ELEKTRONICKÉ BANKOVNICTVÍ A JEHO BEZPEČNOST

Gabriela Oškrdalová

ANOTACE

Předmětem příspěvku „Elektronické bankovnictví a jeho bezpečnost“ je analýza elektronického bankovnictví a jeho bezpečnosti. Příspěvek tak pojednává o aktuálním vývoji elektronického bankovnictví, jeho výhodách, nevýhodách a bezpečnosti.

KLÍČOVÁ SLOVA

Elektronická komerce, elektronické bankovnictví, bezpečnost, riziko, bezpečnostní rizika

ÚVOD

E-svět, žijeme v něm a ani si to možná neuvědomujeme. I když není spojen pouze s internetem, je právě internet asi jednou z nejčastějších věcí, které nás v souvislosti s elektronickým světem (e-světem) napadnou. Možná je to i tím, že pokud dnes máme připojení k internetu, nemusíme již v podstatě ani opouštět dům. V pohodlí domova můžeme vyřizovat poštu, telefonovat, pracovat, nakupovat, studovat, obchodovat, podávat daňová přiznání...

CÍL A METODIKA

Cílem příspěvku je analýza elektronického bankovnictví a jeho bezpečnosti. Stanoveného cíle je dosaženo pomocí obecně-vědních metod, především analýzy, deskripce, komparace, syntézy, indukce a dedukce. V práci je použita pozitivistická i normativní metodologie.

VÝSLEDKY

Ve vyspělých zemích dnes internet používá zřejmě každý člověk, který jej používat chce. V USA je to 70 % dospělých, ve Velké Británii přes 60 %, v Evropské unii 43 %. V České republice, podle údajů Českého statistického úřadu, používalo v roce 2005 internet 36 % dospělé populace[1].[2] Počet uživatelů internetu navíc celosvětově každoročně roste, stejně jako počet lidí, kteří ho považují za nedílnou součást svého života.

Velkou pozornost veřejnosti upoutalo v posledních letech elektronické obchodování (e-komerce). Začalo prodejem knih, hudebnin, hraček, elektroniky, cenných papírů, pojištění a letenek a brzy se rozšířilo o prodej nábytku a velkých domácích spotřebičů, o nabídku domácího bankovnictví, objednávek potravin s donáškou až do domu, poradenských a dalších služeb.[3]

Elektronické bankovnictví se dnes již těší značné oblibě nejen ve světě, ale i v České republice. Jeho obliba nepochybně souvisí s výhodami, které přináší zúčastněným subjektům. Mezi nejčastěji zmiňované výhody elektronického bankovnictví z pohledu klientů bank, kteří využívají služeb elektronického bankovnictví, patří především výrazná úsporu času, nižší

[1] Pokud se podíváme na celou populaci, tak podle Internet World Stats je v České republice 5,1 mil. uživatelů internetu, tzn. 49,9 % populace. (PILÍK, M. Žijeme v E-světě. Dostupné na WWW: <http://www.marketingovenoviny.cz/index.php3?Action=View&ARTICLE_ID=4640>)

[2] Trendy v telekomunikačním průmyslu v roce 2007. Dostupné na WWW: <http://www.marketingovenoviny.cz/index.php3?Action=View&ARTICLE_ID=4878>.

[3] KOTLER, P. Marketing od A do Z : Osmdesát pojmů, které by měl znát každý manažer. 2003, s. 45.

ceny, možnost využívat tyto služby odkudkoliv a celých 24 hodin denně 7 dní v týdnu, pohodlí, diskrétnost a komplexnost nabízených služeb. Pro banky pak elektronické bankovnictví znamená především nulovou chybovost při zpracování transakcí klientů, možnost omezit výši celkových nákladů z důvodu nižších transakčních nákladů na provádění platebního styku a z důvodu určité úspory pracovních sil ve front-office a back-office, možnost zvýšit efektivnost bankovní činnosti, posílit svoji konkurenceschopnost, zvýšit svůj tržní podíl a kvalitu poskytovaných služeb.

Z různých výzkumů veřejného mínění vyplývá, že některé občany odrazuje od používání produktů elektronického bankovnictví značná nedůvěra v zajištění bezpečnosti těchto transakcí. A nelze přitom bohužel říci, že by tyto obavy byly vždy neoprávněné. Vždyť i na straně bank se sem tam objeví některé problémy s bezpečností, které by asi většina z nás ani nečekala[4].

Bezpečnost, kvalita a důvěra jsou přitom v e-světě klíčovými pojmy. Jsou předpokladem úspěchu elektronického bankovnictví a jeho produktů, ale i elektronické komerce jako celku. Jejich narušení může mít dalekosáhlé důsledky nejen na danou banku nabízející produkty elektronického bankovnictví, ale i na vývoj celého elektronického bankovnictví, resp. celé elektronické komerce.[5]

Bezpečnost elektronického obchodu a elektronického bankovnictví a její zajištění je projednávána i v orgánech Evropské unie. Z poslední doby lze zmínit např. iniciativu europoslankyně Zuzany Roithové, která hodlá prosadit, aby Evropská komise vydala Evropskou chartu práv uživatele v digitálním prostředí, která by měla přispět ke zvýšení kvality on-line komunikací a ke zvýšení spolehlivosti a bezpečnosti internetových obchodů.[6]

Do elektronického bankovnictví patří platební karty a různé systémy elektronické komunikace klienta s bankou, které umožňují přímé provádění vybraných operací, tzn. bez fyzické přítomnosti klienta na pobočce banky. Elektronické bankovnictví tak zahrnuje takové produkty jako je telefonické bankovnictví, GSM banking, WAP banking, PDA banking, internetové bankovnictví a homebanking. V budoucnu k těmto produktům bude možná patřit i komunikace s bankou prostřednictvím digitální televize.[7] Již samo vymezení elektronického bankovnictví naznačuje, že se jedná o značně různorodou skupinu produktů, které se liší nejen používanými technickými a softwarovými prostředky, ale i různou úrovní a způsobem zabezpečení, resp. výší podstupovaných bezpečnostních rizik zúčastněných subjektů.

---

[4] Např. v srpnu 2000 si jedna z hlavních clearingových bank ve Velké Británii podkopala důvěru svých klientů v oblasti služeb on-line banking třemi „drobnými“ nehodami. V prvním případě systém banky umožnil uživatelům přístup k bankovním účtům ostatních klientů, v druhém se jeden z uživatelů náhodou dostal k finančním údajům svého souseda a ve třetím neprošla on-line aplikace kontrolou zabezpečení – poté, co se uživatel odhlásil a následně stisknul tlačítko „Zpět“, zjistil, že je stále ještě přihlášen. Média těmto problémům pochopitelně věnovala dostatečnou pozornost a kritika v diskusních skupinách byla velmi silná a vydržela několik týdnů. Tyto nedostatky negativně ovlivnily reputaci on-line služeb nejen této banky, ale celého bankovního sektoru (PHILLIPS, D. *Online public relations.* 2003, s. 41).

[5] Význam důvěry a její vztah k technologiím zabezpečení zkoumali např. Whinston a Zhang. Tvrdí, že existuje rovnováha mezi zabezpečením předávané informace a pověstí důvěryhodnosti, které spoluvytvářejí účinné vztahy, že bezpečnost, kvalita a nejistota patří mezi největší překážky elektronické komerce (PHILLIPS, D. *Online public relations.* 2003, s. 38 – 39).

[6] SOS: V testu uspělo pouze 37 procent internetových obchodů. Dostupné na WWW: <http://mam.ihned.cz/c4-10000125-19753380-100000_d-sos-v-testu-uspelo-pouze-37-procent-internetovych-obchodu>.

[7] SEDLÁČEK, J. *E-komerce : internetový a mobil marketing od A do Z.* 2006, s. 179.

Mezi bezpečnostní rizika platebních karet lze zařadit riziko zneužití karty cizí osobou, riziko zneužití nedoručené karty a riziko padělání karet. Se zneužitím ztracených nebo odcizených karet cizími osobami jsou spojeny největší ztráty vydavatelů. Velmi důležité je v tomto případě, aby držitel karty pravidelně kontroloval, zda ji stále ještě vlastní, a zjistí-li, že ji ztratil nebo že mu byla odcizena, tak o této skutečnosti neprodleně informoval svoji banku. Ta ihned po oznámení provede tzv. stoplistaci karty. Odpovědnost za ztráty způsobené zneužitím odcizené karty nese držitel podle podmínek banky, která kartu vydala. V členských zemích Evropské unie je dnes toto riziko omezeno částkou 150 eur, pokud klient nezpůsobil škodu hrubou nedbalostí nebo spoluúčastí na trestném činu. Jestliže je škoda vyšší, tak zbývající částku hradí vydavatel karty. Ochrana platebních karet před zneužitím cizí osobou je založena na ověřování totožnosti držitele karty, výběry hotovosti jsou u bankomatů vázány na znalost osobního identifikačního kódu PIN a v pobočkách bank a směnárnách na předložení průkazu totožnosti a podepsání účtenky shodně s podpisovým vzorem na kartě. U peněžních transakcí se rovněž vždy provádí autorizace. Při placení zboží a služeb je nejčastěji nutné podepsat prodejní doklad a/nebo zadat správný PIN. Tato opatření významně ztěžují zneužití karty cizí osobou. Novinkou roku 2001 bylo zavedení tzv. zamykání karet pomocí SMS (tuto službu jako první na světě nabídla svým klientům česká eBanka). Další z bezpečnostních rizik platebních karet představuje možnost zneužití nedoručené karty. Většina bank v rozvinutých zemích zasílá platební karty klientům poštou v oddělené zásilce od PINu a některé z těchto karet jsou během přepravy odcizeny a zneužity. Posledním ze zde zmíněných rizik je riziko padělání karet. Toto riziko lze snížit používáním ochranných prvků – hologramu, mikrotextu, ceninového tisku, speciálních podpisových proužků citlivých na chemikálie a gumování. Podstatné snížení tohoto rizika je očekáváno se zavedením čipových karet s programovatelným mikroprocesorem. Celkovou výši škod již dnes snižují speciální detekční systémy bank a platebních systémů, které včas odhalí, že se jedná o padělek.[8] Podstupovaná bezpečnostní rizika jsou v případě platebních karet výrazně snižována používáním primárních a sekundárních ochranných prvků. Mezi primární patří různé identifikační prvky držitele (např. fotografie držitele karty, jeho podpis) a prvky sloužící k snadnému ověření pravosti dokladu (barevnost, hologram, sklopný efekt atd.), které jsou snadno ověřitelné v místě kontroly a které nevyžadují zvláštní vyškolení nebo technická zařízení. Jestliže při primární kontrole vznikne podezření na změnu nebo padělání karty, přichází na řadu sekundární kontrola, která je založena na ověření pravosti pomocí jednoduchých pomůcek (mikrotext, gilošové ozdoby, hologramy, UV barvy aj.) nebo pomocí speciálních zařízení. Ochranu karty zvyšuje používání běžně nedostupného materiálu (speciálně, laboratorně ověřitelné složení), speciálních, obtížně padělatelných znaků a údajů (např. laserová graviatura), zvláštní ochrany dat (šifrování údajů, komerčně nedostupné čipy, speciální operační systémy apod.) a verifikačních prvků, které potvrzují totožnost klienta, který manipuluje s kartou (PIN, otisk prstu aj.).[9]

Bezpečnostní rizika jednotlivých systémů elektronické komunikace klienta s bankou, které umožňují „přímý přístup klienta do banky“, jsou výrazně ovlivněna používanými technickými a softwarovými prostředky. Vzhledem k tomu, že vysvětlení každého systému a jeho bezpečnostních rizik překračuje možnosti této práce, omezím se zde na shrnutí základních principů přispívajících k minimalizaci podstupovaných bezpečnostních rizik.

[8] JUŘÍK, P. *Platební karty : Velká encyklopedie, 1870 – 2006*. 2006, s. 201.
[9] JUŘÍK, P. *Encyklopedie platebních karet : Historie, současnost a budoucnost peněz a platebních karet*. 2003, s. 228.

Pro zajištění bezpečnosti elektronické komunikace klienta a banky, resp. pro minimalizaci bezpečnostních rizik této komunikace je třeba zajistit:

- důvěrnost zpráv – za důvěrnou se považuje zpráva, kterou může číst pouze oprávněná osoba, tj. její příjemce. Bezpečnost přenášených dat dnes všechny banky řeší především pomocí účinného kódování.
- identifikaci banky – klient musí mít naprostou jistotu, že komunikuje se svojí bankou a ne s někým jiným.
- identifikaci klienta – banka musí jednoznačně vědět, s kým skutečně komunikuje a zda je tato osoba oprávněná provádět jednotlivé operace. Z tohoto důvodu jsou vstup do daného systému a provádění jednotlivých bankovních operací podmíněny zadáním správného hesla, uživatelského jména apod. Některé banky dnes nabízí svým klientům různé způsoby jejich identifikace, které ovlivňují nejen výslednou úroveň zabezpečení, ale i „komfort“ uživatele daného systému elektronického bankovnictví. Záleží pak jen a pouze na klientovi, jaký způsob svojí identifikace zvolí a jaká bezpečnostní rizika bude nakonec podstupovat.
- prokazatelnost původu zprávy – klientovi nebo bance lze prokázat, že poslal(a) určitou zprávu. Původ zprávy se v praxi prokazuje obdobným způsobem, jakým probíhá identifikace klienta, resp. banky.

Bezpečnost komunikace mezi klientem a bankou v rámci elektronického bankovnictví je zajišťována pomocí šifrování – data jsou zašifrována odesílatelem a jejich odšifrování by měl být schopen provést pouze příjemce. K šifrování dat se v současné době používají různé techniky a metody. Od nejjednodušších, užívaných při telefonickém bankovnictví, až po technicky značně náročné používanými speciálními komunikačními programy, např. v rámci home bankingu. V rámci těch nejjednodušších technik se používá jméno a heslo, stanovení limitu platby, příp. i zasílání informační SMS na mobilní telefon klienta při každém přihlášení do systému s možností zablokování účtu prostřednictvím telefonu. Vyšší zabezpečení telefonické komunikace lze dosáhnout používáním tří prvků, např. identifikačního čísla IPPID, PINu a hesla. Ještě vyšší zabezpečení je pak možné při používání mobilního telefonu, pomocí kterého se generuje PIN nebo pomocí kterého dochází k přenášení kódových zpráv přímo z aplikace nahrané na SIM toolkitové kartě zabezpečené pomocí BPINu. Nejdokonalejší a technicky nejnáročnější zabezpečení telefonického bankovnictví nabízí PIN kalkulátor (elektronický klíč), který musí mít klient u sebe, pokud chce tuto službu použít. Při komunikaci prostřednictvím speciálních programů se nejčastěji používají tzv. elektronické podpisy (asymetrické šifrovací algoritmy), programy, které jsou založeny na bázi dvou klíčů, tajného a veřejného. Dalším doplněním zabezpečení je využití tzv. hashovací funkce, pomocí které lze vytvořit tzv. otisk zprávy – hash.[10]

Zajištění bezpečnosti, resp. minimalizace bezpečnostních rizik elektronického bankovnictví není jen záležitostí banky, ale i každého klienta používajícího některý z produktů. Klienti by tak měli dodržovat následující zásady:

- používat pouze důvěryhodné služby a vždy se ujistit, že opravdu komunikují s daným poskytovatelem služeb.
- při vstupu do systému a při zadávání pokynů zkontrolovat, zda je spojení řádně zabezpečeno a zda komunikují skutečně se svou bankou.
- chránit své elektronické klíče, hesla, PINy a osobní informace.
- hesla a PINy volit tak, aby nebyly snadno uhádnutelné nebo odvoditelné z informací o jeho osobě.

[10] MÁČE, M. *Platební styk – klasický a elektronický*. 2006, s. 164 – 166.

– pravidelně kontrolovat pohyby na svých účtech a platby platební kartou.
– v případě jakýchkoliv pochybností, nejasností a nesrovnalostí kontaktovat svoji banku.

Zajištění bezpečnosti, resp. minimalizace bezpečnostních rizik elektronického bankovnictví bankou vyžaduje, aby si sama banka a její zaměstnanci uvědomili, že bezpečnost těchto produktů není jen záležitostí počítačových specialistů. Úspěšné řízení bezpečnostních rizik bankou navíc předpokládá přijímání potřebných opatření nejen v oblasti technologické, ale i personální, procesní a fyzické. Kromě výše uvedených opatření lze zmínit používání soustav speciálních softwarových ochranných zdí, resp. speciálních počítačů, které neustále kontrolují komunikaci banky s vnějším světem (jedná se o tzv. firewally), a oddělení rolí správců jednotlivých systémů. Tato opatření mají zabránit proniknutí do banky zvenčí. Jak již bylo uvedeno, je třeba zabránit zneužití systému i zevnitř banky. Jednotliví interní uživatelé by tak měli mít pečlivě nastavena svá přístupová práva, měli by být pravidelně proškolování v otázkách bezpečnosti, prověřováni, při práci se systémem by měla být dodržována zásada „co není dovoleno, je zakázáno“, a to se stejnou důsledností, s jakou je uplatňován princip komisionálnosti, tj. účasti minimálně dvou osob při prováděných operacích. Banka by rovněž měla věnovat dostatečnou pozornost „vzdělávání“ svých klientů v oblasti podstupovaných bezpečnostních rizik a jejich možné minimalizaci z jejich strany.

ZÁVĚR

Elektronické bankovnictví se dnes těší značné oblibě nejen ve světě, ale i v České republice. Bezpečnost, kvalita a důvěra jsou v e-světě klíčovými pojmy. Jsou nutným předpokladem úspěchu elektronického bankovnictví a jeho produktů. Zajištění bezpečnosti je společným cílem klientů, bank i dalších zúčastněných osob (např. internetových obchodů).

LITERATURA

1. APEK: E-commerce v ČR – první pohled zblízka. *APEK* [on-line]. [cit. 26. ledna 2007]. Dostupné na WWW: <http://www.apek.cz/tiskove-informace/tiskove-zpravy/e-commerce-v-cr-prvni-pohled-zblizka>.
2. Český statistický úřad: Informační a komunikační technologie v domácnostech a mezi jednotlivci. *Český statistický úřad* [on-line]. [cit. 31. ledna 2007]. Dostupné na WWW: <http://www.czso.cz/csu/redakce.nsf/i/domacnosti_a_jednotlivci>.
3. JUŘÍK, P.: *Encyklopedie platebních karet : Historie, současnost a budoucnost peněz a platebních karet*. 1. vyd. Praha : Grada Publishing, 2003. 312 s. ISBN 80-247-0685-7.
4. JUŘÍK, P.: *Platební karty : Velká encyklopedie, 1870 – 2006*. 1. vyd. Praha : Grada Publishing, 2006. 296 s. ISBN 80-247-1381-0.
5. KOTLER, P.: *Marketing od A do Z : Osmdesát pojmů, které by měl znát každý manažer*. 1. vyd. Praha : Management Press, 2003. 203 s. ISBN 80-7261-082-1.
6. MÁČE, M.: *Platební styk – klasický a elektronický*. 1. vyd. Praha : Grada Publishing, 2006. 220 s. ISBN 80-247-1725-5.
7. M&M: SOS: V testu uspělo pouze 37 procent internetových obchodů. *M&M* [on-line]. [cit. 2. března 2007]. Dostupné na WWW: <http://mam.ihned.cz/c4-10000125-19753380-100000_d-sos-v-testu-uspelo-pouze-37-procent-internetovych-obchodu>.
8. Marketingové noviny: Trendy v telekomunikačním průmyslu v roce 2007. *Marketingové noviny* [on-line]. [cit. 31. ledna 2007]. Dostupné na WWW: <http://www.marketingovenoviny.cz/index.php3?Action=View&ARTICLE_ID=4878>.
9. PARDUBICKÝ, T., RUCKMAN, M.: Elektronické bankovnictví není tak snadné, jak se zdá. *Virtuální inovační park* [on-line]. [cit. 28. března 2007]. Dostupné na WWW: <http://www.park.cz/elektronicke_bankovictvi_neni_tak_snadne_jak_se_zda/>.

10. PHILLIPS, D.: *Online public relations*. Praha : Grada Publishing, 2003. 216. ISBN 80-247-0368-8.
11. PILÍK, M.: Žijeme v E-světě. *Marketingové noviny* [on-line]. [cit. 31. ledna 2007]. Dostupné na WWW: <http://www.marketingovenoviny.cz/index.php3?Action=View&ARTICLE_ID=4640>.
12. PŘÁDKA, M., KALA, J.: *Elektronické bankovnictví : Rady a tipy*. 1. vyd. Praha : Computer Press, 2000. 166 s. ISBN 80-7226-328-5.

Ing. Gabriela Oškrdalová
Katedra financí ESF MU
Lipová 41a
602 00 Brno
tel.: +420 549495682
oskrdalo@econ.muni.cz