

A banki ügyfél-azonosítás anomáliái, bűnügyi aspektusai és a paradigmaváltás lehetőségei

A banki számítástechnikai rendszerek belső hálózatainak nagyfokú biztonsági szintje, szinte lehetetlenné teszi az illetéktelen hozzáférést, és ezen keresztül a számlafosztogatást. Ezért az ügyfélszámlák támadhatósága, csak a bemeneti adatok meghamisítása révén valósítható meg. Ennek egy lehetséges elkövetési formája, ha a számlakezelésre jogosult ügyfél szerepét egy csaló veszi át, aki megfelelően hamisított igazoló okmányok birtokában, az ügyfél ismeretéből, szokásaiból és az aláírás-hamisításból felkészülten, az ügyintézőt félrevezetve jut a számla kezelési jogához.

Több elágazást tapasztalhatunk e megoldás Magyarországon jellemző kivitelezésében, az egyszeri gyors lefosztástól a netbanki számlakezelő-rendszer fölötti kezelési jog átvételéig bezárólag. Természetesen megállapíthatóak közös jellemzők az elkövetésben, amelyek a megelőző lépések bevezetését elősegíthetik. Ezek a következők:

- ▶ a belső együttműködő partner beszerzése,
- ▶ a megfelelő ügyfél kiválasztási előszűrése,
- ▶ a számlatartalom, számlaforgalom megismerése,
- ▶ az ügyfélszokások megismerése,
- ▶ a hiteles adatokon alapuló fényképcserés igazolványok elkészítése,
- ▶ az akcióidőpont megszervezése.

Az ügyfélkiválasztás a belső tippadótól indul döntően, aki általában az illetéktelen betétkéntés módszerével jut a megfelelőnek tartott ügyfél adataihoz, számlaszokásainak ismeretéhez.

Az ügyfél-megszemélyesítést szinte mindig a honos fiók kikerülésével valósítják meg az elkövetők.

Az ügyfél-azonosítás jelenlegi szabályait alkalmazva a csalót igazolványa bemutatására, valamint a hitelesen regisztrált, általa alkalmazott aláírás minta szerinti aláírására kérjük fel.

Mivel nem honos fiókban jelentkezik, ezért a személyes ismeret veszélye nem fenyegeti, így a fényképcseré/személycsere nem derülhet ki. Ha kellően begyakorolta az aláírást, akkor azon sem bukik el. A cég és az ügyfélszokás ismeretének bennfentes jelzése,

szintén bizalomfokozó tényező, elősegíti a csalás sikerességét.

A számlajogosult személy adatainak, szokásainak megszerzése, és ez alapján a megismerése révén sok bosszúságot, veszteséget okoztak bűnözők már a magyar pénzintézeteknek. A személyazonosítás jelenleg ismert, elfogadott és alkalmazott módszereit már az intelligens bűnözés ki tudja játszani, nagy pontosságú másoló- hamisítószerzőkkel, valamint a kifinomult célirányos adatgyűjtésből származó módszerekkel. A személyazonosítási kontrolleszközök halmozott alkalmazása sem hozta meg a kockázat és ár/érték arányos elvárt eredményt.

Az Egyesült Királyságban például a személyazonosság ellopása a pénzügyi szektorban a legnagyobb károkozó, 2008-ban több mint 100 000 magánszemélyt érintve, ezáltal kb. 1,7 millió £ kárt okozva.

A szigorításokon alapuló módszerek, mint például a személyes, vagy személyhez fűződő adatok változtatásának végrehajtását csak honos fiókban, saját ügyintézőnél lehessen végezni, korlátozzák az ügyfelek által elvárt rugalmas, dinamikus számlakezelési lehetőségeket, ezért nem sikeresek.

Az aláírássellenőrzés nem automatizálható ipari méretekben, csak egyedi esetekben végezhető el, felkészített ügyintézők alkalmazásával.

Járható, bár nem olcsó megoldás az igazolványok eredetiségét ellenőrző eszközök beszerzése és alkalmazása fióki szinten. Ezzel kiszűrhetőek az illegálisan gyártott, kiváló

minőségű, megtevesztésre kiválóan alkalmas, hamisítványok is. Ezzel az ügyfél valószínű személyazonossága megállapítható.

Tökéletes, félrevezethetetlen megoldást, paradigmaváltást a számlatulajdonos azonosítására alkalmas biometrikus eszközök bevezetése jelenthet e témakörben. A biometria jelenleg az alábbi lehetőségekre terjed ki ipari méretekben e feladat végrehajtására:

- ▶ ujjlenyomat, ▶ arcfelismerő, ▶ hangfelismerő, ▶ íriszfelismerő, ▶ retinafelismerő, ▶ kézgeometria, ▶ vénafelismerő.

A biometrikus azonosítás alapja az egyedi személyes jellemzők mérésén, összehasonlításán alapuló rendszerek alkalmazása, azonban az egyes módszerek alkalmazása és eredményessége között nagy különbség van. A biometrikus azonosítók terén a legelterjedtebbek az ujjlenyomat-leolvasóra és a retinaszkenerre épülő módszerek, azonban az előbbi magas hibaszázaléka és utóbbi magas ára miatt problematikus az ipari alkalmazásuk. Az ujjlenyomat-leolvasót idegenrendészeti és igazságügyi szervezetek egyaránt használják. A vénaszennozos módszer viszont, a vénaminta vételével, ami csak élő szövet esetében lehetséges, belső azonosítónak minősül, mivel nem hagy nyomot az ujjlenyomattal szemben, emiatt a bűnüldözésben azonosításra nem alkalmazható.

Az egyes biometrikai eljárásokat az Amerikai Bírák Szövetsége (*American Judges Association*) összehasonlítottatta. Ennek eredménye a **táblázatunkban** található.

A lehetőségek elemzését értékelve, (**táblázat**) arra a következtetésre juthatunk, hogy a vénaszennozos érzékelés alkalmazása az ügyfél-azonosítás terén valódi paradigmaváltást hozhat.

ÁLTALÁNOS BEVEZETÉS A BIOMETRIKÁBA ÉS A VÉNÁ- SZENZOR BEMUTATÁSA

A biometrikus azonosítórendszer olyan technika, amely méri és rögzíti egy személy egyedi fizikai, testi jellemzőit és ezeket az adatokat azonosításra és hitelesítésre használja fel, például beléptető/azonosító rendszereknél. **A vénaszkenner a beolvasandó testrészben található vénaszervezetet azonosítja be és ezáltal hitelesíti a személyt egyedülálló módon.**

Technológia	Azonosítási opció	Pontosság	Hibaszázalék (FRR)	Megbízhatóság	Hibaforrás	Biztonsági szint	Használhatóság
Ujjlenyomat	Igen	Nagyon magas	1 az 500-ból	Magas	száraz bőr, kosz, sérülés, az emberek 10%-nak nem olvasható a lenyomata	Magas	Magas
Arcfelismerés	Nem	Magas	nincs adat	Közepes	fény, életkor, haj, szemüveg	Közepes	Közepes
Kézgeometria	Nem	Magas	1 az 500-ból	Közepes	sérülés, életkor	Közepes	Magas
Hangfelismerés	Nem	Közepes	1 az 50-ból	alacsony	zaj, időjárás, nátha	Közepes	Közepes
Írisz-szkenner	Igen	Nagyon magas	1 a 131 000-ből	Magas	fényviszonyok, egészségügyi változások	Magas	Közepes
Retina-szkenner	Igen	Nagyon magas	1 a 10 000 000-ből	Magas	szemüveg, kontaktlencse	Magas	Alacsony
Írásfelismerés	Nem	Közepes	1 az 50-ből	Alacsony	alírási változtatása	Alacsony	Magas
LifePass vénaszkenner	Igen	Nagyon magas	1 a 10 000 000 000-ből	Nagyon magas	kesztyű	Magas	Nagyon magas

A vénaszkennerben rejlő újdonság, hogy belső, kívülről nem látható ismérvet azonosít, a minta nem másolható vagy reprodukálható, így titkos adatgyűjtésre nem alkalmas.

A VÉNASZENZORON ALAPULÓ TECHNOLOGIA EGYEDISÉGE, ELŐNYEI

- ▶ 5 000 000 ponton azonosítja be az adott testrész vénatérképét 0,8–1 másodperc időintervallum alatt, így a legalacsonyabb hibaszázalékkal működik.
- ▶ Külső időjárási, fény- és egyéb viszonyoktól függetlenül működik.
- ▶ Használata során nem hagy nyomot, így titkos adatgyűjtés nem lehetséges.
- ▶ Nem készít képet, hanem azonnal titkosított adatsomagba képezi a vénalenyomatot és azonosítást követően visszavonhatatlanul azonnal törli a beadott mintát.
- ▶ Az azonosítandó személy egészségügyi állapotára való következtetésre nem alkalmas a készülék, illetve az általa készített adatsomag.

A TECHNOLOGIA NEMZETKÖZI ELISMERÉSEI, MINŐSÍTÉSEI

■ Common Criteria minősítés:

Legmagasabb nemzetközi biztonságtechnikai informatikai minősítés, mely kiemelten az adatlopás, beazonosítás minősége és adatvédelem területén vizsgálja meg az adott technológiát.

Tehát ha az ügyfél tárolt adatai közé a vénaszkenner által előállított HASH kód is bekerül,

akkor a tranzakciót végezni kívánó személy minden kétséget kizáróan azonosítható. Ezeknek a vénaszkenneres eszközöknek a fióki alkalmazása esetén bármely fiókban elvégezhető az ügyféli adatmódosításhoz szükséges személyellenőrzés. Technikai problémát a HASH kód őrzése jelenthet, az illetéktelen hozzáférés ellen. Persze a kód megszerzése itt nem jelenthet hamisítási lehetőséget, hiszen a kódot mindig az ellenőrző eszköz állítja elő, és küldi összehasonlításra a rendszerbe. A személytelen elektronikus azonosítás esetén van lehetőség a csalásra, de nyilván ez is, kellő figyelemmel kizárható.

Adatvédelmi szempontból vizsgálva, ez a HESS kód irreverzibilis módon képződik, ezért a rögzített személy tenyérvéna-térképe, vagy egyéb személyes jellemzője nem állítható elő belőle.

Ez egy technikai kód, aminek a tulajdonsága az, hogy abból a tenyérből csak az a kód képződik.

A HASH algoritmusok egyirányú kódolási rutinok, amelyek a bemeneti adatból a következő feltételek teljesülése mellett képeznek kimeneti adatot:

- ▶ Adott bemeneti adatból **mindig ugyanazt a kimenetet adja.**
- ▶ A kimeneti adat egyértelműen utal a bemeneti adatra, **de a kimeneti adatból nem állítható elő a bemeneti adat.**
- ▶ A bemeneti adat legkisebb változása is teljesen más kimenetet eredményez.

A vénaszkenner megjelenése és célszerű alkalmazása tehát az ügyfél személyazonos-

ságának megállapításában valódi paradigmaváltást hozhat a magyar pénzintézetek, biztonságvédelmi tevékenységében. Az ellenőrzés, azonosítás egyéb területein is alkalmazhatóak ezek az eszközök.

PÉLDÁUL:

A brazil Bradesco bankcsoport kísérleti jelleggel a Fujitsu és partnerei közreműködésével több mint 22 000 bankomatnál telepítette a vénaszkenzort a legmagasabb biztonság érdekében.

2004-ben a Suruga Bank és a Tokió Mitsubishi Bank kísérleti jelleggel telepítette a vénaszkenzort, mint másodlagos azonosítót a bankomatokra. Több mint 5000 automatára került telepítésre. Ebben az esetben a chipkártyára mentett vénaminta került alkalmazásra.

A 2004-ben elindult projekt főbb adatai: • azóta nem történt jelentősebb biztonsági esemény a vénaszkenzoron keresztüli azonosítással kapcsolatban, • 500 000 kibocsátott bankkártya, amelyen már a vénaminta rajta volt, • több mint 10 000 tranzakció naponta.

A biztonságtechnikai terén a technika új vívmányainak bevezetése, alkalmazása a lehetséges hatékony prevenció a bűnözés kihívásaival szemben.

Fialka György, biztonsági vezető
Budapest Bank Zrt.