

XXXII. Országos Tudományos Diákköri Konferencia
Had- és Rendészettudományi Szekció
Gödöllő, 2015. április 15-17.
Szent István Egyetem Gazdaság- és Társadalomtudományi Kar
Nemzeti Közszerológati Egyetem

A bankkártyákkal való visszaélés gazdaságvédelmi vetülete

Jelige: Joker

Pályamunka lezárásának időpontja: 2014. március

2015.

Tartalomjegyzék

1. Prológus	4
2. A modern világ fizetési módjának kialakulása.....	7
2.1. Történelmi áttekintés	7
2.2. Kialakult fizetési formák	8
2.2.1. Csekk.....	10
2.2.2. Váltó	11
2.2.3. Bankkártya	13
2.2.3.1. Története	13
2.2.3.2. Fajtái, típusai	17
2.2.3.3. Működése	20
2.2.3.4. Előnyei, hátrányai.....	22
3. Bankkártya adatok megszerzése a kártyák fizikai jelenlétével	25
3.1. Ellopott vagy elvesztett kártyák.....	25
3.2. Kézi adatszerző.....	27
3.3. Adatszerzés POS terminálon.....	28
3.4. ATM-nél elkövetett kártya- (Card trapping), készpénz (Cash trapping) és adatlopás (Skimming)	29
3.4.1. Card trapping	30
3.4.2. Cash trapping	30
3.4.3. Skimming	31
3.4.3.1. Mágnescsík adatok illetéktelen személyek általi megszerzése	32
3.4.3.2. Elkövetők általi felszerelt kamerák, billentyűzetek	33
3.4.3.3. Egy trükkös eset	34
3.5. Prevenció.....	35

4. Bankkártya adatokkal való visszaélések a kibertérben (Cyber)	43
4.1. Adathalászat	44
4.1.1. Phishing.....	45
4.1.2. Pharming.....	46
4.1.3. Közösségi oldalak.....	47
4.1.4. Key logger alkalmazások.....	49
4.2. Adattárak feltörése.....	52
4.3. Botnet.....	53
4.4. Darknet – carding sites.....	56
4.5. Felderítési nehézségek	58
4.6. Prevenció.....	59
5. Esettanulmány	62
6. Jogi szabályozás	69
7. Statisztika	75
7.1. Visszaélések során felmerült kár a bankkártya üzletágban (ezer forint).....	75
8. Összegzés	87
9. Felhasznált Irodalom	90
9.1. Nyomtatott források.....	90
9.2. Internetes források.....	91

1. Prológus

A XXI. századra a világ egyre gyorsuló átalakuláson megy keresztül, melynek ütemét szinte semmi sem képes megállítani. Egyre inkább fejlődik, egyre inkább modernizálódik, újabbnál újabb technikai vívmányok látnak napvilágot és „asszimilálódnak” a világ részeként a különböző társadalmakba, civilizációkba. Mindez rengeteg pozitívummal rendelkezik. Többek között az internet egyre szélesebb elterjedésével, az online ügyintézés lehetőségével lehetőség nyílik a természet védelmére, ugyanis rengeteg fa kivágását, erdő kiirtását lehet megelőzni a világháló közreműködésével, mivel az anyagi megjelenés (papír alapú okiratok, igazolások) egyre inkább háttérbe szorul. Másik előnye a sok közül, hogy egy ember rengeteg időt tud megspórolni az interneten történő szinte bármilyen ügyének intézésével. Például nem kell hosszú sorokban állnia és várakoznia mondjuk a postán, vagy például az internetes áruházak megjelenése révén nem kell azzal időt vesztetnie, hogy valamelyik eladó, kisegítő tanácsot adjon neki egy-egy termékkel kapcsolatban, vagy akár hogy az általa kívánt, kiválasztott terméket megvásárolja. Egyszerű internetes átutalással megveszi a kívánt dolgot, és „csak” a kiszállítására vár. Nem kell otthonról kimozdulnia sem. Persze ennek szociológiailag negatív hatásai lehetnek a személy szellemi működésében, de ennek a témának a kifejtése egy külön szociológiai tanulmány lehetne.

Azonban nem csak a személy mentális helyzetében okozhat hátrányos következményeket a modern élet eme technikája. Ez a csúcstechnológia (high technology) ahol a legerősebb, ott a leggyengébb is. Ez miben is nyilvánul meg? A pénzintézetek azért is preferálják a készpénzzel szemben a bank,- vagy hitelkártyát, mert a kártyák működésének biztosítását kevesebb eszközzel, emberrel tudják megoldani, ennek következtében jóval kisebb költséggel jár használatuk. Arról nem is beszélve, hogy annyiival kevesebb felszerelést kell modernizálni, és ezt a pénzt a további fejlesztésekre lehet fordítani, melyek célja szintén a költséghatékony működés. Így fizikailag a pénzmozgás folyamatosan háttérbe szorul, és egyre inkább a számlákon történik.

Azonban a készpénz-helyettesítő fizetési eszközök elterjedése arra „buzdítja” a bűnözők egy részét, hogy az erőszakos vagyon elleni bűncselekmények helyett válasszák a modern bűnözés e válfaját, és váljanak „fehérgalléros” bűnelkövetőkké. Az elkövetők felismerték a gyors, viszonylag könnyű pénzszerzés „illatát”, és a hétköznapi emberek hitét, bizalmát, tájékozatlanságát, valamint nem utolsósorban a szakképzetlenségét kijátszva, kihasználva gazdagodnak meg illegálisan. A visszaéléseket nagy károkat okozva, rendkí-

vül szervezeten követik el az banki ügyfelek és egyben a bankok, pénzüzetek sérelmére. Kiletük megállapítása, stratégiák megismerése, a bünszervezetek felszámolása, és a büntetőeljárás lefolytatására gyakran a nemzetközi társszervekkel való együttműködéssel is nehezen valósul meg. Azért rendkívül fontos a nemzetközi kooperáció, mert eme bűnözői csoportokra jellemző, hogy az egyik országban megszerzett bankkártya adatokat egymásik, külföldi állam közigazgatási területén használják fel pénzszerzés céljából. Azonban, hogy a „fehérgalléros” bűnözés ellen hatékonyan fel lehessen lépni, egy adott országon belüli pénzüzeteknek és a rendőrségnek is szorosan együtt kell működnie egymással!

A téma szakszerű kifejtése érdekében a szakmai kérdésekben konzultációkat, megbeszéléseket folytattam és adatgyűjtést végeztem a Készenléti Rendőrség Nemzeti Nyomozó Iroda¹ Felderítő Főosztály Pénz- és Bankkártya-hamisítás Elleni Alosztály, valamint a KR-NNI Korruptió és Gazdasági Bűnözés elleni Főosztály Csúcstechnológiai Bűnözés Elleni Osztály szaknyomozóival², akik nem csak szakmai információkkal, javaslatokkal, hanem hasznos források megjelölésével, valamint észrevételeikkel segítettek egy tökéletes munka létrehozásában. Ezúton is szeretnék Köszönetet mondani, hogy engedélyezték azt, hogy a dolgozatom megírásánál rájuk támaszkodjak. Köszönöm a kitartásukat, szorgalmukat, segítőkészségüket!

A feldolgozás, kutatás során sokszor kerültek a kezembe idegen nyelvű anyagok, amelyek angol és német nyelvűek voltak. Ahhoz, hogy ezeket sikerüljön kellő mértékben felhasználni, olykor-olykor szükségem volt hallgatótársaim segítségére, akik fordításukkal rengeteg időt spóroltak meg nekem. Az Ő kitartó munkájukat is Köszönöm!

Bízom benne, hogy a sok energia befektetés meghozza hatását, és sikerült egy olyan művet elkészíteni és prezentálni, amely nem csak a rendvédelem területén nyújt segítséget, hanem a civil szférában is. Örömmel töltene el, ha az Olvasó számára a pár sorral fentebb említett mondatomat („... a csúcstechnológia ahol a legerősebb, ott a leggyengébb is.”) kellően megmagyaráztam, kifejtettem. A kutatómunkám során nem csak e téma kifejtésével foglalkoztam, hanem igyekeztem minél több olyan prevenciós megoldást találni, amellyel magunkat védeni tudjuk a bűnözői körökkel szemben.

Igyekeztem a lehető legfrissebb statisztikai adatokat beszerezni, és beépíteni az írásomba, amelyekről egy átlátható, érthető diagramokat kreáltam számszerűen megjelenítve

¹ Továbbiakban: KR-NNI

² Almádi János rendőr őrnagy, Makó Zoltán rendőr alezredes, Béres Csaba rendőr százados, valamint Poór Péter rendőr őrnagy

az egyes értékeket. Próbáltam rávilágítani a változások alakulásainak okára, megmagyarázni, hogy mi miért történhetett.

A téma kifejtéséhez hozzákapcsolódik a jogi szabályozás, melyhez alapul vettem a Nemzeti Közszolgálati Egyetem Rendészettudományi Karán oktatott Büntetőjog kurzusban tanultakat, a megírt tankönyveket, valamint konzultációkat folytattam Dr. Madai Sándor PhD. Úrral, aki véleményezte ezt a fejezetet.

Végül, de nem utolsó sorban Köszönetet Szeretnék mondani a kari (belső) konzulenseknek is, aki nélkül nem sikerülhetett volna a KR-NNI megkeresése és felkérése, hogy a külső konzulensi „szerep” ellátására biztosítson kiváló szakemberei közül néhányat.

A szerző

2. A modern világ fizetési módjának kialakulása

2.1. Történelmi áttekintés

Az idők folyamán, ahogy teltek-múltak az évek, évszázadok, évezredek, egyre jobban fejlődött a kereskedelem, amely az emberei szükségletek kielégítését célozta meg. Hogy miért lehetett probléma? Ha például egy ember valamit szeretett volna venni egy eladótól a piacon, de nála semmi olyan dolog nem volt, ami az eladónak hasznos lett volna, akkor el kellett mennie egy másik eladóhoz, hátha ott szerencsével jár, tehát több lépésős eljárásban juthatott az általa kívánt árucikkhez.

Erre rá is jöttek az adott korban élő emberek, és kialakult a kereskedelem egy közvetítő áru segítségével. Ezt kezdetben a só, a kagyló, az arany és az ezüst testesítette meg, de nem kellett sok idő, amíg ezeket felváltotta a fém. Ez egyszerűbbé tette a kereskedelmi tevékenységet, mert nem kellett azon egy vevőnek sem töprengeni, hogy mit adjon azért az áruért, amit szeretne, hanem adott egy bizonyos mennyiségű árupénzt. Az árupénz egy nagy értéket képviselő dolog volt. Azonban az árupénzt felváltotta a vert pénz, amit nemesfém-ből állítottak elő (először rézből, és vasból verték, majd később ezüsből és aranyból), és amit sokkal könnyebben lehetett kezelni.

Azonban az arany és ezüst nemesfémek bányászása egyre nehezebb feladattá vált a hiányuk miatt és emiatt nem tudták kielégíteni a kereskedelem pénzigényét, ezért a kereskedők azt a megoldást ötlötték ki, hogy váltókat bocsátottak ki, amelyek tanúsították a vevő fizetési ígérését. Sajnos, mivel ezt a módszert egyre több kereskedő kezdte alkalmazni, a váltók annyira szétterjedtek a piacon, hogy egyszerűen nem lehetett a hitelességüket kétséget kizáróan megállapítani.

A kialakult nehézségek megoldását a bankok megjelenése jelentette, mellyel ismét sikerült a kereskedelmet modernizálni és könnyebbé tenni. Ezek a pénzintézetek váltókat bocsátottak ki a forgalomba, melyekből kialakultak a papírpénzek (bankjegy), amelyeket bármikor nemesfémpénzre lehetett beváltani. A bankok további szolgáltatásokat tudtak nyújtani, melyekből további bevételek származott. E körbe sorolhatjuk a pénzügyi tanácsadást, tranzakciós szolgáltatást, valamint a készpénz-helyettesítő fizetési eszközök szolgáltatását: bankkártyák, hitelkártyák kiállítása, kibocsátása, az ezekhez szükséges pénzkidó automata-k kihelyezése és üzemeltetése.³

³ Forrás: <http://ecopedia.hu/penz-tortenete>

2.2. Kialakult fizetési formák

Az idők folyamán többféle fizetési módszer alakult ki. Az egyik legjelentősebb, és a mai napig gyakran alkalmazott fizetési forma a *készpénz*. Rengeteg előnye van. Egyik legfontosabb, hogy meg tudom számolni, mennyi van belőle, ki tudom számolni, hogy mennyit tudok elkölteni egy vásárláskor például, amiből az következik, hogy mínuszba nem tudok kerülni. Bárhol lehet vele fizetni, nincs olyan hely, ahol nem fogadják el. Azonnali tranzakciót biztosít. Azonban a sok előnye mellett akad hátránya is. Például, ha valamit nagy összegért cserébe tudok megvásárolni, akkor sok készpénznek kell az embernél lenni, ami veszélyes is lehet, mert fertőző lehet, vagy olyan pszichés hatása lehet a sok készpénznek, hogy a metakommunikáción kitűnik, ugyanis a legtöbb ember ha sok pénzt tart magánál feszélyezve érzi magát, ideges, és akár a mozgása is akadozott lehet. Ezt pedig az utcán nevelkedett, profi bűnözők könnyen kifigyelhetik, és már is egy potenciális áldozat lehet a személyből.

Egy másik fizetési forma a *készpénz nélküli fizetés*. Itt a személy egy bankszámlaszámmal rendelkezik, és egy megbízást ad a hitelintézetnek, amely a következő műveleteket foglalhatja magába:

- Átutalás: a számlatulajdonos az általa meghatározott summát utalja át a szintén általa megadott bankszámlára (ez a jogosult bankszámlája). Ez a tranzakció a megbízó számláját terheli meg értelemszerűen.⁴
- Beszédési megbízás (inkasszó): a számlatulajdonos megbízza a számlavezető pénzügyintézetét, hogy a meghatározott összeget a bankszámlája javára, és a kötelezettek bankszámlái terhére szedjen be. Ez gyakori eset például a közműdíjak vagy telefonszámlák beszedésénél.”
- Akkreditív: egy kiállított fizetési ígérvény, amely visszavonhatatlan pénzfizetési garanciaként szolgál, tehát ha a kedvezményezett teljesíti a feltételeket, a pénzügyintézetnek kötelessége a meghatározott összeget kifizetni. Leginkább az árukereskedelemben alkalmazzák ezt a műveletet. A fizetések biztonságára érdekében kötelező érvényű nemzetközi szabályok vonatkoznak a fizetési művelet alkalmazására.⁵

Végül, de nem utolsó sorban, egy harmadik kialakult fizetési formáról, a *készpénz kímélő fizetéséről* beszélnek. „A készpénz kímélésének vagy helyettesítésének az tekinthető,

⁴ Dr. Sági Judit: Banktan, Saldo Kiadó Budapest, 2007

⁵ Kónya Judit: Banküzemeltetési alapismeretek. Budapest: Közgazdasági és Jogi. 1994. 226–234. o.

ha a készpénz ki- vagy a befizetés során csak az egyik oldalon jelenik meg valós, fizikai formájában, a másik oldalon már egy ettől eltérő, készpénz nélküli fizetési módozatról (terhelésről és jóváírásról) van szó. Ezért nagyon fontos megkülönböztetni egymástól a bankszámlapénz és a készpénzkímélő forgalmat, mert ugyan a bankszámlapénz is készpénz nélküli, azaz láthatatlan, de mindkét oldalán, azaz a terheléseknél és a jóváírásoknál is az. Ezzel szemben, a készpénzkímélő és helyettesítő módozatok alkalmazását mindig megelőzi vagy követi a készpénzmozgás, azaz egyik lábával a készpénz, a másikkal a bankszámlapénz talaján áll.”⁶ De milyen eszközök tartoznak ebbe a fizetési formába? Ezen eszközök meghatározását célszerű a dolgozat címéből levont következtetés alapján meghatározni, ugyanis a rendőrségi munka egyik alappillére a büntető anyagi jog rendelkezései képezik, amelyek alapján tudjuk az egyes cselekményeket minősíteni. Ez a törvény a Büntető Törvénykönyvről szóló 2012. évi C. törvény. E törvény 459 § (1) 19. pontja értelmében készpénz-helyettesítő fizetési eszköz a hitelintézetekről és a pénzügyi vállalkozásokról szóló törvényben⁷ (továbbiakban: Hpt.) meghatározott készpénz-helyettesítő fizetési eszköz és a forgatható utalvány, a kincstári kártya, az utazási csekk, a kifizetőt terhelő adó mellett vagy adómentesen adható, korlátozott körű áruk vagy szolgáltatások ellenértékének kiegyenlítése céljából törvény alapján kibocsátott utalvány és a váltó, feltéve, hogy kivitelezése, kódolása vagy a rajta lévő aláírás folytán a másolás, a meghamisítás vagy a jogosulatlan felhasználás ellen védett. A Hpt. 6 § 55. pontjában határozza meg a készpénz-helyettesítő fizetési eszközök fajtáit, mely a csekk, az elektronikus pénz és a pénzforgalmi szolgáltató és az ügyfél közötti keretszerződésben meghatározott olyan személyre szabott dolog vagy eljárás, amely lehetővé teszi az ügyfél számára a fizetési megbízás megtételét. Utóbbiban tudnák említeni a többek között váltót, bankkártyát, a hitelkártyát. A bankkártya egyre szélesebb körben terjed el rohamosan fejlődő világunkban, a XXI. században, ugyanis használata gyors, egyszerű, kényelmes. A tulajdonosa a kártyával készpénzt vehet fel és vásárlási valamint egyéb tranzakciós eljárásait bonyolíthatja le.

A szakdolgozat terjedelmi korlátai miatt először pár sorban ismertetném a csekk, a váltó, valamint az elektronikus pénz egyéb jellemzőit, majd a bankkártyával kívánok részletesebben foglalkozni, itt külön kitérve a működésére, fajtáira, típusaira, ezek jellemzőire, előnyeire, hátrányaira, valamint milyen visszaélések elkövetési tárgyává válhat.

⁶ Dr. Huszti Ernő Banktan, Tas Kft. 2002.

⁷ 2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról, mely 2014. január 1-én lépett hatályba, hatályon kívül helyezve az 1996. évi CXII. törvényt.

2.2.1. Csekk

A csekk egy olyan készpénz-helyettesítő értékpapír, és értékpapír voltából jogi szempontból úgy határozhatjuk meg, hogy „olyan okirat, amely a benne tanúsított alanyi jogot úgy testesíti meg, hogy azt a papír nélkül sem érvényesíteni, sem bizonyítani, sem átruházni nem lehet.”⁸ A



csekket kibocsátó

1. kép

arra utasítja a hitelintézetét a csekk kiállításával, hogy az fizesse ki a csekk birtoklójának a meghatározott összeget. Ezt a bank csak akkor teheti meg, ha a csekkre vonatkozó formai követelményeket teljes mértékben teljesítették. Természetesen ezen felül még szükséges, hogy a számlatulajdonos kössön a bankjával egy csekkszerződést, amelynek birtokában jogosult csak csekk kibocsátására. A kiállításával azonban nem fizetés történik. A kifizetésre csak akkor kerül sor, ha a csekk birtokosa elmegy a bankba beváltani. Persze a bank csak akkor váltja be, ha a már említett alaki követelményeknek a csekk megfelel. A csekknek tartalmaznia kell:

- a csekk elnevezést az okirat szövegében, éspedig az okirat kiállításának nyelvén;
- a határozott pénzösszeg fizetésére szóló feltétlen meghagyást;
- a fizetésre kötelezett nevét (címzett);
- a fizetési hely megjelölését;
- a csekk kiállítási napjának és helyének megjelölését;
- a kibocsátó aláírását.⁹

⁸ Balogh László et al. Pénzügytan II., 1999., 143. o.

⁹ 2/1965. (I.24.) IM rendelet 1 § (1)

A csekk szólhat

- megnevezett személy rendeletére: a csekk forgatással átruházható, úgy mint a váltó
- megnevezett személyre: a meghatározott összeg csak annak a személynek fizethető ki, akinek a nevét a csekk tartalmazza. Ebből az következik, hogy ez a fajta nem forgatható.
- bemutatóra: a kifizetést annak a személynek kell teljesíteni, aki a csekket a kiállítás napjától megszabott határidőn belül bemutatja. Ez a fajta is forgatható az alakiasságok betartásával.

A csekk alaki és jogi szabályozását a 2/1965. (I.24.) IM rendelet adja.

2.2.2. Váltó

A váltó egy olyan forgatható értékpapír, amelynek kiállítója arra vállal kötelezettséget, hogy a váltón meghatározott összeget a meghatározott helyen és időben, saját maga vagy harmadik személy meg fogja fizetni a váltó jogosultja részére. Mint a fogalmi meghatározásból láthatjuk, a váltó is egy értékpapír, hisz a pénzkövetelést megtestesítő értékpapírok közé tartozik. Két formáját különböztetjük meg. Az egyik a saját váltó, amelyen a kibocsátó saját maga tesz nyilatkozatot arról, hogy a kedvezményezett részére teljesíti a fizetési kötelezettségét egy későbbi időpontban. A másik formáját idegen váltónak nevezzük, amelyben a kibocsátó felszólítást tesz a címzettnek, hogy a váltóban meghatározott és feltüntetett összeget a kedvezményezettnek fizesse meg. Ennél a váltó típusnál szükséges a címzett aláírása is, mert ő az, aki hozzájárulását adja a kifizetéshez. A váltó értékkel, és névértékkel is rendelkezik. Az érték lehet áru vagy szolgáltatás, a névérték meg már tartalmazza a kamatot is.

Az idegen váltó kellékei

Kibocsátva:.....keretében	Kelt: 2008. ...2.....
1 VÁLTÓösszegről	
.....3.....-án fizessen Ön ezen VÁLTÓ -nál fogva	
.....4.....-nak vagy rendeletére	
.....5.....összeget	
Címzett:.....6.....	Kibocsátó:.....7.....
.....	
Fizetés helye:.....8.....(Bank)	
Elfogadva:.....	

2. kép

A váltó használata során az ügyletben szereplők köre aszerint alakul, hogy melyik váltóformát kívánjuk kiállítani. Saját váltó esetében kétszereplős modellt tudunk felvázolni. Az egyik szereplő a kibocsátó, aki a váltóban egy későbbi fizetést ígér, a másik személy pedig a rendelvényes, akinek, vagy aki rendelkezése szerinti kedvezményezettnek ígéri a fizetést. Az idegen váltónál ez a modell egy harmadik személlyel bővül ki. Itt ugyan úgy,

mint a saját váltó modelljében, van egy kibocsátó, aki az a személy, aki a címzettet fizetésre szólítja fel. Ez a címzett lesz az a szereplő, aki a saját váltónál nem jelenik meg. A címzett az a személy, akit fizetésre szólít fel az intézmény. Jelen van még a rendelvényes, aki nek a rendelkezése szerint a fizetést teljesíteni kell.

A váltónak ahhoz, hogy kibocsátása érvényes legyen, bizonyos törvényi kellékeket tartalmaznia kell, melyek a következők:

- a váltó elnevezése
- határozott pénzösszeg fizetésére szóló feltétlen megbízás
- a fizetésre kötelezett (címzett) neve
 - ez csak az idegen váltón kötelező tartalmi kellék, a saját váltón elhanyagolható
- az esedékesség megjelölése
- a fizetés helyének megjelölése
- a kedvezményezett neve
- a váltó kiállításának helyének és napjának megjelölése
- a kiállító aláírása.

A váltóval végezhető ügyletek közé soroljuk például a leszámítolást. A leszámítolás az a pénzügyi ügylet, amikor a váltó birtokosa eladja a váltóját a banknak az esedékesség előtt. Ebben az esetben a pénzintézet leszámolja a névértékből az esedékességig jelentkező kamatot, így az eladó a csökkentett értéket kapja meg, és az adós majd a banknak kell, hogy teljesítsen. A hitelintézeteknek pedig további lehetőségük is van a váltóval, ugyanis a már leszámított váltókat a jegybanknál (Magyarországon a Magyar Nemzeti Bank [MNB]) viszontleszámíthatják. Ilyenkor a bank az MNB-nek adja el a leszámított váltóját.¹⁰

A váltó alaki és jogi szabályozását az 1/1965. (I.24.) IM rendelet adja.

¹⁰ Trefort Ágoston Két Tanítási Nyelvű Fővárosi Gyakorló Szakközépiskola, Dr. Forgách Ádám 2009. év január hó 29. napon leadott oktatása nyomán

2.2.3. Bankkártya

2.2.3.1. Története

Az első kártya formátumú tárgyak, amelyekkel kedveskedtek az ügyfeleknek, az 1914-es években „láttak napvilágot”, még az első világháború kezdete előtt. Ezek közül az egyik egy hűségkártya volt, amelyet a Western Union nevű egyesült államokbeli szervezet állított ki. Vele együtt jelent meg még a fém telegramkártya, ami a telefonkártya elődjének felel meg, valamint még ezek között kell megemlíteni a Sears amerikai áruházóriás első hitelkártyáját. Ezeket a kezdetleges törekvéseket a MobilOil által kibocsátott hitelkártya követte, amiket a legjobb ügyfelek birtokába adtak.

A készpénzkímélő és –helyettesítő eszközök és rendszerek fejlődésének az első világháború, valamint a kicsit később tomboló gazdasági világválság (1929) keresztezte az útját. Ez a negatív hatású időszak egészen a második világháború végéig uralkodott. A legenda szerint egy amerikai bankár étkezése után vette észre, amikor már hozták neki a számlát, hogy nincs miből kifizetnie az ebédjét. Ez a szituáció teremtette meg a „második Arkhimédészi csodát”, ugyanis a bankár így találta fel azt a bankkártyát, amely egy bankhoz kapcsolódik, lehetővé téve azt, hogy szinte mindenhol fel lehet használni. A bank kifizeti a vásárláskor felhalmozott összeget, és azt később követeli az ügyfelén. 1950-ben az a bank, ahol a legenda főszereplője is dolgozott, a Hamilton Credit Corporation adta ki az első olyan bankkártyát, ami bankhoz kötődött. Ez volt a Diners Club. Ez egy utazási és szabadidő kártya volt, mely mellé a kibocsátó bank adott egy prospektust, ahol felsorolta azokat a vendéglátó ipari egységeket, ahol a kártyát elfogadják.

Az első, ténylegesen a mindennapi vásárlásra alkalmas plasztik hitelkártyát 1951-ben dobta piacra a Franklin National Bank. Mind a mai napig ez jelenti a ma működő hitelkártya-rendszer alapkövét. Az akkori rendszer azon az elven működött, hogy ha valaki meghaladta az engedélyezett limitet, a kereskedőnek fel kellett hívnia a bankot, és az összeg leemelésére felhatalmazást kellett kérnie. Ez már egy nagy áttörést ért el abban az időben. Több kisebb pénzintézet is állított ki hitelkártyát ügyfeleinek. Úgy tűnt, nem kifizetődő egy ilyen rendszerbe befektetni és fejleszteni, hisz a várt profit nem érkezett meg. Ámde 1958-ban a fejlettebb bankok is elkezdtek érdeklődni a hitelkártyák iránt, köztük lehetne megemlíteni a Bank of American nevű pénzintézetet. Ez a bank még ugyanebben az évben kiállította az American Express szabadidő és utazási kártyáját, valamint később, a mai Visa kártya honatyját, az Americard-ot. Ennek konkurens kártyáját az Inter Bank adta ki, ugyanabban az évben, ami a Master Card elődjét testesíti meg. Ezt a kártyát Master

Charge-nek becézték. A fejlődési mechanizmus ennek hatására exponenciálisan növekedve folytatódott. Megalakultak a bankkártya-szövetségek, mint például az Interbank Card Association és a Charge Master a '60-as években. Miután elkezdtek működni, üzletpolitikájukat abba az irányba terelték, hogy egy esetleges egyesüléssel sokkal nagyobb profitra tudnak szert tenni. Sikerült is mindenben megegyezniük, így hát 1967 után egy szervezetté olvadtak össze.

Az amerikai vizekről átevezve az európai hullámokra, magunkkal hozva az amerikai áramlatot a kontinens nagyobb országában is elindultak az úttörő bankok törekvései. Köztük említeném meg a nagy-britanniai Barclaycard¹¹, amely a Barclays Bank PLC. kereskedelmi neve és kártyája. Ez a bank a XXI. században is Nagy-Britannia egyik vezető bankja. köztudott róla, hogy az angliai első osztályú labdarúgó liga (Premier League) elsődleges, hivatalos támogatója. Említhetném még a Franciaországban székelő Francia Rothschild bankot, ami forgalomba hozta a Carte Bleue névre hallgató bankkártyáját. Ezen a földrészén az első kooperáció az 1967-es évben jelent meg. A svéd és a francia együttműködés eredményeként megszületett az Eurocard, ami kezdetben szállodai és éttermi szolgáltatásokkal vétette észre magát a piacon.

A hitelkártyákon megjelentek a kártya, a kibocsátó bank és a kártyabirtokos neve, valamint a kártyaszám, az érvényességi dátum és végül, de nem utolsó sorban egy aláíráscsík. Kicsivel később megjelent a dombornyomott kártya is, mellyel a biztonságot igyekeztek növelni. A mágnescsík, mint kártyatartozék csak akkor lehetett a kártya része, amikor az International Standardization Organisation (továbbiakban: ISO) kidolgozta és elfogadta a szabványát.

1968-ban megjelentek az első pénzjegykiadó automaták (ATM¹²), melyből az első darabot Párizsban üzemelték be. Ezzel lehetővé vált a kártya tulajdonságainak és szolgáltatásainak modernizálása, ugyanis a kor kártyái már alkalmasak voltak készpénz felvételére. Annak érdekében, hogy a modernizációs törekvés mellett a töretlen bizalom is megmaradjon a kártyákban, mágnescsíkot és PIN-kódot¹³ is használtak.

Ugorva egy kicsit az időben, de még európai bankkártya történelmet boncolgatva, 1978-ban megalakult a Visa International Service Association. Egy évre rá a Visa összes kártyáját felszerelték mágnescsíkkal. Megkezdődtek az ATM automaták telepítési folya-

¹¹ <http://www.barclaycard.co.uk/personal>

¹² **Automated Teller Machine**: olyan elektromechanikus berendezés, mely lehetővé teszi a készpénz-felvételt valamint más szolgáltatások igénybevételét. (forrás: <http://hu.wikipedia.org/wiki/Bankautomata>)

¹³ **Personal Identification Number**= személyi azonosító szám: egy olyan titkos kód, mely személyes szolgáltatásokat véd (Forrás: http://hu.wikipedia.org/wiki/PIN_k%C3%B3d)

mata is. Egyre több helyen installálták őket, könnyítve a készpénzfelvételt. 1981-ben az Interbank Card Association MasterCard International-re változtatta nevét, és szorosabb együttműködésbe fonódott az Eurocard International-lel.

Tovább haladva keletre, de még Európában maradva, elérkezünk a magyar vizekre. Természetesen a magyar bankkártya keletkezésének is van egy legendája, mint sok más dolognak. A történet úgy hangzik, hogy egy magyar bankár, aki a Magyar Külkereskedelmi Bank (továbbiakban: MKB) alkalmazottja volt, Amerikában volt üzleti úton. Azt tudni kell róla, hogy csak egymás után szívta a cigarettát. Történt egyszer, hogy egy éjszaka kifogyott a tobacco-ból. A szállodája recepciójánál kívánta hiányát pótolni, de nem tudta megtenni, ugyanis a hotelben csak bankkártyával lehetett fizetni, az pedig a magyar bankárnak nem volt. Ennek hatására az MKB tárgyalásokba kezdett a Visa International-lel, ami addigra már eléggé közismert volt Amerikában és az nyugat-európai országok többségében. A tárgyalás eredményeként 1988-ban Magyarországon is bekerült a piacra az első bankkártya. Kezdetben csak devizabetéttel rendelkező cégek kaphattak, de később már magánszemélyek is igényelhettek kártyát. 1989-ben az Országos Takarékpénztár (OTP) is kiállította saját bankkártyáját, melyet mágnescsíkkal is ellátott. Ezzel a kártyával az ügyfelek a kihelyezett ATM automatáknál készpénzt is fel tudtak venni. Forint alapon működött, de nem rendelkezett még nemzetközi logóval (EC/MC), ezért nemzetközileg még nem lehetett hasznukat venni. Azonban erre sem kellett sokat várni az ügyfeleknek, hisz az MKB, az OTP de még a Budapest Bank is belépett az EC/MC emblémás kártyakibocsátók körébe. Ezzel arra ösztönözték a többi Magyarországi pénzintézetet, hogy minél előbb lépésre szánja el magát, ami kiválóan segítette a bankkártya üzletág fejlődését, modernizációját. A hitelintézetek belátták azt is, hogy a kártya fejlesztése csupán csak egy út a siker felé, amit szélesíteni lehet és kell. Elkezdtek az ATM automaták modernizációját is.

A bankkártya „életútja” rendkívül színes, szerteágazó, az egész világot átölelő „karrier”, melynek során különféle változatai, típusai jelentek meg, színesítve a világát. Még mielőtt azonban megismerkednénk velük, célszerű először is tisztába kerülnünk, mi is tulajdonképpen a bankkártya.

Mi micsoda a bankkártyán?

Az elején látható adatok:

1. A bankkártya tulajdonosának a neve.
2. A bankkártya száma.
3. A bankkártya kiállításának a dátuma.
4. A bankkártya lejáratának a dátuma.

A hátulján látható adatok:

5. A bankkártya biztonsági száma, CVV. Ez általában az utolsó három számjegy, amely internetes vásárlása is alkalmas, dombor nyomott kártyákon szerepel. (A képen be is van karikázva.)



3. kép

Egységes, mindenki által elfogadott definícióra nem bukkantam, így hát igyekeztem minél több helyről beszerezni egyet, melyből általánosítani lehet. Először nyomtatott forrásokban kerestem fogalmi meghatározást, erre pedig a legjobb könyv a Magyar Értelmező Kéziszótár¹⁴. „A tulajdonosa számláján levő összeg erejéig készpénz felvételére és áruk, tások kifizetésére jogosító, névvel ellátott és azonosító kóddal használható, kártya alakú műanyag lap.”

A keresgélésem kiterjedt a világháló tartalmaira is, ahol a következő definiálások keringenek.

1. „A bank által kibocsátott bankszámla alapú, elektronikus fizetési eszköz, amely lehetővé teszi a számla feletti rendelkezést.”¹⁵
2. „A bankkártya egy modern készpénzkímélő fizetési eszköz. A bankkártya valamely bank, vagy bankkártya-társaság által kibocsátott, mágnes csíkkal ellátott plasztik lap. Alkalmas vásárlásra és készpénzfelvételre egyaránt. Névre szól, ez lakossági bankszámla esetén magánszemély, céges vagy vállalkozói bankkártyák esetében a cég neve ill. a kártya használatára feljogosított személy is lehet. A bankkártya tulajdonosa minden esetben az azt kibocsátó bank.”¹⁶
3. „A bankkártya egy olyan készpénzfizetést helyettesítő eszköz, melyet a bank ad(hat) a nála számlát vezető ügyfeleinek. Szinte mindegyik bankszámlához kapcsolódhat valamilyen típusú bankkártya. Használatával lehetőség van vásárolni és ATM-ekben készpénzt felvenni.”¹⁷
4. „A bankkártya hitelintézetek által kínált készpénz-helyettesítő és -kímélő fizetési eszköz. A kártya birtokosa az adott banknál vezetett számla terhére fizethet, vagy vehet fel pénzt. A bankkártyák szabványmérete: 86 x 54 x 0,76 mm. A kártyán található mágnescsíkon, vagy mikorchipen található adatok alapján történik a fizetés, a birtokos személyazonosságának elektromos vagy személyes úton történő ellenőrzésével. Fontos, hogy a kártya tulajdonosa a hitelintézet marad, amely csak meghatározott időre bocsátja az ügyfele rendelkezésére a kártyát.”¹⁸

¹⁴ Magyar Értelmező Kéziszótár Tintakönyvkiadó Budapest, 2007. I. kötet 81. o.

¹⁵ <http://meszotar.hu/keres-bankk%C3%A1rtya>

¹⁶ <http://penzugy.uw.hu/fogalomtar>

¹⁷ <http://www.bankracio.hu/fogalom/187-bankkartya>

¹⁸ <http://ecopedia.hu/bankkartya>

5. „Pénzintézet által kibocsátott, szabványméretű műanyag lap, segítségével banki számlához vagy hitelkerethez lehet hozzáférni. Egyes kártyatípusokkal (ATM-kártya) csak készpénzt lehet felvenni a bankjegykiadó automatákból és bankpénztáránál, esetleg postahivatalokban, az elektronikus kártyákkal emellett vásárolni is lehet, de csak olyan üzletekben, ahol a pénztárgép és a banki számítógéppont között közvetlen kapcsolatot teremtő készülék (POS terminál) van. A dombornyomású kártyák, amelyeken a kártyabirtokos neve, a kártya sorszáma és lejáratának ideje valóban kidomborodik, pénzfelvételen és vásárláson kívül használhatóak például interneten vagy postán való rendeléshez és olyan éttermekben, szállodákban, üzletekben is, ahol nincs ugyan POS-terminál, de az adatokat rögzítő lehúzás kártyaelfogadó készülék működik. A legegyszerűbb kártyák éves díja és a velük való visszaélés lehetősége a legkisebb. A kártyabirtokos számára díjmentes a kártyahasználat, ha vásárol vele, a pénzfelvétel azonban annak helyétől függően díjköteles. A bankkártyákon mágneses csík (vagy elektronikus chip) rögzíti a gépi azonosításhoz szükséges adatokat.”¹⁹

Most, hogy több oldalról meg megismertük a bankkártyát, megismerkedhetünk egy egyes változataival.²⁰

2.2.3.2. Fajtái, típusai

Több halmazt is tudunk képezni, amelyek szerint a bankkártyáknak helyet adhatunk világukban. Az egyik ilyen halmaz tartalmazhatja a kártyákat fajtájuk szerint. A következőkképpen jelenik meg:

- Előre fizetett kártya (prepaid card): egy olyan kártya, amelyet a kiváltója egy előre meghatározott összeggel szerez meg. Ezt az összeget vagy a kártya, vagy a mögötte lévő számla tárolja. Ezt a kártyát leginkább készpénz felvételre, illetve vásárlásra használjuk. A kártya addig használható, amíg az az összeg, amivel megváltották, el nem fogy. Egyes fajtáit újra lehet tölteni, mások fajtáit pedig a használat után el lehet dobni. Van egy speciális fajtája is, amit elektronikus pénztárcának hívunk. Ezt bármikor újra fel lehet tölteni, amelyet a kártya elektronikus pénz formájában tárol. Ez azonban lehetővé teszi a kártya birtokosa számára, hogy számlakapcsolat illetve kész-

¹⁹ <http://www.enc.hu/1enciklopedia/mindennapi/bankkartya.htm>

²⁰ E alfejezet megírásakor nagyban támaszkodtam az alábbiakra:
<http://www.bankkartya.hu/hirkegategoria/sajtoszemle/cikk/359-a-hitelkrtya-trtnete>
<http://www.bankweb.hu/a-bankkartya-tortenete/>

pénz nélkül tudja felhasználni. Olyan piaci területen fordul elő, ahol olcsóbb árut kell kifizetni. Ilyen lehet például a parkolójegy automata.

- Betéti kártya (debit card): a bankkártyák ezen fajtája egy bankszámlához kapcsolódik, ami a bankkártya birtokosáé. A számla tulajdonosa a számláján lévő limit erejéig tudja a betéti kártyát igénybe venni. A kártyával végzett műveletek esetén a bank a kártyához tartozó számlát megterhelheti, bár most, aki nyilatkozik arról, hogy ingyenesen szeretne készpénzt felvenni, neki minden egyes hónapban 150. 000 Ft értékig teheti meg, egy hónapban kétszer. Ha bármelyik limitet túllépi a kártya birtokosa, a pénzügyintézet megterheli a kártyához tartozó számlát. A betéti kártyához tartozó folyószámla bármikor, bármekkora egységgel feltölthető.
- Hitelkártya (credit card): ez a kártyatípus egy meghatározott összegű hitelkerethez tartozik, melynek értékét bank és az ügyfél közötti szerződés határozza meg. A hitelkeretet általában az igazolt nettó jövedelemhez igazodik. A kártyabirtokos a maximum hitelkeretig kap kölcsönt a banktól. Kijelölt időközönként a bank küld egy számlakivonatot a kártya birtokosának, melyben feltünteti az összeget, amit vissza kell fizetni, valamint megjelöli ennek határidejét is. Azt nem határozza meg a hitelintézet, hogy egyben kell visszafizetni avagy sem. Ezt a kártya birtokosa döntheti el. Ha a vevő a meghatározott határidő végéig teljes mértékben visszafizeti a „kölcsönt”, kamatmentes periódus következik. Amennyiben nem fizeti meg, vagy nem a teljes összeget téríti meg határidőre, akkor a kamat mértéke úgy alakul, hogy megnézik a felhasznált hitelkeret összegét, és ez alapján számolják fel.
- Terhelési kártya (charge card, delayed debit card): ez a kártya azon a működési elven működik, mint a hitelkártya, annyi különbséggel, hogy a tartozást ennél a típusnál a bank által meghatározott határidőig a teljes összegre vonatkozóan ki kell egyenlíteni.

Egy másik halmaz a technikai felszereltségük alapján rendszerezné a bankkártyákat. Technikai szempontból a következőket különböztetjük meg:

- Mágnescsíkos kártya: a kártya hátoldalán, szabványszerűen helyezkedik egy fekete csík, amely ferromágneses részecskéket tartalmaz. Ez alkalmas adatok tárolására, amely adatok azonosítják az országot, a bankot, az ügyfe-

let, a kártyát. További információként hordozza a PAN²¹ számot, ami a számlaszám, a kártyabirtokos neve és a kártya érvényességi ideje; a CVV²² (Visa kártya esetén) vagy CVC²³ (Europay esetén) számot, ami három számjegyből áll és a kártya ellenőrző kódja. A kártyához tartozik egy négyjegyű PIN-kód, ami elektronikus aláírásként funkcionál. On-line rendszereknél használható.

- Dombornyomású kártya: a kártya szintjéből a kártyabirtokos neve, a PAN-kód és a kártya érvényességi ideje kiemelkedik. Kezdetben Off-line-os vásárlásra használták. Ezzel a kártyával az összes POS terminálon lehet fizetni, valamint az ATM automatáknál készpénz felvételére is alkalmas. Az interneten történő vásárlás is ezt a kártyát privilegizálja.
- Chipes kártya: a kártyára és annak tulajdonosára vonatkozó adatokat egy mikroprocesszor tartalmazza, mely a kártya tartozékát képezi. Ezzel növelték a bankkártya biztonsági rendszerét. A chip segítségével a kártya tartalma írhatóvá és olvashatóvá vált. Rögzíti a tranzakció adatait is. Mivel ilyen modern technológiát tartalmaz, ezért nagyon drága. On-line és Off-line rendszeren egyaránt használható.
- Hibrid kártya: a dombornyomású és a mágnesescíkos kártya, illetve a mágnesescíkos kártya és a chipes kártya ötvözetéből született meg. Előnye, hogy ez is On-line és Off-line rendszereken egyaránt elfogadott. Általában azért kérnek ilyen tulajdonságú bankkártyát, hogy azokban az államokban, ahol még a technológia nem olyan fejlett, hogy chipes kártyát tudjanak olvasni, illetve kezelni, ott is tudják a vevők a kártyáikat használni. Fontosnak találok megemlíteni, hogy a hibrid kártyának két, ma már közkedvelten internetes vásárlásoknál használt fajtája terjedt el. Az egyik ilyen hibrid kártya a *PayPass kártya*²⁴. „Egy érintés nélkül használható, pici rádióadót tartalmazó kártya, amit ha elég közel tartunk az erre alkalmassá tett PIN bevételére szolgáló billentyűzethez, akkor minden további teendő nélkül megtörténik a tranzakció. Se PIN kód, se kártyalehúzás. A rendszer nem ellenőrzi, hogy van-e fedezet a kártyánkon, azaz nem épít fel a kártyaelfogadó terminál kapcsolatot a saját bankjával, az a kártyatársaság számítógépével, ami

²¹ Primary Account Number- Egyedi számsor

²² Card Verification Value

²³ Card Verification Code

²⁴ <http://kiszamolo.hu/fizess-egyszeruen-a-paypass-kartyakrol/>

lekérdezi a számlavezető bankunkat. Emiatt gyorsabb és kényelmesebb fizetni vele, mint készpénzzel.” Azonban ahol a legerősebb a rendszer, ott a leggyengébb is. Mivel PIN-kód nélkül lehet vele vásárolni, egy elhagyás illetve egy lopás esetén könnyen áldozattá válhat a kártyabirtokos, hisz akár a megtaláló akár a tolvaj bárhol használhatja a kártyát.

A másik rohamosan fejlődő hibrid kártyatípus a *V-PAY kártya*²⁵. Egyesíti a modern betéti kártyák jellemzőjét és előnyét. A kártya tartalmaz egy számkijelzőt, valamint egy billentyűzetet. Ez a billentyűzet állhat akár egy nyomógombból, amelynek megnyomásával a kijelző egyes funkciói választhatók, de lehet akár számjegybillentyűs is, mely a számjegybevitellel összefüggő funkciót biztosítja. Elsősorban az internetes vásárlás megkönnyítését és biztonságosabbá tételét hivatott a kártya megteremteni.

A típusok ismertetés során előjött az On-line és az Off-line rendszer, amelynek rövid ismertetését a következő alfejezetben tenném meg, ezzel is elősegítve, hogy melyik kártyát milyen rendszeren tudom megfelelően igénybe venni.²⁶

2.2.3.3. *Működése*

Ha a fogalmi meghatározásokból indulunk ki, akkor megismerhetjük, mire is jó tulajdonképpen a bankkártya. Ebben segít a Magyar Értelmező Kéziszótár által meghatározott definíció és a legtöbb internetről begyűjtött fogalom. Ezek alapján a következő műveleteket hajthatjuk végre, amely egyben a bankkártya használatát jelenti.

Az első, amit először prezentálok, a legismertebb és elég gyakran alkalmazott módszer, az ATM automata. Ez egy olyan berendezés, amelyen az ember készpénzt tud felvenni a számlája terhére bizonylattel vagy a nélkül, számlájának egyenlegét ellenőrizheti, mobiltelefon feltöltést hajthat végre, miután természetesen a PIN-kódja helyes megadásával igazolta, hogy ő a kártya birtokosa. Előnye abban rejlik, hogy az ügyfélnek nem kell elmenni külön a bankjához, hogy ezeket az információkat beszerezze vagy tranzakciót végrehajtsa. Így rengeteg időt lehet megspórolni.

A második lehetőség, amelyre a kártya alkalmas, az üzletekben, kereskedelmi és vendéglátói helyeken történő vásárlás. Az ilyen ipari egységekben vagy POS terminál működik, vagy egy ún. kézi nyomtató, amely a POS terminál egyszerűsített szerkezete. A

²⁵ <http://bankkartya.hu/hirkegategoria/hirek/cikk/8034-vilgjdonsg-bejelentse-budapesten-indulnak-a-szmkielzs-s-billentyzettell-elltott-krtyk-a-mastercardnl>

²⁶ Az alfejezet kifejtésekor nagyban támaszkodtam az alábbi forrásra:
http://bankkartya.blog.hu/2010/04/22/a_bakkartya_fajtai

POS terminál vagy a mágnescsíkról olvassa le a kódolt adatokat, vagy a chipről elemzi őket, és a megerősítés jeléül a zöld gomb benyomása után kell megadni a kártyához tartozó PIN-kódot, majd a zöld gombbal jóváhagyni, hogy helyes a bepötyögött kód. Ezután nyomtatja ki a terminál a bizonylatot, melyet a vásárlónak, aki egyben a kártya használója, alá kell írnia a kártyán szereplő teljes nevével. Ez lehetőséget adhat arra, hogy az eladó ellenőrizze, a két aláírás hasonlít-e egymásra. A terminál mind mágneskártyával, mind chipes kártyával, mind dombornyomású kártyával használható, csak úgy, mint az ATM automata.

A kézi nyomtató egy olyan berendezés, amely csak a dombornyomású kártya olvasására képes. A kártyáról készít egy lenyomatot, és a kártya adatait egy 3 példányos bizonylatra nyomtatja. A bizonylaton feltünteti még az elfogadó hely nevét, a vásárlás idejét, valamint az áru vagy szolgáltatás összegét.

A harmadik, de nem utolsó hely, ahol a kártya segítheti a vásárlás menetét, az az Internet, és az azon meglévő internetes web áruházak. Az Internet egy egyfajta „táguló Univerzum”. Napról napra nagyobb, terjedelmesebb. A kereskedelmi egységek majdnem mindegyikének van saját weboldala, sőt olyat is tudunk említeni, akinek csak internetes oldala van, és csak online lehet terméket vagy szolgáltatást vásárolni. Az Interneten rendkívül gyorsan lehet tájékozódni egy bizonyos termékről. Fent van a róla készített kép, róla egy rövid leírás. A vásárlás egyszerűen és gyorsan, otthonról elvégezhető. Ehhez meg kell adni azonban a saját adatainkat, a kívánt fizetési módot, és ha átutalással kívánunk fizetni, akkor a bankszámla számot, azt, hogy melyik banknál van a számla vezetve, valamint a bankkártyánk bizonyos adatait (a kártya számát, a hátoldalon lévő CVV/CVC háromjegyű számkódot). Valahol csak elővétellel, átutalással lehet az áru vagy szolgáltatás összegét kiegyenlíteni. Ezek után meg kell erősíteni a vásárlást, és a rendelést a számítógép rögzíti, majd a munkatársak összeállítják a rendelést, és általában valamelyik futárszolgálat vagy a Magyar Posta szállítja a csomagot.²⁷

2.2.3.4. *Előnyei, hátrányai*

Mint minden új vívmány, úgy a bankkártyák is megjelenésük után fontos szerepet vállaltak a világ alakulásában, ami lehet akár pozitív, akár negatív hatás. Pozitív hatásként értelmezhetjük előnyeiket, negatív befolyásként pedig a hátrányukat. Ezeket legjobb közgazdasági értelemben csoportosítani, ugyanis a bankkártya is egy piacot képez, amely jelenti „a kereslet és a kínálat összességét, a kereslet és a kínálat egymásra hatását, valamint a kereslet és a kínálat találkozási módját és helyét.”²⁸ A közgazdaság két részre tagolódik: *mikroökonómia*ra és *makroökonómia*ra. A mikroökonómia az egyes háztartásokkal és vállalatokkal foglalkozik, míg a makroökonómia a teljes nemzetgazdaságot elemzi, figyelembe véve a mikroökonómiai kutatások eredményeit.

A mikroszinten jelenik meg a *fogyasztó*, vagyis a kártyabirtokos. Számára azért előnyös a bankkártya használata, mivel használata kényelmes, nem kell a készpénzt magánál tartani, illetve fizetéskor külön számolgatni a címleteket. Ez még egyszerűbbé, gördülékenyebbé teszi a vásárlást. A vásárlásnál nem csak a kártya mögötti bankszámlán lévő pénzmennyiséget élheti fel, hanem ezt meghaladóan is, feltéve, hogy ezzel a pénzügyintézetével külön szerződést kötött. Ebből még azt a konzekvenciát is le lehet vonni, hogy nem szükséges egyszerre nagyobb mennyiségű készpénz saját magunknál tartása, mely frusztrációt, kényelmetlen érzést okozhat bizonyos embereknek, ezáltal a tapasztaltabb, „utcán” nevelkedett bűnözők számára potenciális áldozattá válhat. Ráadásul a világ elért egy olyan fejlettségi szintet, hogy már interneten is lehet vásárolni. Ezt a folyamatot nevezzük internetes vásárlásnak. Az ilyen vásárlásnál nem kell az ügyfélnek sehova sem menni, csak internetkapcsolatra van szüksége, na meg persze a bankkártyájára, és akár otthonról, kényelmesen a nappaliból intézve vásárolhat időt és energiát megspórolva ezzel. Mentessül az esetleges fertőzésektől, betegségektől, amelyeket a készpénzek magukon hordozhatnak. A kártyát a világ majdnem bármely pontján használhatja, így nem kell a valutaárfolyamokat figyelemmel kísérnie, valamint az ezekkel járó kényelmetlenségek is elkerülhetők.

Sajnos, ahol előnyös a bankkártya használata, ugyanott hátránnyá válhat. Ezt mondhatnánk úgy is, ahol a legerősebb, ott a leggyengébb. Itt emelném ki, hogy a már többször említett fedezetet meghaladó fizetés/vásárlás esetén előfordulhat az a szituáció, hogy a kártyabirtokos annyira elkényelmesedik a vásárlásnál, hogy egyre többször lépi túl a hitel keretét, amelyet ugyan egy meghatározott szintig enged a bank, de ez ismétlődve

²⁸ Dr. Lázás Piroska, Dr. Solt Katalin: Elméleti Gazdaságtan I. Mikroökonómia, Novoprint Öltevényi Production, Budapest 2006., 30.o./227.o.

komoly tartozásokat halmozhat fel, amely feszültséget generálhat. Későn ébreszti rá a személyt arra, hogy a pénz nem csak boldogít, de romokba is dönthet.

Az internetes vásárlásoknál a nagy hátrány az, hogy így ezáltal ingerszegényebb környezetbe kerül az illető, amely szociológiai problémákat eredményezhet, például határozatlanabb fellépés, ha személyesen megy vásárolni, ugyanis elszokik ettől a légkörtől. Megszokhatja azt, hogy mindent házhoz hoznak neki, úgy mondván kiszolgálják, és ezt visszaköveteli az „élő” kereskedelembe, elfelejtve azt, hogy nem csak egyedül vesz részt a vásárlásban, hanem mások is vannak, tehát kialakul benne egy önzőség, egy felsőbbrendű érzés, hogy először engem szolgáljanak ki, utána a másikat.

Most, egy nagyon aktuális téma, a készpénzfelvétel, amelyről jogszabály²⁹ rendelkezik. Ez rendkívül előnyös, de ha az ember nem figyelmes, a hátrányára válhat. Ez a készpénzfelvétel arról szól, hogy nyilatkozni kell annak, aki havonta kétszer, ingyenesen szeretne készpénzt felvenni, ami maximum 150.000 Ft összegig megengedett. Előnyös, mert a bank nem számol fel kezelési és egyéb költséget a készpénzfelvételnél, azaz ingyenesen zajlik a tranzakció, ámde ha valaki valamelyik engedményt túllépi, azokra magas terheket rónak ki a bankok.

Mikroszinten említhetők meg a fogyasztók mellett a *vállalatok, kereskedők*. Ha kiépíti a kártyaelfogadó rendszert (POS-terminált), akkor egy olyan üzletpolitikát tud folytatni, ami több profit termelésére képes, ugyanis például úgy határozhatja meg az árat, vagy esetleg olyan akciókat hirdethet meg, amely a vásárlót nem tervezett vásárlásra készíti, és ez még akkor is működhet, ha véletlen a vásárlónak nincs a bankszámláján arra kerete, ugyanis a megfelelő szerződéssel ezt a keretet túllépheti, és inkább a vásárlás mellett dönt.

A fizetés során a pénz fizikai valóságában nem jelenik meg, hanem virtuális térben történik a pénzmozgás. Ebből azt vonhatjuk le, hogy nemhogy igazi pénz, de még hamis pénz sem kerül a birtokába. Mindkettővel jól járhat, mert az igazi pénzt az esetek döntő többségében egy adott számlára fizetik be. Ehhez el kell menni a bankba. Ez vállalkozásoknál változik, de annyi biztos, hogy egy rendszer szerint mennek, amelyet a tapasztaltabb bűnözők (visszaesők) kifigyelhetnek, és ezáltal kidolgozhatnak egy támadási stratégiát a pénz megszerzése érdekében. A hamis pénz esetében pedig azért jó ha nem kerül a birtokába, mert ezzel a pénzzel az áru vagy szolgáltatás ellenértéke olyan, mintha ki sem lett volna egyenlítve, így ezzel károsulttá vált.

²⁹ 2009. évi LXXXV. törvény a pénzforgalmi szolgáltatás nyújtásáról

Makroszinten szintén két szereplőt tudunk megemlíteni. Az egyik a *pénzügyi szektor*, ahová tartozik a kibocsátó bank, aki a kártya tulajdonosa is egyben. Számára azért előnyös, mert a bankkártya a konkurens pénzügyintézetek között egy piaci versenyt generál, amely arra sarkallja az egyes bankokat, hogy minél jobb szolgáltatást nyújtsanak szem előtt tartva, hogy nekik ebből bevételük legyen, amit úgy tudnak megvalósítani, hogy minél több ügyfelet csábítanak a saját bankjukhoz. rengeteg kínálatot tudnak nyújtani az ügyfeleknek, egyéb díjak, szolgáltatások, amik ugyancsak gyarapítják a bank pénzét. Az fentebb említett jogilag szabályozott készpénzfelvétel is előnyös lehet a bankoknak, ugyanis jelentős mennyiségű bevételi forrás lehet, ha valaki megszegi az egyik feltételt. Azonban ahhoz, hogy egy jól működő, megbízható, biztonságos rendszert építsenek ki, rengeteg pénzt kell ehhez befektetni. Gondoljunk csak a kártyák tervezésére, kialakítására, modernebb technológiák kifejlesztésére, azok alkalmazására, továbbá az elfogadóhelyek (ATM-automaták) gyártására, kihelyezésére, működésére. Ugyanis, ha nem tesznek meg mindent annak érdekében, hogy magas szintű szolgáltatást és biztonsági szintet nyújtsanak, akkor a bankkártyákkal való visszaéléseknek „ágyaznak meg” és valamilyen szinten ösztönzik a bűnelkövetőket arra, hogy cselekményüket elkövezzék. Ezzel két óriási veszteséget érhetnek el. Egyrészt egyre kevesebb ügyfele lesz, akitől a bevétele származna, így a befektetett pénze szinte sohasem fog megtérülni, arról nem is beszélve, hogy a visszaélésekkel nem csak az imázs romlik, hanem a bankoknak óriási kárai keletkezhetnek a visszaélések által.

A másik makroszintű résztvevő maga az *állam*. Rendkívül sokat képes megtakarítani az állam azzal, hogy preferálja a bankkártyák előállítását és használatát, ugyanis sokkal kevesebb bankjegyet és fém pénzt kell forgalomba hoznia. Itt is megjelenik az az előny, amit a mikroszinten a vállalkozásoknál említettem, hogy kevesebb hamis készpénz kerül forgalomba, mert a bankkártyák elterjedésének köszönhetően az államnak kevesebb pénzt kell előállítani és forgalomba hoznia, amely által rengeteg kiadástól mentesül meg. Ha a személy a bankkártyáját használja fizetéskor, akkor a virtuális térben történik a pénzmozgás, mely az állam számára átláthatóbbá, követhetőbbé válik.

A bankkártyák a sokoldalúságukkal rendkívül megkönnyíthetik a birtokosa életét, ámde ezzel nem csak tulajdonosaiknak, használóiknak a „kedvére tesznek”, hanem a bűnelkövetőkére is, akik különféle módszerek alkalmazásával igyekeznek jogtalan haszonhoz jutni úgy, hogy megszerzik a bankkártyák adatait.

3. Bankkártya adatok megszerzése a kártyák fizikai jelenlétével

A bankkártyák fejlődése során rengeteg biztonsági megoldás látott napvilágot, mely a bizalom erősítésére szolgál. Azonban sajnos eddig nem sikerült olyan védelmi rendszert kialakítani, amely feltörhetetlen lenne. A bűnelkövetők felismerve ezt a lehetőséget rengeteg visszaélési taktikákat fejlesztettek ki a mai napig. Az elkövetők célja olyan információk megszerzése, amelyek alapján készpénzhez, vagy egyéb jogtalan előnyhöz jussanak. Az adatok megszerzésének módszereit célszerű két nagy halmazba besorolni, ugyanis a két halmaz között egy nagy választóvonalat lehet húzni. Az egyik oldalon az elkövetőnek „szüksége van” magára a bankkártyára, amelyen az adatok találhatóak. A másik oldalon viszont az elkövető a kártya fizikai jelenléte nélkül gyűjti be a kártyabirtokos adatait. Ezek alapján tudjuk szétválasztani a különféle, alkalmazott módszereket.

Az előbbi csomagba, azaz ahol a bankkártya is jelen van, az alábbi elkövetői „trükköket” alkalmazzák:

3.1. Ellopott vagy elvesztett kártyák

Ellopott kártyáról akkor beszélünk, amikor az elkövető a kártyabirtokos (sértett) tulajdonában lévő kártyát jogtalanul elveszi. Ez történhet a személy közvetlen testi őrizetéből, ahol megtevesztésként eltereli a sértett figyelmét, hogy a pénztárcájából kivegye a készpénz-helyettesítő fizetési eszközt, de történhet úgy is, hogy például a kártyatulajdonos otthon hagyta a pénztárcáját, és míg távol volt, a lakásba betörték, és akár több eltulajdonított érték mellett magukkal vitték a pénztárcát is a benne lévő bankkártyával. Persze sokféleképpen történhet az eltulajdonítás, de a terjedelmi korlátokra való tekintettel, valamint a felsorolás lehetetlenségére tekintettel csak egy-egy elképzelhető „forgatókönyvet” vázoltam fel. Az elkövetés függ az elkövető személyiségétől, kvalifikáltságától. Azonban írnék egy olyan példát³⁰, ami mindennapos lehet, és bárkivel előfordulhat.

Egy szabadtéri kávézóban az elkövető olyan embert keres, aki egyedül ül az asztalnál. Két társa turistát játszik, és odamennek ehhez a egyedül ülő személyhez megkérni, hogy csináljon róluk egy képet. Amíg elmagyarázzák a vendégnek, mit hogyan kell csinálni a fényképezőgéppel, addig az a csoporttag, aki eddig megfigyelt, akcióba lendül. Tudni kell még, hogy nála van egy nagy utazótáska. Odamegy az asztalhoz, melyet felügyelet nélkül hagyott az épp fényképező áldozat, a tettes a táskáját magához veszi, kinyitja a bőröndöt, belerakja a frissen lopott táskát, és leül az asztalhoz, mintha mi sem történt volna.

³⁰ <http://kiszamolo.hu/bankkartyas-csalasok-ii-resz-2/>

Mikor visszafordul, észreveszi a táská hiányát, és kétségbeesik. Eközben a két, fényképet kérő tettes eltávozik a helyszínről, és a közelben leparkolt kocsijukhoz mennek, arra várva, hogy társuk telefonáljon nekik. A táskájában volt minden irata, pénztárcája, egyéb holmija, mobiltelefonja. A pénztárcájában volt készpénz, bankkártya, egyéb törzsvásárlói kártyák stb. A segítőkész úriember odamegy a károsulthoz, és azt mondja neki, hogy tiltassa le a bankkártyát, ne tudjanak vele visszaélni. „Segít” elérni a sértettnek a bankját a saját telefonjával, majd átadja neki a telefont. Azonban a kutya ott van elásva, hogy a segítséget nyújtó úr nem a bankot, hanem a társát hívja fel, aki a közelben parkoló kocsiban ül és aki egy remek szerepjátékkal elhiteti, hogy ő a bank ügyfélszolgálatán dolgozik. Megkéri a személyt, hogy vagy pötyögje be a telefonba a PIN-kódot, amelyet hangrögzítővel felvesz, melynek segítségével később a hangok által vissza tudják követni, milyen számot billentyűzött be a telefonba. Azonban a történet itt nem ér véget, hisz a PIN-kóddal nem mennek semmire a kártya nélkül, tehát a lopás is ehhez az „akcióhoz” köthető. Ők lopják el a táskát, eljátsszák a segítő állampolgárt, valamint a banki ügyfélszolgálatot, és el is érték a céljukat.

Elveszett kártyával akkor van dolgunk, amikor a kártyabirtokos bankkártyája a saját figyelmetlenségéből, óvatlanságából kerül ki a birtokából (valahol hátrahagyja; kirántja a zsebéből) és a tulajdonos általi visszaszerezhetőségnek már objektív lehetősége nem áll fenn. Ha ez fennáll, és az elkövető így szerzi meg a bankkártyát, akkor az lopott készpénzhelyettesítő fizetési eszköz lesz.

Ezzel a visszaélési módszerrel mind az ügyfélnek, mind a banknak okoznak kárt. Ám kinek kell az okozott kárt megtéríteni?³¹ A kártya birtokosának kell megtéríteni, ha miután észlelte, hogy a kártyáját illetve a hozzá tartozó PIN-kódot ellopták vagy elrabolták, illetőleg elvesztette, továbbá ha jogosulatlan tranzakcióról szerez tudomást, nem jelenti be a kibocsátónak. A bejelentést megelőzően bekövetkezett károkért a kártyabirtokos maximum 45.000 Ft-ig viselheti a kármegtérítést, e összeg felett a kibocsátó költsége (vesztesége) lesz. A kártyabirtokos a felelős a kár megtérítéséért, ha a kár a használó szándékos vagy gondatlan magatartása miatt következett be.

A kibocsátót terheli a kár viselése, ha nem tette meg a bejelentést követően a tőle elvárható valamennyi intézkedést, valamint akkor is ő a felelős, ha a neki felróható technikai hiba miatt nem tudta a kártyabirtokos bejelenteni a bankkártya elvesztését, ellopását stb.

³¹http://www.mnb.hu/Root/Dokumentumtar/MNB/Penzforgalom/Penzforgalom_kiadvanyok/penzforgalomrol_mindenkinek_bankkartyak.pdf, 15. o.-17. o.

3.2. Kézi adatszerző

Ez az elkövetői módszer azon az alapelven működik, hogy az ügyfél kártyájának kétszer történő lehúzása sikerüljön. Az egyik lehúzás legitim (lehet), ugyanis a vevő a vásárlásnál a bankkártyájával fizet, a második lehúzás azonban már illegitim, mert semmilyen törvényes alapja nincs annak, hogy a legitim kártyahasználat előtt vagy után húzzák le a kártyát. Az illegitim használatkor semmilyen tranzakció nem történik, csak ez az ún. kézi adatszerző lementi a mágnescsíkon található összes adatot a kártyabirtokos tudta és beleegyezése nélkül a leolvasó memóriájába, amely akár több személy kártyájának információit képes elraktározni. Ebből a technikai felszereltségből könnyen levonhatjuk azt a konklúziót, hogy az elkövetés hátterében egy bűnszövetség vagy bűnszervezet állhat, mely előre kitervelten, megfelelően felkészülve tevékenykedik úgy, hogy még az eladót is bevonja a tervébe. Ebben a kooperációban mindenkinek megvan a saját feladata, amihez szakértelemmel és attitűddel rendelkezik. A csoport egyes tagjainak a felszerelés megszerzése vagy beszerzése, esetleges összeszerelése (ha nem készen kapják, hanem csak az alkatrészeket szerzik meg) a teljesítendő feladat. Más tagok „hatáskörébe” a szükséges kapcsolatok kialakítása tartozhat (sikerüljön bevonni a tevékenységbe a kereskedelemben dolgozó eladót, és minden olyan információt a tudtára adni, amely a feladatának az elvégzéséhez tartozik.) Ennek a személynek csupán annyi a dolga, hogy a foglalkozása során előkerülő bankkártyákat a lehetőség adta trükk alkalmazásával kétszer lehúzza (az egyiket a neki adott kis kézi adatszerző berendezésen át), és az így megszerzett és elmentett adatokat átadja a csoport egy tagjának. Ez a személy a kinyert információkat egy olyan személyhez viszi, aki fel van szerelve egy kártyakészítő eszközzel, amely segítségével ún. nyers plasztik kártya mágnescsíkjára tudja telepíteni az adatokat. Ez azonban még nem minden. Szükség van még olyan kereskedőre is, aki tovább konspirál és a bejelentési kötelezettségének nem tesz eleget, amikor a „hamis” kártya felhasználása során észleli a kártya hamis voltát, de ennek ellenére a hatóságot nem értesíti.

Azonban ennek a visszaélési formának van egy másik elkövetési módszere. „Kiiktatják” a kereskedőt, aki „elfogadja” a hamis kártyát. Ebben az esetben tehát valódinak látszó bankkártyát állítanak elő, amihez azonban egy hamis személyigazolvány társul, így a vásárló, aki persze a bűnszövetség vagy bűnszervezet tagja, igazolni tudja magát, illetve azt, hogy a kártya jogos birtokosa és használója. Ez úgy kivitelezhető, hogy a személyi azonosító okmányra azokat az adatokat telepítik, amelyeket már korábban megszereztek a

kézi adatszerző eszközükkel. Az így vásárolt terméket tovább értékesítik, mellyel pénzzé váltják a tevékenységüket.

Miután átestünk a módszer elméleti megismerésén, nézzük meg, hogyan is működik ez a gyakorlatban. Egy vendéglátó ipari egységben, egy kávézóban ül a vevő a társaságával. Rendeltek valamit, és beszélgetnek az élet nagy dolgairól vagy egyéb más témáról. Egy nagyon kedves, dekoratív pincérnő szolgálja fel a rendelést, aki azonban kulcsszerepet játszik a történetben. Mikor a vevő fizetési szándékát bejelenti, valamint a fizetés módját (bankkártyával kíván fizetni), a pincérnő hozza a POS terminált. A személy átadja a bankkártyáját a pincérnőnek, aki a POS terminálba történő behelyezésnél elejti. Lehajol, hogy felvegye, azonban még mielőtt felállna, a korábban a bokájára erősített kis kézi adatszerző egységen áthúzza a kártyát, megszerezve az adatait, és a birtokosának erről fogalma sincs. A művelet után feláll, behelyezi a bankkártyát, és kéri a vendéget, hogy üsse be a bankkártya PIN kódját. A pincérnőn, aki fekete ruhát visel, van egy kis mini kamera, amivel megpróbálja a fizető kézmozdulatait felvenni, megszerezve így a PIN kódot, valamint a bankkártya fizikai kinézetét, hogy utána hasonló típusú és kinézetű bankkártyát lehessen legyártani. Természetesen más megoldása is van arra nézve, hogy hol helyezze el magán a kézi adatszerzőt. Az egyik, mint említettem, a boka tájéka. A másik lehet egy ruhának egy deréktájékon lévő zsebe, ahol azt játssza el, hogy a kártyát nem ismeri fel a terminál, ezért törlést imitál. A „tisztítás” során a zsebben lévő adatszerzőn sikeresen áthúzza a kártyát, majd mintha mi sem történt volna, behelyezi a POS terminálba, kéri a PIN-kódot, és a tranzakció, a fizetés lezárult. A vendég nem is sejti, hogy az adatai rossz kezekbe kerültek, abban a hitben távozik, hogy csak fizetett.³²

3.3. Adatszerzés POS terminálon

A POS terminálon, mint már korábban is láthattuk, nem csak egyféle megoldás létezik az adatok illetéktelen birtokba vételére. Ez hasonlít az ATM automatáknál alkalmazott egyik technikai megoldáshoz, ami az álbillentyűzet. A POS esetében is egy alkalmazható módszer a PIN pad kicserélése. PIN pad-nek nevezzük azt a tasztatúrát, amelynek gombjai segítségével a PIN-kódot megadjuk, aktiválva ezzel a fizetési módot. A csere úgy történik, hogy az üresen hagyott kasszához, ahol persze lehetőség van a POS terminál használatára, odamegy egy bandatag és a másodperc töredéke alatt felhelyezi a magával

³² <http://kiszamolo.hu/bankkartyas-csalasok-ii-resz-2/>

hozott, machinált billentyűzetet. Ez a PIN pad azzal a képességgel bír, hogy a bepötyögött PIN-kódokat továbbítja a csoportnak.³³

Van egy olyan módszer is, amikor az egész POS terminált hackelik meg, nem csak a billentyűzetét. Ilyenkor magába a terminálba építenek egy olyan egységet, amely képes az adatok rögzítésére, tárolására. A később kinyert adatok felhasználásával tranzakciókat tudnak lebonyolítani, ami pénzhez juttatja őket.

A POS terminálnál is remekül alkalmazható egy olyan technika, melyet szinte mindenhol bevetnek az elkövetők, ez a minikamera. Ezzel képesek megszerezni a kártya hátulján lévő CVV háromjegyű titkos kódot, melyet internetes vásárlásoknál tudnak felhasználni, megadva, melyik kártyát terheljék meg az áru összegével.

3.4. ATM-nél elkövetett kártya- (Card trapping), készpénz (Cash trapping) és adatlopás (Skimming)

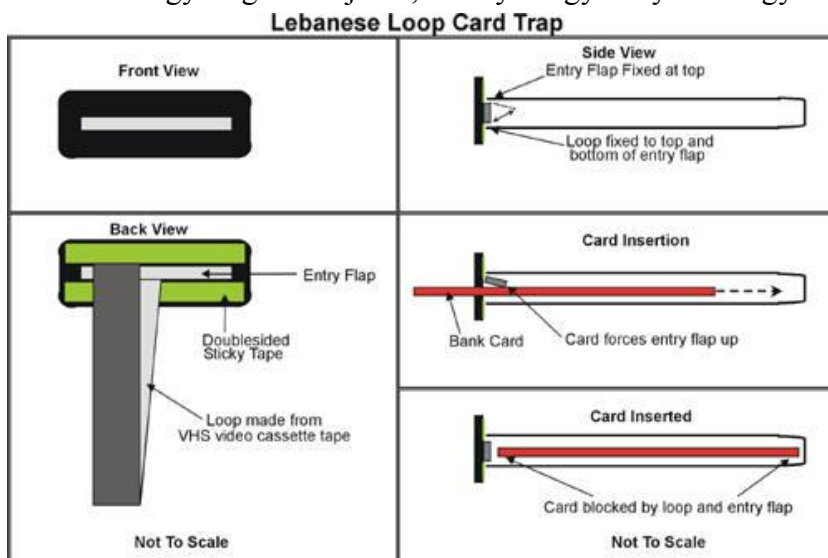
A bankkártya mindennapos használatának más vizére evezve egy olyan adat- illetve pénzszerzési módszerrel ismerkedhetünk meg, amely az ATM-automatákhoz köthető. Rengeteg ember életében fontos szerepet játszik az automata, ugyanis mint ahogy feljebb írtam, készpénzfelvételre, egyenleg megtekintésére, telefonszám egyenlegének feltöltésére és egyéb más tranzakciós folyamat vagy szolgáltatás végrehajtására kínál lehetőséget. Azonban ez nem csak előnyös, hanem rengeteg és bizonyos esetekben nagy kárt tud okozni, ha nem vagyunk eléggé elővigyázatosak. Hozzá kell még fűznöm, hogy egyes módszereknél nem elegendő a puszta óvatosság és elővigyázatosság, mivel az elkövetők olyan felszerelésekkel is rendelkezhetnek, amelyeket szinte észre sem lehet venni, de ezekről az egyes alfejezetek nyújtanak ismereteket.

Mivel kulcsszerepet tölt be a hétköznapiakban, és emberek százezrei használják, a bűnözők is felismerték az ebben rejlő könnyű pénzszerzés lehetőségét. Erre kihegyezve „továbbképzésüket”, különféle technikákat, vívmányokat találtak ki, melyekkel céljaikat el tudják érni. Miket sikerült tehát elsajátítaniuk?

³³ <http://kizsamolo.hu/bankkartyas-csalasok-ii-resz-2/>

3.4.1. Card trapping

Ez egy angol kifejezés, amely magyar nyelvre úgy fordítható le, hogy „kártya-



4. kép

csapda”. A Skimming³⁴ egy formája. A csaló nem arra használja ezt a kártyát benyelő eszközt, hogy lemásolja a kártyáról az adatokat, hanem hogy az bent maradjon a pénzautomatában. Amint a sértett elhagyja a helyszínt és segítséget kezd keresni a benyelt

kártyája miatt, az elkövetők kihasználják ezt az alkalmat, hogy megszerezzék a kártyát. Ahhoz, hogy ezzel a kártyával később pénzt tudjanak felvenni, megpróbálják előtte a PIN-kódot megszerezni.

A technikája úgy működik, hogy vékony szalagokat helyeznek el a kártyabeolvasó egységnél, amivel csapdába ejtik a kártyát. A PIN-kódját vagy egy oda nem illő kamerával szerzik meg, amelyet az elkövetők installálnak olyan helyre, ahonnan tisztán látható, hogy az ügyfél milyen billentyűkombinációt használ a PIN-kód megadására, illetve egy segítő-kész úr odamegy, aki megpróbálja a kártyát kivenni, vagy megkéri, hogy a kódot újra adják meg, és megpróbálja leolvasni.

3.4.2. Cash trapping

Ez egy olyan módszer, amelynél nem feltétlen elég, ha elővigyázatosak illetve figyelmesek vagyunk. Egy olyan eszközt barkácsolnak össze az elkövetők, amely megakadályozza az automatában lévő pénz kiadását. A technika összeszerelése, egységbe foglalása rendkívül egyszerű és olcsó. Szükség van egy kétoldalú ragasztócsíkra és egy fém lemezdarabra. A ragasztócsíkot ráragasztják a lemezre, és ezt a lemezt helyezik fel a pénzkidó nyílás elé. Ez még úgy észrevehető is lenne, ha nem lennének a tettesek mindenre felkészülve. A felhelyezett fémlemez hátoldalát olyan színűre festik le, amilyen az automata, így biztosítva az észrevehetetlenségét. Amikor a vevő pénzt kíván kivenni, sikeres tranz-

³⁴ Ezt a 3.4.3. alfejezet tárgyalja

akció esetében az automata kiadja a pénzt. Mivel a pénzkidő nyílás a ragasztóval ellátott fémdarabbal le van takarva, a pénz beleragad a ragasztóba kiiktatva ezzel az ATM azon biztonsági funkcióját, ami arra hivatott, hogy a pénzt visszahúzza. Az ügyfél, miután nem kapta meg a pénzt, azt gondolhatja, hogy a pénzkidő automata elromlott. A bankkártyáját visszakapja, és elmegy a helyszínről. A trükkös csalónak meg nincs más dolga, mint a csapdába esett pénzt „kiszabadítsa” és azzal szabadon távozzon a helyszínről.

3.4.3. Skimming

Az ATM automatáknál történő csalás egy olyan módja, amikor nem közvetlenül a készpénz megszerzésére irányul a cselekvés, tehát az automatát nem pénzzel a zsebünkben hagyjuk magunk mögött, hanem a megszerzett bankkártya-adatokkal!

A csaló arra használja a Skimminget, hogy a bankkártya mágnescsíkján tárolt adatokat lemásolja, amikor a kártyabirtokos a kártyáját az automatába helyezi. Azért telepítenek fel olyan, majdnem láthatatlan eszközt a pénzautomatán, közvetlenül a kártyanyílás elé, hogy az adatokat az ügyfél tudomása nélkül szerezzék meg. Ugyanebben az időben, mikor a birtokos a kártyáját használja, megpróbálják leolvasni a PIN kódot, például minikamera segítségével, vagy a shoulder surfing alkalmazásával. Azokat az adatokat, amelyeket elloptak, hamis kártyák elkészítésére használják fel.³⁵

De mi az a shoulder surfing? A shoulder surfing³⁶ során a csaló az ügyfél válla felett néz át, amíg a kártyabirtokos tranzakciót hajt végre az automatánál, annak reményében, hogy megismeri a PIN kódot. Amint látta, megpróbálja a tranzakciót végrehajtó személy figyelmét elterelni, hogy a bankkártyáját megszerezze. Hogyan zajlik mindez? A vevő el van foglalva a készpénzfelvétellel. Hirtelen a vevő mögött álló személy kedvesen azt mondja, hogy elejtett egy bankjegyet. A vevő elhiszi, lenéz, és mikor meglátja a földön fekvő pénzt, lehajol érte. Míg ez történik, addigra az elkövető a bankkártyával együtt el is tűnt. Tulajdonképpen ez a személy nem szíveségből várt a sorára, amíg a vevő a tranzakciót hajtotta végre. Ő „csak” a válla felett kukucskált át és próbálta meglesni a biztonsági kódot. Mivel sikerült a bankkártyát és a hozzá tartozó kódot megszereznie, nincs más teendője, mint vagy az eredeti kártyával, vagy egy hamisított kártyával készpénzt lehet felvenni.

A Skimming alkalmazását is többféleképpen lehet eszközölni.

³⁵ <http://safeinternetbanking.be/en/fraud-techniques/skimming-and-card-trapping>

³⁶ <http://safeinternetbanking.be/en/fraud-techniques/shoulder-surfing>

3.4.3.1. Mágnescsík adatok illetéktelen személyek általi megszerzése

Ebben a rohanó világban sajnos egyáltalán nem figyelünk a környezetünkre, így ezáltal valamilyen szinten saját magunkat is áldozattá tesszük, ugyanis a szükséges információ beáramlás, feldolgozás, elemző-értékelő folyamat elmarad, így nem kapunk tiszta képet a körülöttünk lévő dolgokról. Így nehezebb észrevenni, kiszűrni a manipulált ATM automatakat. Örülünk, hogy megvan a pénz, és megyünk is tovább. Észre sem vesszük, hogy valaki más is profitált a tranzakcióból, és az nem a bank.

A készpénzautomaták manipulációjában az egyik cél az ügyfél kártyájának adatainak a megszerzése. Ilyenkor egy kártyaolvasó készüléket helyeznek el vagy a kártyanyílás elé, amelyen ráadásul még egy kis kamera is található, amely a billentyűzetet pásztázza, vagy az adatszerzőt beépítik az automatába a megfelelő adatterületre való rácsatlakoztatásával, energiaellátását pedig az ATM energiaforrását megcsapolva biztosítják. Ennek a kis szerkezetnek az a rendeltetése, hogy a mágnescsíkon tárolt adatokat lementse, tárolja, vagy esetleg rögtön el is küldje a bűnöző csoportnak.

Előfordulhat olyan szituáció is, amikor az ATM egy zárt helyiségben van felállítva, ahova csak úgy lehet bejutni, ha az ajtó mellett feltelepített kártyaolvasó szerkezet mágnescsíkolvasó szerkezetén keresztül lehúzzuk a bankkártyánkat. A rendszer csak ez után nyitja ki az ajtót. Ez a védekezési mechanizmus az ATM-ek védelmét hivatott biztosítani. Az elkövetői csoportoknak több sem kellett, és megtalálták ennek a banki, biztonsági intézkedésnek a „kiskapuját”. Az elkövetők megpróbálják kihasználni az emberek „csőlátását”, szűk gondolkodásmódját a naivságukkal együtt. Nem az ATM automatát hackelik meg adatszerzővel, hanem a bejáratú ajtót működtető kártyaolvasó egységet. Amikor a vevő lehúzza a kártyáját, az adatszerző rögzíti a rajta lévő adatokat. Ahhoz, hogy a megszerzett adatokat egy „nyers” plastik kártyára vagy egy lejárt kártyára rátelepítsék, a csoport a szükséges technikai felszereléssel rendelkezik. Természetes nem csak az adatok megszerzésére specializálódtak, hanem a PIN kódéra, ugyanis nélküle nem tudnának visszaélni. Ezekre többféle módszer is kidolgozásra, kifejlesztésre került, melyet a mai napig előszeretettel alkalmaznak a bűnözők, de a leggyakrabban az automatára szerelt kamerát vetik be. Úgy tesz az elkövető, mintha tranzakciót bonyolítana, és eközben installálja fel az adatszerzőt.

Az elmélet megismerése után nézzük meg a gyakorlat egy szituációját. A tettes egy utcán lévő automatához megy oda, és a táskájából kivéve előveszi a kamerával ellátott

adatrögzítőt³⁷, amelyet elhelyez a kártyanyíláson, majd továbbáll, és vár. Jön az első ügyfél, aki észre sem veszi a „pótalkatrészt”, behelyezi a kártyát, lefolytatja a tranzakciót és sietve távozik. Miután ez a személy elhagyta a készpénzfelvevő berendezést, az elkövető visszamegy, leveszi az adatrögzítőt, majd a társához megy, aki lementi a most szerzett adatokat, megnézik a videofelvételt, és készítik a kártyát, vagy elküldik az adatokat külföldi társaiknak, és ott gyártják le a hamis bankkártyákat.

3.4.3.2. Elkövetők általi felszerelt kamerák, billentyűzetek

Ahhoz, hogy egy bankkártyáról megszerzett adatokkal új kártyát tudjanak készíteni, szükséges annak a bankkártyának a PIN kódjának a megszerzése, amelyeken a korábban megszerzett adatok vannak. Az ATM-en elhelyezett adatrögzítő „csak” a kártya mágnescsíkján lévő információkat szerzi meg, a biztonsági kódot nem, ugyanis ezt a kártya használója az ATM billentyűzetén adja meg. A kód megismerésére különféle kisegítő módszereket vetettek be.

Az egyik módszerként lehetne megemlíteni, amikor egy minikamerát helyeznek el az ATM automatán, mely a billentyűzetét figyeli meg, vagy például egy ál füstjelzőt helyeznek ki az ATM közvetlen környezetébe, amelyben kamera van elrejtve. Ezek a

kép- és videorögzítő berendezések rendkívül éles képet rögzítenek, így visszanézésük során simán kivehető ki, mikor, melyik kártyához milyen PIN kódot ütött be.

A minikamera ráadásul olyan apró, hogy szinte bárhol elhelyezhető észrevétlenül úgy, hogy az megfigyelje és rögzítse a billentyűzetet. Hol is vannak ezek a területek? Rögzíteni lehet a kártyabefogadó nyílás közelébe, vagy az erre helyezett adatszerző egységre, telepíthető az ATM képernyője alatti területre, de felrakható akár még a billentyűzet körü-



5. kép

³⁷ Ez a 2inOne adatszerző egy ritkán alkalmazott eszköz, életszerűbb az, hogy külön helyezik fel a kamerát, és külön az adatszerzőt. (A szerző megjegyzése)

li, kimagasodó peremre illetve a billentyűzet takarását biztosító panelre, valamint akár a Pin pad-et megvilágító lámpatestbe is.

Az elkövetői érdeket szolgáló kamerát még, mint már írtam, az automata közvetlen környezetében installálhatnak, amelyet tipikusan füstérzékelőben helyeznek el, de sok más cseles megoldás létezik még. Ez a módszer az ember egyenes irányú gondolkodását játssza ki, mert ha sikerült a kis kamerát kijátszani, nem biztos, hogy arra is gondol az illető, hogy van egy másik olyan kamera, amelynek ugyanaz a célja, mint a kicsinek, és az nem az automataán található. Ez a megfigyelő készülék a teljes cselekvéssort rögzíti, hogy a vevő mit csinál az ATM automatánál, és mivel egy jobb teljesítményű kamerát alkalmaznak, a sugárzott képet ki lehet nagyítani, amellyel meg lehet figyelni az ügyfél kézmozdulatait, megszerezve ezzel a számkombinációt.

Másik módszer az ún. „álbillentyűzet” alkalmazása, melyet az eredeti tasztatúra felszínére applikálnak. Felhelyezése rendkívül kreatív módon van kivitelezve. Szinte észre sem vehető a billentyűgombok körül lévő, pár milliméterrel magasabban elhelyezkedő perem eltűnése. Azonban az az álbillentyűzet nem csak erre alkalmas, hanem képes még a bepötyögött PIN kódok mentésére és tárolására is.



6. kép

Természetesen ez a felsorolás koránt sem taxatív, inkább példálózó jellegű. Sajnos az elkövetők tárháza sokkal bővebb, de igyekeztem a legtipikusabb, leggyakrabban alkalmazott módszereket kiemelni, ismertetni.

3.4.3.3. Egy trükkös eset

Most, miután megismerkedtünk az ATM automatáknál elkövetett bankkártya csalások néhány módszerével, egy rendkívül komplex esetet ismertetnék, illetve fejtenék ki. Az elkövető egy ATM automata közelében tartózkodik. Egy sérült, mankóval közlekedő hölgy tettestársa odamegy az automatahoz, és arra vár, hogy valaki mögé álljon. Aki mögé áll, az egy jel lesz a közelben tartózkodó bandatagnak, akit az előbb említettem. Az az ügyfél, aki épp vár a sorára, időspórolás céljából előveszi a pénztárcájából a kártyáját. Ezt árgus szemmel figyeli a „figyelő” tettes, akiről annyit kell még tudni, hogy rengeteg hamis

kártya van nála. Meglátja a célszemély bankkártyáját, és átnézi a készletét, nála van-e ugyanolyan kinézetű. Az az akció kritikusnak mondható pillanata. Ha van, akcióba lendül, ha nincs, akkor tovább várnak. Jelen esetben pont van nála olyan típusú kártya. Ilyenkor leadja a jelet az automatánál tartózkodó „sérült” társának, aki a tranzakciója befejezését színlelve odébbáll, hadd jöjjön a következő ügyfél, azaz az áldozat. Megfelelő időzítést követően (mikor észleli, hogy az áldozat már épp helyezné be a kártyáját a nyílásba) elesik, apellálva a segítőkészségére. Így a figyelme rá terelődik, figyelmetlenül hagyva a kezében lévő bankkártyáját. Kialakul a teljes támadási felület. A társ nem is habozik, mapával a kezében, az alatt az ujjai között a hasonló külsejű bankkártyával elindul az eleső nő felé, és közben kiveszi az áldozat kezéből a kártyáját, amit meg előkészített, elejti, elhittetve azt, hogy a meglepődöttségtől elejtette a kártyáját. Ezután már tényleg az elesett nő (társa) segítségére siet. Az áldozat ezek után a hamis kártyával próbálná meg a tranzakciót lefolytatni, de az automata ezt a kártyát bevonja, mert a sértett „elrontja” a Pin kódot.³⁸

3.5. Prevenció

Miután megismerkedtünk az elkövetési módok exemplifikatív taxációjával, könnyebb megismerni, illetve rámutatni azokra a sarokpontokra, amelyekre ha figyelmet szentelünk, csökkenthetjük annak az objektív lehetőségét, hogy áldozatokká, károsultakká váljunk. Nem csak az eset megtörténte után kell a gyors intézkedéseket foganosítani, egy sor olyan megoldás van, amely a prevenció keretében kerülhet alkalmazásra, nyugodtabbá téve életünket, időt és energiát megspórolva. Úgy vélem, hogy az a pár perc, amit pluszba tölténénk el egy készpénzfelvétel idején, sokkal kevesebb, mintha a bűncselekmény megtörténte utáni időráfordítás.

Mindenekelőtt két rendkívül fontos, alapvető dolgot kell megtennünk, ami elengedhetetlen a biztonság érdekében. Az első ilyen, amikor a bankszámlaszámot megnyitjuk, és ehhez bankkártyát igénylünk, törekedjünk arra, hogy az alapértelmezett napi limit a saját vásárlási szokásainkhoz igazodó értéket képviseljen. Ez a limit azt biztosítja, hogy egy nap a meghatározott összegnél több pénz nem vehető le a számláról. Esetleg még azt is kérhetjük, ami azonban visszerhes, hogy a számlán történő pénzmozgásról egy értesítő üzenetet (SMS-t) kapjunk, így lehetővé téve azt, hogy ha véletlen áldozattá válunk, akkor rögtön fel tudjuk mérni azt a helyzetet, hogy az a készpénzlevétel nem általunk lett kivitelezve, és így azonnal le tudjuk tiltani a kártyánkat, megelőzve a további, nagyobb károk

³⁸ <http://kiszamolo.hu/bankkartyas-csalasok-ii-resz-2/>

kialakulását. Ennek az SMS szolgáltatásnak az értéke pénzügyintézetektől eltérően másképp alakulhat. A második releváns cselekedet, amit mi, vevők meg tudunk tenni az az, hogy a kártya kézhezvétele után a kártya hátoldalán lévő CVV/CVC háromjegyű kódot letakarjuk, elkerülve azt, hogy illetéktelenek megszerezzék és megszerzése után az internetes online vásárlásoknál felhasználják.

Az első módszerként a lopást, illetve az elvesztést hoztam fel. A lopást nagyon nehéz kivédekezni, de mint egy alapelvként fel lehet fogni, semmi sem lehetetlen. Célszerű először a legtipikusabb lopásmódszereket figyelembe venni a védelem helyes megválasztása érdekében. Elsőként például említhetném a bevásárlóközpontban, vagy a tömegközlekedési eszközökön való közlekedés során történő zseblogásokat. Büntetőjogilag ez azt jelenti, hogy a sértett közvetlen testi őrizetéből történik az idegen dolog eltulajdonítása. Ez nem csak a tettes technikai ügyességén, ügyes csuklómozdulatain alapszik, hanem a figyelmetlenségünkön, az óvatlanságunkon is. Úgy lehet a legjobban megelőzni ezeket a cselekményeket, ha folyamatosan pásztázzuk a környezetünket, ne engedjünk túlságosan közel magunkhoz senkit (persze ez egy túlszűfolt tömegközlekedési eszközön nem kivitelezhető), de ilyenkor is, és máskor is megtehetjük azt, hogy a táskáinkra, egyéb holmijainkra, fokozottabban figyelünk, mert a szituáció a trükkös tolvajok kezére játszik, kihasználva a testközelséget. Javasolt még az a megoldás alkalmazása, ha az utcán sétálunk a késői órákban, lehetőleg több helyen helyezzük el értékeinket (a nadrág, kabát zsebei, főleg ha van táskánk, akkor abban inkább ne is tartsunk túl sok értéket, csak pár ezer forintot, mert így el tudjuk hitetni a tettessel, hogy nincs nálunk több készpénz, érték, megóvva ezzel akár mobiltelefonunkat, bankkártyánkat, egyéb iratainkat.)

A lopás más módjainak áldozatává is válhatunk. Ez lehet vagy a betöréses lopás, vagy a besurranásos lopás. Ilyenkor magánlakásba, helyiségbe történő behatolás során sikerül az elkövetőknek a lakásban lévő készpénz-helyettesítő fizetési eszközök megtalálása, és ellopása. Rendkívül lényeges, hogy a más megkapott bankkártyát és az ahhoz tartozó PIN kódot különböző helyen tároljuk, és a PIN kódot egy jóval rejtettebb helyre kell elrejtteni.

Sajnos előfordulhat egy harmadik lopás. Ez pedig a postaládából történő bankkártya lopás. Ugyanis a bankszámlaszám nyitásakor az ügyintéző azt a tájékoztatást adja, hogy a számlaszámhoz tartozó bankkártyát a pénzügyintézet postai úton továbbítja, és másik levélben pedig a hozzá tartozó PIN kódot. Ahhoz, hogy ezt a módszert el tudjuk kerülni, igyekezzünk a bankszámlanyitást követő időkből fokozottabban figyelni a postaládát, mielőtt előbb ürítsük ki a levéltárolót, és vegyük birtokba a kártyánkat.

További lehetőség lehet egy bankkártya ellopására, amikor a strandon vagyunk, és mikor megváltjuk a jegyet, bankkártyával fizetünk. Ezt könnyen kifigyelhetik a tolvajok, és amikor bent, strand területén őrizetlenül hagyjuk a felszereléseinket, dolgainkat, könnyen lába is kélhet a bankkártyának. Ezek után meg a visszaélések sorozata kezdődhet meg, amelyek akár külföldi országokban lesznek végrehajtva. A tanulság az, hogy a strandon nem szabad sohasem felügyelet nélkül hagyni a dolgainkat, értékeinket, mindig kell lenni valakinek a közelben, vagy a strandra ne vigyük magunkkal a kártyánkat, és használjunk készpénzt a fizetéskor.

Az elveszett kártya esetében leginkább csak azt lehetne megemlíteni, hogy a saját dolgainkra, értékeinkre fokozottan ügyeljünk, és inkább nézzük meg többször, ha olyan érzésünk támad, hogy nincs meg, vagy valami hiányzik, de azt is úgy hajtsuk végre, hogy ha esetleg megfigyelnének, akkor ne lehessen észrevenni, hogy mit néztem meg, és az az őrizetemben hol található.

Ennél a fejezetnél ismertettem az angol kifejezést, a Card trappinget, melynek lényege, hogy a kártya az automatában „csapdába essen”. A sértettek közül sokan arra vetemedhetnek, hogy a segítség érdekében hátrahagyják az automatát a beragadt bankkártyájukkal abban a hitben, hogy mi történhet ezalatt a pár perc alatt. Elég sok minden, ugyanis ez az időintervallum épp elegendő a bűnözőknek, hogy megkaparintsák a bankkártyát. Rendkívül fontos, hogy ilyen esetben, ha nem kapjuk vissza a kártyánkat, igyekezzünk telefonon segítséget kérni. Próbáljuk meg a bankot felhívni, ha egyedül vagyunk, ha esetleg valaki elkísért minket, akkor kérjük meg, hogy hívjon segítséget. Az automatán fel van ragasztva egy matrica, amin egy telefonszám található, melyet akkor kell hívni, ha valamilyen működési rendellenesség lép fel. Azonban ezt is rendkívül körülményesen kell kezelni, mert előfordulhat, hogy az a telefonszám nem a bank ügyfélszolgálatához vagy diszpécseréhez tartozik, hanem az elkövetői csoport egy tagjához, aki ügyintézőnek adja ki magát. Ezzel nincs is gond, hisz semmilyen kártyaadattal nem rendelkezik, mert a kártyát még nem szerezték meg. Ennek az embernek az a célja, hogy kipuhatolja az elnyelt kártyához tartozó PIN kódot. Tudni kell, és ezt nagyon meg kell jegyezni, hogy a bank soha, semmilyen körülmények között nem kéri PIN kódot nem csak azonosítás céljából, hanem semmilyen egyéb művelethez. Megvannak azok a jól bevált eszközök, amelyekkel úgy lehet azonosítani a személyt, hogy ne sérüljön senkinek a becsülete és az adatvédelmi előírásoknak is megfelel (Pl.: az ügyintéző bizonyos adatokat kérdez meg [anyja neve; születési hely, idő stb.]). Komolyabb esetekben meg megkéri, hogy fáradjon be a bankfiókba személyes ügyintézés céljából.

A 3.2.-es alfejezetben a kézi adatszerzővel történő adatmegszerzést taglaltam. A működési mechanizmusa, és a gyakorlati példa alapján a következő preventív intézkedéseket tehet meg a kártya használója. Bárhol, bármikor, a bankkártya használat során a legfontosabb dolog az az, hogy soha sem szabad szem elől téveszteni a bankkártyánkat. Figyeljük, hogy az eladó, akinél fizetünk, mit csinál a kártyával, nem-e próbálja meg kétszer lehúzni. Ha véletlen elejti, ne hagyjuk, hogy lehajoljon érte, egy udvarias mondattal el lehet utasítani, sőt még segítőkésznek is tűnünk, nem hagyjuk, hogy a kezében lévő POS terminállal leguggoljon a plasztikért. Ha arra hivatkozik, hogy a terminál nem olvassa be, akkor fogjunk gyanút, és kérdezzük meg mit ír ki a POS terminál. Ne engedjük, hogy megtörölje, viszont ha nem sikerül olyan gyorsan lereagálni a mozdulatsort, akkor sincs probléma, mivel a szemünkkel követni tudjuk a kártyánk sorsát, és ha véletlen olyan szituáció kerekedik ki, amelyben nem látom a saját kártyámat, akkor nyugodtan, illedelmesen szólítsuk fel a kasszást vagy pincér(nő)t, hogy engedje látni a kártyánkat. Esetleg a rendőrség értesítése is kulcsszerepet játszhat, hisz akár a nyomozás elrendelését is eredményezheti.

A következő részben a POS terminál kijátszásának alapköveit fektettem le. Az alkalmazott módszerek függvényében szintén több mindenre kell koncentrálnunk egy esetleges POS terminálos fizetés esetében. Fokozottan figyeljünk a kártyákra, amit már fentebb megemlítettem. Ha van terminál, akkor, ha lehetséges kérjük magunkhoz, és helyezzük be mi a kártyánkat. Ha véletlen nem tudnánk a módját, akkor az eladó el fogja magyarázni, de a kártyán egy nyíl is jelzi a behelyezés irányát. A POS rendszernél is, csak úgy, mint az ATM automatáknál, meg kell adnunk a kártyához tartozó PIN kódot. Ezt ugye a terminál billentyűinek segítségével tehetjük meg. A biztonsági kód megadásakor fokozottan ügyeljünk arra, hogy a közelünkben ne álljon senki, és lehetőleg az egyik kezünkkel takarjuk el a tasztatúrát, míg a másik kezünkkel minél látványosabb mozdulatok elkerülésével adjuk meg a számkombinációt. Ámde a POS terminálon előfordulhat a billentyűzet manipulálása, de ez elenyésző számban jelentkezik. Természetesen még mielőtt bepötyögnénk a négyjegyű számot, győződjünk meg a számlap állapotáról, kinézetéről. A gombok közti hézagok és kiemelkedések megvannak-e, vagy más gyanús jel nem figyelhető-e, észrevehető-e magán a terminálon. Ha nem találunk semmi gyanúsat, csak utána nyomkodjuk be a kódot. Fontosnak tartom megjegyezni, hogy lassan valamennyi POS és valamennyi bankkártya chip-esítve lesz, így nincs az a lehúzó mozdulat, amivel le lehetne olvasni mágnescsíkot, megszerezve a PIN kódhoz tartozó adatokat, ugyanis a chip beolvasásához csak félig kell behelyezni a kártyát a terminálba. Ez lehet egy átlagos felhasználó bombabiztos védelme, mert a POS terminálok manipulálása olyan precízen van kivitelezve, hogy

szinte észrevehetetlenek. Az éberség attól még fontos lehet, hisz a hibafaktor nem csak a törvénytisztelő polgárok oldalán található meg, hanem a bűnözői részen is.

A terminálnál előfordulhat olyan eset is, amikor mi, vevőként szinte nem tehetünk semmit, vagy egyáltalán esélyünk sincs észrevenni a machinálást. Előbbi esetben „saszemre”, szerencsére és a hatodik érzékünkre van szükség, hogy egy parányi minikamerát észrevegyünk, mert ezek olyan kis berendezések, és olyan könnyen elrejtethetők akár már egy gombban is, hogy szinte láthatatlanná válik. Ennél már csak akkor van nehezebb dolgunk, amikor magában a POS terminálban van az adatrögzítő egység. Ilyenkor csak a külső burkolaton fellelhető, eshetőleges külsérelmi nyomok engedhetnek következtetni a manipulációra.

A 3.4. alfejezet taglalja a kulcsszerepet betöltő ATM automata „használatával” elkövetett bankkártya csalásokat. Rengeteg lehetőség kínálkozik az elkövetők számára arra vonatkozóan, hogyan szerezzenek pénzt, vagy bankkártya adatokat a pénzkiaadó automatánál. Az egyik ilyen a Cash trapping. Cash trapping esetében arra játszanak, hogy valós pénzt akarunk a birtokunkba tudni. Ilyen esetben, mikor készpénzt szeretnénk felvenni a pénzautomatából, először is győződjünk meg arról, hogy a pénz kiadásának „útja” akadálymentes, tehát hogy nincs semmilyen fémpanellel eltorlaszolva a kiadónyílás. Nagyon nehéz észrevenni, mert a profibb elkövetők olyan színűre festik, mint amilyen az automata. Ha véletlen ezt a lépést elmulasztanánk vagy esetleg az alapos megfigyelésnél, ellenőrzésnél nem észlelnénk, és így áldozattá válunk, nagyon fontos az, hogy az automatát ne hagyjuk hátra, és értesítsük az ATM üzemeltetőjét a felbukkanó hibáról, várjuk meg a szakembert, és utána javaslatai szerint cselekedjünk.

A másik a Skimming, ami további almodszerekre bontható, amelyeket azért egymással párhuzamosan szívesen bevetnek, egyéb technikákkal kiegészítve. Az almodszerek közül először a mágnescsík adatainak a megszerzését ismertettem. Rendkívül komolyan kell venni az ATM ellenőrzését gyanús, oda nem illő, külsérelmi nyomok kutatása során. Hiába kell sietnünk, ezen a pár percen már igazán nem jöhet elő káros hatása, ha nyugodtan, odafigyelve, türelmesen hajtjuk végre az ATM-nél a tranzakciót. Alaposan vegyük szemügyre a kártya behelyező nyílást, és környékét, nincs-e oda felrögzítve egy plusz tartozék, aminek semmi keresnivalója nincs ott. Ezt a kis adatszerző egységet is lefeshetik az automata színére, ami csak nehezíti a felismerését. Általában ehhez párosulni szokott egy minikamera, amelyet vagy az adatszerző készüléken, vagy az ATM automata olyan területén helyezik fel, ahonnan tökéletesen látható a billentyűzet. A minikamerát rendkívül nehéz észrevenni, szinte lehetetlen, de ha látunk is kamerát az automatán, arról azt kell tudni,

hogya az sosem néz a gép billentyűzetére. Mindig egyenesen, az épp az ATM előtt álló ügyfélre fókuszál, rögzíti az eseményeket, és ha esetleges csalásról van szó, akár értékelhető képet is készíthet az elkövetőről vagy elkövetőkről, amelyet tömegkommunikációs eszközök igénybe vételével a körözés során felhasználható. További óvintézkedésként lehetne megemlíteni, ha úgy próbáljuk meg megadni a PIN kódunkat, hogy miután átvizsgáltuk az automatát, semmit sem bízva a véletlenre, igyekezzük minél jobban, és nagyobb részben a másik kezünket eltakarni, amivel a kódot beírjuk. Ügyeljünk arra, hogy a kódot begépelő kezünkkel minél kisebb mozdulatokat tegyünk, ami azért fontos, hogy a kis kamera felvételéről ne lehessen kibogarászni a megadott kódot. Egy olyan trükköt lehetne alkalmazni még, ami a csoportban talán nagy bizonytalanság kiváltására alkalmas. A PIN megadásakor, természetesen a kezünket takarva megadjuk a helyes kódot (nem rontjuk el), viszont az arcminikával illetve a test metakommunikációjával azt sugalljuk, hogy elrontottuk a beírást, és a kezünkkel az eddigi mozgásunkhoz hasonló módon „tovább tevékenykedünk”, imitálva ezzel a törlést, valamint a korrigálást. Természetesen érdemi tevékenység nem történik, mivel a PIN kódunkat helyesen adtuk meg.

Fontos még kiemelni azt a nélkülözhetetlen alkatrészt, ami nélkül az ATM szolgáltatásai semmilyen körülmények között nem vehető igénybe, ez pedig a billentyűzet. Egy billentyűzet úgy épül fel az eszközön, hogy a gombok között hézagok vannak, valamint a gombok kiemelkednek, körülbelül 2-4 milliméterre, egyfajta „úthálózatot” képezve, valamint a kilenc gomb körül van egy perem, ami szintén kimagaslik, ugyanúgy körülbelül 2-4 milliméterre.

Ha az ATM automata billentyűzetet három oldalról takaró pannellel van körülvéve, vegyük ezt is alaposan szemügyre. Nézzük meg a tasztatúra felőli belső részeit, sarkait, nem-e rejtettek el egy mozgóképet rögzítő eszközt. Ha erre utaló jelet találunk, akkor értesítsük a bankbiztonsági szolgálatot, és inkább ne is használjuk azt az ATM automatát. Ne bízzuk el magunkat, hogy ha egy dolgot észrevettünk, ami nem oda illő, és más célt szolgál, mint amire létrehozták és alkalmazták a jog keretein belül, észrevettük a többit is, mert ez korántsem lehet igaz, ugyanis előfordulhat az, hogy magába az ATM automata belsejébe helyezik el az adatszerző eszközt, és olyan szinten eltüntetik a manipuláció külső nyomait, hogy máris bedőltünk a trükknek.

Az ATM nem csak szabad, külső helyszínen fellelhető. Sok esetben állapíthatjuk meg azt, hogy egy elzárt helyiségben kap helyet, ahová csak a bankkártya lehúzás után juthatunk be. Az ilyen esetben is az a teendő, amit az ATM bankkártya behelyezési nyílá-

sánál védekezési mechanizmusként megemlítettem. Gondosan átnézni az azonosító, és egyben a helyiség ajtaját nyitó, kártyaolvasó eszközt.

Egyéb preventív cselekedet, amit ha megejtünk, tovább csökkentjük annak esélyét, hogy sértettek, áldozatok legyenek belőlünk. Ilyen például az, hogy bármikor, akár ATM automatánál állunk, akár egy bankkártyás fizetésnél, soha senki sem legyen a közvetlen környezetünkben! Igyekezzünk megtartani a 2-3 méter tér- és távközt, megelőzve a shoulder surfing PIN-kód szerzési módszert.

Ha véletlen valaki megszólít, hogy leejtettem valamit, vagy bármi olyan dolgot hoz fel, említ meg, ami alkalmas a figyelem elterelésére, ne feledjük el, a bankkártyánk prioritást élvez mindenkor, minden szituációban. Persze ezt nagyon nehéz betartani, és így tenni, mert a meglepetés hatására nem feltétlen tudunk racionálisan gondolkodni, hanem reflexszerűen úgy teszünk, amit épp akkor mondanak. Igyekezzünk minél jobban kontrollálni az agyunkat, a figyelőképességünket, és mindig lebegjen először a szemünk előtt az, hogy a bankkártyám végtelen maradhat, alkalmat adva az eltulajdonítására, rendkívül sok kellemetlenséget, idővesztést okozva magamnak!

Készpénzfelvétel után, a felvett összeget vagy nagyon gyorsan számoljuk meg az automatánál, amelyet meg lehet könnyíteni úgy, hogy mi választjuk ki a címleteket a „tranzakció-varázsló” során. Ezt azonban feltűnésmentesen tegyük meg, nehogy utána később ezért támadjanak meg minket, és raboljanak ki, hogy látták, mennyi pénz lett nálam a készpénzfelvétel után. A készpénzfelvétel kétféle módon történhet. Bizonylattal történik, vagy e nélkül. Nem baj, ha kérünk bizonylatot, sőt a legjobb dolog, ha kérünk, mert tudjuk, hogy mennyi pénz maradt a számlánkon, tartalmazza a felvett összeget, a dátumot, az időt, a helyet, hol került lebonyolításra a tranzakció. Ezek az adatok, ha illetéktelenek kezébe kerülnek, potenciális áldozatok lehetünk, mert olyan bizalmas információk birtokába jutnak az elkövetők, amit nem feltétlen osztunk meg még a közeli ismerőseinkkel sem.

A készpénzfelvételre érdemes olyan ATM automatát választani, ami a bankfiók váróhelyiségében, vagy annak előterében van felállítva, mert az ilyen berendezések több oldalról biztosítottak. Ebből célszerű egy szokást kialakítani, mert annál jobban ismerjük a környezetet, magát az ATM-et, de nem szabad hagyni, hogy ezek miatt ösztönszerűen történjen a készpénzfelvétel.

A bankkártyával kapcsolatban meg kívánom még jegyezni, hogy nagyon figyelmesen válasszuk meg, hova tesszük, akár, amikor magunknál hordjuk, akár otthon a lakásban vagy a házban. Óvjuk meg a külső, fizikai behatásoktól, a mágnesességtől, a hőtől, mert ezek mind működésképtelenné tehetik a plastikot, és mi sem tudjuk használni a saját kár-

tyánkat. A hozzá tartozó PIN kóddal nem lehet egy helyen eltéve, külön-külön rejtekhelyet válasszunk számukra. A legkreatívabb és legbiztonságosabb megoldás az, hogy változtassuk meg a PIN kódot egy általunk könnyen megjegyezhető számkombinációra, ami természetesen nem a születési évszámunk, és nem egy egyszerű számsorozat (pl.: 1234). Így a megküldött PIN kódot tartalmazó biztonsági papírt megsemmisíthetjük, azt nem kell magunknál tartanunk. Ha meg olyanra kerülne sor, hogy valaki akár telefonon, akár e-mailben, akár egyéb manipulált internetes oldalon (ezekről később) próbálja megszerezni, akkor nem szabad senkinek sem megadni! Az azonosítás soha sem zajlik a PIN kód segítségével. Vannak erre más alkalmas, sokkal inkább megfelelőbb azonosítási technikák, amelyekkel az emberi jogok nem szenvednek csorbát.

Véleményem szerint az ügyfél rengeteget tehet a saját maga biztonságaért, ami a pénzügyintézetnek is kötelessége, hogy biztosítsa és tovább erősítse a bankkártyákba vetett bizalom erejét. Bízom benne, hogy hasznos, értelmes tanácsokat sikerült felsorakoztatnom az előző oldalakon keresztül, és ezzel elősegítem a bankkártya-csalások számának csökkenését.

4. Bankkártya adatokkal való visszaélések a kibertérben (Cyber)

A bankkártya adatokkal azonban nem „csak úgy” lehet visszaélni, hogy a kártya fizikai jelenlétét kihasználva, az emberi figyelmetlenséggel megtetézve helyzeti előnyhöz jutva megszerezni a rajta tárolt adatokat, és egy új nyers kártyát előállítva pénzhez jutni, megkoronázva a munkát. Másik nagy módja, amely legalább ugyanolyan veszélyes, mint az utólag legyártott, hamis bankkártya, amikor a megszerzett adatokkal a kibertérben (Cyber) követnek el visszaéléseket a bűnözők, így jutva anyagi vagy egyéb más előnyhöz. Azonban mit nevezünk kibertérnek? A kibertér (cyberspace) a görög kyber (jelentése: hajózni, navigálni) szóból ered és talán úgy lehetne a legjobban meghatározni, hogy egy hajózásra alkalmas tér. A kibertér, mint fogalom feltalálása és magyarázata William Gibson nevéhez fűződik, aki a *Neuromancer* (1984) című regényében így nevezi a hálózatba kapcsolt számítógép-terminálokról közvetlenül elérhető digitális, navigálható teret. A kibertér egy olyan mátrix, ami elektronikus, adattájkép, ahol vagy jobban megfogalmazva, amelyben az egyének és a cégek interaktív kapcsolatba lépnek az információval, sőt kereskedhetnek vele. A fogalom megszületése óta a kifejezést a legkülönbözőbb csoportok használják, amelyből az a konklúzió vonható, hogy gyors ütemben formálódnak a számítógépes kommunikáció és a virtuális valóság fajtái. A világ modernizációja során a regényben szereplő fogalmi meghatározás is átalakult, melyet úgy lehetne kifejezni, hogy a kibertér számítógép-rendszerek és –hálózatok által alkotott olyan virtuális tér, amelyben elektronikus adatokat tárolnak és ami online adatforgalomra, kommunikációra és kapcsolattartásra nyújt lehetőséget. A kibertér általában ott jelentkezik, ahol valamilyen igényt elégíthet ki, vagyis a kibertér tértípusai és alakzatai teljes egészében társadalmi eredetűek. A kiberterről ma már nyugodtan állíthatjuk, hogy a világmindenség részévé vált, hisz emberek milliói élnek az egyes változataiban.³⁹

Sajnos a bűnözésnek több sem kellett, és mivel új terület és bűnözéstől mentes, úgy gondolták a bűnözés képviselői, hogy be kell ezt a világot is hálózni. Eldobták a magvakat, amelyből úgy, mint egy élősködő, kinőtte magát a kiber/számítógépes bűnözés (angolul: cyber crime). „Számítógépes bűnözés alatt olyan bűncselekmények értendők, amelyeket elektronikus kommunikációs hálózatok és információs rendszerek felhasználásával vagy

³⁹ <http://www.pointernet.pds.hu/ujsagok/evilag/2004-ev/04/20070306122418315000000489.html>

ilyen hálózatokkal és rendszerekkel szemben követnek el.”⁴⁰ Szinonimájaként több kifejezés is napvilágot látott, így különösen *számítógépes bűnözés*; *számítástechnikai bűnözés* vagy a *csúcstechnológias bűnözés*. Ennek a bűnözéstípusnak három nagy kategóriáját különböztethetjük meg. Az első nagy kategóriába a „hagyományos” bűncselekmények tartoznak, úgymint csalás vagy hamisítás, de a csoportba való tartozásként azt a feltételt kell felállítani, hogy ezeket a bűncselekményeket az elektronikus kommunikációs hálózatokon és információs rendszereken keresztül kell elkövetni. A második nagy „csokor” az illegális tartalom elektronikus médián keresztül közzétételére vonatkozik (példaként említhetném a gyermekek szexuális kizsákmányolásával kapcsolatos anyagok keltését). A harmadik halmozban az elektronikus hálózatokkal kapcsolatos bűncselekmények tartoznak, mint például az információs rendszerekkel szembeni támadások, a hozzáférés megtagadása és a hacketvékenység.⁴¹

Ezeknek a büntetteknek a felsorolása taxatív nem lehetséges, mivel számtalan tevékenységgel el lehet követni. A felsorolt tettek egy alapkőként szolgálhatnak, amelyeken belül, különféle módokat alkalmazva követik el ezeket a cselekményeket a világ bármely pontján, óriási károkat okozva ezzel nem csak a természetes személyeknek, hanem a pénzintézeteknek is.

4.1. Adathalászat

Az adathalászat egy rendkívül gyorsan terjedő olyan csalástípus, amely az Internet világában van jelen. Fő céljaként a természetes személyek adatainak megszerzése, különös figyelemmel a bankkártya adatokra, személyes adatokra. Többféle módszert dolgoztak ki a bűnelkövetők, amelyekre külön angol megnevezés van a szakzsargonban.

Egyik formája a *Phishing*⁴², amelyről a 4.1.1.-es alfejezet kíván részletesebben foglalkozni.

Másik formaként nevesíthetnénk meg a *Vishing*⁴³-et. Röviden az a lényege, hogy a tettes a kiszemelt áldozatának a telefonszámát megszerzi, és felhívja az adatok kinyerése végett.

⁴⁰ <http://eur-lex.europa.eu/Notice.do?mode=dbl&lang=hu&ihmlang=hu&lng1=hu,en&lng2=bg,cs,da,de,el,en,es,et,fi,fr,hu,it,lt,lv,mt,nl,pl,pt,ro,sk,sl,sv,&val=449272:cs>

⁴¹ <http://eur-lex.europa.eu/Notice.do?mode=dbl&lang=hu&ihmlang=hu&lng1=hu,en&lng2=bg,cs,da,de,el,en,es,et,fi,fr,hu,it,lt,lv,mt,nl,pl,pt,ro,sk,sl,sv,&val=449272:cs>

⁴² Angol szó, három angol szó összevonásából alakult ki: **password harvesting fishing** -- <http://www.cert.hu/content/az-adathal%C3%A1szatr%C3%B3l-phishing-pharming>

Harmadik típus a *Smishing*⁴⁴ néven futó adatszerzési módszer.

A negyedik *Pharming*⁴⁵, amelyről bővebben a 4.1.2. alfejezetben írok.

4.1.1. Phishing

Az Interneten, a „phishing” kifejezés egy olyan bűncselekményre utal, amely csalárd módon szerez meg bizalmas információkat. Számos módja van, hogy a csalás „művésze” megpróbáljon személyese adatokat megszerezni az áldozattól, mint például a TB számot, jogosítvány,- hitelkártyaadatokat vagy bankszámla információkat. Olykor az átverés mestere először azért küld egy jóindulatú e-mailt, hogy beszélgetésbe elegyedjen a kiszemelt áldozattal és azután a pszichikai kapcsolat kialakítása után küld egy adathalász elektronikus levelet. Más esetben már ez a „bevezető”, „felvezető” e-mailt mellőzi az internetes csaló. Az adathalászat az emberi bizalomra épít, ezért a bizalomra építő támadások (social engineering) egy fajtájának tekinthető.

Kijelenthetjük, hogy ennél az esetnél a legfontosabb célja az e-mail küldőjének, hogy bankkártya adatokat (PIN-kód, kártyaszám) szerezzen meg. Először meg kell szerezni az adott pénzügyintézet ügyféllistáját, amelyek alapján felveszi a kapcsolatot az esetek döntő többségében e-mail formájában. Az elektronikus levélben egy figyelemfelhívó üzenet szerepel, és benne van az internetbank weboldalával szinte teljesen megegyezően kinéző oldal, megtévesztve ezáltal a személyt. Ezt az oldalt az elkövető kreálta, valamint manipulálta. Amikor az ügyfél megpróbál belépni az e-bank rendszerébe, az oldal egy hibauzenetet jelez, és tájékoztatja a felhasználót, hogy az internetes banki szolgáltatás valamilyen okból kifolyólag (mondjuk karbantartás miatt) nem üzemel. Ez azonban egy figyelemelterelés, ugyanis a tettes vagy tettesek már megszerezték az adatokat (felhasználónév és jelszó), így hozzáférhetnek a bankszámlán lévő pénzhez és egyéb információkhoz.⁴⁶

⁴³ Angol szó, mely a következőkből tevődhet össze: Voice or Phone Phishing-- <http://blogs.securiteam.com/index.php/archives/467>

⁴⁴ Angol szó a *SMS* and *phishing* kifejezésekből -- <http://www.macmillandictionary.com/buzzword/entries/smishing.html>

⁴⁵ Angol szó, pronounced ‘farming’ szavak képzéséből -- <http://us.norton.com/cybercrime-pharming>

⁴⁶ <https://security.intuit.com/phishing.html>

4.1.2. Pharming

A gyakorlatban úgy alkalmazzák az adathalászatot, hogy „*az adathalászok e-mail üzenetben, azonnali üzenetben vagy szalagcím-hirdetésekből a felhasználót hamis weboldalra invitálják, ahol jelszavának vagy egyéb titkos adatainak megadására kérik*”⁴⁷. Ennek egy speciális változata a pharming, azaz az eltereléses adathalászat. „*Ezzel automatikusan álweboldalra továbbítják a felhasználókat, akik nyugodtan folytatják a tranzakciót abban a hiszemben, hogy a valódi banki vagy kereskedelmi oldalra jutottak*”⁴⁷. Azonban miért nem veszik észre a manipulációt az interneten böngészők? A trükk az ott van, hogy a számítógéphez érő bűnözők az eredeti, legális oldal másolatát készítik el, ugyanolyan fejléccel, logókkal, az oldal kellékeinek megfelelő elhelyezésével. Erről az álinternetes oldalról azt kell még tudni, hogy egy esetleges felhasználó név – jelszó beírásakor (mikor be kívánunk jelentkezni az e-banking felületére) az oldal egy hibát jelez (pl.: Error 404). A laikus felhasználó el is hiszi a hibaüzenetet, így nem tulajdonít neki nagy jelentőséget, de arról egyáltalán nem tud, hogy a bűnelkövetők megszerezték a bejelentkezéshez szükséges adatokat, és így már hozzáférnek az ügyfél bankban lévő pénzéhez, amit kiutalnak a számláról egy, a más általuk korábban létrehozott számlára. A pénz útját meg tudják még bonyolítani, és ezzel egyidejűleg követhetetlenné tudják tenni, hogy több országot érintve mozgatják meg a pénzt, ún. strómanok alkalmazásával, megfelelő védelmet biztosítva magának. A pharmingnak három főlel követési módja ismert.

Az első követési formája a *helyi számítógép DNS megmérgezése*. A DNS szoftver a megadott nevet lefordítja a weboldal hálózati címére, ami az IP- cím. Ez egy időigényes művelet. Ahhoz, hogy a felhasználónak ne kelljen sokat várnia az internetes oldal betöltődésére, a számítógép a korábban meglátogatott oldalak DNS-eiből egyfajta másolatot készít le, amelyet a DNS-gyorsítótárban raktároz el. Mivel weboldalak IP-címeit őrzi meg, egy személyes adatokat fűrkésző trójai vírus⁴⁸ segítségével a tartalma módosítható, így, amikor az ügyfél az e-bank-ját kívánja használni, és megadja az online bankja címét, a számítógépe rögtön a manipulált weboldalt nyitja meg. A felhasználó minden gyanú felmerülése nélkül megadja az azonosító adatait, amelyek így az elkövetőkhöz kerülnek. A módszer azért aljas, mert a számítógép tudatlanságát használja ki, mivel a gép nem tudja,

47

http://securityresponse.symantec.com/hu/hu/norton/library/familyresource/article.jsp?aid=article1_08_06 – mondta Bill Rosenkrantz

⁴⁸ trójai faló: „valamilyen extrafunkcionalitással próbálja rávenni a felhasználót a program elindítására. Máskor rossz indulatú hackerek megtévesztésből való programoknak álcázott trójákat hagynak hátra a rendszerben, és ezek segítségével később visszatérve károkat okozhatnak.”

dr. Simon Béla: A csúcstechnológiai bűnözés és nyomozása, Budapest, 2013., 35. o.

hogyan az IP-cím azért van a gyorsítótárban, mert azt már korábban az URL címsorba írták és megnyitották az oldalt, vagy azért, mert azt egy kártékony program helyezte el ott. Ezeket a trójai vírusokat nem kívánt e-mailek mellékletére, vagy a levélben lévő linkre kattintva lehet feltölteni a gépre, amelyről a számítógépet használó személynek fogalma sincs. Be lehet még szerezni ingyenesen letölthető anyagokon keresztül is (a legtipikusabb ilyen a pornográf jellegű felvételek).

A második elkövetési módja a Cross-Site Scripting (XSS), azaz a valódi weboldalak kódjainak feltörése, megtörése. Egy szkriptet⁴⁹ szűrnak be, amelynek az a funkciója, hogy az oldalon „szörfözőket” becsapják. Ez lehet egy hivatkozás, amire ha rányomnak, az álweboldalra irányít, ami az azonosító adatokra kíváncsi. Ezzel a módszerrel áldozatok ezreit képesek becsapni és megkárosítani.

A harmadik formája a pharmingnak a *szerver alapú DNS mérgezés*. Mint ahogy az első pharming típusnál kitértem, a számítógép rögzíti a DNS lekérdezéseket. Azonban az internetszolgáltató szervere is hasonlóképpen működik. Egy nagyon okos ötletnek mondható, ha ezt a szervert, amely rengeteg személy internetellátásáért felelt, megfertőzik, ugyanis a médiában minden reklámban megemlítik az adott szolgáltatás, üzlet stb. internetes elérhetőségét, weboldalát. Mivel ez a szerver is úgy könnyíti meg a saját, és a használók „életét”, hogy a gyorsítótárába menti a legtöbbször használt internetes oldalakat, ezért ha ebben a tartalomban módosítja jó néhány oldal IP-címét, akkor rengeteg személyt lehet kelepccébe csalni, és manipulált oldalra terelni, ahol meg kell adniuk adataikat, vagy azonosítószerző trójai vírusok telepítését indítja el, miután megnyitják a felhasználók az oldalt.⁵⁰

4.1.3. Közösségi oldalak

Ebben a modern, rohamosan fejlődő világban egyre jobban teret nyer világháló, és azon belül is az egyes közösségi oldalak, ahol minden beregisztrált tag ismerősök után kereshet, kapcsolatot tarthat, személyes élményeit, véleményeit oszthatja meg, valamint képeket tölthet fel, kommentelhet. Nap, mint nap jönne ki, jelennek meg az újabbnál újabb alkalmazások, játékok. Mindezek hatására olyan kapcsolati hálók alakulhatnak ki a kiberterben, amelynek a közvetett segítségével emberek millióihoz lehet kártékony számítógé-

⁴⁹ Szkriptnyelven íródott utasítássor, program. - <http://pcforum.hu/szotar/szkript.html>

Szkriptnyelv: Közvetlenül a forráskódú változatban, futásidőben értelmezett és gépi kódú utasításokká fordított nyelv- <http://pcforum.hu/szotar/Szkriptnyelv.html>

⁵⁰

http://securityresponse.symantec.com/hu/hu/norton/library/familyresource/article.jsp?aid=article1_08_06

pes programokat eljuttatni, telepíteni a számítógépükre. Ezt az elkövetők is nagyon jól tudják! Olyan szinten kihasználják a közösségi oldalak adta lehetőségeket, hogy az ember a barangolás közben észre sem veszi, hogy olyan dolgot nyitott meg, ami a számítógépére káros. Elrejtik például a káros szoftvereket egy játékba, és amíg az betöltődik, addig az alatt feltelepítődik egy adatszerző trójai faló, egy KEY logger alkalmazás (ld. a 4.1.4.-ben), de bevezethetnek olyan „újtásokat”, amelyeket az oldal üzemeltetőinek találmányaként tüntetnek fel, kihasználva az emberiség kíváncsiságát. Legnagyobb veszélyforrásként a fiatalok, közülük is a 14-18 évig terjedő korosztály jelölhető meg, persze ez egyáltalán nem jelenti azt, hogy az idősebb személyek nem lehetnének.

Magyarország egyik legnépszerűbb és legközkedveltebb közösségi oldalán számos hasonló, a már felsorolt trükköket vetették be. A „Facebook” közösségi oldalon az egyik alapvető aktív gomb neve a 'LIKE'. Ha valami tetszik, akár kép, videó, komment stb., akkor ezzel lehet kifejezni az ember nevetését, azt, hogy az adott post elnyerte a tetszését. Ámde, amivel óriási információáramlást tudtak elindítani a számítógép területén jártas bűnelkövetők, az a „DISLIKE” gomb volt. Ha van „LIKE”, miért ne lehetne „DISLIKE” is, ami pont az ellenkezőjét szimbolizálná. A csavar a történetben ott van, hogy ebben az extra opcióban kártékony programok voltak beágyazva, amelyek a plug in (kiegészítő) telepítése alatt aktiválták magukat, megfertőzve ezzel a felhasználó számítógépét és megszerezve a vírusba programozott adatokat, amelyekkel vissza tudnak élni. Általában felhasználónevek és jelszavak. Így is meg tudják szerezni valakinek a fiókjához való jelszót, de előfordulhat az is, hogy feltörik az adott személy facebook profilját. Ennek a személynek ugye elegendő számú ismerőse lehet, akiknek az elkövetők a frissen feltört fiókon keresztül egy linket, vagy képet küldenek. A link fertőzött, nem szabad megnyitni, mert elszabadul a benne rejlő „szörny”, a káros szoftver. Ha képeken pedig vagy segélykérés szerepel és pénzt kérnek, vagy valamilyen felhívás, hogy látogassa meg ezt az oldalt, ne vegyüek komolyan. Említést érdemel még az a jól bevett fogás, amelyet a facebookon alkalmaztak. Egy korábban közkedvelt közösségi oldal (myvip) tulajdonságát ültették át a facebook képességei közé. Ez az a kiegészítő opció, hogy kik nézték meg az adatlapodat. Az oldal azt hirdette magáról, hogy a like-olását, azaz magyarul a „LIKE” gombra kattintva kinyilvánított elismerést követően megmutatja, kik voltak azok, akik előszeretettel láto-gatták a profilod adatlapját. Miután megnyomtuk a feltételként szabott aktív gombot, az oldal küld a mi üzenő falunkra egy „más is lájkolja” postot, viszont amit hirdet, azt nem tárja elénk. A megnyitásával nagyban kockáztatták azonosító és egyéb adatszerző szoftve-
rek telepítését.

A legújabb, a napokban látott közösségi oldalon terjedő vírus az adott oldal tíz éves évfordulója alkalmából adódó kedvességet fertőzte meg. Az adott oldal üzemeltetői a jubileumi napon minden felhasználójának elküldött egy egyperces kis filmet a közösségi oldalon addig „leélt életéről”. A vírus kifejlesztője azt hiteti el, hogy a felhasználó által közzétett megosztások „privát” vagy „XXX” videót ígérnek ismerősüktől. Ez egy link a posztokban. Aki erre rákattint, az az egyik legnagyobb videomegosztó portálon egy figyelmeztető jelzést kap, hogy a Flash Player szoftvere elavult, a videó megtekintése előtt azt frissíteni kell. A „Tovább” („Continue”) gombra kattintva nem az elavult program legfrissebb verziója települ, hanem egy Trojan.FakeFlash. A kártékony program ellopja a felhasználó közösségi oldal hozzáférési adatait, azaz feltöri a fiókot, valamint ellopja a megfertőzött gépet használó képeit, amiket saját maga terjesztésére használ fel. Megoszt egy képet a felhasználó falára, bejelöli rajta az ismerőseit, akik így értesülnek a „hírről”. Aki rákattint, megfertőződik, és a folyamat így megy tovább, láncszerűen. Aki óvatlan volt, és megnyitotta, nézzon körül a böngészésének bővítményei között, mert a vírus oda telepíti fel magát.⁵¹

Sajnos ezek felsorolása sem lehet teljes körű, mert a különféle elkövetési módokat csak az emberi elme szabhat határt, amiről pedig nagyon jól tudjuk, hogy nem ismer korlátokat.

4.1.4. Key logger alkalmazások

A billentyűleütés naplózás (Keystroke logging), amit gyakran neveznek billentyű-naplónak (Key Logging vagy Keyboard Capturing), egy olyan naplózó tevékenység, amikor a billentyűzeten leütött billentyűket úgy rögzíti az ún. Keylogger, hogy a felhasználónak egyáltalán nincs tudomása arról, hogy a leütéseit megfigyelik. Mi is az a Key logger⁵²? Egy olyan számítógépes program, ami a számítógép használója által leütött összes billentyűt naplózza annak érdekében, hogy jelszavakhoz, és egyéb bizalmas információkhoz jusson hozzá a program készítője. Informatikai szempontból két nagy kategóriát tudunk felállítani.

Az egyik a *szoftveralapú Keylogger*-ek, amelyen belül a technikai megvalósulásukat figyelembe véve, több módszer került kidolgozásra. Az első a Hypervisor alapú Keylogger. A program egy operációs rendszer alatt futó vírusban testesül meg. Maga az operációs rendszer érintetlen. A vírus által hatékonyan lesz a gépből virtuális gép. A fo-

⁵¹ http://hvg.hu/tudomany/20140310_facebook_video_virus

⁵² <http://www.oxforddictionaries.com/definition/english/keylogger>

lyamat legjellemzőbb neve a „Kék Halál”. A másodikként a mag alapú Keyloggert említeném. A számítógépen lévő program magában az operációs rendszerben rejtőzik (és innen táplálkozik) valamint innen kezdi meg a billentyűleütéseket naplózni (mert ezek mindig keresztülmennek a „magon”). Az ilyen keyloggerek a „magba” vannak telepítve és emiatt nagyon nehéz őket felfedezni. Azért vannak gyakran rootkit⁵³-ként kivitelezve, hogy megbolondítsa az operációs rendszer „magját” és jogosulatlan hozzáférést biztosítson a hardware-hez (a billentyűzethez). Az ezt a módszert használó keylogger a billentyűzet eszköz-meghajtójaként működhet és így hozzá lehet férni minden olyan adathoz, amelyeket a billentyűzet segítségével írtak be. A harmadik technika az API⁵⁴ alapú billentyűnaplózó. Ezek a keyloggerek átverik a billentyűzet API rendszerében futó alkalmazást. A billentyűzet leütést naplózó program rögzíti a billentyűzetleütési eseményeket, mintha ez az API alkalmazás része lenne. A keylogger ugyanabban az időben érzékeli és rögzíti az eseményt, amikor a felhasználó lenyomja vagy elengedi a billentyűt. A negyedik, amit fontosnak tartok kifejezni, a kötött formán alapuló keylogger. Ezek úgy jelentkeznek be internetes formanyomtatványok kitöltésébe, hogy az internetes böngészést rögzítik. A rögzítés akkor történik meg, mikor a felhasználó befejezi a kitöltést, és rákattint az „OK”, a „Küldés” gombra. Következő módszerként hoznám fel a Memória módosításán alapuló key loggerek titkait. A billentyűnaplózó azért változtatja meg és módosítja a böngészővel és más rendszerfunkciókkal összekapcsolt memóriatáblákat, hogy a naplózó tevékenységét elvégezze. Ezt a technikát azok a víruskészítők alkalmazzák, akik ki akarják kerülni a Windows UAC⁵⁵ funkcióját. Ezt a módszert azonban csak a „Zeus” és a „Spyeye” képes használni. Végezetül, de nem utolsó sorban a Távolról elérhető keyloggerekkel foglalkoznék néhány sorban. A helyi szintű billentyűzet naplózásáért felelős programnak van egy olyan plusz tulajdonsága, amely lehetővé teszi a hozzáférést a célszámítógépen rögzített adatokhoz egy távoli számítógépről. A korábban ismer programok az elkészített naplót visszaszállítják a készítő gépére, ebben az esetben azonban nem.

A másik nagy informatikai kategóriába a *Hardware alapú keyloggerek* tartoznak. Ezek nem függenek semmilyen számítógépszoftver telepítésétől. Főbb fajtái a következők:

⁵³ „Olyan speciális programcsomagok, amelyekkel a támadók beléphetnek a rendszerünkbe, és rendszergazda szintű hozzáférést szerezhetnek.”

dr. Simon Béla: A csúcstechnológiai bűnözés és nyomozása, Budapest, 2013., 39. o.

⁵⁴ Application Programming Interface: alkalmazásprogramozási felület: egy olyan program vagy rendszerprogram azon eljárásainak és azok használatának dokumentációja, amelyeket más programok használnak. Nem kötődik a programozási nyelvhez.

⁵⁵ User Account Control: felhasználói ellenőrzés

A Firmware⁵⁶ alapú keylogger: a BIOS⁵⁷ szintű firmware-t, ami kezeli a billentyűzet eseményeket, úgy lehet módosítani, hogy rögzítse az eseményeket, hogy a szoftvert a BIOS-ba kell betölteni, amihez fizikai és/vagy root szintű hozzáférés szükséges a célszámítógéphez.

A billentyűzet alapú naplózó: Az ezen az elven működő keyloggerek a hardver áramkörének gével használják fel a billentyűzethez való csatlakozás naplózására, ami valahol a számítógép billentyűzete és a számítógép között csatlakozik. Lehet USB alapú, de akár Mini-PCI⁵⁸

kártya is, amit egy nem használt csatlakozóba kell dugni. Több titkos megoldása lehet a szabványos billentyűzet manipulálására. Mindkét megoldás a saját belső memóriájába naplózza a billentyűzet tevékenységet, amelyből később kinyerhető. Nagy előnye még szemben a szoftver alapú keyloggerekkel, hogy nem függ a számítógép operációs rendszerétől, és emiatt nem fogja akadályozni a célgépen futó programokat, illetve más szoftverek (vírusirtók) nem fedezik fel. Ugyanakkor a fizikai jelenlétét ki lehet szűrni, ha például a számítógépen kívül van telepítve a számítógép és a billentyűzet közé.⁵⁹



7. kép



8. kép

Miután látjuk az egyes keyloggerek működési elvét, és ennek célját, kijelenthetjük, hogy ha nem figyelünk oda, akkor könnyen megszerezhetik a bizalmas információinkat, adatainkat. Gondoljunk csak bele, hogy az ügyünk, tranzakciónk kényelmes elintézése érdekében otthon, a számítógépen csatlakozunk az Internetre, és az online bankfiókunkba belépünk. Egy ilyen naplózó a belépéskor szükséges információkat el tudja menteni, mivel billentyűzet segítségével lépünk be az e-bank felületére. Meg kell adnunk az azonosítót, a

⁵⁶ A ROM-ban (Read Only Memory) található program. A ROM egy elektrotechnikai eszköz, amely csak olvasható adatok tárolására alkalmas. A tartalma nem változtatható, a beégett adatok véglegesek.

⁵⁷ Basic Input Output System: a számítógép szoftveres és hardveres része közötti csatlakozás létrehozására szolgál. Az alaplapon lévő BIOS, az egyes bővítményekben lévő BIOS és az ezek eszközmeghajtói alkotják a számítógép BIOS-át.

⁵⁸ Peripheral Component Interconnect: a számítógép és a perifériák összekötésére szolgáló processzorfüggetlen adatbusz

⁵⁹ Képek forrása: http://en.wikipedia.org/wiki/Keylogger#Automatic_form_filler_programs

számlaszámot, és persze a jelszót. Ezt megszerezve az elkövetők is be tudnak lépni, és ki tudnak utalni maguknak annyi pénzt, amennyi a számlán van. Itt már nem is véd a napi limit beállítása, ugyanis már át tudják állítani, vagy ki tudják kapcsolni, és kiutálják az összes pénzt.

Ha az Interneten valaki sűrűn használja az online piactereket, vagy az online webshop-okat, ott is meg kell adni a bankszámlaszámot, a bank nevét, valamint a bankkártyánk CVV vagy CVC háromjegyű biztonsági kódját. Ennek birtokában pedig ők is tudnak a mi számlánkra termékeket venni, amelyeket később értékesítenek, így készpénzzé válva tevékenységüket.

4.2. Adattárak feltörése

Ez egy olyan terület, ahol a bankkártyával rendelkező személy nem tehet semmiről. Ugyanis itt a szolgáltatókat éri támadás, pontosabban azoknak az adatbázisait. A bankoknak, kártyatársaságoknak rendelkezniük kell olyan adatbázisokkal, ahol nyilvántartják a legyártott vagy a kibocsátott kártyákat. A bankoknál pedig az adatbázisban szerepel az ügyfél neve, számlaszáma, az ehhez tartozó bankkártya száma és egyéb olyan személyes adat, amelynek illetéktelenek kezébe kerülése óriási károkat tud okozni. Mind a bankoknak, mind a kártyatársaságoknak olyan informatikai védelmet kell kidolgozniuk és alkalmazniuk, amelyek a lehető legnagyobb védelmet nyújtják az egyes adatbázisoknak, adattáraknak. Ez ugyan rendkívül költséges, de a biztonság terén a pénz nem lehet akadály. Sajnos azonban nem csak a szolgáltatók által alkalmazott informatikus szakértők értenek a védelem kialakításához. A hackerek olyan informatikai tudás birtokában vannak, hogy képesek rengeteg biztonsági rendszer gyengepontjait megtalálni, és ezen keresztül behatolni a rendszer belsejébe, és adatokat lopni. Ezt többféle indítatásból végezhetik. Egyik motivációs tényező lehet, hogy a bűnelkövető banda egy tagja, és az általa megszerzett adatokkal tudnak új kártyát legyártani, vagy pénzt kiutalni, illetve egyéb visszaéléseket végrehajtani. Másik indíték meg az lehet, hogy a hacker semmilyen bűnözői csoportnak nem tagja, hanem „saját vállalkozásként” úgy próbál pénzhez jutni, hogy az általa megszerzett adatokat az ilyen bűncselekményekkel foglalkozó embereknek ad el jó pénzért, akár külön adathordozón, akár az Interneten.

Két nagy, megtörtént példával igyekszem színesíteni eme adatszerzési módszert. Az első nagy eset 2011-ben történt meg Magyarországon, a karácsony előtti vásárlási láz kellős közepén. Akkor több százezer ember kártyájának adatait sikerült megszereznie számítógépkalózkodnak egy a bankokon kívül álló adatkezelőtől. Az adatbázis feltörése egy

ún. Processzor cégen keresztül történt, amely a kúthálózat és a bank között található. Ő kezelte az ügyfelek bankkártya adatait, és azokat a bank felé továbbította. A megszerezett adatok visszaélések lehetőségeinek sokaságára nyújtanak biztos alapot. Természetesen az érintett bankok megtették a szükséges óvintézkedéseket (letiltották a bankkártyákat vagy a vásárlási limitet 0 Ft.-ra állították be, vagy kiemelten monitorizták⁶⁰ az érintett kártyákat). Viszont ezzel az intézkedéssel a bank ellehetetlenítette a sértett kártyák használóinak a bankkártyájuk használatát, ugyanis egyik kereskedelmi egységben sem tudtak vele fizetni.⁶¹

A másik óriási kibertámadás egy online cipőbolt adatbázisának feltörése jelenti, ugyanis közel 24 millió ügyfelének szerezték meg személyes adatait, így különösen a nevüket, telefonszámaikat, szállítási és számlázási címüket, valamint a bankkártyájuk utolsó 4 számjegyét. A teljes kártyaszámot azért nem tudták birtokba venni, mert azokat elkülönítetten tárolták és kezelték. Az online cipőbolt arra kérte az összes felhasználóját, hogy változtasson jelszót.⁶²

Ezekből levonhatjuk azt a következtetést, hogy nincs olyan számítógépes biztonsági rendszer, amely 100 %-os védelmet nyújtana. Itt a szolgáltató vállalkozásoknak kell minél több mindent megtenni a védelem magas fokának biztosításáért. Az ilyen bűncselekményekről még azt érdemes megemlíteni, hogy nagy látencia övezi, mert a nem ilyen nagy horderejű eseteket nem is közlik a nyilvánossággal, és megpróbálják házon belül elintézni, mert ha minden ilyen támadás közismert lenne, az óriási presztízavesztéssel járna, és az még nagyobb kárt okozna az adott cégnek. Jobban megéri neki inkább kifizetni a kárt, minthogy ügyfelek bizalmát veszítse el.

4.3. Botnet

Mi is az a botnet tulajdonképpen? A botnet az ún. zombi számítógépek hálózatának összefoglaló neve. A zombi számítógép olyan számítógép, amelyet különféle vírusokkal és trójai falovakkal irányítás alá vesz egy cracker⁶³ a számítógép használójának tudta nélkül. A számítógép erőforrásait saját célra használja fel.

⁶⁰ Egyes nagybankoknak olyan professzionális rendszerük van, hogy megengedhették maguknak, hogy a kártyatulajdonosok nyugodtan használják tovább a kártyákat, és a 24 órás banki ügyelet figyelte a kártyákat. – A szerző megjegyzése

⁶¹ http://index.hu/gazdasag/magyar/2011/12/15/hazai_bankkartyak_tizezreit_tiltottak_le/

⁶² http://hvg.hu/tudomany/20131004_Elloptak_az_Adobe_Systems_tobb_millio_fel

⁶³ „egy olyan, a számítástechnikához magas színvonalon értő személy, aki tudását elsősorban a saját céljaira használja fel, visszaél vele, és másokat károsít meg. Számítógépekbe hatol be jogtalanul, adatokat szerez meg, és használ fel elsősorban anyagi javakért...”

dr. Simon Béla: A csúcstechnológiai bűnözés és nyomozása, Budapest, 2013., 23. o.

A botnet egyik jellemző célja, hogy nagy teljesítményű, gyors, névtelen infrastruktúrát nyújtson be a spammernek⁶⁴, amellyel könnyen és rendkívül gyorsan tud nagy mennyiségű spam⁶⁵-et küldeni, illetve más illegitim tetteket végrehajtani. Nemcsak a spammerek használnak botnetet, hanem más bűnözői csoportok is, többféle csalárd, ártó szándékkal. Azokat a zombigépeket, amelyeket spamküldésre használnak fel, spambotoknak nevezzük. Ezekkel sikerülhet a spammereknek olyan személyes adatokat megismerni, azokhoz hozzáférni, amelyekkel akár internetes bankfiókba tudnak belépni, és ott illegális átutalásokat végezni.

A botnetet leginkább három területen vetik be. Az egyik az „Address harvesting”⁶⁶, ami spamelők bevált eszköze e-mail címek megszerzésére, begyűjtésére. Egy spamrobot vagy más automatizált program a weboldalakot, chat felületeket vizsgálva összegyűjti az elektronikus levelezési címeket és azokra később spameket küld. Ezek ellen a leggyakoribb védekezési mechanizmus a rejtjelezett⁶⁷ vagy az eldobható e-mail címek⁶⁸ használata.

A másik a DOS vagy DDOS támadás a spammer érdekeit sértő számítástechnikai berendezések ellen. A Denial of Service (röviden DOS) olyasmit jelent, mint hozzáférhetlenné tenni, üzemen kívül helyezni. Technikailag nézve az történik, hogy a DOS-támadások alkalmával egy szerveret olyan sok kéréssel bombáznak, amelynek következtében a rendszer a feladatokat egyszerűen nem képes ellátni, és legrosszabb esetben felmondja a szolgáltatást és összeomlik. Ilyen módon támadtak már ismert szervereket, mint az Amazon, Yahoo, eBay, a normális adatforgalom több mint négyszeresével, és így egy bizonyos időre a normális kérések számára üzemen kívül helyezték.

Azok a programok, amelyeket DOS-támadásokra használnak fel, időközben nagyon fejlődtek, és a támadókat csak nagyon nehezen lehet felderíteni, mert az adatok útja homályban marad. Némely támadás lehetséges bug-okon keresztül, vagyis a programok és operációs rendszerek gyenge pontjainak kihasználásával, vagy a protokollok szabálytalan használatával. Más támadások egyszerűen túlterhelik a rendszert a túl sok kéréssel. Ebből kifolyólag a DOS-támadásnak különböző formái léteznek:

⁶⁴ spam levelek küldőjének gyűjtőneve

⁶⁵ kéretlen, általában elektronikus lánclevél

⁶⁶ http://hu.spam.wikia.com/wiki/Address_harvesting

⁶⁷ az e-mail címeket gyűjtő robotok a weboldalakot vizsgálva keresnek aktív elektronikus levelezési címeket. A robotok többsége a címekben használt kukac (@) karaktert keresi, amit megváltoztat. -- http://hu.spam.wikia.com/wiki/Rejtjelezett_e-mail_c%C3%ADmek

⁶⁸ A spammerek robotjai az address harvesting módszerrel weblapról weblapra lépkedve gyűjtik azokat az e-mail címeket, melyekre később kéretlen reklámleveleket küldenek. Ezek ellen az egyik védekezési mód az eldobható levelek használata a DEA technika (**D**isposable **E**-mail **A**ddress) -- http://hu.spam.wikia.com/wiki/Eldobhat%C3%B3_e-mail

Az egyik a *Syn Flooding*. A kapcsolatok kialakulásának elején egy ún. Handshake (kézfogás) megy végbe, mintha üdvözlőnék egymást a béke jelével. A folyamat idején ún. SYN⁶⁹ és ACK⁷⁰ adatcsomagok cserélődnek ki. Egy ilyen támadás esetén a számítógép rendszerébe olyan SYN csomagok kerülnek, amelyek egy hamis IP címet viselnek. Erre a számítógép megpróbál SYN-ACK csomaggal válaszolni, de a hamis cím miatt nem sikerül. Nagy tömegben érkező, hamis SYN csomagok esetén a megtámadott gép az összes kapacitásával a kapcsolat létrejötte érdekében SYN-ACK csomagokat küld, és így nem lesz más rendszer számára sem elérhető.

Egy másik módja a *Ping Flooding*, azaz az elárasztás. A Ping egy olyan program, amely megvizsgálja, más számítógépek elérhetőek-e az adott rendszerben. Ennél a támadási típusnál a támadó a célszámítógépet rengeteg pinggel árasztja el. Így a gép az ezekre történő válaszokkal van elfoglalva, és a Pingek típusától és méretétől függően a régebbi típusú operációs rendszerek összeomlásához vezethet. Ezzel egyidejűleg akadályozzák azt a hálózatot is, amelynek a megtámadott gép a részét képezi. A rendszerkiesés mellett óriási költségek is keletkeznek.

A következő DOS támadási módszer a *Mail bombázás*. Ennél egy hatalmas méretű üzenet jut el elektronikus levél formájában a címzetthez, vagy egy címzettet terhel meg több ezer ilyen levéllel, ami a levelezési fiók telítettségéhez vezet. Legrosszabb következménye az lehet, hogy a levelezési rendszer teljesen összeomlik, így védtelenné válik, és a támadóknak sokkal egyszerűbb dolga van, és meg tudják így szerezni a kívánt személyes adatokat, PIN kódokat, felhasználói neveket, és egyéb információkat, amelyekkel vissza tudnak élni.

Az utóbbi időben kezdett el leginkább terjedni az ún. „elosztott DOS-támadás” (Distributed Denial of Service). A támadás nem egy gépről, hanem gépek sokaságáról érkezik. A gyakorlatban ez úgy működik, hogy a hacker elosztja támadási programját több ezer indifferens számítógépre. Közkedveltek az egyetemek szerverei, mert ezek éjjel-nappal dolgoznak. Így ezek a támadás eszközeivé avansáltak elő. Amikor megkapják a hackertől a parancsot, gépek kérések tízezreivel sorozzák meg a célterületet (pl.: egy web-szervert) üzemképtelenné téve azt. Az ilyen típusú támadásokat rendkívül nehéz kivédeni, mert először meg kell kapni az adatokat, hogy azokat a célszámítógép megfelelőképpen analizálni tudja. Azonban ez az időpont már késő, mert a támadás „halálos sebet” ejtett.⁷¹

⁶⁹ Szinkronizáló/kapcsolatkezdeményező csomag

⁷⁰ Nyugtázó/elfogadó csomag

⁷¹ <http://www.biztonsagosinternet.hu/tippek/denial-of-service-tamadasok>

A harmadik a különböző típusú és fajtájú spam-ek küldése.

A botnet hálózatot hétköznapi, otthoni, iskolai, esetleg vállalati gépek alkotják. Egy számítógép anélkül is tagja lehet egy ilyen kapcsolatláncnak, hogy ezt a gazdája vagy a használója kérte volna, beleegyezett volna, vagy akár egyáltalán tudna róla. Egy számítógép úgy válhat zombigéppé, hogy egy speciális program települ rá, amely a háttérben is fut anélkül, hogy a számítógépet használó személy ezt érzékelni vagy észrevenné. Ezek a titkosan futó programok bizonyos időközönként kapcsolódnak a spammerhez, aki parancsokat, feladatokat ad neki. Ez a kapcsolódás az esetek többségében egy IRC-szerverhez⁷² történik, ami nyilvános. Egyes csatornák forgalmát figyel, és felismeri a spammer által kódolt formában küldött parancsait.

Egy botnet akár több tízezer számítógépből is összetevődhet. Méretük folyamatosan változik, néhány számítógépről megállapítják, hogy zombivá vált, azonban szinte minden percben csatlakozik egy másik, új számítógép.

4.4. Darknet – carding sites

A Darknet a világhálónak az a része, amelyet egy hétköznapi böngésző nem képes betölteni az Interneten „szörfözőnek”. Tulajdonképpen egy árnyékvilág. A legjobban úgy lehetne jellemezni, mint egy jéghegy. A jéghegy látható része, tehát ami a víz felszíne felett van, az a teljes méretének az 1/8 része. A Darknet esetében is erről beszélhetünk. Ennek tudatában nyugodtan megfogalmazható az a teória, hogy ami nincs az Interneten, azon belül is a Darknet részén, akkor az nem is létezik. A világháló keresőmotorjai segítségével egy laikus azt hiheti, hogy bármit megtalálhat a webes felületen. Ámde óriásit téved, ugyanis a keresőmotorok sem képesek felölelni, elemezni-értékelni bizonyos internetes területeket. A láthatatlan web a World Wide Web (www) azon oldalai részét képezi, amelyek nincsenek indexelve az általános keresők által. Így kijelenthető az, hogy a Darknet a Deep Webnek az a része, amely különböző megoldásokkal anonimizálva és titkosítva van annak érdekében, hogy az adott oldalakon folytatott illegális tevékenységet leplezze. De mit nevezünk Deep Webnek? A Deep Web (más néven: mély/rejtett web) azokat a tartalmakat jelöli, amelyek funkciójukból, struktúrájukból vagy formátumukból adódóan nem kerülnek a keresők által indexálásra, így egy normál keresővel nem is találhatók meg,

⁷² **Internet Relay Chat:** „az Internet IP alapú protokolljaira alapuló kommunikációs szolgáltatás, mely lehetővé teszi tetszőleges számú felhasználó valósidejű társalgását írásos formában. Ez szerver-kliens formában zajlik, azaz a felhasználók erre a célra készített programokkal (a továbbiakban: irckliens, kliens) csatlakoznak a felhasználók közötti kommunikációt lebonyolító központi számítógépekkel”
<http://www.irc.hu/page1.html>

mint ahogy fentebb említettem. Azonban a titkossága, meg a speciális képességei, valamint a felépítése miatt nem egy rossz, illegális területre kell gondolni, sőt azt is meg lehet állapítani, hogy nagy része rendkívül hasznos, bárki által elérhető, ingyenesen hozzáférhető tartalmakból áll. Az egyedüli probléma abban mutatkozik meg, hogy jóval nehezebb megtalálni és elérni, mint a normál internetes - publikálásra szánt - tartalmakat. A Darknetet azért szokták a Deep Web-hez sorolni, mert szintén láthatatlan a legtöbb kereső számára főleg az anonimitása és a titkosítása miatt, emiatt fogalmi zavarok keletkezhetnek. Elsődlegesen a TOR hálózaton működő oldalakat szokták a Darknet-hez sorolni, azonban ennek egy része szintén nem illegális, ugyanis vannak például legálisan működő email, tárhely, stb. szolgáltatások.

Mivel láthatatlan/rejtett, így méretéről sem lehet pontos adatokkal szolgálni. Természetesen megpróbálták megbecsülni a kiterjedését, amelyekről tanulmányok születtek és láttak napvilágot. Ezek szerint mintegy 550-szer lehet nagyobb, mint a felszíni (látható) web. Ez tárterületben kb. 7500 TB (terabyte) információt jelent. A Deep Webről készült tanulmányok különféle, becsült kimutatásokkal jellemezték eme „sötét világot”. A havi forgalma akár 50 %-kal is meghaladhatja a látható webét. A „sötét oldalon” lévő oldalak összekapcsolása magasabb szinten van. A rajta lévő információk sokkal precízebbek, részletesebbek, „mélyebbek” (akár a neve). Nagy előnyeként lehet még megemlíteni, hogy a tartalmának 95 %-a ingyen, mindenféle előfizetések nélkül hozzáférhető, persze ha rendelkezünk megfelelő böngészővel.

Azonban hogyan képes egy ekkora „világ” teljesen láthatatlan a való világ előtt? Rengeteg ok sorakoztatható fel a magyarázatok listáján. Ilyen például, hogy az oldal tartalma egy külön adatbázisból töltődik fel a weblapra. Ehhez különböző adatbázisokat le kell kérdezni. A „sötét oldalra” való bejutás csak regisztráció útján történik, ugyanis meg kell határozni már az elején, hogy a gépünknek milyen szerepet szánunk ebben a rejtett világban. Okként említhető meg a különböző scripteket tartalmazó oldalak teljes vagy részleges kizárása, amelyeknek az URL címe kérdőjelet tartalmaz. Komoly magyarázatként szolgál a titkosságára, hogy egy oldalra vagy egy egész site-ra egyáltalán nem mutat link, így elkerülve azt, hogy a tartalma bekerüljön egy kereső adatbázisába. Hiányoznak az indexeléshez szükséges kulcsszavak. Az adott oldal egyáltalán nincs bejelentve, ha véletlen mégis be lenne, akkor egy még speciálisabb keresőre van szükség a rájuk találásra.

Mit lehet tulajdonképpen ebben az óriási adathalmazban fellelni? Miért éri meg, hogy egyáltalán működjön, fennálljon egy ilyen világ? Azért, mert itt minden olyan illegális tevékenység végezhető, amelyet a hatóságok nem tudnak még felderíteni, és bizonyítani

részben a technika adta titkosításoknak, részben pedig a jogi szabályozás miatt. Egy szóval minden, ami szem szájnak ingere. Bármit meg lehet venni: kábítószer, fegyvert, bérgyilkost, de a témánk szempontjából nagyon fontos a megszerzett bankkártya adatok. Az elkövetői csoportok, akik az adatok megszerzésére specializálódtak, ezen a webes felületen korlátlan mennyiségben, illetve a megszerzett adatok erejéig, de képesek eladni "munkájuk gyümölcsét". Természetesen nem csak a megszerzett adatokkal lehet üzletet kötni, hanem a legyártott adatszerző eszközökkel, azok használati utasításával, tanácsadással, esetleges humán szolgáltatás felajánlásával is. Ennek az üzletnek abszolút, de nincsenek határai, teljesen az emberi fantáziára van bízva, hogy miből próbál meg profitálni. Ezzel olyan szintű károkat tudnak okozni, és olyan jövedelmező üzletet tudnak kötni, amely tovább inspirálja őket tevékenységük folytatására minden empátikus érzést kiölve belőlük. Ezen a világon bármi, bárhova eljuttatható anélkül, hogy bármely hatóság tudomására jutna a cselekvésekből, bűncselekményekből bármi is.

A Darknet „motorjának forgása” három fontos tényezőn alapszik. Egyrészt a Tor⁷³ anonim hálózat routerrendszerén, másrészt a levelezéshez és üzenetküldéshez használt PGP-titkosításon⁷⁴, és harmadrészt a szintén anonim bitcounvalután⁷⁵.

A rejtett weben való keresés során a linkeket nem kezeli a böngésző, mert egy nem hivatalos tartománynév alatt vannak elrejtve. Ez csak a Tor hálózaton keresztül működik. Ha sikerül regisztrálni és belépni, akkor minden oldal lehívása három, titkosított, elrejtett szerveren fut át, így rejtve el a valós IP címet. Ráadásul a Tor böngésző gyakran új kapcsolatot választ, még jobban ellehetetlenítve a visszakövetést.

Azonban nem tud minden rejtve maradni. Az itt vásárolt áruk azonban valamikor, valahol fizikailag testet öltenek, de hát a kézbesítésre is megvannak eme világnak a bevált praktikái, hogy minél jobban konspirálni lehessen a cselekményt.⁷⁶

4.5. Felderítési nehézségek

Rendkívül fontos dolog azzal foglalkozni, hogy lehet ezt az Interneten terjedő, törvénybe ütköző cselekedeteket, bűncselekményeket felderíteni, bizonyítani. Sajnos olyan

⁷³ The Onion Router (magyarul: a Hagyma Elosztó)

⁷⁴ Pretty Good Privacy: egy olyan számítógépes program, ami titkosításra és hitelesítésre egyaránt használható. Egy aszimmetrikus titkosítási eljárást használ, amihez szükség van a címzett nyilvános kulcsára. A címzett a saját kulcsával és az üzenetben található kulccsal képes dekódolni az eredeti üzenetet. Ezt a titkosítási módszert alkalmazzák e-mailek, fájlok, mappák, merevlemezek titkosítására.

⁷⁵ A Darknet nyílt forráskódú, digitális fizetőeszköze.

⁷⁶ http://hu.wikipedia.org/wiki/L%C3%A1thatatlan_web

<http://baserape.hu/darknet-vedett-halozat-vege/>

<http://motherboard.vice.com/blog/darknet-touring-the-hidden-internets-illegal-markets>

szintű technikai fejlettség van az Internet egyes perifériáin, hogy iszonyatosan könnyen képesek megoldani egyre több mennyiségű és nagyobb méretű adatok, információk tárolását. Ezzel képesek növelni a kapacitást, és képesek fejleszteni a már amúgy is ultramodern világot.

Ahhoz, hogy ez a továbbfejlesztés ne legyen akadályozva, egy olyan magas szintű titkosítási eljárást kellett kidolgozni, amely biztosítja a „nyugalmat”. Azt szokás mondani, hogy 100 %-os védelmi rendszer nem létezik. Ez az állítás ugyan igaz, de amit sikerült a Darkneten kiépíteni, az a maximum közelében tartózkodik. Azzal, hogy nincsenek indexelve az oldalak, nincsenek linkek, amik az oldalra ugranának, szinte teljesen ellehetetleníti korábban végrehajtott a böngészési folyamat megismerését.

A titkosítással nem csak a keresések és a meglévő internetes oldalak érintettek. Ahhoz, hogy ez kiteljesedjen, de a rendszer működőképes maradjon, szükség volt a kommunikációs csatorna magas fokú rejtettségére is. Ugyanis, ha ez nem lenne kivitelezve, akkor az egész szinte nem érne semmit, mert megtörtént kommunikáció tartalmából könnyen lehet következtetni, hogy mi lett megbeszélve és mikorra, így ki lehet dolgozni a megfelelő taktikát és egyszerűbbé válhat az elkövetők kézre kerítése.

Komoly hátráltatást jelent még a hatóságok számára, hogy a nemzetközi jogi szabályozás eltérő. Egyes országokban valamit meg lehet tenni a hatóságoknak, máshol ez már törvénybe ütközik. Véleményem szerint, amíg jogilag nincs meg a közös nevező, és nem kapnak a hatóságok valamivel nagyobb intézkedési teret, addig a hatékony fellépés várat magára.

4.6. Prevenció

Természetesen, hogy ne váljunk áldozatokká, mi magunk is elég sok mindent tehetünk meg ennek érdekében. Amikor számítógép vásárlásra adjuk a fejünket, vagy egyáltalán számítógépet használunk, rendkívül fontos, hogy szerezzünk be érvényes licence-ű vírusirtó programot, melyek a jelentkező kártékony programok, számítógépen történő felbukkanása esetén azonnal küldenek egy figyelmeztető üzenetet, és a fertőzött programot karanténba helyezik. Egy friss, érvényes vírusirtó képes a használt böngésző védelmére is. Fontos megjegyezni, hogy nincs tökéletes vírusdetektor program, de nagyban lehet csökkenteni a fertőzés veszélyét. Nem árt az sem, ha havonta lefuttatunk egy teljes ellenőrzést, nem csak a számítógépen, hanem a birtokunkban lévő pendrive-okon, valamint az okostelefonokon.

Ahhoz, hogy böngészni tudjunk, internetes elérhetőségre van szükségünk. Ez történhet vezetékes csatlakozással (LAN), vagy vezeték nélkülivel (WLAN). Magas prioritást élvez, hogy a vezeték nélküli hálózatot megfelelően legyen konfigurálva, el legyen látva jelszóvédelemmel, és a titkosításának beállítottságát sem szabad figyelmen kívül hagyni. Így sokkal nehezebben tudnak a saját hálózatunkra rákapcsolódni, és kártékony programokat elhelyezni a számítógépünkön. A kalibráláshoz nyugodtan fogadjunk fel informatikust, aki megbízható, és nagyon érti ezt a területet.

Miután elértük azt, hogy legyen internetes elérhetőségünk, foglalkoznunk kell a saját tevékenységünkkel, böngészési szokásainkkal, ugyanis az esetek döntő többségében elkerülhető lenne az áldozattá válás, ha megfontoltabbak lennénk, és jobban átgondolnánk, mire is kattintunk. Egy hétköznapi közmondást is át lehet erre fogalmazni, úgymond modernizálni lehet. „Előbb gondolkodj, aztán beszélj!”-ből lehetne „Előbb gondolkodj, aztán klikkelj!”. Meg kell próbálni a saját kíváncsiságunkat legyőzni, és objektíven, reálisan látni a veszélyforrásokat.

Az elektronikus levelezőfiókunkban csak azokat a leveleket nyissuk meg, amelyekről 100 %-ig meg vagyunk győződve, hogy csak nekünk címezték, ismerjük a feladót. Ha nem ismerjük, vagy olyan levél érkezik, hogy „Gratulálunk, Ön nyert!”, és tudjuk, hogy nem játszottunk meg sehol semmit, akkor ne kattintsunk rá, mert ez biztosan ártó szándékú üzenet lesz. Az ilyen kéretlen (spam) leveleket válasza se méltassunk, sőt meg sem szabad nyitni, mert a rafináltabb hackerek azt csinálják, hogy a megnyitással egyidejűleg feltelepítődik a káros program, ami vagy teljesen automatizált, vagy a támadó parancsára vár, és vagy elküldi a billentyű naplózás eredményét, vagy botnet hálózatba kapcsolja a számítógépünket.

Az e-mailekben ráadásul teljesen arcátlanok a támadók, mert olyan funkciókat képesek manipulálni, amelyekre hirtelen nem is gondolnánk, másrészt garantáltan rákattintanak a „szörfözők”. Ilyen lehet például a „Leiratkozás itt” linkbe vagy a reklámlakok jobb felső sarkában elhelyezett „X” (Bezár) gombba, illetve a „Hirdetés átugrása” linkbe elhelyezett vírusok és egyéb kártékony programok.

A mai világban az emberek túlnyomó többségben valamilyen közösségi portálon fiókkal rendelkeznek. Alapszabály, hogy magunkról minél kevesebb személyes adatot osszuk meg! Ne ajándékozzuk meg az elkövetőket azzal, hogy „ezüst tálcán” kínáljuk a hozzánk, illetve a privát dolgainkhoz az elérési útvonalat. Ne dőlünk be minden egyes szolgáltatásnak, újításnak, amelyeket a közösségi oldalakon eszközölnek! Legyünk meg-

fontoltak, és tudjunk parancsolni az agyunknak! Ne legyünk mindenre kíváncsiak, mert a csalások, átverések zöme ezt használja ki.

A folyamatos böngészés során kialakulhatnak olyan igények, hogy időt spóroljunk meg, és egyszerűbbé téve az ügyintézési folyamatot, különféle online felületeket használunk az ügyek elvégzésére (Pl.: netbanking stb.). Ezt a tettesek is nagyon jól tudják, így igyekeznek az adódó lehetőséget kihasználni, és adatokhoz hozzájutni. Ezek módszereit fentebb ismertettem. Megelőzni úgy lehet, hogy egy esetleges hibaüzenetnél megnézzük, hogy hova navigáltak minket, mert hiába szinte 100 %-osan megegyező az újonnan betöltött oldal, azon, ha manipulálva van, érdekes dolgok figyelhetők meg. Ilyen például, hogy rengeteg a helyesírási hiba, esetleg stilisztikai probléma figyelhető meg. Fontos tudni (amit már az előző fejezetben is kifejtettem), hogy a bankok és egyéb szervek sem kérnek semmilyen kódot az azonosításhoz! Ha ilyet kér az adott oldal, akkor biztosan egy kreált, hamis oldalon tartózkodunk. Ha valamilyen nagyon fontos ügyben kell intézkedni, ami nélkülünk lehetetlen, akkor arról úgy is postai úton értesítenek, és személyesen meg kell jelenni a meghatározott fiókban, vagy helyen. Az azonosítás majd a helyszínen történik.

Ellenőrizzen minden azonosítást kérő weboldalt vagy URL-t! Győződjön meg róla, hogy a kért weboldal az ismert, hiteles címen nyílik meg, nincsenek a címben oda nem illő karakterek!

Megbízható, hivatalos internetszolgáltatóval szerződjön! Az eltérítéssel szemben az első védelmi vonalat az internetszolgáltató szigorú biztonsági követelményei jelentik.

Ellenőrizze a tanúsítványt! A weboldal hitelességének ellenőrzése csak pár másodpercet vesz igénybe. Az Internet Explorer legújabb verziója és számos más, általánosan használt webböngésző „Fájl” menüjében kattintson a „Tulajdonságok” menüelemre, vagy jobb egérgombbal kattintson bárhol a böngésző képernyőjére, és a megjelenő menüablakban válassza a „Tulajdonságok” menüpontot. A „Tulajdonságok” ablakban kattintson a „Tanúsítványok” gombra, és ellenőrizze, hogy az adott webhely rendelkezik-e a jogos tulajdonos hiteles és érvényes tanúsítványával!

Ha biztonsági szempontból érzékeny weboldalra kíván látogatni, soha ne közvetlenül e-mailben vagy weboldalon lévő hivatkozásra kattintva tegye. A hivatkozást vágja ki és illessze be egy új böngészőablakba, vagy használjon könyvjelzőt.

5. Esettanulmány

Miután „kiveséztük” a téma elméleti szféráját, ismerkedjünk meg a gyakorlatban történő felbukkanásával, megjelenésével. Az ügyben négy orosz állampolgárságú, és egy nigériai állampolgárságú személy vesz részt. Közülük valamennyien az International Business School (továbbiakban: IBS) iskola hallgatói voltak. Az I. rendű vádlott, aki korábban Moszkvában két évet tanult informatikát, azért jött Magyarországra, hogy tanuljon. Ennek költségeit szülei finanszírozták. Az V. rendű vádlottal élettársi kapcsolatban állt az elkövetést megelőzően, valamint az elkövetés alatt. Korábban még sohasem volt büntetve.

A II. rendű vádlott is szintén orosz nemzetiségű. Az I. rendű vádlott meghívására érkezett Magyarországra, kisebb összeggel a zsebében. Ő is, mint társa, büntetlen előéletű volt.

A III. rendű vádlott nigériai állampolgár, aki már korábban Magyarországon élt, és itt dolgozott. Szintén büntetlen előélettel bíró személy.

A IV. rendű vádlott szintén orosz állampolgárságú személy. Az I. rendű vádlott unokatestvére. Egy Budapesten működő IBS aktív státuszú hallgatója, akit unokatestvéréhez hasonlóan, szülei finanszíroznak a külföldi tanulmányok teljesítésében. Csakugyan, mint rokona, illetve ismerősei, ő sem volt még büntetve.

Végül, de nem utolsó sorban az V. rendű orosz származású vádlott egy Budapesten működő főiskola passzív státuszú hallgatója volt, és mint már említettem az I. rendű vádlottal volt élettársi kapcsolatban. Édesanyja támogatta őt a külföldi ügyeiben, tanulmányaiban. Szintén nem töltött még időt büntetés-végrehajtási intézetben.

Hogyan is alakult a „nagyszabású” életük hazánkban? Az I., a II., és az V. rendű vádlott 2007 második felében bankszámlákat nyitottak egy egyik pénzintézetnél úgy, hogy személyazonosságuk igazolására más, létező személy nevére szóló, valódi, litván útlevéleket használtak fel, melyeket úgy hamisítottak meg, hogy kicserélték a rajtuk lévő képeket, sőt bizonyos esetekben az útlevélekről készített fénymásolatokat is aláírták a névtulajdonosok helyett. Ezeket a bankszámlanyitásnál fel is használták céljaik elérése érdekében.

Ezen vádlottak 2007. évben annak a pénzintézetnek, ahol számlát nyitottak, 63 ügyfelének számítógépére rejtett távirányítással (számítástechnikai rendszer védelmét szolgáló intézkedés kijátszásával) jogosulatlanul beléptek, és megszerezték az internetes (netbanking) felhasználói nevét és jelszavát. Ezen adatok felhasználásával beléptek e pénzintézet szerverének portáljára, és az ügyfelek számláiról jogosulatlanul kezdeményeztek

átutalásokat az általuk már korábban megnyitott bankszámlára. Az összegek nagy részét később készpénzben fel is vették. A bank az érintett ügyfelek kárát megtérítette, így a társaság sérelmére 47. 848. 399 forint értékben kíséreltek meg bűncselekményt elkövetni. A pénzintézet tényleges kára 42.957.717. forintra rúgott, ugyanis néhány cselekményük kísérelti szakban rekedt, így nem jutottak készpénzhez. Ezeken túlmenően ugyanennél a pénzintézetnél további 33 ügyfélnek az internetes (netbanking) hozzáférési adatait szerezték meg a már ismertetett módon, de ezekkel nem történtek visszaélések.

2008-ban az I., a II., a III., és a IV. rendű vádlottak az év első hónapjaiban egy másik pénzintézetnél (továbbiakban: 2. bank) készpénzkiadó automatájára egy, az eredetire megtevesztésig hasonlítható álbillentyűzetet, valamint egy hamis kártyaolvasó nyílást telepítettek, melyek teljes mértékben elfedték a készülék saját billentyűzetét és kártyaolvasó nyílását. A hamis kártyaolvasó nyílás az ügyfelek által behelyezett bankkártyák mágnescsíkján rögzített adatokat-miközben azok keresztülhaladtak rajta- lemásolta, majd az ebbe épített, SMS küldésére alkalmas modulon keresztül továbbította a vádlottaknak. Amikor az ügyfél begépelte a PIN kódját, azt az álbillentyűzet rögzítette, majd ez is a beépített modulon keresztül továbbítódott a tettesek számítógépére. Ily módon 93 ügyfél bankkártyájának adatait sikerült megszerezni, amelyekből 29 esetben hamis készpénzhelyettesítő fizetési eszközt, ún. „fehér (nyers) plastik” bankkártyát, készítettek, amelyekkel ATM automatáknál készpénzfelvételt kíséreltek meg. Az ügyfeleket a kibocsátó pénzintézet minden esetben kártalanította. Az okozott kár 2.005.000 forintot tett ki.

Továbbá további 7 magyar, illetve 8 feltehetően külföldi ügyfél bankkártyájának adatait szerezték meg, amelyek felhasználásával szintén „fehér plastik” kártyákat gyártottak le. Visszaélésekre nem került sor, mert az I. rendű vádlottat tetten érték. Az I. rendű vádlott rendőri intézkedés alá került az egyik ATM automatánál, amelynek során 29 darab nyers plastik kártya, egyik táskájából 849.000 forint, másik táskájából 227.000 forint került elő. Ezt követően az I. és az V. rendű vádlottak bérleményeiben házkutatás fogatosítására került sor. E során megtalálták az álbillentyűzetet, a hamis kártyabefogadó nyílás moduljaiban lévő SIM kártyák tokjait, az eszköz leírását, a „fehér plastik” kártyák készítésére szolgáló számítógépes szoftvert, a készpénzkiadó automaták címeit, fényképeit, valamint a hamis közokiratokat (útleveleket). Az ATM-ből megszerzett adatok egy részével rendelkező nyers kártyákat valahogyan kijutatták az országból. Így ismeretlen társaik 2008 elején egy külföldi városban 29 nyers bankkártyával 67 alkalommal kezdeményeztek készpénzfelvételt. Ezek eredményeképpen 227. 618 forint profitra tettek szert. Az I. rendű vádlott további 339 külföldi ügyfél bankkártyájának adatait szerezte meg lejáratí dátummal

és a három- illetve négyjegyű CVV/CVC kódokkal együtt, így az adatok egy részét az interneten történő vásárlásra használták fel, a többi adatot pedig hamis készpénz-helyettesítő fizetési eszköz mágnescsíkjára telepítették. A IV. rendű vádlott 103 magyarországi felhasználó, különböző internetes alkalmazásához szükséges adatait (számlaszámokat, netbanking felhasználói neveket és jelszavakat, internetes levelezéshez használt azonosítókat és kódokat) és egyéb személyes adatait, valamint további 318 kártya adatait szerezte meg lejárat dátummal és a három- vagy négyjegyű CVV/CVC titkos kódokkal együtt, úgy azok interneten történő vásárlásra, és hamis készpénz-helyettesítő fizetési eszközök előállítására váltak alkalmassá.

Ez ügyben a nyomozást a Nemzeti Nyomozó Iroda (továbbiakban: NNI) 2008. március 21-én vette át a különféle helyi szintű nyomozó hatóságoktól. Az 1. pénzintézet tett feljelentést ismeretlen tettes ellen, akik egyik ügyfelük számlájáról mintegy fél millió forint átutalására adtak megbízást egy IP címről. A kedvezményezett egy litván állampolgár volt, akinek szintén ugyanennél a pénzintézetnél volt nyitva számlája. Az átutalás megtörtént, de a hatóság biztosítási intézkedést⁷⁷ foganatosítva a kérdéses összeget zárolta.

Az IP cím beazonosítása érdekében a *www.ripe.net* internetes oldalról lekérték az említett IP cím felett rendelkező internetes szolgáltatót. Ennek ismeretében megkereséssel lehetett élni a cég felé annak megismerésének reményében, hogy ki az előfizető, de erre sajnos nem tudtak érdemben válaszolni, mert titkosították.

Ugyanez a bűnszervezet 2008-as évben Budapest különböző kerületeiben hasonló időben egyszerre követtek el visszaéléseket más-más ATM automatáknál. Ezek az ATM-ek azonban mind egy bank tulajdonát képezték. Ezek ismeretében folytatólagosan elkövetett készpénz-helyettesítő fizetési eszközzel visszaélés⁷⁸, valamint nagyobb értékre elkövetett készpénz-helyettesítő fizetési eszközzel visszaélés kísérlete miatt folytatódott a büntető eljárás.

A nyomozás fordulópontját jelentette 2008. február 18-án, hogy a XII. kerületben két bejelentés is érkezett, amelyben a bejelentők azt állították, hogy a bankszámlaszámukról most emeltek le egy bizonyos összeget, holott a bankkártyájuk náluk volt, és ők otthont tartózkodtak. A bejelentés hatására kisebb kutatómunka eredményeként a XII. kerület egyik ATM készüléknél több, hamis kártyával kísérelt meg pénzt felvenni az I. rendű vádlott, illetve több sikeres tranzakciót is végrehajtott. A bejelentésre kikerülő XII. kerület járőrei intézkedés alá vonták a kérdéses személyt. E során az I. rendű vádlottnál 29 darab

⁷⁷ 1998. évi XIX. törvény 160 §.

⁷⁸ 2012. évi C. törvény 393 §.

sorszámozott, PIN kódokkal feliratozott, white plastik kártyát, valamint több, mint 1.000.000 forintot találtak meg. Az intézkedő rendőröknek először felajánlott egy millió forintot, hogy engedjék szabadon, mintha mi sem történt volna. A rendőr járőrök nem engedtek a kísértésnek, és visszautasították az ajánlatot. Ennek hatására további egy milliót toldott hozzá a korábban ígért összeghez, de ez a summa sem kellett a kollégáknak. Végso elkeseredettségében, nem leplezve azt a szándékát, hogy mindent bevet annak érdekében, hogy meglógjon a rendőrség karmai közül, felajánlotta a Porsche 911 Carrera személygépjárművét is, kimerítve ezzel a Büntető törvénykönyv 293 §-ba ütköző Hivatali vesztegetés büntetét⁷⁹. Azonban a hatóság embereit ez sem hatotta meg, és az I. rendű vádlottat elő is állították. A motozás eredményeként lefoglaltak ügyfélértesítőket, Western Union átutalási megbízásokat, a nála lévő több mint egy millió forintot, a 29 db hamis bankkártyát, valamint a Porsche 911 Carrera típusú személygépjárművet GPS-sel, papírokkal és a slussz-kulccsal.

Az adatszerzésben érintett pénzintézet munkatársai megállapították, hogy a visszaélések során használt bankkártyák adatait az elkövetők 2008. január-2008. február időintervallum alatt szerezték meg egy VI. kerületi ATM-ről adatszerző és álbillentyűzet segítségével.

A videofelvételen nevezett személy és két társa látható adatszerzés közben. A képeken a IV. rendű vádlott és egy nigériai származású elkövető volt látható.

A jogosulatlan készpénzfelvételeket 10.380.681 forint értékben hajtották végre, melyből 1. 847.000 forint volt sikeres. Ezzel egy időben, mint már említettem, máshol is hajtottak végre visszaéléseket, melyből megalapozottan lehetett arra következtetni, hogy több elkövető van a csoportban.

A megszerzett információk alapján házkutatás⁸⁰ foganatosítására került sor az I. rendű vádlott tartózkodási helyén, mely a XIII. kerületben volt. A kényszerintézkedés során többek között lefoglalásra⁸¹ került 1 db laptop, 2 db SIM kártya, 1 db telefon, több millió forint készpénzben, Western Union átutalási megbízások, bizonylatok, a hamis útlevelek, amelyeket bankszámla nyitására használtak fel. A megszerzett dolgok, így különösen a számítógép és a telefon adattartalmának megismerése céljából igazságügyi szakértő ki rendelése⁸² mellett határozott a nyomozó hatóság. A számítógép átvizsgálására, a rajta lévő

⁷⁹ Az eljárást a Pesti Központi Nyomozó Ügyészség folytatta le, amely alapján az ítélet meghozatalakor a bűncselekmény miatt is felelnie kellett.

⁸⁰ 1998. évi XIX. törvény 149 §

⁸¹ 1998. évi XIX. törvény 151 §

⁸² 1998. évi XIX. törvény 99§

dolgok, illetve a törölt dolgok előhívására igazságügyi számítástechnikai szakértő kirendelésére volt szükség. Az első szakértő nem talált semmilyen olyan adatot, ami bűncselekmény elkövetésére utalt volna, vagy más illegális adattartalmat. Az ügyben eljáró nyomozók kihasználva a törvény adta lehetőséget⁸³ más szakértőt rendelt ki szakvélemény készítésére. Ez a szakértő rendkívül értékes és hasznos információkkal szolgált az NNI munkatársainak. A laptopon egy excel dokumentumban rengeteg bankkártya adat volt elmentve. Meg lehetett mondani, hogy mely bank honlapján hajtottak végre tranzakciót. Így meg lehetett állapítani, hogy ezek a tranzakciók mikor lettek lefolytatva, mely felhasználónévvel, valamint melyik felhasználónévhez melyik jelszó tartozik. Ezek alapján meg lehetett fejteni, hogy melyik számláról mekkora összeget milyen számlára utaltak ki jogtalanul. Ez arra teremtett lehetőséget, hogy a korábban a szóban forgó pénzintézetnek intézett megkeresésre érkezett válaszát részletesebben elemezzék. Ez a válasz azoknak a személyeknek a nevét tartalmazta, akikről a bank tudta, hogy kár érte őket. Így a neveket össze kellett vetni a számítógépből kinyert nevekével, és további sértettek felkutatása sikerült. Természetesen indult ezekben is büntetőügy más kapitányságokon, de ismeretlen tettes miatt megszüntetésre⁸⁴ kerültek.

A számítógép adataiból az Interneten elkövetett csalás módszerére is fény derült, amit internetes chat beszélgetések log listáinak lefordításából lehetett megfejteni. Ez pedig a BOTNET volt. A BOTNET-et bérelték, és arra használták, hogy a magyarországi felhasználók adatait kivonatolja. Hasonló elven működik, mint egy keylogger, annyi specialitással kiegészítve, hogy nem csak a billentyűleütéseket naplózza, hanem azt is, hogy a felhasználó mely oldalakon böngészett, ha valahova be kellett jelentkezni, azt milyen felhasználónévvel és jelszóval tette meg. Ezek az információk pedig az elkövetők számítógépére lettek megküldve, és így nyitva volt a kapu a jogtalan tranzakciók végrehajtására, lebonyolítására. Az orosz és angol nyelvű elektronikus csevegésekből, levelezésekből, amelyeket két NNI-is kolléga fordított le saját maga, még az is megállapíthatóvá vált, hogy mely bankautomatákat szemelték ki a visszaélések elkövetésére, valamint a kézi adatszerző eszköz alkalmazására is találtak használati útmutatót, mint például hogyan kell felhelyezni.

A bankoknak írt megkeresésben arra is rákérdeztek, hogy mely ATM automatáknál történt jogosulatlan készpénzfelvétel. Ezek alapján az ATM-k által rögzített képeken sikerült fényképfelvételeket szerezni az elkövetőkről. A laikus szemnek is látható volt, hogy

⁸³ 1998. évi XIX. törvény 111 § (5)

⁸⁴ 1998. évi XIX. törvény 190 § g)

ugyanazokról az tettesekről van szó, de az igazságügyi antropológus szakértő azonban azt állapította meg, hogy a felvételeken nagy valószínűséggel az elkövetők szerepelnek, amelyet a bíróság nem talált teljes bizonyító erejűnek. Egy újabb használhatatlan szakvélemény született meg az eljárás folyamán.

A telefonszolgáltatóknak megküldött megkeresés is hasznos eredményekkel szolgált. Meg lehetett azt állapítani, hogy a visszaélések időpontjában a korábban lefoglalt telefonkészülékekről melyik bandatag melyik telefont használta. A híváslista elemzése során megállapították, hogy mely telefonszámok lettek a leggyakrabban tárcsázva. Így körvonalazódott az, hogy egymással beszéltek a legtöbbet, különösen az ATM-knél való készpénzfelvételek idején.

A rendelkezésre álló adatok alapján, valamint a fényképek alapján a III. rendű és a IV. rendű vádlott ellen elfogatóparancsot adtak ki, előbbi ellen ráadásul nemzetközi elfogató parancs volt érvényben. A III. rendű vádlottat Spanyolországban fogták meg, mikor át akart kelni Marokkóban bízva azzal, hogy sikerül megúsznia a büntetőjogi felelősségre vonást. A IV. rendű vádlott még a nyomozás ideje alatt eltűnt. Szinte már a nyomozók is letettek róla, hogy meglesz, mikor kapták az információt, hogy az akkor még Ferihegy (ma már Liszt Ferenc) Nemzetközi Repülőtéren a Repülőtéri Rendőr Igazgatóság (továbbiakban: RRI) útlevelel ellenőrző munkatársai az útlevelel ellenőrzése során figyeltek fel a körözött személyre, akit rögtön a helyszínen el is fogtak. Később a vallomásában azt állította, hogy azért jött vissza Magyarországra, hogy a megkezdett tanulmányait befejezze. A II. és a V. rendű vádlott elfogása a lakásukon történt.

Miután az elkövetők kézre kerültek, és megfelelő mennyiségű és minőségű bizonyíték állt a rendelkezésre, vádat emeltek ellenük. Sajnos az eljárás annyi ideig húzódott, hogy az I. és II. rendű vádlott előzetes letartóztatását házi őrizetre⁸⁵ enyhítette a bíróság, amelyet ők kihasználva az Ukrán határon át megszöktek az országból, feltételezhetően haza, Oroszországba, így a büntetésüket nem kezdték meg letölteni.

Valamennyi vádlott letöltendő börtönbüntetést kapott, szerepüktől függően 2-6 év terjedelemben.

Azért tartottam célszerűnek ezt a viszonylag régi ügyet feldolgozni, mert a létrejött bünszervezet olyan szervezetten készült elő a visszaélések elkövetésére, ami egyedülálló. Rengeteg olyan, modern technikai vívmányt, taktikát, trükköt vetettek be a siker elérése érdekében, amelyek a szakdolgozati témám jelentős részét lefedik. Ezen felül rávilágított a

⁸⁵ 1998. évi XIX. törvény 138 §.

felderítés egyes nehézségeire, mint például, hogy a különböző nemzetközi jogsegélyek, szakértői vélemények megérkezése viszonylag sok időt vesz igénybe, és nem feltétlen tudják segíteni a nyomozást, gondolok itt a két szakértő véleményének egymástól való eltérésére, ami ügydöntő fontosságú volt. De prezentálta a nyomozás szépségét is, ugyanis az ilyen esetek megoldásához nemzetközi szinten folyamatos kapcsolattartásra van szükség a rendvédelmi szervek között. A rengeteg befolyó információ közül meg kell találni az adott ügyben relevánsakat, és azokra építve kell kulcsfontosságú stratégiai döntéseket, intézkedéseket hozni. A nyomozó hatóságok tagjainak is ismerniük kell az alkalmazott adatszerző technikákat, ezeket az ismereteket folyamatosan frissíteni kell, azaz figyelemmel kell kísérni az elkövetői oldal fejlődését.⁸⁶

⁸⁶ A az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény rendelkezéseire való tekintettel sem az elkövetőket, sem az ügyben szereplő pénzintézeteket, egyéb szolgáltatókat nem nevezem meg!

6. Jogi szabályozás

A rohamosan fejlődő világban a készpénzforgalom mellett jelentek meg a készpénz-helyettesítő fizetési eszközök. Miután ezek is fokozottan a visszaélések központi figurái lettek, hamar be kellett látni azt, hogy a jogi védelmét is meg kell teremteni ezeknek az eszközöknek, amelynek egyik módja az éppen hatályos magyar Büntető törvénykönyv (továbbiakban: Btk.) Különös Részében történő tényállás létrehozása. Indoka egyrészt az, hogy bűncselekményt kizárólag törvény határozhat meg (*nullum crimen sine lege*), másrészt az elkövetővel szemben csak olyan bűncselekmény miatt lehet büntetést kiszabni vagy intézkedést alkalmazni, amelyről a törvény az elkövetés idején rendelkezett (*nulla poena sine lege*).⁸⁷ Harmadrészt fő indok még, hogy Magyarország jogharmonizációs kötelezettséget vállalt magára az Európai Unióhoz való csatlakozással. Ennek a kötelezettségnek eleget téve be kellett építeni a magyar jogrendszere az Európai Unió Tanácsának 2001/413/B. kerethatározatát.

A magyar Btk. a készpénz-helyettesítő fizetési eszközök fogalmi meghatározását az értelmező rendelkezésében adja meg, háttérszabályként megjelölve a Hitelintézetekről és pénzügyi vállalkozásokról szóló törvényt (továbbiakban: Hpt.). A Btk. hatályba lépésekor még a Hpt. az 1996. évi CXII. törvény volt hatályban, de az az elmúlt évben, 2014. január 1-vel hatálytalanná vált, és egy új törvényt alkottak meg, amely a 2013. évi CCXXXVII. törvény⁸⁸. A készpénz-helyettesítő fizetési eszköz fogalmát a Btk. 459 § (1) 19. pontja is megadja a Hpt.-re hivatkozva.⁸⁹ A Hpt. 55. pontja szerint készpénz-helyettesítő fizetési eszköznek minősül a csekk; az elektronikus pénz; valamint a pénzforgalmi szolgáltató és az ügyfél közötti szerződésben meghatározott olyan személyre szabott dolog vagy eljárás, amely lehetővé teszi az ügyfél számára a fizetési megbízás megtételét. A Hpt. mellett még figyelembe kell venni az Erzsébet utalványról szóló 39/2011. (XII.29.) számú Kormányrendeletet és a Széchenyi Pihenőkártyáról szóló 55/2011. (IV.12.) számú Kormányrendeletet.

A mai magyar, hatályos Btk. három tényállást alkotott meg a készpénz-helyettesítő fizetési eszközök védelme érdekében. Az első a *Készpénz-helyettesítő fizetési eszköz hamisítása*; a második a *Készpénz-helyettesítő fizetési eszközzel visszaélés*; a harmadik pedig a *Készpénz-helyettesítő fizetési eszköz hamisításának elősegítése*.

⁸⁷ 2012. évi C. törvény a Büntető Törvénykönyvről 1§.

⁸⁸ http://njt.hu/cgi_bin/njt_doc.cgi?docid=165854.254745#foot1

⁸⁹ A definíciót lásd a 2.2. alfejezetben.

5.1. Kézpénz-helyettesítő fizetési eszköz hamisítása

A Btk. a következőképpen határozza meg a tényállást:

„392. § (1) Aki felhasználás céljából

a) készpénz-helyettesítő fizetési eszközt meghamisít,

b) hamis készpénz-helyettesítő fizetési eszközt készít, vagy

c) az elektronikus készpénzhelyettesítő fizetési eszközön tárolt adatokat vagy az ahhoz kapcsolódó biztonsági elemeket technikai eszközzel rögzíti,

vétség miatt két évig terjedő szabadságvesztéssel büntetendő.

(2) Aki készpénz-helyettesítő fizetési eszköz hamisítására irányuló előkészületet követ el, elzárással büntetendő.

(3) A külföldön kibocsátott készpénz-helyettesítő, illetve elektronikus készpénz-helyettesítő fizetési eszköz a belföldön kibocsátott készpénz-helyettesítő fizetési eszközzel azonos védelemben részesül.”

A törvényi tényállás által védeni kívánt jogi tárgya a készpénzkímélő eszköz-forgalom biztonságához fűződő társadalmi érdek. „A jogi tárgy az a társadalmi viszonyokban kifejezésre jutó érdek vagy érték, amelyet a bűncselekmény sért vagy veszélyeztet.”⁹⁰

A bűncselekmény készpénz-helyettesítő fizetési eszköz meghamisítására, hamis készpénz-helyettesítő fizetési eszköz készítésére, vagy az elektronikus készpénz-helyettesítő fizetési eszközön tárolt adatok vagy az ehhez kapcsolódó biztonsági elemeket technikai eszközzel rögzítésére irányul. Így megállapíthatjuk azt, hogy a bűncselekmény elkövetési tárgya a készpénz-helyettesítő fizetési eszköz, mivel e delictum e dologra irányul.

Három magatartással lehet a bűncselekményt elkövetni. Az első a *meghamisítás*, amikor egy valódi készpénz-helyettesítő fizetési eszközt megváltoztatnak, és/vagy módosítanak. Egy külső, laikus szemlélőt megtéveszthet, és azt hiheti, hogy az adott tárgy eredeti. A második magatartás egy hamis készpénz-helyettesítő fizetési eszköz *készítése*, ami egy olyan folyamat, amikor egy nem létező készpénz-helyettesítőt gyártanak le, de ennek képesnek kell lennie azoknak a funkcióknak a betöltésére, amelyre egy eredeti képes. A harmadik elkövetési magatartásban tulajdonképpen az *adatok* valamilyen módon történő *megszerzéséről* beszélhetünk, Ezeket a módokat a tényállás nem nevesíti meg, így egy nyitott

⁹⁰ Blaskó Béla: Magyar Büntetőjog Általános Rész Negyedik Átdolgozott Kiadás, Rejtjel Kiadó, Budapest-Debrecen, 2010, 155. o.

törvényi tényállási elemet fogalmazott meg a jogalkotó. Ezeknek a módszereknek leggyakrabban előforduló fajtáról a korábbi fejezetekben esett szó.

A bűncselekményt bárki elkövetheti, nincsen semmilyen egyéb státusz betöltéséhez kötve. Amennyi elkövetési tárgyra követi el a bűncselekményt, annyi rendbeli lesz a delictum, de ha azonos bankszámlára vonatkozik a készpénz-helyettesítő meghamisítása, akkor természetes vagy folytatólagos egységről beszélünk.

Az elhatárolási kérdések⁹¹ terén ki kell emelnünk a Btk. 375. § (5)-ben megfogalmazott Információs rendszer felhasználásával elkövetett csalás II. alapesetét. Az elhatárolás alapja a keletkezett kár. A Btk. 459§ (1) 16. pontja alapján a kár a törvény eltérő rendelkezése hiányában a vagyonban okozott értékcsökkenés. Ha a hamis bankkártya felhasználása során kár keletkezik, akkor a Btk. 375. § (5) bekezdésébe ütköző esetet meg lehet állapítani. Ilyenkor a készpénz-helyettesítő hamisítása eszközselekmény, látszólagos halmazatot keletkeztetve.

A készpénz-helyettesítő fizetési eszköz hamisítása a Hamis magánokirat felhasználásával (Btk. 345. §) nem állapítható meg halmazatban, mert már akkor megvalósul, amikor az elkövető készpénz-helyettesítőt meghamisít, vagy hamisat készít. A felhasználás nem szükséges eleme a befejezettségnek.

5.2. Készpénz-helyettesítő fizetési eszközzel visszaélés

A Btk.-ban szereplő tényállása:

„393. § (1) Aki

a) egy vagy több olyan készpénz-helyettesítő fizetési eszközt, amely nem vagy nem kizárólag a sajátja, vagy amelynek a használatára nem vagy nem kizárólagosan jogosult, mástól, annak beleegyezése nélkül, jogtalanul elvesz vagy megszerez,

b) hamis vagy meghamisított, az a) pontban meghatározott módon elvett vagy megszerzett készpénz-helyettesítő fizetési eszközt, vagy az elektronikus készpénz-helyettesítő fizetési eszközön tárolt adatokat vagy az ahhoz kapcsolódó biztonsági elemeket átad, megszerez, az ország területére behoz, onnan kivisz, vagy azon átszállít,

vétség miatt egy évig terjedő szabadságvesztéssel büntetendő.

(2) A büntetés büntett miatt három évig terjedő szabadságvesztés, ha a készpénz-helyettesítő fizetési eszközzel visszaélést bűnszövetségben vagy üzletszerűen követik el.

⁹¹ Belovics Ervin- Molnár Gábor Miklós- Sinku Pál: Büntetőjog II. Különös rész a 2012. évi C. törvény alapján, Budapest, HVG-ORAC Lap- és Könyvkiadó Kft., 2012., 675.o.-676.o.

(3) A külföldön kibocsátott készpénz-helyettesítő fizetési eszköz a belföldön kibocsátott készpénz-helyettesítő fizetési eszközzel azonos védelemben részesül.

A különös részi törvényi tényállás által védeni kívánt jogi tárgy megegyezik az előző pontban meghatározottakkal (*mutatis mutandis*), csak úgy, mint az elkövetési tárgya is ugyanaz.

A két tényállás között az elkövetési magatartások kifejtésével lehet meghúzni az elhatárolási vonalat. Az a) pontba két magatartást szőtt bele a jogalkotó. Az egyik az elvétel, amelynek a birtoklásának a visszaélés esetén sértenie kell a pénzforgalom biztonságát. A megszerzés pedig a dolog feletti tényleges hatalom megszerzése, aminek jogellenesnek kell lennie és mástól kell történnie. Mikor jogellenes? Ha sem törvény, sem a jogosult nem adja az engedélyét az elvételre. Ha bármelyik fennáll, akkor a megszerzés jogszerű, és így e *delictumot* nem lehet megállapítani.

A b) pontban is több elkövetési magatartás olvasható. E pont elkövetési tárgya lehet hamis, hamisított, vagy az a) pontban meghatározottak szerint megszerzett készpénz-helyettesítő fizetési eszköz, valamint az ezen tárolt adatok vagy a hozzá kapcsolódó biztonsági elemek. A bűncselekmény e pontja akkor valósul meg, ha az elkövető az elkövetési tárgyak közül egyet vagy többet másnak vagy átad, vagy megszerez, vagy az ország területére behoz, onnan kivisz, vagy azon átszállít.

Az *átadás* nem más, mint a megnevezett dolgok más birtokába történő bocsátása. Azért büntethető ez a cselekedet, mert az elkövetési tárgy(ak) hamisak, hamisítottak, vagy azokat jogtalanul szerezték meg.

A *megszerzés* vonatkozásában az a) pontban meghatározottak *mutatis mutandis* irányadók.

Az *ország területére történő behozatal, az onnan való kivitel, vagy az átszállítás* pedig egyfajta jogellenes nemzetközi kereskedelmet jelent.

A bűncselekményt bárki elkövetheti a készpénz-helyettesítő fizetési eszközök tulajdonosait kivéve. Az elkövetők súlyosabb büntetésre számíthatnak, ha a cselekményüket bűnszövetségben vagy üzletszerűen követik el. Bűnszövetség akkor jön létre, „ha a két vagy több személy bűncselekményeket szervezeten kívül, vagy ebben megállapodik, és legalább egy bűncselekmény elkövetését megkísérlik, de nem jön létre bűnszervezet.”⁹² Az

⁹² 2012. évi C. törvény a Büntető Törvénykönyvről 459§ (1) 2. pont

üzletszerűség akkor állapítható meg, „ha valaki ugyanolyan vagy hasonló jellegű bűncselekmények elkövetése révén rendszeres haszonszerzésre törekszik.”⁹³

Az elkövetési tárgyak száma nem befolyásolja a halmazat létrejöttét, ugyanis a tényállásban egy vagy több fizetési eszközre el lehet követni a cselekményt, így egy törvényi egység keletkezik. Akkor sem lehet halmazatként elbírálni a cselekményt, ha ugyanarra a bankszámlához kapcsolódik több fizetési eszköz.

Fontos megjegyezni, hogy valamelyik elkövetési magatartással kár keletkezik. A kár a vagyonban okozott értékcsökkenést jelenti, melyet a Btk. 459§ (1) 16. pontja mondja ki. Ilyenkor azonban nem ezt a bűncselekményt kell megállapítani, hanem az Információs rendszer felhasználásával elkövetett csalást, amelyet a Btk. 375 §-ban pönalizáltak.

E bűncselekmény szoros kapcsolatban áll a magánokirattal elkövetett Okirattal visszaélés delictummal. Mivel az elkövetési tárgy speciális, így mindig ezt a bűncselekményt kell megállapítani, nem pedig az Okirattal visszaélést.

5.3. Kézpénz-helyettesítő fizetési eszköz hamisításának elősegítése

A Btk.-ban szereplő bűncselekmény:

„394. § (1) Aki készpénz-helyettesítő fizetési eszköz hamisításához vagy a készpénzhelyettesítő fizetési eszközön lévő adat technikai eszközzel való rögzítéséhez szükséges anyagot, eszközt, berendezést vagy számítástechnikai programot készít, megszerez, tart, átad, forgalomba hoz, az ország területére behoz, onnan kivisz, vagy azon átszállít, vétség miatt egy évig terjedő szabadságvesztéssel büntetendő.

(2) A büntetés két évig terjedő szabadságvesztés, ha az (1) bekezdésben meghatározott bűncselekményt bűnszövetségben vagy üzletszerűen követik el.

A témához kapcsolódó, harmadik bűncselekmény jogi tárgya is ugyanaz, mint az előző kettő esetében, tehát a készpénz-helyettesítő fizetési eszköz-forgalom biztonságához fűződő társadalmi érdek.

Az elkövetési tárgya a hamisításhoz és az adatok technikai eszközzel való megszerzéséhez és rögzítéséhez szükséges anyag, eszköz, berendezés vagy számítástechnikai program.

Az elkövetési magatartások közül többféle van nevesítve a tényállásban. A első a készítés, ami az elkövetési tárgy létrehozását jelenti. A megszerzés itt is tényleges birtokbavételt takar. A tartás egy hosszabb ideig fennálló állapotot jelöl meg, így ennek elévülés

⁹³ 2012. évi C. törvény a Büntető Törvénykönyvről 459§ (1) 28. pont

az állapot megszűnésétől kezdődik meg. Az átadás más személy számára való hozzáférhetőséget foglal magába, amit az elkövető tesz azzá. A forgalomba hozatal az adott elkövetési tárgy más személyekhez történő eljuttatása, amelynek nem feltétele, hogy visszatérhes legyen, de mivel ez jövedelmező üzlet, amelyet legfőképp internetes oldalakon végeznek a tettesek, nagyobb részben ellenérték fejében kerülnek ki a bűnözők birtokából. Az ország területére való behozatal és a kivitel az országhatár átlépése következtében valósul meg, míg az átvitel az ország területén történő átszállítással valósítja meg a bűncselekményt.

Ennek a tényállás megalkotása egy sui generis előkészületi magatartás külön tényállásban történő pónalizálást eredményezte, melyet bármilyen természetes személy elkövethet.

Súlyosabban büntethető a cselekmény, ha bünszövetségben vagy üzletszerűen követik el. A két kifejezés meghatározására a korábban leírtak mutatis mutandis irányadók.

A tényállások megismerése után nézzük meg a bűncselekmények előfordulásait az elkövetés helye szerint:⁹⁴

⁹⁴http://njt.hu/cgi_bin/njt_doc.cgi?docid=152383.256437 = 2012. évi C. törvény a Büntető Törvénykönyvről

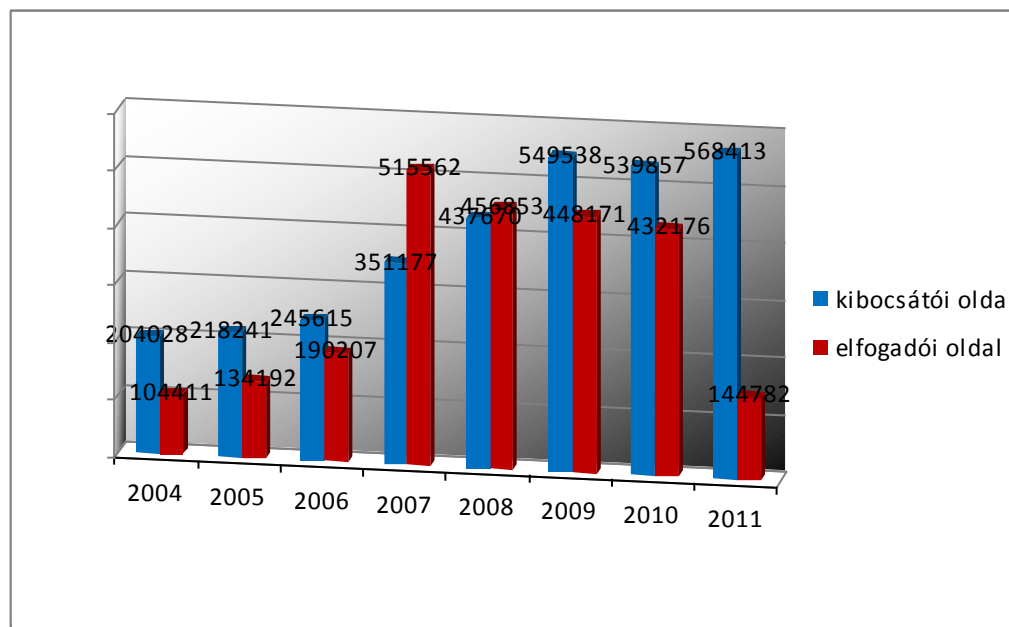
Blaskó Béla-Hautzinger Zoltán-Madai Sándor-Pallagi Anikó-Polt Péter-Schubauer László: Büntetőjog Különös rész II. Budapest-Debrecen, Rejtjel Kiadó, 2013, 285.o.-292. o.

Belovics Ervin- Molnár Gábor Miklós- Sinku Pál: Büntetőjog II. Különös rész a 2012. évi C. törvény alapján, Budapest, HVG-ORAC Lap- és Könyvkiadó Kft., 2012., 672.o.-680.o.

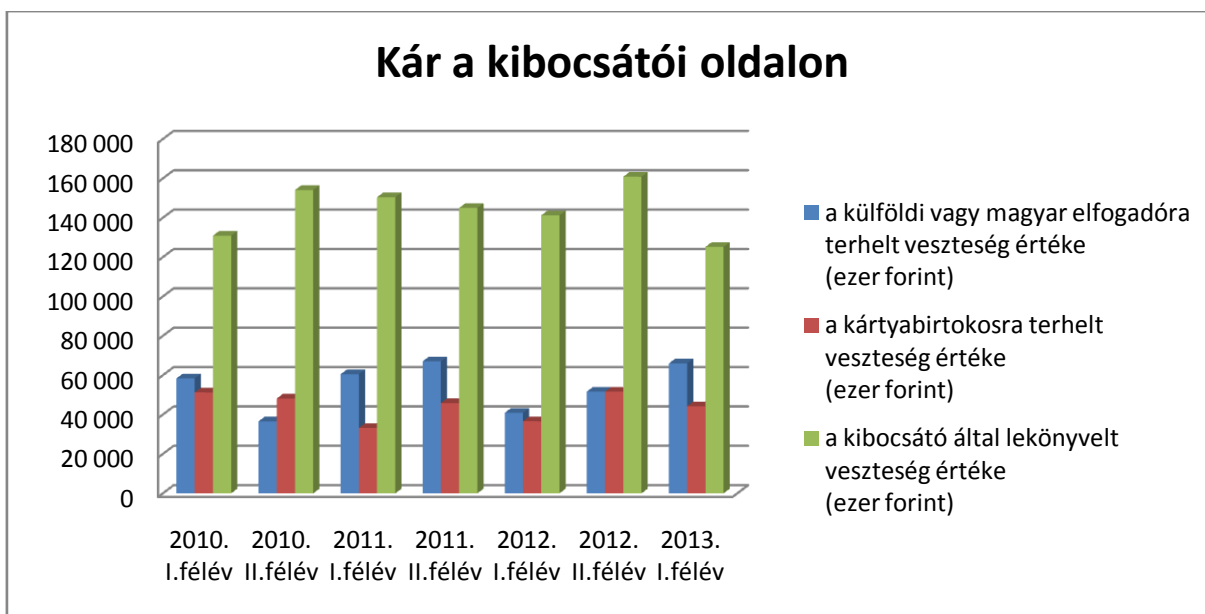
7. Statisztika

A készpénz-helyettesítő fizetési eszközök használata nem csak az állam polgárainak mindennapjaiban, hanem a gazdasági folyamatokban is időről időre egyre nagyobb és fontosabb szerepet tölt be. Egyre gyakrabban használják a bankkártyákat a kereskedelemben, a termékek árának kiegyenlítésére. A kártyák elterjedésében rendkívül nagy szerepet vállaltak az egyes pénzügyintézetek, hiszen használatuk jóval kevesebb eszközt, munkaerőt igényel, és mivel haszonmaximalizálás uralkodik a piacon, a minimum elvet követve, maga után vonta a forradalmasítás minél előbbi elterjesztését. Így sikerült azt elérni, hogy a pénzmozgás csak a virtuális térben jelenik meg, fizikailag a pénz meg sem jelenik. Mivel ilyen elterjedt fizetési módszer, a bűnözők lankadatlan figyelmét is magára vonta. Az elkövetők a rendszer tanulmányozása során felismerték a könnyű és gyors pénzszerzési lehetőséget, amit a személyekben rejlő, bankkártyák iránti szakadatlan bizalom kihasználásával érnek el. Megállapíthatjuk, hogy az alkalmazott visszaélési módszerekkel okozott károk évről évre növekvő tendenciát mutatnak, melyet az alábbi diagram nagyon jól szemléltet:

7.1. Visszaélések során felmerült kár a bankkártya üzletágban (ezer forint)



1. ábra

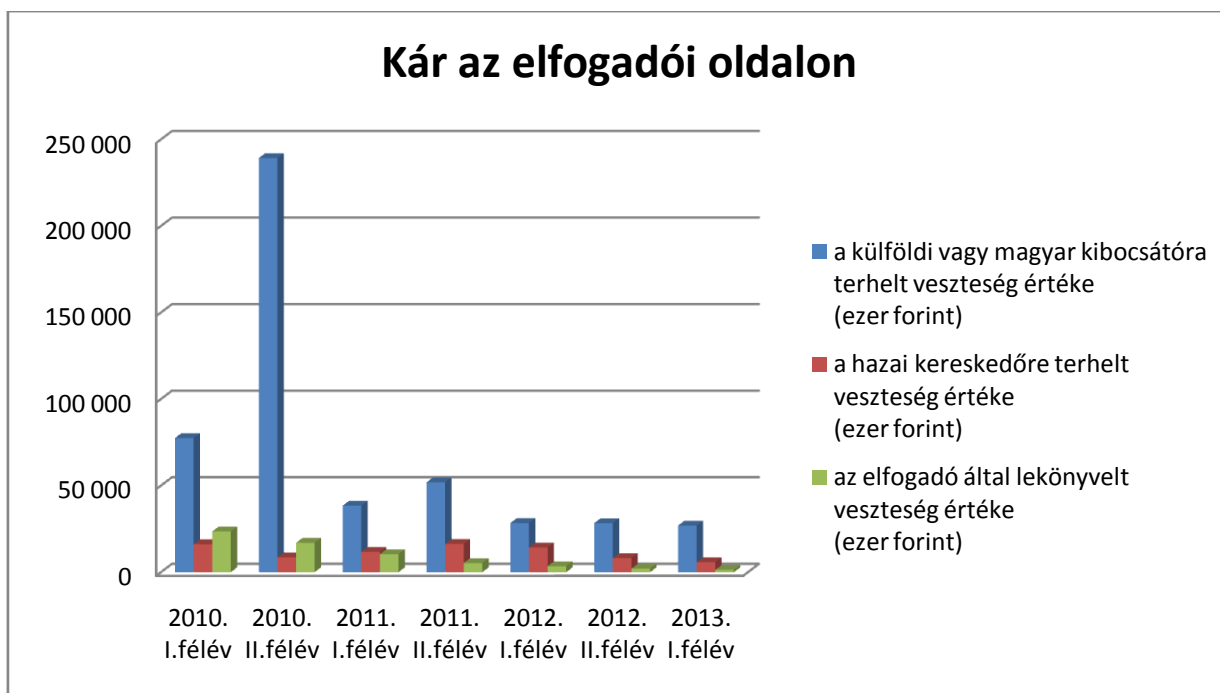


2. ábra⁹⁵

2011-ben a kibocsátói oldalon 502, 2 millió forint kár merült fel, ami három részből tevődik össze. Az egyik része a külföldi vagy magyar elfogadóra terhelt veszteség, amely 127,6 millió forintra rúg. A második a kártyabirtokosra terhelt veszteség értékét tünteti fel, mely számszerűen 79,1 millió forintként jelenik meg. a harmadik partíciót a kibocsátó által lekönyvelt veszteség értéke adja ki, amely jelen esetben 295,5 millió forintot tesz ki. Az előző évhez képest a teljes kibocsátói veszteség 5 %-os növekedést jelent és azóta apránként, de minden évben, ráadásul minden félévben minimálisan ugyan, de növekedik.

Az elfogadói oldalon az elmúlt négy évben tapasztalható folyamatos csökkenés egyrészt a bankok által sikeresen alkalmazott monitoring rendszerek, másrészt az ATM-ek és POS terminálok chipesítésének köszönhető, amelyek a hamis vagy hamisított kártyák kiszűrésére alkalmasak, amely az alábbi ábrán nagyon jól kivehető:

⁹⁵ <http://www.mnb.hu/Statiztika/statiztikai-adatok-informaciok/adatok-idosorok/xiii-penzforgalmi-adatok/penzforgalmi-adatok/penzforgalmi-tablakeszlet/visszaeletek>

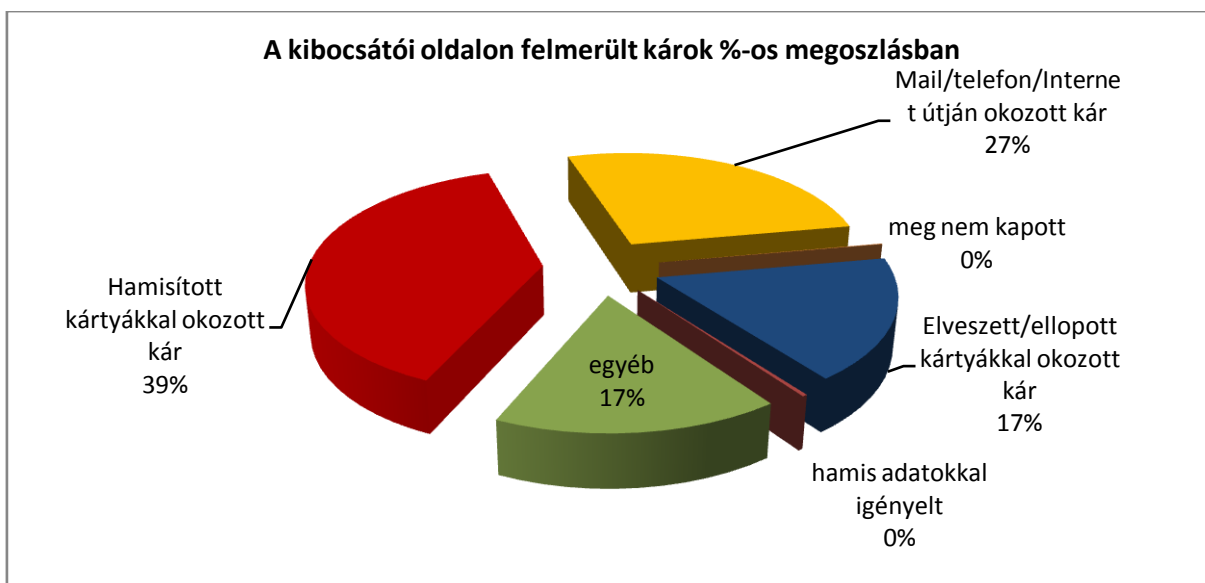


3. ábra⁹⁶

A 2010-es évben látható kiugró veszteség nagy részét az NNI akkor még alosztályként működő bankkártya-hamisítás elleni egysége által a 2011-es év során, a német hatóságokkal közösen felszámolt, román-magyar tagokból álló bankkártyás visszaélésekre szakosodott bűnszervezet okozta.

Az elmúlt években a bankkártyákkal kapcsolatos visszaélések nagy részét, közel 50 %-át a hamis bankkártyákkal történő visszaélések tették ki, míg 1/3-1/3 arányban a lopott vagy az elvesztett kártyákkal, valamint az internetes visszaélések által okozott károk képviseltették magukat.

⁹⁶ <http://www.mnb.hu/Statiztika/statiztikai-adatok-informaciok/adatok-idosorok/xiii-penzforgalmi-adatok/penzforgalmi-adatok/penzforgalmi-tablakeszlet/visszaelesek>



4. ábra⁹⁷

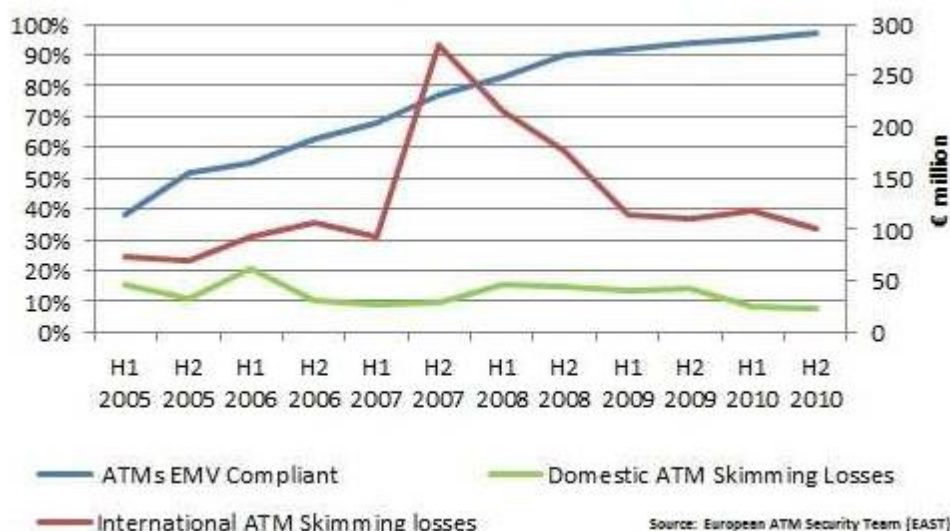
Összességében elmondhatjuk, hogy a magyar kártyákkal való visszaélések tendenciái szorosan követik az Európai Unió trendeket. A CNP tranzakciók aránya folyamatosan növekszik, ami azt jelenti, hogy a hazai (EU-s) bankok elfogadói hálózatában egyre nagyobb arányt képviselnek az internetes csalások aránya.

A CNP⁹⁸ visszaélések elterjedése ellenére azért még mindig fellelhető a hagyományos, ún. „Skimming”, ami a legnagyobb problémát képes okozni.

A pár sorral feljebb említett chipesítés hatására a hazai visszaélések tendenciái szorosan követik az EU-n belül észlelteket, melyek soros korrelációt mutatnak a chipesítés szintjével. A következő diagramon látható az ATM-ek chipesítésének hatása a bankkártyás visszaélésekre, az EU-s tagállamok vonatkozásában:

⁹⁷ <http://www.mnb.hu/Statiztika/statiztikai-adatok-informaciok/adatok-idosorok/xiii-penzforgalmi-adatok/penzforgalmi-adatok/penzforgalmi-tablakeszlet/visszaelesek>

⁹⁸ Card Not Present: bankkártya fizikai jelenléte nélküli tranzakciók ~ ezalatt inkább az internetes visszaéléseket értik

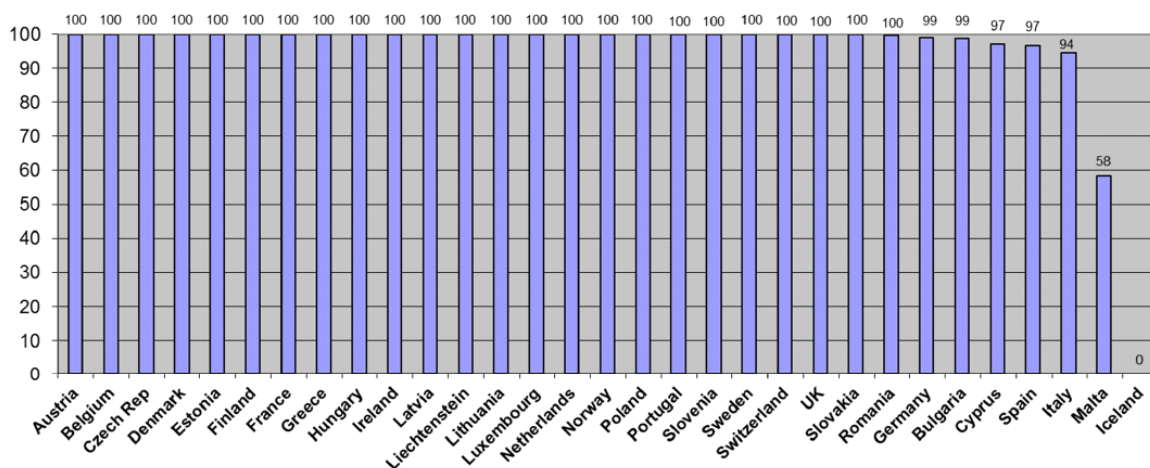


5. ábra

A kék vonal az ATM-ek ún. EMV (Europay, Mastercard, Visa társaságok rövidítése, az általuk közösen megalkotott szabványt jelenti) képességét tükrözi, az „Y” tengelyen ez %-ban érzékelhető. A zöld vonal az EU-n belüli, a piros az EU-n kívüli ATM-eken okozott banki veszteséget mutatja.

A diagramon jól megfigyelhető, hogy az ATM-ek chipesítése maga után vonta az EU kártyák külföldön történő felhasználásának megugrását.⁹⁹ Az EU-n belüli visszaéléseket szemléltető ábrán látható a visszaesés a bankkártyák chipesítéséből fakad. Egyre nagyobb arányban vannak jelen chippel felszerelt kártyák, amelyekkel 100 %-os chipesítés mellett az EU zónában már nem lehetséges visszaéléseket elkövetni. A bankszektor a még forgalomban lévő mágnescsíkos kártyákat kifutó rendszerben cseréli be chipesre. 100 %-os chipesítés mellett a zöld grafikon a 0 felé fog konvergálni, persze, ha az elkövetők nem jönnek rá, hogyan lehet a chiptechnológiát feltörni. Ennek elérése Magyarországon kb. 2015-re várható. Természetesen az EMV szabványnak megfelelő kártyák olvasására EMV szabványú ATM automaták üzemeltetése is szorosan kapcsolódik. Ezt az EU tagországokra lebontva az alábbi diagram (2011. november 31.) szemlélteti:

⁹⁹ Ezt hívják a bani szakzsargonban ún. „fraud migrációnak”- a szerző megjegyzése

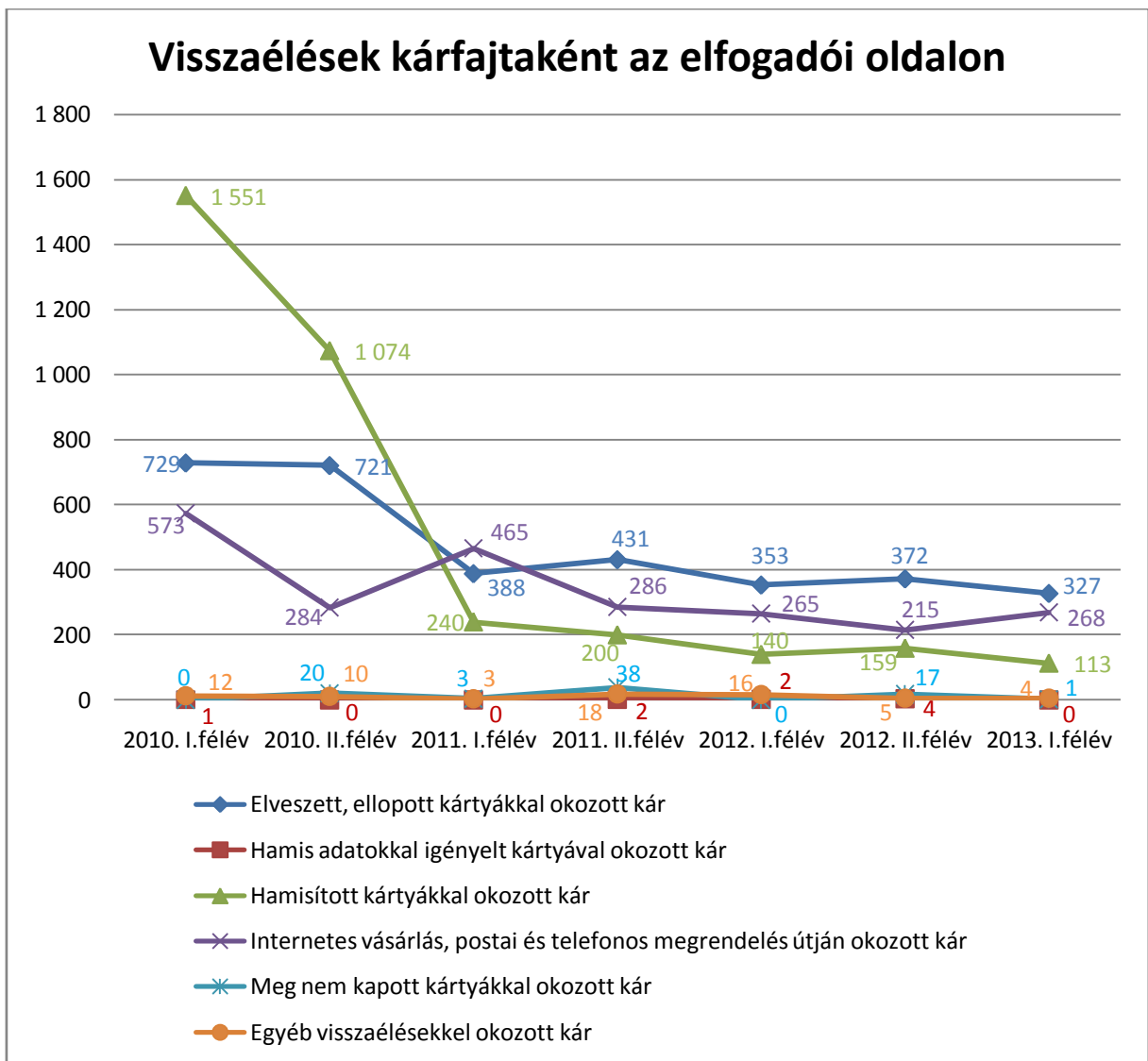


Source: European ATM Security Team (EAST) and the European Payments Council (EPC)

6. ábra

Nagyon jól kivehető, hogy a hazánkban beüzemeltetett ATM-ek összessége megfelel az EMV szabványnak, és ráadásul az egész Európai Unióban csak néhány államban tapasztalható kisebb elmaradottság, de természetes zajlik a korszerűsítés.

Azonban ez a chipesítés hogyan formálta át a visszaéléseket hazánkban? Magyar Nemzeti Bank (továbbiakban: MNB) által, a honlapjukon megjelent statisztikai adatokat felhasználva készítettem el ezt a fejezetet, kiegészítve egy-két más szervezet statisztikájával. Figyelemre méltóan alakult a magyarországi visszaélések alakulása az elfogadói oldalon.



7. ábra¹⁰⁰

A hamisított kártyákkal okozott károk óriási visszaesése figyelhető meg, melynek okaként az ATM automaták chipesítése nevesíthető meg. A teljes ATM készlet modernizálása 2011-es év tavaszi időszakára tehető, így az ezt követően elkövetett visszaélések a csak mágnescsíkkal rendelkező bankkártyákkal lettek elkövetve.

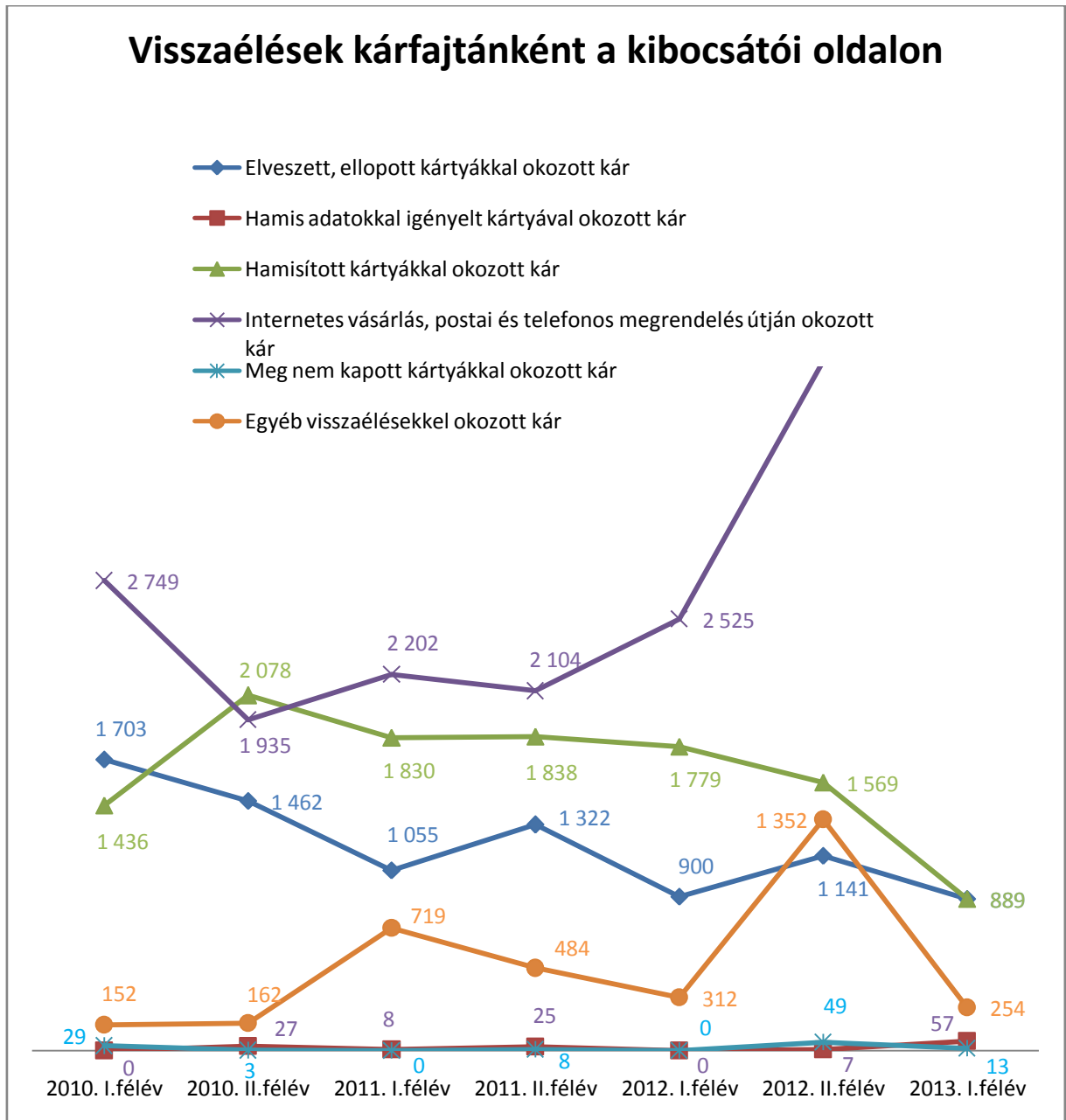
Az ATM-ek kiválasztási módszereiből azt a konklúziót tudjuk levonni, hogy az elkövetői csoportok rendkívül szervezettek, és ami legalább ugyanolyan fontos, nagyon jól informáltak. A fentiekben említett, 2011-ben az NNI speciális egysége által felszámolt bűnszervezet ki tudta deríteni, hogy a Takarékszövetkezetek elmaradottabbak voltak, mint a többi bank, így kisebb késésben voltak a modernizáció területén. Miután megtalálták a

¹⁰⁰ <http://www.mnb.hu/Statisztika/statisztikai-adatok-informaciok/adatok-idosorok/xiii-penzforgalmi-adatok/penzforgalmi-adatok/penzforgalmi-tablakeszlet/visszaelesek>

Az értékek **darabszámot** jelölnek!

rést a magyar pajzson, támadásba lendültek, és a nyugat-európában megszerzett chipes kártyák mágnescsíkján tárolt adatokat használták fel készpénzfelvételre, amellyel több 10 millió forintos anyagi kárt okoztak a takarékszövetkezeteknek.

Magyarország, kibocsátói veszteség



8. ábra¹⁰¹

¹⁰¹ <http://www.mnb.hu/Statiztika/statiztikai-adatok-informaciok/adatok-idosorok/xiii-penzforgalmi-adatok/penzforgalmi-adatok/penzforgalmi-tablakeszlet/visszaelesek>

Az értékek **darabszámot** jelölnek!

A hazai kibocsátó oldalt mutató diagramon érdemes két elkövetési módszerrel foglalkozni. Az egyik ilyen a hamisított kártyával okozott kár, a másik pedig az internetes vásárlás, postai és telefonos megrendelés útján okozott kár, melyet manapság szokásos ún. CNP¹⁰² tranzakciók néven is emlegetni, mely alatt gyakorlatilag már csak az internetes tranzakciókat értjük. Az előbbinél még növekedés realizálható a 2010-es év második felében, de aztán csökkenésnek indult a 2011-es év elejére. Két évig stagnált az így okozott károk mértéke, de aztán 2012. második felére, valamint a tavalyi év elejére ismét csökkent, ez utóbbi elég drasztikus mértékben. A másik az internetes vásárlással, posta vagy telefonos megrendelés útján okozott kár „sorsának” elemzése érdemel nagyobb figyelmet, ugyanis teljesen ellentétesen alakult, mint a hamisított kártyáé. Amíg előbbi a 2010-es év magasságában „tetőzött”, addig az internetes visszaélés valamivel, de kevesebb volt. Aztán fordult a kocka, és az internetes visszaélésekkel okozott károk kezdtek el növekedni. Ezt az emelkedést meg már az utóbbi két évben eszméletlen, szinte megállíthatatlan folyamatként kúszik felfelé, egyre nagyobb károkat okozva. A diagram nem tudja szemléltetni, de míg a 2012-es év első felében 2525 darab volt, ez a szám ezen év második felére 4033 darabra szökött fel, ami 62,6 %-os növekedést jelentett egy fél éven belül. Mi lehet ennek az oka? Feltételezhetjük, hogy az ok az lehet, ami az elfogadói oldalon is szembeötlő változást produkált. Az ATM-ek korszerűsítése, azaz chipesítése. Így a készpénz kiadó automatáknál sokkal kevesebb hamisított kártyával tudtak visszaélni, de az így megszerzett adatokat máshogy tudták hasznosítani. Vagy az internetes vásárlásnál használják fel, és profitálnak belőle, vagy a megszerzett adatokkal Európán kívül (leginkább Dél-Amerikában, és az USA-ban, valamint az utóbbi időben a távol-keleten) követnek el visszaéléseket. Ezekből kiindulva Magyarországon két fő változásra kell rendkívül odafigyelni. Ez utóbbi esetben rendkívül nehéz a nyomozás, mert azok az országok, ahol leginkább a visszaélések kerülnek elkövetésre, még nem csatlakoztak az EMV rendszerhez, ami azt jelenti, hogy a hazai kibocsátó banknak kell a veszteséget kiegyenlíteni, a kárt viselni. Tovább azért nehéz még a felderítés, mert a dél-amerikai és a távol-keleti országok nem válszolgálnak az interpolos megkeresésekre.

Az adatok alapján azt a konklúziót kell levonni, hogy az ilyen jellegű visszaélések visszaszorítására, sikeres leküzdésére erősíteni kell a nemzetközi együttműködéseket. A hazai tapasztalatok azt mutatják, hogy a bankkártyás bűncselekményeket elkövető személyek nagyrészt román állampolgárságúak, de fellelhető még magyar, bolgár vagy ukrán

¹⁰² Card Not Present- kártya fizikai jelenléte nélkül

nemzetiségű is. A román elkövetők dominanciája több tényezőben testesül meg. Jelentős szerepet játszik a két ország szomszédsága, Magyarország tranzit szerepe, és nem szabad elfelejteni, hogy az Erdélyből érkezők magyar nyelvismerete elég magas szinten van. Jó példa erre az általuk elkövetett ún. Cash trapping (ld. 3.4.2. alfejezet), amit 2012. szeptemberétől kezdett megszorodni. A bolgár elkövetők is jelentős számban vesznek részt készpénz-helyettesítő fizetési eszközt érintő bűncselekmények elkövetésében. Ők az átutazó bűnözők körét szélesítik ki. Cseh társszervek jelezték, hogy Csehországban a bankkártyás visszaélésekben a bolgárok a legaktívabbak. Okként a nyelvi rokonságot, valamint a bolgár kisebbséget jelölték meg. Magyarországon a bolgár bűnözők kezdenek aktívak lenni a Skimming területén, így lassan átveszik a románok dominanciáját. A hamis okmányos számlanyitásban csak a sokadik helyen állnak, ott a románok vezetnek, őket meglepő módon baltikumi országok követik, és „csak” utánuk jönnek a bolgárok. A hamis okmányokkal történő bankszámlanyitás azért bevett „szokás”, mert ezekre jogosulatlan átutalások történnek. Ezek mögött jogtalanul megszerzett bankkártya-adatok internetes felhasználása, jogosulatlan online banking hozzáférések által elutalt összegek, valamint az ún. Internetes aukciós csalások állnak.

A magyarok vonatkozásában az figyelhető meg, hogy a hazai elkövető csoportok aktiválták magukat, és Magyarország határain kívül szereznek adatokat, amelyekkel visszaéléseket Amerikában követnek el, és őket román származású személyek is támogatnak.

Megállapítható, és be kell látni, hogy ezek a bűnözői csoportok nemzetközileg szervezettek, egyre hatékonyabban lépnek fel. Elengedhetlenné vált a napi szintű nemzetközi kapcsolattartás az egyes országok között, ugyanis az elkövetők több országot felölelő kapcsolati hálózattal rendelkeznek, melyek egymással kommunikálnak. Egy-egy bűnözői csoport és azok tagjai több országban követnek el bankkártyás bűncselekményeket. Pozitív jelként minősíthetjük, hogy európai szinten sikerült olyan mértékű biztonsági fokot elérni az ATM automaták vonatkozásában, hogy egyre nehezebb az azokon elkövethető visszaélés. Azonban nem szabad hátra dőlni, mert az elkövetők az EU-ban egyáltalán nem akarnak visszaéléseket elkövetni, hanem inkább „csak” adatokat megszerezni, mivel a mágnescsík még mindig megtalálható a bankkártyák hátoldalán és a tettesek újabb és újabb, modernebbnél modernebb eszközökkel vétetik észre magukat az egyes országokban. Az országok közti kommunikáció lehetővé tenné az ilyen eszközök elterjedésére való figyelemfelhívást, és szinte azonnal reagálni lehetne az újabb módszerre egy hatékony védekezési megoldással. Természetesen nem csak erről kell információkat küldeni, hanem hatékonyabbak, sikereesebbek lehetnek a nyomozások, ha az ismertté vált elkövetőkről, a

hozzájuk köthető telefonokról, bankkártyákról, gépjárművekről fellelhető összes információt megosszák egymással az egyes országok. Kreatív megoldás az, amivel az Europol bankkártya-hamisításra szakosodott egysége, a TERMINAL munkacsoport foglalkozik, mert ez hathatós segítséget jelent az EU-n belüli nyomozati munkában. A munkacsoport azzal foglalkozik, hogy bandában lévő egyes személyekről készült képeket közzéteszi. Ezekkel más országok területén elkövetett cselekményükre is fény derülhet, valamint a bűnszervezetben való részvétel bizonyítását is nagymértékben megkönnyíti.

Pár sorral feljebb megemlítésre került, hogy az újonnan bevetett és alkalmazott eszközökről is célszerű a tájékoztatás, ami nem csak egy új védekezés kidolgozását teszi lehetővé, hanem a módszer felismerhetőségét is. A szakember könnyebben ismeri fel a bűncselekményre vonatkozó gyanús jeleket, ha ismeri és tudja, mire kell figyelni.

A nemzetközi együttműködésnek két lehetősége van. Az egyik az EUROPOL, ahol az egyes információk keresztülmennek a másik országba. A másik módja az országok közti közvetlen kapcsolattartás, netán a szakemberek személyes ismeretsége. Az így beszerzett információk a későbbiekben az EUROPOL csatornák felhasználásával, vagy a jogsegély keretében válhatnak felhasználhatóvá egy büntetőeljárásban.

Fel kell venni a kapcsolatot az EMV rendszerhez nem kapcsolódott országokkal is, mivel a visszaélések jelentős részét ilyen országokban követik el a hamisított bankkártyákkal. Hiába jelzi a bankbiztonság a visszaélést, ha a kapcsolat teljes hiánya miatt nem lehetséges az illetékes szervek azonnali értesítése. Így nem csak a delictum valósul meg, hanem még a tettesek kézre kerítése sem történik meg, és cselekményüket tovább tudják folytatni, jelentős károkat okozva. Az INTERPOL-on keresztül a kapcsolatfelvétel lassú, és nyelvi problémák is előjönnek. Ezért lenne jó, ha lenne közvetlen kapcsolat az érintett ország bankkártyás központi egységével, ott kérni egy angolul jól beszélő munkatárs közvetlen elérhetőségét, és szinte rögtön lehet intézkedést fogantatosítani.

Hiányosságként említhető még meg hazai vonatkozásban, hogy nincs egy olyan központ adatbázis, amelyben a Magyarország területén elkövetett adatszerzések és visszaélések lennének nyilvántartva. A kereskedelmi bankok zöme informális tájékoztatást ad a tudomásra jutott bűncselekményekről a KR-NNI speciális bankkártyás egységének.

Követendő példaként lehetne felhozni a Csehországban működő rendszert, ahol a központi (nyomozást végző) szervhez futnak be a bankkártyás bűncselekményekhez tartozó adatok. Azért releváns, mert egy-egy elkövetői csoport egy adott ország különböző területén is tevékenykedik, így az ellenük történő eredményes fellépés feltétele, hogy ezek összekapcsolhatók legyenek. Ezek alapján jobban lehet következtetni a bűnöző csoportok

összetételére, szervezeti felépítésére, tevékenységére, szervezettségére. Felismerve a probléma súlyát a KR-NNI és a Bankszövetség egy hasonló rendszer életre hívásán dolgozik.

8. Összegzés

A szakdolgozati téma aktualitása miatt olyan cél elérését tűztem ki, amelynek elérése sok szempontból bír relevanciával. Egyrészt sikerüljön egy átfogó képet kialakítani az Olvasóban a világ modern területével kapcsolatban, amelyben nemcsak az előnyök jutnak kiemelt szerephez, de a háttérbe taszított hátrányok is szem elé kerülnek, tehát sikerül betekintést nyerni a kulisszák mögé. Másrészt azért volt jelentős az értelmes, logikus témakidolgozás, hogy az egyes károsító tevékenységek lényegét, dinamikáját meg lehessen érteni, és miután ez bekerül az ismeretanyagunkba, képesek legyünk átkódolni az agyunkat, és minden tőlünk telhetőt megtegyünk annak érdekében, hogy csökkentsük az ilyen bűncselekményekkel okozott károk mértékét, valamint megelőzzük saját magunk áldozatává válását.

A logikai felépítés azt a követelményt támasztotta, hogy célszerű a történelem legelején elindulni, hogy meglegyen az az átfogó ismeret, hogyan is jutott el a világ a XXI. századra ilyen technikai fejlettségre, milyen történelmi sarokpontokon keresztül vezetett egészen idáig a készpénz-helyettesítő fizetési eszközök „ösvénye”, milyen különféle változatai alakultak ki az idők folyamán, ezeknek a miértjei. Így jutottunk el magához a bankkártyához, mint készpénz-helyettesítő fizetési eszközhöz.

Ezután célszerűnek tartottam ismertetni az egyes válfajait, és azok jellemzőit, ugyanis nem mindegy, melyik típust válasszuk egy esetleges számlanyitásnál egy adott pénzintézetnél. A különféle típusok tulajdonságai között rengeteg eltérés figyelhető meg, de vannak olyan alapfunkciók, melyekre szinte mindegyiken telepítenek, és amelyeken keresztül illetve segítségével törvénybe ütköző cselekményeket tudnak végrehajtani az elkövetők. Ebbe a körbe sorolnám például a kártya hátulján lévő három vagy négyjegyű CVC/CVV titkos kódot.

Megismertük ezáltal a bűncselekmény tárgyi eszközét. Rátérhettem a visszaélések, adatszerzések különféle trükkjeire, amelyeket előszeretettel vetnek be a bűnözői csoportok. Ezeknek a megismerésében, megismertetésében rengeteg segítséget kaptam a már a Prológusban említett KR-NNI munkatársaitól, akik hasznos, és értékes, feldolgozható információkkal, gyakorlati tapasztalatokkal, javaslatokkal, észrevételekkel, és forrásokkal láttak el. A visszaéléseket, pontosabban a bankkártyán lévő adatok megszerzését két nagy csoportra bontottam. Az egyik nagy csoport az, amikor az adatok megszerzése a kártya fizikai jelenlétével történik meg. Ilyenkor az elkövetők azt a szituáció adta előnyt használják ki, mikor a kártya birtokosa használja a kártyát. Ez történhet ATM automatánál, POS terminálnál, a

vásárlás egyenlegének kielégítésénél. Előfordulhat az is, amikor nem adatok megszerzésére irányul a bűnözői célzat, hanem közvetlenül a pénz megszerzésére (Cash Trapping). Az ebben a körben megemlített technikákhoz különféle eszközök, felszerelések tartoznak, melyek ismerete nélkül nem kaptunk volna teljes képet a témának ezen periferiájáról.

A másik nagy csokorba azok az esetek tartoznak, melyek a kártya fizikai jelenléte nélkül elkövethetők. Ide nem kell más, mint az elkövetőnek egy nagyon jó informatikai háttértudása, na meg persze egy számítógép, ahonnan az egész folyamatot irányítani tudja. Különböző internetes módszerek kifejtésére került sor, melyhez szintén a KR-NNI nyomozói nyújtottak szakmai segítséget. Sokféle típust sajátíthattunk el, reprezentálva azt, hogy mennyire színes a bűnözői tevékenység ezen palettája. Egy profi, szakképzett „informatikus”, akiket inkább crackereknek, vagy hackereknek lehet hívni, képesek olyan szinten leplezni a tevékenységüket, hogy szinte lehetetlen kinyerni a szelet a vitorlájukból. Erre még a virtuális tér is olyan lehetőséget kínál, ami abszolút, de nem a rendvédelmi munka malmára hajtja a vizet.

Igyekeztem az elméleti anyagok után egy nagyon nagy, komplex, a közelmúltban elkövetett bűncselekmény ügyének esettanulmányát olyan szinten kifejtteni, hogy érzékeltessem, mennyire összehangoltak, szervezettek, jól informáltak, eszesek az ilyen bűncselekmények elkövetésére specializálódott, általában külföldi nemzetiségű csoportok. Az ügyet csak úgy, mint már eddig a KR-NNI bocsátotta rendelkezésemre. Azért is sikerült beemelni a műbe, mert már született benne ítélet, így megismerhetővé vált nem csak nekem, hanem a szakdolgozat Olvasója számára is.

Mivel az ilyen cselekményeknek a társadalomra veszélyessége is elég nagy, valamint a jogharmonizációs követelményeknek eleget kellett tenni, és kell is, nem lehetet elfeledni a büntető anyagi jogi szabályozás ismertetését sem, hiszen a rendvédelmi munka alapját képezi, másrészt az állam büntető jogi igényének érvényesítése törvény nélkül lehetetlen. Megismerkedtünk három, ide kapcsolódó különös részi tényállással, amely a hamisításról, a visszaélésről, valamint egy sui generis előkészületi magatartás, ami a hamisítás elősegítését hivatott büntetni rendelni. E minősítések valamelyikében indulhat el akár a nyílt eljárás, akár a titkos információgyűjtés az adott ügyben, ahol felmerül a gyanú.

Nem feledkezhettem meg a közelmúlt statisztikai adatairól sem, hiszen ezek a cselekmények évről évre egyre jobban dominálnak, egyre többet követnek el belőlük, felismerve a viszonylag könnyű pénzszerzés lehetőségét. A statisztikai adatok megjelenítésére remek alapul szolgált a Magyar Nemzeti Bank által elkészített táblázat, amelyen mind a kibocsátói oldal, mind az elfogadói oldal veszteségét lehetett megismerni. Megtudhattok,

hogyan az egyes módszereket hányszor alkalmazzák, és hogy ezekkel mekkora károk keletkeztek. Segítségül hívtam még az ENYÜBS adatbázisában fellelhető adatokat, amelyek az büntető anyagi jogban meghatározott tényállások előfordulási számát tükrözi.

Nagyon bízom benne, hogy a Prológusban felállított követelményeknek, valamint a kiszabott feltételeknek maradéktalanul megfelelően sikerült a dolgozat elkészítése. Remélem érdekes, hasznos információkkal, preventív megoldási javaslatokat foglaltam bele a témába, melyek alkalmazásával megkönnyíthetjük az életünket.

Végül, zárszóként Szendi Gábor egy idézetét említeném, ami véleményem szerint tömören, lényegre törően, és bölcsen jellemzi ezt a területet, valamint ennek a területnek a rohamos fejlődését. „Az evolúció során a tudatosság egészen új keletű dolog, s az evolúció nagy buherátor: sose újat alkot, hanem mindig a meglevőt fejleszti tovább. Az ember receptje: végy egy majomagyat, préselj bele még egy kis tudatosságot, és adj a kezébe egy bankkártyát. Ecce homo¹⁰³.”

¹⁰³ Latin kifejezés, János evangéliumából származik, Jelentése: „Íme az ember!” -- <http://idezet.zin.hu/evolucio-soran-tudatosság-egészen-új-keletű-dolog-s-evolucio-nagy>

9. Felhasznált Irodalom

9.1. Nyomtatott források

- Dr. Sági Judit: Banktan, Saldo Kiadó Budapest, 2007
- Kónya Judit: Banküzemeltetési alapismeretek. Budapest: Közgazdasági és Jogi. 1994. 226–234. o.
- Dr. Huszti Ernő Banktan, Tas Kft. 2002.
- Balogh László et al. Pénzügytan II., 1999., 143. o.
- Trefort Ágoston Két Tanítási Nyelvű Fővárosi Gyakorló Szakközépiskola, Dr. Forgách Ádám 2009. év január hó 29. napon leadott oktatása nyomán
- Magyar Értelmező Kéziszótár Tintakönyvkiadó Budapest, 2007. I. kötet 81. o.
- Dr. Lázás Piroska, Dr. Solt Katalin: Elméleti Gazdaságtan I. Mikroökonómia, Novoprint Öltevényi Production, Budapest 2006., 30.o./227.o.
- dr. Simon Béla: A csúcstechnológiai bűnözés és nyomozása, Budapest, 2013., 23. o. 35. o., 39.o.
- Blaskó Béla-Hautzinger Zoltán-Madai Sándor-Pallagi Anikó-Polt Péter-Schubauer László: Büntetőjog Különös rész II. Budapest-Debrecen, Rejtjel Kiadó, 2013, 285.o.-292. o.
- Belovics Ervin- Molnár Gábor Miklós- Sinku Pál: Büntetőjog II. Különös rész a 2012. évi C. törvény alapján, Budapest, HVG-ORAC Lap- és Könyvkiadó Kft., 2012., 672.o.-680.o.

9.2. Internetes források

- <http://ecopedia.hu/penz-tortenete>

- 1. kép:

https://www.google.hu/search?q=csekk&tbm=isch&tbo=u&source=univ&sa=X&ei=J9zfUtuWO6PJygOV1YGwAQ&ved=0CC0QsAQ&biw=1366&bih=643#facrc=_&imgdii=_&imgsrc=r7ydrDr4FlQfvM%253A%3BU6Vjxn6DKmlliM%3Bhttp%253A%252F%252Fwww.teletipp.hu%252FCSEKK75.jpg%3Bhttp%253A%252F%252Fwww.teletipp.hu%252Fcsykk.htm%3B580%3B254

- 2. kép:

https://www.google.hu/search?q=v%C3%A1lt%C3%B3&source=lnms&tbm=isch&sa=X&ei=_Q7gUt7RAcPiywODmoDgCA&ved=0CAcQ_AUoAQ&biw=1366&bih=643#facrc=_&imgdii=_&imgsrc=1ezM5rB0eXfRCM%253A%3B18gJ4pzCeC87xM%3Bhttp%253A%252F%252Fwww.discimus.hu%252Fokjvizsga%252Fuzletiszakmenedzser%252Fnagykepek%252Fidegen_valto.jpg%3Bhttp%253A%252F%252Fwww.discimus.hu%252Fokjvizsga%252Fuzletiszakmenedzser%252Fokmanytar.html%3B1584%3B907

- <http://www.bankkartya.hu/hirkategoria/sajtoszemle/cikk/359-a-hitelkartya-trtnete>
- <http://www.bankweb.hu/a-bankkartya-tortenete/>
- <http://www.barclaycard.co.uk/personal>
- <http://hu.wikipedia.org/wiki/Bankautomata>
- http://hu.wikipedia.org/wiki/PIN_k%C3%B3d
- <http://meszotar.hu/keres-bankk%C3%A1rtya>
- <http://penzugy.uw.hu/fogalomtar>
- <http://www.bankracio.hu/fogalom/187-bankkartya>
- <http://ecopedia.hu/bankkartya>
- <http://www.enc.hu/1enciklopedia/mindennapi/bankkartya.htm>
- http://bankkartya.blog.hu/2010/04/22/a_bakkartya_fajtai
- <http://kiszamolok.hu/fizess-egyszeruen-a-paypass-kartyakrol/>

- <http://bankkartya.hu/hirkategoria/hirek/cikk/8034-vilgjdonsg-bejelentse-budapesten-indulnak-a-szmkijelzs-s-billentyezettell-ellott-krtyk-a-mastercardnl>
- http://www.mnb.hu/Root/Dokumentumtar/MNB/Penzforgalom/Penzforgalom_kiadvanyok/penzforgalomrol_mindenkinek_bankkartyak.pdf
- <http://kiszamolo.hu/bankkartyas-csalasok-ii-resz-2/>
- 3. kép:

https://www.google.hu/search?q=%C3%A1l+billenty%C5%B1zet&source=lnms&tbm=isch&sa=X&ei=5iYrU_zgAYm6ygPXlYKADA&ved=0CAcQ_AUoAQ&biw=1366&bih=643#q=atm+%C3%A1lbillenty%C5%B1zet&tbm=isch&facrc=_&imgsrc=qJds52S2UDbx8M%253A%3BoHMnJHxCqtIQzM%3Bhttp%253A%252F%252Fwww.runet.hu%252Fportal%252Fpub%252F2009_augusztus%252Fatm3.jpg%3Bhttp%253A%252F%252Fportal.runet.hu%252Farticle200.html%3B622%3B467

- 4. kép:
- https://www.google.hu/search?q=card+trapping&espv=2&es_sm=122&source=lnms&tbm=isch&sa=X&ei=c4AjU5fYA4P8ygP2n4CICw&ved=0CAkQ_AUoAQ&biw=1366&bih=643#facrc=_&imgdii=_&imgsrc=ulx0GtPdj2qT8M%253A%3BmXAKsLiOMlkYFM%3Bhttp%253A%252F%252F2.bp.blogspot.com%252FcD91XQ0ISW4%252FT2l5O7hKqTI%252FAAAAAAAB5c%252FQp7H1IfvjJs%252Fs1600%252Fjebakan%252Bcard%252Btrapping.jpg%3Bhttp%253A%252F%252Fwww.mafiakartukredit.com%252F2012%252F03%252Ftechnik-modus-card-trapping.html%3B500%3B333
- <http://safeinternetbanking.be/en/fraud-techniques/skimming-and-card-trapping>
- <http://safeinternetbanking.be/en/fraud-techniques/shoulder-surfing>
- <http://www.pointernet.pds.hu/ujsagok/evilag/2004-ev/04/20070306122418315000000489.html>
- <http://eur-lex.europa.eu/Notice.do?mode=dbl&lang=hu&ihmlang=hu&lng1=hu,en&lng2=bg,cs,da,de,el,en,es,et,fi,fr,hu,it,lt,lv,mt,nl,pl,pt,ro,sk,sl,sv,&val=449272:cs>

- <http://eur-lex.europa.eu/Notice.do?mode=dbl&lang=hu&ihmlang=hu&lng1=hu,en&lng2=bg,cs,da,de,el,en,es,et,fi,fr,hu,it,lt,lv,mt,nl,pl,pt,ro,sk,sl,sv,&val=449272:cs>
- <http://www.cert.hu/content/az-adathal%C3%A1szatr%C3%B3l-phishing-pharming>
- <http://blogs.securiteam.com/index.php/archives/467>
- <http://www.macmillandictionary.com/buzzword/entries/smishing.html>
- <http://us.norton.com/cybercrime-pharming>
- <https://security.intuit.com/phishing.html>
- http://securityresponse.symantec.com/hu/hu/norton/library/familyresource/article.jsp?aid=article1_08_06
- http://securityresponse.symantec.com/hu/hu/norton/library/familyresource/article.jsp?aid=article1_08_06
- <http://pcforum.hu/szotar/szkript.html>
- <http://pcforum.hu/szotar/Szkriptnyelv.html>
- http://hvg.hu/tudomany/20140310_facebook_video_virus
- <http://www.oxforddictionaries.com/definition/english/keylogger>
- http://en.wikipedia.org/wiki/Keylogger#Automatic_form_filler_programs
- http://index.hu/gazdasag/magyar/2011/12/15/hazai_bankkartyak_tiz_ezreit_tiltottak_le/
- http://hvg.hu/tudomany/20131004_Elloptak_az_Adobe_Systems_to_bb_millio_fel
- http://hu.spam.wikia.com/wiki/Address_harvesting
- http://hu.spam.wikia.com/wiki/Rejtjelezett_e-mail_c%C3%ADmek
- http://hu.spam.wikia.com/wiki/Eldobhat%C3%B3_e-mail
- <http://www.biztonsagosinternet.hu/tippek/denial-of-service-tamadasok>
- <http://www.irc.hu/page1.html>
- http://hu.wikipedia.org/wiki/L%C3%A1thatatlan_web
- <http://baserape.hu/darknet-vedett-halozat-vege/>

- <http://motherboard.vice.com/blog/darknet-touring-the-hidden-internets-illegal-markets>
- http://njt.hu/cgi_bin/njt_doc.cgi?docid=152383.256437 = 2012. évi C. törvény a Büntető Törvénykönyvről
- <http://www.mnb.hu/Statisztika/statisztikai-adatok-informaciok/adatok-idosorok/xiii-penzforgalmi-adatok/penzforgalmi-adatok/penzforgalmi-tablakeszlet/visszaelesek>
- <http://idezet.zin.hu/evolucio-soran-tudatossag-egesen-uj-keletudolog-s-evolucio-nagy>