MASARYKOVA UNIVERZITA
Ekonomicko - správní fakulta

Krízový management elektronického bankovnictví

Krízový management v elektronickom obchodovaní a elektronickom bankovníctve

seminárna práca

Vypracovali: Zuzana Fogašová , 137467
Martin Železník, 137762
Seminárna skupina: PFKMEB/4
Dátum: 6.10.2007

Obsah

Úvod

Internet sa stal súčasťou nášho života. Stále viac ľudí ho považuje za každodennú a neoddeliteľnú časť nášho života. Využívame ho nielen ako zdroj informácií ale aj ako pracovný a komunikačný prostriedok. Takisto si väčšina z nás dnes už nevie predstaviť svoj život bez bankového účtu a služieb, ktoré sú s ním spojené. Platobné karty, bankomaty a elektronické bankovníctvo sú súčasťou nášho života. Veľa z nás tieto produkty aktívne alebo pasívne aj využíva a v najbližšom období bude počet ich aktívnych používateľov rásť a ich dostupnosť sa bude zvyšovať. Všetko to súvisí s rozvojom technológií, internetu a rozvojom bezpečnosti takýchto systémov.

Mnohí ľudia, a medzi nimi aj tí čo elektronické bankovníctvo využívajú však nevedia ako systém elektronického bankovníctva funguje a niektorí z nich si takisto vôbec neuvedomujú riziká spojené s využívaním týchto služieb. Preto často ani nevedia ako sa proti prípadným rizikám či nebezpečenstvám môžu brániť, alebo na druhej strane tiež nevedia čo všetko robí banka alebo elektronický obchodník pre ochranu údajov svojich klientov a pre dobré fungovanie takýchto služieb .

Cieľom našej práce je na úvod definovať a popísať niektoré základné pojmy, ktoré sú s touto témou úzko spojené. Ďalej sa budeme zaoberať výhodami a nevýhodami systému elektronického obchodovania a elektronického bankovníctva a v neposlednej rade tiež bezpečnosťou takto prevádzaných obchodov a komunikácie medzi zákazníkom a bankou.

1. Základné pojmy

1.1. Krízové riadenie

Vo všeobecnej terminológii je krízové riadenie (krízový management) slovom, ktoré sa viaže k problematike rozličných nežiaducich (nebezpečných) situácií.

Pôvodne sa jednalo o pojem z oblasti politiky. Prvý krát tento termín spomenul a jeho prvé použitie sa pripisuje prvému americkému prezidentovi G. Washingtonovi. Neskôr sa stalo súčasťou slovníku ďalšieho amerického prezidenta J. F. Kennedyho, ktorý ju dával do súvislosti s kubánskou krízou v roku 1962. Neskôr bol tento termín „crisis management“ prevzatý do terminológie NATO a takmer po celú dobu studenej vojny bol nástrojom pre riešenie rôznych krízových situácii vojenského charakteru, ktoré vznikali medzi NATO

a Varšavskou zmluvou. Nasledujúce politické zmeny a to rozpad bipolárneho sveta, pád železnej opony v Európe a ďalšie zmeny spôsobili, že pojem krízový management opustil na počiatku 90. rokov vojenské chápanie a stal sa univerzálnym pojmom pre pomenovanie procesov spojených so zvládaním krízových situácii prírodného, antropogénneho, sociálne-spoločenského, ekonomického či podnikovo-hospodárskeho charakteru.

V podmienkach našej práce je možno tento termín chápať ako súhrn riadiacich činností príslušných ľudí zameraných na:

- analýzu a vyhodnocovanie rizík
- plánovanie
- organizovanie
- realizáciu
- kontrolu činností

vykonávaných v súvislosti s riešením krízovej situácie.

V širšom poňatí možno tento termín chápať ako proces spojený s riadením rizík, s nasledujúcimi fázami:

- prevencia,
- pripravenosť
- odozva
- obnova.

„Krízové riadenie teda predstavuje **ucelený súbor prístupov, názorov, skúseností, doporučení, metód, opatrení a väzieb, uplatňovaný v hierarchizovanom a funkčne prepojenom systéme vecne príslušných orgánov verejnej správy, právnických a fyzických osôb**, ktorého cieľom je **minimalizovať možnosti vzniku krízy** (formou prevencie a korekcie krízových situácií v spojitosti s účinnou protikrízovou intervenciou) alebo (v prípade, že už kríza nastala) **redukovať rozsah škôd a minimalizovať dobu trvania krízy**. Dôležitou súčasťou krízového riadenia je i **odstraňovanie následkov pôsobenia negatívnych faktorov krízových situácií a obnova systému do nového (vylepšeného) bežného stavu**.“[1]

[1] *Pramen: ANTUŠÁK, K., KOPECKÝ, Z.: Úvod do teorie krizového managementu I. 2. vyd. Praha: Vysoká škola ekonomická v Praze, Oeconomica, 2003. 19 str. ISBN 80-245-0548-7*

1.2. Elektronické obchodovanie

Elektronické obchodovanie, e-commerce alebo e-business sú pojmy, s ktorými sa stretávame stále častejšie bez toho aby sme ich vedeli presne definovať. Obyčajný človek by povedal, že je to jedno a to isté, avšak také jednoduché to nie je.

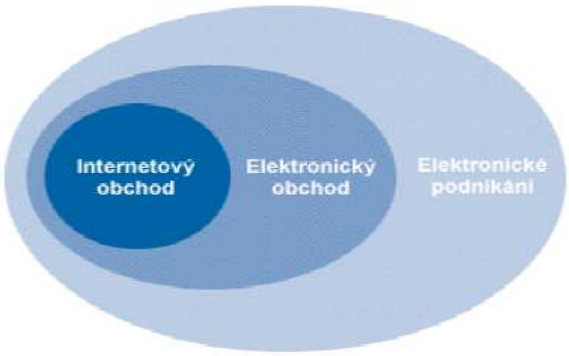
E-commerce je možno definovať ako elektronický marketing alebo obsluhu klientov prostredníctvom počítačových sietí. Iná definícia hovorí o e-commerce ako o prevádzaní obchodnej komunikácie a managementu prostredníctvom elektronických metód ako EDI[2] alebo prostredníctvom automatických systémov zberu dát.

E-business je definovaný ako akýkoľvek informačný systém alebo digitálna aplikácia, ktorá umožňuje prevádzať obchodné procesy. E-business dáva firmám možnosť efektívnejšie a pružnejšie spolupracovať s dodávateľmi a partnermi a tak lepšie uspokojiť potreby a očakávania svojich zákazníkov. E-commerce je teda podmnožinou E-business. Oba tieto pojmy splývajú v našom prostredí do pojmu elektronické obchodovanie.

Elektronické obchodovanie je taká forma obchodných operácii, pri ktorých spolu partneri komunikujú častejšie elektronickou formou než fyzicky. Znamená to teda, že bez fyzického stretnutia prebehnú napr. tieto transakcie a to: výber tovaru, dohodnutie obchodných podmienok, objednávka, prevod peňazí atď. Elektronické obchodovanie je spôsob podnikania využívajúci informačných a komunikačných technológií ako v oblasti riadenia podniku, tak v oblasti spolupráce s partnerskými podnikmi. Pojem elektronický obchod sa nerovná pojmu internetový obchod, ako niekedy nepresne používa. Na elektronický obchod sa totiž okrem internetu využívajú aj iné komunikačné prostriedky.

[2] Electronic Data Interchange - *automatizovaná výmena elektronických dokladov podporujúca elektronickú výmenu štrukturovaných štandardných správ medzi dvoma aplikáciami na nezávislých subjektoch*

Obrázok 1: Schéma vzťahu medzi pojmami elektronické podnikanie, elektronický obchod a internetový obchod



Zdroj: Froulík R., Elektronický obchod – význam, rozdělení a vybrané pojmy. Dostupný na: < http://www.e-studio.cz/dokumenty/elektronicky_obchod.pdf>

Základom pre úspešné využitie tejto technológie v podniku je:

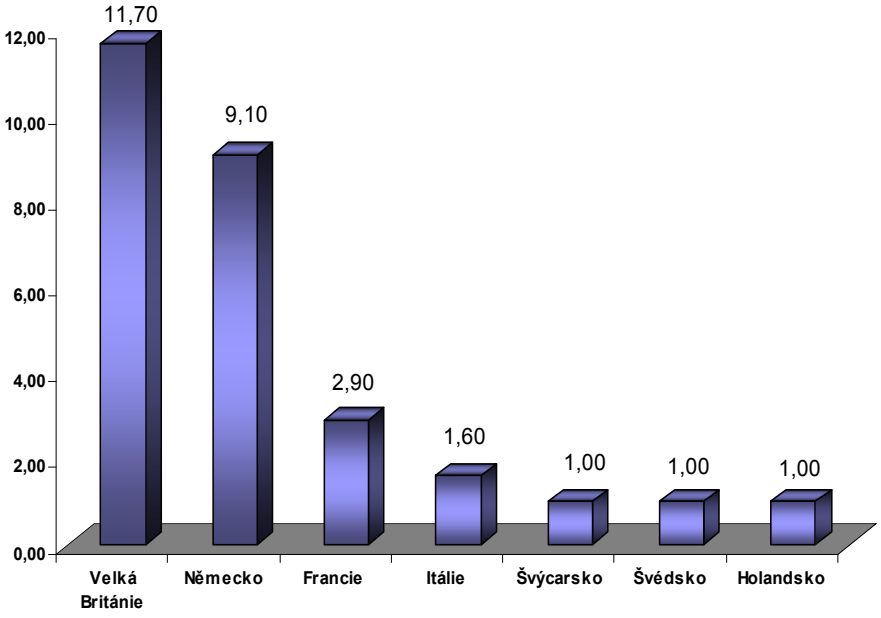
- kvalitná, priechodná, spoľahlivá infraštruktúra lokálnej podnikovej siete zaručujúca bezpečné dátové prenosy
- pripojenie lokálnej siete do vysokorýchlostného internetu
- servery vybavené silným hardwarom s vyhovujúcimi technickými parametrami a vhodným operačným systémom, ktorý garantuje bezpečnosť uložených dát v tomto systéme
- programové vybavenie, ktoré spĺňa funkčné ale aj bezpečnostné požiadavky a poskytujúce zrozumiteľné ale aj pohodlné užívateľské rozhranie
- kvalifikovaný a vyškolený personál, zaisťujúci funkčnosť všetkých vymenovaných zložiek

Pod pojmom elektronické obchodovanie sa väčšinou tiež rozumie predaj či poskytovanie služieb prostredníctvom Internetu. Internet slúži ako prostredie, kde si zákazník objednáva. Tento proces prechádza neustálym vývojom. Vďaka elektronickému obchodu sa zmenší význam veľkosti firmy. Podnikateľsky úspešná môže byť i menšia firma bez väčšieho zázemia (veľký počet zamestnancov, skladu, atď.). Menšie firmy majú naopak väčšiu výhodu vďaka svojej väčšej pružnosti a prispôsobivosti.

Podľa typu týchto zúčastnených strán môžeme v elektronickom podnikaní rozlíšiť niekoľko typov vzájomných vzťahov:

- B2B (Business to Business) – na obidvoch koncoch sú obchodní partneri, ktorí robia medzipodnikové transakcie
- B2C (Business to Customer) – na jednej strane vystupuje zákazník a na druhej strane obchodník alebo poskytovateľ služby
- B2G (Business to Government) – ide o elektronickú komunikáciu s orgánmi verejnej správy
- C2C (Customer to Customer) – elektronický obchod medzi dvoma spotrebiteľmi

Graf 1: Maloobchodné tržby B2C v západnej Európe (v mld. EUR, r. 2003)



Zdroj: eMarketer: Internet, Business & E-commerce Statistics [on-line]. Dostupný na: <http://www.emarketer.com>.

1.2.1. Výhody a nevýhody B2C

Výhody:

- zníženie transakčných nákladov
- zjednodušenie administrácie obchodu
- presná znalosť kupujúceho
- individuálny prístup k zákazníkovi
- možnosť rýchlo a pružne reagovať na požiadavky zákazníka
- optimalizácia výroby a skladu,
- trvalá dostupnosť,
- možnosť využitia B2C portálov,

- lacný a globálny marketing,
- získanie konkurenčnej výhody

Nevýhody:

- jedinou zrejmou nevýhodou tohto druhu obchodovania je bezpečnosť a preto sa jej budeme v ďalšom texte venovať

Na rozvoji elektronického obchodovania sa významnou mierou podpisuje rastúci vplyv techniky a nových technológií na podnikanie a celú ekonomiku. Elektronický obchod by sme potom podľa niektorých ekonómov mohli označiť ako aplikáciu technológií, a teda ako piatu tzv. Kondratevovskú vlnu[3], v obchodnom podnikaní.

1.3. Elektronické bankovníctvo

V súčasnosti sme svedkami rýchleho a razantného zavádzania elektronického styku medzi bankami a ich klientmi, a to nielen tými väčšími v podnikovej sfére, pod názvom homebanking, ale aj s menšími klientmi pomocou internet bankingu, mail bankingu, SMS (GSM) bankingu a telephone bankingu.

1.3.1. Výhody elektronické bankovníctva

Väčšie a kapitálovo silnejšie firmy už nebudú mať toľko výhod, pretože v celosvetovom elektronickom obchodovaní už nebude hrať úlohu fyzická lokácia firmy a to ani v zmysle vzdialenosti od zákazníka a dostupnosti produktov a ani v dôsledku pozitívnej externality a to síce z dobrého umiestnenie firmy v lukratívnych častiach miest. Tento fakt významne určuje a zvyšuje transparentnosť trhu, to znamená, že zákazník má ľahší prístup k informáciám, ale aj o predajcoch toho istého produktu, môže veľmi jednoducho porovnávať ceny, solídnosť firmy a služby, ktoré poskytujú a tak sa odstráni množstvo bariér, ktoré poznáme z „tradičného trhu“. Dôležité je, že sa zvyšuje tlak na konkurenciu, čo okrem iného prinesie zníženie koncových cien produktov a tým sa dostávame k známemu a vítanému stavu „ best service – best price“.

[3] Nikolaj Kondratev, ruský ekonóm, označil za príčinu zmien v ekonomike novou techniku a technológiu. Neskôr boli podľa rozvoja techniky definované štyri Kondratevovské vlny. Obdobie od roku 1990 sa dá definovať ako obdobie informačných a komunikačných technológií. Táto vlna sa niekedy nazýva tiež ako tzv. nová ekonomika.

Tým sa všeobecne zvyšuje informovanosť na obidvoch stranách či už je to na strane kupujúcich alebo predávajúcich a už dnes sa objavujú servery, ktoré poskytujú informácie o neplatičoch, spreneverách a podvodníkoch, čo je veľmi užitočné.

Transparentnosť je ďalej posilňovaná znížením počtu prostredníkov na ceste medzi výrobcom a konečným užívateľom, či už uskutočnený obchod chápeme ako business-to-business alebo business-to-customers. Je jasné, že prvý z dvoch menovaných sa uskutočňuje oveľa častejšie a predstavuje tak niekoľko násobne vyššie obraty .

Náklady na reklamu sú na Internete nižšie a veľké firmy a reťazce tak stratia výhodu, ktorou bola možnosť nechať si vytvoriť veľmi nákladnú reklamnú kampaň, ktorá zaručuje úspech medzi kupujúcimi a menšie firmy si niečo také dovoliť nemohli. Samozrejme je jasné, že do budúcnosti aj reklama na internete bude klásť vysoké nároky na reklamné stratégie a samotné prevedenie reklamy. Niektorí z analytikov elektronického obchodovanie preto odhadujú, že dôjde k určitému prepadu zárobkov v reklamnom priemysle a v priemysle „public relations“[4]. Znamená to teda, že možnosť reklamy bude so vstupom firmy do virtuálneho sveta rozšírená a to v podstatnom merítku, bude prístupnejšia a istým spôsobom špecifická. Spolu s elektronickým obchodovaním sa preto rozvíjajú i metódy a stratégie marketingu v internetovom prostredí.

Pre vstup na elektronický trh netreba tak vysoký kapitál, ako je tomu pri zakladaní porovnateľnej firmy v „tradičnej podobe“. Na druhej strane je treba povedať, že skúsenosti ukazujú, že zavedenie, realizácia a prevádzka profesionálneho a úspešného systému pre elektronické obchodovanie na sieti stojí veľké investície a to nielen finančné, ale i časové a ľudské. Odhady budúceho vývoja elektronického obchodu sú však veľmi optimistické, pretože náklady na vytvorenie systému elektronického obchodu by sa mali skôr či neskôr v nie veľmi veľkom časovom okamžiku vrátiť zriaďovateľovi, pretože zavedenie elektronického obchodovania vytvorí predpoklady pre celý rad ďalších procesov, ktoré zničia tých, ktorí sa do systému nezapoja.

[4] PR - vzťahy k verejnosti

1.3.2. Nevýhody elektronického bankovníctva

Pre prechod na plné využívanie všetkých prostriedkov modernej IT pre elektronické obchodovanie môže byť bariérou skutočnosť, že vo svojej podstate neexistuje overený alebo vyskúšaný model takéhoto systému a zároveň sa väčšina analýz zhoduje v tom, že elektronický trh bude v mnohých svojich charakteristikách odlišný od toho tradičného. Inak povedané, hrozí dosť veľké riziko neúspechu. S tým súvisia tiež otázky vhodného softwaru. Doteraz neboli vytvorené dostatočne silné a výkonné nástroje pre ovládanie jednotlivých činností spojených s elektronickým obchodovaním. Rôzne programové aplikácie samozrejme vznikajú, avšak ich tvorba je chaotická, nekoordinovaná a jedným z hlavných problémov, ktoré zo sebou nesú je ich vzájomná nekompatibilita. Tým sa samozrejme zvyšujú náklady na takýto systém. Na druhú stranu bez rizika a bez experimentovanie nemožno rozbehnúť žiadny podnik a už vôbec nie taký, akým je virtuálne obchodovanie.

Táto vzájomná nekompatibilita však existuje aj v legislatívnom prostredí, napr. rôzne štáty majú napr. rôzne dôchodkové systémy, alebo daňové systémy a veľmi veľa právnych opatrení nie je kompatibilných tak, aby mohol prebiehať globálny obchod.

Okrem obáv zo straty kontroly vlády môže byť celkom reálna obava zo straty národnej identity a to takým spôsobom, že ak by české podniky obchodovali elektronickou cestou, museli by pravdepodobne používať anglický jazyk ako komunikačný jazyk Internetu. To môže byť odradzujúce pre českých zákazníkov avšak na druhej strane môže prilákať aj zahraničných kupujúcich, k tomu sa ešte pridáva aj náročnosť viacjazyčnej komunikácie so zákazníkmi.

Podobne skresľujúce môže byť aj zdanlivá schopnosť systému pre virtuálne obchodovanie vyhovieť konkrétnym požiadavkám jednotlivých konkrétnych zákazníkov, a stým súvisiaca evidencia veľkého množstva informácii o klientoch a s tým súvisiaca možnosť marketingu tzn. ponuky šité priamo na mieru zasielané do poštovej schránky konkrétneho zákazníka, prepojenie niekoľkých firiem a predávanie si zákazníkov. Hrozí nebezpečenstvo straty súkromia. Veľmi ľahko sa tak môže stať, že raz zadané osobné údaje nebude možno viac zmazať iba preto, lebo zákazník nevie, kde sú jeho dáta uložené a kde všade boli zaslané/predané.

Doteraz sa v existujúcich systémoch elektronického obchodovania najviac uplatnil predaj takých komodít, ktoré nepodliehajú skaze a sú atraktívne pre hlavnú časť užívateľov Internetu (software, hardware, knihy či CD). Zdá sa, že ani v budúcnosti s plne rozvinutými systémami elektronického obchodovania nebude možné predávať úplne všetky druhy tovarov a služieb, pretože u niektorých môžu nastať problémy s dodávkou(potraviny) alebo môže existovať iné prekážky, napr. sociálne.

2. Bezpečnosť

Oproti jasným výhodám internetového bankovníctva stoja aj nevýhody a riziká. Takými je aj problematika zabezpečenia v oblasti elektronického bankovníctva, ktorá asi najviac brzdí vývoj v tejto oblasti. Prípadné zneužitie takéhoto systému by mohlo mať za následok stratu dôvery a ochoty klientov nielen pre danú postihnutú banku ale aj pre celé odvetvie a mohlo by to zásadne ovplyvniť jeho ďalší vývoj.

Zabezpečeniu elektronického bankovníctva sa venuje značná pozornosť a preto sa naň môžeme dívať ako na špecifickú oblasť elektronickej komunikácie. Aby sme mohli dané riešenie považovať za bezpečné, musí spĺňať štyri podmienky[5]:

1. Dôvernosť komunikácie

Prenášané dáta sú utajené a prečíta ich len oprávnená osoba. Obvykle je to zaistené pomocou šifrovania, kedy sa obe strany dohodnú na kľúči, pomocou ktorého sa všetka komunikácia šifruje kryptografickým algoritmom. Samotná bezpečnosť potom už závisí len na zvolenom algoritme.

2. Integrita správy

Zaisťuje sa pomocou digitálnych podpisov. K odosielanej správe sa vygeneruje tzv. hash – unikátny zašifrovaný kód, ktorý patrí práve k danej správe a je spolu s ňou aj odosielaný. Príjemca si z hash odšifruje obdržanú správu, porovná ju s pôvodnou správou a zistí či správa nebola cestou pozmenená. Ak sa obe správy zhodujú, tak nedošlo k zmeneniu.

[5] spracované podľa: Bezpečnost internetového bankovnictví: situace a trendy. [cit. 30.9.2007]. Dostupné na WWW:
< http://bankovnictvi.ihned.cz/3-13981880-elektronick%E9+bankovnictv%ED-900000_d-38>

3. Autentizácia

Je ňou overená totožnosť odosielateľa. Poznáme autentizáciu na základe 3 metód. Môže to byť heslo, nejaký predmet či kľúč, alebo biometrické vlastnosti. Pre bezpečný prístup treba použiť aspoň dve z týchto autentizačných metód.

4. Neodmietnuteľná zodpovednosť

Je zaručené, že odosielateľ nebude môcť v budúcnosti poprieť autorstvo danej správy. Zaisťuje sa voľbou vhodnej kryptografickej technológie.

Všetky štyri bezpečnostné požiadavky splňujú len digitálne certifikáty, teda riešenia založené na asymetrickej kryptografii.

2.1. Metódy zabezpečenia elektronického bankovníctva

Záujem užívateľov elektronického bankovníctva o ich súkromie a bezpečnosť ich informácií je vysoký, a je samozrejme aj pochopiteľný, pretože možnosti zneužitia zle zabezpečenej databázy hesiel a iných osobných údajov zákazníkov banky je nespočetne veľa. Práve kvôli tomuto je dôležitým a častým problémom takzvaný identity management. Jedná sa o komplex riadenia a administrácie užívateľských práv jednotlivých osôb, ktoré sú zúčastnené na podnikaní.

Najčastejšie sa v elektronickom bankovníctve používajú tri metódy. Jedná sa o tieto tri spôsoby zabezpečenia[6]:

a) zabezpečenie pomocou hesiel

Je to užívateľsky najjednoduchší spôsob zabezpečenia, no preto aj najmenej bezpečný. Každý kto pozná heslo a použije ho, je považovaný za právoplatného účastníka transakcie. Preto sa táto metóda odporúča využívať len pre pasívny prístup k informáciám. Bezpečnosť hesiel je možné zvýšiť aj tu, a to napríklad kombináciou rôznych identifikačných údajov, ktoré sú požadované od klienta, či požadovanie vždy inej časti hesla. Napriek všetkému nie je táto metóda vyhovujúca a to aj preto, že nespĺňa podmienky integrity správ a neodmietnuteľnej zodpovednosti.

[6] spracované podľa: Bezpečnost internetového bankovnictví: situace a trendy. [cit. 30.9.2007]. Dostupné na WWW:
< http://bankovnictvi.ihned.cz/3-13981880-elektronick%E9+bankovnictv%ED-900000_d-38>

b) zabezpečenie pomocou elektronického kľúča

Elektronické kľúče generujú postupnosti jednorázovo použiteľných autorizačných kódov. V praxi teda klient operáciu vždy potvrdí jednorázovým heslom, ktoré mu vygeneruje takýto elektronický kľúč. Kľúčom je buď nejaký kalkulátor, ktorý generuje kódy alebo môže byť kľúč zavedený aj do PDA či do mobilného telefónu.

Pri tomto zabezpečení je zaistená podmienka autentizácie spolu s identifikáciou klienta, avšak nie je zaručená neodmietnuteľná zodpovednosť.

c) zabezpečenie digitálnym certifikátom

Digitálny certifikát viaže dokopy dva kľúče, ktoré vlastní klient. Je to verejný kľúč, ktorý je k dispozícii komukoľvek a súkromný kľúč, ktorý by mal klient držať v tajnosti pretože určuje identitu osoby, ktorej patrí verejný kľúč. Súkromný kľúč môže byť uložený buď na pevnom disku počítača alebo na špecializovaných pamäťových zariadeniach (disketa, pamäťová karta, USB flash disk), ktoré sa nazývajú tokeny, či na čipovej karte. Kľúče sú neoddeliteľné v tom zmysle, že to čo jeden zašifruje, je možné odšifrovať len druhým z nich. Ich vydávanie majú na starosti certifikačné autority, alebo si častokrát vydávajú certifikáty banky aj samy. Tieto digitálne certifikáty vychádzajú z asymetrickej kryptografie a zaručujú tým všetky štyri požiadavky bezpečnej elektronickej komunikácie medzi bankou a klientom.

2.2. Metódy zabezpečenia v budúcnosti

Nedávno sme mali možnosť zaznamenať pokrok v oblasti autentizácie a to hlavne prechod od jednoduchých hesiel k tzv. silnej autentizácií, ktorý bol z dôvodu zvyšujúceho sa počtu on-line používateľov služieb bánk a iných obchodníkov a zvyšovania nárokov na ich bezpečnosť.

Nastupuje tu dvojfaktorová autentizácia, ktorá je pre obe strany pohodlná, ale čo je hlavnejšie je bezpečnejšia. To znamená, že užívateľ bude používať jediné heslo do viacerých systémov a odpadne mu tak nutnosť pamätať si veľa hesiel.

Veľké nádeje sa vkladajú takisto do biometrických metód. Užívateľ sa jednoznačne identifikuje svojou biologickou vlastnosťou, ktorá je jedinečná. Najčastejšie sa jedná o otlačok prsta, geometriu dlane, očné pozadie, tvar dúhovky, či môže ísť aj o dynamiku podpisu alebo hlas. Ich veľkou výhodou je užívateľská prívetivosť, úplná mobilita a minimálna možnosť zneužitia. K takémuto prístupu však treba širšiu dostupnosť správnych čítacích a porovnávacích zariadení či

softwarov, ich spoľahlivé fungovanie a hlavne ich cenová dostupnosť. Aj napriek týmto počiatočným prekážkam sa však zdá, že vývoj sa bude uberať týmto smerom.

Významným objavom v kryptoanalýze, ktorý má vplyv na zabezpečenie dát je prelomenie hashovacej funkcie MD5 čínskym výskumným tímom. Ten zistil kolízie, pomocou ktorých sa dá vytvoriť správy alebo certifikáty s rovnakým digitálnym odtlačkom. Nepríjemné je, že algoritmu MD5 už nie je úplne spoľahlivý – týka sa to najmä overovania certifikátov. Firmy zaoberajúce sa vydávaním certifikátov však situáciu pozorne sledujú a sú pripravené reagovať.

Jedným z najvážnejších problémov súčasnosti a výzvou na zlepšenie do budúcnosti pre on-line bankovníctvo a obchodovanie všeobecne je tzv. phishing[7]. Phishing je podvod, pri ktorom páchateľ zneužíva legitímne vyzerajúce e-mailové správy od známych bánk a požaduje prostredníctvom nich údaje o osobnom účte a hesle a takto potom zneužíva tieto informácie.

Novým nástupcom phishingu je tzv. pharming čo znamená, že obeť zadá do prehliadača adresu svojej banky, ktorú však trójsky kôň presmeruje inam, a zvyčajne sa jedná o takmer dokonalú kópiu tejto stránky a tak sa útočník môže ľahko dostať k osobným údajom používateľa. Cieľom takýchto útokov sa už stali známe domény ako Google.com, Ebay.de alebo Amazon.com.

Napriek všetkému však dochádza aj k prípadom zneužitia systémov elektronického bankovníctva či elektronického obchodu. Jedným z najrozsiahlejších prípadov zneužitia bol prípad Philipa Cummingsa z New Yorku, ktorý pracoval vo firme Teledata Communications, ktorá mala na starosti správu databáz pre rôzne banky. Mal prístup k množstvu údajov, k osobným, detailom o bankových účtoch a prihlasovacích menách a heslách. Tieto údaje potom podsúval tretím stranám. Škoda, ktorú takto spôsobil sa odhaduje na päťdesiat až sto miliónov dolárov.

[7] Slovo phishing (to phish) ma pôvod v anglickom slove fish (čítajú sa rovnako). Obe znamenajú to isté – loviť, alebo uloviť. Phishing teda znamená niečo ako ‘lov informácií‘.

Záver

Internet si našiel svoje miesto aj v bankovníctve a obchode a stále častejšie používame pojmy ako e-commerce či e-banking alebo e-business. Už nemožno poprieť, že budúcnosť týchto odvetví sa bude uberať práve týmto smerom a bude patriť mobilným zariadeniam, bezdrôtovým technológiám a vysokorýchlostnému internetu.

Elektronické bankovníctvo a elektronický obchod má svoje nesporné výhody, ako sú úspora času či nákladov pre banku, obchod aj klienta, pohodlnosť takýchto transakcií, či prístup 24 hodín denne a 7 dní v týždni no skrýva aj svoje nevýhody a riziká.

Podiel elektronického obchodu na celkovom HDP je však aj tak stále nízky. Môže zato nielen pomerne slabé využívanie internetu a to hlavne v malých a stredných podnikoch, ale aj neznalosť či nízka informovanosť u laickej verejnosti. V Českej republike, takisto ako na Slovensku stále panuje pomerne veľká nedôvera v takéto formy bankovníctva a obchodu a to najmä u strednej a staršej generácie. A to je aj jeden z dôvodov jeho slabšieho využívania.

Dôležitá je takisto aj otázka bezpečnosti, ktorej sme sa venovali aj v našej práci. V minulosti sa vyskytli problémy či zneužitia, no aj vďaka nim sa teraz kladie oveľa väčší dôraz na krízový management a vyvíjajú sa stále nové a bezpečnejšie zabezpečovacie metódy. Aj v budúcnosti môžeme očakávať ich ďalší rozvoj, pri ktorom sa budú klásť stále väčšie nároky na bezpečnosť elektronického obchodovania, ochranu spotrebiteľov ako aj krízové riadenie.

Prílohy

Tabuľka 1 - Počet užívateľov Internetu v EÚ

Krajina	Počet obyvateľov (odhad pre rok 2005)	Počet užívateľov Internetu	Nárast užívateľov (2000-2005)	Penetrácia (percentuálny podiel z počtu obyv.)	% užívateľov z celej EÚ
Rakúsko	8,163,782	4,630,000	120.5 %	56.7 %	2.1 %
Belgicko	10,443,012	5,100,000	155.0 %	48.8 %	2.4 %
Cyprus	950,947	250,000	108.3 %	26.3 %	0.1 %
ČR	***10,230,271***	***3,530,000***	***253.0 %***	***34.5 %***	***1.6 %***
Dánsko	5,411,596	3,720,000	90.8 %	68.7 %	1.7 %
Estónsko	1,344,840	621,000	69.4 %	46.2 %	0.3 %
Fínsko	5,246,920	3,260,000	69.2 %	62.1 %	1.5 %
Francúzsko	60,293,927	24,848,009	192.3 %	41.2 %	11.5 %
Nemecko	82.726,188	46,312,662	93.0 %	56.0 %	21.5 %
Grécko	11,212,468	3,800,000	280.0 %	33.9 %	1.8 %
Maďarsko	10,083,477	3,050,000	326.6 %	30.2 %	1.4 %
Írsko	4,027,303	2,060,000	162.8 %	51.2 %	1.0 %
Taliansko	58,608,565	28,610,000	116.7 %	48.8 %	13.3 %
Lotyšsko	2,306,489	936,000	524.0 %	40.6 %	0.4 %
Litva	3,430,836	695,000	208.9 %	20.3 %	0.3 %
Luxemburg	455,581	170,000	70.0 %	37.3 %	0.1 %
Malta	384,594	120,000	200.0 %	31.2 %	0.1 %
Holandsko	16,316,019	10,806,328	177.1 %	66.2 %	5.0 %
Poľsko	38,133,891	10,600,000	278.6 %	27.8 %	4.9 %
Portugalsko	10,463,170	3,600,000	44.0 %	34.4 %	1.7 %
SR	***5,379,455***	***1,820,000***	***180.0 %***	***33.8 %***	***0.8 %***
Slovinsko	1,956,916	800,000	166.7 %	40.9 %	0.4 %
Španielsko	43,435,136	14,590,180	170.8 %	33.6 %	6.8 %
Švédsko	9,043,990	6,656,716	64.4 %	73.6 %	3.1 %
Veľká Británia	59,889,407	35,179,141	128.4 %	58.7 %	16.3 %
EÚ	**459,938,780**	**215,765,036**	**131.6 %**	**46.9 %**	**100.0**

Prameň: Internet World Stats, dáta k 28.3.2005

Tabuľka 2: Najväčšie prekážky rozvoja elektronického obchodu

Překážky rozvoje e-obchodu	Jihomoravský kraj	Jihočeský kraj	Plzeňský kraj	Královéhradecký kraj	Liberecký kraj	Celkem
Nízká úroveň znalostí o IT	30	30	38	22	20	27
Malé znalosti přínosů e-obchodu	20	19	17	15	23	19
Bezpečnost transakcí a dat	11	15	11	27	18	16
Nedostatečný právní rámec	10	8	6	6	8	8
Technologická nevybavenost	8	8	8	13	12	10
Malý rozsah českého trhu	7	6	10	6	5	7
Problém plateb přes Internet	6	7	4	4	11	7
Malá ochota manažerů	7	6	4	7	3	5
Jiné	1	1	2	0	0	1

Prameň: Eliáš A.,Zelená kniha o elektronickém obchodu, Dostupné na WWW:<http: //vsol.obce.cz/clanek.asp?id=2002103>

Zoznam použitej literatúry

Petrželová, J. (2005): *Bezpečnost v elektronickém bankovnictví v ČR*, diplomová práca, Masarykova Univerzita

Rosecký, M. (2005): *Bezpečnosť elektronického bankovníctva*, diplomová práca, Masarykova Univerzita

Petr., A. (2005): *Možnosti elektronického bankovnictví pro e-commerce*, diplomová práca, Masarykova Univerzita

Dvořáček, A. (2006): *Vybrané otázky elektronického obchodování*

Mejtský, J. (2005): *Elektronické obchodování (e-Commerce)*, bakalárska práca, Masarykova Univerzita

Andrýsová, V., DiS. (2005): *Krizové řízení na úrovni obcí a měst*, bakalárska práca, Masarykova Univerzita

Kozák D, : *Příručka E-Business*. *Hospodářska komora České republiky*, 2007.[online].[cit. 30.9.2007]. Dostupné na WWW:
< http://www.komora.cz/Files/Soubory/P%C5%99%C3%ADru%C4%8Dka_e-Business.pdf>

Froulík R, : *Elektronický obchod – význam, rozdělení a vybrané pojmy*. [online].[Cit. 30.9.2007]. Dostupné na WWW: < http://www.e-studio.cz/dokumenty/elektronicky_obchod.pdf>
Hajník F, : *Bezpečnost internetového bankovnictví: situace a trendy*.[online]. [cit. 5.10.2007]. Dostupné na WWW: < http://bankovnictvi.ihned.cz/3-13981880-elektronick%E9+bankovnictv%ED-900000_d-38>

Eliáš A,: *Zelená kniha o elektronickém obchodu*. [online].[cit. 5.10.2007]. Dostupné na WWW: <http://vsol.obce.cz/clanek.asp?id=2002103>