MASARYKOVA UNIVERZITA

Ekonomicko-správní fakulta

Předmět Krizový management elektronického bankovnictví

RIZIKA V ELEKTRONICKÉM OBCHODOVÁNÍ

Bohdana Říhová 99644, Lenka Zvěšková 137850

Na rizika elektronického obchodování se dá pohlížet z více stran. Jako mince má dvě strany, tak i elektronický obchod probíhá mezi dvěma stranami. Mezi subjekty, které nabízejí a mezi subjekty, které od těchto nakupují. Proto v této práci rozlišíme rizika ze strany prodávajících a rizika ze strany kupujících. Všeobecně se dá říci, že na straně nabízejících subjektů stojí firmy a na straně kupujících firmy i jednotlivci. Jedná se buď o obchod business-to-business nebo business-to-customers.

1.1 Riziko ztráty výhod

První riziko se týká velkých firem u elektronického obchodování a to ztráta výhod při tomto obchodování. V elektronickém obchodování nerozhoduje fyzická alokace firmy, a to ani ve smyslu fyzické vzdálenosti od zákazníka a dostupnosti produktů, ani ve smyslu tzv. „dobrých adres“ v lukrativních čtvrtích měst. Tento fakt významně napomáhá transparentnosti trhu: zákazník má přístup k informacím o prodejcích téhož produktu, může pohodlně srovnávat ceny, solidnost firmy a servis, množství bariér známých z "tradičního trhu" tak odpadá. Zvyšuje se tlak na konkurenci, což - kromě jiných faktorů - snižuje koncové ceny produktů, dostáváme se k vítanému stavu "best service - best price". Obecně by se tak měla zlepšit informovanost na straně kupujících i prodávajících, již dnes se například objevují servery, které informují o neplatičích, zpronevěrách, podvodnících apod.

Dále náklady na reklamu jsou na internetu relativně nižší a velké firmy a řetězy firem tak ztratí konkurenční výhodu v možnosti pořádat bombastické reklamní kampaně, které si téměř žádná z malých a středních firem nemohla v tradiční podobě dovolit. Na druhou stranu je samozřejmé, že "být viděn" na Internetu bude i do budoucna klást vysoké nároky na reklamní strategie i samotné provedení reklamy. Někteří z analytiků elektronického obchodování přesto odhadují, že dojde k určitému propadu výdělků v reklamním a PR průmyslu. Lze tedy říci, že možnosti reklamy a PR budou se vstupem firmy do virtuálního světa podstatně rozšířeny, přístupnější i specifické.

Dalším faktorem, který hraje roli, je fakt, že pro vstup na elektronický trh není dále potřeba tak vysoký vstupní kapitál, jako je tomu při zakládání srovnatelné firmy v "tradiční podobě". Na druhou stranu je však třeba poznamenat, že dosavadní zkušenosti ukazují, že zavedení, realizace a provoz profesionálního a úspěšného systému pro elektronické obchodování na síti stojí velké investice časové, finanční i lidské a zatím se kromě pionýrů oboru (prodej knih, letenek, software nebo porno) velké zhodnocení těchto investic nedostavuje.

Odhady budoucího vývoje elektronického obchodu jsou vesměs optimistické: náklady na vytvoření systému elektronického obchodu by se měly dříve nebo později jeho zřizovateli vrátit, ať již je jím stát nebo konkrétní firma, především proto, že přechod na systém elektronického obchodování nastartuje celou řadu dalších procesů, které jako lavina převálcují ty, kteří se do systému nezapojí a zároveň nastartují podobné procesy ve svém fyzickém i virtuálním okolí.

Pro přechod na plné využívání všech prostředků moderní IT pro elektronické obchodování může být bariérou skutečnost, že v podstatě neexistuje ověřený a vyzkoušený model takového systému a zároveň se většina analýz shoduje v tom, že elektronický trh bude v mnohém odlišný od tradičního. Jinými slovy, hrozí podstatně větší riziko neúspěchu.

Na druhou stranu bez určitého rizika a počátečního experimentování nelze rozjet žádný podnik a už vůbec ne takový, jakým je virtuální obchodování. Skeptici si snad mohou vzít příklad z podobných systémů, které již fungují na podobné bázi: teleshopping a především finanční sektor a burza.

Existuje i reálná obava ze ztráty národní identity: pokud by například české podniky obchodovaly elektronickou cestou, musely by pravděpodobně používat angličtinu jako komunikační jazyk Internetu. To může být na jednu stranu odrazovacím momentem pro české zákazníky, na druhou stranu může dvoj- a vícejazyčná komunikace se zákazníky firmu značně vyčerpávat.

1.2 Riziko informační

Další obrovské riziko hrozící při e-obchodování je informační. Hlavními příčinami mohou být[1]:

- Nejsou řízena rizika nového typu - tzv. e-rizika. Prudký rozvoj používání Internetu je doprovázen významným zvýšením úrovně informačních rizik, bezpečnost nestačí nastolenému tempu.
- Bezpečnost není brána seriozně. Organizace nevěnují dostatek času ani zdrojů na řízení rizik.
- Počet a závažnost bezpečnostních průniků vzrůstá. Ve srovnání s předchozími lety ve všech sledovaných oblastech počet bezpečnostních průniků vzrostl.
- Bezpečnost je stále podřízena IT a ne podnikání (obchodním činnostem), to znamená, že podnikatelské požadavky na bezpečnost jsou málokdy správně (důkladně, řádně) identifikovány, a implementovány.
- Kvalita logického řízení přístupů k informacím se nijak významně nezlepšuje. Procedury pro správu řízení logického přístupu jsou zatím slabé. Uživatelé si většinou musí pamatovat několik hesel pro přístup do systémů, biometrické způsoby identifikace se zatím využívají jen minimálně.
- Byla pozorována pouze mírná zlepšení v tradičním chápaní bezpečnosti IT. Organizacím se lépe daří řídit tradiční oblasti bezpečnosti IT, mezi které patří zejména bezpečnostní politika IT, fyzická ochrana zařízení IT a plánování obnovy IT po havárii a nepředvídané události.

1.3 Riziko zajištění důvěry

[1] http://www.dsm.tate.cz/print.php?typ=DAA&showid=44&id=58584 11.10.2007

S informačním rizikem souvisí jeden z hlavních problémů v e-commerce, a to zajištění důvěry v bezpečí. Ale nejde jen o bezpečnost, ale jde i o budování důvěry v bezpečí. Například, v okamžiku, kdy se podnikání mění a stává se elektronickým, objeví se nové, odlišné a náročné problémy se zajišťováním vzájemné důvěry. Organizace podnikající v elektronickém obchodování nemohou setrvat na tradičních metodách ověřování důvěry partnerů v probíhajících transakcích. Partneři transakcí se vzájemně nevidí, ani si nemohou vzájemně verbálně sdělit příslušná fakta. Z principu o sobě mohou vzájemně vědět mnohem méně. Proto je pro obě strany podstatné, aby si vzájemně důvěřovaly. Tuto důvěru je třeba budovat jak v B2B obchodování, tak v B2C obchodování. V myslích spotřebitelů vzniká nedůvěra pramenící ze třech důležitých hledisek, která spotřebitel při použití služeb elektronického obchodování uplatňuje:

- Budou moje osobní údaje bezpečné nebo mohou být zneužity?
- Bude moje platba bezpečná?
- Budou zakoupené výrobky respektive služby doručeny tak, jak je slibováno?

Spotřebitelé vyhledávají ve výše uvedených aspektech jistý komfort. Pokud používají Internetu pro spojení s bankou, potřebují pro posílení své důvěry vědět, že nedílnou součástí spojení a transakce je jistá úroveň bezpečnosti a že banka se bude ujišťovat o jejím stavu. Obvykle je úroveň bezpečnosti a důvěry podporována pomocí dobrého jména a renomé banky.

Dosažení stavu důvěry mezi podniky má jiné aspekty než v případě koncového spotřebitele. Dva podniky, které vzájemně obchodují, se obvykle dobře znají a zpravidla mají smluvní vztah. Ten vytyčuje rámec důvěry a očekávaní na obou stranách. Pokud se stane, že obchodní vztahy začnou větší mírou záviset na technologických řešeních, pak nastavení důvěry vyžaduje mnohem adresnější prověrku toho, že na obou stranách byly implementovány všeobecně uznávané standardy pro bezpečnost a kontrolu. V celkovém rámci důvěry, jakmile je to provedeno jakýmkoli způsobem, se pak o všech transakcích mezi partnery předpokládá, že jsou důvěryhodné. Z těchto důvodů je pro organizace důležité zřízení infrastruktury veřejných klíčů (Public Key Infrastructure). Jejím prostřednictvím a s využitím digitálních certifikátů řádně spravovaných uznávanou certifikační autoritou se vybuduje mezi podniky společenství důvěry. Tak se význam důvěry aplikovaný v organizaci transformuje i do širšího podnikového prostředí. Přesto i tyto zdravé systémy neustále potřebují jistou úroveň externě prováděného auditu a verifikace. Externí audit přispívá k formování podstatné části společenství důvěry. Podle našeho názoru může certifikace jednoznačně přispět ke zkvalitnění služeb poskytovaných na Internetu. Měla by zaručit spotřebiteli a nakupujícím určitý standard kvality a jakosti a především korektního přístupu ze strany prodejce. Také musí zaručit dodržování právních předpisů, a to včetně ochrany spotřebitele, který většinou o protější straně, se kterou uzavírá smlouvu, neví vůbec nic a o seriózności prodejce může usuzovat jen maximálně podle jeho internetových stránek.

1.4 Riziko anonymity

Při provádění elektronického obchodu většina nakupujících nemá tušení, s kým obchoduje, kdo je na té druhé straně obchodu. Ke snížení tohoto rizika existují systémy dobrovolné certifikace, v rámci kterých se internetoví obchodníci zavazují k dobrovolnému plnění určitých kritérií a na oplátku o tom získávají od důvěryhodné certifikační autority osvědčení (obvykle v podobě tlačítka na internetovém serveru). Tím se stávají důvěryhodnější pro spotřebitele, který by měl dát přednost e-obchodu, který je certifikovaný. Certifikovat nebo akreditovat je možné samozřejmě produkty a služby v mnoha oblastech. Certifikace elektronických obchodů není upravena žádným obecně závazným právním předpisem. Ať již je certifikace prováděna dle zákonné úpravy nebo na základě dobrovolnosti, aby toto mělo smysl, musí být stanovena jasná pravidla pro udělení certifikátů. Pokud e-obchod pravidla splní, potom musí mít (právní) nárok na udělení certifikace, a pokud naopak přestane podmínky splňovat, musí mu certifikát být odebrán.

Certifikačními autoritami se někdy stávají také spotřebitelské organizace. V Evropské unii již osm spotřebitelských organizací za finanční podpory Evropské komise provozuje mezinárodní certifikační systém WebTrader. Značka "Web Trader" je určená pro elektronické obchody, které splní určité standardy. Jejich splnění je pro spotřebitele určitou zárukou kvality a důvěryhodnosti. Značku Web Trader udělují spotřebitelské organizace z osmi evropských zemí (Belgie, Francie, Itálie, Nizozemí, Portugalska, Řecka, Španělska a Velké Británie). Aby tato značka byla udělena, musí být mj. splněny následující podmínky. Musí být uváděny jasné a úplné ceny, které splňují požadavky dané legislativy zejména v otázkách ochrany dat a zabezpečení serveru. Udělení značky obvykle předchází kontrola webových stránek společnosti, přezkoumání zákonnosti obchodních a smluvních podmínek. Po udělení pak následuje průběžný monitoring. Sledují se stížnosti, analyzují trendy a provádí se testovací nákupy.

V České republice se certifikaci internetových obchodů věnuje Asociace pro elektronickou komerci (APEK). Certifikovaný e-obchod je dle APEK obchod, který poskytuje zákazníkům standardní úroveň základních služeb. To znamená, že například dodržuje slíbené dodací lhůty, odpovídá za kvalitu prodávaného zboží, odpovídá za zboží a řeší reklamace, zveřejňuje pravdivé informace atd. Jinými slovy dodržuje tzv. certifikační pravidla stanovená Asociací pro elektronickou komerci jako nejvyšší tuzemské autority v oblasti elektronického obchodování.

APEK obchody, které certifikuje, také pravidelně kontroluje (nebo by měl kontrolovat), jestli dodržují pravidla certifikace, a výsledky z těchto kontrol jsou zveřejňovány na webových stránkách APEK. Obchody, které certifikaci získají, budou APEK a jeho partnery propagovány a obdrží certifikační tlačítko umístitelné na stránkách internetové prodejny. V příloze č.2 jsou povinná certifikační pravidla dle APEK a v příloze č.3 je seznam certifikovaných e-obchodů dle APEK.

1.5 Riziko ztráty soukromí

Týká se především jednotlivců. Nepříjemnými pocity může být doprovázena jedna ze zdánlivých velkých výhod systémů pro virtuální obchodování: schopnost systému zaznamenávat přání jednotlivých konkrétních zákazníků, evidence velkých objemů informací o klientech a s tím související možnosti marketingu - komerční nabídky šité na míru rozesílané přímo na email konkrétního zákazníka, propojení několika firem a předávání zákazníků. Hrozí totiž nebezpečí ztráty soukromí a negativní pocity související s malou kontrolou evidence osobních údajů. Zákazník si sice může nastavit na svém elektronickém účtě různé filtry na "junk mail", samotný fakt, že někde někdo vypátral jeho zálibu v masožravých květinách a nyní mu pravidelně každý týden anonymní server zasílá obsáhlé komerční nabídky na hnojiva na masožravé květiny, může silně obtěžovat, byť se jedná o slušné a někdy dokonce i podepsané e-maily. Velice snadno se také může stát, že jednou zadaná osobní data nelze definitivně smazat prostě proto, že zákazník neví, kde jsou uložena nebo kam všude byla zaslána/prodána.

1.6 Rizika oklamání spotřebitele

Existují nekalé postupy, jak oklamat své zákazníky. Nikdo z nás se ale určitě nechce zařadit mezi podvedené zákazníky. Základní rada zní: každá informace musí být ověřitelná a pravdivá, neexistující adresa nebo nesrovnalosti v osobách zastupujících e-obchod by měly být znamením, že zde není něco v pořádku a měli bychom tyto skutečnosti ověřit. Shrňme si některé možnosti, jak napálit zákazníka a vydělat na jeho nepozornosti, neopatrnosti a dezinformovanosti[2].

Řadíme sem kontaktní informace, falešné reference, velikost e-obchodu, použití ikonky APEK, triky pro programátory, ankety, dodací lhůty, potvrzení objednávky, zaslání jiného nebo žádného zboží, matení v číslování dokladů, reklamační řád.

Co se týče kontaktních informací, jedná se o to, že prodejci o sobě často uvádějí nedostatečné kontaktní informace (e-mail nebo mobilní telefon). Obě tyto služby lze zřídit anonymně a nenesou vyšší informační hodnotu. Informace nesoucí vyšší hodnotu jsou název provozovatele, jeho IČo a DIČo.

Dále nekalí obchodníci využívají falešných referencí, kdy napíší několik řádků kladných referencích o svém obchodu, napíší nepravé jméno a příjmení a třeba ještě město odkud pochází. Propracovanější metoda falešných referencí je ukryta ve vytvoření příslušných e-mailových adres "spokojených zákazníků", takže obchodník může jejich jménem reagovat na dotazy nedůvěřivého návštěvníka.

[2] http://interval.cz/clanky/10-spinavych-triku-internetovych-obchodniku/ 10.10.2007

Pod trikem velikosti obchodu se skrývá stav, kdy obchodník si vymyslí některé (až všechny) své zaměstnance. Pro větší důvěryhodnost jim zřídí firemní e-mailové adresy. Odpovídání na případné dotazy je také jednoduché. Emaily se mohou přesměrovat na běžně používanou e-mailovou adresu a i z té se dá odpovídat jakoby z každé adresy zvlášť. Na tomto principu se dá vytvořit celý tým.

Manipulovat se zákazníky výše popsanými způsoby není těžké. Další manipulace už probíhá na „profesionální“ úrovni, kde je potřeba vyšší znalost programování. Kam až tyto hrátky mohou dojít?

Oživujícím prvkem webových obchodů bývá anketa, ve které necháte návštěvníky o něčem hlasovat. Většina obchodníků se snaží mít na svých stránkách tématické ankety, které jdou ruku v ruce s cílem podnikání. Není problémem, aby obchodník mírně poupravil zdrojový kód ankety a k otázce, kterou chce zviditelnit, přiřadil přičítání od určité hodnoty. Co to udělá s vnímáním zákazníka, když si přečte, že většina uživatelů přikládá vyšší důraz na rychlé dodání zboží na úkor nižší ceny, je snadno předvídatelné.

Postup s nekalými dodacími lhůtami může vypadat následovně: Obchodník u většiny svého sortimentu poskytne uživateli informaci o dostupnosti zboží, kterou ve skutečnosti nemůže garantovat. Spoléhá se na to, že jakmile si zákazník něco objedná, může si obchodník vymyslet cokoli věrohodného, jen aby udržel zákazníka a dodal mu zboží v obvyklých (tedy obvyklých pro obchodníka) expedičních termínech. Pro zvýšení motivace a jako projev "soucítění s klientem" může obchodník poskytnout určitou slevu za "zpoždění" dodání. Ve většině případů je opět obchodník vítězem, neboť předem počítá s tímto typem zvýhodnění a zanese ho do ceny zboží, které nabízí.

Nekalý postup v podobě zaslání jiného nebo žádného zboží je jasný. Zákazník dostane zboží, které nečeká nebo které nechce. Bojovat proti tomuto je těžké, protože poškozený musí dokázat, že v balíčku bylo v lepším případě něco jiného.

V matení při číslování dokladů se nejedná o přímé ohrožení klienta, ale sděluje se zde nepravdivá informace. Pokud to obchodníkovi projde u finančního úřadu, mění si svoje číselné řady a zákazníkovi je tedy podsouvána informace, že před ním bylo mnohem více zákazníku, než je pravda.

Mezi netradiční špinavé triky lze zařadit i časté úpravy reklamačních řádů a jiných dokumentů, které upravují vztah mezi obchodníkem a zákazníkem. Následně je už snadné "nachytat" zákazníka na nějaké nepřesnosti nebo špatně sdělenou formulaci.

1.7. Riziko hackerských útoků

Díky stále vynalézavějším hackerům a internetovým podvodníkům mohou být ohroženy nejen osobní údaje, ale i platební prostředky nakupujícího. Pokud se například rozhodneme, že zaplatíme za zboží platbou z embosované platební

karty, zadáme kód z karty, její číslo a datum exspirace. V případě krádeže karty se můžeme bránit tak, že kartu necháme zablokovat, ale peníze nám z ní mohou odtékat, aniž by nám ji kdokoliv fyzicky odcizil. Existují různé stopovací programy, tzv. keyreadery, které čtou všechny klávesy, které při práci s počítačem stiskneme. Hrozí tedy např. to, že se nám někdo tímto způsobem naboural do internetového bankovnictví – bude-li znát přístupové číslo/kód a heslo, může ho zastavit jen mnohanásobné ověření platby (např. potvrzení platby kódem z sms zprávy). Hrozí bohužel ale i to, že si na nás někdo počká ve svém e-obchodě, nechá nás provést platbu kartou přes internet, údaje si schová a z naší karty může stejným způsobem utrácet jinde (a přitom může být z jiného kontinentu).

2.1 Legislativa

V současné době není elektronický obchod jako takový upraven žádnou právní normou. Některé předpisy sice s obchodním stykem v elektronické podobě počítají - např. obchodní zákoník, zákon o elektronickém podpisu - ucelená norma, která by upravovala na jednom místě práva a povinnosti spojené s elektronických obchodem, zatím ale chybí.

Samotná právní podstata Internetu je komplikovaná. 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.

K zajištění náležité ochrany subjektivních práv a zákonem chráněných zájmů by ve většině případů mělo postačit důsledné aplikování stávajících právních předpisů. Problémem je bohužel dosud chybějící judikatura soudů, která by pomohla stanovit standardizované řešení na Internetu vznikajících modelových situací.

Mezi nejdůležitější právní normy, které oblast elektronického obchodu přímo v některé jeho části upravují nebo které se elektronického obchodu dotýkají nepřímo, patří především

- Zákon o elektronickém podpisu, č. 227/2000 Sb.
- Právní normy o ochraně osobních údajů č. 256/1992 Sb.
- Právní normy upravující duševní vlastnictví
    - Autorský zákon č. 121/2000 Sb.
    - Patentový zákon č. 527/1990 Sb.

2.1.1 Zákon o elektronickém podpisu, č. 227/2000 Sb.[3]

[3]Zdroj: http://www.businessinfo.cz/cz/clanek/zakony/zakon-o-elektronickem-podpisu/1001184/4763/ 14.10.2007

Souvisí s ním Nařízení vlády č. 304/2001 a Vyhláška č. 366/2001, upravuje používání elektronického podpisu, poskytování souvisejících služeb, kontrolu stanovených povinností a sankce. Elektronický podpis jsou obecně údaje v elektronické podobě, které jsou připojené k datové zprávě a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě. Zákon definuje např.: soulad s originálem, povinnosti podepisující osoby a poskytovatele certifikačních služeb, odpovědnost za škodu, způsob akreditace a dozoru, podmínky udělení akreditace a další.

Platí, že pravidla „kamenného" a elektronického obchodování jsou stejná. Pokud bude někdo například podnikat bez příslušného živnostenského oprávnění, dopustí se neoprávněného podnikání bez ohledu na to, že jde pouze o internetový obchod.

Pro smlouvy uzavřené za pomoci zaručeného elektronického podpisu platí tentýž právní režim jako pro klasicky uzavřené smlouvy. Tyto obchodní vztahy se řídí obchodním zákoníkem. Co se týče mezinárodního obchodu, pak právní řád, kterým se bude smluvní vztah řídit, stanoví mezinárodní právo soukromé, popř. dohoda účastníků.

Komise OSN pro mezinárodní obchodní právo (UNCITRAL) připravila tzv. modelový zákon o elektronickém obchodu. Tento modelový zákon není závaznou právní normou, strany smlouvy ovšem v této smlouvě mohou sjednat, že pro ně závazný bude.[4]

2.1.2. Směrnice *Evropské Rady a Evropského parlamentu 2000/31/*ES *o některých právních aspektech služeb informační společnosti*

Vlastní právní úpravu elektronického obchodu má i Evropská Unie. Například pokud jde o tzv. služby informační společnosti (telefonní linky, video on demand, Internetová telefonie atd.), tyto se odlišují od klasických služeb tím, že se u nich částečně stírá rozdíl mezi domácím a mezinárodním poskytováním a jejich faktický příjem nezávisí na skutečném sídle. Pokud by každý stát Evropské Unie reguloval poskytování tohoto typu služeb rozdílně, docházelo by k vzájemné nekompatibilitě právních úprav, což by omezilo rozvoj tohoto odvětví. Proto se Evropská Komise již v roce 2000 rozhodla *směrnicí Evropské Rady a Evropského parlamentu* ***2000/31/ES*** *o některých právních aspektech služeb informační společnosti* alespoň částečně sjednotit regulační rámec pro poskytování služeb informační společnosti. Takzvaná směrnice o e-commerce byla do českého zákonu přenesena zákonem 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů.

Podstatou směrnice jsou ustanovení, která omezují členské státy v jejich pravomoci nepřiměřeně regulovat poskytování služeb informační společnosti.

---

[4] Zdroj: http://www.businessinfo.cz/cz/clanek/elektronicky-obchod/elektronicky-obchod/1000819/7013/ 10.10.2007

Směrnice ale neřeší soukromoprávní záležitosti, například neřeší vztah mezi poskytovatelem služby a jejím příjemcem. Ve vztahu poskytovatel a příjemce se pouze omezuje na informační povinnost poskytovatele a reguluje určité požadavky na vyžádaná a nevyžádaná obchodní sdělení.

Směrnice konkrétně zavádí:

1. Princip země původu v oblasti poskytování sužeb informační společnosti
2. Požadavky na povolovací režim poskytovatelů služeb informační společnosti
3. Právní úpravu obchodních sdělení
4. Nakládání se smlouvami uzavíranými elektronickou cestou
5. Odpovědnost poskytovatelů zprostředkovatelských služeb
6. Obecnou informační povinnost poskytovatelů služeb informační společnosti [5]

3.1 Možná opatření

Ze strany obchodníka

Nejdůležitější je být opatrný a připravený. Rizika samozřejmě číhají nejen na spotřebitele, ale i na obchodníky.

Existuje plno „internetových výtržníků/vtipálků“, kteří mohou díky anonymitě bezstarostně připravovat ostatní o peníze či jim zvyšovat náklady. Je to prosté, stačí např. zadat jinou adresu a nechat si zboží zaslat na dobírku. V závislosti na „zákeřnosti výtržníka“ zboží doputuje třetí osobě, která si nic nekoupila a nebo zadaný adresát neexistuje. Zásilka čeká na poště či u speditéra a po uplynutí jisté lhůty se vrací zpět obchodníkovi. Vznikají mu tak náklady – již zaplatil za expedici – a ušel mu zisk z prodaného zboží – které již mohl prodat někomu jinému. Zde bohužel nenajdeme konkrétní opatření, která by těmto situacím zabránila. Někteří obchodníci se proto snaží zboží zasílat až po platbě na účet (toto je také zohledněno v ceně za dopravu, která je samozřejmě nižší než u platby na dobírku).

Proti nekalým praktikám konkurentů, providerů a také zákazníků je možné se bránit pojištěním IT/IS. Na českém trhu je nabízeno například pojištění pro organizace, které se chtějí prezentovat na Internetu a kromě toho také chtějí realizovat touto cestou obchodní či jinou činnost. Zatím není rozšířené, ale pojišťovny již mají přesné požadavky: audity a bezpečnostní prověrky, tři kategorie rizikovosti. Když si nenecháte udělat jednou ročně bezpečnostní audit či rychle neodstraníte chyby při něm nalezené, jednoduše vám pojistku zruší. Cílovou skupinu pojištění IT/IS rizik tvoří tedy všechny organizace vystupující na

---

[5] Zdroj: http://www.mpo.cz/zprava34954.html 10.10.2007

Internetu. Jediné omezení může být takové (v případě českého pojišťovacího subjektu), že server, na němž je umístěna domovská stránka nebo další software pro realizaci obchodu (např. webshop apod.), musí být provozován na území České republiky. Pro účely pojištění jsou potenciální zájemci rozděleni do tří rizikových skupin na

- uživatele prezentace na Internetu umístěné na serveru externího poskytovatele
- organizace nabízející elektronické obchodování, jehož webové stránky jsou provozovány v České republice na serveru jiným poskytovatelem
- provozovatele vlastního web serveru[6]

Ze strany spotřebitele

Platí zde totéž co pro obchodníky – být opatrný a připravený. Existuje mnoho rad, co všechno musí návštěvník (a potažmo budoucí zákazník) internetového obchodu prověřit, než učiní v e-obchodu objednávku a poté za ni i zaplatí.

Zde jsou návrhy jednotlivých opatření:

- každá informace musí být ověřitelná – například zadání sídla obchodníka do mapového vyhledávače vyhledá skutečné fyzické místo na mapě (pokud existuje)
- zjistit, zdali provozovatel e-obchodu vlastní IČ, DIČ včetně příslušného oprávnění pro podnikání
- ověřit si reference od spokojených zákazníků
- zjistit ve kterých sdruženích na ochranu spotřebitele je e-obchod registrován
- zjistit zdali je e-obchod certifikován a je-li jeho certifikát v platnosti
- nespoléhat se na zprávy o dostupnosti zboží, kdy obchodník např. uvádí, že zboží je očekáváno do jistého data, velmi často se toto několikrát za sebou prodlužuje
- u dobírky si ověřit, že požadovaná částka souhlasí s částkou uvedenou v elektronické smlouvě
- pečlivě si pročíst podmínky ve smlouvě, podmínky dodání, reklamační řád a další důležité dokumenty
- věnovat pozornost tomu, co zaklikáváme (obrana proti nevyžádané poště apod.) a s čím vším souhlasíme
- prozrazovat na sebe jen to, co skutečně chceme internetovým obchodníkům odhalit[2]

[6] Zdroj: http://www.lupa.cz/clanky/koncepce-pojisteni-e-obchodu-z-pohledu-eliminace-pojistovanych-rizik/ 10.10.2007

Přílohy:

1. *S*měrnice Evropské Rady a Evropského parlamentu **2000/31/ES** o některých právních aspektech služeb informační společnosti[4]
2. Povinná certifikační pravidla dle APEK
3. Seznam certifikovaných obchodů dle APEK

Příloha č. 1: *S*měrnice Evropské Rady a Evropského parlamentu **2000/31/ES** o některých právních aspektech služeb informační společnosti

ad1) **Princip země původu** ve směrnici o službách informační společnosti znamená, že členský stát nemůže na základě svého vlastního právního řádu omezovat poskytování služeb informační společnosti z jiného členského státu. Směrnice tak například zabraňuje tomu, aby členský stát omezoval poskytovatele Internetových služeb (například služby video on demand) a blokoval na svém území jeho Internetové stránky pouze z toho důvodu, že "své" poskytovatele tohoto typu služeb omezuje, nebo poskytování tohoto typu služby přímo zakazuje. Pokud poskytovatel tohoto typu služby může legálně poskytovat tuto službu na území svého státu, může ji tedy automaticky nabízet i příjemcům z jiných států. Z tohoto pravidla existuje výjimka pouze v případě naléhavého obecného zájmu, který umožňuje, aby stát příjemce služby takovou službu omezil (např. zablokoval Internetové stránky). Naléhavý důvod obecného zájmu je však poměrně striktně definován a členské státy tak pod tento pojem nemohou v žádném případě libovolně podřadit jakýkoli požadavek jejich právního řádu.

ad2) **Požadavky na povolovací režimy** v oblasti poskytování služeb informační společnosti jsou poměrně stručně shrnuty v jednom ustanovení směrnice a obnáší zákaz vyžadovat po poskytovateli služeb informační společnosti předchozí povolení a také jakýkoli jiný požadavek se stejným účinkem. Z toho zákazu jsou však vyloučena ta povolení, která se netýkají zvláště a výhradně služeb informační povinnosti. To znamená, že povolení k výkonu služby určitého typu obecně mohou členské státy vyžadovat (např. povolení architekta k výkonu jeho profese) nemohou však již vyžadovat další povolení, pokud se poskytovatel rozhodne jím nabízenou službu poskytovat také elektronickou formou (například pokud architekt začne nabízet zhotovení architektonických plánů přes webový portál).

ad3) **Úprava obchodních sdělení a nevyžádaných obchodních sdělení** (tzv. spam) se ve směrnici o některých službách informační společnosti soustředí na definování požadavků, které musí poskytovatel služby informační společnosti ve vztahu k obchodnímu sdělení splnit. Jedná se především o kvalitativní požadavky na to, jak má obchodní sdělení vypadat (jasně rozeznatelné, že jde o obchodní

sdělení, jasně rozeznatelný příjemce atd.). Směrnice však definuje také požadavky na nevyžádaná obchodní sdělení, pokud je členské státy vůbec povolují, což je ponecháno na vůli každého státu. Český transpoziční zákon nevyžádaná obchodní sdělení dovoluje pouze v případě, že jejich příjemce dal s příjmem těchto sdělení předchozí souhlas, že jsou všechna nevyžádaná obchodní sdělení takto označena a že příjemce má možnost jednoduchým způsobem, zdarma a kdykoli odmítnout souhlas s příjmem dalších nevyžádaných obchodních sdělení.

ad4) Směrnice o službách informační společnosti zavazuje také členské státy umožnit ve svém právním řadu **elektronické uzavírání soukromoprávních smluv**. Tato povinnost je stanovena bez dalšího definování detailní úpravy pouze s tím, že připouští výjimku v několika případech smluv specifického charakteru, které budou moci být nadále uzavírány pouze písemně. Jedná se o smlouvy zakládající práva k nemovitostem, smlouvy vyžadující zásah orgánů státní moci, smlouvy o zárukách a jistotách a smlouvy v oblasti rodinného či dědického práva. Jak již bylo řečeno, směrnice pouze ukládá členským státům závazek umožnit tento typ uzavírání smluv, vlastní splnění této povinnosti (konkrétní právní úpravu) pak již může členský stát specifikovat sám.

ad5) Směrnice také přináší **limitaci odpovědnosti poskytovatelů zprostředkovatelských služeb informační společnosti.** Jedná se především o odpovědnost providerů, provozovatelů datových úložišť a portálů atd. Tito obecně neodpovídají za informace s nimiž pracují v případě, že sami do procesu poskytování služby aktivně nezasahují (informaci nemění, nevolí příjemce informace, nejsou účinně seznámeni s protiprávní povahou informací atd.) a pokud se tak stane, účinně jednají s cílem tyto informace odstranit nebo k nim znemožnit přístup. Navíc, členské státy nemohou uložit poskytovatelům tohoto typu služeb obecnou povinnost dohledu. To znamená, že např. poskytovatelé služeb datového úložiště (slovy směrnice; služba spočívající v ukládání informací) nemusí z vlastního podnětu zkoumat povahu informací, které uchovávají, ale musí se touto povahou zabývat až v okamžiku, kdy jsou s ní účinně seznámeni (např. jiným uživatelem služby). Členské státy však mohou uložit poskytovatelům tohoto typu služeb povinnost okamžitě informovat orgány veřejné moci o pravděpodobných protiprávních činnostech nebo informacích, které poskytují.

ad6) **Obecná informační povinnost** zavazuje členské státy vyžadovat na poskytovatelích služeb, aby před, po i v průběhu poskytování služby příjemci sdělili řadu informací o službě, stejně tak jako o poskytovateli samotném. Tato informační povinnost nenahrazuje, ale pouze doplňuje informační povinnosti, které mají poskytovatelé vůči příjemcům služby obecně i v případě, se nejedná o službu informační společnosti (např. na základě zákona o ochraně spotřebitele).

Příloha č.2: Povinná certifikační pravidla dle APEK

(Pokud chce e-obchod získat certifikace od APEK, musí splňovat následující podmínky)[7]

I. Zveřejnění základních údajů o provozovateli

Přímo z titulní stránky obchodu musí vést viditelný odkaz na stránku obsahující základní údaje:

1. kdo je prodávající (tj. partner pro obchodní smlouvu se zákazníkem); jméno firmy s korespondenční adresou, kontaktní osoba, telefon, fax, email, IČO/DIČ
2. reklamační řád prodejny; zejména musí obsahovat:
    1. jak má zákazník postupovat, chce-li zboží reklamovat,
    2. jaké jsou záruční doby zboží (v případě, že se odchylují od zákonné lhůty),
    3. u potravinářského zboží označení trvanlivosti zboží,
    4. na co se záruka vztahuje, popřípadě nevztahuje,
    5. kdo reklamaci vyřizuje včetně plné korespondenční adresy, telefonického a faxového kontaktu.
3. popis, jakým je objednávka vyřizována (zejména komunikace se zákazníkem)

II. Styk se zákazníkem - nákupní řád

Rovněž z titulní stránky obchodu musí vést viditelný odkaz na stránku obsahující následující údaje:

1. nákupní řád obsahující zejména: závaznost objednávek (zda je učiněná objednávka závazná či ne), jak je zákazník o učiněné objednávce informován (preferované je potvrzení emailem),
2. způsoby a doby dodávky (doba do předání zboží dodávací službě s uvedením termínu, který tato služba zaručuje),
3. standardní metody plateb, standardní výše poštovného a balného, popřípadě jakýchkoli dalších poplatků.

Zákazník musí mít možnost se s těmito údaji seznámit, než začne provádět své nákupy.

III. Realizace dodávky, platby, poštovné a balné

Obchod musí obsahovat:

1. jasné platební podmínky včetně poštovného a balného, vyčíslené před okamžikem schválení platby. Zákazník musí mít možnost schválení (či odmítnutí) koupě v okamžiku, kdy ví:

---

[7] Zdroj:http://www.lupa.cz/clanky/certifikace-elektronickych-obchodu-8211-krok-spravnym-smerem/ 11.10.2007

1. co přesně kupuje
2. jakou částku zaplatí včetně poštovného, balného, kurýrní dopravy atd.,
3. zásilka zboží musí obsahovat daňové doklady definované platnými právními předpisy a záruční list na zboží, které je servisováno třetí stranou.
4. Prodejce, pokud je plátcem DPH, je povinen na požádání zákazníka dodatečně zaslat i daňový doklad. O této skutečnosti musí být zákazník předem informován v nákupním řádu internetového obchodního domu,
5. kdy bude zboží expedováno, případně předběžný termín dle dodacích podmínek.

2. vyřešení storna ze strany obchodu, tj. odmítnutí objednávky obchodem, a způsob vrácení peněz u platby předem u tohoto případu, pokud obchod není schopen dodat zboží, nebo jej není schopen dodat zčásti,
3. definování servisních podmínek u zboží, na které se to vztahuje (počítače, audio/video atd.)

IV. Ochrana osobních údajů

Obchod musí odkazem z titulní strany deklarovat, jak bude zacházet se svěřenými osobními daty při personalizaci (jejich předávání či prodávání dál atd.).

Příloha č.3: Seznam certifikovaných obchodů dle APEK

Jméno	Datum certifikace	Datum poslední kontroly
Vltava	08.11.99	12.09.2003
Enc	09.11.99	12.09.2003
Spotřebák	26.11.99	12.09.2003
Cybex.cz	12.12.99	16.10.2003
Obchodní dům	24.01.2000	12.09.2003
Kosmas	25.01.2000	12.09.2003

Paměti	01.03.2000	12.09.2003
Korunka	22.03.2000	12.09.2003
Faxy	21.06.2000	12.09.2003
Filmcity	23.06.2000	12.09.2003
Officesystem	05.07.2000	12.09.2003
Český porcelán	05.08.2000	12.09.2003
BORA.cz	21.08.2000	16.10.2003
Sedin	31.08.2000	12.09.2003
Ticketpro	19.09.2000	12.09.2003
PC Online.cz	24.10.2000	12.09.2003
Omegashop.cz	12.11.2000	12.09.2003
Ben Car	29.11.2000	12.09.2003
MAXShop	16.03.2001	12.09.2003
iStore	28.06.2001	28.06.2003
Zverinec.cz	21.09.2001	21.06.2003
c-shop	01.11.2001	01.08.2003
e-store	11.12.2001	11.09.2003
Showpark	25.01.2002	25.10.2003
Rumburak.cz	08.03.2002	08.09.2003

TiVis	22.03.2002	22.09.2003
MShop.cz	29.05.2002	28.08.2003
BILEZBOZI.CZ	10.07.2002	10.10.2003
Všechny knihy.cz	19.08.2002	19.08.2003
SkvelyObraz.cz	05.11.2002	05.08.2003
AudioVideo.cz	15.11.2002	15.08.2003
PCmegastore	03.12.2002	03.09.2003
BaTom.cz	14.12.2002	14.08.2003
AAAmobil	11.02.2003	11.08.2003
d-shop.cz	06.03.2003	06.09.2003
Stahuj.cz	15.04.2003	15.07.2003
HiFiShop	28.05.2003	28.08.2003
DesignDesign	26.08.2003	
1M.cz	02.09.2003	

Zdroj:http://www.lupa.cz/clanky/certifikace-elektronickych-obchodu-8211-krok-spravnym-smerem/ (11.10.2007)