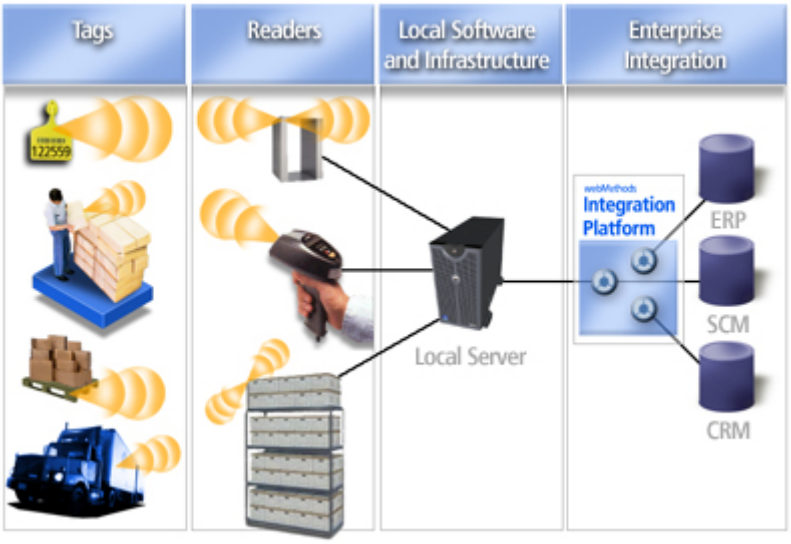
9 Nnové trendy

a) RFID

Technologie RFID (Radio Frequency Identification, identifikace na rádiové frekvenci) se prezentovala původně jako rádiová náhrada čárových kódů. Není bez zajímavosti, že největší zájem na zavedení RFID byl iniciován od firmy, která před desetiletími prosadila i čárové kódy – od WalMartu. Firma si od nové technologie slibuje další konkurenční výhody. Nový systém lze úspěšně nasadit v mnoha odvětvích a oblastech, kde je kladen důraz na co nejrychlejší a přesné zpracování informací a okamžitý přenos těchto načtených dat k následnému zpracování.Informace jsou v elektronické podobě ukládány do malých čipů-tagů, ze kterých je lze následně načítat a opakovaně přepisovat pomocí rádiových vln, toto zpracování se však neděje po jednotlivých čteních jako u v současnosti používaných čárových kódů, ale hromadně. Současná čtecí zařízení dokážou zatím najednou načíst až několik set tagů za minutu.

Technologie RFID je v současné době považována za přímého nástupce čárových kódů; dnes se využívají tiskárny, které dokáží potisknout RFID tag informacemi s čárovým kódem. Takové tiskárny při potisku zároveň zapisují informace do tagu a dokonce pokud je RFID tag poškozen, toto zjistí a tag označí. Podobně jako u čárových kódů se informace zaznamenávají na nosič dat - tzv. RFID tag , který je připevněn na sledované objekty, tag obsahuje malý čip s anténou a pamětí. RFID tagy jsou základem systému pro ukládání a přenos informací pomocí elektromagnetických vln. Může je hromadně přečíst a zaznamenat příslušné čtecí zařízení, které může být pevné nebo mobilní. Pomocí vln vyzářených z čtecího zařízení dojde k nabití chipu a následně se informace uložená v chipu bezdrátově přenese zpět do čtecího zařízení (každý tag obsahuje tzv. EPC kód - electronic product code, jedná se o jednoznačné sériové číslo tagu). Mario Cardullo kterému náleží U.S. Patent 3 713 148 z roku 1973 byl první otcem moderních RFID. Vynalezl totiž pasivní vysílač radiových vln s pamětí. První demonstrátory těchto RFID zařízení, která jsou stále používána, byla vyrobena v roce 1973 v Los Alamos Scientific Laboratory.

Každá implementace RFID technologie obsahuje RFID tagy pro označení objektů, čtecí zařízení a tzv. middleware (řídící systém, který zajišťuje hromadné zpracování všech načtených tagů v dosahu čtecích zařízení a přenesení zpracovaných dat do návazného informačního či řídícího systému).



Důvodem tohoto rozdělení je umožnění čtení dat z mobilního zařízení (tag) RFID čtečkou a jejich následné zpracování potřeb konkrétní aplikace. Data poskytovaná tagy se mohou týkat identifikace či místa nebo specifik ohledně ceny barvy, data zakoupení.
V typickém RFID systému, každý objekt zvlášť je vybaven malým levným RFID tagem. Tag obsahuje vysílač s digitálním paměťovým čipem, který má svoji unikátní identifikaci. Čtečka, anténa spolu s vysílačem a dekodérem, vysílá signál, který aktivuje RFID tag a může číst a zapisovat data. Když RFID tag prochází elektromagnetickým polem, detekuje aktivační signál čtečky. Čtečka dekóduje data obsažena v obvodě tagu (křemíkový čip) a data odešle na server. Aplikace data vyhodnotí a může provést odfiltrování četných nadbytečných čtení téhož tagu. RFID tagy mají oproti štítkům s čárovým kódem několik zásadních výhod. Štítek s čárovým kódem musí být umístěn na viditelném místě pro čtecí zařízení a tím je zároveň vystaven vlivům poškození - odtržení, poškození, teplotní vlivy, povětrností vlivy. RFID tagy lze také umístit do značeného objektu tak, aby nebyl těmto vlivům vystaven, a tím je několikanásobně odolnější oproti štítku s čárovým kódem. Nejlevnější EPC RFID čipy, které využívají například firmy Wal-Mart, Tesco ve Velké Británii, jsou dostupné za 5 centů. Jejich velikost spolu s anténou se pohybuje od rozměrů poštovní známky až k velikosti pohlednice.

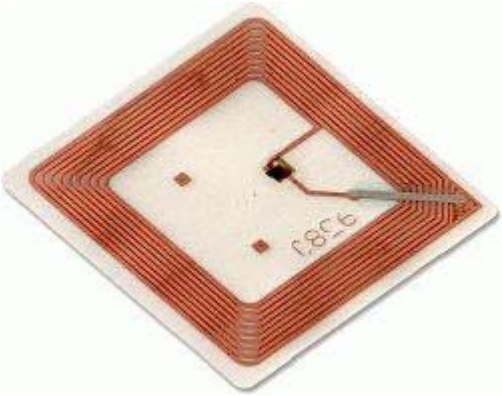
Cena aktivních čipů velikosti mince se pohybuje okolo několika dollarů. Příkladem úspěšné aplikace technologie aktivních RFID v logistice je Ministerstvo obrany USA, kde se využívá již více než 15 let.

Aktivní čipy vysílají samy své údaje do okolí (TTF tag talks first), toto umožňuje vlastní miniaturní baterie umístěna v čipu, která vydrží cca 1-5 let. Tyto čipy však kvůli baterii mají menší odolnosti na teplotu a je nutné provádět výměnu baterie. Tyto čipy je možné využít i v náročnějších prostředích jako jsou voda a kov nebo na delší vzdálenosti (nejvíce se využívají pro sledování osob, vozového a technologického parku, sledování zvířat a tam kde leze čip opětovně použít). Aktivní čipy mají vzdálenost čtení až 100m, ale vyžadují poměrně vysoké náklady na pořízení, velikost paměti na čipu může dosahovat až 100Kb. Aktivní čipy je také možné doplnit například o sledování teploty, vlhkosti, otřesů, radiace, světla či detekci ethylenu ve vzduchu.

Pasivní čipy jsou cenově výrazně levnější, mají různou akční vzdálenost čtení od 0,5m do 10m, dlouhou životnost čipu a používají metodu (RTF reader talk first). Tagy, které pracují na nejvyšší frekvenci UHF mají rádius - cca 3 až 10m (EPC, ISO 18000-6), ty s frekvencí

nejnižší LF 125kHz mají dosah jen cca 0,5m (ISO 14443). V současné době jsou nejvíce rozšířeny pasivní čipy a to zejména kvůli své nízké ceně, nenáročnosti na obsluhu a odolnosti, velikost paměti 64 - 256 bitů, a to i přes jejich menší spolehlivost.

Takto pasivní RFID čip vypadá – čtverečky kolem jsou anténa, uprostřed je čip. Aktivní čip vlastní navíc ještě nezávislý zdroj napájení.



V případě použití pasivního RFID musí vysílač (snímač) periodicky vysílat pulsy prostřednictvím antény do okolí. Pokud se v blízkosti objeví pasivní RFID čip, využije přijímaný signál k nabití svého napájecího kondensátoru (jeho kapacita je dostatečná k odeslání odpovědi). Anténa tohoto čipu je tedy konstruována k hromadění energie tak vysílání signálu. V případě, že se jedná o aktivní systém, nosič informace okamžitě odpoví. Tento signál snímač od nosiče informací přijme a po jeho vyhodnocení (ochranné kódy atd.) jej předá dále do systému.

Absence zdroje napájení pasivních RFID vede k jejich velmi malým velikostem, ta v tomto roce dosáhla 0,15mm x 0.15 při tloušťce menší než papír (7.5μm).

V současné době se k výrobě pasivních RFID tagů využívá čipů na bázi křemíku, přičemž jsou vyvíjeny také polymerové. V minulém roce již byly představeny tyto polymerové čipy společností PolyIC (Německo) a Philips(Nizozemsko). Jejich zavedení by přineslo možnost vzniku tzv. inteligentních štítků a značné zlevnění technologie.

RFID tagy se v současné době vyrábějí v několika variantách, dle velikosti a materiálu a s tím souvisejícího použití (tagy produktové, kartonové, paletové, malé tagy na láhve) a dle způsobu použití (nalepení přímo na objekt), tzv. "Inlays" pro další použití pro výrobce - přímo zabudované do produktů a zapouzdřené (například plastové - mají větší odolnost a používají se i v případě umístění tagu na kovový materiál, zde zajišťují oddálení čipu a antén od rušivého podkladního materiálu kovu).

Otázka je, proč by obchodníci měli prahnout po zabudovávání identifikačních čipů do jimi prodávaného zboží. Odpověď je jednoduchá – aby měli lepší přehled za méně peněz. Zaprvé se tak zjednoduší logistika zboží. Zatímco u čárového kódu má každý výrobek stejného druhu stejný čárový kód, v případě RFID má každý jednotlivý kus svůj jednoznačný 96bitový identifikátor EPC (Electronic Product Code – elektronický produktový kód). Lze tedy sledovat pohyb jednotlivých kusů zboží, ztrátovost, prošlé lhůty atd.

Kromě toho u čárových kódů je třeba každý kus zboží přiložit k optickému snímači. V případě RFID zvládne snímač přijmout kódy zboží bez fyzického kontaktu se zbožím. V praxi by stačilo, aby u pokladny člověk zastavil u snímače, snímač během několika vteřin zjistí všechny kódy, nakupující zaplatí a vše je vyřízeno bez vykládání zboží na pás.

Pro obchodníky je navenek nejzajímavější rychlejší odbavení zákazníků. Hesla jako "žádné fronty u pokladen" znějí hezky a dobře se presentují, více podstatná je ale část logistická, tedy sledování pohybu zboží a data mining – následná analýza na těchto datech.

Kupříkladu jedou ze součástí RFID implementace mají být LCD cenovky. Místo doposud běžně používaných papírových cenovek by na regálech byly malé cenovky vybavené LCD a snímačem. Cenovky by zjistily, vedle jakého zboží jsou a podle toho by si z centrálního počítače načetly aktuální cenu zboží. To ještě ale není tak zajímavé. Zajímavější je to, že by se takto mohla cena aktualizovat dynamicky – koncepty počítají s tím, že přes noc by počítač hypermarketu zjistil, jaké zboží se lépe prodává a jaké nejde, a podle toho by upravil ceny. Ležáky, které jsou na skladě příliš dlouho, by šly s cenou dolů, hity, kterých je zrovna málo skladem a počítač zjistil, že další dodávky se čekají až za delší dobu, by šly s cenou nahoru.

A tady je ta chvíle, kdy celá záležitost je komerčně velmi zajímavá pro velké ICT firmy. Rozsáhlá práce s daty (velké hypermarkety mají skladem desetitisíce různých druhů zboží) je náročná na software i hardware. Je zapotřebí mít k dispozici výkonný server, dobré zálohování, kvalitní databázi a dobrou aplikaci se slušně vybalancovanými cenovými změnami, reportingem a data miningem. RFID sice může přinést obrovské úspory – ale do začátku vyžaduje obrovské počáteční náklady. Je tedy jasné, že malí obchodníci na RFID nepřejdou a propast mezi malými obchodníky a obrovskými řetězci se bude dále zvyšovat. Jen podle odhadů WalMartu by zavedení RFID umožnilo snížit ceny o další průměrně čtyři procenta díky tomu, že bude potřeba méně pokladních, a tedy budou menší náklady na lidskou sílu. Ačkoliv se do počátku neočekává, že by se pokladny obešly zcela bez pokladních, obsluha bude hrát spíše roli dozoru, informátora a přebírače platebních karet – a ze začátku i obsluhovat klasickou pokladnu. Ačkoliv WalMart již seriózně uvažuje o tom, že by většina jeho pokladen byla striktně bezhotovostní a pouze jedna či dvě pokladny by přijímaly hotovost.

Až do současnosti bránila vyšší míře využívání RFID čipů jejich vysoká cena, která však již začala (a v příštích letech ještě jistě bude) klesat. Proto byly RFID čipy nejčastěji používány jen pro značení zboží ve vnitropodnikových procesech. V současné době nalezneme jejich použití v logistických a výrobních firmách a do mnoha dalších odvětví hospodářství se rychle rozšiřuje.

Nespornou a nenahraditelnou výhodou čipů oproti čárovým kódům je skutečnost, že čtecí zařízení nemusí mít s čipem optický kontakt. Čip může tedy být uložen i uvnitř obalu nebo na výrobku samotném a tak chráněn před vlivem vlhkosti, teploty, nečistoty a poškození. V případě čárových kódů musí při zpracování dat docházet k postupnému načítání jednotlivých kódů za sebou a čtecí vzdálenost je minimální, v případě RFID chipů lze však naráz přečíst a zpracovat velké množství čipů a to i na větší vzdálenosti do 10m, v případě aktivních čipů až do vzdáleností 100m.

Je zde však ještě jedna vlastnost, kterou čárové kódy nikdy neumožní a to je možnost nejenom informaci z čipu číst, ale také ji tam zapisovat a přepisovat, teprve tato technologie umožňuje převratné možnosti. Je snadné zjistit cestu výrobku ze samotné výroby až k příjemci.

Celá došlá zásilka je nasnímána RFID čtečkami během několika sekund a tato informace (násobně větší objem) se přenáší do informačního systému. Výsledkem je okamžitá informace o stavu našeho skladu, a dramatické zrychlení jejího získání. Vybavíme-li stejnou technologií také výrobu ve společnosti, získáme tak stejné informace z jednotlivých částí výroby (stav výroby, průběžné zásoby na pracovišti). Dramatické zrychlení sběru informací v rámci logistiky/výroby umožňuje daleko lepší plánování zásob společnosti. Pokud máme plán výroby a stavy zásob, tak zásoby, které máme na skladě můžeme odpovědně řídit ne z hlediska Q (množství), ale z hlediska T (času). Tím se zcela zásadním způsobem zjednodušuje systém predikce objednávek a otevírá se velký prostor pro optimalizaci skladových zásob - úspory na vázaném kapitálu.

Příklad ukazuje jen jedno z možných využití RFID na toku hodnot ve společnosti. Takových příkladů lze nalézt v každé společnosti více. Otázkou pak zůstává, do jaké míry lze kvantifikovat přínos, jakého dosáhneme tak radikální změnou vybraného procesu.

Několik oblastí, kde lze dosahovat pomocí RFID zlepšení:

Logistika :

- zrychlení procesu příjmu, výdeje, přesunu a inventarizace produktu
- odstranění chyb obsluhy a zpřesnění celé evidence produktů
- minimalizace nákladů spojených se značením produktů
- opakovaný zápis údajů zboží do čipu během celého logistického pohybu
- přesná evidence spotřebitelských jednotek, kartónů, palet
- velká odolnost RFID čipů (vlhkost, teplota, atd.)
- rychlé načtení údajů - není nutná přímá viditelnost označených jednotek

Výroba :

- přesné řízení toku materiálu ve výrobě (snížení zásob)
- dohled na správnou kompletaci celku
- zpětná dohledatelnost až na úroveň jednotlivých materiálů
- okamžitá informace o stavu výroby
- možnost zápisu informací do čipu během výroby
- sledování využití a činnostech na pracovišti
- možnost umístit čip natrvalo do výrobku a informace poté využít v distribuci

Evidence majetku:

- snížení chybovosti při evidenci a inventarizaci majetku
- výrazné zrychlení procesu inventarizace majetku
- možnost zápisu více dat do čipu na majetku, např.uložení poslední inventarizace
- finanční úspory v nákladech na obsluhu při inventarizaci

- zrychlení procesu příjmu, výdeje, přesunu a inventarizace produktu

Každý obchodní produkt od svého vzniku-výroby až k konečnému spotřebiteli, prochází složitou cestou distribuce. Na této cestě se podílí řada firem a každá z těchto firem s tímto produktem provádí řadu činností. Základní operace jsou, příjem na skladové místo, přesun v rámci skladu a poté výdej ze skladu další firmě v distribučním řetězci. V současné globální ekonomice je výrazným faktorem, který ovlivňuje zda firma je úspěšná či nikoliv, především rychlost. Současné značení produktů čárovým kódem umožňuje pouze postupné načítání jednotlivých čárových kódů z každého produktu, čárový kód na produktu musí mít přímou viditelnost na čtecí zařízení. Značení produktů RFID čipy umožňuje současně načíst až 1000 čipů/sec najednou, jednotlivé čipy nemusí být přímo viditelné čtecím zařízením. Paletový přepravník tak může projet celým RFID čtecím portálem a v jeden čas dojde k současnému načtení všech čipů na paletě.

- odstranění chyb obsluhy a zpřesnění celé evidence produktů

Životnost produktu na trhu se za poslední dobu výrazně zmenšila, silná konkurence si žádá tvorbu dalších nových produktů. Toto je velice náročné na přesnost zásobování. Firmy se snaží pomocí značení produktů a informačních systému mít neustálý přehled o skladových zásobách. Hlavně se snaží tyto zásoby minimalizovat, mimo jiné z důvodů rychlé obměny produktu na trhu. Tento proces zrychlení toku produktů klade velké nároky na přesnost evidence a odstranění chyb obsluhy. Časté chyby obsluhy vedou k finančním ztrátám a mohou ohrozit konkurenceschopnost firmy na trhu. RFID čipy společně se čtecím zařízením vylučují možnost vzniku chyby obsluhy, které vzniknou například tím, že obsluha načte pouze část čárových kódů na paletě.

- minimalizace nákladů spojených se značením produktů

Značení produktů etiketou s čárovým kódem, je v současné době nejčastěji používaný proces. Protože však čárový kód musí být na viditelném místě, dochází poměrně často k poškození etikety. RFID čip nemusí být umístěn na viditelném místě a proto jej lze do produktu nebo jeho balení umístit již v samotné výrobě. Informace o produktu jsou potom shodné po celou cestu produktu ke koncovému spotřebiteli. Tímto dojde k výrazným úsporám nákladů a tím i ke snížení koncové ceny produktu.

- opakovaný zápis údajů zboží do čipu během celého logistického pohybu

RFID čip má oproti etiketě s čárovým kódem hlavní výhodu v tom, že do čipu lze informace i zapisovat a nejenom číst, jak je to v případě čárového kódu. Tato vlastnost bude v budoucnosti klíčová a rozhodne v mnoha odvětvích pro úplnou náhradu čárového kódu RFID čipem. Do čipu lze navíc informace zapisovat a měnit opakovaně, lze takto do každého produktu zapsat datum výroby a poté také připsat jednotlivé logistické zápisy, které vznikají po celou dobu cesty produktu.

- přesná evidence spotřebitelských jednotek, kartónů, palet

Představte si jednoduchý model distribuce zboží: jednotlivý produkt má svůj obal a na něm čárový kód, X produktů je zabaleno do kartonu, ten má další čárový kód a Y kartónů je zabaleno na paletě, paleta má opět vlastní čárový kód. Paleta je celá v ochranném obalu z důvodu poškození.

V současnosti při samotném logistickém procesu obsluha načte čárový kód palety, ale

již není schopna ověřit, zda je na paletě správný počet kartónů a správný počet produktů. Jediným řešením by bylo paletu rozebrat a postupně načíst všechny čárové kódy. RFID čtecí portál však načte najednou všechny RFID čipy na paletě nalezené. Navíc dle typu čipu dokáže vyhodnotit počet RFID čipů kartónů i počet RFID čipů samotných produktů.

- velká odolnost RFID čipů (vlhkost, teplota, atd.)

Etiketa s čárovým kódem podléhá teplotním a povětrnostním vlivům a následně dochází k poškození etikety. Je tomu hlavně proto, že je nutné etikety s čárovým kódem umisťovat tak, aby je bylo možné načíst čtecím zařízením a tudíž z venku. RFID čip je umístěn uvnitř produktu nebo balení a tím je odolný jak proti teplotě, vodě i povětrnosti. V současné době na trhu již existují RFID čipy, které navíc mohou obsahovat čidla - například pro měření vlhkosti nebo teploty.

- rychlé načtení údajů - není nutná přímá viditelnost označených jednotek

RFID čip má oproti etiketě s čárovým kódem dvě hlavní výhody - rychlost čtení a nepřímou viditelnost čtecího zařízení na čip. Současné standardy UHF RFID čipů umožňují načíst najednou až 1000 čipů/sec, tato hodnota se však s příchodem novějších a výkonnějších zařízení bude zvyšovat. RFID čtecí zařízení nepotřebuje mít přímou viditelnost na jednotlivé čipy, čtení i zápis probíhá bezdrátově a to do vzdálenosti cca 15m u pasivních čipů a až 100m u aktivních čipů.

Inventarizace pomocí etiket s RFID čipem je mnohem jednodušší. Čtecí zařízení dokáže číst RFID čip až na vzdálenost 10m, obsluha nemusí při vstupu do místnosti pracně na každém inventárním majetku hledat, kde je etiketa umístěna ani manipulovat se čtečkou na krátkou vzdálenost. Čtecí zařízení stačí umístit do vzdálenosti cca 3m od majetku a ihned lze vyhodnotit údaje o nalezeném či nenalezeném majetku.

V případě velmi drahého inventárního majetku lze použít také aktivní RFID čipy, které lze číst až na vzdálenost 100m. Při vstupních a výstupních branách lze také instalovat čtecí portály RFID a tím online sledovat pohyb těchto zařízení v rámci instituce.

Zdravotnictví je specifický obor, ve kterém v případě vzniku chyby nehrozí pouze finanční ztráty, ale chyby mohou ohrozit i zdraví pacientů či zaměstnanců.

Jedním z problémů, který tyto technologie pomáhají velice úspěšně řešit je jednoznačná identifikace pacientů a léků. Posledních 10 let se pro identifikaci osob velice úspěšně používají speciální náramky s čárovým kódem, pro identifikaci léků pak etiketa s čárovým kódem.

Technologie RFID (radiofrekvenční identifikace) je však pro identifikaci osob mnohem efektivnější, protože RFID čip zajišťuje nejenom čtení dat, ale umožňuje i zápis údajů přímo do čipu na náramku pacienta. Navíc není nutná viditelnost mezi náramkem a čtečkou.

Pacient při příjmu do nemocnice získá identifikační náramek s RFID čipem. Veškeré úkony s tímto pacientem mohou být automaticky zapisovány nejen do centrálního informačního systému, ale hlavně přímo do samotného čipu v náramku. Zapisovat lze například každé měření teploty, transfúze krve, infúze, injekce, podávané léky, atd.

Každé zdravotnické místo je vybaveno snímačem RFID a tak lze okamžitě identifikovat pacienta a zobrazit jeho údaje a to nejenom v zařízení samotném, ale i na odloučených pracovištích, kde není možné zajistit napojení čtecích zařízení na centrální informační systém.

Pomocí náramků s RFID čipem lze v kombinaci s čtecím vstupním portálem okamžitě

lokalizovat pacienty a případně povolit či zamezit vstup pacienta na jednotlivé oddělení.

Každá nemocnice také musí řešit nakládání s použitým prádlem. Špinavé prádlo je většinou sváženo do prádelen dodavatelskou firmou, která zajišťuje odvoz, vyprání a dovezení čistého prádla zpět do nemocnice

Prádlo bývá evidováno v pytlích na kilogramy. Řada nemocnic považuje za velice problematické prokazovat skutečné měsíční plnění dodavatele.

Pokud je každý pytel označen RFID čipem, obsluha po jeho naplnění prádlem načte identifikační číslo z čipu.

Do centrálního systému se okamžitě zapíší informaci o datu , času, váze, obsahu a zároveň informace může zapsat i do samotného čipu. Lze tak jednoduše a efektivně sledovat skutečnou váhu odvezeného prádla za měsíc, dobu od svozu k návratu prádla a případné ztráty.

RFID technologie se také uplatňuje při evidenci odebraných vzorků krve.

RFID technologie zde dokáže zamezit zbytečným záměnám a nesrovnalostem. Každý odebraný vzorek krve je označen RFID čipem, do čipu je zapsána informace o jménu pacienta, datu a času odběru a zdravotnickém útvaru.

Zdravotnická zařízení disponují značným inventárním majetkem. Každý pracovník, který má na starosti evidenci majetku ví, jak náročné je provádět ze zákona povinné značení a roční inventarizaci majetku.

Majetek je v nemocnici v neustálém pohybu a často na místech, kde je složité zajišťovat dohled. Běžně se dnes využívá k identifikaci majetku etiketa s čárovým kódem. Na každé etiketě je uveden název majetku, inventární číslo a čárový kód a v centrálních databázích je majetek umístěn v jednotlivých lokacích (místnosti, patra, budovy apod.). Etikety s čárovým kódem musí být na majetek umístěny tak, aby nedošlo k nechtěnému poškození majetku, následně pak inventární čety musí pracně manipulovat s čtecím zařízením např. pod stolem, operace samotné inventarizace je časově, fyzicky a finančně náročná.

Inventarizace pomocí etiket s RFID čipem je mnohem jednodušší. Čtecí zařízení dokáže číst RFID čip až na vzdálenost 10m, obsluha nemusí při vstupu do místnosti pracně na každém inventárním majetku hledat, kde je etiketa umístěna ani manipulovat se čtečkou na krátkou vzdálenost.Čtecí zařízení stačí umístit do vzdálenosti cca 3m od majetku a ihned lze vyhodnotit údaje o nalezeném či nenalezeném majetku.

V případě velmi drahého inventárního majetku lze použít také aktivní RFID čipy, které lze číst až na vzdálenost 100m. Při vstupních a výstupních branách lze také instalovat čtecí portály RFID a tím online sledovat pohyb těchto zařízení v rámci zdravotnického zařízení.

Na známém logistickém portálu **About Logistics (Logistics/Supply chain)** se v diskuzním fóru objevil velice zajímavý a aktuální příspěvek. Šlo o **SWOT analýzu RFID technologie,** identifikace výhod a nevýhod, ovlivnění obchodních vztahů a výhledu do budoucna.

Silné stránky RFID:

- **Real time** informace
- Komplexnější informace o prodejích (marketing)
- Zrychlení produkce
- **Zlepšení kvality** výroby
- Velký výběr možných variant (transpondéry, čtecí/zapisovací jednotky)
- Patentová ochrana
- Opakované použití některých značek (tagů), robustnost řešení
- **Snížení nákladů** na obsluhu
- Více informací – unikátní data
- Nejsou potřeba žádné další kontroly
- **Redukce provozních nákladů**
- **Redukce zásob a ztrát**
- **Efektivita celého Supply chain**
- **Zvýšení kvality řízení zásob**
- Umožňuje čtení na delší vzdálenosti

Slabé stránky

- Vysoká nákladová struktura
- Obrovské množství dat (systém nemusí 100% pracovat) – ztráta přesnosti
- Nedostatek známosti mezi potenciálními zákazníky
- Prozatím příliš drahé
- Vyšší náklady na údržbu katalogu výrobků
- Možné prolomení technologie pot. zloději
- Čtení kódu na dálku – pot. zloději
- Otázka soukromí
- Příliš vysoké náklady na jednotku
- Každý produkt je vystopovatelný
- Implementace RFID
- Náklady na údržbu celého systému

Příležitosti

- Nová technologie (zvýšení flexibility výroby)
- Ztráta regulace
- Zdroj možné konkurenční výhody
- Možné globální rozšíření
- Rostoucí trh (zvýšení počtu zákazníků)
- Stopování kriminálníků – vládní dozor
- Kvalitní monitoring
- Zvýšení bezpečnosti
- Obrovský růst uvnitř supply chainu
- Budoucí implementace
- Snížení nákladů na jednotlivé operace
- Ideální pro Just in time systémy

Ohrožení

- Zpomalení ekonomického růstu může zastavit poptávku
- Růst trhu může přilákat konkurenci
- Nová technologie může zmrazit poptávku po některých produktech – obsoletní materiál
- **Nová procesní technologie -** konkurence s nižšími náklady
- Legislativa – sledování materiálového toku
- Možná negativní publicita
- **Neochota implementace u dodavatelů**
- Žádná legislativní omezení
- Ochrana dat – důležitá data
- **Obavy zákazníků -** ztráta důležitých dat, zákaznické profily apod.
- Dobrá vůle firem sdílet informace
- Možné napadení důležitých dat o produktech konkurencí

b) Ochrana osobních údajů-nový segment trhu

V zemích EU byly příslušné zákony o ochraně osobních údajů přijímány již v sedmdesátých a osmdesátých letech, které se týkají ochrany osobních údajů v nejrůznějších modifikacích. Později se přidávají další světové regiony. Analýzou materiálů Mezinárodní obchodní komory a časopisů Singapore Journal of Legal Studies, World Data Protection Report, Data Protection and Policy, Statewatch, Privacy Laws and Business a dalších lze identifikovat trend konvergence modelů EU a APEC:

V zásadě existují 2 systémy úprav osobních údajů:

1. **EU–typ** (Belgie, Česko, Dánsko, Estonsko, Finsko, Francie, Irsko, Itálie, Kypr, Litva, Lotyšsko, Lucembursko, Maďarsko, Malta, Německo, Nizozemsko, Polsko, Portugalsko, Rakousko, Řecko, Slovensko, Slovinsko, Spojené království, Španělsko a Švédsko) a
2. **APEC–typ** (Austrálie, Brunej, Čína, Filipíny, Hongkong, Indonésie, Japonsko, Kanada, Korejská republika, Malajsie, Nový Zéland, Singapur, Tchaj–wan, Thajsko, USA; Chile, Mexiko, Papua–Nová Guinea, Peru, Rusko a Vietnam).

EU–typ je charakterizován jedním úřadem na ochranu osobních údajů a jedním právním předpisem o ochraně osobních údajů. APEC–typ je charakterizován žádným úřadem na ochranu osobních údajů a mnoha právními předpisy o ochraně osobních údajů.[1]

V příštích letech se bude prohlubovat už existující trend konvergence obou systémů. EU–typ si ponechá jeden úřad na ochranu osobních údajů, ale dosud jednotná úprava ochrany osobních údajů se rozdrobí. V APEC–typu naopak vzniknou institucionální struktury na ochranu osobních údajů.

USA

- Přijetí odpovídající legislativy, týkající se ochrany osobních údajů, probíhá po dvou kolejích. Na federální úrovni zatím návrh člena sněmovny reprezentantů Cliffa Stearnse nezískal dostatečnou podporu, ale předpokládá se, že se zákonodárný sbor k problematice vrátí v roce 2007. Na úrovni států USA již 23 států přijalo nejrůznější odpovídající ustanovení v souvislosti s ochranou osobních údajů.

Dalším významným hráčem v USA je Federální komise pro obchod (U. S. Federal Trade Commission, FTC), která s platností 1. června 2005 implementovala tzv. „disposal rule“ (pravidla pro použití…), která ukládají firmám, pokud disponují informacemi o spotřebitelích (úvěrové informace, lékařských zprávy a zaměstnanecké posudky aj.), realizovat náležitá opatření pro zamezení neautorizovaného přístupu. Současně FTC penalizovala dvě firmy (BJ´Wholesale Club a DSW, Inc.) za porušování stanovených pravidel pro ochranu osobních údajů spotřebitelů. Dalším trendem v USA je ochrana osobních údajů na základě autorského zákona (17 US Code 101). Pokud jde o spyware pokračuje přijímání samostatných dílčích zákonů ve státech USA; zatím přijaly odpovídající zákony: Alaska, Arizona, Arkansas, California, Georgia, Indiana, Iowa, New Hampshire, Texas, Utah, Virginia, Washington. Velmi agresivně postihuje rovněž spyware Federální komise pro obchod FTC, která je velmi aktivní rovněž pokud jde o marketing a spam (např. 13. prosince 2005 byla udělena finanční penalizace 5,3 milionu USD v telekomunikačním sektoru). Pokud jde o phishing/pharming,

Washington, Virginia a New Mexiko již přijaly legislativu, kriminalizující phishing a další státy odpovídající ustanovení připravují. V Californii a Minnesotě jsou již před schválením.

Čína
Čína měla v červenci roku 2006 celkem 123 milionů uživatelů internetu (podle China Internet Network Information Centre). Ministerstvo informačního průmyslu oznámilo anti–spamovou regulaci. Firmy, které budou ustanovení porušovat, mohou přijít o podnikatelskou licenci a být finančně penalizovány. Pokud jde o výskyt spamu, zaujímá Čína druhou pozici po USA.

Hong Kong
Hong Kong na rozdíl od Číny, kde nebyla zatím přijata obecná legislativa ochrany osobních údajů, přijal legislativu podobnou EU a Kanadě již v roce 1996.

Indie
I když Indii chybí explicitní zákony o ochraně osobních údajů podobné EU a Kanadě, ochrana osobních údajů je zakotvena v dodatku (srpen 2005) zákona o informačních technologiích i v trestním zákoně.

Jižní Korea
Od roku 2005 připravuje vláda zákon o ochraně osobních údajů, který předpokládá zřízení komise pro ochranu osobních údajů (Personal Information Protection Commission). Návrh bude předložen do parlamentu na přelomu 2006/2007 .

Na přelomu 2006/2007 schválí odpovídající zákon o ochraně osobních údajů jako hybrid mezi EU a APEC modelem rovněž **Jižní Afrika**.

Japonsko
Japonsko má zkušenosti se značnými a častými úniky informací např. v roce 2005 regionální japonská banka ztratila záznamy a 1. 31 milionech bankovních zákazníků a o rok dříve prosákly informace o 6. 6 milionech uživatelů serveru. Časté jsou i úniky informací směrem k vymahačským gangům. Japonský zákon o ochraně osobních údajů pro veřejný sektor je v platnosti od roku 2003 a pro soukromý sektor od roku 2005. Nařízení, vztahující se na ochranu osobních údajů vydává rovněž Ministerstvo hospodářství, obchodu a průmyslu (MEZI) a velmi podrobně Finanční agentura (FSA).

Argentina
Zákon o ochraně osobních údajů byl přijat v roce 2000 vychází z modelu EU. K praktickým důsledkům přijetí zákona patří skutečnost, že firma ChoicePoint shromažďovala informace o obyvatelích Latinské Ameriky a po zásahu a vyšetřování argentinského úřadu zastavila svou činnost v této zemi.

Kanada
Podobně jako v Argentině, systém ochrany osobních údajů je v EU přijímán jako adekvátní, na rozdíl od jiných zemí APEC. Příslušný kanadský zákon je v platnosti od 1. ledna 2001 pro vládní sektor a od roku 2004 závazný pro všechny organizace.

Austrálie
Pro vládní agendy je federální zákon o ochraně osobních údajů v platnosti od roku 1988; od roku 2000 pro soukromý sektor. Zákon je tolerantnější než příslušná ustanovení v EU a Kanadě.

Rusko

27.července 2006 prezident V.Putin podepsal dva nové zákony s účinností od února 2007, vztahující se na ochranu osobních údajů; zákony nahradily starší zákon z roku 1995 . Podle časopisu PRIVACY LAWS @ BUSINESS 8/2006 zákony zrcadlí (mirrors) Direktivu 95/46 Evropské komise. Přestože oba zákony jsou pro Rusko velmi významné, právnička Lana Haworth upozorňuje na skutečnost, že oba zákony neobsahují jasná pravidla pro vymahatelnost práva na ochranu osobních údajů a v tom vidí značný problém.

Celkově lze identifikovat tyto další trendy:

I. Legislativní realizace koncepce ochrany osobních údajů se lavinovitě šíří po celém světě a dochází ke konvergenci EU modelu (s úřadem) a APEC modelu (bez úřadu), kde ochrana osobních údajů je upravena v několika zákonech (Indie, Chile). Lze předpokládat, že do roku 2010 přijme odpovídající legislativu převážná většina zemí OSN.

II. Nástup nových sofistikovaných technologií (RFID, phishing, pharming, braingate) povede k přijetí odpovídajících samostatných zákonů. Problematika SPAMu bude postupně řešena vytvářením inteligentních Internetů se samoorganizujícími se schopnostmi. Současný Internet se může stát vyhledávaným smetištěm.

III. Krizi v systému ochrany osobních údajů vystřídá během několika let konjunktura:
- nárůst počtu porušování ochrany osobních údajů si vyžádá v budoucnosti (kolem roku 2010) „privatizaci ochrany osobních údajů“. Prověrky budou provádět specializované firmy, které budou mít od národních úřadů pro ochranu osobních údajů certifikaci (auditoři pro ochranu osobních údajů),
- budou sílit tendence k ustavení evropského úřadu pro ochranu osobních údajů (podobný trend je v telekomunikačním sektoru i v dalších sektorech),
- trh si vyžádá konstrukci robotů–programů pro odhalování porušování zákona o ochraně osobních údajů.

S ochranou osobních údajů souvisí i následující skutečný a jen zdánlivě žertovný případ.

Australská banka vydala kreditní kartu kočce (podle seznam.cz 7.1.2007 04.47)

Kreditní kartu může v Austrálii získat i kočka.

Výmluvy bankovního domu, který spravuje její finance, že zpoždění v proplácení účtů je způsobeno řadou bezpečnostních opatření zavedených ve prospěch klientů, nakonec popudilo Katherine Campbellovou z australského Queenslandu natolik, že se rozhodla tvrzení finančníků prověřit. Tím, že požádala o vydání druhé kreditní karty. Nenechala ji však vystavit na sebe, ale na jistého Messiaha Campbella, jak se jmenuje její kocour.

SYDNEY - Bank of Queensland žádosti vyhověla, vyřídila ji přímo kosmickou rychlostí a navíc bez vědomí majitelky účtu jejímu držiteli přiklepla úvěrový limit ve výši 4200 australských dolarů, což v přepočtu činí přes 117 tisíc korun.

"Skutečnost, že kocouru Messiahovi kreditka skutečně došla, mě ohromila," přiznává Katherine Campbellová a dodává, že od té doby si láme hlavu, v čem vlastně spočívají ta moderní bezpečnostní opatření, které mají uchránit vklady klientů před vytunelováním.

Nic na tom nemění skutečnost, že finanční ústav se jí za lehkomyslné počínání omluvil a okamžitě po zveřejnění celé záležitosti nechal kocourkovi kartu zablokovat.

c) ovládání počítače hlasem:

- Člověk: Počítači, zapni se!
- Počítač: Provedeno.
- Člověk: Počítači, přečti mi poslední můj e-mail!
- Během několika let se stane tento rozhovor skutečností u většiny PC. Již dnes nabízí firma
- Voicetronic sofistikovaný systém Program VoiceWin – Voicetronic.

Jedním nebo více slovy můžete pustit některý program, listovat v něm, počítač vypnout, zapnout restartovat, připojit se k Internetu a podobně. K tomu lze používat program VoiceWin od firmy Voicetronic a samozřejmě mikrofon. Jeho ovládání je velice jednoduché. Některé povely jsou předem naprogramované, jiné si můžete udělat sami. Aby to všechno fungovalo, musí být povely předem několikrát namluveny. Program si záznamy ukládá do databáze a pak je porovnává s tím, co řeknete. Téměř nikdy se program nesplete a spolehlivě rozpozná povely. Ovšem funguje to jen na váš hlas a někoho jiného bude program stěží poslouchat. I na to mysleli autoři programu. Můžete využít možnosti více uživatelů s nezávislými hlasovými databázemi.
Ještě hodně vody však uplyne, než budou počítače zaznamenávat v textu, co mu diktujete. Tak daleko program ještě nedospěl. Zadávat celé věty s tím, že si je počítač analyzuje, jde zatím opravdu jenom ve Star treku. I když je zde k dispozici několik složených povelů. Můžete říct "nahoru o šest" a např. v průzkumníku se označená položka posune o šest nahoru. [1]

Program MyVoice – Fugasoft

O programu MyVoice

Program MyVoice byl vyvinut s cílem pomoci zejména handicapovaným lidem v přístupu k počítačové technice a k informačním technologiím. Na výzkumu se podílela Technická univerzita v Liberci(viz. http://itakura.kes.vslib.cz/kes/projekty.html) Umožňuje totiž:

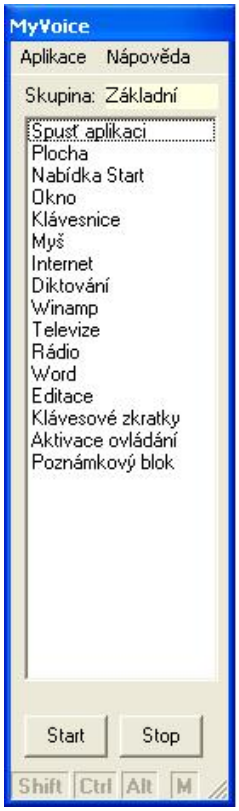
- **ovládat počítač** a na něm nainstalované programy výhradně **pomocí hlasových povelů**. Těmito povely lze uskutečnit tytéž akce, k jejichž provedení by jinak byla nutná klávesnice a myš.

- **diktovat text** po jednotlivých písmenkách či předem připravených celých slovech nebo frázích. (Diktování po slovech je ovšem omezeno jen na omezený okruh slov a vyžaduje pečlivou výslovnost. Pro tento účel je připraven malý slovník 10 000 nejčastějších českých slov.) Další slova či fráze si uživatel může do slovníku programu přidat podle vlastní potřeby.

- **zadávat nové hlasové povely**, upravovat ty stávající nebo tvořit celé nové skupiny příkazů pro ovládání jakékoli aplikace běžící pod systémy Windows 2000, XP nebo novějšími.

Program umožňuje hlasové ovládání počítače všem osobám, které jsou schopny dobře vyslovovat krátké české povely a zároveň očima sledovat dění na obrazovce počítače.

Díky programu MyVoice je možné hlasem ovládat jakýkoliv program určený pro operační systém MS Windows (od verze 2000 výše). Videoukázky dokumentující možnosti práce s programem MyVoice najdete na stránce Videoukázky.



Důležité rysy programu MyVoice

Program je schopen okamžitě rozpoznávat hlasové povely od libovolné osoby, nevyžaduje tedy, aby tato osoba předem cokoliv namluvila. Program je již od dodavatele vybaven několika stovkami základních povelů, které jsou rozděleny do skupin, např. povely pro diktování (po jednotlivých hláskách), pro ovládání myši, pro textový editor Word, atd. Uživatel má možnost přidávat si své vlastní povely či modifikovat stávající, čímž si může usnadnit práci se svým oblíbeným programem. Uživatel si může, zejména pro účely diktování, sestavit seznam nejčastěji používaných slov nebo frází či krátkých vět, které pak může vkládat jediným hlasovým povelem. Tvořením vlastních povelů lze postupně rozšiřovat možnosti hlasového ovládání na nově instalované programy i hardwarové komponenty.

Pomocí programu MyVoice můžete mimo jiné:

- Hlasem spouštět libovolné programy, ať jsou umístěny na ploše, v Nabídce Start nebo kdekoliv na disku počítače.
- Hlasem nadiktovat textový dokument (např. v programu Word nebo Poznámkový blok), přičemž diktování se provádí po písmenech, případně po celých slovech nebo frázích (pokud je má uživatel předem

připravené).

- Hlasem ovládat elektronickou poštu, tj. přijímat i odesílat dopisy.
- Hlasem ovládat internetový prohlížeč, tj. navštěvovat webové stránky na celém světě, pohybovat se po odkazech, vyplňovat formuláře na Webu, listovat v elektronickém tisku, atd.
- Hlasem spouštět a ovládat programy určené pro zábavu i pro vážnou práci, např. hry, programy pro kreslení, prohlížeče obrázků a videonahrávek, přehrávače hudby, apod.
- Hlasem řídit televizi i rádio, pokud je v počítači nainstalována karta pro příjem televize a rádia.
- Hlasem vytočit telefonní číslo a vést telefonní hovor, pokud je k počítači připojen speciální modem...

Minimální systémové požadavky

Procesor : Intel kompatibilní (o frekvenci > 1 GHz pro ovládání náročnějších aplikací)
Operační paměť : 128 MB a více, pro Windows XP doporučujeme 512 MB
Místo na disku : nejméně 10 MB volného místa
Operační systém : Windows 2000 nebo Windows XP a novější
Zvuková karta : kvalitní 16 a více bitová (neměla by být integrována na základní desce)
Mikrofon : vyšší kvality, doporučujeme náhlavní typ se sluchátky a mikrofonem (HEADSET), krajně nevhodný je naopak tzv. tyčkový typ

K dalším známým systémům patří: virtuální pomocník Clarissa – NASA XEROX.

Smysluplná konverzace s roboty či palubním počítačem, která byla desetiletí jedním ze základních prvků literatury science fiction, se stává skutečnostní díky spolupráci vědců z Amesova výzkumného centra NASA a odborníků společnosti Xerox.
Koncem června 2005 vyústila spolupráce NASA a Xeroxu v představení pokročilého systému pro hlasové ovládání počítačových systémů na 25. výročním setkání Asociace pro počítačovou lingvistiku. Cílem systému, který nese označení Clarissa, je usnadnit astronautům jejich každodenní pracovní úkoly na palubě International Space Station (ISS).
„Clarissa je plně hlasem ovládaný virtuální asistent posádky, který astronautům umožňuje plně se věnovat zadaným úkolům za pomoci hlasových příkazů," představuje Clarissu Beth Ann Hockey, vedoucí týmu, který tento systém v laboratořích Amesova výzkumného centra vyvíjí. Astronauti během svého pobytu na Mezinárodní vesmírné stanici vykonávají přibližně 12 000 úkonů, které zahrnují například údržbu systémů pro podporu života, kontrolu skafandrů, vědecké experimenty nebo pravidelné zdravotní prohlídky. Clarissa přitom reaguje na hlasové povely členů posádky a nahlas předčítá instrukce potřebné pro bezchybné plnění připravených úkolů.
„Jen si zkuste provést analýzu vzorku vody za současného sledování podrobného manuálu na počítačové obrazovce, když se vznášíte v mikrogravitačním poli," upozorňuje na problémy pobytu ve vesmíru astronaut Michael Fincke, který se nedávno vrátil z šestiměsíčního pobytu na ISS. „Možnost mluvit na počítač, naslouchat podrobným instrukcím a mít volné ruce pro plnění potřebných úkolů nám poskytne komfort srovnatelný s přítomností dalšího člena posádky."

NASA jako základní požadavek na hlasem ovládaný počítačový systém vesmírné stanice

označila jeho neustálou připravenost přijímat a reagovat na povely. Původní verze Clarissy se pokoušela zpracovat veškerou komunikaci v prostoru vesmírné stanice včetně rozhovorů mezi jednotlivými členy posádky, ale tento přístup vedl k problémům při rozlišování mezi skutečnými příkazy směřujícími k palubnímu počítači a běžnou konverzací.
NASA se proto v roce 2004 obrátila na Jeana-Michela Renderse z evropské vývojové laboratoře Xeroxu s návrhem možné spolupráce na řešení tohoto problému. Zástupci NASA přitom doufali, že zkušenost Xeroxu se strojovým učením, lingvistikou a zpracováním textu pomohou zvýšit přesnost systému Clarissa při rozpoznávání příkazů v rámci sledování všech hlasových projevů astronautů.
„NASA si přála systém, který bude připraven reagovat na příkazy bez toho, aby musel být aktivován nějakým speciálním klíčovým slovem," vysvětluje Renders. „Proto nebylo možné využít „startrekovského" řešení v podobě oslovení systému specifickým výrazem před zadáním příkazu. Museli jsme vylepšit schopnost systému automaticky rozlišovat mezi příkazy a konverzací."
Technologie, kterou Renders použil pro splnění požadavků NASA, je také používána v Xeroxu pro zvýšenou přesnost kategorizace výsledků při rozpoznávání obsahu tištěných dokumentů a textových souborů. Technologie Xeroxu umožňuje systému Clarissa přesněji analyzovat každou větu. Clarrisa umí rozpoznat jednotlivá slova, ale také kompletní věty a slova v kontextu a dokáže reagovat na velké množství příkazů vyjádřených různým způsobem. Celý systém rozpoznávání řeči nyní zpracovává jednotlivá slova ve větě, definuje pravděpodobnost, podle které jsou jednotlivý slova správně identifikována, a následně aplikuje složitý algoritmus se schopností učit se na základě již získaných informací. Tento algoritmus vyhodnocuje jednotlivé fragmenty komunikace a rozhoduje, zda jde nebo nejde o příkaz podobně, jako antispamové systémy rozhodují, zda jde o legitimní zprávy nebo nevyžádanou reklamní poštu. Tento přístup výrazně zvyšuje schopnost systému odhalit rozdíl mezi příkazy zadávanými systému a běžnou komunikací uživatelů tohoto systému.
Vylepšení, která do Clarissy implementoval Xerox, podle Renderse snížila chybovost systému o více než polovinu. Clarissa v aktuálním stádiu vývoje podporuje rozpoznání 75 různých příkazů, které mohou být zadány prostřednictvím 260 slov. V plánu je další rozšiřování počtu dostupných příkazů a slovníku výrazů, na které Clarissa umí reagovat. „Některé příkazy jsou opravdu jednoduché, ale další jsou naopak poměrně složité," vysvětluje vedoucí projektu v laboratořích NASA Beth Ann Hockey. „Často jen řeknete ‚další' nebo ‚přejdi na krok osm'. Ale někdy také potřebujete říct něco jako ‚v 10:25 zruš nastavený alarm' nebo ‚přejdi na ověřovací režim u kroků tři až čtrnáct'."
„Spolupráce s Xeroxem na vývoji systému Clarissa ukazuje výhody, které nabízí partnerství mezi výzkumnými ústavy," dodává Beth Ann Hockey, vedoucí vývojového týmu NASA. První využití systému ve vesmíru se odehrálo 27. června 2005, kdy výcvik se systémem Clarissa absolvoval na palubě Mezinárodní vesmírné stanice astronaut John Phillips. Test systému byl úspěšný a nyní probíhá jeho vyhodnocování pracovníky NASA, kteří rozhodnou o harmonogramu implementace hlasově ovládaného počítačového systému do běžného vybavení ISS a dalších projektů.

Program ViaVoice – IBM

Nová technologie mění rozpoznávání řeči v běžnou konverzaci. S novým softwarem IBM Embedded ViaVoice 4.4 nemusí řidiči a uživatelé mobilů používat předdefinované příkazy, ale mohou mluvit přirozeně

Společnost IBM oznámila převratnou hlasovou technologii, která umožňuje řidičům automobilů a uživatelům mobilních zařízení používat přirozené mluvené příkazy, aniž by se museli učit konkrétní, předem určené povely.

Tato pokroková technologie, která je součástí právě uvolněného softwarového balíku IBM Embedded ViaVoice 4.4, je určena pro mobilní zařízení a pro navigační systémy v automobilech. Nový produkt má uživatelům poskytnout novou flexibilitu a přesnost při používání zabudovaných hlasových zařízení. Pro interakci se systémy rozpoznávání řeči se dosud uživatelé museli naučit, zapamatovat a používat pevně stanovený soubor frází a příkazů. Ovšem nová technologie IBM umožňuje řidiči například naladit rádio 104,3 FM mluvenými pokyny: „Naladit 104,3," „Nastavit rádio na 104,3," nebo „Změnit rádio na 104,3." Široké spektrum intuitivních povelů přeladí rádio na požadovanou frekvenci, takže si uživatel nemusí pamatovat seznam konkrétních příkazů.

Software IBM Embedded ViaVoice 4.4 obsahuje technologii „rozpoznávání volných příkazů," která pomocí vyspělého statistického modelování jazyka a sémantické interpretace dovoluje porozumět přirozenému jazyku při komunikaci mezi uživatelem a systémem rozpoznávání hlasu. Rozpoznávání volných příkazů umožňuje lidem používat intuitivní povely při ovládání rádia nebo navigačních systémů v automobilech nebo při práci s příručními zařízeními.

Nový produkt také dosahuje podstatně lepší celkovou přesnost rozpoznávání za různých hlukových podmínek. Používá totiž nové akustické modely, zdokonalené techniky trénování akustických modelů a vylepšenou detekci řeči a ticha. Právě ta zajišťuje odfiltrování krátkodobých šumů, způsobených například hrboly na vozovce, troubením nebo drncáním na železničním přejezdu.

Noví uživatelé mohou systém začít okamžitě používat bez toho, aby si pamatovali konkrétní slova nebo fráze, takže se mohou soustředit na řízení. Uživatelé handheldů mohou plynuleji provádět potřebné úkoly v rámci svých normálních činností. Nový systém nejen umožňuje používat volné příkazy, ale také tyto příkazy snadno rozpoznává ve více jazycích.

IBM Embedded ViaVoice verze 4.4 je špičková technologie řeči pro mobilní zařízení, například navigační systémy v autech, handsfree sady k telefonům, kapesní počítače (PDA) a další inteligentní zařízení. Aplikace v těchto zařízeních mohou používat technologii IBM buď pro automatické rozpoznávání řeči (ASR), kdy jsou příkazy zadávány přirozenou řečí, nebo pro syntézu řeči z textu (TTS), kdy syntetický hlas čte text a další informace z mobilního zařízení.

IBM ViaVoice Pro USB Edition je software, který uživatelům PC umožní diktovat text, editovat a opravovat jej. Je kompatibilní s Windows XP i s Microsoft Office. Dále je možné tvořit různá makra. Cena Pro USB Edition 190,- $. Moduly ViaVoice se používají v jazykových počítačových učebnicích pro kontrolu výslovnosti. [3]

Za deset let bude podle mezinárodních analýz běžné, že počítače umožní uživateli inteligentně komunikovat a zaznamenávat jeho hlasové pokyny.
Zcela běžný budou také software, který rozpoznají váš rukopis a budou s ním umět pracovat.

Otázky a úkoly:
1. Najděte na internetu výraz RFID .
2. Co obsahuje internetová adresa **http://www.oou.cz** ?
3. Najděte na **http://www.uoou.cz**stanoviska Úřadu pro ochranu osobních údajů
4. Porovnejte kompetence Úřadu pro ochranu osobních údajů a Telekomunikačního úřadu (**http://www.ctu.cz**)
5. Zkuste experimentovat s demoverzemi firem, které nabízejí software pro ovládání počítače hlasem.
6. Najděte na http://www.gartner.comnejnovější technologické trendy
7. Co je to rizikový kapitál? (Najděte odpověď na internetu.)
8. Proveďte analýzu webové stránky http://www.tcav.cz, jaké služby pro podnikatele v nových trendech nabízí?
9. Proveďte analýzu webové stránky http://www.wfs.com, jaké informace pro podnikatele v nových trendech nabízí?
10. Čím se zabývá společnost IEEE Spektrum?

Klíčová slova: RFID, ochrana osobních údajů, ovládání počítače hlasem

10 První certifikační autorita

ICA: první certifikační autorita

Ing. Petr Budiš, Ph.D. se narodil 24. února 1970. Absolvoval Elektrotechnickou fakultu VUT v Brně. Studium ukončil v roce 1994. Poté nastoupil v PVT, a.s. na pozici programátora. Zároveň zahájil studium pedagogiky a psychologie, které ukončil státní zkouškou a postgraduální studium, které ukončil úspěšným složením doktorandské zkoušky (Ph.D.) V PVT, a.s. postupně prošel pozicemi vedoucí projektu, ředitel produktu, ředitel vývoje a ředitel divize. Vedl projekty zejména v oblasti bankovnictví a bezpečnosti, jako IPB Homebanking a Internetbanking a dále projekty v oblasti bezpečné komunikace a CA (projekt I.CA). Zastával pozici předsedy dozorčí rady společnosti DTCA, a.s. a člena dozorčí rady PVT-Slovakia, s.r.o..
V současné době je předsedou představenstva a ředitelem společnosti První certifikační autorita, a.s.

Budování a současnost společnosti I.CA
Certifikáty a certifikační autorita – vhled do problematiky

Stále více se pro předávání informací používají elektronické cesty. Téměř každá banka nabízí svým klientům komunikaci po Internetu. Obecně se zdá, že rozvoji elektronické komunikace nic nebrání, a je to jen otázka času a přiměřených investic. Je to však opravdu tak jednoduché?

Bohužel není. Jestliže přijdete do banky, musíte před provedením operace s vaším účtem především prokázat kdo jste a následně také to, že jste k dané operaci oprávněn. Po Internetu to však není tak jednoduché. Toho, kdo je na opačném konci nevidíme, natož aby se nám prokazoval nějakým dokladem. V případě využití moderních komunikačních technologií mluvíme o elektronickém průkazu totožnosti a elektronickém podpisu. Řešení založená na elektronickém podpisu mohou za určitých okolností plně nahradit použití vlastnoručního podpisu, se všemi důsledky vyplývajícími z jeho použití.

Elektronický průkaz totožnosti se nazývá certifikát. Hlavním úkolem tohoto dokumentu je neoddělitelně spojit fyzickou totožnost daného subjektu s totožností elektronickou, prezentovanou jedinečnými, digitálními daty. Certifikát obsahuje i podobné údaje, jako nám běžně známý průkaz totožnosti, tedy občanský průkaz. V certifikátu je zpravidla uvedeno jméno a příjmení, bližší identifikační údaje, jako jsou např. firma a adresa, aby bylo možné subjekt identifikovat jednoznačně a dále jednoznačné číslo certifikátu, opět podobně jako u OP. Velice důležitou položkou certifikátu je doba platnosti a jednoznačná identifikace vydavatele certifikátu. Ta je na rozdíl od desetileté platnosti OP zpravidla kratší. Je to daň bezpečnosti komunikace.

Aby měl certifikát smysl a mohl plnit svoje poslání, musí obsahovat elektronickou část naší totožnosti, tedy jedinečná data. Tato data jsou pro běžného uživatele nic neříkajícím obsahem, změtí nečitelných znaků. Této části certifikátu zase lépe rozumí váš počítač.

Použití certifikátů v praxi je velice jednoduché. Standardní prostředky pro přístup k Internetu mají podporu využívání certifikátů v sobě již implementovánu. Poslání zabezpečeného, elektronicky podepsaného, e-mailu je otázkou stisku jediného tlačítka a zabezpečená webovská komunikace může probíhat dokonce i zcela automaticky.

Institucí vydávající certifikáty je certifikační autorita. Certifikační autorita provádí několik základních úkonů. Je to především přijímání žádostí o certifikát a následné vydání certifikátu. Aby bylo možné certifikátu důvěřovat, musí při jeho vydávání certifikační autorita především důvěryhodným způsobem provézt ověření totožnosti žadatele. Tento krok pak prakticky nahrazuje při následné komunikaci s certifikáty ověření totožnosti. Vašeho komunikačního partnera prověří certifikační autorita za vás. To vyžaduje osobní účast žadatele o certifikát na pracovišti certifikační autority. Při velkém počtu certifikátů a žadatelů by bylo nemožné, aby všichni žadatelé přišli na jediné místo. Těžko si představit, že by byly občanské průkazy vydávány pouze na pražském ředitelství policie. Proto certifikační autorita zřizuje svoje detašovaná pracoviště, takzvané registrační autority. Získání certifikátu je obdobné, jako je získání například elektronického pasu, pouze se provádí na počkání.

Preambule

První certifikační autorita, a.s. (dále jen I.CA) byla založena v roce 2001 jako společnost, jejíž náplní je zajišťování činností bezprostředně souvisejících s poskytováním služeb certifikační autority. Určujícím motivem pro tento krok byly mimo jiné zvyšující se potřeby trhu a rozsah požadavků klientů, tedy v zásadě jakási mezera na trhu.

Projekt certifikační autority byl zahájen již v roce 1996 a dnes má za sebou více jak devítiletou dobu nepřetržitého provozu. Lze konstatovat, že se I.CA stala prvním komerčním poskytovatelem komplexních služeb vydávání a správy certifikátů v České republice a jedním z prvních v Evropě. Rozhodujícím faktorem pro vysokou kvalitu poskytovaných služeb je využívání vlastního know-how a zkušeností, nabytých v rámci realizace a provozu tohoto projektu.

Úřad pro ochranu osobních údajů udělil společnosti První certifikační autorita, a.s. akreditaci pro výkon činnosti akreditovaného poskytovatele certifikačních služeb ve smyslu Zákona č.227/2000 Sb., o elektronickém podpisu, a to s účinností od 18. 3. 2002.

Osvědčení pro výkon akreditovaných certifikačních činností získala I.CA také v létě roku 2004 pro Slovenskou republiku, kde spolupracuje s partnerskou společností D.Trust Certifikačná autorita, a.s.

Pozice na trhu

I.CA je v současnosti největším poskytovatelem certifikačních služeb v České republice v oblasti komerčních certifikátů a kvalifikovaných certifikátů. I.CA je dále jediným poskytovatelem služby kvalifikovaných časových razítek.

Pro zajištění realizace požadavků svých klientů provozuje infrastrukturu tzv. Registračních autorit a v současnosti jich spravuje více než 400 na území České republiky a Slovenska. Významnou konkurenční výhodou je jejich plošné celorepublikové rozmístění. Tato kontaktní pracoviště I.CA umožňují optimální dostupnost nabízených produktů a služeb.

Mezi obchodní partnery I.CA patří přední světoví i tuzemští dodavatelé kryptografických technologií. Spolupráce s nimi umožňuje I.CA nabízet klientům komfortní služby na nejvyšším stupni bezpečnosti, reagující na poslední světové trendy.

Historie a současnost společnosti I.CA

Vlastní projekt certifikační autority (projekt I.CA) byl zahájen v roce 1996 v rámci společnosti PVT, a.s.. V té době bylo využití elektronické komunikace a zejména Internetu pro komerční projekty v plenkách. Jednoznačně největším problémem byla anonymita komunikujících stran a nejasnost jejich právního vztahu. Bylo vypracováno mnoho právních rozborů, popisujících složitost regulace Internetu a odpovědností poskytovatelů jednotlivých služeb s Internetem spojených. Navíc se začaly objevovat konkrétní projekty, které vyžadovaly vyřešení komerčního využití elektronické komunikace.

Mezi prvními byly základní verze elektronického bankovnictví, tehdy prezentované především Investiční a poštovní bankou, a dále požadavky z oblasti kapitálových trhů. Tyto projekty byly navíc dostatečně finančně silné, aby umožnily vývoj u nás do té doby nepoužívaných a neznámých technologií. Většina aktuálně používaných technologií pro zabezpečení elektronické komunikace byla v rukou armády a obdobných složek, a tudíž pro komerční prostředí nedostupná. Situaci navíc komplikovalo i embargo na vývoz bezpečnostních technologií z USA. Technologické firmy si začínaly vzniklou příležitost uvědomovat, každá z nich však volila jiný přístup a standardizace rozhodně nebyla prioritní.

V první etapě jsme se rozhodli pro detailní studium dostupných norem, z nichž valná většina byla pouze ve fázi draftů a doporučení. Volba padla na kombinaci technologie symetrické a asymetrické kryptografie, na technologii nazývanou digitální podpis, dnes známou spíše jako elektronický podpis. Tato technologie umožňovala splnit všechny požadavky uvažovaných projektů, nebyla nedostupná a měla ambice stát se standardem, což pro nás byla jasná podmínka dalšího komerčního úspěchu.

Po prezentaci v top managementu společnosti PVT byl schválen podnikatelský záměr na vybudování PKI infrastruktury a zejména certifikační autority jako klíčového prvku celého řešení,. Bylo nutné v rámci běžících projektů zajistit financování rozběhu projektu, což se také podařilo. Koncem roku 1996 byl k dispozici první technický projekt a v polovině roku 1997 byly vydány první testovací certifikáty. Zároveň bylo nutné vypracovat mnoho dokumentů, počínaje veřejnými dokumenty popisujícími jak s certifikáty pracovat a konče interní bezpečnostní dokumentací. Celý realizační tým, pracující na projektu I.CA, měl tehdy 4, respektive 5 členů.

Koncem roku 1997 byl projekt spuštěn v rutinním provozu pro uzavřené projekty a počátkem roku 1998 jsme otevřeli první, veřejně dostupnou registrační autoritu. Ekonomické výsledky projektu certifikační autorita nebyly v letech 1996 až 1999 sledovány samostatně, ale jen v rámci běžících projektů. V těchto letech nabízela I.CA pouze služby vydávání certifikátů,

kterých byly vydávány stovky ročně.

V roce 1998 byl v ČR zahájen proces „legalizace“ elektronického podpisu. Prostřednictvím sdružení SPIS, politiků a odborné veřejnosti byly zahájeny práce na Zákonu o elektronickém podpisu a následně i vyhlášek k zákonu. Byla vytvořena pracovní skupina, v níž jsme měli zastoupení. Mohli jsme se již podělit o poměrně rozsáhlé praktické zkušenosti.

Zákon vstoupil v platnost v roce 2000 a ČR se tak stala třetí zemí na světě, která upravila používání elektronického popisu v legislativě. To bylo jasným potvrzením správnosti vybrané cesty a zvoleného modelu řešení (projekt I.CA) a zároveň startem nových obchodních aktivit. Po vstupu zákona v platnost bylo možné a často i nutné využívat elektronický podpis nejen v oblasti komerční komunikace, ale i v oblasti komunikace občana a státních institucí. Tím přišel nový impuls k rozvoji trhu s certifikáty.

Vzhledem k tomu, že v době vzniku legislativy byl projekt I.CA současně již největší certifikační autoritou v ČR, bylo zřejmé, že rozšíření o oblast kvalifikovaných certifikátů je dalším přirozeným krokem ve vývoji služeb poskytovaných I.CA.

Pro poskytování těchto služeb bylo nutné získat tzv. akreditaci v souladu s požadavky zákona. Zde bylo nutné zajistit jeden ze zákonných požadavků, a to ten, že společnost, žádající o akreditaci, nesmí poskytovat jiné služby. Tento impuls a současně skutečnost, že produkt I.CA se velmi úzce profiloval v oblasti bezpečné komunikace, vedly v březnu roku 2001 ke vzniku samostatné společnosti První certifikační autorita, a.s. jako dceřiné společnosti PVT, a.s. Jako samostatný subjekt se mohla společnost již plně věnovat přípravě na získání akreditace a rozšíření svých služeb. To se povedlo v březnu roku 2002, kdy se I.CA stala první certifikační autoritou v ČR, která akreditaci získala.

Také na Slovensku vyvrcholily v roce 2002 několik let trvající přípravy legislativy vznikem zákona. I.CA v této době již hledala možnosti poskytování služeb na trhu Slovenské republiky a výsledkem byl vznik společnosti D.Trust Certifikačná autorita, a.s. (dále jen DTCA), kde se akcionářem stala společnost PVT, a.s., Tatrabanka, a.s. a společnost Ditec, a.s. DTCA se stala poskytovatelem služeb I.CA na Slovensku a v roce 2004 také získala akreditaci.

V roce 2004 společnost První certifikační autorita, a.s. zaznamenala několik významných událostí. Tou nejvýznamnější byla změna v akcionářské struktuře společnosti. Novými akcionáři se kromě PVT, a.s. staly také společnosti ČSOB, a.s., Česká spořitelna, a.s., Eurotel Praha, spol. s.r.o. a STÁTNÍ TISKÁRNA CENIN, státní podnik.

Vstup silných akcionářů do vlastnické struktury společnosti byl jasným signálem o perspektivě v oblasti elektronické komunikace a elektronického podpisu. Pozitivní trendy jsou zřejmé také z rostoucího počtu klientů a spolupracujících firem.

Technologický vývoj

Z technologického pohledu lze vývoj společnosti považovat od svého vzniku spíše za extenzivní. Technologie certifikační autority je už dnes do značné míry spojena s obecně platnými a zaběhlými normativy, a také proto nelze očekávat zásadní, revoluční změny. Velká pozornost je věnována zejména uživatelskému komfortu certifikačních služeb, protože to byla jedna z překážek masivního rozšíření elektronického podpisu v běžném životě.

Přelom nastal v roce 2004, kdy bylo zahájeno poskytování služby vydávání časových razítek. Tato služba sice nemá přímou vazbu na technologii certifikační autority, ale její využití je nutné pro zajištění bezpečné komunikace v aktuálním pojetí, tedy rychlých a průkazných přenosů informací. Časové razítko je nástroj, který hodnověrným způsobem zajišťuje přiřazení aktuálního časového údaje k existujícím datům, informacím, souborům atd.

Spojení nezpochybnitelného časového údaje a konkrétních dat je nezbytné zejména pro účely jejich zpětného ověřování v budoucnosti. Časová razítka jsou využívána především při práci s elektronickými dokumenty či daty, u kterých je nutné jednoznačné doložení času, ve kterém dokument v daném tvaru existoval. V praxi se jedná především o smluvní dokumenty, různá elektronická podání nebo také logové záznamy o činnosti systémů. Časové razítko pak nejen zajišťuje jednoznačné doložení času, ale také to, že dokument či data není možné zpětně změnit, aniž by došlo k neplatnosti příslušného časového razítka.

Služba časových razítek byla v roce 2005 poskytována formou komerčních časových razítek. Na základě žádosti, podané Ministerstvu informatiky České republiky, byl zahájen proces udělení akreditace. Proces byl úspěšně ukončen k 1.2.2006, kdy I.CA získala souhlas MIČR pro vydávání kvalifikovaných časových razítek.

Pohled do ekonomiky společnosti

Úspěšnost projektu I.CA i společnosti První certifikační autorita, a.s. lze dokumentovat vývojem hospodářských výsledků za celé období působnosti společnosti od jejího založení v roce 2001. Ve všech pěti předchozích letech dosáhla První certifikační autorita, a.s. zisku, rovněž tak i v pololetí roku 2007. Celkový výsledek hospodaření před zdaněním za celé období dosahuje zhruba 24 mil.Kč, což prezentuje zisk v průměru více jak 4 mil.Kč ročně.

Tržby za prodej vlastních výrobků a služeb mají od počátku činnosti společnosti rostoucí trend, v roce 2001 bylo dosaženo zhruba 13,5 mil.Kč tržeb, v posledních letech se však výše tržeb ustálila již na cca 40 mil.Kč. Očekávaná skutečnost tržeb v roce 2006 je ve výši cca 55 mil.Kč

Vývojem činností a rozšiřováním produktů společnosti se měnila rovněž struktura tržeb. Na začátku tvořily rozhodující podíl především tržby za prodej a za obnovu komerčních certifikátů. Společnost byla v té době orientována zejména na plnění služeb v rámci elektronického bankovnictví pro ČSOB. Postupně se rozšiřovaly výsledky společnosti o tržby za další produkty a služby, po získání akreditace za kvalifikované certifikáty a dále zejména za dodávky čipových karet Starcos jaké média pro ukládání certifikátů, za dodávky klientských čteček apod.

Významným přínosem pro tržby společnosti se staly dále dodávky registračních autorit, a to

nejen tržbami za jejich vlastní prodej, instalaci a školení operátorů, ale následně i tržbami za vydané certifikáty. V roce 2004 byl zahájen úspěšný projekt vydávání časových razítek, které významným způsobem využívá zejména Česká spořitelna a Slovenský colný úrad. V roce 2006 získala společnost První certifikační autorita, a.s. akreditaci MIČR a od dubna 2006 tak vydává kvalifikovaná časová razítka. Tržby za časová razítka mají trvale rostoucí trend.

Další oblastí, kde se zejména v roce 2006 daří navyšovat tržby společnosti, jsou softwarová řešení pro zákazníky, tedy účast I.CA na jejich projektech. Vedle dodávaných standardních produktů a služeb se tak První certifikační autorita, a.s. uplatňuje nově dodávkami projekčních řešení. Příkladem jsou zejména projekty pro státní správu, řešení pro MPSV a další. Naplňuje se tak cíl společnosti a její velká přednost, kterou je poskytování komplexních služeb podle potřeb zákazníků včetně účasti na významných projektech.

Cílem v oblasti rozvíjení hospodářských výsledků společnosti, zakotveném ve schválené Koncepci na období 2006 – 2009, je zejména udržet pozici na trhu České republiky a dále rozvíjet výši tržeb u zákazníků na Slovensku, kde doposud působila společnost První certifikační autorita, a.s. prostřednictvím spolupráce s DTCA. Získání přímé akreditace pro slovenský trh se předpokládá ještě v letošním roce.

První certifikační autorita, a.s. dále uvažuje o získání akreditace i v dalších zemích, zejména Evropské unie, např. v Polsku. Již dnes využívá certifikáty I.CA zhruba 1.100 občanů jiných států z více jak 80 zemí světa. Jednáním se zastoupeními zahraničních IT firem pro Českou republiku, např. s TietoEnator či Centics, pak počítá První certifikační autorita, a.s. i se zapojením se nově připravovaných projektů, směřovaných jak na Český trh, tak i na trhy zahraniční. Tento postup a jeho úspěšnost bude do značné míry záviset na vývoji legislativy.

Současný trend společnosti je nastaven na její trvalý růst a prosperitu a První certifikační autorita, a.s. má veškeré předpoklady splnění těchto cílů.

První certifikační autorita, a.s., sídlí v Praze, kde vedle vedení společnosti jsou soustředěni pracovníci zajišťující především oblast rozvoje společnosti, bezpečnosti, tvorby dokumentů společnosti (politiky, směrnice, bezpečnostní normy) a dále zajišťující obchodní aktivity, podporu zákazníkům formou helpdesku vč. technologické podpory při spouštění nových projektů.

Provozní zabezpečení I.CA je soustředěno v Otrokovicích, kde je ve dvousměnném provozu zajištěna kontrola podaných žádostí, přičemž pro konkrétní potřeby zákazníků je po dohodě zajišťována tato služba i mimo běžnou provozní dobu, výjimečně i o víkendech. Provozní zabezpečení zahrnuje stálý monitoring provozu všech systémů I.CA, zpracovávání přehledů zneplatněných certifikátů (CRL), kontrolu systému vydávajícího kvalifikovaná časová razítka atd. Rovněž pracovníci provozu Otrokovice poskytují podporu partnerům, zákazníkům a projektům, ve kterých se vydávající certifikáty I.CA.

V souvislosti se snahou mít pod „vlastní kontrolou“ vývoj systémů I.CA vytváří od 1.8.2006 společnost První certifikační autorita, a.s. vlastní vývojový tým se sídlem v Brně. Od působení tohoto týmu si slibujeme vedle operativních řešení úpravy systémů I.CA podle potřeb daných

platnou legislativou a strategií společnosti také účast projektantů na jednáních u zákazníků a účast na prezentacích produktů a služeb společnosti.

Ze silných stránek společnosti lze vyzdvihnout především znalost problematiky poskytování certifikačních služeb a vysokou odbornost pracovníků společnosti, dále rozsah a portfolio služeb, technologickou vyspělost, schopnost reakce na měnící se požadavky trhu, velké množství kontaktních míst po celém území ČR, poskytování služeb mobilních registračních autorit I.CA a silnou akcionářskou základnu, která reprezentuje významnou ekonomickou i sociálně-politickou sílu, v neposlední řadě pak i množství obchodních vazeb a know-how.

11 Dvě vybrané legislativní normy z oblasti ICT

ZÁKON
ze dne 29. června 2000

o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)

Změna: 226/2002 Sb.
Změna: 517/2002 Sb.
Změna: 440/2004 Sb.
Změna: 635/2004 Sb.
Změna: 501/2004 Sb. , 444/2005 Sb.

Parlament se usnesl na tomto zákoně České republiky:

ČÁST PRVNÍ

ELEKTRONICKÝ PODPIS

§ 1

Účel zákona

Tento zákon upravuje v souladu s právem Evropských společenství 1) používání elektronického podpisu, elektronické značky, poskytování certifikačních služeb a souvisejících služeb poskytovateli usazenými na území České republiky, kontrolu povinností stanovených tímto zákonem a sankce za porušení povinností stanovených tímto zákonem.

§ 2

Vymezení některých pojmů

Pro účely tohoto zákona se rozumí
a) elektronickým podpisem údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě,

b) zaručeným elektronickým podpisem elektronický podpis, který splňuje následující požadavky1. je jednoznačně spojen s podepisující osobou,
2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
4. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat,

c) elektronickou značkou údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které splňují následující požadavky1. jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného

systémového certifikátu,
2. byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou,
3. jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat,

d) datovou zprávou elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích, používaných při zpracování a přenosu dat elektronickou formou,

e) podepisující osobou fyzická osoba, která je držitelem prostředku pro vytváření elektronických podpisů a jedná jménem svým nebo jménem jiné fyzické či právnické osoby,

f) označující osobou fyzická osoba, právnická osoba nebo organizační složka státu, která drží prostředek pro vytváření elektronických značek a označuje datovou zprávu elektronickou značkou,

g) držitelem certifikátu fyzická osoba, právnická osoba nebo organizační složka státu, která požádala o vydání kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu pro sebe nebo pro podepisující nebo označující osobu a které byl certifikát vydán,

h) poskytovatelem certifikačních služeb fyzická osoba, právnická osoba nebo organizační složka státu, která vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy,

i) kvalifikovaným poskytovatelem certifikačních služeb poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty nebo kvalifikované systémové certifikáty nebo kvalifikovaná časová razítka nebo prostředky pro bezpečné vytváření elektronických podpisů (dále jen "kvalifikované certifikační služby") a splnil ohlašovací povinnost podle § 6,

j) akreditovaným poskytovatelem certifikačních služeb poskytovatel certifikačních služeb, jemuž byla udělena akreditace podle tohoto zákona,

k) certifikátem datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování elektronických podpisů s podepisující osobou a umožňuje ověřit její identitu, nebo spojuje data pro ověřování elektronických značek s označující osobou a umožňuje ověřit její identitu,

l) kvalifikovaným certifikátem certifikát, který má náležitosti podle § 12 a byl vydán kvalifikovaným poskytovatelem certifikačních služeb,

m) kvalifikovaným systémovým certifikátem certifikát, který má náležitosti podle § 12a a byl vydán kvalifikovaným poskytovatelem certifikačních služeb,

n) daty pro vytváření elektronických podpisů jedinečná data, která podepisující osoba používá k vytváření elektronického podpisu,

o) daty pro ověřování elektronických podpisů jedinečná data, která se používají pro ověření elektronického podpisu,

p) daty pro vytváření elektronických značek jedinečná data, která označující osoba používá k vytváření elektronických značek,

q) daty pro ověřování elektronických značek jedinečná data, která se používají pro ověření elektronických značek,

r) kvalifikovaným časovým razítkem datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem,

s) prostředkem pro vytváření elektronických podpisů technické zařízení nebo programové vybavení, které se používá k vytváření elektronických podpisů,

t) prostředkem pro ověřování elektronických podpisů technické zařízení nebo programové vybavení, které se používá k ověřování elektronických podpisů,

u) prostředkem pro bezpečné vytváření elektronických podpisů prostředek pro vytváření elektronického podpisu, který splňuje požadavky stanovené tímto zákonem,

v) prostředkem pro bezpečné ověřování elektronických podpisů prostředek pro ověřování podpisu, který splňuje požadavky stanovené tímto zákonem,

w) nástrojem elektronického podpisu technické zařízení nebo programové vybavení, nebo jejich součásti, používané pro zajištění certifikačních služeb nebo pro vytváření nebo ověřování elektronických podpisů,

x) prostředkem pro vytváření elektronických značek zařízení, které používá označující osoba pro vytváření elektronických značek a které splňuje další náležitosti stanovené tímto zákonem,

y) elektronickou podatelnou pracoviště orgánu veřejné moci určené pro příjem a odesílání datových zpráv,

z) akreditací osvědčení, že poskytovatel certifikačních služeb splňuje podmínky stanovené tímto zákonem pro výkon činnosti akreditovaného poskytovatele certifikačních služeb.

§ 3

Soulad s požadavky na podpis

(1) Datová zpráva je podepsána, pokud je opatřena elektronickým podpisem. Pokud se neprokáže opak, má se za to, že se podepisující osoba před podepsáním datové zprávy s jejím obsahem seznámila.

(2) Použití zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu a vytvořeného pomocí prostředku pro bezpečné vytváření podpisu umožňuje ověřit, že datovou zprávu podepsala osoba uvedená na tomto kvalifikovaném certifikátu.

§ 3a

(1) Použití elektronické značky založené na kvalifikovaném systémovém certifikátu a vytvořené pomocí prostředku pro vytváření elektronických značek umožňuje ověřit, že datovou zprávu označila touto elektronickou značkou označující osoba.

(2) Pokud označující osoba označila datovou zprávu, má se za to, že tak učinila automatizovaně bez přímého ověření obsahu datové zprávy a vyjádřila tím svou vůli.

§ 4

Soulad s originálem

Použití zaručeného elektronického podpisu nebo elektronické značky zaručuje, že dojde-li k porušení obsahu datové zprávy od okamžiku, kdy byla podepsána nebo označena, toto porušení bude možno zjistit.

§ 5

Povinnosti podepisující osoby

(1) Podepisující osoba je povinna

a) zacházet s prostředky, jakož i s daty pro vytváření zaručeného elektronického podpisu s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití,

b) uvědomit neprodleně poskytovatele certifikačních služeb, který vydal kvalifikovaný certifikát, o tom, že hrozí nebezpečí zneužití jejích dat pro vytváření zaručeného elektronického podpisu.

(2) Za škodu způsobenou porušením povinností podle odstavce 1 odpovídá podepisující osoba podle zvláštních právních předpisů. 1a) Odpovědnosti se však zprostí, pokud prokáže, že ten, komu vznikla škoda, neprovedl veškeré úkony potřebné k tomu, aby si ověřil, že zaručený elektronický podpis je platný a jeho kvalifikovaný certifikát nebyl zneplatněn.

§ 5a

Povinnosti označující osoby

(1) Označující osoba je povinna
a) zacházet s prostředkem, jakož i s daty pro vytváření elektronických značek s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití,

b) uvědomit neprodleně poskytovatele certifikačních služeb, který vydal kvalifikovaný systémový certifikát, o tom, že hrozí nebezpečí zneužití jejích dat pro vytváření elektronických značek.

(2) Označující osoba je povinna zajistit, aby prostředek pro vytváření elektronických značek, který používá, splňoval požadavky stanovené tímto zákonem.

(3) Za škodu způsobenou porušením povinnosti podle odstavce 1 odpovídá označující osoba, i když škodu nezavinila, podle zvláštních právních předpisů, 1a) odpovědnost za vady podle zvláštních předpisů tím není dotčena. 1a) Odpovědnosti se však zprostí, pokud prokáže, že ten, komu vznikla škoda, neprovedl veškeré úkony potřebné k tomu, aby si ověřil, že elektronická značka je platná a její kvalifikovaný systémový certifikát nebyl zneplatněn.

§ 5b

Povinnosti držitele certifikátu

Držitel certifikátu je povinen bez zbytečného odkladu podávat přesné, pravdivé a úplné informace poskytovateli certifikačních služeb ve vztahu ke kvalifikovanému certifikátu a ve vztahu ke kvalifikovanému systémovému certifikátu.

§ 6

Kvalifikovaný poskytovatel certifikačních služeb

(1) Kvalifikovaný poskytovatel certifikačních služeb je povinen
a) zajistit, aby se každý mohl ujistit o jeho identitě a jeho kvalifikovaném systémovém certifikátu, na jehož základě označuje vydané kvalifikované certifikáty nebo kvalifikované systémové certifikáty a seznamy certifikátů, které byly zneplatněny, nebo kvalifikovaná časová razítka,

b) zajistit, aby poskytování kvalifikovaných certifikačních služeb vykonávaly osoby s odbornými znalostmi a kvalifikací nezbytnou pro poskytování kvalifikované certifikační služby a obeznámené s příslušnými bezpečnostními postupy,

c) používat bezpečné systémy a bezpečné nástroje elektronického podpisu, zajistit dostatečnou bezpečnost postupů, které tyto systémy a nástroje podporují, a zajistit dostatečnou kryptografickou bezpečnost těchto nástrojů; systémy a nástroje jsou považovány za bezpečné, pokud odpovídají požadavkům stanoveným tímto zákonem a prováděcí vyhláškou, nebo pokud splňují požadavky technických norem uvedených v rozhodnutí Komise vydaném na základě článku 3 (5) směrnice 99/93/ES,

d) používat bezpečné systémy pro uchovávání kvalifikovaných certifikátů a kvalifikovaných systémových certifikátů nebo kvalifikovaných časových razítek v ověřitelné podobě takovým způsobem, aby záznamy nebo jejich změny mohly provádět pouze pověřené osoby, aby bylo možno kontrolovat správnost záznamů a aby jakékoliv technické nebo programové změny porušující tyto bezpečnostní požadavky byly zjevné,

e) mít po celou dobu své činnosti k dispozici dostatečné finanční zdroje nebo jiné finanční zajištění na provoz v souladu s požadavky uvedenými v tomto zákoně a s ohledem na riziko vzniku odpovědnosti za škodu,

f) před uzavřením smlouvy o poskytování kvalifikovaných certifikačních služeb s osobou, která žádá o poskytování služeb podle tohoto zákona, informovat tuto osobu písemně o přesných podmínkách pro využívání kvalifikovaných certifikačních služeb, včetně případných omezení

pro jejich použití, o podmínkách reklamací a řešení vzniklých sporů a o tom, zda je, či není akreditován Ministerstvem informatiky (dále jen "ministerstvo") podle § 10; tyto informace lze předat elektronicky.

(2) Není-li poskytovatel certifikačních služeb akreditován ministerstvem, je povinen ohlásit ministerstvu nejméně 30 dnů před zahájením poskytování kvalifikované certifikační služby, že ji bude poskytovat, a okamžik, kdy její poskytování zahájí. Zároveň předá ministerstvu k ověření svůj kvalifikovaný systémový certifikát uvedený v odstavci 1 písm. a).

(3) Pokud byla kvalifikovanému poskytovateli certifikačních služeb, který získal akreditaci podle § 10 tohoto zákona, akreditace ministerstvem odňata, je povinen bez prodlení informovat o této skutečnosti subjekty, kterým poskytuje své kvalifikované certifikační služby, a další dotčené osoby.

(4) Kvalifikovaný poskytovatel certifikačních služeb poskytuje služby podle tohoto zákona na základě smlouvy. Smlouva musí být písemná.

(5) Kvalifikovaný poskytovatel certifikačních služeb uchovává informace a dokumentaci související s poskytovanými kvalifikovanými certifikačními službami podle tohoto zákona, zejména
a) smlouvu o poskytování kvalifikované certifikační služby, včetně žádosti o poskytování služby,

b) vydaný kvalifikovaný certifikát, vydaný kvalifikovaný systémový certifikát nebo vydané kvalifikované časové razítko,

c) kopie předložených osobních dokladů podepisující osoby nebo dokladů, na jejichž základě byla ověřena identita označující osoby,

d) potvrzení o převzetí kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu držitelem, případně jeho souhlas se zveřejněním kvalifikovaného certifikátu v seznamu vydaných kvalifikovaných certifikátů,

e) prohlášení držitele certifikátu o tom, že mu byly poskytnuty informace podle odstavce 1 písm. f),

f) dokumenty a záznamy související s životním cyklem vydaného kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu, jejichž náležitosti upřesní prováděcí vyhláška.

(6) Veškeré informace a dokumentaci o poskytovaných službách podle tohoto zákona uchovává kvalifikovaný poskytovatel certifikačních služeb po dobu nejméně 10 let. Kvalifikovaný poskytovatel je povinen zajistit uchovávané informace a dokumentaci před ztrátou, zneužitím, zničením nebo poškozením za podmínek, které upřesní prováděcí vyhláška. Informace a dokumentaci podle věty první může kvalifikovaný poskytovatel certifikačních služeb pořizovat a uchovávat v elektronické podobě. Pokud tento zákon nestanoví jinak, postupuje se při nakládání s informacemi a dokumentací podle zvláštního právního předpisu. 2)

(7) Zaměstnanci kvalifikovaného poskytovatele certifikačních služeb, případně jiné fyzické osoby, které přicházejí do styku s osobními údaji a daty pro vytváření elektronických

podpisů podepisujících osob a elektronických značek označujících osob, jsou povinni zachovávat mlčenlivost o těchto údajích a datech a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení těchto údajů a dat. Povinnost mlčenlivosti trvá i po skončení pracovního nebo jiného obdobného poměru nebo po provedení příslušných prací; uvedené osoby může zbavit mlčenlivosti ten, v jehož zájmu tuto povinnost mají, nebo soud.

§ 6a

Povinnosti kvalifikovaného poskytovatele certifikačních služeb při vydávání kvalifikovaných certifikátů a kvalifikovaných systémových certifikátů

(1) Kvalifikovaný poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty nebo kvalifikované systémové certifikáty (dále jen "certifikáty vydané jako kvalifikované"), je povinen
a) zajistit, aby certifikáty jím vydané jako kvalifikované obsahovaly všechny náležitosti stanovené tímto zákonem,

b) zajistit, aby údaje uvedené v certifikátech jím vydaných jako kvalifikované byly přesné, pravdivé a úplné,

c) před vydáním certifikátu jako kvalifikovaného bezpečně ověřit odpovídajícími prostředky identitu podepisující osoby nebo identitu označující osoby, případně i její zvláštní znaky, vyžaduje-li to účel takového certifikátu,

d) zjistit, zda v okamžiku podání žádosti o vydání certifikátu jako kvalifikovaného měla podepisující osoba data pro vytváření elektronických podpisů odpovídající datům pro ověřování elektronických podpisů nebo označující osoba data pro vytváření elektronických značek odpovídající datům pro ověřování elektronických značek, která obsahuje žádost o vydání certifikátu,

e) zajistit provozování bezpečného a veřejně přístupného seznamu certifikátů vydaných jako kvalifikované, k jejichž zveřejnění dal držitel certifikátu souhlas v souladu s § 6 odst. 5 písm. d), a zajistit dostupnost tohoto seznamu i dálkovým přístupem a údaje v seznamu obsažené při každé změně bez zbytečného odkladu aktualizovat,

f) zajistit provozování bezpečného a veřejně přístupného seznamu certifikátů vydaných jako kvalifikované, které byly zneplatněny, a to i dálkovým přístupem,

g) zajistit, aby datum a čas s uvedením hodiny, minuty a sekundy, kdy je certifikát vydaný jako kvalifikovaný vydán nebo zneplatněn, mohly být přesně určeny,

h) přijmout odpovídající opatření proti zneužití a padělání certifikátů vydaných jako kvalifikované,

i) poskytovat na vyžádání třetím osobám podstatné informace o podmínkách pro využívání certifikátů vydaných jako kvalifikované, včetně omezení pro jejich použití, a informace o tom, zda je, či není akreditován ministerstvem; tyto informace lze poskytovat elektronicky.

(2) Pokud kvalifikovaný poskytovatel certifikačních služeb, který vydává certifikáty

jako kvalifikované, vytváří pro podepisující osobu data pro vytváření elektronických podpisů nebo pro označující osobu data pro vytváření elektronických značek,
a) musí zajistit utajení těchto dat před jejich předáním, nesmí tato data kopírovat a uchovávat je déle, než je nezbytné,

b) musí zaručit, že tato data odpovídají datům pro ověřování elektronických podpisů nebo datům pro ověřování elektronických značek.

(3) Kvalifikovaný poskytovatel certifikačních služeb, který vydává certifikáty jako kvalifikované, musí neprodleně zneplatnit certifikát, pokud o to držitel, podepisující osoba nebo označující osoba požádá, nebo pokud ho uvědomí, že hrozí nebezpečí zneužití jejich dat pro vytváření elektronických podpisů nebo elektronických značek, nebo v případě, že byl certifikát vydán na základě nepravdivých nebo chybných údajů.

(4) Kvalifikovaný poskytovatel certifikačních služeb musí rovněž neprodleně zneplatnit certifikát vydaný jako kvalifikovaný, dozví-li se prokazatelně, že podepisující nebo označující osoba zemřela nebo zanikla nebo ji soud způsobilosti k právním úkonům zbavil nebo omezil, 2a) nebo pokud údaje, na jejichž základě byl certifikát vydán, pozbyly pravdivosti.

§ 6b

Povinnosti kvalifikovaného poskytovatele certifikačních služeb při vydávání kvalifikovaných časových razítek

(1) Kvalifikovaný poskytovatel certifikačních služeb, který vydává kvalifikovaná časová razítka, je povinen
a) zajistit, aby časová razítka jím vydávaná jako kvalifikovaná obsahovala všechny náležitosti stanovené tímto zákonem,

b) zajistit, aby časový údaj vložený do kvalifikovaného časového razítka odpovídal hodnotě koordinovaného světového času při vytváření kvalifikovaného časového razítka,

c) zajistit, aby data v elektronické podobě, která jsou předmětem žádosti o vydání kvalifikovaného časového razítka, jednoznačně odpovídala datům v elektronické podobě obsaženým ve vydaném kvalifikovaném časovém razítku,

d) přijmout odpovídající opatření proti padělání kvalifikovaných časových razítek,

e) poskytovat na vyžádání třetím osobám podstatné informace o podmínkách pro využívání kvalifikovaných časových razítek, včetně omezení pro jejich použití a informace o tom, zda je, či není akreditován ministerstvem; tyto informace lze poskytovat elektronicky.

(2) Kvalifikovaný poskytovatel certifikačních služeb vydá kvalifikované časové razítko neprodleně po přijetí žádosti o jeho vydání.

§ 7

Odpovědnost za škodu

(1) Za škodu způsobenou porušením povinností stanovených tímto zákonem odpovídá kvalifikovaný poskytovatel certifikačních služeb podle zvláštních právních předpisů. 1a)

(2) Kvalifikovaný poskytovatel certifikačních služeb neodpovídá za škodu vyplývající z použití certifikátu vydaného jako kvalifikovaný, která vznikla v důsledku nedodržení omezení pro jeho použití podle § 12 odst. 1 písm. i) a j) a § 12a písm. h).

§ 8

Ochrana osobních údajů

Ochrana osobních údajů se řídí zvláštním právním předpisem. 3)

§ 9

Akreditace a dozor

(1) Udělování akreditací k působení jako akreditovaný poskytovatel certifikačních služeb, jakož i dozor nad dodržováním tohoto zákona náleží ministerstvu.

(2) Ministerstvo

a) uděluje a odnímá akreditace k působení jako akreditovaný poskytovatel certifikačních služeb subjektům působícím na území České republiky,

b) vykonává dozor nad činností akreditovaných poskytovatelů certifikačních služeb a kvalifikovaných poskytovatelů certifikačních služeb, ukládá jim opatření k nápravě a pokuty za porušení povinností podle tohoto zákona,

c) vede evidenci udělených akreditací a jejich změn a evidenci kvalifikovaných poskytovatelů certifikačních služeb,

d) vede evidenci vydaných kvalifikovaných systémových certifikátů, které používá kvalifikovaný poskytovatel certifikačních služeb podle § 6 odst. 1 písm. a) a které byly podle § 6 odst. 2 ověřeny ministerstvem,

e) průběžně uveřejňuje přehled udělených akreditací, přehled kvalifikovaných poskytovatelů certifikačních služeb a jejich kvalifikovaných služeb a kvalifikované systémové certifikáty podle písmena d), a to i způsobem umožňujícím dálkový přístup,

f) vyhodnocuje shodu nástrojů elektronického podpisu s požadavky stanovenými tímto zákonem a prováděcí vyhláškou,

g) plní další povinnosti stanovené tímto zákonem.

(3) Za účelem výkonu dozoru je akreditovaný poskytovatel certifikačních služeb a kvalifikovaný poskytovatel certifikačních služeb povinen pověřeným zaměstnancům ministerstva umožnit v nezbytně nutném rozsahu vstup do obchodních a provozních prostor, na požádání předložit veškerou dokumentaci, záznamy, doklady, písemnosti a jiné podklady související s jeho činností, umožnit jim v nezbytně nutné míře přístup do svého informačního systému a poskytnout informace a veškerou potřebnou součinnost.

(4) Není-li tímto zákonem stanoveno jinak, postupuje ministerstvo při výkonu dozoru podle zvláštního právního předpisu. 4)

(5) Kvalifikovanému poskytovateli certifikačních služeb, který nesplnil povinnost součinnosti podle odstavce 3, lze uložit pořádkovou pokutu do výše 1 000 000 Kč.

§ 10

Podmínky udělení akreditace pro poskytování certifikačních služeb

(1) Každý poskytovatel certifikačních služeb může požádat ministerstvo o udělení akreditace pro výkon činnosti akreditovaného poskytovatele certifikačních služeb.

(2) V žádosti o akreditaci podle odstavce 1 musí žadatel doložit
a) v případě právnické osoby obchodní firmu nebo název, sídlo, popřípadě adresu organizační složky zahraniční osoby na území České republiky, a identifikační číslo žadatele, bylo-li přiděleno; v případě fyzické osoby jméno, popřípadě jména, příjmení, případně dodatek, místo usazení, místo podnikání, pokud je odlišné od místa usazení, a identifikační číslo žadatele, bylo-li přiděleno,

b) doklad o oprávnění k podnikatelské činnosti a u osoby zapsané do obchodního rejstříku také výpis z obchodního rejstříku ne starší než 3 měsíce,

c) výpis z rejstříku trestů podnikatele - fyzické osoby nebo statutárních představitelů právnické osoby v případě, že žadatelem je právnická osoba, ne starší než 3 měsíce,

d) věcné, personální a organizační předpoklady pro činnost kvalifikovaného poskytovatele certifikačních služeb podle § 6, 6a a 6b tohoto zákona,

e) údaj o tom, které kvalifikované certifikační služby hodlá žadatel poskytovat.

(3) Jestliže žádost neobsahuje všechny požadované údaje, ministerstvo řízení přeruší a vyzve žadatele, aby ji ve stanovené lhůtě doplnil. Jestliže tak žadatel v této lhůtě neučiní, ministerstvo řízení zastaví.

(4) Splňuje-li žadatel všechny podmínky předepsané tímto zákonem pro udělení akreditace, vydá ministerstvo rozhodnutí, jímž mu akreditaci udělí. V opačném případě žádost o udělení akreditace zamítne.

§ 10a

Podmínky pro rozšíření služeb akreditovaného poskytovatele certifikačních služeb

(1) Akreditovaný poskytovatel certifikačních služeb může rozšířit poskytování kvalifikovaných certifikačních služeb o vydávání kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů, kvalifikovaných časových razítek nebo o vydávání prostředků pro bezpečné vytváření elektronických podpisů podle tohoto zákona (dále jen "rozšiřované služby").

(2) Akreditovaný poskytovatel certifikačních služeb je povinen rozšíření podle odstavce 1 oznámit ministerstvu tak, aby ministerstvo oznámení obdrželo alespoň 4 měsíce před zahájením poskytování služby.

(3) V oznámení musí akreditovaný poskytovatel certifikačních služeb doložit věcné, personální a organizační předpoklady pro zajištění rozšiřovaných služeb.

(4) Nedoloží-li akreditovaný poskytovatel certifikačních služeb skutečnosti podle odstavce 3, anebo jsou-li tyto skutečnosti neúplné nebo nepřesné, ministerstvo na to akreditovaného poskytovatele certifikačních služeb upozorní s tím, že nebudou-li tyto vady ve lhůtě, kterou k tomu určí, odstraněny, rozhodnutím rozšiřování služeb zakáže.

(5) Ministerstvo oznámené rozšíření zakáže, pokud akreditovaný poskytovatel certifikačních služeb nesplnil všechny podmínky předepsané tímto zákonem pro poskytování rozšiřovaných služeb.

(6) O zákazu rozšíření poskytování kvalifikovaných certifikačních služeb vydá ministerstvo rozhodnutí nejpozději do 90 dnů od okamžiku, kdy obdrželo oznámení.

§ 11

(1) V oblasti orgánů veřejné moci je možné za účelem podpisu používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb (dále jen "uznávaný elektronický podpis"). To platí i pro výkon veřejné moci vůči fyzickým a právnickým osobám. Pokud je uznávaný elektronický podpis užíván v oblasti orgánů veřejné moci, musí kvalifikovaný certifikát obsahovat takové údaje, aby osoba byla jednoznačně identifikovatelná. Strukturu údajů, na základě kterých je možné osobu jednoznačně identifikovat, stanoví ministerstvo prováděcím právním předpisem.

(2) Písemnosti orgánů veřejné moci v elektronické podobě označené elektronickou značkou založenou na kvalifikovaném systémovém certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb nebo podepsané uznávaným elektronickým podpisem mají stejné právní účinky jako veřejné listiny vydané těmito orgány.

(3) Orgán veřejné moci přijímá a odesílá datové zprávy podle odstavce 1 prostřednictvím elektronické podatelny.

§ 12

Náležitosti kvalifikovaného certifikátu

(1) Kvalifikovaný certifikát musí obsahovat
a) označení, že je vydán jako kvalifikovaný certifikát podle tohoto zákona,

b) v případě právnické osoby obchodní firmu nebo název a stát, ve kterém je kvalifikovaný poskytovatel usazen; v případě fyzické osoby jméno, popřípadě jména, příjmení, případně dodatek, a stát, ve kterém je kvalifikovaný poskytovatel usazen,

c) jméno, popřípadě jména, a příjmení podepisující osoby nebo její pseudonym s příslušným označením, že se jedná o pseudonym,

d) zvláštní znaky podepisující osoby, vyžaduje-li to účel kvalifikovaného certifikátu,

e) data pro ověřování podpisu, která odpovídají datům pro vytváření podpisu, jež jsou pod kontrolou podepisující osoby,

f) elektronickou značku poskytovatele certifikačních služeb založenou na kvalifikovaném systémovém certifikátu poskytovatele, který kvalifikovaný certifikát vydává,

g) číslo kvalifikovaného certifikátu unikátní u daného poskytovatele certifikačních služeb,

h) počátek a konec platnosti kvalifikovaného certifikátu,

i) případně údaje o tom, zda se používání kvalifikovaného certifikátu omezuje podle povahy a rozsahu jen pro určité použití,

j) případně omezení hodnot transakcí, pro něž lze kvalifikovaný certifikát použít.

(2) Omezení pro použití kvalifikovaného certifikátu podle odstavce 1 písm. i) a j) musí být zjevná třetím stranám.

(3) Další osobní údaje smí kvalifikovaný certifikát obsahovat jen se svolením podepisující osoby.

§ 12a

Náležitosti kvalifikovaného systémového certifikátu

Kvalifikovaný systémový certifikát musí obsahovat
a) označení, že je vydán jako kvalifikovaný systémový certifikát podle tohoto zákona,

b) v případě právnické osoby obchodní firmu nebo název a stát, ve kterém je kvalifikovaný poskytovatel usazen; v případě fyzické osoby jméno, popřípadě jména, příjmení, případně dodatek, a stát, ve kterém je kvalifikovaný poskytovatel usazen,

c) jednoznačnou identifikaci označující osoby, případně prostředku pro vytváření

elektronických značek,

d) data pro ověřování elektronických značek, která odpovídají datům pro vytváření elektronických značek, jež jsou pod kontrolou označující osoby,

e) elektronickou značku poskytovatele certifikačních služeb založenou na kvalifikovaném systémovém certifikátu poskytovatele, který kvalifikovaný systémový certifikát vydává,

f) číslo kvalifikovaného systémového certifikátu unikátní u daného kvalifikovaného poskytovatele certifikačních služeb,

g) počátek a konec platnosti kvalifikovaného systémového certifikátu,

h) omezení pro použití kvalifikovaného systémového certifikátu, přičemž tato omezení musí být zjevná třetím stranám.

§ 12b

Náležitosti kvalifikovaného časového razítka

Kvalifikované časové razítko musí obsahovat
a) číslo kvalifikovaného časového razítka unikátní u daného kvalifikovaného poskytovatele certifikačních služeb,

b) označení pravidel, podle kterých kvalifikovaný poskytovatel certifikačních služeb kvalifikované časové razítko vydal,

c) v případě právnické osoby obchodní firmu nebo název a stát, ve kterém je kvalifikovaný poskytovatel usazen; v případě fyzické osoby jméno, popřípadě jména, příjmení, případně dodatek, a stát, ve kterém je kvalifikovaný poskytovatel usazen,

d) hodnotu času, která odpovídá koordinovanému světovému času při vytváření kvalifikovaného časového razítka,

e) data v elektronické podobě, pro která bylo kvalifikované časové razítko vydáno,

f) elektronickou značku kvalifikovaného poskytovatele certifikačních služeb, který kvalifikované časové razítko vydal.

§ 13

Povinnosti kvalifikovaného poskytovatele certifikačních služeb při ukončení činnosti

(1) Kvalifikovaný poskytovatel certifikačních služeb musí záměr ukončit svou činnost ohlásit ministerstvu nejméně 3 měsíce před plánovaným datem ukončení činnosti a musí vynaložit veškeré možné úsilí k tomu, aby evidence vedená podle § 6 odst. 5 byla převzata jiným kvalifikovaným poskytovatelem certifikačních služeb. Kvalifikovaný poskytovatel certifikačních služeb dále musí prokazatelně informovat každou podepisující osobu, označující osobu a držitele, kterým poskytuje své certifikační služby, o svém záměru ukončit svoji činnost

nejméně 2 měsíce před plánovaným datem ukončení činnosti.

(2) Nemůže-li kvalifikovaný poskytovatel certifikačních služeb zajistit, aby evidenci vedenou podle § 6 odst. 5 převzal jiný kvalifikovaný poskytovatel certifikačních služeb, je povinen to nejpozději 30 dnů před plánovaným datem ukončení činnosti ministerstvu ohlásit. V takovém případě ministerstvo převezme evidenci a oznámí to dotčeným subjektům.

(3) Ustanovení odstavců 1 a 2 se použijí přiměřeně také v případě, když kvalifikovaný poskytovatel certifikačních služeb zanikne, zemře nebo přestane vykonávat svoji činnost, aniž splní ohlašovací povinnost podle odstavce 1.

§ 14

Opatření k nápravě

(1) Zjistí-li ministerstvo, že akreditovaný poskytovatel certifikačních služeb nebo kvalifikovaný poskytovatel certifikačních služeb porušuje povinnosti stanovené tímto zákonem, uloží mu, aby ve stanovené lhůtě zjednal nápravu, a případně určí, jaká opatření k odstranění nedostatků je tento poskytovatel certifikačních služeb povinen přijmout.

(2) V případě, že se akreditovaný poskytovatel certifikačních služeb dopustí závažnějšího porušení povinností stanovených tímto zákonem nebo ve stanovené lhůtě neodstraní nedostatky zjištěné ministerstvem, je ministerstvo oprávněno mu udělenou akreditaci odejmout.

(3) Rozhodne-li ministerstvo o odnětí akreditace, může současně rozhodnout o zneplatnění certifikátů vydaných jako kvalifikované poskytovatelem certifikačních služeb v době platnosti akreditace.

§ 15

Zrušení kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu

Ministerstvo může nařídit kvalifikovanému poskytovateli certifikačních služeb jako předběžné opatření 7) zneplatnění certifikátu vydaného jako kvalifikovaný, pokud existuje důvodné podezření, že certifikát byl padělán, nebo pokud byl vydán na základě nepravdivých údajů. Rozhodnutí o zneplatnění certifikátu vydaného jako kvalifikovaný může být vydáno také v případě, kdy bylo zjištěno, že podepisující nebo označující osoba používá prostředek pro vytváření podpisu nebo prostředek pro vytváření elektronických značek, který vykazuje bezpečnostní nedostatky, které by umožnily padělání zaručených elektronických podpisů nebo elektronických značek nebo změnu podepisovaných nebo označovaných údajů.

§ 16

Uznávání zahraničních kvalifikovaných certifikátů

(1) Certifikát, který je vydán poskytovatelem certifikačních služeb usazeným v některém z členských států Evropské unie jako kvalifikovaný, je kvalifikovaným certifikátem ve smyslu tohoto zákona.

(2) Certifikát, který je vydán jako kvalifikovaný ve smyslu tohoto zákona v jiném než členském státu Evropské unie, je kvalifikovaným certifikátem ve smyslu tohoto zákona, pokud
a) poskytovatel certifikačních služeb splňuje podmínky práva Evropských společenství 1) a byl akreditován k působení jako akreditovaný poskytovatel certifikačních služeb v některém z členských států Evropské unie,

b) poskytovatel certifikačních služeb usazený v některém z členských států Evropské unie, který splňuje podmínky práva Evropských společenství, 1) převezme odpovědnost za platnost a správnost certifikátu ve stejném rozsahu jako u svých kvalifikovaných certifikátů,

c) to vyplývá z mezinárodní smlouvy.

§ 17

Prostředky pro bezpečné vytváření a ověřování elektronických podpisů

(1) Prostředek pro bezpečné vytváření podpisu musí za pomoci odpovídajících technických a programových prostředků a postupů minimálně zajistit, že
a) data pro vytváření podpisu se mohou vyskytnout pouze jednou a že jejich utajení je náležitě zajištěno,

b) data pro vytváření podpisu nelze při náležitém zajištění odvodit ze znalosti způsobu jejich vytváření a že podpis je chráněn proti padělání s využitím existující dostupné technologie,

c) data pro vytváření podpisu mohou být podepisující osobou spolehlivě chráněna proti zneužití třetí osobou.

(2) Prostředky pro bezpečné vytváření podpisu nesmí měnit data, která se podepisují, ani zabraňovat tomu, aby tato data byla předložena podepisující osobě před vlastním procesem podepisování.

(3) Prostředky pro bezpečné vytváření elektronických podpisů musí být před svým použitím bezpečným způsobem vydány a data pro vytváření elektronických podpisů musí být důvěryhodným způsobem v těchto prostředcích vytvořena nebo do nich přidána.

(4) Prostředek pro bezpečné ověřování podpisu musí za pomoci odpovídajících technických a programových prostředků a postupů minimálně zajistit, aby
a) data používaná pro ověření podpisu odpovídala datům zobrazeným osobě provádějící ověření,

b) podpis byl spolehlivě ověřen a výsledek tohoto ověření byl řádně zobrazen,

c) ověřující osoba mohla spolehlivě zjistit obsah podepsaných dat,

d) pravost a platnost certifikátu při ověřování podpisu byly spolehlivě zjištěny,

e) výsledek ověření a totožnost podepisující osoby byly řádně zobrazeny,

f) bylo jasně uvedeno použití pseudonymu,

g) bylo možné zjistit veškeré změny ovlivňující bezpečnost.

§ 17a

Prostředky pro vytváření elektronických značek

(1) Prostředek pro vytváření elektronických značek musí za pomoci odpovídajících technických a programových prostředků a postupů minimálně zajistit, že
a) data pro vytváření elektronických značek jsou dostatečným způsobem utajena a jsou označující osobou spolehlivě chráněna proti zneužití třetí osobou,

b) označující osoba je informována, že zahajuje používání tohoto prostředku.

(2) Prostředek pro vytváření elektronických značek musí být nastaven tak, aby i bez další kontroly označující osoby označil právě a pouze ty datové zprávy, které označující osoba k označení zvolí.

(3) Prostředek pro vytváření elektronických značek musí být chráněn proti neoprávněné změně a musí zaručovat, že jakákoli jeho změna bude patrná označující osobě.

§ 18

Správní delikty právnických osob

(1) Kvalifikovanému poskytovateli certifikačních služeb, který
a) nezajistí, aby se každý mohl ujistit o jeho identitě a jeho kvalifikovaném systémovém certifikátu podle § 6 odst. 1 písm. a),

b) nezajistí, aby poskytování kvalifikovaných certifikačních služeb vykonávaly osoby s odbornými znalostmi a kvalifikací nezbytnými pro poskytované kvalifikované certifikační služby a obeznámené s příslušnými bezpečnostními postupy,

c) nezajištěním dostatečné bezpečnosti používaných systémů a nástrojů elektronického podpisu a postupů, které tyto systémy a nástroje podporují podle § 6 odst. 1 písm. c) a d), ohrozí bezpečnost poskytovaných kvalifikovaných certifikačních služeb,

d) nedisponuje dostatečnými finančními zdroji nebo jiným finančním zajištěním na provoz podle § 6 odst. 1 písm. e), a tím ohrozí bezpečnost poskytovaných kvalifikovaných certifikačních služeb,

e) nesplní informační povinnost podle § 6 odst. 1 písm. f), § 6 odst. 3 nebo § 13 odst. 1,

f) nesplní ohlašovací povinnost podle § 6 odst. 2, včetně předání kvalifikovaného systémového certifikátu k ověření nebo podle § 13 odst. 1 nebo 2,

g) poskytne certifikační služby na základě jiné než písemné smlouvy,

h) neuchovává informace a dokumentaci podle § 6 odst. 5,

i) neuchovává veškeré informace a dokumentaci podle § 6 odst. 6 po dobu nejméně 10 let, nebo

j) nezajistí uchovávané informace a dokumentaci před ztrátou, zneužitím, zničením nebo poškozením podle § 6 odst. 6,

se uloží pokuta do výše 10 000 000 Kč.

(2) Kvalifikovanému poskytovateli certifikačních služeb, který vydává kvalifikované certifikáty nebo kvalifikované systémové certifikáty a který

a) nezajistí, aby certifikáty jím vydané jako kvalifikované obsahovaly všechny náležitosti stanovené tímto zákonem,

b) nezajistí, aby údaje uvedené v certifikátech vydaných jako kvalifikované byly přesné, pravdivé a úplné,

c) neověří identitu osoby podle § 6a odst. 1 písm. c),

d) nezajistí soulad dat podle § 6a odst. 1 písm. d),

e) nezajistí provozování bezpečného a veřejně přístupného seznamu certifikátů vydaných jako kvalifikované a nezajistí jeho dostupnost a aktualizaci podle § 6a odst. 1 písm. e),

f) nezajistí provozování bezpečného a veřejně přístupného seznamu certifikátů vydaných jako kvalifikované, které byly zneplatněny, a to i dálkovým přístupem,

g) nezajistí, aby datum a čas s uvedením hodiny, minuty a sekundy, kdy je certifikát vydaný jako kvalifikovaný vydán nebo zneplatněn, mohly být přesně určeny,

h) nepřijetím odpovídajících opatření proti zneužití a padělání certifikátů vydaných jako kvalifikované ohrozí bezpečnost poskytovaných kvalifikovaných certifikačních služeb,

i) nesplní informační povinnost podle § 6a odst. 1 písm. i),

j) nezajistí soulad a utajení dat podle § 6a odst. 2, pokud tato data pro podepisující nebo označující osobu vytváří,

k) kopíruje a uchovává data podle § 6a odst. 2, pokud tato data pro podepisující nebo označující osobu vytváří, nebo

l) nezneplatní certifikát podle § 6a odst. 3 a 4, se uloží pokuta do výše 10 000 000 Kč.

(3) Kvalifikovanému poskytovateli certifikačních služeb, který vydává kvalifikovaná časová razítka a který
a) nezajistí, aby časová razítka jím vydávaná jako kvalifikovaná obsahovala všechny náležitosti stanovené v § 12b,

b) nezajistí, aby časový údaj vložený do kvalifikovaného časového razítka odpovídal hodnotě koordinovaného světového času při vytváření kvalifikovaného časového razítka,

c) nezajistí, aby data v elektronické podobě, která jsou předmětem žádosti o vydání kvalifikovaného časového razítka, odpovídala datům v elektronické podobě obsaženým ve vydaném kvalifikovaném časovém razítku,

d) nepřijme odpovídající opatření proti padělání kvalifikovaných časových razítek, a tím ohrozí bezpečnost poskytovaných kvalifikovaných certifikačních služeb,

e) nesplní informační povinnost podle § 6b odst. 1 písm. e), nebo

f) nevydá kvalifikované časové razítko neprodleně po přijetí žádosti o jeho vydání,
se uloží pokuta do výše 10 000 000 Kč.

(4) Kvalifikovanému poskytovateli certifikačních služeb, který vydává prostředky pro bezpečné vytváření elektronických podpisů a který
a) nevydá prostředky pro bezpečné vytváření elektronických podpisů bezpečně podle § 17 odst. 3, nebo

b) nevytvoří v těchto prostředcích nebo nepřidá do těchto prostředků data pro vytváření elektronických podpisů důvěryhodným způsobem podle § 17 odst. 3,
se uloží pokuta do výše 10 000 000 Kč.

(5) Akreditovanému poskytovateli certifikačních služeb, který nesplní oznamovací povinnost podle § 10a odst. 2, se uloží pokuta do výše 10 000 000 Kč.

(6) Akreditovanému poskytovateli certifikačních služeb, který poruší zákaz vydaný ministerstvem podle § 10a odst. 5, se uloží pokuta do výše 10 000 000 Kč.

§ 18a

Přestupky

(1) Kvalifikovaný poskytovatel certifikačních služeb se dopustí přestupku tím, že
a) nezajistí, aby se každý mohl ujistit o jeho identitě a jeho kvalifikovaném systémovém certifikátu podle § 6 odst. 1 písm. a),

b) nezajistí, aby poskytování kvalifikovaných certifikačních služeb vykonávaly osoby s odbornými znalostmi a kvalifikací nezbytnými pro poskytované kvalifikované certifikační služby a obeznámené s příslušnými bezpečnostními postupy,

c) nezajištěním dostatečné bezpečnosti používaných systémů a nástrojů elektronického podpisu a postupů, které tyto systémy a nástroje podporují podle § 6 odst. 1 písm. c) a písm. d), ohrozí

bezpečnost poskytovaných kvalifikovaných certifikačních služeb,

d) nedisponuje dostatečnými finančními zdroji nebo jiným finančním zajištěním na provoz podle § 6 odst. 1 písm. e), a tím ohrozí bezpečnost poskytovaných kvalifikovaných certifikačních služeb,

e) nesplní informační povinnost podle § 6 odst. 1 písm. f), § 6 odst. 3 nebo § 13 odst. 1,

f) nesplní ohlašovací povinnost podle § 6 odst. 2, včetně předání kvalifikovaného systémového certifikátu k ověření nebo podle § 13 odst. 1 nebo 2,

g) poskytne certifikační služby na základě jiné než písemné smlouvy,

h) neuchovává informace a dokumentaci podle § 6 odst. 5,

i) neuchovává veškeré informace a dokumentaci podle § 6 odst. 6 po dobu nejméně 10 let, nebo

j) nezajistí uchovávané informace a dokumentaci před ztrátou, zneužitím, zničením nebo poškozením podle § 6 odst. 6.

(2) Kvalifikovaný poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty nebo kvalifikované systémové certifikáty, se dopustí přestupku tím, že
a) nezajistí, aby certifikáty jím vydané jako kvalifikované obsahovaly všechny náležitosti stanovené tímto zákonem,

b) nezajistí, aby údaje uvedené v certifikátech vydaných jako kvalifikované byly přesné, pravdivé a úplné,

c) neověří identitu osoby podle § 6a odst. 1 písm. c),

d) nezajistí soulad dat podle § 6a odst. 1 písm. d),

e) nezajistí provozování bezpečného a veřejně přístupného seznamu certifikátů vydaných jako kvalifikované a nezajistí jeho dostupnost a aktualizaci podle § 6a odst. 1 písm. e),

f) nezajistí provozování bezpečného a veřejně přístupného seznamu certifikátů vydaných jako kvalifikované, které byly zneplatněny, a to i dálkovým přístupem,

g) nezajistí, aby datum a čas s uvedením hodiny, minuty a sekundy, kdy je certifikát vydaný jako kvalifikovaný vydán nebo zneplatněn, mohly být přesně určeny,

h) nepřijetím odpovídajících opatření proti zneužití a padělání certifikátů vydaných jako kvalifikované ohrozí bezpečnost poskytovaných kvalifikovaných certifikačních služeb,

i) nesplní informační povinnost podle § 6a odst. 1 písm. i),

j) nezajistí soulad a utajení dat podle § 6a odst. 2, pokud tato data pro podepisující nebo označující osobu vytváří,

k) kopíruje a uchovává data podle § 6a odst. 2, pokud tato data pro podepisující nebo označující osobu vytváří, nebo

l) nezneplatní certifikát podle § 6a odst. 3 a 4.

(3) Kvalifikovaný poskytovatel certifikačních služeb, který vydává kvalifikovaná časová razítka, se dopustí přestupku tím, že
a) nezajistí, aby časová razítka jím vydávaná jako kvalifikovaná obsahovala všechny náležitosti stanovené v § 12b,

b) nezajistí, aby časový údaj vložený do kvalifikovaného časového razítka odpovídal hodnotě koordinovaného světového času při vytváření kvalifikovaného časového razítka,

c) nezajistí, aby data v elektronické podobě, která jsou předmětem žádosti o vydání kvalifikovaného časového razítka, odpovídala datům v elektronické podobě obsaženým ve vydaném kvalifikovaném časovém razítku,

d) nepřijme odpovídající opatření proti padělání kvalifikovaných časových razítek, a tím ohrozí bezpečnost poskytovaných kvalifikovaných certifikačních služeb,

e) nesplní informační povinnost podle § 6b odst. 1 písm. e), nebo

f) nevydá kvalifikované časové razítko neprodleně po přijetí žádosti o jeho vydání.

(4) Kvalifikovaný poskytovatel certifikačních služeb, který vydává prostředky pro bezpečné vytváření elektronických podpisů, se dopustí přestupku tím, že
a) nevydá prostředky pro bezpečné vytváření elektronických podpisů bezpečně podle § 17 odst. 3, nebo

b) nevytvoří v těchto prostředcích nebo nepřidá do těchto prostředků data pro vytváření elektronických podpisů důvěryhodným způsobem podle § 17 odst. 3.

(5) Fyzická osoba se dopustí přestupku tím, že poruší povinnost mlčenlivosti podle § 6 odst. 7.

(6) Za přestupky podle odstavců 1 až 4 lze uložit pokutu do výše 10 000 000 Kč.

(7) Za přestupek podle odstavce 5 lze uložit pokutu do výše 250 000 Kč.

§ 19

Společná ustanovení

(1) Právnická osoba za správní delikt neodpovídá, jestliže prokáže, že vynaložila veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránila.

(2) Při určení výměry pokuty právnické osobě se přihlédne k závažnosti správního deliktu, zejména ke způsobu jeho spáchání a jeho následkům a k okolnostem, za nichž bylo spácháno.

(3) Odpovědnost právnické osoby za správní delikt zaniká, jestliže správní orgán o něm nezahájil řízení do 1 roku ode dne, kdy se o něm dozvěděl, nejpozději však do 3 let ode dne, kdy byl spáchán.

(4) Správní delikty podle tohoto zákona v prvním stupni projednává ministerstvo.

(5) Na odpovědnost za jednání, k němuž došlo při podnikání fyzické osoby 8) nebo v přímé souvislosti s ním, se vztahují ustanovení zákona o odpovědnosti a postihu právnické osoby.

(6) Pokuty vybírá a vymáhá místně příslušný celní úřad. Výnos z pokut je příjmem státního rozpočtu.

§ 20

Zmocňovací ustanovení

(1) Ministerstvo stanoví prováděcím právním předpisem způsob splnění informační povinnosti podle § 6 odst. 1 písm. a) a f) a odst. 3, kvalifikační požadavky podle § 6 odst. 1 písm. b), požadavky na bezpečné systémy a bezpečné nástroje podle § 6 odst. 1 písm. c) a d), způsob uchovávání informací a dokumentace podle § 6 odst. 5 a 6 a způsob, jakým se splnění těchto požadavků dokládá.

(2) Ministerstvo stanoví prováděcím právním předpisem způsob ověření souladu dat podle § 6a odst. 1 písm. d), způsob zajištění bezpečnosti seznamů podle § 6a odst. 1 písm. e) a f), určení data a času podle § 6a odst. 1 písm. g), náležitosti opatření podle § 6a odst. 1 písm. h), způsob splnění informační povinnosti podle § 6a odst. 1 písm. i), způsob ochrany a zajištění souladu dat podle § 6a odst. 2, způsob zneplatnění certifikátů podle § 6a odst. 3 a 4 a způsob, jakým se splnění těchto požadavků dokládá.

(3) Ministerstvo stanoví prováděcím právním předpisem způsob zajištění přesnosti času při vytváření kvalifikovaného časového razítka podle § 6b odst. 1 písm. b), způsob zajištění souladu dat podle § 6b odst. 1 písm. c), náležitosti opatření podle § 6b odst. 1 písm. d), způsob splnění informační povinnosti podle § 6b odst. 1 písm. e) a způsob, jakým se splnění těchto požadavků dokládá.

(4) Ministerstvo stanoví prováděcím právním předpisem strukturu údajů, na základě kterých je možné osobu jednoznačně identifikovat, a postupy orgánů veřejné moci uplatňované

při přijímání a odesílání datových zpráv prostřednictvím elektronické podatelny podle § 11 odst. 3.

(5) Ministerstvo stanoví prováděcím právním předpisem způsob zajištění postupů, které musí podporovat prostředky pro bezpečné vytváření a ověřování elektronických podpisů při ochraně dat pro vytváření elektronických podpisů podle § 17 a prostředky pro vytváření elektronických značek při ochraně dat pro vytváření elektronických značek podle § 17a, a způsob, jakým se splnění těchto požadavků dokládá.

ČÁST DRUHÁ

Změna občanského zákoníku

§ 21

Zákon č. 40/1964 Sb. , občanský zákoník, ve znění zákona č. 58/1969 Sb. , zákona č. 131/1982 Sb. , zákona č. 94/1988 Sb. , zákona č. 188/1988 Sb. , zákona č. 87/1990 Sb. , zákona č. 105/1990 Sb. , zákona č. 116/1990 Sb. , zákona č. 87/1991 Sb. , zákona č. 509/1991 Sb. , zákona č. 264/1992 Sb. , zákona č. 267/1994 Sb. , zákona č. 104/1995 Sb. , zákona č. 118/1995 Sb. , zákona č. 89/1996 Sb. , zákona č. 94/1996 Sb. , zákona č. 227/1997 Sb. , zákona č. 91/1998 Sb. , zákona č. 165/1998 Sb. , zákona č. 159/1999 Sb. , zákona č. 363/1999 Sb. , zákona č. 27/2000 Sb. a zákona č. 103/2000 Sb. , se mění takto:

V § 40 odst. 3 se doplňuje tato věta:

"Je-li právní úkon učiněn elektronickými prostředky, může být podepsán elektronicky podle zvláštních předpisů.".

ČÁST TŘETÍ

Změna zákona č. 337/1992 Sb. , o správě daní a poplatků

§ 22

Zákon č. 337/1992 Sb. , o správě daní a poplatků, ve znění zákona č. 35/1993 Sb. , zákona č. 157/1993 Sb. , zákona č. 302/1993 Sb. , zákona č. 315/1993 Sb. , zákona č. 323/1993 Sb. , zákona č. 85/1994 Sb. , zákona č. 255/1994 Sb. , zákona č. 59/1995 Sb. , zákona č. 118/1995 Sb. , zákona č. 323/1996 Sb. , zákona č. 61/1997 Sb. , zákona č. 242/1997 Sb. , zákona č. 91/1998 Sb. , zákona č. 168/1998 Sb. , zákona č. 29/2000 Sb. , zákona č. 159/2000 Sb. a zákona č. 218/2000 Sb. , se mění takto:

V § 21 odstavce 2 a 3 znějí:

"(2) Stanoví-li tak tento nebo zvláštní zákon, podávají daňové subjekty o své daňové povinnosti příslušnému správci daně přiznání, hlášení a vyúčtování na předepsaných tiskopisech. Tiskopisy zveřejněné v elektronické podobě lze podepsat elektronicky podle zvláštních předpisů.

(3) Jiná podání v daňových věcech, jako jsou oznámení, žádosti, návrhy, námitky,

odvolání apod., lze učinit buď písemně nebo ústně do protokolu nebo elektronicky podepsané podle zvláštních předpisů či za použití jiných přenosových technik (dálnopis, telefax apod.).".

ČÁST ČTVRTÁ

zrušena

§ 23

zrušen

ČÁST PÁTÁ

Změna občanského soudního řádu

§ 24

Zákon č. 99/1963 Sb. , občanský soudní řád, ve znění zákona č. 36/1967 Sb. , zákona č. 158/1969 Sb. , zákona č. 49/1973 Sb. , zákona č. 20/1975 Sb. , zákona č. 133/1982 Sb. , zákona č. 180/1990 Sb. , zákona č. 328/1991 Sb. , zákona č. 519/1991 Sb. , zákona č. 263/1992 Sb. , zákona č. 24/1993 Sb. , zákona č. 171/1993 Sb. , zákona č. 117/1994 Sb. , zákona č. 152/1994 Sb. , zákona č. 216/1994 Sb. , zákona č. 84/1995 Sb. , zákona č. 118/1995 Sb. , zákona č. 160/1995 Sb. , zákona č. 238/1995 Sb. , zákona č. 247/1995 Sb. , nálezu Ústavního soudu č. 31/1996 Sb. , zákona č. 142/1996 Sb. , nálezu Ústavního soudu č. 269/1996 Sb. , zákona č. 202/1997 Sb. , zákona č. 227/1997 Sb. , zákona č. 15/1998 Sb. , zákona č. 91/1998 Sb. , zákona č. 165/1998 Sb. , zákona č. 326/1999 Sb. , zákona č. 360/1999 Sb. , nálezu Ústavního soudu č. 2/2000 Sb. , zákona č. 27/2000 Sb. , zákona č. 30/2000 Sb. , zákona č. 46/2000 Sb. , zákona č. 105/2000 Sb. , zákona č. 130/2000 Sb. , zákona č. 155/2000 Sb. a zákona č. 220/2000 Sb. , se mění takto:

V § 42 odst. 1 věta první zní: "Podání je možno učinit písemně, ústně do protokolu, v elektronické podobě podepsané elektronicky podle zvláštních předpisů, telegraficky nebo telefaxem.".

ČÁST ŠESTÁ

Změna trestního řádu

§ 25

Zákon č. 141/1961 Sb. , o trestním řízení soudním (trestní řád), ve znění zákona č. 57/1965 Sb. , zákona č. 58/1969 Sb. , zákona č. 149/1969 Sb. , zákona č. 48/1973 Sb. , zákona č. 29/1978 Sb. , zákona č. 43/1980 Sb. , zákona č. 159/1989 Sb. , zákona č. 178/1990 Sb. , zákona č. 303/1990 Sb. , zákona č. 558/1991 Sb. , zákona č. 25/1993 Sb. , zákona č. 115/1993 Sb. , zákona č. 292/1993 Sb. , zákona č. 154/1994 Sb. , nálezu Ústavního soudu č. 214/1994 Sb. , nálezu Ústavního soudu č. 8/1995 Sb. , zákona č. 152/1995 Sb. , zákona č. 150/1997 Sb. , zákona č. 209/1997 Sb. , zákona č. 148/1998 Sb. , zákona č. 166/1998 Sb. , zákona č. 191/1999 Sb. , zákona č. 29/2000 Sb. a zákona č. 30/2000 Sb. , se mění takto:

V § 59 odstavec 1 zní:

"(1) Podání se posuzuje vždy podle svého obsahu, i když je nesprávně označeno. Lze je učinit písemně, ústně do protokolu, v elektronické podobě podepsané elektronicky podle zvláštních předpisů, telegraficky, telefaxem nebo dálnopisem.".

ČÁST SEDMÁ

Změna zákona o ochraně osobních údajů

§ 26

Zákon č. 101/2000 Sb. , o ochraně osobních údajů a o změně některých zákonů, se mění takto:

V § 29 se doplňuje odstavec 4 , který zní:

"(4) Úřad uděluje a odnímá akreditace k působení jako akreditovaný poskytovatel certifikačních služeb a provádí dozor nad dodržováním povinností stanovených zákonem o elektronickém podpisu.".

ČÁST OSMÁ

Změna zákona o správních poplatcích

§ 27

Zákon č. 368/1992 Sb. , o správních poplatcích, ve znění zákona č. 10/1993 Sb. , zákona č. 72/1994 Sb. , zákona č. 85/1994 Sb. , zákona č. 273/1994 Sb. , zákona č. 36/1995 Sb. , zákona č. 118/1995 Sb. , zákona č. 160/1995 Sb. , zákona č. 301/1995 Sb. , zákona č. 151/1997 Sb. , zákona č. 305/1997 Sb. , zákona č. 149/1998 Sb. , zákona č. 157/1998 Sb. , zákona č. 167/1998 Sb. , zákona č. 63/1999 Sb. , zákona č. 166/1999 Sb. , zákona č. 167/1999 Sb. , zákona č. 223/1999 Sb. , zákona č. 326/1999 Sb. , zákona č. 352/1999 Sb. , zákona č. 357/1999 Sb. , zákona č. 360/1999 Sb. , zákona č. 363/1999 Sb. , zákona č. 46/2000 Sb. , zákona č. 62/2000 Sb. , zákona č. 117/2000 Sb. , zákona č. 133/2000 Sb. , zákona č. 151/2000 Sb. , zákona č. 153/2000 Sb. , zákona č. 154/2000 Sb., zákona č. 156/2000 Sb. a zákona č. 158/2000 Sb. , se mění takto:

1. V příloze k zákonu (Sazebník správních poplatků) se doplňuje nová část XII , která zní:

ČÁST XII

ŘÍZENÍ PODLE ZÁKONA O ELEKTRONICKÉM PODPISU

Položka 162
a) podání žádosti o akreditaci poskytovatele certifikačních služeb
Kč 100 000,-
b) podání žádosti o vyhodnocení shody nástrojů elektronického podpisu s požadavky Kč 10 000,-.".

2. REJSTŘÍK K SAZEBNÍKU se doplňuje o část XII , která zní:

ČÁST XII

Řízení podle zákona o elektronickém podpisu 162.".

3. Tečka za částí XI se vypouští.

ČÁST DEVÁTÁ

ÚČINNOST

§ 28

Tento zákon nabývá účinnosti prvním dnem třetího kalendářního měsíce po dni jeho vyhlášení.

Klaus v. r.

Havel v. r.

Zeman v. r.

Vybraná ustanovení novel

Čl.II zákona č. 440/2004 Sb.

Přechodná ustanovení

Poskytovatelé certifikačních služeb, kterým byla udělena akreditace k působení jako akreditovaný poskytovatel certifikačních služeb přede dnem nabytí účinnosti tohoto zákona, jsou povinni přizpůsobit službu vydávání kvalifikovaných certifikátů zákonu č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění čl. I tohoto zákona, do 1. července 2005.

---

1) Směrnice Evropského parlamentu a Rady 99/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy.

1a) Zákon č. 40/1964 Sb. , občanský zákoník, ve znění pozdějších předpisů.

2) Zákon č. 97/1974 Sb. , o archivnictví, ve znění pozdějších předpisů.

2a) § 10 zákona č. 40/1964 Sb. , občanský zákoník, ve znění pozdějších předpisů.

3) Zákon č. 101/2000 Sb. , o ochraně osobních údajů a o změně některých zákonů.

4) Zákon č. 552/1991 Sb. , o státní kontrole, ve znění pozdějších předpisů.

5) Zákon č. 368/1992 Sb. , o správních poplatcích, ve znění pozdějších předpisů.

7) § 43 zákona č. 71/1967 Sb. , o správním řízení (správní řád), ve znění pozdějších předpisů.

8) § 2 odst. 2 zákona č. 513/1991 Sb. , obchodní zákoník, ve znění pozdějších předpisů.

b) ochrana osobních údajů: současnost a nové trendy

Nové technologie, ke kterým patří i RFID, zvyšují možnosti neoprávněné manipulace s osobními údaji.

V ČR byl přijat zákon o ochraně osobních údajů č. 101/2000 Sb. v roce 2000, který definuje základní předmět úpravy, základní pojmy,kompetence úřadu, mechanismy i sankce:

§ 1

Předmět úpravy

Tento zákon v souladu s právem Evropských společenství,[1)] mezinárodními smlouvami, kterými je Česká republika vázána,[1a)] a k naplnění práva každého na ochranu před neoprávněným zasahováním do soukromí upravuje práva a povinnosti při zpracování osobních údajů a stanoví podmínky, za nichž se uskutečňuje předání osobních údajů do jiných států.

§ 2

(1) Zřizuje se Úřad pro ochranu osobních údajů se sídlem v Praze (dále jen "Úřad").

(2) Úřadu jsou svěřeny kompetence ústředního správního úřadu pro oblast ochrany osobních údajů v rozsahu stanoveném tímto zákonem a další kompetence stanovené zvláštním právním předpisem.[1b)]

§ 3

Působnost zákona

(1) Tento zákon se vztahuje na osobní údaje, které zpracovávají státní orgány, orgány územní samosprávy, jiné orgány veřejné moci, jakož i fyzické a právnické osoby.

(2) Tento zákon se vztahuje na veškeré zpracovávání osobních údajů, ať k němu dochází automatizovaně nebo jinými prostředky.

(3) Tento zákon se nevztahuje na zpracování osobních údajů, které provádí fyzická osoba výlučně pro osobní potřebu.

(4) Tento zákon se nevztahuje na nahodilé shromažďování osobních údajů, pokud tyto údaje nejsou dále zpracovávány.

(5) Tento zákon se dále vztahuje na zpracování osobních údajů,

a) jestliže se právní řád České republiky použije přednostně na základě mezinárodního práva veřejného, i když správce není usazen na území České republiky,

b) jestliže správce, který je usazen mimo území Evropské unie, provádí zpracování na území České republiky a nejedná se pouze o předání osobních údajů přes území Evropské unie; v tomto případě je správce povinen zmocnit postupem podle § 6 na území České republiky zpracovatele.

Jestliže zpracování provádí správce prostřednictvím svých organizačních jednotek umístěných na území Evropské unie, musí zajistit, že tyto organizační jednotky budou zpracovávat osobní údaje v souladu s národním právem příslušného členského státu Evropské unie.

(6) Ustanovení § 5 odst. 1 a § 11 a 12 se nepoužijí pro zpracování osobních údajů nezbytných pro plnění povinností správce stanovených zvláštními zákony pro zajištění

a) bezpečnosti České republiky,[4)]

b) obrany České republiky,[5)]

c) veřejného pořádku a vnitřní bezpečnosti,[6)]

d) předcházení, vyhledávání, odhalování trestné činnosti a stíhání trestných činů,[7)]

e) významného hospodářského zájmu České republiky nebo Evropské unie,[8)]

f) významného finančního zájmu České republiky nebo Evropské unie, kterým je zejména stabilita finančního trhu a měny, fungování peněžního oběhu a platebního styku, jakož i rozpočtová a daňová opatření,[9)]

g) výkonu kontroly, dozoru, dohledu a regulace spojených s výkonem veřejné moci v případech uvedených v písmenech c), d), e) a f),[10)] nebo

h) činností spojených se zpřístupňováním svazků bývalé Státní bezpečnosti.[10a)]

§ 4

Vymezení pojmů

Pro účely tohoto zákona se rozumí

a) osobním údajem jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho

fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu,

b) citlivým údajem osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a jakýkoliv biometrický nebo genetický údaj subjektu údajů,

c) anonymním údajem takový údaj, který buď v původním tvaru nebo po provedeném zpracování nelze vztáhnout k určenému nebo určitelnému subjektu údajů,

d) subjektem údajů fyzická osoba, k níž se osobní údaje vztahují,

e) zpracováním osobních údajů jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace,

f) shromažďováním osobních údajů systematický postup nebo soubor postupů, jehož cílem je získání osobních údajů za účelem jejich dalšího uložení na nosič informací pro jejich okamžité nebo pozdější zpracování,

g) uchováváním osobních údajů udržování údajů v takové podobě, která je umožňuje dále zpracovávat,

h) blokováním osobních údajů vytvoření takového stavu, při kterém je osobní údaj určitou dobu nepřístupný a nelze jej jinak zpracovávat,

i) likvidací osobních údajů se rozumí fyzické zničení jejich nosiče, jejich fyzické vymazání nebo jejich trvalé vyloučení z dalších zpracování,

j) správcem každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak,

k) zpracovatelem každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona,

l) zveřejněným osobním údajem osobní údaj zpřístupněný zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu,

m) evidencí nebo datovým souborem osobních údajů (dále jen "datový soubor") jakýkoliv soubor osobních údajů uspořádaný nebo zpřístupnitelný podle společných nebo zvláštních kritérií,

n) souhlasem subjektu údajů svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů,

o) příjemcem každý subjekt, kterému jsou osobní údaje zpřístupněny; za příjemce se nepovažuje subjekt, který zpracovává osobní údaje podle § 3 odst. 6 písm. g).

HLAVA II

PRÁVA A POVINNOSTI PŘI ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

§ 5

(1) Správce je povinen

a) stanovit účel, k němuž mají být osobní údaje zpracovány,

b) stanovit prostředky a způsob zpracování osobních údajů,

c) zpracovat pouze přesné osobní údaje, které získal v souladu s tímto zákonem. Je-li to nezbytné, osobní údaje aktualizuje. Zjistí-li správce, že jím zpracované osobní údaje nejsou s ohledem na stanovený účel přesné, provede bez zbytečného odkladu přiměřená opatření, zejména zpracování blokuje a osobní údaje opraví nebo doplní, jinak osobní údaje zlikviduje. Nepřesné osobní údaje lze zpracovat pouze v mezích uvedených v § 3 odst. 6.[11)] Nepřesné osobní údaje se musí označit. Informaci o blokování, opravě, doplnění nebo likvidaci osobních údajů je správce povinen bez zbytečného odkladu předat všem příjemcům,

d) shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanového účelu,

e) uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování. Po uplynutí této doby mohou být osobní údaje uchovávány pouze pro účely státní statistické služby, pro účely vědecké a pro účely archivnictví. Při použití pro tyto účely je třeba dbát práva na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů, a osobní údaje anonymizovat, jakmile je to možné,

f) zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny. Zpracovávat k jinému účelu lze osobní údaje jen v mezích ustanovení § 3 odst. 6, nebo pokud k tomu dal subjekt údajů předem souhlas,

g) shromažďovat osobní údaje pouze otevřeně; je vyloučeno shromažďovat údaje pod záminkou jiného účelu nebo jiné činnosti,

h) nesdružovat osobní údaje, které byly získány k rozdílným účelům.

(2) Správce může zpracovávat osobní údaje pouze se souhlasem subjektu údajů. Bez tohoto souhlasu je může zpracovávat,

a) jestliže provádí zpracování nezbytné pro dodržení právní povinnosti správce,[12)]

b) jestliže je zpracování nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro jednání o uzavření nebo změně smlouvy uskutečněné na návrh subjektu údajů,

c) pokud je to nezbytně třeba k ochraně životně důležitých zájmů subjektu údajů. V tomto případě je třeba bez zbytečného odkladu získat jeho souhlas. Pokud souhlas není dán, musí správce ukončit zpracování a údaje zlikvidovat,

d) jedná-li se o oprávněně zveřejněné osobní údaje v souladu se zvláštním právním předpisem.[13)] Tím však není dotčeno právo na ochranu soukromého a osobního života subjektu údajů,

e) pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby; takové zpracování osobních údajů však nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života,

f) pokud poskytuje osobní údaje o veřejně činné osobě, funkcionáři či zaměstnanci veřejné správy, které vypovídají o jeho veřejné anebo úřední činnosti, o jeho funkčním nebo pracovním zařazení, nebo

g) jedná-li se o zpracování výlučně pro účely archivnictví podle zvláštního zákona.

(3) Provádí-li správce zpracování osobních údajů na základě zvláštního zákona,12) je povinen dbát práva na ochranu soukromého a osobního života subjektu údajů.

(4) Subjekt údajů musí být při udělení souhlasu informován o tom, pro jaký účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci a na jaké období. Souhlas subjektu údajů se zpracováním osobních údajů musí být správce schopen prokázat po celou dobu zpracování.

(5) Provádí-li správce nebo zpracovatel zpracování osobních údajů za účelem nabízení obchodu nebo služeb subjektu údajů, lze pro tento účel použít jméno, příjmení a adresu subjektu údajů, pokud tyto údaje byly získány z veřejného seznamu nebo v souvislosti se svojí činností jakožto správce nebo zpracovatele. Správce nebo zpracovatel však nesmí uvedené údaje dále zpracovávat, pokud s tím subjekt údajů vyslovil nesouhlas. Nesouhlas se zpracováním je nutné vyjádřit písemně. Bez souhlasu subjektu údajů nelze k uvedeným údajům přiřazovat další osobní údaje.

(6) Správce, který zpracovává osobní údaje podle odstavce 5, může tyto údaje předat jinému správci pouze za splnění těchto podmínek:

a) údaje subjektu údajů byly získány v souvislosti s činností správce nebo se jedná o zveřejněné osobní údaje,

b) údaje budou využívány pouze za účelem nabízení obchodu a služeb,

c) subjekt údajů byl o tomto postupu správce předem informován a nevyslovil s tímto postupem nesouhlas.

(7) Jiný správce, kterému byly předány údaje podle odstavce 6, nesmí tyto údaje předávat jiné osobě.

(8) Nesouhlas se zpracováním podle odstavce 6 písm. c) musí subjekt údajů učinit písemně. Správce je povinen informovat každého správce, kterému předal jméno, příjmení a adresu subjektu údajů, o tom, že subjekt údajů vyslovil nesouhlas se zpracováním.

(9) Za účelem vyloučení možnosti, že jméno, příjmení a adresa subjektu údajů budou opakovaně použity k nabídce obchodu a služeb, je správce oprávněn dále zpracovávat pro svoji vlastní potřebu jméno, příjmení a adresu subjektu údajů přesto, že subjekt údajů vyslovil nesouhlas podle odstavce 5.

§ 6

Pokud zmocnění nevyplývá z právního předpisu, musí správce se zpracovatelem uzavřít smlouvu o zpracování osobních údajů. Smlouva musí mít písemnou formu. Musí v ní být

zejména výslovně uvedeno, v jakém rozsahu, za jakým účelem a na jakou dobu se uzavírá, a musí obsahovat záruky zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů.

§ 7

Povinnosti stanovené v § 5 platí obdobně také pro zpracovatele.

§ 8

Jestliže zpracovatel zjistí, že správce porušuje povinnosti stanovené tímto zákonem, je povinen jej na to neprodleně upozornit a ukončit zpracování osobních údajů. Pokud tak neučiní, odpovídá za škodu, která subjektu údajů vznikla, společně a nerozdílně se správcem údajů. Tím není dotčena jeho odpovědnost podle tohoto zákona.

§ 9

Citlivé údaje

Citlivé údaje je možné zpracovávat, jen jestliže

a) subjekt údajů dal ke zpracování výslovný souhlas. Subjekt údajů musí být při udělení souhlasu informován o tom, pro jaký účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci a na jaké období. Existenci souhlasu subjektu údajů se zpracováním osobních údajů musí být správce schopen prokázat po celou dobu zpracování. Správce je povinen předem subjekt údajů poučit o jeho právech podle § 12 a 21,

b) je to nezbytné v zájmu zachování života nebo zdraví subjektu údajů nebo jiné osoby nebo odvrácení bezprostředního závažného nebezpečí hrozícího jejich majetku, pokud není možno jeho souhlas získat zejména z důvodů fyzické, duševní či právní nezpůsobilosti, v případě, že je nezvěstný nebo z jiných podobných důvodů. Správce musí ukončit zpracování údajů, jakmile pominou uvedené důvody, a údaje musí zlikvidovat, ledaže by subjekt údajů dal k dalšímu zpracování souhlas,

c) se jedná o zpracování při zajišťování zdravotní péče, ochrany veřejného zdraví, zdravotního pojištění a výkon státní správy v oblasti zdravotnictví podle zvláštního zákona[15)] nebo se jedná o posuzování zdravotního stavu v jiných případech stanovených zvláštním zákonem,[15a)]

d) je zpracování nezbytné pro dodržení povinností a práv správce odpovědného za zpracování v oblasti pracovního práva a zaměstnanosti, stanovené zvláštním zákonem,[16)]

e) jde o zpracování, které sleduje politické, filosofické, náboženské nebo odborové cíle, prováděné v rámci oprávněné činnosti občanského sdružení, nadace nebo jiné právnické osoby nevýdělečné povahy (dále jen "sdružení"), a které se týká pouze členů sdružení nebo osob, se kterými je sdružení v opakujícím se kontaktu souvisejícím s oprávněnou činností sdružení, a osobní údaje nejsou zpřístupňovány bez souhlasu subjektu údajů,

f) se jedná o údaje podle zvláštního zákona nezbytné pro provádění nemocenského pojištění, důchodového pojištění (zabezpečení), státní sociální podpory a dalších státních sociálních dávek, sociální péče a sociálně-právní ochrany dětí, a při zajištění ochrany těchto údajů v souladu se zákonem,

g) se zpracování týká osobních údajů zveřejněných subjektem údajů,

h) je zpracování nezbytné pro zajištění a uplatnění právních nároků, nebo

ch) jsou zpracovány výlučně pro účely archivnictví podle zvláštního zákona.

§ 10

Při zpracování osobních údajů správce a zpracovatel dbá, aby subjekt údajů neutrpěl újmu na svých právech, zejména na právu na zachování lidské důstojnosti, a také dbá na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů.

§ 11

(1) Správce je při shromažďování osobních údajů povinen subjekt údajů informovat o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny, nejsou-li subjektu údajů tyto informace již známy. Správce musí subjekt údajů informovat o jeho právu přístupu k osobním údajům, právu na opravu osobních údajů, jakož i o dalších právech stanovených v § 21.

(2) V případě, kdy správce zpracovává osobní údaje získané od subjektu údajů, musí subjekt údajů poučit o tom, zda je poskytnutí osobního údaje povinné či dobrovolné. Je-li subjekt údajů povinen podle zvláštního zákona osobní údaje pro zpracování poskytnout, poučí jej správce o této skutečnosti, jakož i o následcích odmítnutí poskytnutí osobních údajů.

(3) Informace a poučení podle odstavce 1 není povinen správce poskytovat v případech, kdy osobní údaje nezískal od subjektu údajů, pokud

a) zpracovává osobní údaje výlučně pro účely výkonu státní statistické služby, vědecké nebo archivní účely a poskytnutí takových informací by vyžadovalo neúměrné úsilí nebo nepřiměřeně vysoké náklady; nebo pokud ukládání na nosiče informací nebo zpřístupnění je výslovně stanoveno zvláštním zákonem. V těchto případech je správce povinen přijmout potřebná opatření proti neoprávněnému zasahování do soukromého a osobního života subjektu údajů,

b) zpracování osobních údajů mu ukládá zvláštní zákon nebo je takových údajů třeba k uplatnění práv a povinností vyplývajících ze zvláštních zákonů,

c) zpracovává výlučně oprávněně zveřejněné osobní údaje, nebo

d) zpracovává osobní údaje získané se souhlasem subjektu údajů.

(4) Předchozími ustanoveními nejsou dotčena práva subjektu údajů požadovat informace podle zvláštních zákonů.[18)]

(5) Při zpracování osobních údajů podle § 5 odst. 2 písm. e) a § 9 písm. h) je správce povinen bez zbytečného odkladu subjekt údajů informovat o zpracování jeho osobních údajů.

(6) Žádné rozhodnutí správce nebo zpracovatele, jehož důsledkem je zásah do právních a právem chráněných zájmů subjektu údajů, nelze bez ověření vydat nebo učinit výlučně na základě automatizovaného zpracování osobních údajů. To neplatí v případě, že takové rozhodnutí bylo učiněno ve prospěch subjektu údajů a na jeho žádost.

(7) Informační povinnost upravenou v § 11 může za správce plnit zpracovatel.

§ 12

Přístup subjektu údajů k informacím

(1) Požádá-li subjekt údajů o informaci o zpracování svých osobních údajů, je mu správce povinen tuto informaci bez zbytečného odkladu předat.

(2) Obsahem informace je vždy sdělení o

a) účelu zpracování osobních údajů,

b) osobních údajích, případně kategoriích osobních údajů, které jsou předmětem zpracování, včetně veškerých dostupných informací o jejich zdroji,

c) povaze automatizovaného zpracování v souvislosti s jeho využitím pro rozhodování, jestliže jsou na základě tohoto zpracování činěny úkony nebo rozhodnutí, jejichž obsahem je zásah do práva a oprávněných zájmů subjektu údajů,

d) příjemci, případně kategoriích příjemců.

(3) Správce má právo za poskytnutí informace požadovat přiměřenou úhradu nepřevyšující náklady nezbytné na poskytnutí informace.

(4) Povinnost správce poskytnout informace subjektu údajů upravenou v § 12 může za správce plnit zpracovatel.

§ 13

Povinnosti osob při zabezpečení osobních údajů

(1) Správce a zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů.

(2) Správce nebo zpracovatel je povinen zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy.

§ 14

Zaměstnanci správce nebo zpracovatele a jiné osoby, které zpracovávají osobní údaje na základě smlouvy se správcem nebo zpracovatelem, mohou zpracovávat osobní údaje pouze za podmínek a v rozsahu správcem nebo zpracovatelem stanoveném.

§ 15

(1) Zaměstnanci správce nebo zpracovatele, jiné fyzické osoby, které zpracovávají osobní údaje na základě smlouvy se správcem nebo zpracovatelem, a další osoby, které v rámci plnění zákonem stanovených oprávnění a povinností přicházejí do styku s osobními údaji u správce nebo zpracovatele, jsou povinni zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů. Povinnost mlčenlivosti trvá i po skončení zaměstnání nebo příslušných prací.

(2) Ustanovením předchozího odstavce není dotčena povinnost zachovávat mlčenlivost podle zvláštních zákonů.[19)]

(3) Povinnost zachovávat mlčenlivost se nevztahuje na informační povinnost podle zvláštních zákonů.[20)]

§ 16

Oznamovací povinnost

(1) Ten, kdo hodlá jako správce zpracovávat osobní údaje nebo změnit registrované zpracování podle tohoto zákona, s výjimkou zpracování uvedených v § 18, je povinen tuto skutečnost písemně oznámit Úřadu před zpracováváním osobních údajů.

(2) Oznámení musí obsahovat tyto informace:

a) identifikační údaje správce, u fyzické osoby, která není podnikatelem, jméno, popřípadě jména, příjmení, datum narození a adresu místa trvalého pobytu, u jiných subjektů obchodní firmu nebo název, sídlo a identifikační číslo, pokud bylo přiděleno, a jméno, popřípadě jména, a příjmení osob, které jsou jejich statutárními zástupci,

b) účel nebo účely zpracování,

c) kategorie subjektů údajů a osobních údajů, které se těchto subjektů týkají,

d) zdroje osobních údajů,

e) popis způsobu zpracování osobních údajů,

f) místo nebo místa zpracování osobních údajů,

g) příjemce nebo kategorie příjemců,

h) předpokládaná předání osobních údajů do jiných států,

i) popis opatření k zajištění ochrany osobních údajů podle § 13.

(3) Obsahuje-li oznámení všechny náležitosti podle odstavce 2 a není-li zahájeno řízení podle § 17 odst. 1, lze po uplynutí lhůty 30 dnů ode dne doručení oznámení zahájit zpracování osobních údajů. Úřad v takovém případě zapíše informace uvedené v oznámení do registru.

(4) Neobsahuje-li oznámení všechny náležitosti podle odstavce 2, Úřad neprodleně zašle oznamovateli výzvu, v níž upozorní na chybějící nebo nedostatečné informace a stanoví lhůtu k doplnění oznámení. V případě doplnění oznámení začíná běžet lhůta podle odstavce 3 dnem doručení doplnění oznámení. V případě, že Úřad neobdrží doplnění oznámení ve stanovené

lhůtě, nahlíží na učiněné oznámení tak, jako by nebylo podáno.

(5) O provedení registrace vydá Úřad na žádost správce osvědčení, které obsahuje datum vyhotovení, číslo jednací, jméno, příjmení a podpis osoby, která osvědčení vydala, otisk úředního razítka, identifikační údaje správce a účel zpracování.

(6) Na postup Úřadu podle odstavců 1 až 5 se nevztahuje správní řád.

§ 17

(1) Vznikne-li z oznámení důvodná obava, že při zpracování osobních údajů by mohlo dojít k porušení tohoto zákona, zahájí Úřad z vlastního podnětu řízení.

(2) Zjistí-li Úřad, že oznámeným zpracováním neporušuje správce podmínky stanovené tímto zákonem, řízení zastaví a provede zápis podle § 16 odst. 3. Nejdříve dnem následujícím po provedení zápisu lze zahájit zpracování osobních údajů. V případě, že oznámené zpracování nesplňuje podmínky stanovené tímto zákonem, zpracování osobních údajů Úřad nepovolí.

§ 17a

(1) Zjistí-li Úřad, že správce, jehož oznámení bylo zapsáno do registru, porušuje podmínky stanovené tímto zákonem, rozhodne o zrušení registrace.

(2) Pomine-li účel, pro který bylo zpracování zaregistrováno, Úřad z vlastního podnětu nebo na žádost správce rozhodne o zrušení registrace.

§ 18

(1) Oznamovací povinnost podle § 16 se nevztahuje na zpracování osobních údajů,

a) které jsou součástí datových souborů veřejně přístupných na základě zvláštního zákona,

b) které správci ukládá zvláštní zákon nebo je takových osobních údajů třeba k uplatnění práv a povinností vyplývajících ze zvláštního zákona, nebo

c) jde-li o zpracování, které sleduje politické, filosofické, náboženské nebo odborové cíle, prováděné v rámci oprávněné činnosti sdružení, a které se týká pouze členů sdružení, nebo osob, se kterými je sdružení v opakujícím se kontaktu souvisejícím s oprávněnou činností sdružení, a osobní údaje nejsou zpřístupňovány bez souhlasu subjektu údajů.

(2) Správce, který provádí zpracování podle § 18 odst. 1 písm. b), je povinen zajistit, aby informace, týkající se zejména účelu zpracování, kategorií osobních údajů, kategorií subjektů údajů, kategorií příjemců a doby uchování, které by byly jinak přístupné prostřednictvím registru vedeného Úřadem podle § 35, byly zpřístupněny, a to i dálkovým přístupem nebo jinou vhodnou formou.

§ 19

Jestliže správce hodlá ukončit svoji činnost, je povinen Úřadu neprodleně oznámit, jak naložil s osobními údaji, pokud se na jejich zpracování vztahuje oznamovací povinnost.

§ 20

Likvidace osobních údajů

(1) Správce nebo na základě jeho pokynu zpracovatel je povinen provést likvidaci osobních údajů, jakmile pomine účel, pro který byly osobní údaje zpracovány, nebo na základě žádosti subjektu údajů podle § 21.

(2) Zvláštní zákon stanoví výjimky týkající se uchovávání osobních údajů pro účely archivnictví a uplatňování práv v občanském soudním řízení, trestním řízení a správním řízení.

§ 21

(1) Každý subjekt údajů, který zjistí nebo se domnívá, že správce nebo zpracovatel provádí zpracování jeho osobních údajů, které je v rozporu s ochranou soukromého a osobního života subjektu údajů nebo v rozporu se zákonem, zejména jsou-li osobní údaje nepřesné s ohledem na účel jejich zpracování, může

a) požádat správce nebo zpracovatele o vysvětlení,

b) požadovat, aby správce nebo zpracovatel odstranil takto vzniklý stav. Zejména se může jednat o blokování, provedení opravy, doplnění nebo likvidaci osobních údajů.

(2) Je-li žádost subjektu údajů podle odstavce 1 shledána oprávněnou, správce nebo zpracovatel odstraní neprodleně závadný stav.

(3) Nevyhoví-li správce nebo zpracovatel žádosti subjektu údajů podle odstavce 1, má subjekt údajů právo obrátit se přímo na Úřad.

(4) Postup podle odstavce 1 nevylučuje, aby se subjekt údajů obrátil se svým podnětem na Úřad přímo.

(5) Pokud vznikla v důsledku zpracování osobních údajů subjektu údajů jiná než majetková újma, postupuje se při uplatňování jejího nároku podle zvláštního zákona.[22)]

(6) Došlo-li při zpracování osobních údajů k porušení povinností uložených zákonem u správce nebo u zpracovatele, odpovídají za ně společně a nerozdílně.

(7) Správce je povinen bez zbytečného odkladu informovat příjemce o žádosti subjektu údajů podle odstavce 1 a o blokování, opravě, doplnění nebo likvidaci osobních údajů. To neplatí, pokud je informování příjemce nemožné nebo by vyžadovalo neúměrné úsilí.

§ 22 až 24

zrušeny

§ 25

Náhrada škody

V otázkách neupravených tímto zákonem se použije obecná úprava odpovědnosti za škodu.[23),24)]

§ 26

Povinnosti podle § 21 až 25 se obdobně vztahují i na osoby, které shromáždily osobní údaje neoprávněně.

HLAVA III

PŘEDÁNÍ OSOBNÍCH ÚDAJŮ

§ 27

(1) Volný pohyb osobních údajů nemůže být omezován, pokud jsou údaje předány do členského státu Evropské unie.

(2) Do třetích zemí mohou být osobní údaje předány, pokud zákaz omezování volného pohybu osobních údajů vyplývá z mezinárodní smlouvy, k jejíž ratifikaci dal Parlament souhlas, a kterou je Česká republika vázána,1a) nebo jsou osobní údaje předány na základě rozhodnutí orgánu Evropské unie. Informace o těchto rozhodnutích zveřejňuje Úřad ve Věstníku.

(3) Není-li podmínka podle odstavců 1 a 2 splněna, může být předání osobních údajů uskutečněno, jestliže správce prokáže, že

a) předání údajů se děje se souhlasem nebo na základě pokynu subjektu údajů,

b) jsou v třetí zemi, kde mají být osobní údaje zpracovány, vytvořeny dostatečné zvláštní záruky ochrany osobních údajů, například prostřednictvím jiných právních nebo profesních předpisů a bezpečnostních opatření. Takové záruky mohou být upřesněny zejména smlouvou uzavřenou mezi správcem a příjemcem, pokud tato smlouva zajišťuje uplatnění těchto požadavků nebo pokud smlouva obsahuje smluvní doložky pro předání osobních údajů do třetích zemí zveřejněné ve Věstníku Úřadu,

c) jde o osobní údaje, které jsou na základě zvláštního zákona součástí datových souborů veřejně přístupných nebo přístupných tomu, kdo prokáže právní zájem; v takovém případě lze osobní údaje zpřístupnit jen v rozsahu a za podmínek stanovených zvláštním zákonem,

d) je předání nutné pro uplatnění důležitého veřejného zájmu vyplývajícího ze zvláštního zákona nebo z mezinárodní smlouvy, kterou je Česká republika vázána,

e) je předání nezbytné pro jednání o uzavření nebo změně smlouvy, uskutečněné z podnětu subjektu údajů, nebo pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů,

f) je předání nezbytné pro plnění smlouvy uzavřené v zájmu subjektu údajů mezi správcem a třetí stranou, nebo pro uplatnění jiných právních nároků, nebo

g) je předání nezbytné pro ochranu práv nebo životně důležitých zájmů subjektu údajů, zejména pro záchranu života nebo pro poskytnutí zdravotní péče.

(4) Před předáním osobních údajů do třetích zemí podle odstavce 3 je správce povinen požádat Úřad o povolení k předání, nestanoví-li zvláštní zákon jinak.[25)] Při posuzování žádosti Úřad přezkoumá všechny okolnosti související s předáním osobních údajů, zejména zdroj, konečné určení a kategorie předávaných osobních údajů, účel a dobu zpracování, s přihlédnutím k dostupným informacím o právních nebo jiných předpisech upravujících zpracování osobních údajů ve třetí zemi. V povolení k předání Úřad stanoví dobu, po kterou může správce předání

provádět. Pokud dojde ke změně podmínek, za kterých bylo povolení vydáno, zejména na základě rozhodnutí orgánu Evropské unie, Úřad toto povolení změní nebo zruší.

HLAVA IV

POSTAVENÍ A PŮSOBNOST ÚŘADU

§ 28

(1) Úřad je nezávislý orgán. Ve své činnosti postupuje nezávisle a řídí se pouze zákony a jinými právními předpisy.

(2) Do činnosti Úřadu lze zasahovat jen na základě zákona.

(3) Činnost Úřadu je hrazena ze samostatné kapitoly státního rozpočtu České republiky.

§ 29

(1) Úřad

a) provádí dozor nad dodržováním povinností stanovených tímto zákonem,

b) vede registr zpracování osobních údajů,

c) přijímá podněty a stížnosti na porušení tohoto zákona a informuje o jejich vyřízení,

d) zpracovává a veřejnosti zpřístupňuje výroční zprávu o své činnosti,

e) vykonává další působnosti stanovené mu zákonem,

f) projednává přestupky a jiné správní delikty a uděluje pokuty podle tohoto zákona,

g) zajišťuje plnění požadavků vyplývajících z mezinárodních smluv, jimiž je Česká republika vázána,

h) poskytuje konzultace v oblasti ochrany osobních údajů,

i) spolupracuje s obdobnými úřady jiných států, s orgány Evropské unie a s orgány mezinárodních organizací působícími v oblasti ochrany osobních údajů. Úřad v souladu s právem Evropských společenství plní oznamovací povinnost vůči orgánům Evropské unie.[25a)]

(2) Při výkonu dozoru ve formě kontroly se postupuje podle zvláštního právního předpisu.[26)]

(3) Dozor nad zpracováním osobních údajů, které provádějí zpravodajské služby, stanoví zvláštní právní předpis.[27)]

HLAVA V

ORGANIZACE ÚŘADU

§ 30

(1) Zaměstnanci Úřadu jsou předseda, inspektoři a další zaměstnanci.

(2) Kontrolní činnost Úřadu provádějí inspektoři a pověření zaměstnanci (dále jen "kontrolující").

(3) Na zaměstnance Úřadu se vztahují ustanovení zákoníku práce, pokud tento zákon nestanoví jinak.

(4) Předseda Úřadu má nárok na plat, náhradu výdajů a naturální plnění jako prezident Nejvyššího kontrolního úřadu podle zvláštního zákona.[26a)]

(5) Inspektoři Úřadu mají nárok na plat, náhradu výdajů a naturální plnění jako členové Nejvyššího kontrolního úřadu podle zvláštního zákona.[26a)]

§ 31

Kontrolní činnost Úřadu se provádí na základě kontrolního plánu nebo na základě podnětů a stížností.

§ 32

Předseda Úřadu

(1) Úřad řídí předseda, kterého jmenuje a odvolává prezident republiky na návrh Senátu Parlamentu České republiky.

(2) Předseda Úřadu je jmenován na dobu 5 let. Může být jmenován maximálně na 2 po sobě jdoucí období.

(3) Předsedou Úřadu může být jmenován pouze občan České republiky, který

a) je způsobilý k právním úkonům,

b) je bezúhonný, splňuje podmínky stanovené zvláštním právním předpisem[30)] a jeho znalosti, zkušenosti a morální vlastnosti jsou předpokladem, že bude svoji funkci řádně zastávat,

c) má ukončené vysokoškolské vzdělání.

(4) Bezúhonnou je pro účel tohoto zákona fyzická osoba, která nebyla pravomocně odsouzena pro úmyslný trestný čin nebo i trestný čin spáchaný z nedbalosti v souvislosti se zpracováním osobních údajů.

(5) S výkonem funkce předsedy Úřadu je neslučitelná funkce poslance nebo senátora, soudce, státního zástupce, jakákoliv funkce ve veřejné správě, funkce člena orgánů územní samosprávy a členství v politických stranách a hnutích.

(6) Předseda Úřadu nesmí zastávat jinou placenou funkci, být v dalším pracovním poměru ani vykonávat výdělečnou činnost s výjimkou správy vlastního majetku a činnosti vědecké, pedagogické, literární, publicistické a umělecké, pokud tato činnost nenarušuje důstojnost nebo neohrožuje důvěru v nezávislost a nestrannost Úřadu.

(7) Z funkce je předseda Úřadu odvolán, přestal-li splňovat některou z podmínek pro jeho jmenování.

(8) Z funkce může být předseda odvolán také tehdy, jestliže nevykonává po dobu 6 měsíců svoji funkci.

§ 33

Inspektoři Úřadu

(1) Inspektora jmenuje a odvolává prezident republiky na návrh Senátu Parlamentu České republiky.

(2) Inspektor je jmenován na období 10 let. Může být jmenován opakovaně.

(3) Inspektor vykonává kontrolu, řídí kontrolu, vypracovává kontrolní protokol a provádí další úkony, jež souvisejí s úkoly Úřadu.

(4) Činnosti podle odstavce 3 vykonává 7 inspektorů Úřadu.

§ 34

(1) Inspektorem může být jmenován občan České republiky, který je způsobilý k právním úkonům, bezúhonný, splňuje podmínky stanovené zvláštním právním předpisem30) a má ukončené odborné vysokoškolské vzdělání.

(2) S výkonem funkce inspektora je neslučitelná funkce poslance nebo senátora, soudce, státního zástupce, jakákoliv funkce ve veřejné správě, funkce člena orgánů územní samosprávy a členství v politických stranách a hnutích. Inspektor nesmí zastávat jinou placenou funkci, být v pracovním poměru ani vykonávat výdělečnou činnost s výjimkou správy vlastního majetku a činnosti vědecké, pedagogické, literární, publicistické a umělecké, pokud tato činnost nenarušuje důstojnost nebo neohrožuje důvěru v nezávislost a nestrannost Úřadu.

(3) Z funkce je inspektor odvolán, přestal-li splňovat některou z podmínek pro jeho jmenování.

HLAVA VI

ČINNOST ÚŘADU

§ 35

Registr

(1) Do registru zpracování osobních údajů se k osobám správců zapisují informace z oznámení podle § 16 odst. 2 a datum provedení, případně zrušení registrace.

(2) Informace zapsané do registru, s výjimkou informací uvedených v § 16 odst. 2 písm. e) a i), jsou veřejně přístupné, zejména způsobem umožňujícím dálkový přístup.

(3) Zrušení registrace podle § 17a oznamuje Úřad ve Věstníku Úřadu.

§ 36

Výroční zpráva

(1) Výroční zpráva Úřadu obsahuje zejména informace o provedené kontrolní činnosti a její zhodnocení, informace a zhodnocení stavu v oblasti zpracovávání a ochrany osobních údajů v České republice a zhodnocení ostatní činnosti Úřadu.

(2) Výroční zprávu předkládá předseda Úřadu pro informaci Poslanecké sněmovně a Senátu

Parlamentu České republiky a vládě České republiky do 2 měsíců po skončení rozpočtového roku a zveřejňuje ji.

§ 37

Oprávnění kontrolujících

Kontrolující jsou při provádění kontroly oprávněni

a) vstupovat do objektů, zařízení a provozů, na pozemky a do jiných prostor kontrolovaných správců a zpracovatelů nebo každého, kdo zpracovává osobní údaje, (dále jen "kontrolovaný"), pokud to souvisí s předmětem kontroly; do obydlí mohou vstupovat pouze v případě, že tato slouží také k provozování podnikatelské činnosti,

b) požadovat na kontrolovaných a na jiných osobách, aby ve stanovených lhůtách předložily originální doklady a další písemnosti, záznamy dat na paměťových médiích, výpisy a zdrojové kódy programů, pokud je vlastní, výpisy a opisy dat (dále jen "doklady"), pokud to souvisí s předmětem kontroly, a provádět vlastní dokumentaci,

c) seznamovat se s utajovanými informacemi za podmínek stanovených zvláštním právním předpisem,[31)] jakož i dalšími skutečnostmi, které jsou chráněny povinností mlčenlivosti,

d) požadovat na fyzických i právnických osobách poskytnutí pravdivých a úplných informací o zjišťovaných a souvisejících skutečnostech,

e) zajišťovat v odůvodněných případech doklady; jejich převzetí musí kontrolovanému písemně potvrdit a na jeho žádost mu ponechat kopie převzatých dokladů,

f) pořídit kopie obsahu paměťových médií, obsahujících osobní údaje, nacházejících se u kontrolovaného,

g) požadovat, aby kontrolovaní podali ve stanovené lhůtě písemnou zprávu o odstranění zjištěných nedostatků,

h) používat telekomunikační zařízení kontrolovaných v případech, kdy je jejich použití nezbytné pro zabezpečení kontroly.

§ 38

Povinnosti kontrolujících

(1) Kontrolu nesmějí provádět ti kontrolující, u nichž se zřetelem na jejich vztah ke kontrolovaným nebo k předmětu kontroly jsou důvodné pochybnosti o jejich nepodjatosti.

(2) Kontrolující je povinen bezprostředně po tom, co se dozví o skutečnostech nasvědčujících jeho podjatosti, oznámit to předsedovi Úřadu.

(3) O námitce podjatosti kontrolujícího rozhodne předseda Úřadu bez zbytečného odkladu. Do rozhodnutí o námitce podjatosti činí kontrolující pouze úkony, které nesnesou odkladu.

(4) Proti rozhodnutí o námitce podjatosti se nelze odvolat.

(5) Kontrolující jsou povinni

a) prokázat se kontrolovanému průkazem, jehož vzor upraví nařízení vlády,

b) oznámit kontrolovanému zahájení kontroly,

c) šetřit práva a právem chráněné zájmy kontrolovaných,

d) předat neprodleně převzaté doklady, jakož i kopie paměťových médií kontrolovanému, pominou-li důvody jejich převzetí,

e) řádně ochraňovat zajištěné doklady proti jejich ztrátě, zničení, poškození nebo zneužití,

f) pořizovat o výsledcích kontroly kontrolní protokol,

g) zachovávat mlčenlivost o skutečnostech zjištěných při výkonu kontroly a nezneužít znalosti těchto skutečností. Povinností mlčenlivosti není dotčena oznamovací povinnost podle zvláštních zákonů. Povinnost mlčenlivosti přetrvává i po skončení pracovněprávního vztahu k Úřadu. Povinnosti mlčenlivosti může kontrolujícího zbavit předseda Úřadu. Povinnost mlčenlivosti se nevztahuje na anonymizované a zobecněné informace.

(6) Kontrolní protokol obsahuje zejména popis zjištěných skutečností s uvedením nedostatků a označení ustanovení právních předpisů, které byly porušeny, a opatření, která byla uložena k nápravě, a stanovení lhůt, do kdy je třeba je učinit. V kontrolním protokolu se uvádí označení Úřadu a jména kontrolujících na kontrole zúčastněných, označení kontrolovaného, místo a čas provedení kontroly, předmět kontroly, skutečný stav, označení dokladů a ostatních dokumentů a zjištění, o které se protokol opírá. Kontrolní protokol podepisují kontrolující, kteří se kontroly zúčastnili.

(7) Povinností kontrolujících je seznámit kontrolované s obsahem kontrolního protokolu a předat jim jeho stejnopis. Seznámení s kontrolním protokolem a jeho převzetí potvrzují kontrolovaní podpisem kontrolního protokolu. Odmítne-li kontrolovaný seznámit se s kontrolním protokolem nebo toto seznámení potvrdit, vyznačí se tyto skutečnosti v kontrolním protokolu.

§ 39

(1) Každý je povinen v souvislosti s výkonem kontroly poskytnout kontrolujícím při výkonu jejich činnosti potřebnou součinnost.

(2) Tomu, kdo neposkytne Úřadu při výkonu kontroly potřebnou součinnost, může být uložena pořádková pokuta do výše 25 000 Kč, a to i opakovaně. Za neposkytnutí součinnosti se považuje i nesplnění opatření uložených k nápravě zjištěného stavu ve stanovené lhůtě.

Opatření k nápravě

§ 40

(1) Zjistí-li kontrolující, že došlo k porušení povinností uložených tímto zákonem, uloží inspektor, jaká opatření je třeba učinit, aby byly zjištěné nedostatky odstraněny, a stanoví lhůtu pro jejich odstranění.

(2) Byla-li uložena likvidace osobních údajů, jsou osobní údaje do likvidace blokovány. Proti uložení likvidace může správce podat námitku k předsedovi Úřadu. Do doby, než bude o námitce rozhodnuto, musí být osobní údaje blokovány. Proti rozhodnutí předsedy lze podat

žalobu podle předpisů o správním soudnictví. Do doby, než bude soudem rozhodnuto, jsou údaje blokovány.

(3) Kontrolovaný je povinen ve stanovené lhůtě podat zprávu o přijatých opatřeních.

§ 41

V řízení ve věcech upravených tímto zákonem se postupuje podle správního řádu,[32)] pokud ustanovení tohoto zákona nestanoví jinak.

§ 42

Provozováním informačních systémů nakládajících s osobními údaji podle dosavadních předpisů se rozumí zpracování osobních údajů.

§ 43

Oprávnění a povinnosti při dozoru

Oprávnění a povinnosti kontrolujících a kontrolovaných osob se řídí zvláštním právním předpisem,26) pokud tento zákon nestanoví jinak.

HLAVA VII

SANKCE

§ 44

Přestupky

(1) Fyzická osoba, která

a) je ke správci nebo zpracovateli v pracovním nebo jiném obdobném poměru,

b) vykonává pro správce nebo zpracovatele činnosti na základě dohody, nebo

c) v rámci plnění zvláštním zákonem uložených oprávnění a povinností přichází u správce nebo zpracovatele do styku s osobními údaji, se dopustí přestupku tím, že poruší povinnost mlčenlivosti (§ 15).

(2) Fyzická osoba se jako správce nebo zpracovatel dopustí přestupku tím, že při zpracování osobních údajů

a) nestanoví účel, prostředky nebo způsob zpracování [§ 5 odst. 1 písm. a) a b)] nebo stanoveným účelem zpracování poruší povinnost nebo překročí oprávnění vyplývající ze zvláštního zákona,

b) zpracovává nepřesné osobní údaje [§ 5 odst. 1 písm. c)],

c) shromažďuje nebo zpracovává osobní údaje v rozsahu nebo způsobem, který neodpovídá stanovenému účelu [§ 5 odst. 1 písm. d), f) až h)],

d) uchovává osobní údaje po dobu delší než nezbytnou k účelu zpracování [§ 5 odst. 1 písm. e)],

e) zpracovává osobní údaje bez souhlasu subjektu údajů mimo případy uvedené v zákoně (§ 5 odst. 2 a § 9),

f) neposkytne subjektu údajů informace v rozsahu nebo zákonem stanoveným způsobem (§ 11),

g) odmítne subjektu údajů poskytnout požadované informace (§ 12 a 21),

h) nepřijme nebo neprovede opatření pro zajištění bezpečnosti zpracování osobních údajů (§ 13),

i) nesplní oznamovací povinnost podle tohoto zákona (§ 16 a 27).

(3) Fyzická osoba se jako správce nebo zpracovatel dopustí přestupku tím, že při zpracování osobních údajů některým ze způsobů podle odstavce 2

a) ohrozí větší počet osob svým neoprávněným zasahováním do soukromého a osobního života, nebo

b) poruší povinnosti pro zpracování citlivých údajů (§ 9).

(4) Za přestupek podle odstavce 1 lze uložit pokutu do výše 100 000 Kč.

(5) Za přestupek podle odstavce 2 lze uložit pokutu do výše 1 000 000 Kč.

(6) Za přestupek podle odstavce 3 lze uložit pokutu do výše 5 000 000 Kč.

§ 45

Jiné správní delikty

(1) Právnická osoba nebo fyzická osoba podnikající podle zvláštních předpisů se jako správce nebo zpracovatel dopustí správního deliktu tím, že při zpracování osobních údajů

a) nestanoví účel, prostředky nebo způsob zpracování [§ 5 odst. 1 písm. a) a b)], nebo stanoveným účelem zpracování poruší povinnost nebo překročí oprávnění vyplývající ze zvláštního zákona,

b) zpracovává nepřesné osobní údaje [§ 5 odst. 1 písm. c)],

c) shromažďuje nebo zpracovává osobní údaje v rozsahu nebo způsobem, který neodpovídá stanovenému účelu [§ 5 odst. 1 písm. d), f) až h)],

d) uchovává osobní údaje po dobu delší než nezbytnou k účelu zpracování [§ 5 odst. 1 písm. e)],

e) zpracovává osobní údaje bez souhlasu subjektu údajů mimo případy uvedené v zákoně (§ 5 odst. 2 a § 9),

f) neposkytne subjektu údajů informace v rozsahu nebo zákonem stanoveným způsobem (§ 11),

g) odmítne subjektu údajů poskytnout požadované informace (§ 12 a 21),

h) nepřijme nebo neprovede opatření pro zajištění bezpečnosti zpracování osobních údajů (§ 13),

i) nesplní oznamovací povinnost podle tohoto zákona (§ 16 a 27).

(2) Právnická osoba jako správce nebo zpracovatel se dopustí správního deliktu tím, že při zpracování osobních údajů některým ze způsobů podle odstavce 1

a) ohrozí větší počet osob svým neoprávněným zasahováním do soukromého a osobního života, nebo

b) poruší povinnosti pro zpracování citlivých údajů (§ 9).

(3) Za správní delikt podle odstavce 1 se uloží pokuta do výše 5 000 000 Kč.

(4) Za správní delikt podle odstavce 2 se uloží pokuta do výše 10 000 000 Kč.

§ 46

(1) Právnická osoba za správní delikt neodpovídá, jestliže prokáže, že vynaložila veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránila.

(2) Při rozhodování o výši pokuty se přihlíží zejména k závažnosti, způsobu, době trvání a následkům protiprávního jednání a k okolnostem, za nichž bylo protiprávní jednání spácháno.

(3) Odpovědnost právnické osoby za správní delikt zaniká, jestliže správní orgán o něm nezahájil řízení do 1 roku ode dne, kdy se o něm dozvěděl, nejpozději však do 3 let ode dne, kdy byl spáchán.

(4) Porušení povinností podle § 44 a 45 projednává Úřad.

(5) Na odpovědnost za jednání, k němuž došlo při podnikání fyzické osoby nebo v přímé souvislosti s ním, se použijí ustanovení o odpovědnosti a postihu právnické osoby.

(6) Pokuta je splatná do 30 dnů ode dne, kdy rozhodnutí o jejím uložení nabylo právní moci.

(7) Pokutu vybírá Úřad a vymáhá místně příslušný celní úřad podle zvláštního zákona.[34)] Výnos z pokut je příjmem státního rozpočtu.

HLAVA VIII

USTANOVENÍ SPOLEČNÁ, PŘECHODNÁ A ZÁVĚREČNÁ

§ 47

Opatření pro přechodné období

(1) Každý, kdo zpracovává ke dni nabytí účinnosti tohoto zákona osobní údaje a na něhož se vztahuje povinnost oznámení podle § 16, je povinen tak učinit nejpozději do 6 měsíců ode dne nabytí účinnosti tohoto zákona.

(2) Zpracování osobních údajů prováděné před účinností tohoto zákona je nutno uvést do souladu s tímto zákonem do 31. prosince 2001.

(3) V případě, že kontrolující zjistí porušení povinnosti podle odstavce 2, ustanovení § 46 odst. 1 a 2 se v takovém případě do 31. prosince 2002 nepoužijí.

§ 48

Zrušovací ustanovení

Zrušuje se zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech.

ČÁST ČTVRTÁ

ÚČINNOST

§ 51

Tento zákon nabývá účinnosti dnem 1. června 2000, s výjimkou ustanovení § 16, 17 a 35, která nabývají účinnosti dnem 1. prosince 2000.

Otázky a úkoly ke kapitole VIII:

1. porovnejte kompetence Úřadu pro ochranu osobních údajů a Telekomunikačního úřadu na základě informací z www.uoou.cz a www.ctu.cz .

2. zpracujte studii stanoviska Úřadu pro ochranu osobních údajů na základě www.uoou.cz

3. co obsahuje stránka www.uoou.cz ?

4. jaké jsou webové adresy úřadů pro ochranu osobních údajů v EU ?

5. jaké jsou webové adresy telekomunikačních úřadů v EU ?

12 Přílohy

12.1 Varovné modely: Enron a WorldCom:

12.1.1 Účetní skandály

V roce 2002 zasáhla veřejnost ve Spojených státech vlna izolovaných a často i propojených účetních skandálů. V několika případech se jednalo o podvody v miliardách USD.
Protože probíhá v současnosti konvergence energetických a telekomunikačních sítí (i v ČR je možný přístup k internetu pomocí energetické sítě) byla vybrána jako varovný model významná energetická firma.

12.1.2 Enron

Americká energetická společnost Enron byl založen v Houstonu v Texasu. Před svým bankrotem v závěru roku 2001, měl Enron více než 21 000 zaměstnanců a byl jedním z největších světových obchodníků s elektřinou, zemním plynem, celulózou a papírem. Patřil mezi přední společnosti na trhu s komunikacemi s celkovými příjmy 111 miliard USD v roce 2000. Fortune (ekonomický časopis) charakterizoval Enron jako„nejprogresivnější americkou společnost“ za uplynulých šest let. Na konci roku 2001 došlo k odhalení skutečnosti, že oznámený stav financí byl z valné části ovlivněn promyšleným a systematickým připraveným účetním podvodem na kterém se podílela i auditorská firma.

12.1.3 Počátek společnosti

Enron byl založen v roce 1985 když se po jednání zorganizovaném HNG CEO (Chief Executive Office – výkonný předseda společnosti) Kennethem Layem spojily společnosti Houston Natural Gas a Internorth. Lay se stal CEO spojených společností a ihned přejmenoval HNG/InterNorth na Enron Corporation s novým sídlem v Houstonu. Enron se na začátku své činnosti zabýval přenosem a distribucí elektřiny a plynu po celých Spojených státech a vývojem, konstrukcí a provozem elektráren, ropovodů a další infrastruktury po celém světě.V průběhu prvních let po fúzi, Enron spolupracoval v oblasti ropného průmyslu se společností Spektrum 7, jejíž předseda a CEO byl Georgie W. Bush, syn tehdejšího vice-presidenta Georgie H. W. Buse. V roce 1998 se Enron zaměřil na obchod s vodou vytvořením společnosti Azurix Corporation. Azurix se vstupem na trh s užitkovou vodou neuspěl a jeden z jejich hlavních investičních záměrů v Buenos Aires v Argentině představoval jeden z velkých finančních neúspěchů. V dubnu 2001 Enron oznámil svůj záměr společnost Azurix zrušit a odprodat její aktiva.
Společnost Enron zabezpečila svůj růst na základě originálního marketingu: propagaci své výkonnosti a produktů v oblasti širokopásmové komunikace a souvisejících derivátů jako obchodovatelných finančních nástrojů, zahrnujících v sobě například neobvyklé položky jako deriváty počasí. Výsledkem tak bylo, že Enron byl vyhlášen časopisem Fortune za uplynulých šest, od roku 1996 do roku 2001 jako „nejprogresivnější Americká společnost“. V roce 2000 byl Enron na seznamu „100 nejlepších společností v Americe“ vyhlášených časopisem Fortune. Enron byl oslavován po všech stánkách. V té době většina, včetně odborů a zaměstnanců, chválila Enron za rozsáhlé a dlouhodobé penze a výhody pro zaměstnance a nesmírně efektivní management, samozřejmě až do okamžiku odhalení společného podvodu.
Jak bylo později odhaleno, množství záznamů Enronu o aktivech a ziscích bylo uměle navýšeno, či dokonce zcela falešných a neexistujících, záznamem dluhů a ztrát ve vytvořených „offshore“ jednotkách, které nebyly zahrnuty do finančních výsledků společnosti a použitím dalších sofistikovaných a záhadných finančních transakcí mezi Enronem a spřízněnými společnostmi byly přeměněny do podoby nevýnosných položek v účetních knihách společnosti.

12.1.4 Oblast podnikání

Enron podnikal ve více než 30 oblastech, včetně níže uvedených:
Transport ropy & zemního plynu (Oil & LNG Transportation)
Petrochemický průmysl (Petrochemicals)*

Umělé hmoty (Plastics)*
Elektrická energie (Power)*
Základní investice (Principal Investments)
Celulóza & papír (Pulp & Paper)*
Řízení rizika pro komodity (Risk Management for Commodities)
Lodní/ nákladní doprava (Shipping/Freight)
Ocel (Steel)*
Prostředky pro transport (Streaming media)
Voda & odpadní voda (Water & Wastewater)
Řízení rizika v oblasti počasí (Weather risk management)*
Položky označené * byly obchodovatelné na EnronOnline
Rovněž to byly rozsáhlé budoucí investice zahrnující cukr, kávu, obilí, vepřové a další masné produkty.

12.1.5 Enron Online

V listopadu 199, Enron spustil EnronOnline. EnronOnline byl první internetový transakční systém, který umožňoval, kupujícím a prodávajícím, nakupovat, prodávat a obchodovat s komoditami globálně. Uživatelům tento systém umožňoval obchodovat pouze s Enronem. Díky nezměrné potřebě hotovosti pro EnronOnline a mrhání peněz společnosti v dalších oblastech jako broadband, Azurix, Enron Energy Services, a likvidováním původních provozů spojených s provozem ropovodů, které generovaly hotovost se tak Enron sám připravil o zdroj příjmů. Oddělení Globálních financí Enronu tak muselo vypracovat kreativní finanční operace, aby bylo možné udržet společnost v chodu.

12.1.6 Úpadek

Celosvětová pověst Enronu byla podkopána dlouhodobými zvěstmi o úplatcích a politickém tlaku za účelem ochrany kontraktů ve Střední a Jižní Americe, Africe a na Filipínách. Zvláště sporný byl 3 miliardový kontrakt uzavřený s Maharastra State Elektricity Board v Indii, kde jak se uvádí, vedoucí činitelé Enronu využili svých kontaktů na administrativu prezidentů Clintona a Bushe za účelem vyvinutí určitého tlaku na výbor.
Série skandálů zahrnující účetní operace na hranici podvodu, ke kterým došlo během 90. let, zapletly Enron s účetní firmou Artur Andersen. To nakonec stálo na počátku největšího bankrotu v historii v polovině listopadu 2001. Snaha o v podobě podobné menší energetické společnosti Dynegy se ukázala jako nereálná. Enron dospěl k bankrotu 2 prosince 2001. Jakmile byl finanční skandál v roce 2001 odhalen, klesly akcie Enronu z více než 90.00 USD na pouhých 0.30 USD. Akcie Enronu byly předtím označeny jako „blue chip stock“ (tj. za stabilní akcie společnosti bez významných finančních závazků)., došlo tak k neobvyklé a nebezpečné události ve finančním světě. Prudkému pádu Enronu došlo poté, co vyšlo najevo, že většina z jeho zisku a příjmů byla výsledkem obchodů (dohod) se subjekty se zvláštním účelem (společnosti s ručením omezeným, které Enron kontroloval). Výsledkem bylo že většina dluhů a ztrát, které utrpěl nebyla uvedena v jeho finančních výsledcích.
Došlo rovněž k zániku společnosti Artur Andersen, zbyly tak pouze čtyři velké mezinárodní účetní společnosti, což do dnešního dne způsobuje těžkosti velkým společnostem, které vyžadují více než jednu účetní firmu pro služby spojené s auditem a dalšími neauditními službami.
2. ledna 2002 ministerstvo spravedlnosti USA oznámilo svůj záměr zahájit vyšetřování spojené s bankrotem společnosti Enron, slyšení kongresu začalo 24 ledna.

12.1.7 Vnitřní obchodování

12.1.7.1 Počátky

Společnost Enron měla problémy s vnitřním obchodováním již na konci 80. let. První zdokumentovaný případ se stal v roce 1988. Dva auditoři, David Woytek a John Beard objevili bankovní záznamy odhalující, převody milionů USD z Enronu na osobní účty Louise Borgeta a Thomase Mastroeniho.

Tvrdí se, že oba, Borget a Mastroeni se stýkali s vládci Saudské Arábie a Kuvajtu za účelem získání interních informací z organizace OPEC. Navzdory tomu, že podle tvrzení Woyteka se toto narčení ukázalo nepravdivé, tak vyšší management věřil, že toto byl pravý důvod. Získané interní informace údajně vedly k vyšším ziskům v obchodu s ropnými produkty do doby, než došlo Woytekm a Beardem k odhalení finančních toků z Enronu na osobní účty na placení prostitutek. Oba auditoři byli výkonným předsedou společnosti Kennethem Layem požádáni o pokračování ve vyšetřování, aby zajistili navrácení veškerých finančních prostředků na správné účty; přesto k žádným okamžitým krokům proti odpovědným osobám nedošlo.

Woytek a Beard by pravděpodobně získali dostatek informací k tomu, aby prokázali, že Borget a Mastroeni se podíleli na vnitřním obchodování a okrádání společnosti. Tyto informace obsahovaly bankovní výkazy s finančními toky, které nebyly uvedeny v záznamech společnosti, spolu s pozměněnými výkazy, které Borget dodal společnosti. Přes tato zjištění a navzdory veškerým důkazům, které shromáždili, byli oba auditoři presidentem Enronu Mickem Seidlem a výkonným finančím předsedou Keithem Kernem požádáni o ukončení vyšetřování. Naneštěstí pro Woyteka a Bearda, Borget přinesl společnosti desítky milionu dolarů. Enron tak dal Woytekovi a Beardovi najevo, že roční zisk, který Borget společnosti přinesl byl mnohem podstatnější než dodržování legálních postupů.

12.1.7.2 Pozdější vnitřní obchodování

Pokud obchodníci společnosti Enron byli skutečně zapleteni do vnitřního obchodování během 80. let, tak se patrně z faktu, že byli téměř chyceni Davidem Woytkem a Johnem Boardem, nevzali žádné poučení. Auditorům se zdálo, že v honbě za vyššími zisky by byl Enron ochoten použít i nezákonných postupů.

Enron vytvořil tzv. „offshore entities“ (okrajové subjekty), subjekty které byly použity pro plánování a vyhýbání se placení daní, což samozřejmě vedlo ke zvýšení ziskovosti obchodu. Toto bylo umožněno díky jejich vlastnictví, managementu s absolutní svobodou pohybu finančních prostředků a plnou anonymitou, což vedlo ke skrytí ztrát, které společnost utrpěla. Výše uvedené subjekty učinili z Enronu mnohem ziskovější společnost, než ve skutečnosti byl, došlo k vytvoření nebezpečné spirály, díky které museli úředníci společnosti každý kvartál provádět stále křečovitější finanční podvody, aby vytvořili iluzi miliardových zisků, zatímco ve skutečnosti docházelo ve společnosti k finančním ztrátám. Tato praxe vyhnala nahoru ceny akcií, na základě čehož řídící pracovníci začali vylepšovat interní informace a měnit akcie Enronu v ceně milionů dolarů. Řídící pracovníci a zasvěcenci v Enronu věděli o „offshore“ účtech, které kryly ztráty společnosti, oproti tomu investoři o tom žádné informace neměli. Výkonný předseda účetního oddělení Andrew Fastow vedl team, který vytvořil falešné knihy společnosti a zfalšoval dohody za účelem poskytnutí sobě, své rodině a svým přátelům stovky milionů dolarů garantovaného příjmu na úkor společnosti pro kterou pracoval a akcionářů společnosti.

V srpnu 2000 akcie společnosti Enron dosáhly nejvyšší hranice 90 USD. V tomto bodě řídící pracovníci společnosti, kteří znali interní informace o skrytých ztrátách společnosti začali odprodávat nakoupené akcie. Ve stejné době, byla požádána široká veřejnost a investoři Enronu aby akcie kupovali. Řídící pracovníci, zatímco se skrytě zbavovali svých balíků akcií,

investorům sdělili, že cena akcie by měla i nadále růst a dosáhnout pravděpodobně 130 až 140 USD.
Řídící pracovníci odprodávali své podíly akcií, cena začala klesat. Investorům bylo i nadále řečeno, aby s nákupem akcií pokračovaly a případným prodejem akcií počkali, protože by mělo ve velmi krátkém období dojít k opětovnému vzestupu ceny akcií. Taktika Kennetha Laye na pokračující problémy Enronu spočívala v jeho chování. Jako už mnohokrát Lay vydal prohlášení nebo učinil vystoupení, aby investory uklidnil a ujistil je, že Enron se ubírá správným směrem.
Do 15. srpna klesla cena akcií Enronu na 42 USD. Mnoho investorů Layovi stále věřilo, že Enron bude na trhu opět opět dominovat. Pokračovaly v nákupu nebo držbě akcí a ztrácely každý den stále větší peníze. Na konci října akcie spadly na 15 USD. Mnoho investorů tuto skutečnost považovalo, vzhledem k tomu, co Kenneth Lay uváděl ve sdělovacích prostředcích, jako velkou příležitost k nákupu akcií. Jejich víra a optimismus byly naprosto mylné.
Operace Enronu v Evropě dospěly k bankrotu 30. listopadu 2001, ve Spojených státech požádal Enron o ochranu před věřiteli podle 11. kapitoly 2. prosince. V té době se jednalo o největší bankrot v historii Spojených států, o práci přišlo na 4000 zaměstnanců.
Lay byl obviněn z odprodeje akcií v hodnotě více než 70 milionů USD, které použil na splacení půjček v hotovosti s maximální výší úvěru. Dále odprodal akcie za 20 milionů USD na volném trhu. Jeho žena Linda byla obviněna z prodeje 500 000 akcií Enronu v celkové částce 1.2 milionu USD 28. ledna 2001. Peníze získané z tohoto prodeje nešly na účet rodiny, ale na účty charitativních organizací, které již obdržely přísliby příspěvků z nadace. Záznamy ukazují že paní Layová dala příkaz k prodeji někdy mezi 10:00 až 10:20 dopoledne. Zpráva o problémech Enronu obsahující informace o milionových ztrátách, které byly skrývány před veřejností, byla uveřejněna v 10:30 ráno, cena akcií brzy poté spadla pod jeden dolar.
Bývalá řídící pracovnice Enronu Paula Rikerová byla obviněna z nezákonného vnitřního obchodování. Riekerová si opatřila 18,380 akcií Enronu za cenu 15,51. V červenci 2001 tento balík prodala týden před tím, než veřejně oznámila, že ví o ztrátě okolo 102 milionů USD za cenu 49,77 USD/ akcie.

12.1.8 Následky

Kenneth Lay, bývalý předseda výboru a výkonný předseda společnosti a Jeffrey Skilling, bývalý výkonný předseda společnosti a prezident akciové společnosti se účastní soudu za podíl na skandálu Enronu v lednu 2006. 53 bodů obžaloby, 65 stran obvinění zahrnují širokou škálu finančních přečinů včetně bankovních podvodů, zhotovování falešných prohlášení bankám a auditorům, falešných záruk, podvodů spáchaných za pomoci elektronické komunikace, praní peněz, spiknutí za účelem praní špinavých peněz a vnitřního obchodu. Okresní soudce Sim Lake již dříve odmítl návrhy obžalovaných na oddělené procesy a na přesun projednání případu mimo Houston, kde jak obžalovaní tvrdily, by negativní publicita obklopující zánik Enronu mohla ovlivnit spravedlivý soud.
Pan Lay vinu v případě 11 obvinění z trestných činů nepřiznal. Lay uvedl, že byl uveden v omyl lidmi z jeho okolí. V čase jeho smrti U.S. Securities Exchange Commission (SEC) požadovala po Layovi kromě občanskoprávních pokut více než 90 milionů USD.
Případ obklopující Lindu Layovou je nejkomplikovanější. Layová prodala 28. prosince 2001 přibližně 500 000 akcií Enronu deset až třicet minut předtím, než byla uveřejněna informace, že Enron směřuje k bankrotu. Toto byla skutečnost, o které řídící pracovníci věděli více než rok. Zmíněná časová posloupnost událostí představuje velice závažný důvod pro soudní stíhání.
Bývalý vrchní ředitel pro vztahy s investory Enronu Paula Riekerová přiznala u federálního soudu vinu v souvislosti s obviněním z vnitřního obchodování. Jedno závažné obvinění proti Riekerové představuje maximální trest v podobě deseti let ve vězení a pokutu 1 milion USD.

Riekerová souhlasila s tím, že nikdy nebude pracovat jako úředník nebo ředitel veřejné společnosti. V případě, že federální soud schválí dohodu, tak Riekerová zaplatí SEC 499.333 USD, což představuje zisk z prodeje 18,380 akcií Enronu. Riekerová představovala pro vládu cenného svědka díky skutečnosti, že připravovala zprávy o příjmech a konferenční hovory s analytiky Enronu.
28. prosince 2005 bývalý CAO Richar Causey přiznal vinu týkající se falešných záruk. Stráví 7 let ve vězení a vládě Spojených států zaplatí 1,25 milionu USD. Causey má možnost strávit ve vězení pouhých 5 let v případě, že bude spolupracovat a vypovídat proti Lay Skillingovi.
13. ledna 2006 přiznal lobista Willian „Art" Roberts během vyšetřování vinu členům Senátu. Robertse najala německá banka v červnu 20004 aby získal dopis od podvýboru senátu prohlašující, že banka provedla náležité kroky při vyšetřování zániku Enronu, jako součást obrany banky proti podání žaloby Londýnskou bankou.
Lay a Skilling byli obžalováni z poskytování falešných záruk a podvodů spáchaných za pomoci elektronické komunikace v červenci 2004 což vedlo k velmi sledovanému soudnímu procesu ve kterém byl Lay uznán vinným ze 6 trestných činů a Skilling byl usvědčen z 19 z celkových 28 bodů obžaloby 25. května 2006. 5 června 2006 Lay zemřel ve věku 64 let když trávil dovolenou v Aspenu, v Coloradu, poté co utrpěl zjevný rozsáhlý srdeční infarkt 4. června. Měl být odsouzen 23 října 2006.

12.1.9 Důsledky

Dlouhotrvající soudní procesy a dopady zániku Enronu jsou místy nejasné, ale je tu i přesto zřejmé značně velké politické selhání ze strany Spojených států a Spojeného království týkající se finančních prostředků, které Enron věnoval politickým postavám (okolo 6 milionů USD od roku 1990). Přibližně tři čtvrtiny amerických příspěvků šla na účet republikánské strany, zahrnující značné příspěvky na prezidentskou kampaň Georgie W. Bushe.
Dopad skandálu se rychle rozšířil mimo Enron a ty které s ním byli spojeni. Soudní proces se společností Artur Andersen obžalované z bránění výkonu spravedlnosti spojené s Enronem, pomocí s odhalením účetního podvodu ve společnosti WorldCom. Následný bankrot této telekomunikační společnosti okamžitě spustil vlnu dalších účetních skadálů. Tato vlna zachvátila velké množství společností, odhalila vysokou korupci, účetní chyby a vnitřní obchodování. Ačkoli byl pád Enronu největším bankrotem v historii, byl nakonec zatlačen do pozadí pádem společnosti WorldCom.
Bývalý CFO Enronu Andrew Fastow, duchovní otec sítě „offshore" společností a pochybných účetních postupů byl obžalován 1 prosince 2002 federální velkou porotou v Houstonu z 78 trestných činů včetně podvodu, praní špinavých peněz a spiknutí. On a jeho žena Lea Fastowová, bývalá asistentka pokladního přijali dohodu 14 ledna 2004. Andrew Fastow stráví podle rozsudku 10 let ve vězení a vzdá se 23,8 milionů USD, jeho žena Lea stráví ve vězení 5 měsíců a rok na svobodě pod dohledem, z čehož bude 5 měsíců v podobě domácího vězení, na oplátku oba poskytnou svědectví proti zbylým úředníkům společnosti Enron.
Ben Glisan Jr., bývalý pokladník Enronu byl prvním lčověkem, který byl poslán do vězení po skandálu s Enronem. Přiznal vinu v bodu obžaloby týkající se jednoho spiknutí, aby se vyhnul obvinění z poskytnutí falešných záruk a obvinění z podvodů spáchaných za pomoci elektronické komunikace.
John Forney bývalý obchodník s energií, který vynalezl různé strategie jako například „Death Star", byl obviněn v prosinci 2002 z 11 trestných činů spiknutí a z podvodů spáchaných za pomoci elektronické komunikace. Jeho soudní proces byl naplánován na 12 října 2004. Jeho dva nadřízení, Timothy Belden a Jeffrey Richter přiznali vinu na spiknutí aby se vyhnuli obvinění z poskytnutí falešných záruk a obvinění z podvodů spáchaných za pomoci elektronické komunikace a nyní pomáhají žalobcům ve vyšetřování toho skandálu.

Jeffrey Skilling byl zatčen FBI 11. února 2004. Kenneth Lay byl za účast na skandálu obviněn federální velkou porotou 7 července 2004. Před soudem 9. července prohlásil, že se necítí vinen.
25 května 2006 porota v soudním procesu s Layem a Skillingem vynesla svůj verdikt. Skilling byl uznán vinným v 19 z 28 bodů obžaloby obvinění z poskytnutí falešných záruk a obvinění z podvodů spáchaných za pomoci elektronické komunikace, ve zbylých 9 bodech byl zproštěn obžaloby, včetně obvinění z vnitřního obchodování. Čelil celkovému trestu v délce 185 let vězení. Lay byl uznán vinným ve všech šesti bodech obžaloby z poskytnutí falešných záruk a obvinění z podvodů spáchaných za pomoci elektronické komunikace pro které byl souzen a čelil celkovému trestu v délce 45 let vězení. Lay zemřel 5. července 2006 před vynesením rozsudku. 12 července 2006 bylo v parku v severovýchodní části Londýna nalezeno mrtvé tělo Neila Coulbecka, důležitého svědka k případu Enron, který měl být vydán do Spojených států. Spojené státy tvrdí že Coulbeck s dalšími se spikl spolu s bývalým CFO Enronu Andrewem Fastowem. Všehovšudy bylo 16 lidí shledáno vinnými za přečiny v souvislosti se společností a pět dalších, včetně čtyř zaměstnanců Merilla Lynche, bylo shledáno vinnými při soudním procesu. Vypovídalo osm bývalých řídících pracovníků Enronu, korunní svědek byl Fastow, který svědčil proti svým bývalým nadřízeným Layovi, Skillingovi.

12.1.10Penze

V okamžiku kdy Enron padl, ztratily tisíce jeho zaměstnanců a investorů své celoživotní úspory, úspory na studium pro své děti, penze. Soudní řízení jménem poloviny akcionářů Enronu bylo podáno proti řídícím pracovníkům a ředitelům Enronu. V tomto soudním procesu bylo celkem obviněno dvacet devět řídících pracovníků a ředitelů z vnitřního obchodování a z matení veřejnosti.
Díky tomu, že 401(k) (část Internal Revenue Code) je navržen jako příspěvkový plán, tak nebyl u PBGC (Pension Benefit Garanty Corporation) pojištěn a zaměstnanci tak ztratili peníze které investovaly do cenných papírů Enronu. Mohli tak pouze podat žalobu na odpovědné osoby pro porušení povinností podle ERISA (Employee Retirement Income Security Act) článku 404. Pension Benefit Garanty Corporation uvažuje o náhradě některých, popřípadně i všech slíbených výhod.

12.1.11Arthur Andersen

15 června 2002 byla společnost obviněna z bránění výkonu spravedlnosti z důvodu skartace dokumentů týkajících se auditu v Enronu. Od doby, kdy U.S Securities and Exchange Comission (SEC) nepovoluje obžalovaným kontrolovat veřejné společnosti společnost souhlasila s tím že se vzdá svých licencí před SEC 31 srpna. 31 května 2005 vrchní soud spojených států jednomyslně změnil obvinění společnosti Andersen vzhledem k procesním chybám. I přes toto rozhodnutí je velmi nepravděpodobné, že se Anderson vrátí jako životaschopná společnost. Společnost ztratila téměř všechny své klienty když byla obviněna, dále bylo na společnost podáno více než 100 trestních oznámení v souvislosti jejími audity v Enronu a v dalších společnostech. Po obvinění společnost omezila své aktivity v Americe. Z celkového počtu 28 000 zaměstnanců ve Spojených státech a 85 000 zaměstnanců po zbylém světě je společnost na samém dně s přibližně asi 200 zaměstnanci umístěnými zejména v Chicagu. Většina jejich aktivit je dnes spojena se soudními procesy.
Andersen byla členem „Big Five“ velkých mezinárodních účetních firem. Po jejím zánik tak zbyly pouze čtyři velké mezinárodní firmy. Tato skutečnost do dnešní doby způsobuje těžkosti velkým společnostem, které potřebují využít služeb více než jedné účetní společnosti pro auditní a neauditní služby. Dále ceny za účetní služby jsou méně pružné a velké společnosti mají dojem že musí využít pouze služeb zbylých čtyř velkých společností.

12.1.12Společenský a legislativní dopad

Pád Enronu přispěl k přijetí tzv. „Sarbanes-Oxley Act“ (SOX, Sarbanes-Oxleyho zákon) schváleného 30. července 2002. tento zákon je považován ze nejvýznamnější změnu v oblasti zákonů o cenných papírech od FRD’s New Deal ve třicátých letech 20. století. Další země rovněž upravily svou legislativu. Tento zákon ustanovuje přísnější tresty za podvody, mezi dalšími body vyžaduje po veřejných společnostech vyvarování se půjčkám managementu, uveřejňování více informací, poskytuje větší nezávislost auditorů, a nejkontroverznější část týkající se oznámení výsledků auditu, jejich interních kontrolních procedur.

12.2 MCI WorldCom

MCI, Inc. byla americká telekomunikační společnost se sídlem v Ashbum, ve Virginii. Společnost vznikla spojením WorldCom (dříve známá jako LDDS později LDDS WorldCom) a MCI Communications, následně pak společnost používala název MCI WorldCom,. Po bankrotu byla společnost koupena telekomunikační společností Verizon Communications na základě dohody podepsanou 6. ledna 2006 a v současné době existuje jako jedna z divizí společnosti Verizon.

Historie společnosti MCI v sobě spojuje historii společností, které získala, odráží v sobě dále většinu trendů, které hýbaly telekomunikačním trhem v Americe v druhé polovině 20. století. Společnost se účastnila legislativních a regulačních změn, které vedly ke zrušení monopolu společnosti AT&T, která dominovala na americkém telekomunikačním trhu; koupě společností WorldCom a pozdější bankrot ve světle účetních skandálů byly příznačné pro Internetový exces na konci devadesátých let. Společnost nakonec přijala nabídku odkoupení od společnosti Verizon za 7,6 miliard dolarů.

Po určitou dobu byla společnost WorldCom (WCOM) druhou největší telekomunikační společností (největší byla AT&T). WorldCom se rozrůstal díky získáváním jiných telekomunikačních společností, za pozornost stoji MCI Communications. Dále vlastnil Tier 1 ISP, UUNET, hlavní část páteřní sítě. Ta byla založena v Clintonu v Mississippi, poté se přesunula do svého nynějšího sídla.

12.2.1 Historie

12.2.1.1 Budování společnosti

Long Distance Discount Services, Inc (LDDS) vznikla v Jacksonu v Mississippi v roce 1983. V roce 1985 byl na post výkonného předsedy společnosti LDDS zvolen Bernard Ebbers. Společnost se stala veřejnou (akciovou) v srpnu 1989, když se spojila se společností Advantage Companies, Inc. Jméno společnosti bylo v roce 1995 změněno na LDDS WorldCom, později pouze WorldCom.

Růst společnosti způsoben zejména jejími akvizicemi během devadesátých let a dosáhl svého vrcholu při získání společnosti MCI v roce 1998. Mezi společnostmi které byli koupeny nebo sloučeny se společností WorldCom byly Advanced Communications Corp. (1992), Metromedia Communication Corp.(1993), Reurgens Communications Group(1993), IDB Communications Group, Inc (1994), Williams Technology Group, Inc. (1995), a MFS Communications Company (1996). Spojení se společností MFS zahrnovalo UUNet Technologies, Inc., které se krátce předtím spojily se zmíněnou společností MFS. V únoru 1998 došlo ke složitému jednání, kdy WorlCom odkoupil Compu Serve od její mateřské společnosti H&R Block. WorldCom si poté ponechal divizi CompuServe Network Services, a její online služby prodal společnosti America Online, a získal divizi AOL's network, ANS. Získání společnosti Digex (DIGX) v červnu 2001 bylo rovněž komplikované, WorldCom nejdříve získal otcovskou firmu, Intermedia Communications a poté prodal veškerá aktiva, která nesouvisela se společností Digex, společnosti Allegiance Telecom.

12.2.1.2 Získání MCI

10 listopadu 1997 společnosti MCI a WorldCom oznámili své sloučení v celkové hodnotě 37 miliardy USD a vytvoření společnosti MCI WorlCom, což představovalo největší fůzi v historii Spojených států. 15 září 1998 nová společnost MCI WorldCom začala obchodovat.

12.2.1.3 Spojení se společností Sprint

5 října 1999 Sprint Corporation a MCI WorldCOm oznámili spojení svých společností

v celkové hodnotě 129 miliard USD. Tato dohoda by představovala do té doby největší spojení dvou společností v historii. Nová společnost by byla WorldCom a stala by se největší telekomunikační společností ve Spojených státech. Tato fúze by tak odsunula AT&T na pozici dvojky v oblasti komunikací. Nakonec k dohodě díky tlaku ze strany amerického ministerstva spravedlnosti a EU z obavy o vytvoření monopolního prostředí nedošlo. 13 července 2000 správní rady obou společností oznámili odstoupení od zamýšlené fúze. Později téhož roku se společnost MCI WorldCom se i bez spojení se společností Sprint přejmenovala na WorldCom.

12.2.1.4 Finanční skandály

Bernard Ebbers se stal díky vzestupu ceny cenných papírů své společnosti WorldCom velmi zámožnou osobou. Nicméně, krátce po akvizici se společností MCI v roce 1998 dočlo na telekomunikačním trhu k poklesu a strategie společnosti utrpěla vážnou trhlinu, když bala donucena zrušit zamýšlenou fúzi se společností Sprint na konci roku 2000. V té době začala cena cenných papírů společnosti klesat a Ebbers se tak dostal pod tlak bank, díky tomu že své další aktivity financoval svými akciemi WorldComu (mezi jinými dřevařství a yachting). Během roku 2001 Ebbers přesvědčil správní radu, aby mu poskytla firemní půjčky a záruky v celkové výši 400 milionu USD za účelem pokrytí svých ztrát, tato taktika nakonec definitivně selhala a Ebbers byl z postu výkonného předsedy odvolán v dubnu 2002 a nahrazen Johnem Sidgnorem, bývalým řídícím pracovníkem UUnet Technologies, Inc.
Od začátku roku 1999 do května 2002 společnost (pod vedením Scotta Sullivana (CFO), Davida Myerse (kontrolor) a Budforda „Buddyho“ Yatese (ředitele celkového účetnictví)) používala podvodné účetní metody k zakrytí zhoršující se finanční situace společnosti vytvářením falešného obrazu o finančním růstu a ziskovosti za účelem zvednutí ceny cenných papírů WorldComu.
Podvod byl dokonalý díky dvěma skutečnostem:
1 Snížením „nákladů na linku“ (nákladů na propojení s jinými telekomunikačními společnostmi) díky uvedení těchto nákladů v rozvaze místo toho aby byly náležitě vyúčtovány
2 Nafukováním příjmů v účetních zápisech z podnikových účtů s nerozděleným ziskem
Interní kontrolní oddělení WorldComu v červnu 2002 odhalilo při běžné kontrole výdajů podvod v celkové výši 3,8 miliard USD a upozornilo nové auditory společnosti z KPMG (kteří nahradily Arthur Andersen, externí auditory WorldComu). Krátce po provedeném auditu společnosti byla o podvodu informována správní rada společnosti, která zareagovala velice rychle: Sullivan byl vyhozen, Meyers odstoupil, Artur Andersen stáhl zprávu o auditu týkající se roku 2001 a 26. června 2002 komise Securities and Exchange Commission (SEC) zahájila vyšetřování událostí. Ke konci roku 2003, bylo odhadnuto, že došlo k podvodnému navýšení aktiv společnosti o přibližně 11 miliard USD.

12.2.2 Bankrot

21. července 2002 společnost WorldCom požádala podle článku 11 o ochranu před věřiteli, jednalo se o do té doby největší bankrot v historii Spojených států. Společnost WorldCom změnila svůj název na MCI a 14. dubna 2003 přesunula sídlo společnosti z Mississippi do státu Virginia.
V rámci dohody o restrukturalizaci společnosti po bankrotu společnost zaplatila komisi SEC 750 milionů USD v hotovosti a v akciích nové společnosti MCI, které původně byly určeny na platby poškozeným investorům.
V květnu 2003 společnost MCI získala od ministerstva obrany Spojených států kontrakt na výstavbu mobilní sítě v Iráku. Dohoda byla kritizována ze strany konkurenčních společností a dalšími, kteří poukazovaly na nedostatek zkušenosti společnosti MCI v této oblasti. Bankrot představoval tvrdý úder morálce společnosti.

12.2.3 Po bankrotu

V roce 2004 společnost podle kapitoly 11 překonala bankrot s 5,7 miliardami dluhů a 6 miliardami v hotovosti. Přibližně polovina hotovosti měla být použita k uhrazení různých pohledávek a vyrovnání. Předchozí držitelé obligací dostali 35,7 centů za dolar v dluhopisech a akciích nové společnosti MCI. Předešlé balíky akcií byly bezcenné.
V současné době tak společnost musí vyplatit valnou část svých věřitelů, kteří dva roky čekali dlužnou částku. Mnozí z malých věřitelů, včetně bývalých zaměstnanců, zejména ti kteří ztratili práci v červnu 2002 a jejichž odstupné a benefity jim nebyly vypláceny od okamžiku bankrotu WCOMu.
7. srpna 2002 byla znovu zahájila provoz skupina exWorldCom 5100. Byla složena z bývalých zaměstnanců WorldComu se společným požadavkem na vyplacení odstupného a a benefitů podle odstupného plánu WorldComu. Číslo 5100 představuje počet zaměstnanců, kteří přišli o místo, když WorldCom zbankrotoval.
15 března 2005 byl Bernard Ebbers shledán vinným ze všech obvinění a usvědčen z podvodu, spiknutí, falšování dokumentů – vše se souviselo s 11 miliardovým účetním skandálem telekomunikační společnosti, kterou založil. Byl odsouzen k 25 letům vězení. Další bývalí úředníci WorldComu byli obviněni z trestných činů týkajících se nesprávného uvádění stavu financí společnosti, včetně CFO Scotta Sullivana (přiznal vinu 2 března 2004 v bodech obžaloby investiční podvod, spiknutí za účelem investičního podvodu, uvádění nepravdivých informací), bývalý kontrolor David Myers (27. září 2002 přiznal vinu na podvod v účetnictví, spiknutí za účelem investičního podvodu, uvádění nepravdivých informací), bývalý účetní ředitel Buford Yates (7. října 2002 přiznal vinu na spiknutí a účetních podvodech) a bývalí účetní manažeři Betty Vinsonová a Tro Normand (10. října 2002 oba přiznaly vinu na spiknutí a investičních podvodech).
13. července 2005 byl Bernard Ebbers odsouzen k 25 letům vězení. V době vynesení rozsudku bylo Ebbersovi 63 let. Teoreticky tak bude ve vězení do svých 83 let, kdy bude moci požádat o propuštění za dobré chování. Ebbers nasoupit do vězení k výkonu trestu v úterý 26. září 2006.
V březnu 2005 16 ze 17 bývalých ručitelů uzavřelo dohodu s investory. Citigroup se spokojila s 2,65 milardou USD 10. května 2004.

12.2.4 Velký podíl na záchraně společnosti WorldCom měl Michael Capella, vynikající krizový manažer řeckého původu. Podívejme se na jeho CV:

Michael Capellas (narozen 19. srpna, 1955 ve městě Warren v Ohiu) byl předseda společnosti a CEO (výkonný předseda) společnosti MCI do doby než byla odkoupena společností Verizon a stala se tak její součástí. Předtím působil i ve společnosti Compaq, odkud odešel krátce poté, kdy došlo k fúzi se společností HP. Capellas říká, že odhodlanost rozhodnost zdědil po svém otci, Řekovi, který bojoval po boku americké armády proti německé armádě v Itálii během druhé světové války. Rodina se přestěhovala do Ohia, kde otec vypracoval z dělníka až k postu vedoucího oddělení ve společnosti Republic Steel Corporation. Michael Capellas o svém otci řekl: „Můj otec měl neuvěřitelný smysl pro pracovní morálku. Byl neuvěřitelně věrný společnosti. Pracoval v ní více než třicet let.“ Jako vysokoškolský student na Kent State University propadl kouzlu počítačů. Krátce po absolvování univerzity se oženil a po následujících více jak 20 let cestoval po světě podle toho, jak postupoval na postech společností, pro které pracoval. Capellas vystřídal 22 různých zaměstnání v šesti společnostech včetně softwarové společnosti Oracle Corporation, poté přešel ke společnosti Compaq na pozici ředitele pro informace (chief information officer). Během jednoho roku došlo pod jeho vedením ke stabilizaci společnosti Compaq. Capellas přebudoval společnost s cílem zvýšit její dravost, omezit náklady, zvýšit její denní online prodej z 1 milionu na 6 milionu USD a oživit zavádění inovací. Ve druhé čtvrtině příjmy vzrostly o 7,5 % na 10.13 miliard USD – po roce

stagnace – dík japonskému růstu o vražedných 40 % a růstu v Jižní Americe až o 29%. Společnost vydělala 387 milionu USD v porovnání s 184 milionovou ztrátou v porovnáním se čtvrtletím o rok dříve.
30. července 1999 se Capellas napomohl urovnání vztahů mezi Microsoftem a společností Compaq, které byly po mnoho let na bodu mrazu. Jeho snaha vyústila ve strategické partnerství Compaqu se společností Microsoft při spuštění operačního systému Windows 2000. V prosinci 2002 se stal Michael Capellas presidentem a výkonným předsedou společnosti MCI, před tím pracoval na pozici prezidenta společnosti Hewlett-Packard.
Zkušený šéf Michael Capella zachránil WorldCom a přesvědčil neústupné věřitele a i Arthura Gonzalese, člena amerického federálního bankrotového soudu, aby schválil plán reorganizace WorldCom, a tím tuto firmu s 55 tisíci zaměstnanci zachoval při životě.Zmizelo i zdiskreditované jméno WorldCom a bylo nahrazeno zkratkou MIC.
Bylo nutné zvýšit dluh o 750 miliónů dolarů, které firma zaplatila americké Komisi pro cenné papíry jako pokutu za účetní podvody. M.Capellas se nemusel znepokojovat dalšími finančními požadavky, které věřitelé a investoři adresují především bývalým manažerům.
Společnost byla 14.4. 2003 přejmenována na MCI a po necelých dvou letech, 14. února 2005 došlo k uzavření smlouvy o fúzi se známou společností Verizon, kde MCI je jednou z divizí.
A tak hororový příběh, s pohádkovým začátkem, skončil pro zaměstnance WorldComu přijatelným způsobem. Škoda jen, že Enron, operující v energetickém sektoru s analogickými účetními praktikami, nenašel krizového manažera obdobných kvalit…

12.3 Reakce vlády Spojených států

Všechny případy vykazují podobné charakteristiky. Jedná se o nedostatek transparentnosti, skrytou defraudaci a zadluženost nebo neefektivní kontrolu ze strany auditorů a regulačních úřadů. Podstatný rozdíl nicméně spočívá v postoji USA a Evropy ke kolapsům velkých firem. Enron i WorldCom byly ponechány svému osudu bez zájmu státu o osudy zaměstnanců (mnoho z nich ztratilo práci bez jakékoliv kompenzace) nebo jiných osob, které například investovaly do akcií podnikových penzijních systémů a o slibované důchody přišly. V případě řešení problémů těchto firem se postupovalo standardně podle amerického bankrotového zákona. Jejich potíže se tak odrazily v přístupu vůči bankám, které zajišťovaly jejich financování, nebo vůči auditorům. [integrace cz]
Americkou reakcí na krachy daných firem bylo přijetí takzvaného Sarbanes-Oxleyho zákona. Ten mimo jiné vyžaduje u společností vedených na burze povinnost vytvořit výbor pro audit a stanoví mu určité, velmi specifické povinnosti. Výbor nese zodpovědnost za jmenování externích auditorů a za odsouhlasení a projednání odměny vyplácené těmto externím auditorům. Dále má výbor pro audit funkci dozoru nad prací vykonávanou externími auditory. Vystupuje tedy jako kontrolní orgán v rámci veškerých činností spojených s auditem, vykonávaných externími auditory dané společnosti. Zákon klade velký důraz na problematiku spojenou se zveřejňováním finančních údajů a stanovuje, že výbor pro audit musí být seznámen se všemi účetními problémy, které jsou pro společnost kritické. Zákon dále zakazuje, aby jakýkoli externí auditor pobíral od určité společnosti odměnu za provedení externího auditu a zároveň od té samé společnosti získával odměnu za konzultační činnost. V takovém případě by docházelo k jasnému střetu zájmů. Výbor pro audit by měl také přijímat a vyřizovat veškeré stížnosti týkající se údajů ve finančních výkazech a zajišťovat proces včasného upozorňování na potenciální potíže. Pokud někdo ze společnosti zjistí určité důležité informace, úkolem výboru pro audit je tuto osobu vyslechnout a chránit před případnými postihy ze strany vrcholového managementu. Je důležité zdůraznit, že výbory pro audit existovaly ve většině firem kótovaných na burzách již před účinností tohoto zákona. Ten tak pouze konkretizoval jejich postavení a povinnosti. [integrace.cz]

Skutečnou novinkou zákona je zakotvení odpovědnosti generálního a finančního ředitele. Osoby v těchto funkcích musí prohlásit, že zkontrolovaly finanční výkazy, závěrečné finanční výkazy ke konci roku a další zprávy, které jsou o dané společnosti zveřejňovány. Mají za úkol i ověřit, že dané zprávy a účetní výkazy odrážejí správný obraz společnosti, že v nich nic nechybí a že neobsahují nesprávné údaje. Dále zodpovídají za vnitřní kontrolu v oblasti zveřejňovaných finančních výsledků a rovněž musí zajistit, aby kontrolní i řídicí mechanismy umožňovaly přístup k informacím o každé důležité události ve společnosti či v jejích pobočkách. Jejich další povinností je prověřovat účinnost těchto kontrolních a řídicích mechanismů. Je třeba zdůraznit, že se nejedná jen o formální prohlášení v podobě papíru s podpisem. Americká Komise pro cenné papíry může ředitele kdykoli požádat o prokázání, zda byl tento proces skutečně realizován. [integrace cz]
Závěrem je vhodné dodat, že generální i finanční ředitel musí jednat také s externími auditory a informovat je o jakýchkoli nedokonalostech a slabých místech vnitřního systému nebo o zpronevěře. Externí auditoři budou povinni hodnotit prohlášení daných osob. Všechny společnosti kótované na burze nyní musí přikládat ke svým výročním zprávám také zprávu o vnitřních kontrolách, jež bude doplněna podpisy generálního a finančního ředitele. SEC přitom za vnitřní kontrolu pokládá všechno, co společnosti umožňuje zajistit, aby byly transakce řádně ověřeny a správně zaneseny do účetnictví tak, aby byla aktiva chráněna proti zneužití. Americký regulátor také stanovil, že když hovoří o transakcích, má na mysli transakce aktiv v širším pojetí, to znamená veškeré pohyby v rámci společnosti. Aktiva samozřejmě zahrnují nejen fyzická aktiva, ale také hmotná aktiva, nehmotná aktiva, zaměstnance, továrny, vybavení, tedy vše, co je majetkem společnosti.

K znamenitě řízeným organizacím patří CzechTrade a CzechInvest; obě se významnou měrou podílí na skutečnosti, že ČR vykazuje nově přebytek v zahraničním obchodě a je mimořádně úspěšnou zemí v celosvětovém měřítku, pokud jde o zahraniční investice.

CzechTrade

&

CzechInvest

Úvodní profil společnosti CzechTrade

Krátká charakteristika

- Česká agentura na podporu obchodu, jinak CzechTrade, byla založena 1. května 1997 jako příspěvková organizace
- plní funkci národní proexportní agentury Ministerstva průmyslu a obchodu České republiky
- hlavním úkolem je zvyšovat exportní výkonnost a konkurenceschopnost českých firem na zahraničních trzích prostřednictví širokého spektra služeb a informací
- v roce 2002 získala jako třetí v Evropě certifikát systému kvality managementu jakosti ISO 9001:2000, v letech 2003 -2005 tento certifikát úspěšně obhájila

Vize společnosti

„Být první volbou pro české firmy při jejich podnikání a rozvoji na mezinárodních trzích."

Z uvedené vize vyplívají následující všeobecné cíle společnosti:

- špičkový servis pro české exportéry
- profesionální přístup k zákazníkům
- individuální řešení podle přání zákazníků
- budování dlouhodobého partnerství s klienty

Poslání

CzechTrade je vládní agentura s unikátními informacemi o světových trzích a širokou sítí zahraničních (konkrétně 32 kanceláří v 29 zemích) a regionálních kanceláří. Nabízí individuální řešení pro zákazníkův úspěšný export.

Kritické faktory úspěchu

- Vysoká přidaná hodnota
  Hlavním výstupem agentury CzechTrade jsou služby na podporu a zvýšení exportu jejích klientů. Veškeré hlavní, podpůrné a rozvojové činnosti musí přispívat k jeho výraznému růstu.
- Klientsky orientovaná agentura
  Rozvoj a zlepšení služeb agentury musí být v souladu s potřebami jejích zákazníků. Nejlepším zdrojem růstu agentury do budoucna a nejúčinnějším marketingem je využití znalosti potřeb klientů, jejich odraz v nabízených službách a doporučení klientů agentury k využití jejích služeb ostatním.
- Kvalitní síť pro export
  Síť kanceláří CzechTrade je sítí klient agentury, která je přibližuje úspěšnému využití příležitostí na zahraničních trzích. Síť je budována tam, kde je třeba, a je rozvíjena pro české exportéry. Základem sítě jsou profesionální a motivovaní zaměstnanci doma i v zahraničí.

Poskytované služby

Společnost nabízí individuální servis při vyhledávání vhodných vývozních oblastí s následnou asistencí při oslovení relevantních partnerů. Kromě toho nepřetržitě zprostředkovává databázi aktuálních obchodních příležitostí a veřejných zakázek. Dále organizuje specializované vzdělávání pro mezinárodní obchod. V neposlední řadě prostřednictvím svých konzultantů spoluvytváří zákazníkovu exportní strategii. Při plnění

těchto cílů se opírá o zkušenosti pracovníků v rozsáhlé síti zahraničních poboček, pražské centrále i ve všech regionech České republiky.

Hlavní prioritou agentury CzechTrade je důkladná znalost podnikání a pochopení potřeb klienta, což umožňuje připravit klienta na export a seznámit ho s kroky, se kterými může CzechTrade pomoci.

Nabídky je sestavena v krocích, které by měl exportér postupně realizovat, pokud chce uspět v zahraničních teritoriích.

Příprava exportních aktivit
Úvodní konzultace

Návrh kroků, které je třeba realizovat, aby zákazník mohl být úspěšný na zahraničních trzích.

Exportní vzdělávání

Vzdělávací akce zaměřené převážně na různé aspekty mezinárodního obchodu. Účastník získá co nepraktičtější informace důležité pro rozhodování, přípravu a úspěšný vstup na zahraniční trhy. Patří sem jednodenní semináře a workshopy, semináře v regionech, konzultační dny v regionech, firemní školení, e-learning apod.

Manuál úspěšného exportéra

Řada odpovědí na otázky, které si kladou exportéři v oblasti techniky zahraničního obchodu.

Informace o trzích

Informační služby zahraničních kanceláří

Informační služby, které klientům pomohou při rozhodování o vstupu na nový trh. Jedná se především o:

- zpracování základních charakteristik trhu (vývoj poptávky, trendy, struktura dovozu)
- určení tržních segmentů a produktů (typy zákazníků, produktové řady)
- analýza vlivu zahraničního prostředí (legislativa, daně, omezení zahraničního obchodu)
- poskytnutí základních informací o konkurenci
- základní cenový průzkum pro cílový trh
- monitoring veletrhů a výstav
- zjištění technických překážek (předpisy, certifikace)
- návrh a možnosti překonání bariér vstupu na trh, a další

Exportní příležitosti

On-line databáze s aktuálními informacemi o exportních příležitostech pro české podnikatelské subjekty. Konkrétně se jedná o:

- Zahraniční investiční příležitosti

- Zahraniční poptávky
- Zahraniční nabídky
- Zahraniční projekty a trendy
- Zahraniční udělené zakázky
- Zahraniční noviny
- Zahraniční zástupci

CzechTrade denně

Denní elektronické zasílání ověřených obchodních příležitostí ze zahraničí. Nastavením vhodného profilu budete do svého e-mailu dostávat pouze relevantní informace.

Obchodní kontakty

Vyhledání obchodních kontaktů

Vyhledávání distributorů, potenciálních odběratelů a obchodní údajů o firmách v zahraničí z databáze Kompass podle zadaných kritérií, z teritorií: východní, západní Evropa; dálný, blízký východ; USA; Kanada

Zjištění bonity firmy

Zjištění bonity firmy ve spolupráci se zahraničními kancelářemi a smluvními partnery, cílem je pomoci zákazníkovi při rozhodování o jeho exportních aktivitách.

Asistenční služby zahraničních kanceláří

Služby, které vám pomohou při hledání nových obchodních partnerů v zahraničí.

Programy zahraniční rozvojové spolupráce EU: Konzultačně-informační centrum HELPDESK

Centrum informací o možnostech účasti českých společností na programech zahraniční rozvojové spolupráce Evropské Unie. Aktuality a příležitosti, které pro firmy v rámci zahraniční rozvojové spolupráce EU vznikají, informace o podmínkách a postupech účasti ve výběrových řízeních.

Marketingová podpora

Exportní klub CzechTrade

Vytváří přirozenou půdu pro osobní setkávání a komunikaci exportérů a přestavitelů státní sféry.

Prezentace v zahraničí

Kvalitní prezentace české firmy v zahraničí, která je nutnou podmínkou k navázání úspěšných obchodních kontaktů.

Konzultační dny se zástupci zahraničních kanceláří CzechTrade v regionech ČR

Konzultační dny Vám nabízejí možnost osobního setkání s řediteli zahraničních kanceláří CzechTrade přímo v regionu, kde Vaše firma působí.

Dotace

Agentura CzechTrade vystupuje v roli implementační agentury pro 2 dotační programy: Aliance a Marketing. Tyto programy jsou určeny pro malé a střední podniky, které provozují obchodní aktivity na zahraničních trzích.

Program Aliance je financován ze státního rozpočtu ČR. Program Marketing je součástí Operačního programu průmysl a podnikání, který je dotován ze strukturálních fondů Evropské unie.

Aliance: Program vytváření aliancí a jejich prezentace v zahraničí

CzechTrade je poskytovatelem podpory v rámci programu ALIANCE, který vyhlásilo Ministerstvo průmyslu a obchodu v rámci programů podpory malého a středního podnikání s platností od roku 2005 do roku 2006.

Program Marketing

Agentura CzechTrade je implementační agenturou pro program Marketing v rámci Operačního programu Průmysl a podnikání.

Program Marketing má za cíl podporu konkurenceschopnosti českých podnikatelů na zahraničních trzích. Program má přispět k rozvoji aktivit exportérů po vstupu České republiky do Evropské unie na zahraničních trzích a zvýšit možnosti využití exportních příležitostí, které na světovém trhu existují. Monitorovacím kritériem je zvýšení exportu do daného teritoria.

Další služby
BusinessInfo – oficiální portál pro podnikatele

Agentura CzechTrade zastřešuje a koordinuje portál BusinessInfo, který je společným projektem řady státních a nestátních institucí, svazů a sdružení s cílem překonat roztříštěnost informací ze státní správy. Portál se zaměřuje na podporu podnikání a exportu. Nabízí odpovědi na otázky z oblasti zahraničního obchodu, financí, daní, legislativy, Evropská unie, podpory podnikání a dalších.

Euroservis

Portál Euroservis byl zřízen na půdě vládní agentury CzechTrade. **Jeho činnost se zaměřuje** jednak na sběr, třídění a distribuci podnikatelských informací o EU, které jsou zajímavé a potřebné pro české podniky; jednak na tvorbu programů a získávání finančních prostředků na jejich spolufinancování ze zdrojů EU.

Nabídka publikací CzechTrade

Přehled publikací jak tištěných, tak elektronických, které vydal a připravil CzechTrade nejen pro české exportéry. Například Průvodce veřejnými zakázkami v Evropské unii, Zahraniční obchod ČR v roce 2003, Čtvrtletní analýzy zahraničního obchodu ČR atd.

Projekt JPD3 – Posílení konkurenceschopnosti pražských podnikatelů v programech zahraniční rozvojové spolupráce evropských společenství

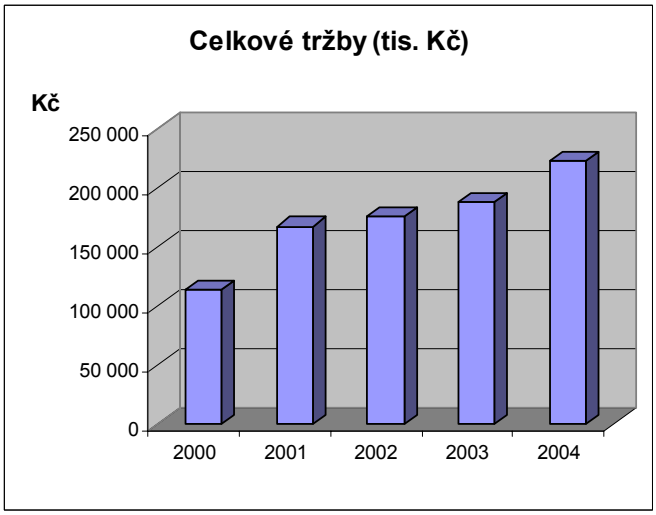
Tento projekt se zabývá posílením konkurenceschopnosti firem v rámci výběrových řízení na realizaci projektů zahraniční rozvojové spolupráce Evropských společenství. Tyto programy poskytují pomoc v podobě služeb, dodávek a realizace stavebních prací pro státy vně EU - např. kandidátské státy, rozvojové státy aj.

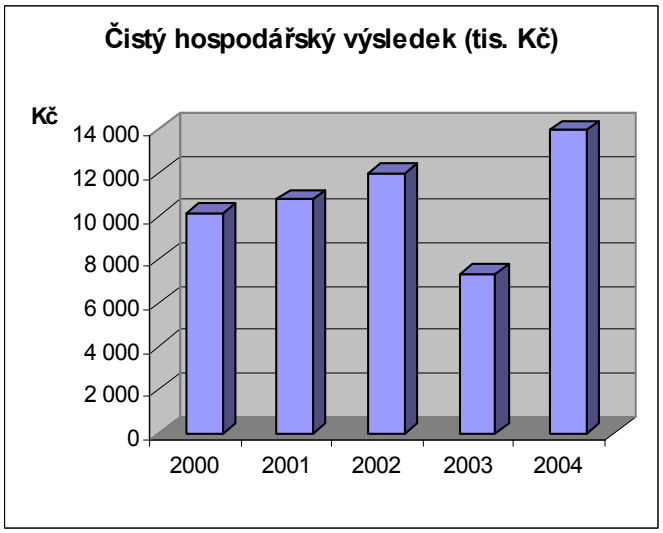
CERN - Evropské centrum pro nukleární výzkum

Informace o veřejných zakázkách a dalších příležitostech pro české firmy, které nabízí CERN - mezivládní evropské středisko, zaměřené na základní fyzikální výzkum elementárních částic a struktury hmoty.

Meziroční srovnání ukazatelů
Přehled ekonomických výsledků

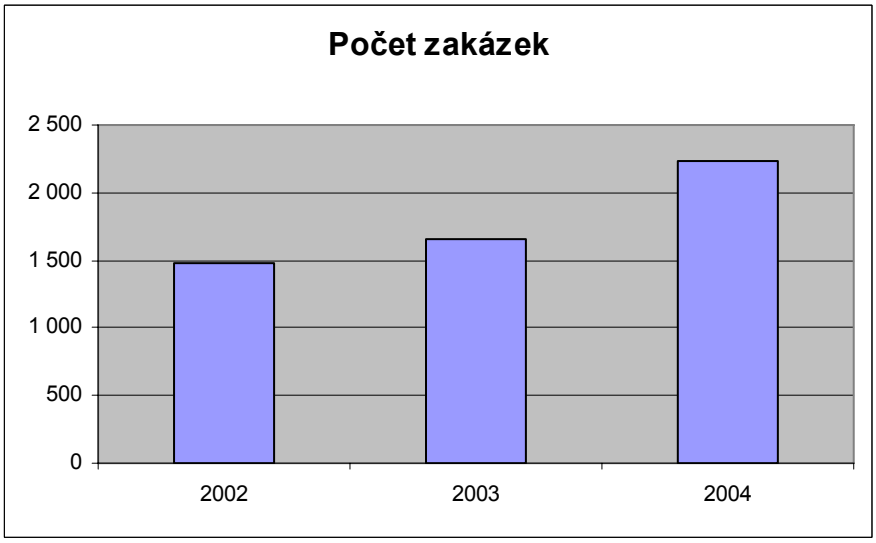
Ekonomické výsledky v letech	2000 v tis. Kč	2001 v tis. Kč	2002 v tis. Kč	2003 v tis. Kč	2004 v tis. Kč
Tržby celkem	**113 570**	**167 641**	**175 806**	**187 757**	**223 062**
Tržby za služby	3 507	8 265	24 019	285 337	29 420
Jiné ostatní tržby a výnosy	7 783	4 390	3 229	2 786	5 484
Příspěvek na provoz od zřizovatele	102 280	154 986	148 558	156 634	188 158
Náklady celkem	**103 450**	**156 881**	**160 107**	**176 753**	**209 090**
z toho: spotřebované nákupy	16 442	9 693	8 713	10 684	9 439
služby	59 126	108 532	105 168	112 269	140 169
osobní náklady	23 105	30 448	33 813	37 993	39 764
ostatní náklady	4 777	8 208	12 413	15 807	19 718
Odvod z hosp. výsledku	**0**	**0**	**3 700**	**3 672**	**0**
Hospodářský výsledek po odvodu	**10 120**	**10 760**	**11 999**	**7 332**	**13 972**

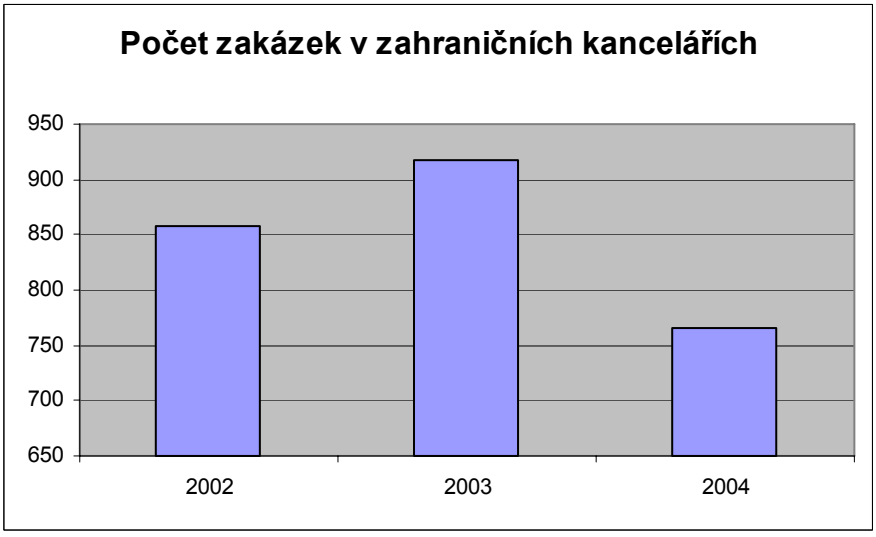




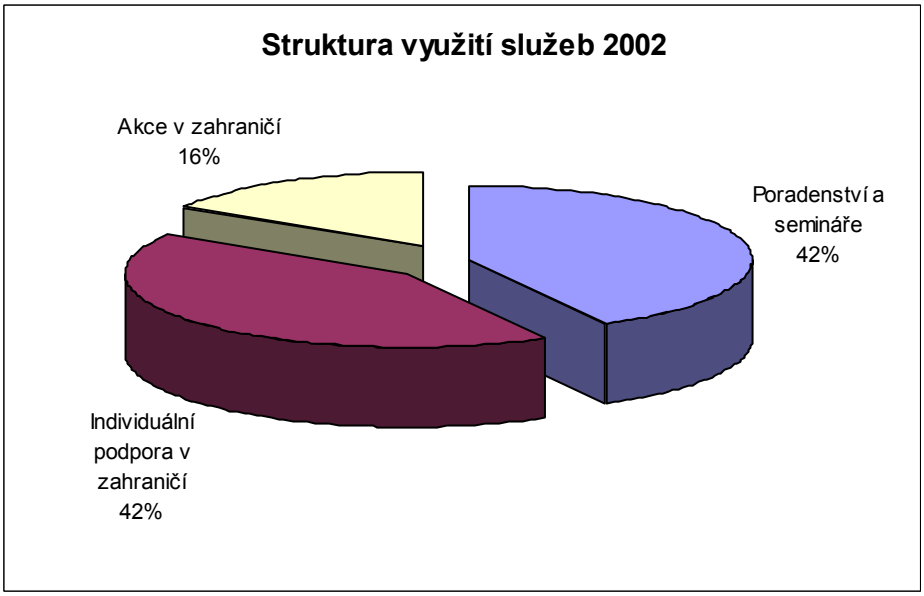
Přehled klíčových ukazatelů

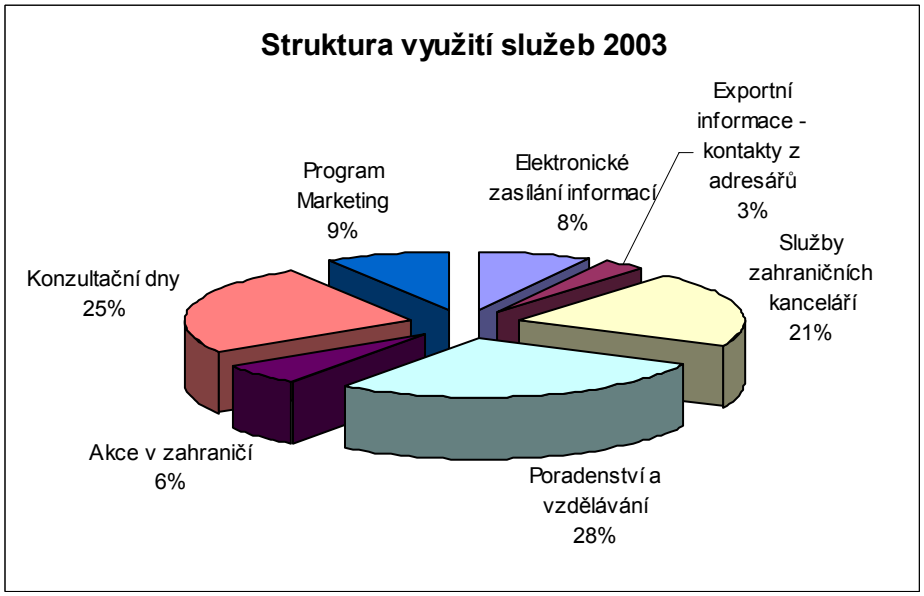
Přehled klíčových ukazatelů	2002	2003	2004
Počet zakázek	1 484	1 658	2 238
Počet zakázek v zahr. kancelářích	858	918	766
Tržby agentury	24 019 000 Kč	28 336 914 Kč	29 419 875 Kč
Počet vzdělávacích akcí a seminářů	62	127	93
Program marketing - počet dotovaných podniků	354	410	373
Realizované dotace programu Marketing	63 738 827 Kč	70 000 000 Kč	68 849 808 Kč

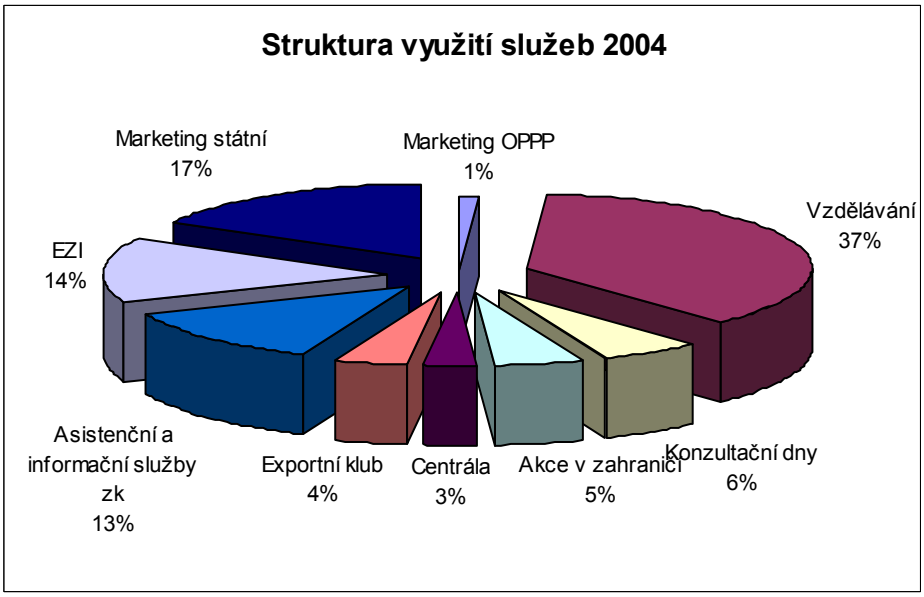




Struktura využití služeb

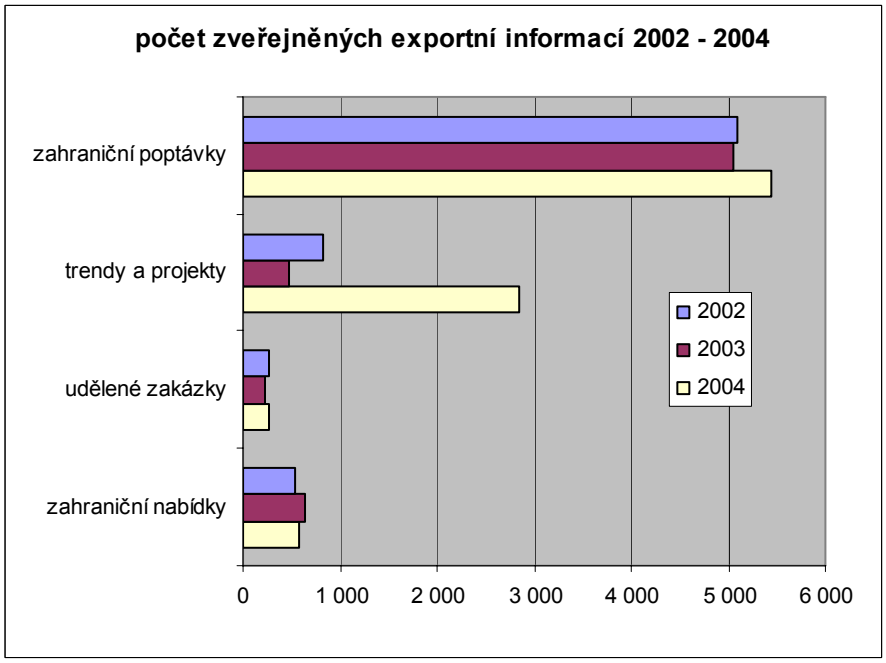






Počet zveřejněných exportních informací

Zveřejněné exportní informace	2002	2003	2004
zahraniční nabídky	538	629	585
udělené zakázky	271	218	278
trendy a projekty	816	484	2 853
zahraniční poptávky	5 085	5 045	5 434



Strategie pro období 2006 – 2010

Vysoká přidaná hodnota

Přidanou hodnotu indikuje počet úspěšných případů vývozu a objem výše exportu klientů realizovaných s využitím služeb CzechTrade. Tyto dva základní indikátory zůstanou hlavním předmětem měření i do budoucna, ovšem s tím, že budou rozšířeny o další kategorie přínosů klientům – ne všechny služby agentury totiž mají bezprostřední vztah k exportu – například poskytnutí informací o konkurenci na zahraničním trhu.

Po vzoru zahraničních „Trade Promotion Organizations" bude agentura postupně realizovat dva typy průzkumů zaměřených na přidanou hodnotu.

Prvním z nich je kvantitativní průzkum přidané hodnoty služeb klientů CzechTrade využívajících služby zahraničních kanceláří. Průzkum bude sledovat především následující okruh témat:

- Pozitivní dopad na finanční výsledky
- Doporučení CzechTrade partnerům a klientům
- Úspora času
- Snížení nákladů souvisejících s aktivitami na zahraničním trhu
- Pomoc pro lepší rozhodnutí
- Zlepšení konkurenceschopnosti

Takto získané informace se stanou jedním z pilířů budování silné značky. Jednak budou využity pro zlepšení PR a marketingové komunikace a jednak poslouží jako prodejní argumenty konzultantů, kteří se v průběhu jednání budou moci opřít o tvrzení vycházející z hodnocení klientů.

„Například 80% našich klientů potvrzuje, že díky službám CzechTrade dosahuje úspor nákladů a času."

Druhým průzkumem pak bude kvalitativní měření přidané hodnoty. Tento kvalitativní průzkum umožní agentuře získat zpětnou vazbu nejen o tom, zda přinášejí jednotlivé služby zvýšení exportu, ale i o tom, v jaké míře pro jednotlivé cílové skupiny. Takto získané informace budou využity zejména k optimalizaci nabídky služeb a rovněž se stanou dalším významným prodejním argumentem v podobě doporučení pro jednotlivé cílové skupiny pro výběr a využití konkrétní služby.

Kromě toho neméně významným cílem měření přidané hodnoty bude zlepšování konkurenceschopnosti, která nebude zaměřena na domácí schopnosti firmy, ale na realizaci exportních aktivit firmy vůči konkurenci na zahraničním trhu.

Rozvoj služeb

Současný rozsah služeb je srovnatelný s nabídkou vyspělých organizací na podporu exportu. V dalším rozvoji služeb hodlá agentura vycházet především z klíčových potřeb klientů podle fáze životního cyklu rozvoje exportéra:

- Příprava na export
- Výběr trhu
- Vstup na trh
- Rozvoj a růst na trhu

Tento přístup strukturování služeb je charakteristický pro většinu vyspělých zahraničních agentur na podporu exportu v zemích, jako je Velká Británie, Dánsko, Irsko, Švédsko, Finsko, Kanada a Nový Zéland.

Při rozvoji služeb bude agentura stavět na následující hodnotové propozici služeb – poskytovat kombinaci konzistentní kvality, jednoduchého nákupu služeb a přijatelné ceny, kterou nedokáže nabídnout žádný komerční subjekt vzhledem k využití kvalitní sítě zahraničních kanceláří.

Poskytování exportního poradenství bude založeno na realizaci standardizovaných produktů s jasnou potřebou na straně klienta a přidanou hodnotou na straně agentury.

Před změnami a uváděním zlepšených nebo inovovaných služeb na trh budou intenzivně využívány marketingové nástroje průzkumu potřeb zákazníků, „focus groups“, pracovní semináře apod. V tomto směru bude posílena role odboru marketingu CzechTrade, který bude kromě inovací také odpovědný za kvalitu a úspěšný prodej jednotlivých typů služeb.

Novým prvkem systematického zlepšování služeb agentury CzechTrade bude využití nejlepších postupů zahraničních „Trade Promotion Organizations“, přičemž hlavním cílem je rychlejší zavádění služeb a trvalé zvyšování kvality tak, aby rostla přirozená poptávka po službách CzechTrade.

Orientace na klienta

Segmentace klientů do jednotlivých skupin je základem pro kvalitní uspokojení jejich rozdílných potřeb a současně také východiskem pro efektivní alokaci zdrojů agentury. Cílení služeb vychází ze tří základních kritérií – zkušenost s exportem, velikost firmy a plánované exportní aktivity.

Segment A

- Firma nemá žádnou nebo minimální zkušenost s vývozem (nepravidelný export na základě poptávky).
- Malá nebo střední firma podle kritérií Evropské unie.
- Firma chce vyvážet a chce se připravit na vývoz nebo potřebuje vytížit volné výrobní kapacity.

Segment B

- Firma vyváží na jeden nebo dva trhy a chce pronikat na další. Podíl exportu na tržbách je minimální.

- Malá nebo střední firma podle kritérií Evropské unie.
- Firma stojí před výběrem vhodného trhu a vstupem na trh.

Segment C

- Firma působí na více než dvou trzích nebo vývoz tvoří výrazné procento obratu firmy.
- Malá, střední nebo velká firma.
- Firma vybírá další trh, vstupuje na trh nebo realizuje rozvojové aktivity na existujícím trhu.

Cílení služeb je důležitým aspektem efektivnosti při poskytování nejen hlavních služeb agentury, ale i v realizaci marketingových aktivit pro české exportéry. Z tohoto hlediska se soustředíme na realizaci marketingových aktivit podle potenciálu jednotlivých oborů na zahraničních trzích a odpovídající nabídky českých exportérů.

Segment	Přístup	Klíčová služba	Cenotvorba
A	Domácí poradce	Program „První export“	Pevná částka za absolvování programu
B	Regionální konzultant	Informační služby zahraničních kanceláří	Na základě pracnosti a hodinové sazby
C	Regionální konzultant	Asistenční služby zahraničních kanceláří	Na základě pracnosti a hodinové sazby

Kvalitní síť pro export

V souladu s Exportní strategií ČR pro období 2006 - 2010 bude rozšířena kapacita sítě zahraničních kanceláří. Cílovým stavem v roce 2010 je 42 zahraničních kanceláří.

Zakládání nových kanceláří a kapacitní posílení bude vycházet ze tří základních kritérií:

- otvírání nových kanceláří na rozvíjejících se trzích v souladu s exportní strategií
- poptávka českých firem po službách kanceláře v daném teritoriu
- využití disponibilního času zahraniční kanceláře

Činnost kanceláří v teritoriích, kde neexistuje zájem o vývoz, bude utlumena, a jejich kapacita přesunuta do zemí, o které je vysoký zájem exportérů nebo nabízejí strategické exportní příležitosti.

Z hlediska kvality sítě zahraničních kanceláří se zvýší flexibilita dostupných kapacit. V případě převisu poptávky českých firem nad možnostmi pracovníků zahraniční kanceláře budou využity místní síly na základě časově omezeného kontraktu. V rámci efektivnějšího využití časového fondu zahraničních kanceláří bude kladen důraz na sladění společných aktivit a priorit zaměstnanců zahraničních kanceláří CzechTrade a pracovníků obchodně ekonomických úseků. Základem spolupráce se stanou společné plány činnosti, které budou zavedeny v rámci nového systému řízení služeb státu v zahraničí.

Zlepšení strategického řízení zahraničních kanceláří dosáhneme také posílením principu

neustálého zlepšování a soutěžení mezi jednotlivými kancelářemi z hlediska dosažených výsledků.

Dalším prvkem rozvoje kvality sítě zahraničních kanceláří bude systematická příprava pracovníků CzechTrade před vysláním do zahraniční kanceláře v rámci projektu Exportní akademie. Posíleny budou prvky rotačního systému, které umožní nejschopnějším pracovníkům výjezd do dalších teritorií případně nástup na odpovídající pozice v centrále CzechTrade.

V rámci procesu založení kanceláře budou zavedeny marketingové aktivity a prodej služeb před odjezdem pracovníka do nově založené kanceláře. Soustředíme se na to, aby pracovník odjížděl z centrály do teritoria již s prvními zakázkami.

Součástí rozvoje sítě CzechTrade nejsou pouze zahraniční kanceláře, ale také Regionální exportní místa (REM). V roce 2006 došlo ve spolupráci s Hospodářskou komorou ČR k založení 13 kanceláří v jednotlivých regionech České republiky. Základní výzvou je rychlé zapojení regionálních míst do marketingových a prodejních aktivit. Prvním předpokladem je změna organizační struktury, kdy se regionální místa stávají součástí šesti regionálních týmů. Regionální týmy vedou zkušení pracovníci CzechTrade, kteří mají odpovědnost nejen za výsledky vlastní práce, ale také za rozvoj a výsledky pracovníků REM.

CzechInvest
Úvod

Agentura pro podporu podnikání a investic CzechInvest informuje o programech podpory průmyslu a podnikání, zprostředkovává českým podnikům přístup k dotacím ze strukturálních fondů EU a státního rozpočtu, pomáhá zlepšovat konkurenceschopnost firem a rozvíjet podnikatelské prostředí.

Co je CzechInvest?

CzechInvest je agentura pro podporu podnikání a investic. Jde o státní příspěvkovou organizaci podřízenou Ministerstvu průmyslu a obchodu ČR. Vznikla 2. ledna 2004 sloučením s dalšími dvěma agenturami ministerstva – s Agenturou pro rozvoj podnikání (ARP) a Agenturou pro rozvoj průmyslu ČR (CzechIndustry).

Původní záměr

Hlavním úkolem původního CzechInvestu, který byl založen v roce 1992, byla propagace České republiky jako ideálního místa pro zahraniční investice a současně podpora přílivu přímých zahraničních investic do České republiky.

Současný záměr

Hlavním posláním nového CzechInvestu je podpora konkurenceschopnosti českých podnikatelů. Zejména se jedná o podporu zpracovatelského průmyslu a inovací (inkubátory, vědeckotechnologické parky) prostřednictvím Operačního programu Průmysl a podnikání Ministerstva průmyslu a obchodu ČR.

K rozvoji domácích společností a vzniku nových firem přispívá CzechInvest prostřednictvím svých služeb, rozvojových programů a práce na zlepšování podnikatelského prostředí. Zároveň zůstává výhradním příjemcem žádostí o poskytnutí investičních pobídek a jeho úkolem i nadále zůstává získávání přímých zahraničních investic pro ČR.

V rámci zjednodušení komunikace mezi státem, podnikateli a EU tak vzniklo jedno kontaktní místo, kde domácí i zahraniční podnikatelé dostanou kvalitní informace o veškerých formách podpory podnikání v ČR a kde si mohou o jednotlivé druhy podpor také zažádat.

Vize agentury CzechInvest
Motto:
„Česká republika - jedna z nejvíce konkurenceschopných zemí Evropské unie“

S cílem maximálně zjednodušit a zpřístupnit poskytování podpory pro malé a střední podnikatele ve zpracovatelském průmyslu otevřel CzechInvest 13 regionálních poboček na úrovni krajů. Pracovníci těchto regionálních kanceláří poskytují informace o strukturálních fondech EU a systému státní podpory, pomáhají při vyplňování žádostí o podporu, tyto žádosti přijímají a dohlédnou také na čerpání finančních prostředků pro jednotlivé projekty.

Historie

Počátky vzniku

Od svého založení v listopadu 1992 posiluje agentura CzechInvest (CI) prostřednictvím svých služeb a rozvojových programů konkurenceschopnost české ekonomiky, a to především prostřednictvím podpory přílivu přímých zahraničních investic (PZI). Svým klientům, respektive zahraničním investorům poskytuje potřebné informace a poradenství a zprostředkovává nezbytné kontakty. Hlavní smyslem práce CzechInvestu bylo až do poloviny roku 2003 propagovat Českou republiku jako ideální lokalitu pro PZI a pomáhat potenciálním investorům s realizací jejich projektů v oblasti výroby, výzkumu a sdílených služeb. Veškeré služby CzechInvestu jsou českým i zahraničním subjektům poskytovány bezplatně.

Nový směr

Od začátku roku 2003 se CzechInvest začal připravovat na novou roli – roli rozvojové agentury, která bude zastřešovat podporu podnikání ve zpracovatelském průmyslu. Rozhodnutí ministra průmyslu a obchodu o sloučení CzechInvestu s dalšími dvěma agenturami – Agenturou pro rozvoj podnikání a CzechIndustry – vedlo ve druhé polovině roku k velkým změnám v jeho struktuře. Byla zahájena příprava na sloučení, ať už po technické stránce (potřebné prostory), tak po personální (nové členění, vznik nových divizí a odborů, nábory). Především ale bylo třeba zajistit obsah nových činností, které se vedle původního poslání měly stát pro další práci CzechInvestu klíčovými – podpora malého a středního podnikání a implementace Operačního programu Průmysl a podnikání. Všechny tyto přípravy vyvrcholily 2. ledna 2004 vznikem nové Agentury pro podporu podnikání a investic CzechInvest.

V souvislosti s novými aktivitami zejména na poli podpory domácích podnikatelů a také vzhledem k neustále se zvyšujícím nárokům na kvalitu poskytovaných služeb se agentura CzechInvest v roce 2004 rozhodla vybudovat a zavést vlastní systém managementu jakosti podle požadavků normy ISO 9001:2000. Stvrzující certifikát od společnosti Det Norske Veritas obdržel CzechInvest na sklonku minulého roku. Tento certifikát pokrývá veškeré služby poskytované CzechInvestem v České republice i v zahraničí v oblasti podpory přílivu zahraničních investic, rozvoje domácích podniků, vzniku nových firem a rozvoje podnikatelského prostředí. Jedná se o tvorbu a implementaci programů podpory podnikání ze Strukturálních fondů EU, Phare a národních programů a poskytování souvisejících informací a služeb. Certifikát managementu jakosti nejen prokazuje schopnost udržet a kontrolovat stálou kvalitu služeb, ale současně signalizuje, že jeho držitel je spolehlivou a důvěryhodnou organizací.

CzechInvest se snaží přispívat k rozvoji a zlepšování podnikatelského prostředí. S problémy, které mají investoři či podnikatelé a snahou CzechInvestu je pomáhat při jejich řešení. Rada pro rozvoj podnikatelského prostředí je do budoucna důležitou platformou pro hledání řešení problémů tohoto typu a CzechInvest je jejím výkonným sekretariátem.

V radě spolu působí zástupci státní správy, podnikatelů, zaměstnanců a vysokých škol, což garantuje hledání takových řešení, která nejsou odtržena od ekonomické reality. Rada rovněž připravuje konkrétní návrhy pro tvorbu národohospodářské politiky a hospodářské strategie a srovnává vývoj podnikatelského prostředí České republiky s vývojem v ostatních zemích, zejména EU.

Možnosti financování
Přímé zahraniční investice

Ještě jako agentura podporující zejména příliv zahraničních investic se CzechInvest postupně soustředil na vybrané sektory zpracovatelského průmyslu – výrobu automobilů a jejich komponentů, elektroniku a mikroelektroniku, chemický průmysl, farmacii nebo přesné strojírenství. V poslední době se k těmto oblastem přidal také letecký průmysl, zdravotnická technika a biotechnologie. V souladu s trendem v západních zemích také narůstá počet projektů v oblasti výzkumu a vývoje (technologická centra) a strategických služeb (centra zákaznické podpory, finanční a účetní služby).

V těchto svých snahách je CzechInvest podporován Sdružením pro zahraniční investice – AFI, jehož členové se rekrutují z řad renomovaných společností, které mají dlouhodobé zkušenosti s českým prostředím a poskytují služby v oblastech klíčových pro příliv a realizaci zahraničních investic (jedná se například o konzultační, právní, HR, IT a další služby). Hlavním cílem spolupráce CzechInvestu a Sdružení pro zahraniční investice je zajistit, aby vstup zahraničních investorů na český trh byl maximálně usnadněn.

Oba subjekty společně založily projekt „Partnerství pro podporu přímých zahraničních investic“, otevřený široké podnikatelské obci, jehož účastníci reprezentují silné a renomované společnosti, které svou účastí v něm podporují poslání a aktivity agentury CzechInvest.

Investiční pobídky

V devadesátých letech bylo významnou změnou v rámci investičního prostředí České republiky vypracování systému investičních pobídek. Pobídky se investorům začaly nabízet nejdříve na základě přijetí vládního usnesení z dubna 1998 a později i usnesení vlády z prosince téhož roku. Takto získané zkušenosti pomohly ministerstvu průmyslu a obchodu, CzechInvestu i dalším státním institucím předložit návrh nového zákona o investičních pobídkách. Zákon o investičních pobídkách (č. 72/2000), vstoupil v platnost 1. května 2000 a domácím i zahraničním investorům stanovuje stejná práva a podmínky. Později byl systém investičních pobídek rozšířen o podporu strategických služeb a technologických center – rámcový program pro podporu technologických center a center sdílených služeb. Česká republika se tak stala prvním státem v regionu střední a východní Evropy, kde byl systém investičních pobídek určen zákonem. Tento zákon navíc splňoval kritéria stanovená Evropskou komisí pro povolenou míru veřejné podpory. Navíc díky tzv. euronovele zákona o investičních pobídkách, schválené v roce 2003, může Česká republika poskytovat státní podporu i po svém vstupu do Evropské unie.

Za přispění programu Phare realizuje CzechInvest od roku 1999 Program podpory subdodavatelů. Cílem programu je zintenzívnit a prohloubit kontakty mezi domácími subdodavateli a nadnárodními firmami, které plánují investovat v ČR nebo zde již působí. V databázi CzechInvestu, která je volně přístupná na webové stránce agentury, je nyní víc než 2000 českých firem, potenciálních subdodavatelů.

Průmyslové zóny

Kvalitní investiční nabídka musí obsahovat také připravenou průmyslovou zónu. Proto vláda schválila systém veřejné podpory trhu podnikatelských nemovitostí, který byl oficiálně zahájen v roce 1999. Díky Programu podpory rozvoje průmyslových zón vzniklo do konce roku 2003 v České republice 82 průmyslových zón. V roce 2001 byl uvedený program rozšířen o další podprogramy, a to Regenerace průmyslových zón, Výstavba a regenerace nájemních objektů a Akreditace

průmyslových zón.

Dosažené výsledky

CzechInvest se během své existence podílel na víc než 600 investičních projektech v celkové hodnotě převyšující 460 miliard korun. Díky těmto investicím by mělo postupně vzniknout téměř 125 tisíc přímých pracovních míst. V oblasti průmyslu u nás tradičně nejvíce investují firmy z Německa (27 %) a Japonska (20 %). Společnosti sídlící v České republice zaujímají s 11 % třetí pozici. Kromě tradičních sektorů, jako jsou automobilový (43 %) a elektrotechnický (16 %) průmysl, se stále častěji objevují investice do inovací a moderních odvětví (mikroelektronika, přesné strojírenství).

Strategie

I. priorita: Rozvoj podnikatelského prostředí

V rámci priority budou rozvíjeny jednotlivé níže uvedené programové oblasti tak, aby se ČR stala místem, kde může růst a prosperovat podnikání s vysokou přidanou hodnotou, v podnicích všech velikostí a původu kapitálu.

Programové oblasti:

- Infrastruktura pro inovace, výzkum a vývoj:

zajistit rozvoj vědecko-technologických parků a inkubátorů včetně komplexních služeb tak, aby se zintenzivnila spolupráce vysokých škol a vědecko-výzkumných instituci s průmyslem a maximálně usnadnil proces transferu výsledků vědy a výzkumu do výroby

- Nemovitosti pro podnikání:

zajistit dostatečnou nabídku nemovitého majetku - pozemků i objektů tak, aby vyhovovaly potřebám podnikatelů a aby jejich nedostatek nebyl barierou pro vytváření nových podnikatelských subjektů

- Infrastruktura pro rozvoj lidských zdrojů:

zaměřit rozvoj lidských zdrojů na inovace a technologický rozvoj, využití informačních a komunikačních technologií

- Služby:

zajistit dostupnost kvalitních a nákladově efektivních expertních poradenských služeb

- Informace:

využití moderních informačních technologií při zajištění jednotného kontaktního místa (one-stop-shop) pro poskytování informací a služeb podnikatelům

- Zdokonalování podnikatelského prostředí Bariéry:

spolupráce s vládou a podnikatelskou veřejností při identifikaci a průběžném odstraňování byrokratických, administrativních a legislativních překážek rozvoje firem a konkurenceschopnosti ČR s cílem trvale zkvalitňovat podnikatelské prostředí

II. priorita: Podpora zakládání nových a rozvoje stávajících podniků

V rámci priority budou rozvíjeny níže uvedené programové oblasti s cílem zajistit, aby podniky se sídlem v ČR byly vybavené dovednostmi a zdroji, které jim umožní konkurovat na globálním trhu.

Programové oblasti:

- Nově zakládané podniky s růstovým potenciálem:
  využití rizikového kapitálu a dalších mechanismů financování v kombinaci s poskytováním vhodných prostor pro podnikání a poradenstvím pro začínající podnikatele

- Nové technologie a inovace:
  granty, půjčky a poradenství pro využití nových technologií, rozvoj nových výrobků nebo výrobních procesů a jejich uplatnění na trhu

- Přístup k financím:
  zajistit, aby podniky všech velikostí ve všech stupních rozvoje nebyly omezovány nedostatkem vhodných a konkurenceschopných zdrojů financí, včetně finančních zdrojů rizikového kapitálu

- Pobídky:
rozvoj systému investičních pobídek tak, aby jejich využití efektivně a účinně posilovalo konkurenceschopnost ČR

- Rozvoj lidských zdrojů:
  granty na podporu firem usilujících o trvalý růst kvalifikace svých zaměstnanců

- Informační a komunikační technologie:
  využití informačních technologií k podpoře zkvalitnění řízení podniků, efektivnosti výroby a poskytování služeb zákazníkům

- Zlepšení výsledků a výkonů:
  podpora vyhodnocování a porovnávání konkurenceschopnosti českých podnikatelských subjektů oproti praxi nejúspěšnějších podniků na světovém trhu (benchmarking), poskytování poradenství a finanční podpory na posílení jejich konkurenceschopnosti.

III. priorita: Globální vazby

V rámci priority budou rozvíjeny níže uvedené programové oblasti tak, aby jejich prostřednictvím ČR trvale posilovala konkurenceschopnost podnikatelského prostředí v globálním měřítku a současně, aby podniky se sídlem v ČR byly schopné identifikovat a využít investiční a obchodní příležitosti na globálním trhu.

Programové oblasti:

- Přímé zahraniční investice:
  zajistit, aby si Česká republika zachovala konkurenceschopné postavení na globálním trhu a prostřednictvím přílivu přímých zahraničních investic posilovala technologický rozvoj, rozvoj kvalifikací, moderních metod řízení, inovace a konkurenceschopnost

- Dodavatelské řetězce:

podpora českých subdodavatelů především v oblastech výroby s vysokou přidanou hodnotou s cílem podpořit jejich působení na globálním trhu

- Poskytování služeb „After Care“:

udržovat trvalý kontakt se zahraničními podnikateli v ČR s cílem podpořit jejich další investiční činnost v ČR, přispívat k růstu podílu domácích subdodavatelů a trvalému zvyšování podílu přidané hodnoty na jejich místní produkci

- Podpora investic českých podniků v zahraničí:

ve spolupráci s agenturou CzechTrade posilovat postavení českých podnikatelských subjektů na globálním trhu podporou jejich investičních aktivit v zahraničí.

IV. priorita: Rozvoj klastrů (specifická nová oblast podpory)

Cílem této nové programové iniciativy je zajistit, aby inovace a konkurenceschopnost v klíčových průmyslových odvětvích českého průmyslu byly posilovány komplexní podporou a vytvářením rozvojových partnerství mezi seskupeními vzájemně na sebe navazujících výrobních podniků a poskytovatelů služeb (klastry)

Programové oblasti:

- Identifikace klastrů:

identifikace stávajících a potenciálních klastrů na základě národní a regionálních odvětvových analýz

- Rozvojová partnerství:

vytváření národních i regionálních partnerství s cílem realizace koncentrované, komplexní a specifické podpory pro daný klastr v oblastech financování, marketingu, rozvoje lidských zdrojů, infrastruktury a inovací

Prioritní sektory

Na základě zhodnocení trendů vývoje jednotlivých sektorů na domácím i globálním trhu a současně i zmapováním investičního prostředí České republiky a nabídkových faktorů pro umístění nových investic byly stanoveny následující prioritní sektory:

Tradiční sektory českého průmyslu s růstovým potenciálem

- Elektronika
- Přesné strojírenství a automobilový průmysl
- Chemie a plasty

Hi-tech výrobní oblasti

- Mikroelektronika/polovodiče
- Biotechnologie a farmacie
- Optoelektronika

Hi-tech služby

- Informační a komunikační technologie, vývoj softwaru
- Strategické služby - Centra sdílených služeb, expertní a řešitelská centra
- Opravárenská centra

Programové nabídky pro podnikatele

Poradenství

Nejen vstup do podnikání, ale i každodenní provoz firmy přináší řadu úskalí, se kterými možná potřebujete poradit. S něčím vám může pomoct CzechInvest, respektive jejich regionální kanceláře působící na úrovni krajů, jindy už potřebujete pomoc poradenské firmy nebo odborného konzultanta.

Agentura CzechInvest umožňuje malým a středním podnikům využít poradenských služeb za cenově zvýhodněných podmínek v rámci programu Poradenství. Tyto služby poskytuje síť regionálních a poradenských informačních center (RPIC) a podnikatelských a inovačních center (BIC).

Pokud nepotřebujte přímo konzultovat své podnikatelské projekty, ale rádi byste využili zkušeností jiných úspěšných firem nebo získali srovnání, využijte benchmarkingu. Jeho podstatou je vyhledávání nejlepších podnikatelských praktik dosahovaných v daném oboru a jejich porovnávání s výsledky vlastního podniku.

Malým a středním podnikům může při vstupu na zahraniční trhy poradit agentura CzechTrade. Ty, které mají své sídlo mimo území hlavního města Prahy, mohou také využít program Marketing, v rámci nějž lze čerpat finanční podporu na aktivity vedoucí k propagaci podniku v zahraničí.

CzechInvest myslí i na ty, kteří naopak chtějí působit jako dodavatelé zahraničního koncernu zde, v České republice, a to v rámci Projektu rozvoje českých dodavatelů. CzechInvest ale také spravuje rozsáhlou databázi dodavatelských firem.

Investice a inovace

Hlavním smyslem systému podpory podnikání je zvýšit konkurenceschopnost českého průmyslu i celého podnikatelského prostředí v České republice. Jednotlivé programy podpory jsou určeny především progresivním firmám s růstovým potenciálem, firmám, které hodlají do svého rozvoje investovat. K podpoře vyváženého a udržitelného rozvoje jednotlivých regionů ČR vyhlašují jednotlivé kraje programy Společného regionálního operačního programu.

Jednou z cest, jak posílit konkurenceschopnost podniku, je zavádění nových výrobků, služeb či technologií. Díky programu Inovace mohou podniky bez ohledu na svou velikost získat podporu na realizaci projektů zaměřených na zvýšení technických a užitných hodnot výrobků, technologií a služeb nebo na zavedení pokrokových metod řízení či jiných netechnických inovací. Cílem programů Rozvoj a Technologie je zase zvýšit výkonnost malých a středních podniků podporou technické vybavenosti, zavádění certifikací a mezinárodních standardů.

Jakkoli je i malá firma růstová nebo má významný inovační potenciál, realizace podnikatelského záměru se nikdy neobejde bez financování. Při nedostatku volných prostředků lze využít například zvýhodněných úvěrů, které nabízí Českomoravská záruční a rozvojová banka. Velcí investoři – čeští i zahraniční – již zase několik let využívají systém zvýhodnění v podobě investičních pobídek.

Důležitou součástí moderního podnikání je šetrnost k životnímu prostředí, konečně, je to také jedna z obecných podmínek pro čerpání podpory v rámci Operačního programu Průmysl a podnikání. V rámci tohoto programu lze podporovat také projekty, které se přímo týkají úspor energií a využívání obnovitelných zdrojů.

Rozvoj lidských zdrojů

Podnikání není jen pořizování nemovitostí a strojů, jsou to především lidé, kteří pracují. Státní podpora se dosud zaměřovala především na tvorbu pracovních míst. Zaměstnavatelé ale často řeší také to, že pravidelné investice do zvyšování kvalifikace zaměstnanců představují stále významnější položku jejich rozpočtu. Důležitou součástí podpory podnikání z evropských fondů je tak podpora rozvoje lidských zdrojů – ať už se jedná o dotace na školení zaměstnanců nebo zavádění standardů jejich rozvoje.

Podstatnou součástí rozvoje lidských zdrojů v České republice je samozřejmě také vzdělávání. Zaměřili jsme se tedy na podporu spolupráce institucí terciárního vzdělávání (vyšší odborné školy a vysoké školy) s podniky.

Při řešení problematiky rozvoje lidských zdrojů velmi úzce spolupracuje CzechInvest také s Ministerstvem školství, mládeže a tělovýchovy a Radou vlády pro rozvoj lidských zdrojů.

Podnikatelské nemovitosti

CzechInvest aktivně působí na trhu podnikatelských nemovitostí České republiky – monitoruje a zprostředkovává informace o místním trhu komerčních, maloobchodních, logistických a skladových nemovitostí, a současně podporuje výstavbu a rozvoj nemovitostí a zón pro potřeby zpracovatelského průmyslu a služeb (průmyslové, kancelářské nemovitosti).

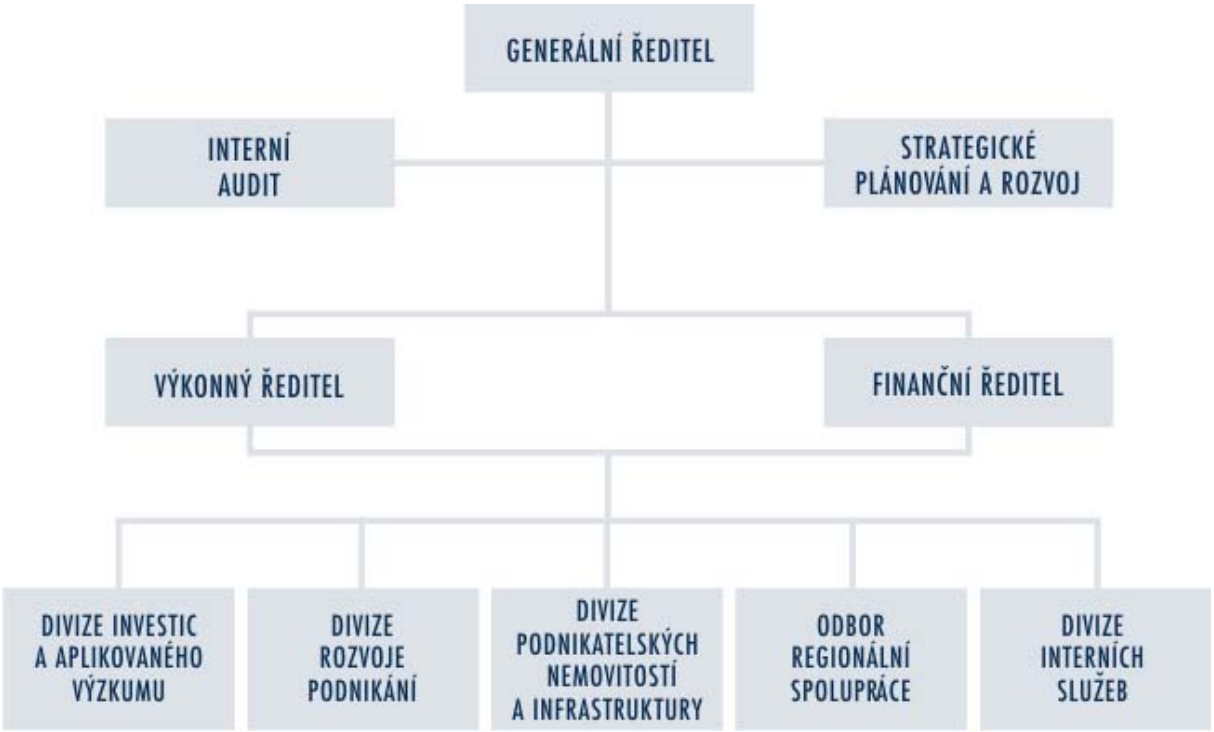
Dlouhodobě podporuje výstavbu podnikatelských nemovitostí, které pak nabízí investorům – zahraničním i domácím. Patří k nim průmyslové a podnikatelské zóny, výrobní haly (často s přidruženými skladovými a administrativními částmi), kancelářské prostory vhodné pro strategické služby a nemovitosti pro vědu a výzkum. V poslední době se také podílí na projektu identifikace a regenerace nevyužívaných či zanedbaných průmyslových nemovitostí (brownfields).

Prostřednictvím CzechInvestu mohou veřejné i soukromé subjekty (města, obce, svazky obcí, kraje, developerské firmy, malé a střední podniky a další) získávat finanční podporu z programů na rozvoj podnikatelské infrastruktury ze strukturálních fondů EU (Program Reality) nebo ze státního rozpočtu (Program na podporu rozvoje průmyslových zón). Tyto zdroje podpory se liší nejen svými podmínkami, ale hlavně cíli a možností žadatelů podporu získat – finance ze státního rozpočtu jsou určeny především na rozvoj průmyslových zón pro předem známého investora, naopak program Reality se vztahuje na širší okruh žadatelů a projektů.

CzechInvest spravuje rozsáhlou databázi podnikatelských nemovitostí. Prostřednictvím této databáze mohou municipality či podnikatelské subjekty nabízet vhodné pozemky, výrobní haly, prostory pro výzkum a vývoj či kanceláře pro podnikání v celé České republice. Z této databáze připravujeme nabídky pro investory, kteří v České republice chtějí realizovat své záměry v oblasti zpracovatelského průmyslu, strategických služeb, technologických center či zájemcům z řad developerských společností a jiných subjektů hledajících vhodné příležitosti pro realizaci developerských projektů. Ukázka nabídky nemovitostí, kterou jsme schopni na základě vašich požadavků připravit.

Dále shromažďujeme základní informace o jednotlivých regionech a připravujeme regionální analýzy a koncepce. Předmětem našeho zájmu je především ekonomický potenciál regionů a měst, lidské zdroje, IT a telekomunikace, doprava a související infrastruktura pro podnikání.

Organizační struktura agentury



Kontakty

Agentura CzechInvest má centrálu v Praze a dále můžete najít její zastoupení ve 13 krajích České republiky a na 9 zahraničních zastoupeních.

Centrála
info@czechinvest.org
tel.: 296 342 500
fax: 296 342 502
Štěpánská 15
Praha 2
120 00

Tiskové oddělení
press@czechinvest.org
tel.: 296 342 508
fax: 296 342 502

Regionální kanceláře

Na začátku roku 2004 založil CzechInvest síť 13 regionálních zastoupení přímo v jednotlivých krajských městech. V rámci zjednodušení komunikace mezi státem, podnikateli a Evropskou unií tak pro každý kraj existuje jedno kontaktní místo, kde dostanou domácí i zahraniční podnikatelé komplexní informace o formách podpory podnikání v České republice a jednotlivých programech podpory, ať z Evropských fondů nebo ze státního rozpočtu.

Regionální kanceláře agentury CzechInvest: usnadní vstup do podnikání; poskytují informace o strukturálních fondech EU a systému státní podpory; poskytují poradenství žadatelům o

podporu; pomáhají při vyplňování žádostí o odporu z fondů EU; přijímají žádosti o podporu k posouzení výběrovou komisí; kontrolují formální správnost a přijatelnost žádostí o podporu; dohlížejí nad čerpáním finančních prostředků pro projekt; spolupracují s regionálními a místními subjekty, institucemi a orgány.

Regionální kancelář pro Královéhradecký kraj
hradeckralove@czechinvest.org
tel.: 495 817 557, 495 817 558
fax: 495 817 556
Budova Krajského Úřadu
Wonkova 1142
Hradec Králové
500 02

Zahraniční zastoupení

Benelux a Francie
Britsko-irská kancelář
EU, Brusel
Japonská kancelář
Jihovýchodní Asie - Hong Kong
Německo - Kolín nad Rýnem
Německo - Mnichov
USA - Chicago
USA - Silicon Valley

13 Literatura a internetové zdroje

http://www.antiphishing.org
http://www.centrum.cz/
http://www.czechinvest.cz
http://www.czechtrade.cz
http://www.ewizard.cz/weblog/2004-05.html
http://www.ezavinac.cz
http://www.fugasoft.cz
http://www.iaudit.info
http://www.ibm.com
http://www.lupa.cz
http://www.mesec.cz
http://www.micr.cz
http://www.pooh.cz
http://www.rfidportal.cz
http://www.uoou.cz
http://www.worldbank.com
http://www.zive.cz

Budiš, P.:Bezpečná komunikace a certifikační autorita. DSM, č.1, 1997, ISSN 1211-8737
Budiš, P.:Certifikáty a certifikační autorita. Lancom, č. 7-8, 2000, ISSN 1210-2997
Budiš, P.: Certifikační autorita I.CA. DSM, č.6, 2000, ISSN 1211-8737
Budiš, P.: Elektronický podpis v praxi. DSM, č.3, 2002, ISSN 1211-8737
Gregušová, D. , Dulak, A. , Chlipala, M., Susko, B.: Právo informačných a telekomunikačných technológií. Bratislava: Slovenská technická univerzita vo Vydavateľstve STU, 2005. 186 s.
Mates P.,Smejkal V.: E-government v českém právu,
Linde Praha, 2006, ISBN 80-7201-614-8
Štědroň B., Manažerské řízení a informační technologie,
Grada 2006, ISBN 978-80-247-2052-4
Stedron, B. Forecast for Artificial Intelligence, In:FUTURIST (USA), March-April 2004, pp.24-25, ISSN 0016-3317.
Stedron, B. Law for the future. International conference LEFIS, Firenze Italy,
February 2006, www.lefis.org/meetings/general/firenze_2006/presentations/TXT72.pdf.
Stedron, B. Forecast for the Data Protection, In: Privacy Law and Business 3/2006.
Stedron, B. The possible Scenarios of the Data Protection,
In: Datenschutz und Datensicherheit 11/2006.
Vaculíková Naděžda: Aplikácia práva a právne princípy. Právny obzor 2003, číslo 3, strany 273 – 282.
Vaculíková Nadežda: Pojem aplikácie a interpretácie práva v diele Františka Weyra. In: Místo normatívní teorie v soudobém právním myšlení. K odkazu Františka Weyra a Hanse Kelsena. Masarykova univerzita Brno 2003, strany 123 – 130.
Vaculíková Nadežda: Uváženie štátneho orgánu pri aplikácii právnej normy. In: Slušnosť v práve. Anstëntigkeit in Recht. Právnická fakulta UK/Právnický inštitút Ministerstva spravodlivosti SR, Bratislava 1993, strany 249 – 254.

Tato skripta jsou spolufinancována
Evropským sociálním fondem a státním rozpočtem České republiky