BURIÁN GÁBOR

AZ INTERNET BANKING KOCKÁZATAI*

A huszadik század végének egyik legjellemzőbb vonása az internet elterjedése. Ennek következtében a minket körülvevő világ is megváltozott. Életünk egyre jobban kötődik e médiához, mely az információkhoz való korlátlan hozzáférésen túl alkalmas a szolgáltatások széles skálájának nyújtására, ezen keresztül új üzletek alapítására. A bankszektorban tapasztalható világméretű verseny fokozódásával lépést kell tartani a technológiai innovációkkal ahhoz, hogy az adott hitelintézmény szolgáltatásai továbbra is vonzóak maradjanak az ügyfeleik szemében, így a bankok is egyre-másra jelennek meg szolgáltatásaikkal a világhálón. A pénzügyi intézményeknek messzemenően elemezniük kekk az internet tulajdonságait, a magában hordozott veszélyeket és kockázatokat ahhoz, hogy az elektronikus felületet valóban előnyükre tudják fordítani.

Az internet banking lendületes növekedésben van, és a tendenciák alapján ez az expanzió még évekig tartani fogja magát. Rendkívül izgalmasnak találom a világháló lehetőségeinek és jövőjének kutatását, így dolgozatom célja az internet banking fejlődéséből származó kockázatok összegyűjtése volt. Elképzelésem szerint egy logikus rendszerbe foglalt egységes áttekintést nyújtok azokról a rizikófaktorokról, melyeket az internet banking generál. Ennek megfelelően megpróbálom feltérképezni és rendszerezni a megváltozott technológiai környezet hatására a stratégiai, üzleti és pénzügyi kockázatokban beálló változásokat. Bízom abban, hogy munkám hozzásegíthet ahhoz, hogy az internet bankinggal kapcsolatos lehetőségek és veszélyek tudatosabbá váljanak az Olvasó számára.

BEVEZETÉS

Dolgozatom az elektronikus banki szolgáltatások közül elsősorban az internet banking népszerűvé válásával foglalkozik. Mivel a köztudatban nem egyértelmű, hogy ez a fogalom mit takar pontosan, ezért fontosnak tartom tisztázni a különbséget az elektronikus kereskedelem alá tartozó kategóriák jelentései között.

Az elektronikus kereskedelem alatt termékek vagy szolgáltatások értékesítését

* Lektorálta: dr. Szabó Kristóf, Raiffeisen Bank Rt., főosztályvezető.

értjük elsősorban az interneten keresztül, de ide tartozónak tekinthetjük a telefonon, telefaxon, televízión vagy más zárt rendszereken keresztül folyó elektronikus információtovábbítást is. (Kolozsi 2000)

A *pc banking* kifejezést az olyan kétirányú adatforgalommal járó banki tevékenységekre használjuk, melyek a felhasználó személyi számítógépén keresztül intézhetőek. Ennek alapvetően két típusát különböztethetjük meg: az egyik egy olyan *on-line* folyamat – mely „home banking" néven vált elterjedtté –, ahol a tranzakciók egy zárt hálózaton belül folynak. Ebben az esetben a felhasználóknak olyan speciális szoftverre van szükségük, melyet a bank bocsát a rendelkezésükre. (Szabó, 2001) A folyamat jellemzője, hogy a felhasználónak csak a program segítségével van lehetősége pénzügyei alakítására, így a home banking esetén nincsen mód a banki szolgáltatások kötöttségek nélküli elérésére. A másik típusa az *internet banking,* mely a kilencvenes évek közepétől terjedt el, igaz ekkor még csak információk nyújtására használták a hálózatot. A zárt hálózatoktól eltérő módon az internet banking lehetővé teszi a felhasználó számára, hogy szinte minden internetcsatlakozással rendelkező terminálról elérhesse a banki szolgáltatásokat. Ez azt jelenti, hogy mindenféle szoftver- és hardvermegkötés nélkül, egyszerű web-böngészőn keresztül intézhetőek el a kívánt tranzakciók.

Ennek előnye a „home bankinghoz" képest az, hogy a felhasználók több számítógépről – például: munkahelyiről, otthoniról, internet kávézóból – is rendezhetik ügyeiket. Ezzel lehetővé válik a tejes kommunikáció elektronikus csatornákon történő megvalósulása. A vázolt folyamat biztonsági és jogi hátterét segíti elő a hazánkban már négy éve legalizált, de sok tekintetben még óriási fejlődési lehetőség előtt álló digitális aláírás alkalmazása.

Számos faktor – például a versenyképes költségek, a vevőszolgáltatás és a demográfiai megfontolások – motiválja a bankokat, hogy átértékeljék a rendelkezésükre álló technológiát, eszközöket, elektronikus rendszereket és az internet banking stratégiájukat. A legtöbb kutatás gyors növekedést prognosztizál az on-line pénzügyi szolgáltatások és termékek piacán. A bankok és más pénzügyi szolgáltatók számára igazi kihívást fog jelenteni, hogy megfelelően alkalmazzák a kockázatkezelési eljárásaikat és menedzseljék tevékenységüket ebben az új, rohamosan változó környezetben. Az utóbbi években mind hazánkban, mind külföldön egyre több bank és ügyfél ismeri fel az internet banking előnyeit, mely hozzájárult az elektronikus piac rohamos fejlődéséhez.

Bizonyos keretek között – fogyasztó- és adatvédelmi okokból – az elektronikus tranzakciók lehetővé teszik a fogyasztói szokások figyelemmel kísérését. A megfelelő adatbázis kialakítása képessé teszi a bankokat arra, hogy a fogyasztók különböző csoportjainak speciális igényeire kialakított ajánlatokkal álljanak elő. Így az internet banking lehetővé teszi azt, hogy a bankok személyre szabott megoldásokkal állhassanak elő a vásárlók felé, ami erősíti a meglévő ügyfelek elégedettségét, és hozzájárulhat új felhasználók megnyeréséhez is. (Pricewaterhouse Coopers, 1999)

Az elektronikus kereskedelemben való részvétel hozzásegítheti a bankokat új és

vonzó fogyasztói szegmensek megnyeréséhez is. A felmérések szerint a 14 és 69 év közötti korosztály egyharmada internetezik rendszeresen az Európai Unióban. (Deutsche Bundesbank, 2000) Ez az a csoport, amely egyre többször használja az internetet a banki tranzakciójának lebonyolítására. A tanulmány szerint a világháló-használók az átlagosnál jobban képzettek, és – ami a bankok számára még fontosabb – magasabb jövedelemmel is rendelkeznek. Mára azonban árnyaltabb a helyzet, hiszen az internet elterjedésével egyre szélesebb rétegek reprezentálják magukat az elektronikus kereskedelemben.

Az elektronikus kereskedelem megjelenése a banki világban tehát számos előnnyel járhat a hitelintézmények számára, azonban figyelembe kell venni a következő hét fontos jellemzőt, melyek véleményem szerint leginkább hatással vannak a bankok által viselt kockázatokra:

- Az e-banking elmossa a nemzetek és a szektorok közötti határokat. Az elektronikus kereskedelem jellege miatt a banki tranzakciók már nem kötődnek a nemzeti határokhoz, és hasonlóan elmosódnak a határok a banki és nem banki termékek között is.
- Az információtechnológia biztonsága és hatékony fejlődése kulcsfontosságú az e-banking sikeres alkalmazásához. Az értéklánc minden egyes foka, a fejlesztéstől a termelésen át, marketing- és pénzügyi szempontból is nagymértékben függ az IT-től.
- Dinamikus. Egy interneten bevezetett új termék életciklusa jóval rövidebb, mint a hagyományosoké. Már a bevezetés szakaszát is egyszerűbbé és gyorsabbá teszi a nélkülözhetetlen reklám elektronikus megjelenésének lehetősége. Rövid időn belül kivitelezhető egy webes hirdetés, melynek elektronikus jellegét kihasználva a figyelem felkeltésére számos attraktív eszköz áll rendelkezésre, például speciális grafikák, animációk, villogó, forgó feliratok, valamint szembetűnő videofelvételek. Ugyanez a „felgyorsulás" figyelhető meg a növekedés és érettség szakaszaiban a web nyújtotta feltételek kihasználásából fakadóan. Napjainkban az e-businessre jellemző gyors technológiai és infrastrukturális fejlődés tehát az életciklusszakaszok rövidülését vonja maga után, ami dinamikus változásokat eredményez az elektronikus szolgáltatások és termékek piacán.
- Fogyasztóorientált. A technológia és a megnövekedett piaci transzparencia miatt csökken az információs aszimmetria a fogyasztók és a bankok között. A fogyasztók egyre erősebb informáltságának ténye nem csak árelőnyökhöz juttatja őket, hanem az e-banking szolgáltatók a minőség területén is egyre élesebb versenyre kényszerülnek. Ennek alapján bátran állíthatom, hogy az internet létezése hozzájárul a szolgáltatók és a felhasználók közötti erőviszonyok kiegyenlítődéséhez, illetve ahhoz, hogy csakis a fogyasztók érdekeit szem előtt tartó, őket kiszolgáló szolgáltatók maradjanak életképesek a piacon.
- Egyre erősödő verseny. Számos tényező összejátszása okozza e jelenség növekedését. A termékek és az árak összehasonlításának lehetősége fokozza a piaci transzparenciát, emellett az inter-

net miatt a belépési korlátok csökkennek, a versenyt eddig akadályozó térbeli és időbeli korlátok megszűnnek. (Pricewaterhouse Coopers, 1999)
- Költségcsökkentés. Az elektronikus kereskedelem csökkentheti az összköltséget az alacsonyabb tranzakciós költségeken keresztül. Az ügyfélszolgálat és kapcsolattartás megfelelően előkészített és kivitelezett on-line módja költségkímélőbb megoldást jelenthet a hagyományos kiszolgáláshoz képest. (Collinge, 2004)
- A jövő útja. Az eMarketer tanulmánya azt állítja, hogy a széles sávú internet egyre könnyebb elérhetőségének köszönhetően sokkal elfogadottabbá válik az e-kereskedelem, így az ebből fakadó bevétel évről évre növekszik, és egyre több ügyfél veszi igénybe az on-line szolgáltatásokat. A tanulmány előrejelzése szerint az amerikai fogyasztók több mint 133 milliárd dollárt fognak on-line vásárlásra költeni 2005-ben, ami közel 50%-os növekedést jelent a 2003-ra előre jelzett 90,1 milliárd dollárhoz képest. (Infinit hírlevél, 2003) Ebben a folyamatban a bankoknak is növekvő részt kell vállalniuk, hiszen véleményem szerint a mai világban csak az e-kereskedelem megfelelő megvalósításával maradhat versenyképes egy intézmény.

Az internet banking hatása az egyes kockázattípusokra

Egy mai, modern pénzügyi intézmény sikere nagyban függ attól, hogy mennyire tudja javítani és fejleszteni az ügyfeleivel való kapcsolatát, mely cél elősegítéséhez egyre több és több bank használja ki az e-kereskedelem nyújtotta előnyöket. Egyre-másra látunk megjelenni hagyományos bankokat a virtuális kereskedelmi térben, ugyanakkor a nálunk fejlettebb országokban már léteznek úgynevezett internet-only (csak interneten jelen lévő) bankok is. A banki tevékenység – természetéből fakadóan – magas kockázatot hordoz magában. A hagyományos bankok fő kockázatait a stratégiai, üzleti és pénzügyi kockázatok teszik ki. Az internet – mint új értékesítési csatorna – önmagában is jelent új veszélyeket a bankok életében, valamint az eddigi kockázati kitettséget is átrendezi. A fő üzleti tevékenység és az információs technológia szoros összefonódásából fakadóan a teljes kockázati térkép átrendeződését vonja maga után az elektronikus értékesítés innovációja. A bankok számára létkérdéssé válik, hogy a vezetés és a kockázatkelő szakembereik átlássák és kezelni tudják a környezet radikális megváltozásából fakadó veszélyeket.

Stratégiai kockázat

A hagyományos banki szolgáltatások internetre való „kiterjesztése" mára stratégiai fontosságúvá vált a bankok számára. A stratégiai kockázat a gazdasági és politikai környezet alapvető megváltozásának lehetőségéből fakad. (P. Jorion, 1999) A stratégiai kockázatot megkülönböztetett figyelemmel kell kezelni más kockázattípusokhoz képest, hiszen a többitől alapvetően különbözik abban, hogy természetéből fakadóan sokkal általáno-

sabb és szélesebb körű, így hatással van az egész szervezet működésére és alapvető missziójára is. A vezetőség által meghozott stratégiai döntések jelentős hatással vannak az összes többi kockázati kategóriára is. (Mann, 2003) A sikeres implementációhoz nagy szükség van arra, hogy a menedzsment is tisztában legyen azzal, hogy – átlátva lehetőségeit – az eddigi környezethez képest a szolgáltatások jóval nagyobb földrajzi, vagy gazdasági területekre terjedhetnek ki.

A gyors technológiai változások, illetve a többi bankkal és egyéb versenytársakkal folytatott verseny élesedése miatt a nem megfelelően megvalósított, gyenge vagy teljes körűen nem átgondolt elektronikus stratégia alapvető versenyhátrányba sodorhatja a vállalkozásokat környezetükkel szemben. (Hawke, 2000)

A stratégiai kockázat származhat az internetes rendszer nem megfelelő tervezéséből és bevezetéséből, ami akár jelentős hátrányokat is okozhat a bank számára. Ennek veszélye világosan rámutat arra, hogy mekkora hatása van az új lehetőségeknek a teljes üzleti stratégiára. Egy rosszul megszerkesztett vagy nem megfelelően funkcionáló honlap, illetve az olyan on-line szolgáltatások, melyeket a hagyományos tevékenységek kárára vezettek be, gyengébb pénzügyi teljesítményt okozhatnak, negatív hatással van a jövedelmezőségre, és ezáltal a befektetők bizalmának elvesztését eredményezheti.

A hagyományos tevékenységek internet alapúvá történő átalakítása is magában hordozza a veszély lehetőségét. Az elektronikus bankkal kapcsolatos stratégiai kockázat gyakran összekapcsolható a megvalósítás ütemezésével. Kockázatos lehet az új technológia megvalósítójának, bevezetőjének lenni, főleg a bizonytalan és gyorsan változó technológiai környezetben. De ugyancsak kockázatot jelenthet az is, ha csak a technológia követőjeként viselkedik a bank, hiszen a gyorsan kialakuló és elmélyülő piacokon utólag nehézkes lehet a megfelelő pozicionálás és részesedés elnyerése. Így sokszor kérdéses, hogy melyik a kifizetődőbb: első belépőnek és rendszermegvalósítónak lenni (és ezzel többletkockázatot vállalni), vagy kivárni, ami magában hordozza a piacvesztés lehetőségét. Ugyanakkor a nagyon új tevékenységek esetén annak is megvan a veszélye, hogy a fogyasztók nem akceptálják azt, így nem válik sikeressé az újítás.

Sok bankár gondolja azt, hogy az elektronikus banki értékesítési csatorna lehetővé teszi az intézmény számára a működési költségek csökkentését, így az internetes fejlesztések hosszú távú célja a versenyképesség fenntartása mellett a költségek redukálása is. A technológia fejlődése ugyan egyre inkább lehetővé teszi az ügyintézés gépi formáját, de meggyőződésem szerint a felhasználók egy része – talán azok, akik idegenkednek a technikai újításoktól – még jó ideig előnyben fogják részesíteni az ügyintézés és felvilágosítás hagyományos, emberi kapcsolaton alapuló formáját. (Szabó, 2001) Az a feltételezés, hogy sok banki ügyfél továbbra is személyes kapcsolatot kíván fenntartani pénzügyei intézése során, nem teszi lehetővé a bankok számára, hogy teljes egészében felszámolják a hagyományos „fizikai” kapcsolatra épülő kiszolgá-

ló létesítményeiket. Azok az ügyfeleknek, akik az ügyintézés nem elektronikus formáját választják, továbbra is lehetőségük lesz arra, hogy betérjenek bankfiókjukba. Véleményem szerint az interneten keresztüli, kényelmes, sorban állás nélküli ügyintézés hatással van – és lesz – a hagyományos bankfiókokra is, így a jövőben modernizált, gyorsabb, az ügyfelek igényeihez jobban alkalmazkodó kiszolgálással lehet találkozni a hitelintézeteknél.

A fenti okfejtésből fakadóan, meglátásom szerint hazánkban egyelőre csak a hagyományos bankok által nyújtott elektronikus szolgáltatások életképesek. Ezeknek a hitelintézeteknek az ügyfelekkel már meglévő, élő kapcsolata van, rendelkeznek megfelelő tapasztalattal és anyagi háttérrel az eddigi tevékenységükből fakadóan. A világháló nyújtotta előnyöket kihasználhatják kommunikációs és marketingcéljaik erősítésére, továbbá problémamentesen valósítható meg a keresztértékesítés is az összbevétel növelése érdekében. A hagyományos bankok esetében megvan annak is a lehetősége, hogy a technológiai újításoktól idegenkedő, bizalmatlan ügyfeleket csak a későbbiekben győzzék meg az elektronikus szolgáltatások előnyeiről.

Ez azt is jelenti, hogy a bankoknak – a közeljövőben mindenképpen – többcsatornás értékesítési hálózatot kell fenntartaniuk, így a hagyományos mellett az internetes értékesítés plusz kiadásként jelenik meg. A technológiai-környezeti változások abba az irányba mutatnak, hogy a jövőben egyre kevesebb munkaerőre lesz szükség, és az elektronikus szolgáltatások elterjedésével jóval kisebb számú fizikai kapcsolatot kell fenntartani az ügyfelekkel. Ennek következtében az operációs költségek csökkentésébe vetett hit valószínűleg csak hosszabb távon fog megvalósulni. Persze minden innovációnak megvan a maga kockázata, melyet jól példáz az alábbi felmérés.

A Computer Weekly magazinban megjelent cikk alapján az európai nagy bankok többségének az eddigi beruházásai mellett még legalább 300 millió font nagyságrendű összeget kell invesztálni a többcsatornás szolgáltatásaik fejlesztésébe, mielőtt a költségeik csökkenését tapasztalhatnák. A Forrester Research piackutató intézet (Cambridge, Massachusets) szerint a különböző elektronikus csatornákon (internet, wap, telebanking) az ügyfelek megszerzéséért indított harc az egyes csatornák inkompatibilitásába torkollott. A bankok a kilencvenes évek közepétől kezdtek az új értékesítési csatornákba nagyobb összegeket beruházni, de az utóbbi öt év 200-600 millió eurós invesztíciója a technológiai környezet gyors változása és az egyes gazdasági részlegek közötti elégtelen kommunikáció miatt veszni látszik. (Pánczél, 2003) Mára a bankok célja az lett, hogy megpróbálják összehangolni az egyes hardvereket, szoftvereket és platformokat, hiszen a különböző csatornák sokszor képtelenek egymással kommunikálni és információt cserélni.

Mindez az ügyfelek számára jelentheti azt, hogy például az on-line bonyolított pénzátutalás részleteiben a bank telefonos ügyfélszolgálatának munkatársai nem tudnak segíteni, mivel számukra ezek az információk nem láthatóak. Továbbá meg kell említeni, hogy a modern pénzügyi szabályozók – például a pénzmosás elleni

törvény – sem valósítható meg az informatikai rendszerek összekötése nélkül. Így a jelenlegi helyzetben a bankoknak érdemesebb lenne a meglévő rendszereik hatékonyabbá tételére koncentrálni, és összehangolni a különféle elektronikus szolgáltatásaikat, sem mint új rendszerek fejlesztésébe ölni a pénzüket. A felmérés szerint az összekapcsolódások megvalósításával a költségek 30%-kal csökkenhetnek, ám ehhez újabb 70-400 millió eurónak megfelelő összeget kell elkölteni a következő néhány évben. (Pánczél, 2003)

A bank vezetésének gondosan át kell gondolnia, hogy az internetes stratégiája hogyan tudja fenntartani a versenyképességét és profitábilitását anélkül, hogy az ne okozzon lényeges vagy befolyásolhatatlan növekedést az intézmény kockázati profiljában. A felügyeleti szerveknek is kényszeríteni kell a bankokat arra, hogy megfelelő alapossággal becsüljék meg az elektronikus szolgáltatások bevezetésével járó stratégiára ható pró- és kontra hatásokat.

Üzleti kockázat

„Az üzleti kockázat alatt olyan fenyegetettséget értünk, amely szerint egy esemény vagy egy tevékenység meggátolja a szervezetet abban, hogy a tulajdonosi értéket maximálja, és a saját kitűzött céljait elérje”. (Ernst and Young, 2005)

Üzleti kockázat alatt tehát a vállalat tudatosan vállalt magatartását értjük, melynek célja, hogy versenyelőnyt szerezzen a többiekkel szemben. (P. Jorion, 1999) A bankok számára az internet alkalmazásából származó üzleti kockázat a világhálóval kapcsolatos fejlesztésekből, innovációkból és a radikálisan új értékesítési csatornához tartózó alkalmazandó marketingeszközökből áll.

Az internet egyre inkább terjedő használata és a hozzáférések általánossá válása a határok felbomlásához vezet. Ennek eredményeképpen az új média a hagyományos marketingeszközökhöz képest jóval nagyobb tömeghez való hozzáférést biztosít. A részvényesek vagyonának növelésére lehetőséget nyújt a világháló segítségével elérhető, az eddiginél nagyobb és el nem ért piacok meghódítása. A bankok számára azonban meggondolandó, hogy valóban limitálás nélkül fogadjanak ügyfeleket a világ minden pontjáról. A földrajzilag távolabbi területeken élő ügyfelek eltérő szokásai, kultúrája és jogi berendezkedése miatt készen kell állni arra, hogy a problémák és pereskedések gyakoribbak lesznek. A kiszélesített ügyfélkör miatt tehát több figyelmet és forrást kell biztosítani az esetleges problémák és bírósági ügyek kezelésére.

Az interneten vásárlók sajátossága, hogy hajlandóak több időt szentelni a legolcsóbb ajánlatok felkutatására, miközben a lojalitásuk jóval kisebb, mint az átlagos vásárlóké. (Mann, 2003) Ez a tény a bankok vonatkozásában erőteljesen növelheti a betétállomány volatilitását, melyet például a többi piaci résztvevő betéti kamatlábainak változása idézhet elő. Az ennek következtében kialakuló óriási verseny arra késztetheti a résztvevőket, hogy az ügyfelek megnyerése érdekében további, pluszkockázatot vállaljanak, így például kisebb hitel- és nagyobb betéti kamatlábakkal rukkoljanak elő.

A vezetésnek teljeskörűen fel kell tárnia az internet bankinggal kapcsolatos kockázatokat, mielőtt döntést hoznak az új technológia üzletmenetbe történő bevezetéséről. A menedzsmentnek át kell látnia az elektronikus csatornákon keresztül értékesített termékekből és szolgáltatásokból fakadó kockázatokat és e döntés következményeit is. Megfelelő fejlettségű technológiai színvonal és vezetői információs rendszer szükséges az ilyen típusú üzleti vállalkozások támogatásához (Mann, 2003). Sok bank fog versenybe szállni más pénzügyi vállalkozásokkal szemben a jelenlegi üzleti területén kívül is az internet lehetőségeinek kihasználásával, ami megköveteli a szoros kapcsolatot az alkalmazott technológiák és a bank stratégiai tervezése között.

Az intézményeknek készen kell állniuk arra, hogy a piaci változásokra gyorsabban kell reagálniuk, mint eddig. Ehhez, mindig megfelelő eszköz/forrás arányt kell fenntartaniuk, a likviditásra és a szolvenciára még az eddigieknél is nagyobb hangsúlyt kell fektetni. A piac apró rezdülései is nagyobb hatással lehetnek a bankokra, így a piacelemzések, analízisek szerepe növekedni látszik.

Pénzügyi kockázatok

Működési kockázat

A működési kockázatok az alkalmazott rendszerek hiányosságaiból, a vezetés által elkövetett hibákból, az ellenőrzés elégtelenségéből, vagy csalások, támadások és emberi mulasztások miatt következnek be. (P. Jorion, 1999)

1992-ben alakult meg a Banki Szabványok Európai Bizottsága (ECBS, European Committee for Bank Standards), mely kidolgozta a fizetési megbízásokkal kapcsolatos, ma is alkalmazott szabványokat: az IBAN-t (International Bank Account Number) és a nemzetközi fizetési megbízást (IPI, International Payment Instruction). Az IPI azok között a partnerek között biztosít szabványos felületet, amelyek nem elektronikusan érintkeznek egymással, így az internet banking vonatkozásában ez irreleváns. Az IBAN alkalmazásával lehetővé vált az emberi beavatkozás felszámolása a fizetési láncolatban. (Bartha, 2003) Az IBAN – mely alfanumerikus karakterek sorozatából álló sztenderd forma – biztosítja azt, hogy a nem harmonizált belföldi számlastruktúrák is átfordíthatóak legyenek, ezzel lehetővé téve a nemzetközi átutalási megbízások automatikus vagy más néven STP (Straight Through Processing = manuális beavatkozás nélküli) továbbítását a fizetések feldolgozásának teljes láncolatában. (MNB, 2001) Az ECBS fejlesztéseinek köszönhetően mára rendelkezésre állnak azok a szabványok, melyek lehetővé teszik a fizetések gyors és automatizált feldolgozását. Jelenleg a bankokon van a sor, hogy belső informatikai rendszereiket is képessé tegyék a szabványok kezelésére és létrehozzák a szabványok alkalmazásához szükséges elszámolási rendszereiket. Az internet bankinggal kapcsolatos működési kockázatok alatt a továbbiakban tehát az STP fizetési rendszer működésének kockázatát kell érteni.

A működési kockázat tehát az internet bankingban alkalmazott informatikai és

biztonsági rendszerek tökéletlenségéből és az integritás hiányának kihasználásából fakadhat. Az e-banking szinte minden területe erőteljesen támaszkodik a technológiai feltételekre, emiatt az operációs kockázat markánsan jelen van ezen a területen. A működési kockázat csökkentése érdekében a bankok feladata egy egész vállalatot átölelő és integrált technológiai infrastruktúra létrehozása, mely megkönnyíti a különböző szervezeti egységek közötti együttműködést, biztosítja a biztonságos üzemeltetést, az adatintegritást és rendelkezésre állást, valamint támogatja a vezetést a külső szolgáltatókkal való kapcsolattartás során. (Hawke, 2000) A jövőben a technológiai fejlődés drámaian meg fogja változtatni a most alkalmazott üzleti modelleket és operatív eljárásokat, így a bankoknak biztosítaniuk kell, hogy megfelelő kontrollal rendelkezzenek a különböző folyamatok és audit eljárások felett.

Sok nagybank szembesül azzal a feladattal, hogy olyan integrált rendszert hozzon létre, mely lehetőséget nyújt az e-banking tevékenységek mellett a hagyományos banki aktivitások folytatására is. Ha nem sikerül megvalósítani az e-banking tökéletes integrációját, akkor e bankoknak jelentős működési kockázattal kell számolniuk a tranzakciók feldolgozásából fakadó hibák miatt. (Comptroller's handbook, 1999) Amíg ezen fejlesztések pozitívan hatnak a nagy bankokra, addig a teljes banki iparágnak további fejlesztésekre van szüksége ahhoz, hogy olyan fejlettebb belső rendszereket és kockázatkezelési infrastruktúrát hozzon létre, amely hatékonyan tudja támogatni az elektronikus kereskedelmet. A kis és közepes bankok számára jelentős kihívást jelentenek e fejlesztések, hiszen a rendelkezésre álló költségvetés limitálja az új hardverek, szoftverek és a technológiai személyzet tartásának lehetőségeit. A kisebb bankok többsége számára csak az a megoldás marad, hogy külső szolgáltató igénybevételével hozza létre és tartsa fenn az e-bankinghoz szükséges technológiai infrastruktúrát. Azonban ebben az esetben is biztosítani kell a hitelintézeteknek azt, hogy a működésük továbbra is jól ellenőrzött és irányított maradjon.

Hírnév és reputációs kockázat

A reputációs kockázat a bázeli definíció szerint a működési kockázat része. A bankok jó hírnevének alapját az ügyfeleik bizalma jelenti. Az elektronikus bankot támogató megbízható hálózat létrehozása kritikus fontosságú, hiszen az intézmény jó hírneve gyorsan tönkretehető egy roszszul működő rendszerrel. A bank reputációja csorbát szenvedhet, ha az e-banking nem képes a biztonságos és pontos működésre. (Hawke, 2000)

A pénzügyi intézmények internetes banki tevékenységeivel kapcsolatos negatív publicitás könnyen okozhatja a bizalom megrendülését a jelenlegi és a jövendőbeli ügyfelek körében is, ami hosszabb távon a nyereségesség csökkenéséhez vezethet. A banki szektorban a különlegesen fontos jó hírnév tönkretételét okozhatja az az internetes felület, mely nem teljesen ügyfélbarát, túl lassú vagy pontatlan. Erre bizonyíték a Stanford University Persua-

sive Technology Lab által 2002-ben folytatott felmérés is, melyben egyesült államokbeli és európai internetezőket kérdeztek meg. Az interjúalanyok nyolcvan százaléka szerint nagyon fontos, hogy egy oldal tartalmában meg lehessen bízni. A tanulmányból kiderül, hogy a felhasználói bizalom csökkenését okozhatja akár egy honlapon szereplő apró helyesírási hiba is, mely közvetlen módon befolyásolja a mögötte álló bank reputációját. (NRC, 2002)

Az ügyfelek bizalma tehát kulcsfontosságú szerepet játszik a bankok életében, de még ennél is fontosabbat az elektronikus pénzügyi szolgáltatások területén. Erre próbálnak garanciát nyújtani a titkosítási eljárások, melyek célja a biztonságos használhatóság kialakításán keresztül az ügyfelek bizalmának megerősítése vagy megalapozása. A titkosítási eljárásban három fél vesz rész: a bank, az ügyfél és a hitelesítő szervezet. Ennek a bizonyos harmadik félnek a feladata a virtuális térben az egyes identitások azonosítása. (Comptroller's handbook, 1999) Sok felhasználó gondolja úgy, hogy ez a résztvevő egyfajta on-line közjegyzőként funkcionál. De a koncepció lényege a bizalom erősítésében rejlik, hiszen a hitelesítő valójában a jó hírnevét, márkanevét adja a két fél közötti tranzakcióhoz, ezzel segítve elő az üzletkötést. Ez hasonlítható a bankok korai funkciójához, vagyis amikor igazolták a náluk letétbe helyezett pénzt, ezáltal erősítve a kereskedelmi ügyletben részt vevő két fél bizalmát egymás iránt, természetesen díjazás ellenében.

Ehhez kapcsolódóan ráadásul egyre inkább elszaporodnak a biztonságos használatot fenyegető illegális (hacker-cracker) tevékenységek is, melyek elsődleges célja a felhasználói adatokhoz való hozzáférés.

Az E-marketer piackutató cég 2003-as felmérése alapján a banki ügyfelek nem elégednek meg a pénzügyi adataik biztonságának garantálásával, vagy a személyazonosságuk lopás elleni védettségével az e-banking területén. Sok esetben merül fel az ügyfelekben az a félelem is, hogy maga a bank sem tartja tiszteletben a személyes adatvédelmet. A Ponemon Institute, adatvédelemmel és üzleti etikával foglalkozó amerikai kutatóintézet, a 25 legnagyobb bank ügyfelei körében végzett felmérést az Egyesült Államokban. Az eredmények jól tükrözik a fenti hipotézist, hiszen a felmérés eredményéből kitűnik, hogy az öt leginkább bizalmat keltő bank ügyfelei között a megkérdezettek csupán 25%-a veszi biztosra, hogy bankja elkötelezett az egyének adatvédelme szempontjából. Ugyanakkor a legkevesebb bizalmat élvező öt bank ügyfelei körében ugyanez az arány csupán 8%-ra tehető. Az öt leginkább bizalomgerjesztő bank ügyfélkörében 74% emlékszik úgy, hogy bankja kipostázta adatvédelmi nyilatkozatát, míg az öt legkevésbé bizalmat ébresztő intézet esetében ez az arány 46%. Az öt rangos bank esetében a válaszadók 55%-a olvasta el az adatvédelmi politikáról szóló dokumentumot, míg az utolsó öt helyen végző pénzintézet ügyfelei esetében csupán 33%-ról mondható el ugyanez. (Szabó, 2003)

Sok hitelintézményről elmondható, hogy túl nagy hangsúlyt fordít az új online és vezeték nélküli technológiák bevezetésére, ahelyett, hogy a már meglévő

elektronikus szolgáltatásaikat tennék biztonságosabbá, megbízhatóbbá. A Jupiter piackutató MMXI. jelentéséből kiderül, hogy a bankok vezetői inkább az új elektronikus szolgáltatások bevezetésére, míg az ügyfelek a már meglévő on-line rendszerek biztonságosabbá tételére helyezik a hangsúlyt. A megkérdezett banki felsővezetőknek csupán egynegyede nevezte meg alapvető fontosságúnak ügyfeleik bizalmának erősítését, miközben a felhasználók 59%-a tartja az állami garanciát döntő szempontnak a hitelintézmény-választáskor. (Enos, 2004) A felmérésből kitűnik, hogy a fogyasztók többsége elsősorban a biztonságra törekszik a szolgáltatások igénybevételekor, amit figyelembe kell venni a bankoknak az e-banking rendszereik bevezetésekor és működtetésekor.

Az interneten gyakorta alkalmazott technika a hyperlink, mely kifejezésen a hiperszöveges rendszerek két elemét összekötő kapcsot értjük. A legismertebb hiperkapcsok a webes linkek, amelyek a web elemeit kötik össze egymással. Ezt az eljárást sok esetben alkalmazzák a bankok is, amikor honlapjukon más szolgáltató weboldalára mutató linket helyeznek el. A kiemelten fontos ügyfélbizalom megóvása érdekében a hitelintézeteknek érdemes világosan tisztázni a felhasználók számára, hogy a weblapján mely szolgáltatások tartoznak saját hatáskörbe, és melyek jelentik egy harmadik fél termékeit. Az oldal elhagyásával egyértelművé kell tenni az ügyfelek számára, hogy innentől fogva más felelőssége a nyújtott szolgáltatás. Ennél a megállapításnál azt is meg kell jegyezni, hogy az intézményeknek szintén van felelősségük abban, hogy egyáltalán milyen linkeket engednek az oldalukra feltenni. Ugyancsak hátrányosan érintheti a pénzügyi szervezetet, ha az ügyfelektől beérkező tudakozó jellegű e-mailekre nem válaszol időben, vagy nem tudja szavatolni a felhasználók adatainak bizalmasságát. A korábban említett Stanford Univerity által végzett felmérés kimutatta, hogy egy interneten nyújtott kereskedelmi szolgáltatás fogyasztói megítélését leginkább meghatározó elemek között szerepel az ügyfelek leveleire adott gyors válaszadás is. (Enos, 2004)

Biztonság

A működési kockázatok között kell említeni a technológiai kockázatot is, amelyek az alkalmazott rendszerek védelméből és az illetéktelen behatolások és hamisítások elleni védelemből származnak. (P. Jorion, 1999) Számos bank a biztonsággal kapcsolatos kockázatot tartja a leginkább aggodalomra méltónak az e-bankinggal kapcsolatban. Az internetes banki környezetben működő pénzintézet nagymértékben ki van téve a belső (dolgozók által elkövetet) vagy külső (hacker) illegális behatolásoknak, de veszély forrásai lehetnek a szándékos vagy az akaratlan fogyasztói visszaélések is. Egyes tanulmányok kimutatták, hogy a rendszerek sokkal sérülékenyebbek a belső behatolásokkal szemben, hiszen az ott dolgozóknak nagyobb a tapasztalatuk, az ismeretük, és jobb eszköztár áll rendelkezésükre a támadások kivitelezéséhez.

A már korábban említett digitális aláírásról szóló törvény értelmében a biztonságos működés alapfeltétele a hitelesség, a

partnerazonosítás, az integritás és a letagadhatatlanság négyesének egyidejű megvalósítása.

- Hitelesség (Authenticity): egyértelműen legyen beazonosítható, hogy egy adott üzenet honnan származik, ki küldte azt. Erre azért van szükség, mivel az egyetemesen használt TCP/IP protokoll az ügyfelek azonosítására olyan titkosítási eljárást használ, amely hozzáértők számára elfogható vagy a kulcsa megfejthető. Az azonosításra szolgáló másik lehetőség az IP címek vizsgálata, ami szintén félrevezető lehet, hiszen ezeket a címeket is meg lehet változtatni, ezáltal nagyon nehézzé válik a küldő fél azonosítása.
- Titkosítás / Személyiségi jogok védelme (Privacy): a fent leírt azonosításon túl a bankoknak és ügyfeleiknek biztosnak kell lenniük abban, hogy az általuk küldött és fogadott adatokat rajtuk kívül más nem látja. Az adatok bizalmas jellegét garantálni kell, emellett magát az információtartalmat is védeni szükséges az illetéktelen fenyegetések ellen. Emiatt vált gyakorlattá, hogy kódolt adatokkal kommunikál egymással a bank és az ügyfele, így biztosítva azt, hogy a kódolt üzenet tartalmát csak a dekódolás kulcsát ismerő másik fél fedheti fel.
- Épség megőrzése / Integritás (Integrity): ha biztosítva van az, hogy az adott adatot ki küldte, és az is bizonyos, hogy más nem láthatta az információt, további alapvető elvárás, hogy a védendő adatot „útközben" ne módosítsák. Jelezhetővé kell tenni, hogy az eredetileg elküldött és a megérkezett üzenet nem egy és ugyanaz, tehát módosult-e (véletlenül vagy szándékosan) a tartalma az átvitel során.
- Letagadhatatlanság / visszautasíthatatlanság (Nonrepudiation): a fent említett biztonságos működéshez szükséges három alapvető elváráshoz kívánkozik egy negyedik is, melynek célja annak biztosítása, hogy az üzenet küldője ne tagadhassa le, hogy ő küldte az üzenetet. Ennek jelentősége, hogy ne alakulhasson ki vita az elektronikus fizetés esetén a megrendelő és a fizető (pl. bankkártya-tulajdonos) személyének különbözőségét illetően.

A külső fenyegetések, mint a „*hackelés",* a „*sniffing"* és a „*szolgáltatás visszautasítására"* irányuló támadások óriási kockázatnak teszik ki a bankokat. A nyitott elektronikus értékesítési csatornák új fejezetet nyitnak a biztonságos működés fenntartása kapcsán, hisz a bankoknak fenn kell tartaniuk a bizalmas adatok kezelésére és integritására vonatkozó szabályokat, továbbá nem utasíthatnak vissza szolgáltatás nyújtására vonatkozó kérést, valamint továbbra is teljes biztonsággal kell azonosítaniuk ügyfeleiket és azok hozzáférési jogait. (Hawke, 2000)

A támadások fajtái

A *hackelés* egy számítógépbe vagy számítógép-hálózatba történő engedély nélküli, rosszindulatú behatolást jelent. Célja legtöbbször az anyagi haszonszerzés, illetve a célintézménynek vagy -személynek való károkozás, de a hackelés oka lehet más, akár személyes indok is.

A hackelés gyakorta alkalmazott módszere a session lopás vagy más néven IP splicing, ami olyan támadást jelent, ahol a támadó egy aktív, éppen fennálló kapcsolatot „csíp el" és vonja ennek irányítását a saját kezébe. A támadás alapja az, hogy a hacker az azonosítási procedúra után támadja meg a kapcsolatot. A módszer lényege, hogy a rendszert oly módon téveszti meg a behatoló, hogy a belépéshez szükséges kódok feltörése nélkül válik képessé más számlája feletti jogosulatlan rendelkezésre.

Az internetes banki szolgáltatásokat igénybe vevő ügyfelek, illetve bankok ellen irányuló támadások esetén egyre gyakoribbak az e-mailben érkező, látszólag adminisztrációs célú fenyegetések. 2004 novemberében pontosan ilyen támadást intéztek ismeretlen hackerek Magyarország legnagyobb kereskedelmi bankja ellen. Módszerük a következő volt: lemásolták a bank internetes oldalát, és a felhasználók között szétküldtek egy e-mailt, melyben arra kérték őket, hogy adják meg a belépéshez szükséges adataikat, természetesen a klón honlapon. Az ilyen levelek általában biztonsági okokra hivatkozva számlainformációk begépelésére kérik az ügyfeleket. Az eredetinek tűnő e-mailben még linket is lehet találni, melyre kattintva a bank hivatalos honlapjának pontos másán találjuk magunkat. Az így szerzett adatokkal ezután a hackerek hozzáférhettek az ügyfelek számláihoz is. Az OTP gyorsan reagált a támadásra, és smsen, illetve honlapján hívta fel az ügyfelek figyelmét a fenyegető veszélyre. Az MTI információi szerint a hackerek ezzel a módszerrel csak egy felhasználó adatait tudták megszerezni, de neki sem tudtak kárt okozni. (MTI, 2004)

Az egyesült királyságbeli APACS (Association for Payment Clearing Services – az Egyesült Királyság fizetési iparágát összefogó szervezet) 2004-es felmérése szerint sok internetes felhasználó egyáltalán nem is próbálja megvédeni önmagát és számláját az on-line banki csalások ellen. A felmérés eredménye azt mutatta, hogy az ügyfeleknek csupán negyede jár utána annak, hogy lehet-e hinni az e-mailben írtaknak, ugyanakkor mintegy 4%-uk habozás nélkül megadja a kért adatokat. A többiek pedig úgy döntenek, hogy tudomást sem vesznek az ilyen típusú levelekről. A biztonságra vonatkozó kérdések eredményéből kitűnik, hogy a felhasználók 40%-a tűzfallal sem rendelkezik, és nagyon kevesen használnak hatékony vírusirtót. (Szabó, 2004)

A *„sniffing"* egy kis program elhelyezését jelenti egy hálózat valamely számítógépén, melynek feladata, hogy „elhalássza" a felhasználók személyes adatait, jelszavait stb. Az így megszerzett adatokkal később támadást lehet intézni a célhálózat ellen.

Ilyen típusú támadás ért például 2004 augusztusában többek között olyan neves angol bankokat is, mint az Abbey, a Barclays vagy a Lloyds. A támadók pénzt próbáltak átirányítani brit számlákról oly módon, hogy a számítógépeket „trójai programokkal" fertőzték meg, melyek titokban rögzítik a felhasználók által leütött billentyűket, ha a kliensek egy bank oldalára látogatnak. A nem megfelelően védett számítógépek e-maileken keresztül vagy internetes letöltések során fertőződhettek meg. Ezután a bizalmas adatokat elküld-

ték egy Oroszországban regisztrált internetes oldalra, így lehetővé vált, hogy a hackerek hozzáférjenek a bankszámlákhoz. (Fleming, 2004)

A helyzetet tovább súlyosbítja – az Infosurv on-line piackutató cég szerint –, hogy a felhasználók többsége ugyanazt a jelszót használja az egy bankon belüli különböző szolgáltatások eléréséhez is, és a különböző bankoknál lévő számlái esetén is. Ennek köszönhetően, ha a rosszindulatú behatolók megszereznek akárcsak egy jelszót, akkor képessé válnak több fronton támadást intézni az ügyfelek ellen. Ezt jól példázzák a statisztikai adatok is, hiszen az elmúlt hat hónapban világszerte megduplázódott a korábbi időszakokhoz képest a „sniffing" típusú támadások száma az on-line bankok ellen. (McGann, 2005) Az on-line bankok használóinak tisztában kell lenniük azzal, hogy előfordulhat az is, hogy a világ másik feléről kirabolják őket miközben biztonságosnak tűnő karosszékükben üldögélnek otthon.

Az eddig említett rosszindulatú támadásfajtákon kívül azonban még számtalan egyéb módja létezik az elektronikus fenyegetéseknek: (Comptroller's handbook, 1999)

- Jelszógenerátorok alkalmazása: ezek olyan rosszindulatú szoftvereket jelentenek, melyek az internet banking belépési felületén kért jelszavakat generálnak. A szoftver egy bizonyos algoritmus szerint „gyártja" a jelszavakat, míg rá nem lel az igazira.
- A *„spoofing"* célja a rendszer megtévesztése oly módon, hogy egy illetéktelen behatolási szándékot jogos bejelentkezéseként tüntessen fel.
- Nyers erő támadás (brute force]: olyan technológia, mellyel a támadó a titkosított üzeneteteket fogja el, és egy szoftver segítségével feltöri annak kulcsát. Ezáltal lehetővé válik a felhasználó azonosítása, és jelszavának megszerzése.
- Véletlen tárcsázás: a támadók egy bank telefonközpontjának minden számát feltárcsázzák, abból a célból, hogy találjanak egy csatlakozott modemes kapcsolatot, ami a támadás pontjaként szolgál.
- Szociális ráhatás: a rossz szándékú támadó a bank telefonos szolgáltatását veszi igénybe úgy, hogy kiadja magát egy ügyfélnek, aki elvesztette a kódját vagy baleset érte stb. A cél az, hogy a telefonkezelőt személyesen meggyőzze arról, hogy valóban ő a jogosult, és így a későbbiekben a megváltoztatott jelszóval ráteheti a kezét a jogos felhasználó értékeire.

A nem megfelelő biztonsági rendszer hatással lehet a reputációs vagy a jogi kockázat megnövekedésére is, hiszen a felhasználók adatainak nem megfelelő védelme okozhat bankkal szembeni pereket és/vagy a bank jó hírnevének csökkenését is. Nemzetközi viszonylatban a bankfelügyeleteknek ösztönözniük kell azt a széles körű megközelítést, mely szerint a bankoknak megfelelő kockázatkezelési eljárásokat kell alkalmazniuk mind a külső, mind a belső támadások kivédésére.

Rendelkezésre állás

A sikeres elektronikus szolgáltatás nyújtása érdekében létrehozott biztonságos belső informatikai hálózaton kívül, fontos

a megfelelő kapacitásigény felmérése a kifelé irányuló elektronikus termékek és szolgáltatások számára.

Kockázatot rejthetnek magukban azon internetes banki tevékenység során értékesítésre került termékek is, melyek nem lettek megfelelően és körültekintően megtervezve, megvalósítva vagy ellenőrizve. Azon bankoknak, melyek pénzügyi termékeket kínálnak az interneten keresztül, képesnek kell lenniük arra, hogy kielégítsék az ügyfeleik elvárásait, így megfelelő termékösszetétellel kell kiállniuk a piacra. Ennek párosodnia kell a szolgáltatások pontos, biztonságos, és megbízható teljesítésével, annak érdekében, hogy fenntarthassák, illetve megalapozzák a márkanevüket.

A tranzakciók száma egyre erősödő ingadozást mutat, ahogy az ügyfelek árérzékenysége és automatizáltsága is növekszik. A versenyhelyzet élesedése és az ügyféloldali technológiai adottságok fejlődése hozzájárult ahhoz, hogy a felhasználók egyre inkább elvárják a biztonságos üzemeltetést a nap 24 órájában, a hét minden napján, és egyre kevésbé tolerálják a hibákat. A folyamatos rendelkezésre állás mára a bizalom fenntartásának alapfeltételévé vált az elektronikus környezetben. Ezen felül a versenyben maradás és a piaci pozíció növelésének titka – a jó hírnév megtartásán keresztül – az elektronikus banki szolgáltatások és termékek választékának és összetételének biztonságos, pontos és következetes kialakításában rejlik. Ehhez hozzájárul az is, hogy a befektetési lehetőségeket az interneten keresőkre alacsony tolerancia jellemző a hibák és késedelmek tekintetében. (Hawke, 2000) Az ebből fakadó viszontagságok olyan bankok esetében jelentkezhetnek, amelyek nem rendelkeznek megfelelően kifinomult belső kontrollal, mely képessé tenné őket az internetes banki tevékenységeik megfelelő menedzselésére. Az internetes felületen folyó tranzakciók monitorozása technikailag viszonylag egyszerű feladat, de segítségével a menedzsment olyan információkhoz juthat, mint például a forgalom volumene, a tranzakciók lebonyolításának időigénye vagy kényszerűségből a várakozásra fordított idő. (Mann, 2003) Az ilyen típusú monitoring tevékenység segítheti a bank vezetését, hogy olyan beruházási döntéseket hozzon, melyek javíthatják a rendelkezésre állás minőségét.

A felhasználók folyamatos és megbízható rendelkezésre állást követelnek meg a webes alapon nyújtott szolgáltatásoktól, mely kihangsúlyozza az üzletmenet folytonosságának, helyreállításának és a hibákra való reagálás stratégiáinak jelentőségét. Az outsorcing alkalmazása miatt a bankoknak azt is biztosítaniuk kell, hogy a külső szolgáltatóknál is rendelkezzenek a folyamatos működéshez szükséges tervekkel.

A folyamatos rendelkezésre állás ellen is irányulhatnak támadások a világhálón keresztül. Az alkalmazott internet banking rendszerek védelme az illetéktelen behatolások ellen a technológiai kockázatok közé sorolandó. Én mégis az előző pontban taglalt támadástípusoktól elkülönítve kezelem ezt a kategóriát, mivel az elektronikus kereskedelem egyik alappillérének számít a folyamatos szolgáltatás nyújtása. Az interneten keresztüli banki ügyintézés

egyik legvonzóbb tulajdonsága szintén a 24 órán keresztüli rendelkezésre állás, így fontossága miatt külön figyelmet fordítok az ezt megakadályozni akaró világháló irányából érkező támadásokra.

A szolgáltatások visszautasítása típusú támadások (DoS – Denial of Service) még tovább növelik a folyamatos működés fenntartásának kockázatait. A támadás nagymennyiségű kérelemmel halmozza el a kiszolgáló szervert, ami ezáltal megbénul, és nem képes fogadni a jogos felhasználók igényeit sem Az ilyen típusú külső támadások egyre gyakrabban ütik fel fejüket az internetet használó szervezetek ellen.

2003 augusztusában DoS támadás érte a Microsoft szoftveróriás központi szerverét. A támadás során a hackerek nagy mennyiségű hibás adatcsomaggal bombázták a kiszolgálót, ami ennek következtében órákra megbénult. (Tóth, 2003) Elgondolkodtató, hogy mi történt volna, ha egy bankot érte volna ez a támadás. Az ügyfeleknek számos kára származna abból, hogy nem tudnak hozzáférni számláikhoz, vagy – ami talán még súlyosabb – nem tudnak tőzsdei tranzakciókat folytatni. A szolgáltatás – egy bizonyos időtartamon túli – kimaradása miatt a felhasználóknak okozott kár az Amerikai Bankszövetség szerint (ABA – American Banking Society) a bankokat terheli, ami komoly anyagi és reputációs kockázattal is járhat az intézmény számára. (http://progressive banks.com/Agents/ib_policy.asp)

A hálózati elemek egyikének meghibásodása is okozhatja a teljes rendszer leállását, így fontos hogy a hálózat sebezhető pontjai folyamatos ellenőrzés és elemzés alatt álljanak. A szoftver- vagy hardverhibából fakadó leállás elkerülhető, ha létezik az úgynevezett tartalék rendszer. A rendszer kritikus pontjait érdemes duplán biztosítani, hisz az elsődleges szoftver- vagy hardverelem kiesése esetén annak helyét átveheti a másodlagos eszköz, mely megakadályozza a rendelkezésre állás megszakadását.

Az internet bankinghoz szükséges szoftverek is meglehetően széles skálán mozognak, így nagy szabadsága van a felhasználónak a közöttük való választásban. A bank és a felhasználó oldaláról történő kompatibilitás a két fél közötti kommunikáció alapfeltétele.

Kiszervezés – outsorcing

További kockázat származhat abból is, hogy a bankok internet alapú szolgáltatásba gyakorta kénytelenek bevonni egy harmadik (külső) vállalkozást is, amely ezáltal mélyebb ismereteket és nehezen ellenőrizhető befolyást szerezhet a pénzügyi intézmény adott része felett. A bankok egyre gyakrabban használják az outsorcingot mint a költségcsökkentés és hatékonyságnövelés eszközét. A kiszervezésre támaszkodás meghatározó szerepet játszik minden banki szervezet kockázatokra való kitettségében, talán erőteljesebben is, mint más elektronikus kereskedelemben részt vevő szervezet számára. A nagyobb bankok sorra szervezik ki tevékenységeiket, aminek célja, hogy csak az alapvető üzleti célra kelljen koncentrálni. Számos esetben lépnek partneri viszonyba más szervezetekkel azon területeken,

melyek kívül esnek a fő tevékenységi körükön. (Hawke, 2000) A kis bankoknak viszont muszáj kiszervezniük a magas technológiai tudás- vagy eszközigényes területeket, annak érdekében, hogy működtetni tudják az elektronikus értékesítési csatornáikat. A kiszervezés költségvonzatának folyamatos csökkenése miatt a kisebbeknek egyre jobban megéri az e-bankinghoz szükséges infrastruktúra külső féltől történő beszerzése. A fent említett fejlődési tendenciák pozitív hatása, hogy nő a hatékonyság és lehetővé válik a kisebb intézmények számára is részt venni a versenyben. Ugyanakkor az operációs kockázat megnövekedésével kell számolni a folyamat miatt.

A nem megfelelő partner kiválasztása miatt okozott károk – például a bizalmas adatok illetéktelen kezekbe kerülése – egyértelműen a bank felelősségére róhatóak fel. A kiszervezéssel kapcsolatos kockázatok kezelése érdekében a bankoknak figyelemmel kell kísérniük a külső részt vevő cégben zajló eseményeket, folyamatokat is. A szerződésekben szereplő határidők betartásának és a szolgáltatás minőségének elérésének és fenntartásának ellenőrzése fontos a jogi kockázatok elkerülése végett.

2000-ben ismeretlen támadók feltörték a HSBC bank weblapját. A támadó a bank honlapján különböző követelésekkel állt elő a kormányzattal szemben. A londoni bank utólag nem győzte hangsúlyozni, hogy magát a honlapot nem a saját szakemberei üzemeltették, hanem egy külső cég. A weblapot üzemeltető cég nem megfelelő biztonsági rendszere tette lehetővé, hogy az ügyfelek körében komoly aggodalmat keltő támadást lehessen intézni az óriásbank ellen. Az ügyfelek megnyugtatására számos sajtótájékoztatón hangsúlyozták, hogy az on-line banki tranzakciók adatai nem forogtak veszélyben és nem kerültek illetéktelenek kezébe. (Mortimer, 2000) Biztosra veszem, hogy az eset nem tett jót a bank hírnevének. Habár a HSBC közvetlenül nem hibázott, de a külső fél által üzemeltetett honlap minősége, megbízhatósága az ügyfelek szemszögéből nagyban meghatározza a bank megítélését. Véleményem szerint a példa rámutat arra, hogy a hitelintézeteknek kiemelkedő figyelemmel kell eljárniuk a partnereik kiválasztásában, a fent leírt eset elkerülése érdekében.

Jogi kockázat

Jogi kockázat alatt a vonatkozó törvények, szabályok és rendelkezések megszegésének kockázatát értjük, melyet pénzügyi intézmény követhet el. A szabályok megszegésével a bankoknak, és főleg azok vezetőinek, sokszor bírsággal vagy egyéb más büntetésekkel kell szembenézniük. A szabályszegések is vezethetnek a jó hírnév elvesztéséhez, az üzleti lehetőségek beszűküléséhez, profiteséshez és a szerződések kikényszeríthetőségének megszűnéséhez.

Általánosságban azok a szabályok, melyek a hagyományos bankokra vonatkoznak, ugyanúgy vonatkoznak az elektronikus banki szolgáltatásokra is. Ide tartozik leginkább a fogyasztók védelme, akik elsősorban megfelelő biztonságot követelnek a tranzakciók lebonyolítása folyamán. (Comptroller's handbook, 1999) Ezen kí-

vül a banki titoktartásnak, a betétbiztosításnak és minden egyéb vonatkozó törvénynek meg kell feleli az internet alapú banknak is.

Azonban nem mindig világos, hogy hogyan lehet a hagyományos bankokra vonatkozó törvényeket és szabályokat implementálni a folyamatosan változó technológiai környezetben működő internetes bankokra. A kockázatokat figyelembe véve, a törvények és egyéb jogszabályok – melyek alanyai a világhálón szolgáltatásokat nyújtó pénzügyi intézmények – még tovább szigorodhatnak. Az internetes banki szolgáltatások eljuthatnak más országokban élő felhasználókhoz is, mely által a szabályozás összetettsége és bonyolultsága tovább fokozódhat, hiszen az egyes országok rá akarják kényszeríteni a bankokra a saját országuk azon törvényeit, melyek az ott lebonyolított tranzakciókra vonatkoznak.

Hitelkockázat

A hitelkockázat a pénzügyi veszteségek kockázata, melyet az intézmény azáltal szenved el, hogy az adósok vagy kötelezettek nem teljesítik a szerződésbe foglalt kötelezettségeiket. A hitelkockázat felfedezhető minden olyan tevékenység esetén, ahol az ügylet sikere függ egy harmadik fél (hitelező vagy adós) teljesítményétől.

A hitelintézmények e-banking tevékenysége többféle módon fejtheti ki hatását a hitelkockázatra. Az internet mint értékesítési csatorna segítségével még a relatíve kis vállalkozások is gyors növekedésre lehetnek képesek, ami megköveteli az eszközök magasabb minőségét és a kockázatok kezelésének fejlettebb módját. (Mann, 2003) A világháló hozzájárul az eddig elérhető piacok földrajzi értelemben történő expanziójához, s ez megköveteli az egyes piacok sajátosságainak, jellemzőinek és kockázati tényezőinek megértését.

A személyes találkozás, megismerkedés hiánya, az óriási földrajzi távolságok és a különböző biztonsági előírások ellenőrzésének nehézsége megsokszorozhatja a hitelkockázatot a bankok életében. A könnyebben ellenőrizhető földrajzi területen kívül eső hitelkihelyezések megnövekedése további kockázatot jelenthet. Az ügyfelek bonitás-, illetve a felajánlott biztosítékok vizsgálata és ellenőrzése szintén kihívást jelenthet egy területen kívül nyújtott kölcsön esetén.

A hitelkockázat vizsgálata tovább bonyolódik azzal a bizonytalan kérdéssel, hogy tulajdonképpen melyik ország törvényeit kell az egyes esetekben figyelembe venni.

A vezetőség számára egy olyan hitelportfólió menedzselése, melyet az interneten keresztüli értékesítéssel alakítottak ki, nagyfokú szakértelmet, gyakorlatot és a fő kockázatokra való éles rálátást kíván.

A fent említett hitelek esetében meg kell bizonyosodni arról, hogy az üzletszabályzat és az alkalmazott gyakorlat alkalmas-e és megfelelően működik-e a kockázatok kezelése területén.

Likviditási kockázat

A likviditási kockázatnak alapvetően két formája létezik. Az első, a piaci/termék-likviditás, mely a tranzakciók lebonyolí-

tásának lehetetlenségét jelenti a piac elégtelen likviditása miatt. (P. Jorion, 1999) Az internet banking szolgáltatások viszont likvid termékekre vonatkoznak. Magyarországon a bankok által nyújtott elektronikus befektetési lehetőségek kereskedelme esetén (állampapírok, befektetési jegyek, részvények) a terméklikviditás elégtelenségének veszélye nem áll fenn. A likviditási kockázat másik típusa, a pénzáramlási/finanszírozási likviditás, mely abból származik, hogy a bank nem tud eleget tenni kötelezettségeinek anélkül, hogy elfogadhatatlanul nagy veszteséget ne szenvedjen. (P. Jorion, 1999) A likviditási kockázat azon képesség hiányára utal, hogy előre nem tervezett események felszínre kerülése esetén a bank forrásait nem képes tovább finanszírozni. Továbbá a likviditási kockázat rámutat arra is, hogy a bank nem képes a piac változásait megfelelően érzékelni, illetve képtelen reagálni oly módon, hogy eszközeit pénzé tegye veszteségei minimalizálása érdekében.

Az a szédületes sebesség, mellyel a valódi és a dezinformációk mozognak az interneten, hatással lehet a bank likviditási kockázatára. Ellenséges szándékoktól vezérelve bárki könnyedén elhinthet akár igaz, akár nem igaz információkat egy bankról. Az interneten keresztüli elektronikus üzenőfalak, hírlevelek vagy fórumok könnyedén lehetővé teszik az ilyen típusú támadásokat. A rossz hírek hatására a betétesek tömegesen vehetik ki pénzüket a bankból a nap bármely időszakában. Összességében az internet tovább növelheti a bankbetétek volatilitását, hiszen könnyebbé válik az ügyfelek számára az egyes bankok közötti váltás. A likviditási problémák elkerülése végett több energiát kell a bankoknak fordítaniuk a betétállomány pillanatnyi nagyságárának ellenőrzésére, ami szoros összefüggésben lehet az ügyfelek e-banki aktivitásával.

Piaci kockázat

A piaci kockázat a jövedelemben vagy a tőkében bekövetkező változások, melyek a kereskedett portfóliók és pénzügyi termékek értékváltozásából adódnak. Ez a kockázattípus a kamatlábbal, a valuta- és devizaárfolyammal kapcsolatos üzletekből, valamint az értékpapír- és árutőzsdén való részvételből származik. Az interneten keresztüli különböző értékpapírokkal való kereskedelem felfutásának hatása a bankok kockázati profiljára meglehetősen összetett. Piaci szemszögből nézve, a világháló miatt az értékpapírok kereskedett mennyiségének megnövekedése egyrészt a piac likviditásának javulásához, másrészt viszont a volatilitás emelkedéséhez járul hozzá. Egy adott bank szempontjából viszont, az e-banking miatti értékpapír-bizományosi és értékpapír-kereskedelmi tevékenységek felfutásából adódóan, a bankok jobban ki vannak téve a piaci kockázatnak, mint korábban.

Valuta- és devizaárfolyamok mozgásából fakadó kockázat

Egy hitelintézet ki lehet téve a valutaárfolyamok változásából fakadó kockázatnak, ha külföldi ügyfelektől fogad el betétet,

vagy ha olyan számlát vezet, mely nem a hazai valutában denominált. Az interneten keresztüli banki tevékenységeknek viszont éppen az a legnagyobb előnye, hogy az ügyfelek földrajzi korlátozás nélkül választhatnak a hitelintézetek kínálatából. A világháló segítségével a bankok egyre jobban kiszélesítik piacaik földrajzi határait nemzetközi viszonylatban is, következésképpen ezek a szervezetek egyre inkább ki vannak téve az árfolyamok változásából fakadó kockázatoknak. Egy külföldi ország fizetési eszközének árfolyamát meghatározza a politikai, gazdasági, társadalmi és számos egyéb tényező, melyeket egy idegen országból nehézkes átlátni.

Magyarország tavaly májusi uniós csatlakozásával leegyszerűsödtek az európai bankok határon átnyúló szolgáltatásainak lehetősége. Az uniós székhelyű bankoknak nem kell a magyar ellenőrző hatóságtól (Pénzügyi Szervezetek Állami Felügyelete) engedélyt kérniük a működésre, csak regisztrációs kötelezettség van érvényben. A liberális feltételeknek köszönhetően a külföldi bankoknak nem kell létrehozniuk leányvállalatot vagy hazai fiókhálózatot a magyarországi működés érdekében, hanem csupán elektronikus úton is árulhatják szolgáltatásaikat és termékeiket az interneten keresztül. (HVG, 2005. január 28.)

ZÁRÓGONDOLAT

Az elektronikus kereskedelem egyre nagyobb térhódítása elkerülhetetlen, és meglehet, hogy ez lesz a jövőben az értékesítés fő csatornája. A hagyományos kereskedelem feltételeihez képest merőben új környezet azonban veszélyeket is rejt magában. A bank vezetésének és szakembereinek muszáj megérteniük és tisztán látniuk az internetes környezet okozta változásokat. Az új gazdaság alapját képező hálózatot el kell fogadniuk a bankoknak, és a versenyképesség megtartása miatt hatékonyan is kell működtetniük az elektronikus rendszereiket. Az internet számos lehetőséget rejt magában, melynek kihasználásával további növekedés érhető el a pénzintézetek számára. A hálózatnak persze megvannak a maga veszélyei is, melyekre tekintettel kell lenni a stratégia megalkotásakor. Az „új” kockázatok és fenyegetések figyelembevétele és megértése nélkül nagy veszélyeket rejt az elektronikus kereskedelmi platform alkalmazása.

IRODALOM

ANONYMUS [2003]: Infinit hírlevél. http://www.ittk.hu/infinit/2003/0508/index5.html

BARTHA LAJOS [2003]: Fizetési rendszerek az Európai Unióban. A Miniszterelnöki Hivatal Kormányzati Stratégiai Elemző Központ és a Külügyminisztérium közös kiadványa.

COLLINGE, ANDY [2004]: Strategic Management of E-Commerce Risk, Earnst&Young publications. http://www.hos.horizon.ie/presentations/bb040500/ernst_young.pdf

Comptroller of the Currency Administrator of National Banks [1999]: internet banking comptroller’s handbook http://www.occ.treas.gov/handbook/intbank.pdf

Deutsche Bundesbank [2000]: Monthly Report, Electronic banking from a prudential supervisory perspective. http://www.bundesbank.de/download/volkswirtschaft/mba/2000/200012mba_art03_ebanking.pdf

ENOS, LORI [2004]: Report: Critical Errors in On-line Banking. http://www.ecommercetimes.com/story/8867.html

Ernst and Young [2005]: Kockázatkezelési folyamat. http://www.ey.com/global/content.nsf/Hungary/Business_Risk_Kockazatkezelesi_Folyamat

FLEMING, NICK [2004]: Russian „spyware" hits on-line banks. http://telegraph.co.uk

HAWKE, JOHN D. [2000]: Electronic Banking Group Initiatives and White Papers, Committee for Banking Supervision. http://www.bis.org/publ/bcbs76.pdf)

JORION, PHILIPPE [2001]: Value at Risk. A kockáztatott érték. Panem, Budapest.

KOLOZSI SÁNDOR [2000]: Elektronikus kereskedelem, Fogyasztóvédelmi Főfelügyelőség. http://www.fvf.hu/fvf.php3?page=20059

MAGYAR NEMZETI BANK [2001]: Új nemzetközi pénzügyi szabványok bevezetése Magyarországon. MNB Pénzforgalmi önálló osztály kiadványa

MANN, ROBERT [2003]: internet Banking: A Risk Management Primer For Directors http://www.nubank.com/stories/12-05-01_internet-banking-for-directors

MCGANN, ROBERT [2005]: Phishing Attacks Surge in Last Six Months. http://www.clickz.com/stats/sectors/finance/article.php/3458321

MORTIMER [2000]: Támadás a HSBC bank ellen. http://www.sg.hu/cikk.php?cid=12856&PHPSESSID=dacf9c4cbb8b14f784f98494ac6d59af

NRC PIACKUTATÓ KFT. [2002]: A bizalom a részletekben van. http://www.nrc.hu/index.php?name=OE-News&file=index&page=details&news_id=249

PÁNCZÉL GÁBOR [2003]: A fejlődés ára. http://e-ker.hu/news.php?id=3340

Pricewaterhouse Coopers Technology Centre [1999]: E-Business Technology Forecast.

SZABÓ GÁBOR [2003]: Adatvédelem és on-line bankolás. http://e-ker.hu/news.php?id=3638

SZABÓ GÁBOR [2004]: On-line bankolókból élnek a csalók. http://e-ker.hu/news.php?id=4171

SZABÓ ZOLTÁN [2001]: Biztonsági kérdések. http://informatika.bkae.hu/root/Project/telepiac.nsf/0/92b077551d828a3dc1256a86002e5378?OpenDocument

SZABÓ ZOLTÁN [2001]: Pénzügyi Szolgáltatások. http://informatika.bkae.hu/root/Project/telepiac.nsf/0/4feaf380263f8e73c12569d60045297d?OpenDocument

TÓTH KRISTÓF [2003]: DoS támadás érte a Microsoft weboldalát. http://hirek.prim.hu/cikk/34317/