Műszaki Katonai Közlöny

XXII. évfolyam, 2012. 1. szám

VERES VIKTÓRIA

AZ IDENTITÁS- ÉS ADATLOPÁS, MINT NAPJAINK ÚJ KIHÍVÁSA

THE IDENTITY AND DATA FRAUD, TODAY`S NEW CHALLENGE

Absztrakt

Az elmúlt években számos kutatás látott napvilágot az internet, a közösségi oldalak, az e-banking, a bankkártya-használat elterjedéséről, emellett pedig ugyancsak több tanulmány foglalkozik az identitás-lopás, bankkártyás csalások es az ezekkel elkövetett bűncselekmények szinte megállíthatatlan terjedéséről. Mit is jelentenek valójában ezek, mi történik, ha személyes es pénzügyi adataink illetéktelen kezekbe kerülnek? Miért jelenthet az egyének megkárosítása akár nemzeti vagy nemzetközi fenyegetést? További kérdés, hogy milyen válaszok adhatóak az ilyen veszélyek csökkentésére es mi határozza meg ezek működőképességét? A szerző ebben a tanulmányban vizsgálja az identitás, mint értékkategória fogalmát, az ellene elkövetett cselekményeket, különös tekintettel, a pénzügyi adatainkkal való visszaélésre.

Kulcsszavak: identitás, pénzügyi adat, online adat, identitás-lopás

Abstract

In the recent years many research has been published about the rapidly increasing use of the internet, social networking sites, e-banking and the credit/debit cards, in addition many more and more experts have been researching the spread of fraud and crime using ID theft and credit card fraud. What do these mean and what happens if our personal and financial data gets into the hands of fraudsters? Why may the defrauding of individuals lead to a national or international threat? Further question is what response can be given to reduce these risks and what determines their functionality? The author examines the definition of identity as value category and the threats against it with special attention to financial data fraud.

Key words: identity, financial data, online data, identity fraud

BEVEZETŐ

Az internetes ügyintézés elterjedésének korszakát éljük. Mindez megkönnyíti a mindennapjainkat, ugyanakkor kiszolgáltatottabbá tesz bennünket. Az identitásunk, és annak minden eleme támadhatóbbá vált, így a pénzügyi adataink is. Növekedett az ezek ellen való visszaélések száma mind egyéni, mind közösségi szinten. A pénzügyi adataink elleni támadás, majd az azokkal való visszaélés nem csak az egyén, hanem a társadalom számára is rendkívül veszélyes, és messzemenő hatási lehetnek. Ebben a cikkben célul tűztem ki, hogy vizsgálom az identitás fogalmát, összetevőit, különös tekintettel a pénzügyi adatokra, majd néhány példát hozok az ezek ellen való támadások típusaira, céljaira, valamint vázolok pár lehetőséget a támadások elleni védelemre. A célok elérése érdekében elemeztem a téma internetes irodalmát, vizsgáltam néhány pénzintézet napi gyakorlatát, valamint a saját pénzintézeti munkám tapasztalatait.

Mindenek előtt tekintsük át, hogy mit jelent az identitás, elemezzük az ezzel kapcsolatos adatok körét, valamint a pénzügyi adat fogalmát, és vizsgáljuk meg az adatlopás és az azzal való visszaélés lehetőségeit!

1. AZ IDENTITÁS, ÉS AZ ÁLLAMPOLGÁROK ÉS CÉGEK IDENTITÁSA ELLEN ELKÖVETETT CSELEKMÉNYEK

Az identitásunk jogi értelemben olyan meghatározott állandó és változó adatok halmaza, amely megkülönböztet minket másoktól. Ennek sok összetevője van, de az egyik legfontosabb a pénzügyi adat. A személyes pénzügyi adat a személyes adatok részeként mindazon adatok összessége, amelyek a jelenleg birtokunkban lévő pénzösszegek, befektetési alapok stb. nagyságát, formáját, lejáratát, kamatait stb. tartalmazzák, vagy amit pénzügyeink bárminemű intézéséhez, jövőbeni pénzügyi szolgáltatások igénybevételéhez megadunk. és ami nem tartozik a nyilvános pénzügyi adatok köréhez.

A pénzügyi adat egyben az egyén szempontjából egy rendkívül fontos értékkategória, amely révén megőrzi a szuverenitását a mikro- és makro-környezetében. Széles értelemben véve mára ide tartoznak a banki adataink is. Az elmúlt időszak társadalmi, technikai változásai, az elszegényedés, a bűnözés elterjedése, a nemzetközi gazdasági dekonjunktúra mind erősítették azt a tendenciát, hogy az identitás a széles

értelemben vett biztonság egyik kategóriájává vált. A híradások egyre többször számolnak be az identitásunkat fenyegető cselekményekről. Ezeket az adatokat napi szinten használjuk, hiszen ezek alapján kapjuk és használjuk dokumentumainkat, illetve veszünk igénybe szolgáltatásokat: ezért identitásunknak értéke, és a bűnözők számára ára is van.[1] Sokkal szembetűnőbben igaz ez a pénzügyi adatainkra, banki információnkra es bankkártyánkra. Egy 2010-es amerikai felmerés szerint az egyéni bankkártya-használók 12%-a esett áldozatul valamilyen visszaélésnek..[2]

Az identitás- és adatlopás gyakran nem elsődleges célja a bűnözőknek, hanem az egyéb értékeink eltulajdonítása során "akaratlanul" is hozzájutnak az értékeinkkel együtt tárolt adatainkhoz. (Lásd 1. sz. ábra).

1. sz. ábra: Trükköznek a zsebesek[3]

Mikor válik az identitás- és adatlopás pénzügyi értelemben véve szándékos csalássá? Az identitással és adatlopással elkövetett csalás olyan folyamat, amely során az elkövetők célzottan ezeket az adatokat keresik, és az adatok eltulajdonítása, majd azok felhasználása révén jogtalan előnyökhöz jutnak, megkárosítva ezzel az egyéneket,

[1] National Institute of Justice Focus Group Meeting: Identity Theft Literature Review 2005 https://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf
[2] http://www.creditcards.com/credit-card-news/credit-card-industry-facts-personal-debt-statistics-1276.php
[3] Forrás: http://www.biharlap.hu/hirek/lop%E1s,Bihari+h%EDrek/index.html (2012. 04.16.)

közösségeket, társaságokat. A folyamat 3 lépésből áll: az adatok megszerzése, az adatok felhasználása és a leleplezés.[4]

Az identitásunk és adataink kezelése az információ-, az adatvédelem- és adatbiztonság keretében kell, hogy megvalósuljon mind jogi, mind műszaki és egyéb értelemben, komplex módon,[5] hiszen az identitás- és adatlopás nem csak a megkárosítottak vesztesége, de komoly erőforrásokat kíván a kivizsgálásban résztvevő szervektől, szervezetektől is,[6] és közvetve komoly veszélyt jelenthet az egész társadalomra. Lásd. 2. sz. ábra.

2. sz. ábra: Szalay Dániel: Veszélyben a PayPass ügyfelek? (2.) 2011.Forrás:[7]

Gondoljunk csak az elmúlt hetekben ismeretlen csoportok által a több ezer izraeli állampolgár banki adatai ellen elkövetett cselekményekre, amikor is 15 ezer bankkártya adatát a világnak szánt újévi „ajándékként" hozta nyilvánosságra egy hacker. A 7 millió bankkártya használóból 15 ezer ügyfél adata nem képvisel nagy százalékot (0.2%) és a bankok is időben blokkolták ezeket a kártyákat, a kevés érintett ügyfél kárát pedig gyorsan megtérítették. Aggasztó azonban, hogy bár pénzösszegben kifejezve alig származott kára az ügyfeleknek, de nevük, címük, telefonszámuk is illetéktelen kezekbe került. Az

---

[4] National Institute of Justice Focus Group Meeting: Identity Theft Literature Review 2005 https://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf

[5]Szadeczky Tamás: Szabályozott Biztonság PHD értekezés 2011. http://doktori-iskola.law.pte.hu/files/tiny_mce/File/Archiv2/szadeczky/ertekezes_szadeczky_nyilv.pdf

[6]National Institute of Justice Focus Group Meeting: Identity Theft Literature Review 2005 https://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf

7 Forrás: http://computerworld.hu/elektronikus-zsebtolvajlas-veszelyben-a-paypass-ugyfelek.html letöltés: 2012. 04.17

esetleges identitás-lopásból származó veszélyeket pedig sokáig tart majd felmérni az illetékes szerveknek.[8],[9]

Joggal merül fel a kérdés, hogy ha egy bankot vagy önkormányzatot felelősség terheli az adataink biztonságáért, miért tekintjük az egyént áldozatnak, akkor, ha adatai felfedhetőséget könnyű hozzáféréssel es nyilvánosságra hozással önmaga „segítette". Az, hogy hol húzódik az a bizonyos határvonal az áldozat és a gondatlan felhasználó között, akár egy külön kutatás témája is lehetne. Egy azonban biztosan kijelenthető, az identitás- és adatlopás megelőzése az egyenek felelőssége is, egyetlen nemzeti vagy nemzetközi szereplő, hatóság sem lephet fel hatékonyan adataink biztonságáért, ha az adataink kikerülésének forrásai mi magunk vagyunk.

2. A LEGISMERTEBB SZEMÉLYES- ÉS PÉNZÜGYIADAT-SZERZÉSI MÓDSZEREK ÉS AZOK CÉLJA, CÉLCSOPORTJAI

Vizsgáljuk meg, hogy milyen módszerek terjedtek el az adataink ellenei támadásokra. Az, hogy milyen úton jutnak, és milyen mértékben adataink illetéktelen kezekbe, napról napra fejlődik, változik, egyre szofisztikáltabb módszerek látnak napvilágot, ami az internet használatával, gyorsaságával és népszerűségével terjedt el: több információt, adatot, lehet megszerezni es könnyebben, gyorsabban lehet átadni, akár globális keretek között és távolságokra is.[10]

A módszereket vizsgálva számos megoldással találkozunk, e cikk keretében nem térhetek ki mindegyikre, ezért csak néhány a tradicionális és modern adatlopás-módot ismertetek.

8 Israel vows to hit back after credit cards hacked
http://www.haaretz.com/news/diplomacy-defense/israel-vows-to-hit-back-after-credit-cards-hacked-1.406004 (2012.1.7)

[9] Bank of Israel: 15 thousand credit card details have been stolen
http://www.globes.co.il/news/article.aspx?did=1000712125

[10] National Institute of Justice Focus Group Meeting: Identity Theft Literature Review 2005 https://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf

2.1 ADATSZERZÉSI MÓDSZEREK

A tradicionális identitás- és pénzügyi információlopás még mindig nagy százalékban van jelen még a legfejlettebb országokban, így Amerikában is. A materiális módszerek, az elvesztett vagy ellopott irattárcák es bankkártyák az egyik vezető forrásai a visszaéléseknek. Emellett még mindig jellemző a fizikai adat-halászat másik módszere, amely a címünkre küldött vagy általunk eldobott értékes információt tartalmazó papírok összeszedését jelenti és a dokumentumaink lefényképezését, leolvasását (ATM automatánál, POS pontnál stb.) Előfordulhat azok fénymásolása majd visszajuttatása például egy hotelben). Nem utolsó sorban pedig számos olyan identitáslopás kerül bejelentésre, amelyet családtagok, ismerősök, munkatársak adtak illetéktelen kezekbe.[11]

A legmodernebb módszerek mára már azonban az internetre vagy elektronikus adatbankokra támaszkodnak, bankkódjaink vagy egyéb adatainkat tartalmazó rendszerekhez való egyéni belepési kódjaink megszerzése, illetve adatagregátorok, bankok, társadalombiztosítási és egyéb nyilvántartó rendszerekbe való betörések, mint a cybercrime révén.

Mindenki által jól ismert modern módszer a ***Spam/Cookie/Vírus küldése***, amely letöltés, rákattintás után lehetővé teszi az adatcserét a felhasználó tudta nélkül, vagy akár egyszerű módon csak személyes információt kér a felhasználótól. Szintén elterjedt a ***key logging***, amely figyeli a billentyűzet használatát es így nyer információt, és a ***pharming*** vagy ***skimming*** (ami a felhasználó átirányítása hamis weboldalra akkor is, ha az igazi keresett weboldalt gépeli be, például eBank oldalak vagy különböző ügyfélkapu rendszerek) még mindig vezető módszerek az információgyűjtésben.[12]

Adatok természetesen legkönnyebben olyan forrásokból szerezhetőek, amikhez szinte semmilyen módszerrel sem kell behatolni a felhasználók rendszerébe, tehát a hozzájutás könnyűsége adott, és még nem is illegális. Erre a legalkalmasabbak a ***közösségi weboldalak*** és azok alkalmazásai. Ugyanakkor a fent említett módszerek bármelyike nagyobb sikerrel is alkalmazható, hiszen egy „barátunknak" szívesebben nyitjuk meg az üzeneteit, mint egy email levelesládánkba érkező levelet, és gyanú nélkül adjuk át az adatainkat. A közösségi oldalakon közzétett és/vagy rögzített információ sokszor elegendő

[11] National Institute of Justice Focus Group Meeting: Identity Theft Literature Review 2005 https://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf
[12] Identity Theft Assistance Center; IDSentinel Product Information http://www.itacsentinel.com/idtheftandyou.html

identitásunk másolására, nevünk, születési dátumunk, iskoláink, munkahelyeink, geo-információink, házastársunk, gyerekeink, iskolatársaink, munkatársaink információi és még sok más, elegendőek lehetnek visszaélések elkövetéséhez, a teljes személyiségünk lemásolásához.[13]

Fokozza a bajt, hogy a vírusok, a férgek és a trójai programsorok számos csatornát használnak fel készülékeink megtámadásához. Nem csupán letöltéseken keresztül, de MMS-en, SMS-en, chatszolgáltatókon, Wi-Fi-hotspotokon és Bluetooth-on keresztül is fertőznek[14] és akár hónapok telhetnek el, mire felfedezzük őket az eszközeinken.

A modern módszerek közé tartozik a nagytételű adatlopás vagy más néven ***aggregált lopás,*** amely belső forrásból vagy kívülről jövő betörések nyomán (hacking) történik, és jellemzője, hogy jól szervezett, széleskörű számítógépes ismeretekkel rendelkező csoportok hajtják végre olyan szervezetek ellen, amelyek sok személyes és pénzügyi adatot tárolnak és dolgoznak fel (bankok, biztosítók, állami szervek stb.).

A fentiekben vázolt módszereket gyakran ismerjük, kevésbé ismert azonban, hogy mi a célja az adatok ellopásának. Vizsgáljunk meg néhány célt!

2.2 AZ IDENTITÁS- ÉS ADATLOPÁS LEGISMERTEBB LEHETSÉGES CÉLJAI ÉS CÉLCSOPORTJAI

Az adatlopás céljait sokfélekeppen lehet csoportosítani, itt a legjellemzőbb célcsoportokat említem aszerint, hogy kis vagy nagytételű adatszerzésről van szó, illetve, hogy mi ezek kimenetele (pénzügyi haszonszerzés vagy más jellegi cselekmény).

Az adat- és identitáslopás legegyértelműbb célja az ***egyének és a cégek pénzének leemelése*** a bankszámlájukról, hitelek felvétele a nevünkben, vagy bankkártyájuk (jogi kifejezéssel élve készpénzt helyettesít fizetési eszközük) illetéktelen felhasználására irányul. Különösen igaz ez olyan bankszámlák esetében, ahol napi szinten sok tranzakció történik és később, akár csak hónap végén, vagy még ritkábban egyeztetik a számlákon történt pénzmozgást. Ezek rendszerint a vállalatok, intézmények, civil szervezetek. Természetesen a pénzügyi tranzakciók interneten keresztül történő lebonyolítása

[13] Entrepreneurs' Organization: How Social Media Networks Facilitate Identity Theft and Fraud http://www.eonetwork.org/knowledgebase/specialfeatures/pages/social-media-networks-facilitate-identity-theft-fraud.aspx

[14] Android védelmezők: http://nonstopmobil.hu/android-vedelmezok-20111207.html

országonként eltérő, de mindenhol az a jellemző, hogy a cégek nagy része online intézi a pénzügyeit. Ezért egy szintén amerikai megkérdezéses felmerés vizsgálta a cégek és alkalmazottjaik attitűdjét az általuk igénybevett banki szolgáltatásokról. Meglepő adatok jöttek ki mind a saját pénzintézetük megítélésében, mind az ezzel kapcsolatos ismereteik vonatkozásában.

A megkérdezett cégek több mint 50%-a nem volt biztos abban, hogy az általuk használt céges online banki szolgáltatások megfelelően biztonságosak-e, mindössze 12%-uk használ web application tűzfalat es 40%-uk valamilyen encryption vagy VPN technológiát annak ellenére, hogy a megkérdezettek 59%-a tapasztalt 2-nél több csalást a banki tranzakcióival kapcsolatban. A megkérdezettek 35%-a ugyanakkor úgy tartja, hogy az adataikkal való visszaélésben egy belső alkalmazott játszott közre (közvetlenül vagy közvetetten) és nem külső adatlopás áldozatai voltak. Érdekes adat, hogy 5%-uk a közösségi oldalakon történő adathalászatot teszi felelőssé a lopásért, és az, hogy 21%-uk egyáltalán nem tudta, hogy hogyan jutott illetéktelen kezekbe a bankszámlájuk. A jelentésből kiderül, hogy a cégeknek nem csak pénzügyi veszteséget, de átmenetileg produktivitás-visszaesést is okozott a csalás, 53%-uk azonban mégsem változtatott online belső biztonsági politikáján.[15] Egy másik kutatásból pedig az derül ki, hogy egyenes korreláció van a cég mérete, alkalmazottainak száma és a jelentett csalások között, minél nagyobb a szervezet, annál nagyobb az esélye, hogy célpont lesz.[16]

A cégek mellett természetesen több olyan célcsoport veszélyeztetettsége is megjegyzendő, melyek könnyebben esnek áldozatul: ők például ***a fiatalok***, akik egyre korábban vesznek igénybe banki és online banki szolgáltatásokat[17] ***és a nők***, de ide sorolhatóak a szolgálatukat töltő ***katonák*** is, hiszen ők sokszor hosszú hónapokig nem ellenőrzik pénzügyeiket, számláikat. Számos cikk, felhívás és irodalom jelent meg a katonák identitáslopásának terjedéséről, és ennek kiváltó okairól. Ilyen például az amerikai Social Security Number (Nemzeti Társadalombiztosítási Szám) felhasználásáról. (Ezt a katonai személyes iratokra is rányomtatták, így egy lopással a személyhez köthető teljes

[15] Business Banking Trends Study http://www.guardianananalytics.com/researchandresources/researchstudies_resources/2011_truststudy_full_report.pdf

[16] PriceWaterhouseCoopers: Cypbercrime: protecting against the growing threat Global Economic Crime Survey http://www.pwc.com/en_GX/gx/economic-crime-survey/assets/GECS_GLOBAL_REPORT.pdf

[17] MNO.hu: Egyre korabban `bankolnak` a fiatalok http://mno.hu/gazdasag/egyre-korabban-bankolnak-a-fiatalok-1071449

adatok elérhetőek voltak a csalók számára) E szám kötelező használatának korlátozását és jobb adatbiztonsági rendszerek kiépítését már az illetékes szervek is megkezdték.[18].

A felmerések szerint a szolgálatot töltő katonák 3,3%-át károsították meg csalók,[19] ugyanakkor megrendítő, hogy bejelentések érkeztek Afganisztánban és Irakban elhunyt katonák nevében elkövetett csalásokról is.[20] A katonák és családjuk számára mára már lehetőség van távollétük alatt „Duty Alert" szolgáltatásra, amely figyeli a különböző adataik és pénzügyi tranzakcióik mozgását, pénzügyi tranzakciók előtt extra megerősítést kérnek a felhasználótól és e-mailben is jelentést küldenek, ha bármilyen furcsa mozgást tapasztalnak.[21]

A pénzünk megszerzése mellett természetesen megjelennek olyan motivációk is, mint valamilyen ***juttatáshoz, szolgáltatáshoz való hozzájutás***, ilyen például a jogtalanul igénybevett társadalom- és egészségbiztosítás.[22] Egyre gyakoribbak ugyanakkor az állami, a banki és a privát szektor pénzügyi információs rendszerei elleni jól szervezett támadások is, melyek célja nemcsak az adatokhoz való tömeges hozzájutás és tovább-értékesítés lehet, hanem ***a nyilvánosság keresése, a nyomásgyakorlás*** vagy akár a ***versenytársunk rossz hírnevének keltése.***[23], továbbá a szolgáltatásokhoz való hozzájutás korlátozása (blackouts), akadályozása. Jó példa a nyilvánosság keresésére, hogy 2008-ban Nikolas Sarközy bankszámlájára történt betörés, mely során csak kisebb összegeket vettek le a csalók.[24]

Érdemes megemlíteni, hogy miért olyan népszerű az identitás- és a banki adatlopás, akkor is, ha annak célja nem a pénzünk eltulajdonítása vagy valamilyen szolgáltatás igénybe vétele a nevünkben. Adatainkat felhasználva a technológia már lehetővé teszi, hogy bármilyen dokumentumot előállítsanak, majd ezeken keresztül hivatalos iratot igényeljenek, amely majd alapul szolgálhat ember, drog- és fegyverkereskedelemhez, pénzmosáshoz és terrortámadásokhoz is. Az EUROPOL 2011-ben is kiemelte, hogy a

---

[18] Identity theft.com: Identity Theft and Military Personnel
http://www.identitytheft.com/article/identity_theft_military
[19] The New York Times: Service Members Face New Threat: Identity Theft
http://www.nytimes.com/2010/12/07/technology/07identity.html?_r=1&pagewanted=all
[2020] Amy Bushatz Military.com: Fallen Warriors Victims of ID Theft
http://www.military.com/news/article/fallen-warriors-victims-of-id-theft.html
[21] Federal Trade Commission: Military Personnel & Families Fighting Back Against Identity Theft
http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt02.shtm
[22] Washington Coalition of Crime Victim Advocates: Washington State Identity Theft Alliance
http://www.wccva.org/identitytheftalliance.htm
[23] Proposal for a Directive on attacks against information systems, repealing Framework Decision 2005/222/JHA http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/463
[24] ArcSights: Combating Fraud & Data Theft in the financial services industry research 016-081509-05
http://www.arcsight.com/collateral/whitepapers/ArcSight_Whitepaper_Banking.pdf

szervezett bűnözés egyik alapeleme a személyes és egyéb dokumentumok hamisítása és felhasználása.[25]

Különösen fontos az ezek elleni védekezés és megelőzés nekünk, európaiaknak és magyaroknak a Schengeni övezet őreiként, az illegális bevándorlás és csempészet kiszűrésének felelőseiként. A visszaéléseket kutatva, elemezve az ilyen weboldalakat, a megfelelő keresőszavak beírásával hamis dokumentum-készítő weboldalak tömegével találkozhatunk. Akár órák alatt hozzájuthatunk hamis dokumentumokhoz és megdöbbentő módon „1-et fizet, 2-őt kap" akcióval egybekötött ajánlatokkal spórolhatunk. Egy hamis útlevél 80 USD+szállítási költségtől beszerezhető, míg hamis közüzemi számlák már 30 USD- tól elérhetőek. Egyes weboldalak pedig nyíltan hirdetik, hogy 150 ország személyes iratait tudják olcsón és nagytételben hamisítani, ugyanakkor a „Szerződési Feltételek" felhívják a figyelmet, hogy ezek felhasználása csak oktatási célra ajánlott, és nem vállalnak felelősséget más jellegű felhasználásáért.

A dokumentum-hamisítás és az ehhez való adatfelhasználás nem pusztán pénzszerzés céljából történő kivitelezésének kérdésére a választ talán legjobban a 2001. szeptember 11-es terrortámadás szemlélteti,[26] amely mérföldkő volt az identitás- és banki adatlopás, az azzal elkövetett nem csupán pénzügyi célú csalások és a bűnözés, nemzeti és nemzetközi veszélyeztető tényezőként való megítélése tekintetében.

3. sz. ábra: Hamisítható? Forrás:[27]

[25] OCTA 2011 EU Organized Crime Threat Assessment
https://www.europol.europa.eu/sites/default/files/publications/octa2011.pdf p.37
[26] Dr Gary R Gordon and Mr. Norman A. Willox, Jr.: Identity Fraud: A critical National and Global Threat
http://www.utica.edu/academic/institutes/ecii/publications/media/identity_fraud.pdf
[27] Forrás: http://www.unco.edu/cie/passport.html

Az identitáslopás szerepe a szervezett bűnözésben, illegális bevándorlásban és a terrorizmus támogatásában egyre inkább előtérbe kerül a nemzeti es nemzetközi biztonság-kutatási folyamatokban. A biztonságpolitikusok ráirányították a figyelmet a terrorkutatások során, hogy az egyik fontos tényező az adatlopás, identitás-lopás, különösen a cselekményhez szükséges dokumentumok előállítása és a pénzek mozgatása során.

3. AZ ADATLOPÁSOK ELLENI KÜZDELEM, ÉS ANNAK NÉHÁNY FORMÁJA

A fentiekben vázoltam az identitás- és adatlopás veszélyeit, formáit, céljait. Ezek tükrében vizsgáljuk meg, milyen módszerek alakultak ki, amelyekkel ezek ellen a cselekmények ellen sikeresen fel lehet lépni.

A 2001-es eseményekből ugyan tanultunk (US Patriot Act, új adatbiztonsági szabályok stb.), de amint azt az elmúlt évek katasztrófáinak példája, a mindennapok ilyen irányú eseményei mutatják, nem sikerült az identitás- és adatlopást teljes mértékben feltérképezni, megfelelő mechanizmusokat kiépíteni és a lakosságot felkészíteni erre a veszélyre. Hogyan érzékelik a vállalatok és pénzintézetek a saját helyzetüket ebben a folyamatban?

A Price Waterhouse Coopers 2011. novemberben 78 országra kiterjedően készült felméréséből kiderül, hogy a cégek legnagyobb félelme, hogy a cybercrime hírnevük elvesztéséhez és a személyes adatok kijutásához vezethet, mégis a megkérdezettek többségének nincs megfelelő krízisterve a számítógépes bűnözés ellen. Érdekes adat, hogy a válaszadók 46%-a a cypbercrime-ot kívülről jövő jelenségnek tartja, míg csak 13%-uk gondolja úgy, hogy csak a szervezeten belülről várható támadás, sokuk meggyőződése pedig az, hogy az IT osztály dolgozói lehetnek a legnagyobb okozói, mert ők rendelkeznek a legnagyobb tudással és hozzáféréssel, míg a HR es jogi osztályok a legkevésbé. [28]

Nem meglepő tehát, hogy úgy látják, hogy az elbocsátott dolgozók 60%-a tart meg információt, amely később felhasználható a vállalat ellen, a következő munkahelyen alkupozícióként[29] vagy egyszerűen eladható az interneten. Ugyanakkor a Financial

[28] PriceWaterhouseCoopers: Cybercrime: protecting against the growing threat Global Economic Crime Survey http://www.pwc.com/en_GX/gx/economic-crime-survey/assets/GECS_GLOBAL_REPORT.pdf
[29] PCT Tools Security News 2010 December 7: Disgruntled Employees & Desperate Job Seekers Increasingly Committing Cyber fraud http://www.pctools.com/security-news/disgruntled-employee-cyberfraud/

Services Authority (FSA, UK) által is közzétett és megerősített McAfee felmérés azt mutatja, hogy többnyire nem a dolgozók adatkiviteli tevékenysége, hanem általában a gondatlanság is okozta a rést a „biztonsági" rendszeren: például a nem biztonságos programok letöltése, és ehhez a biztonsági rendszer időleges kikapcsolása. Ezért a dolgozók biztonsági ismereteinek bővítése első is elengedhetetlen eszköze az adatbiztonság fenntartásának.[30]

Az előző hónapok, magyar viszonylatú bankkártya csalásai éreztették a hátasukat, a pénzügyi tranzakciókban érintett szervezeteknek, cégeknek (bankoknak és kártya-elfogadó helyeknek egyaránt) mára már mindenütt nem csak a jogszabályi előírások miatt, hanem a hírnevük, az ügyfelek bizalmának kiépítése es megtartása miatt is, érdekükben áll többszintű és szerteágazó védelmi rendszerek kiépítése.[31]

Az adatlopás elleni küzdelem néhány formája

A személyes adatok lopásának kulcsa az egyén maga: fontos a dokumentumaink fizikai védelme, személyes információk átadásakor a körülmények megvizsgálása, a „csak amennyi feltétlen szükséges" elv szem előtt tartása, számítógépeink, laptopjaink, telekommunikációs eszközeink megfelelő tűzfalakkal való ellátása, körültekintő es veszély-tudatos használata, és nem utolsó sorban a szolgáltatóink tudatos megválasztása. Az erre való felkészítésnek sok országban nagy hagyományai vannak, Magyarországon a bankok weboldalain mar fellelhetők biztonsági felhívások a pénzügyi adataink, kódjaink védelme érdekében, de nem az általános személyi adatok tekintetében, ezért nálunk még sok a teendő ezen a téren.

Szervezeti szinten a műszaki és a logikai biztonsági eszközök megléte fontos feltétele az adatbiztonságnak.[32] Ezekre a módszerekre nem térek ki, mert számos rendszerező tanulmány és cikk készült és folyamatosan készül ebben a témában. Azért

---

[30] Financial Services Authority: Countering Financial Crime Risks in Information Security – Financial Crime Sector Report http://www.fsa.gov.uk/pubs/other/fcrime_sector.pdf

[31] Payment Card Industry Data Security Standard Self Assessment Questionnaire Instructions and Guidelines https://www.pcisecuritystandards.org/documents/pci_dss_saq_instr_guide_v2.0.pdf

[32] A mistake biztonság magában foglalja az elemi, a műszaki követelmények és a műszaki megbízhatóság hiányából bekövetkező károkat. A logikai biztonság pedig magában foglalja `a szoftver elemek megbízhatóságát, a szándékos károkozás elleni védelmet, a hálózati protokollok biztonságát, és a hozzáférés-menedzsmentet.`
Forrás: Szadeczky Tamás: Szabályozott Biztonság PHD értekezés 2011 http://doktori-iskola.law.pte.hu/files/tiny_mce/File/Archiv2/szadeczky/ertekezes_szadeczky_nyilv.pdf p.32-33

megemlítendő, hogy a klasszikus fizikai biztonsági megoldásokat az adatlopások megakadályozására mára inkább felváltották a digitális tároló-rendszerek védelmére fejlesztett megoldások, és ezzel párhuzamosan az esetlegesen kikerülő adatok „olvashatatlanná" és használhatatlanná tételére irányuló fejlesztések Egyre több kutatóhely kezdett ilyen irányú fejlesztésekbe. „Az amerikai védelmi minisztériummal szerződött kutatók olyan módokat keresnek, amelyek révén jelszóként használhatók valakinek a gépelési szokásai, ezáltal folytonosan igazolni lehet az azonosságot. Szerintük ez a megoldás különösen akkor lehet értékes, amikor egy katona laptopja harci helyzetben ellenséges kezekbe kerül."[33]

Ugyanilyen fontos szerepet kapott a biometrikus azonosítási rendszer, mint az íriszes, az újlenyomatos stb. és a viselkedésre alapozott azonosítás. Egy új kutatás szerint a gesztusok is sajátosak, egyediek, így használhatók arra, hogy csak általuk lehessen hozzáférni az eszközhöz, illetve elindítani az alkalmazást, amelyik a biztonságos hozzáféréshez szükséges sokféle jelszót őrzi. Erre épül Nasir Memon számítástechnika-professzor és munkatársai kutatása a New York University Polytechnic Institute-on, amely során „a feladat egy kombinációs zár elfordítása volt kilencven fokkal, egy másik esetben pedig a kísérleti alanynak meg kellett jelölnie a nevét a képernyőn és kiderült, hogy mindenkinek egyedi ez a mozdulat." [34]

Ezek a módszerek ma meg nem használatosak a mindennapokban, és nehezen elképzelhető, hogy ujjlenyomatunkkal vagy íriszünkkel kell majd azonosítanunk magunkat, és bankkártyánkat a szupermarketben, ugyanakkor ezek hasznos azonosítási eszközök lehetnek új személyes iratok kiállításakor elengedhetetlen személyazonosításhoz, bevándorláshoz, bankszámlanyitáshoz stb. ezzel is csökkentve a hamis dokumentumok elfogadásából származó csalások, bűncselekmények elkövetésének lehetőségét.

[33] Még mindig korai temetni a jelszavakat http://www.sg.hu/cikkek/87779/meg_mindig_korai_temetni_a_jelszavakat, 2012. február 16. Forrás: MTI
[34] Még mindig korai temetni a jelszavakat http://www.sg.hu/cikkek/87779/meg_mindig_korai_temetni_a_jelszavakat, 2012. február 16. Forrás: MTI

4. sz. ábra: Mindenki másképp fordítja el a virtuális zárat: egyedi a kézméret, az ujjak távolsága, a forgatás sebessége és szöge, Forrás: [35]

Mivel a megelőzés gyakran sikertelen, ezért a bekövetkezett lopásokat követő adatfelhasználás megakadályozása is hozhat eredményt. Dr. Gary R Gordon and Mr. Norman A. Willox: *Az Identitas-csalás: A kritikus nemzeti és nemzetközi fenyegetés* című műben új megközelítést, részletes elemzést tálalhatunk a csalások és a bűnözés elleni védekezés nehézségeiről, módszereiről. Az írás nem az adatlopás megelőzését, hanem az ellopott adatok ***illegális felhasználása elleni küzdelmet*** és módszereit priorizálja. Arról, hogy hogyan azonosítsuk az elénk tárt adatok valóságát, és az előttünk „álló" személy identitását. A témát tehát az adatokat es dokumentumokat elfogadó szervezetek, állampolgárok szempontjából vizsgálja, szem előtt tartva a másodlagos, hamis dokumentumok beszerzésének egyszerű mivoltát.[36] Ha a személyes adataink ellopása nem is állítható meg, de felhasználásának megakadályozása a „felhasználói" pontokon sikeresebb lehet.

A következő fontos megelőzési lépés lehet, amely már túlmutat az egyénen és a pénzintézeteken, cégeken, az előírások, a védelemnek megfelelő szabályzások tovább fejlesztése. Egy példa erre a PCI DSS az „5 Bankkártya Társaság" (Mastercard, VISA, AMEX, Discover, JCB) által közösen létrehozott adatbiztonsági szabvány, amely a

[35]Forrás: U.ott
[36] Dr Gary R Gordon and Mr Norman A Willox, Jr.: Identity Fraud: A critical National and Global Threat http://www.utica.edu/academic/institutes/ecii/publications/media/identity_fraud.pdf p.8

bankkártya adatok biztonságos kezelésének szabályait tartalmazza az üzleti folyamatoktól egészen a mély technikai részletekig”[37]

A már említett izraeli példára hivatkozva itt érdemes megemlíteni, hogy a 15 ezer bankkártya adat nem közvetlenül a bankok weboldalának és adatbázisának feltörése nyomán került nyilvánosságra, hanem egy újonnan fejlesztett kuponokat kínáló szolgáltatás által, amelyet úgy dobtak piacra, hogy annak PCI kompatibilissé tétele meg nem fejeződött be. [38]

Míg az állami vagy céges rendszerek biztonsági előírásainak szabályozására már vannak nemzetközi, nemzeti és a magánszektor által kezdeményezett előírások (ISO, PCI, COBIT stb.), az egyének viszonylatában ez még nem így van. Ezzel párhuzamosan gyors fejlődésnek indultak, egyre népszerűbbek és keresettebbek lettek az erre a problémára megoldást kínáló új technológiák és magáncégek is, amelyek megpróbálják kiszolgálni mind az állami, mind a magánszektor cégeinek és egyéneinek biztonsági szükségleteit. Magyarországon is számos tanácsadó, szakértő és auditor lelhető fel identitás- és adatbiztonság témakörben, de ők főleg cégeknek, bankoknak, biztosítóknak, bankkártya vagy online tranzakciókat (card-not-present) elfogadó helyeknek kínálnak megoldásokat. Ugyanakkor, még nem terjedtek el az egyénre szabott szolgáltatások.

Több országban, így az USA-ban is, számos olyan tanácsadót találtam, melynek fő profilja az ügyfelek identitásának, adatainak, pénzügyi forgalmának elemzése és védelme. Ehhez kapcsolódóan pedig különböző biztosítási termékeket is ajánlanak arra az esetre, ha az adatlopás és az azzal való visszaélés mégis megtörténne. Ezek széleskörű jogi- es egyéb segítséget nyújtanak az áldozatoknak az „újrakezdésében.”[39] Ezek a szolgáltatók, a megfelelő jogszabályi és auditálási környezet kialakulása után (ez még nem biztosított) azért lehetnek hatékonyabbak a bankok kockázat-kezelésénél, mert nem csak számla-történetünket, hanem egyéb adatainkat is képesek valós időben összevetni.

[37] AperSKY: PCI DSS kérdések és válaszok, http://www.apersky.hu/pci-dss-info/pci-dss-faq
[38] Bank of Israel: 15 thousand credit card details have been stolen http://www.globes.co.il/news/article.aspx?did=1000712125
[39] Erre 2 példa ITAC Sentinel http://www.itacsentinel.com/index.html vagy a National ID Recovery LLC http://www.nationalidrecovery.com/

Összességében megállapítható, hogy napjaink új kihívása az identitás- és adatlopás, különösen igaz ez a pénzügyi adatainkra. Az identitás- és adatlopással elkövetett csalás olyan folyamat, amely során az elkövetők célzottan ezeket az adatokat keresik, és az adatok eltulajdonítása, majd azok felhasználása révén jogtalan előnyökhöz jutnak, megkárosítva ezzel az egyéneket, közösségeket, társaságokat.

Az ilyen irányú támadások fő célja az érintettek pénzének eltulajdonítása, de más cselekményeknek is alapja lehet, mint például az adott személy vagy cég nevében elkövetett csalások, és bűncselekmények. Sajnálatos módon az adatlopás és felhasználás segítheti a terrorcselekmények, a közösségek egymás elleni küzdelme kiszélesedését, a szervezett bűnözés, a tömegpusztító fegyverek elterjedését, továbbá más, a Nemzeti Biztonsági Stratégiában kihívásként megfogalmazott cselekmények terjedését.

A pénzügyi adatok védelme elleni küzdelemnek több pólusa van, melynek egyik legfontosabbja maga a tulajdonos, akinek veszélytudatosabban kell kezelnie a saját adatait. Ennek alapfeltétele a felkészítés. Már gyermekkorban tudatosítani kellene az adataink felelőtlen kezelésének veszélyeit. Különösen fontos lenne a kiskorúak figyelmét ráirányítani az interneten, közösségi oldalakon magukról közölt információkkal kapcsolatos felelősségükre. A felnőtt lakosság irányába széleskörű felvilágosító tevékenységet kellene folytatni, ahogy teszik azt már sok országban.

Az adatbiztonság másik pólusát a pénzügyi szolgáltatók képezik. A pénzintézetekből, pénzügyi szolgáltatást nyújtóktól való adatlopás fókuszpontja a logikai védelem hiányosságaiban és a nem kellő tudatosságban keresendő (néhány esetben pedig magában a fizikai védelemben). Részükről a kódok és egyéb információk védelme hagyományos és új formáinak alkalmazása alapvető elvárás. Figyelniük kell továbbá a saját munkatársaik felkészítésére, és az adatkivitel szándékos vagy véletlen, esetleg gondatlan formáinak megakadályozására. Az adatbiztonság mára nem csak az IT részlegeken ismert fogalom. A klasszikus tűzfalak monopóliuma lejárt, és a tűzfal a jól működő adatvédelmi rendszer „csupán” egy szegmense lett. A műszaki és logikai biztonsági eszközök, a hozzájuk kapcsolódó írásban lefektetett belső szabályok, kívülről adoptált szabályrendszerek, rendszeres auditok és tesztek adhatnak teljes keretet az adatok biztonsága megőrzéséhez.

xxx

IRODALOMJEGYZÉK

Amy Bushatz Military.com: Fallen Warriors Victims of ID Theft
http://www.military.com/news/article/fallen-warriors-victims-of-id-theft.html
utolsó letöltés ideje 2012.04.24.

AperSKY: PCI DSS kérdések és válaszok, http://www.apersky.hu/pci-dss-info/pci-dss-faq
utolsó letöltés ideje 2012.04.24.

ArcSights: Combating Fraud & Data Theft in the financial services industry research 016-081509-05
http://www.arcsight.com/collateral/whitepapers/ArcSight_Whitepaper_Banking.pdf
utolsó letöltés ideje 2012.04.24.

Globes.co.il: Bank of Israel: 15 thousand credit card details have been stolen
http://www.globes.co.il/news/article.aspx?did=1000712125
utolsó letöltés ideje 2012.04.27.

Guardian Analytics: Business Banking Trends Study
http://www.guardiananalytics.com/researchandresources/researchstudies_resources/2011_truststudy_full_report.pdf
utolsó letöltés ideje 2012.04.24.

Creditcards.com: Credit card statistics, industry facts, debt statistics
http://www.creditcards.com/credit-card-news/credit-card-industry-facts-personal-debt-statistics-1276.php utolsó letöltés ideje 2012.04.24.

Dr Gary R Gordon and Mr Norman A Willox, Jr.: Identity Fraud: A critical National and Global Threat
http://www.utica.edu/academic/institutes/ecii/publications/media/identity_fraud.pdf
utolsó letöltés ideje 2012.04.24.

Entrepreneurs' Organization: How Social Media Networks Facilitate Identity Theft and Fraud http://www.eonetwork.org/knowledgebase/specialfeatures/pages/social-media-networks-facilitate-identity-theft-fraud.aspx utolsó letöltés ideje 2012.04.24.

Federal Trade Commission: Military Personnel & Families Fighting Back Against Identity Theft http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt02.shtm
utolsó letöltés ideje 2012.04.24.

Financial Services Authority: Countering Financial Crime Risks in Information Security – Financial Crime Sector Report http://www.fsa.gov.uk/pubs/other/fcrime_sector.pdf
utolsó letöltés ideje 2012.04.24.

ID Sentinel: Identity Theft Assistance Center IDSentinel Product Information
http://www.itacsentinel.com/idtheftandyou.html utolsó letöltés ideje 2012.04.24.

Identity theft.com: Identity Theft and Military Personnel http://www.identitytheft.com/article/identity_theft_military utolsó letöltés ideje 2012.04.24.

Haaretz.com: Israel vows to hit back after credit cards hacked http://www.haaretz.com/news/diplomacy-defense/israel-vows-to-hit-back-after-credit-cards-hacked-1.406004 utolsó letöltés ideje 2012.04.24.

SG.hu: Még mindig korai temetni a jelszavakat http://www.sg.hu/cikkek/87779/meg_mindig_korai_temetni_a_jelszavakat, 2012. február 16. Forrás: MTI utolsó letöltés ideje 2012.04.26.

MNO.hu: Egyre korabban `bankolnak` a fiatalok http://mno.hu/gazdasag/egyre-korabban-bankolnak-a-fiatalok-1071449 utolsó letöltés ideje 2012.04.24.

National Institute of Justice Focus Group Meeting: Identity Theft Literature Review 2005 https://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf utolsó letöltés ideje 2012.04.24.

OCTA 2011 EU Organized Crime Threat Assessment https://www.europol.europa.eu/sites/default/files/publications/octa2011.pdf p.37 utolsó letöltés ideje 2012.04.24.

PCI Security Standards.org: Payment Card Industry Data Security Standard Self Assessment Questionnaire Instructions and Guidelines https://www.pcisecuritystandards.org/documents/pci_dss_saq_instr_guide_v2.0.pdf utolsó letöltés ideje 2012.04.24.

PcTools.com: PCT Tools Security News 2010 December 7: Disgruntled Employees & Desperate Job Seekers Increasingly Committing Cyber fraud http://www.pctools.com/security-news/disgruntled-employee-cyberfraud/ utolsó letöltés ideje 2012.04.24.

PriceWaterhouseCoopers: Cypbercrime: protecting against the growing threat Global Economic Crime Survey http://www.pwc.com/en_GX/gx/economic-crime-survey/assets/GECS_GLOBAL_REPORT.pdf utolsó letöltés ideje 2012.04.24.

Europa.eu: Proposal for a Directive on attacks against information systems, repealing Framework Decision 2005/222/JHA http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/463 utolsó letöltés ideje 2012.04.24.

Szadeczky Tamás: Szabályozott Biztonság PHD értekezés 2011. http://doktori-iskola.law.pte.hu/files/tiny_mce/File/Archiv2/szadeczky/ertekezes_szadeczky_nyilv.pdf utolsó letöltés ideje 2012.04.24.

The New York Times: Service Members Face New Threat: Identity Theft http://www.nytimes.com/2010/12/07/technology/07identity.html?_r=1&pagewanted=all utolsó letöltés ideje 2012.04.24.

Washington Coalition of Crime Victim Advocates: Washington State Identity Theft Alliance http://www.wccva.org/identitytheftalliance.htm utolsó letöltés ideje 2012.04.24.

Képek forrásai:

http://www.biharlap.hu/hirek/lop%E1s,Bihari+h%EDrek/index.html (2012. 04.16.)

http://computerworld.hu/elektronikus-zsebtolvajlas-veszelyben-a-paypass-ugyfelek.html utolso letöltés: 2012. 04.17

Android védelmezők: http://nonstopmobil.hu/android-vedelmezok-20111207.html

http://www.unco.edu/cie/passport.html utolsó letöltés ideje 2012.04.24.

Sg.hu: Még mindig korai temetni a jelszavakat http://www.sg.hu/cikkek/87779/meg_mindig_korai_temetni_a_jelszavakat, 2012. február 16. Forrás: MTI utolsó letöltés ideje 2012.04.24.