# EGY BANK BIZTONSÁGI RENDSZERÉNEK FELÉPÍTÉSE

***Boda Péter PhD. hallgató***[1]

Az elmúlt hónapokban nem múlt el hét bankrablás nélkül. A rablók azonban általában mindig kevés pénzzel távoznak, és sokszor pár órán belül elfogják őket, köszönhetően a pénzintézetek fejlett biztonsági rendszerének.

A bankok kültéri és beltéri biztonságának egy adott szintet el kell érnie, a védelmi rendszer lényege pedig az, hogy késleltesse a behatolást. Többkörös, egymásra integrált védekezés épül ki: a fizikai biztonságtól a behatolás-érzékelőkön, a beléptető rendszeren és a videó-dokumentáló rendszeren túl magában foglalja az intézmény működési rendjét is.

A bankban dolgozók minden helyzetben tudják, mi a megfelelő viselkedés, tisztában vannak azzal, hogy az esetleges rendkívüli eseményekre hogyan reagáljanak. Itt hívnám fel a figyelmet a megfelelően képesített szakember gárdára.

A dokumentálás kulcsfontosságú, hiszen a beléptető rendszerek és a képrögzítés követhetővé teszik az adott személyt és az eseményeket egyaránt. A bankbiztonság fontos eleme a folyamatos képrögzítés - amely ma már korszerű digitális videotechnikával történik -, hiszen e nélkül a szakemberek egy bankrablás esetén nem tudnák elemezni a cselekményt, megkeresni a legapróbb árulkodó részleteket.

A kameráknak több előnye is van, ezek közül párat emelnék ki:

- Tökéletes minőségben rögzítenek;
- A felvételek visszajátszhatóak, sőt még az interneten keresztül is élőben, kényelmesen követhetőek az események;

[1] ZMNE BJKMK Katonai Műszaki Doktori Iskola

- Mozgásdetektálási terület meghatározásával lehetőség van egy adott terület figyelésére a felesleges időintervallumok kihagyásával;
- A felhasználókhoz különböző felhasználási jogosultságok rendelhetőek (pl. kik azok, akik törölhetik a felvételeket, és ki melyik kamera képét figyelheti).

A kameráknak többféle típusa ismeretes pl.: normál-rejtett, fekete-fehér, színes, vízálló, éjjel látók, rádiós átjelzésű, dome kamerák (1. sz. ábra), ipari távvezérelhető és vandálbiztos stb.

**1. számú ábra: Beltéri dome kamera**

A dolgozók rendszeres oktatást kapnak, hogy ha bekövetkezik a rablótámadás, hogyan kell viselkedniük. Ha ugyanis bankrabló követeli az egyik ügyintézőtől a pénzt, megnyomják a támadásjelző gombot - amely mindegyikük keze ügyében ott van -, sőt a biztonsági őr zsebében is van egy mobil támadásjelző. Ekkor aktiválják a csendes riasztást, ami a rendőrségre fut be.

A pénzintézetek sikeres üzletmenete, jó hírneve alapvetően függ attól, hogy szolgáltatásaikat megbízhatóan, folyamatosan, zavartalan és nem utolsó sorban biztonságos módon legyenek képesek nyújtani. Így ennek a stabil állapotnak fenntartása a pénzintézetek alapvető üzleti érdeke, kritikus sikertényezője. Az ügyfelek oldaláról ez természetesen azt jelenti, hogy értékeik,

adataik kezelése, tárolása a vonatkozó jogszabályok, a pénzintézettel kötött szerződések és persze az ügyfelek szándékai, elvárásai szerint történik.

A rabló egyik bankfiókban se juthat hozzá könnyen nagyobb pénzösszeghez, hiszen a pénzvédelmi eszközök egyik leghatásosabb módja az időzár. A széfek az ügyintézőtől függetlenül vannak programozva, így hosszú percekbe telik, mire ki lehet azokat nyitni. Akkor sem érezheti magát biztonságban a bankrabló, ha a pénz már a kezében van, mert lehet, hogy a köteg csapdát rejt: rádióadó van a bankók között, vagy az is előfordulhat, hogy robbanó pénzt zsákmányolt, amely bármikor sűrű füstöt bocsáthat ki és színes, szinte lemoshatatlan festékkel ken össze mindent maga körül.

A pénzintézetek szolgáltatásainak döntő többsége már nagyon régen igényel valamilyen szintű számítógépes támogatást, így tehát amikor egy bank megbízható és folyamatos működéséről beszélünk, szükségszerűen beszélnünk kell a pénzintézetek információs hátteréről, és az ezt támogató informatikai rendszer biztonságáról, megbízhatóságáról. **A megbízható és folyamatos működés elválaszthatatlan a pénzintézet informatikai rendszerétől.** Egy pénzintézet biztonságának megteremtése rendkívül komplex feladat, ezért e szervezetek biztonsági tevékenységük és operációs kockázataik kezelése kapcsán az objektumvédelem (vagyonvédelem, őrzésvédelem, tűzvédelem, építészet és épületgépészet biztonsági vonatkozásai), az információvédelem (titokvédelem, adatbiztonság, adatvédelem) és a humán-strukturális védelem (alkalmazottak, ügyfelek, külső szervezetek és személyek, személyvédelem, munkavédelem, baleset elhárítás) és a biztosítások kérdéseit, mint egymással szoros összefüggésben lévő, egymástól elválaszthatatlan biztonsági tényezőket kezelik. Ezt a felfogást célszerű követni a pénzintézet bankbiztonsági szervezetének struktúrájának kialakításával.

Egy pénzintézet informatikai rendszere eszközeiben, adataiban rendkívül nagy értéket képvisel, megbízható és biztonságos működése az adott pénzintézet

tevékenysége és működése szempontjából kritikus, ezért e szakterület biztonsági kérdéseinek különös jelentőséget kell tulajdonítani.

A fentiekből egyenesen következik, hogy a hitelintézeti informatikai rendszereinek rendelkezésre állása, az ott kezelt adatok sértetlenségének, bizalmasságának, hitelességének biztosítása nem csak azért fontos, mert számos jogszabály és PSZÁF ajánlás tartalmaz előírásokat e rendszerek tervezésére, fejlesztésére és üzemeltetésre vonatkozóan, de minden pénzintézetnek elemi érdeke is az, hogy – sokszor a jogszabályi előírásokat meghaladva – gondoskodjon informatikai rendszere megfelelő biztonsági színvonaláról.

A fentiek mellett van néhány **speciális körülmény**, melyet a **pénzintézetek informatikai rendszereinek tervezésekor, fejlesztésekor és üzemeltetésekor feltétlenül figyelembe kell venni**. Ezek közül a legfontosabbak:

- Ma a pénzintézetek funkcióinak függése saját informatikai rendszereiktől, illetve külső, nemzetközi informatikai rendszerektől olyan mértékű, hogy **ezen informatikai rendszerek jelentős része nélkül ma már nem lennének képesek alapvető szolgáltatásaikat nyújtani.** Ezen funkciók jelentős része csak nagyon rövid ideig, vagy egyáltalán nem pótolható más eszközökkel, illetve e rendszerek kiesése az érintett banki szolgáltatást vagy belső folyamatot az elviselhetetlen kockázatú tartományba taszítja.
- A **banki szolgáltatások egyre nagyobb köre 7x24 órás típusú**, tehát folyamatos rendelkezésre-állási igényt támaszt, **rendkívül rövid kiesési idő toleranciával.**
- Az elektronikus elszámoló, átutalási, pénzügyi tranzakciókat támogató üzenetkezelő valamint bankkártya-rendszerek mellé (pl. GIRO, SWIFT, VISA, EC/MC, stb.) banki szolgáltatások közül egyre többnek jelenik meg telekommunikációs hálózatokon keresztül, informatikai eszközökkel igénybe vehető változata. Az e-business, e-commerce, e-banking, e-bróker, e-paymant,

stb. csoportokba sorolható szolgáltatások, beleértve a mobil telefonokhoz köthető szolgáltatásokat, a banki informatikai rendszerek nyíltságát és ezzel támadhatóságának lehetőségét és veszélyét tovább fokozza. Ide sorolható az a tendencia is, hogy a fentebb említett „bankfiók független" banki ügyintézési lehetőségek a vezeték nélküli adatátviteli technológiák elterjedésével egyre kevésbe köthetők fizikai, vagy földrajzi helyekhez és e szolgáltatásokat igénybevevő felhasználók ismeretei és biztonságtudatossága sok esetben elmarad a kívánatos szinttől. Így a banki szolgáltatásokhoz hozzáférő végpontok és a banki rendszerek elektronikus kommunikációjának védelme megoldható, de mindenképpen újabb problémákat, kihívásokat jelent a biztonság oldaláról.

- **A pénzintézetek működése során keletkezett, feldolgozott adatok** szinte kivétel nélkül **jogszabályok által titokvédelmi szempontból is védeni rendelt adatok,** hiszen valamennyi bank-, pénztár-, értékpapír-, üzleti titok, vagy személyes adatnak minősülő információ, sőt viszonylag ritkán, de szolgálati és államtitok is előfordulhat a pénzintézeteknél. Ezen adatok titokvédelme természetesen független azok adathordozójától és mivel a pénzintézetek a fenti információk döntő többségét informatikai eszközökön keresztül használják, **e rendszerek bizalmasságának védelme különösen fontos feladat.**

- A pénzintézetek szolgáltatásainak csalárd felhasználása a bank, illetve ügyfeleinek megkárosításával **a fehérgalléros bűnözés egyik jelentős területe.** E támadások közvetett, illetve akár közvetlen eszköze is lehet az informatikai rendszer. E támadások megszervezéséhez, illetve kivitelezéséhez – a várható haszon nagyságának megfelelően – adott esetben igen jelentős anyagi és technikai erőforrásokat, illetve szakértelmet alkalmazhatnak a támadók. Vagyis e támadások kivédése, illetve megelőzése kapcsán **mindig professzionális felkészültségű támadókat kell feltételezni.** E fenyegetettségnek is van titokvédelmi vonatkozása, hiszen a pénzintézeteknél tárolt információk önmagukban is jelentős értéket képviselnek, így bizalmas kezelésük biztonsági,

üzleti és kriminológiai szempontból is egyaránt fontos. Itt természetesen meg kell említeni azt a fenyegetettséget is, amikor a potenciális támadók célja „csak" egy adott banki szolgáltatás, vagy akár a pénzintézet teljes informatikai rendszerének megbénítása, elérhetetlenné tétele, vagy csupán a szolgáltatás megbízhatóságába vetett ügyfél bizalom megingatása.

- Az informatikai rendszerek által tárolt adatok, a rendszer működésére vonatkozó információk valamilyen szinten **szükségszerűen hozzáférhetők a banki alkalmazottak számára, így a belső közreműködéssel megvalósított, vagy tisztán belső támadások kockázata sem elhanyagolható.** Ezért nagyon fontos, hogy megfelelő humánvédelemi eljárások biztosítsák, hogy megbízható személyek kerüljenek alkalmazásba, és megbízhatóságuk tartós legyen. Ezért a bizalmi munkakört ellátó alkalmazottaik kiválasztásakor **értékelni kell minden olyan törvényes eszközökkel beszerezhető, vagy rendelkezésre álló információt, körülményt,** amely azt bizonyítja, hogy az adott személy felkészültsége, lojalitása, becsületessége és megbízhatósága vitathatatlan, jelleme, szokásai, életvitele és kapcsolatai alapján nem vonható kétségbe megfontoltsága vagy helyes ítélőképessége a minősített információk (állam-, szolgálati-, üzleti-, és banktitok stb.) kezelését, felhasználását illetően. Arányosan a fennálló kockázatokkal, a banki alkalmazás feltételeit differenciáltan ugyan, de az általános munkavállalási gyakorlatnál szigorúbban kell megállapítani egy hitelintézet esetében. Sok adatvédelmi vita származott már azon kérdés megválaszolását illetően: milyen adatokat kérhet, és milyen adatszolgáltatási kötelezettségeket írhat elő a pénzintézet, mint munkaadó leendő, illetve már munkaszerződéssel alkalmazott dolgozói számára. Ezért e kérdés kezelésénél különösen körültekintően kell eljárni.

A pénzintézeti informatikai rendszerek biztonsági kérdései nagyban hasonlítanak más informatikai rendszerek biztonsági problematikáira, ugyanakkor a fentebb említett tényezők különleges eljárásokat, speciális eszközöket és megoldásokat indokol(hat)nak:

- Kritikus hardware eszközöket befogadó központi számítógéptermek, telekommunikációs központok kiemelt fizikai védelmet igényelnek. Ezen feltételek első csoportja az informatikai rendszer egyes elemeinek, ezen belül is kiemelten központi géptermeinek, kommunikációs központjainak **megfelelő fizikai védelme.** Itt fontos szerepe van az e helyiségek telepítési környezete kiválasztásának, különös tekintettel védett elhelyezésére és arra, hogy a környezet a lehető legkevesebb kockázatott hordozza a működés szempontjából (megközelíthetőség, szállítási útvonalak, nedves közművektől való biztonságos elhatárolás). Egy forgalmas közterület szomszédsága, nagyfeszültségű, alacsony frekvenciájú elektromágneses terek közelsége, vizes infrastruktúra a rendszert befogadó helység határoló falaiban, magas talajvíz szint, vagy vízcsőtörésből bekövetkező elöntés veszélye, korlátozott szállítási útvonalak, keresztmetszetek, rezgés-szennyezés, stb. mind elkerülendő fenyegetettség egy biztonságosnak szánt pénzintézeti számítógépterem telepítésekor.

- Különös figyelmet kell fordítani e géptermek **fizikai behatolás-védelmére és beléptetés kontrolljára.** Jó, ha a kívülállók számára nem válik nyilvánvalóvá a gépterem épületen belüli elhelyezkedése. Célszerű, ha magának a gépteremnek nincsenek ablakai. Ez nem csak a láthatóságot korlátozza, de egyszerűbbé teszi a gépterem későbbiekben tárgyalt zavarvédelmét is. A gépterem nyílászárói legyenek olyan kivitelűek, melyek valódi fizikai védelmet jelentenek. A határoló falak és nyílászárok kiválasztásakor ajánlott a tűzvédelmi, zavarvédelmi és behatolás-védelmi követelményeket egyaránt kielégítő megoldásokat választani. Géptermeket, az informatikai rendszer kritikus elemeit befogadó helyiségeket, védje mindig regisztrálást is végző, valamely fizikai eszköz (például proximity smart kártya) birtoklását és használatát megkövetelő beléptető rendszer. Ezen helyekre kizárólag számkombinációs beléptető rendszerek alkalmazása már nem tekinthető kockázatarányos megoldásnak. **Szigorúan védendő helyiségek esetében a biometrikus azonosítás, illetve a**

**bizottsági típusú - legalább két személy együttes jelenlétét – megkövetelő megoldásokat is mérlegelni kell.** A térfelügyelet fontos eleme ezen informatikai területeken a zártláncú videó-megfigyelő rendszerek alkalmazása. Fontos, hogy a rendszer által rögzített kép – az adatvédelmi jogszabályok figyelembevételével - rögzítésre kerüljön, a rögzítőrendszer képminősége és időszinkronizálása a pontos időhöz megoldott legyen. A felszerelt videó-rögzítő rendszer kameráinak elhelyezése nem adhat lehetőséget a kezelőszemélyzet felhasználói jelszavainak megfigyelésére, rögzítésére.

- A pénzintézeti géptermek fontosságuknak megfelelően **kiemelt tűzvédelmi megoldásokat igényelnek.** Alapkövetelmény hogy a gépterem egyedi címzésű, automatikus tűzjelző berendezéssel legyen ellátva. Tekintettel a klimatizálási igényekből fakadó jelentős légcsere igényre és az ebből származó viszonylag magas levegőáramlási sebességekre, kifejezetten ajánlott, hogy **a gépterem füst- és hősebesség érzékelőinek elhelyezése füstáramlás-mérésen alapuljon.** Célszerű a nagy értékű és kritikus informatikai eszközök belső terét aspirációs elven működő tűzjelző rendszerrel, sőt helyi, automatikus, rendszerint gázalapú automatikus tűzoltórendszerrel is védeni. **Az automatikus tűzoltórendszerek telepítése e géptermek tekintetében mindenképpen kockázatarányos megoldásnak tekinthető.** Ezen berendezések több megoldása is használatos. Számítógéptermi környezetben legelterjedtebbek jelenleg a gázzal oltó berendezések, de egyre terjednek a már égést nem támogató oxigénkoncentrációt fenntartó megoldások, illetve az un. nevezett vízköddel oltó berendezések, melyek nem keverendők össze, az un. sprinkler alapú berendezésekkel. Ez utóbbiak számítógépes környezetben kifejezetten kerülendők, tekintettel arra, hogy – szemben a gázos, illetve vízködös rendszerrel – működésük során az oltási kár kifejezetten magas, hiszen az oltóanyagként használt víz tönkreteheti az elektronikus eszközöket. Az automatikus oltórendszerek telepítésekor, különös figyelmet kell fordítani e

rendszerek vezérlésére, melyet össze kell hangolni a klimatizálást, és szünetmentes áramellátást biztosító épületgépészeti rendszerekkel, és a beléptető rendszer zárvezérléseivel, hiszen tűz esetén azonnal meg kell szüntetni a levegő-befúvást, az áramellátást az adott helyiségben, ugyanakkor biztosítani kell annak lehetőségét, hogy a veszélyeztetett személyzet minél előbb elhagyhassa a tűzeset közvetlen környezetét.

- **A légkondicionált, pormentes környezet ma már természetes követelmény** a pénzintézeteknél alacsonyabb rendelkezésre állási elvárást támasztó számítógéptermek esetében is. Légkondicionálás természetesen nem csak a stabil hőmérséklettartást jelenti, hanem a levegő páratartalmának megfelelő szinten tartását is, mely – az antisztatikus álpadló és álmennyezett, valamint az ilyen tulajdonságokkal rendelkező bútorzat mellett – **fontos szerepet kap a számítógépek antisztatikus védelme területén.** Különös figyelmet kell fordítani e géptermek tervezésekor ezek bővíthetőségére, ugyanis a serverkonszolidációs törekvések olyan technológia megoldásokkal támogatottak ma már (pl. blade serverekkel zsúfolt rack-ek), mely berendezések eddig soha nem látott hőemissziós tulajdonságokat mutatnak, így belátható idő belül **ezen eszközök közvetlen folyadékhűtése a rendkívül magas energiakoncentráció miatt nem lesz megkerülhető.** E géptermek működés közbeni hőtérképét minden jelentősebb hardware telepítés után célszerű elvégezni.

- A számítógéptermek befogadó környezetének függvényében szükség lehet a központi számítógépek megbízható működésének biztosítása érdekében **speciális rezgéscsillapító megoldások alkalmazására.** Egyszerűbb esetben ez a probléma speciális csillapítási tulajdonságokkal, rendelkező álpadlóval megoldható, de szükség lehet adott esetben olyan nagytömegű, rugózott és hangolható rezonancia-frekvenciájú csillapító megoldások alkalmazására,

melyek a viszonylag nagy amplitúdójú és szélesebb frekvenciatartományba eső káros rezgések hatékony csillapítására is képesek.

- **A pénzintézetek számítógéptermeinek biztonságát célszerű sugárzott és vezetett zavarvédelmi megoldásokkal is fokozni.** Ezek a műszaki-technikai megoldások azt hivatottak biztosítani, hogy az ily módon védett terekben elhelyezett központi számítógépeket ne érhessék az elektromos hálózat, az adathálózat oldaláról, illetve elektromágneses sugárzás révén olyan külső hatások (hálózati zavarokból, villámcsapás első és másodlagos hatásaiból, rádiófrekveciás jelforrásokból származó túlfeszültség vagy túláram), mely működésüket zavarná, a berendezéseket károsíthatná. E műszaki megoldás lényege, hogy a gépterem megfelelő rádiófrekvenciás csillapítást biztosító un. Faraday kalitkába kerül, melybe minden fémes vezetőt alkalmazó hálózat speciális szűrőkön kerül bevezetésre. Ebből következően az ilyen módon kialakított terek speciális megoldásokat igényelnek a fűtés, klimatizálás, világítás, elektromos és kommunikációs hálózatok, valamint a biztonsági berendezések telepítését és az elektromos földelési (mélyföldelés) rendszer kialakítását illetően is.

- Talán **a legalapvetőbb fizikai védelmi megoldás a központi géptermek számítógépeinek folyamatos és megbízható áramellátása.** E területen a független kettős betáplálás mellett, a pénzintézeti követelményekre tekintettel, szünetmentes tápegységekkel (UPS – Uninterruptible Power Supply) kell biztosítani az üzleti szempontból kritikus informatikai rendszerek működését egy esetleges áramkimaradás esetén. E területen a nehézséget az okozza, hogy az ily módon védendő rendszerek döntő többségénél a folyamatos üzem fenntartását kell biztosítani, tehát a szünetmentes tápegységek áthidalási időit viszonylag hosszú, tehát akár több órás áramkimaradásra kell méretezni, és nem lehet megelégedni olyan áthidalási idők biztosításával, melyek csak a rendszerek adatvesztés nélküli leállítására biztosítanának elegendő időt. Tovább

nehezíti a helyzetet és ezzel együtt jelentősen növeli a költségeket az a helyzet, hogy a szünetmentes tápegységek méretezésekor, tervezésekor figyelembe kell venni, e rendszereknek az **áramkimaradáskor táplálni kell a számítógépterem központi gépei mellett az adathálózat működéséhez elengedhetetlen aktív hálózati elemeket ugyanúgy, mint a gépterem hűtését biztosító nagyteljesítményű klímaberendezéseket és a biztonsági rendszer elemeit egyaránt.** Ehhez már csak azt kell hozzátenni, hogy nyilván gondoskodni kell a szünetmentes áramellátást biztosító rendszer tartalék háttér rendszeréről, melynek képesnek kell lennie maradéktalanul ellátni az elsődleges rendszer funkcióit. E komplex probléma megoldásának egyik lehetséges megoldása, hogy a szünetmentes áramellátás biztosításnak **első lépcsőjét néhány órás áthidalási időt biztosító on line üzemű akkumulátoros szünetmentes áramforrásokkal biztosítjuk, az ennél hosszabb idejű áramszüneteket pedig telepített vagy mobil Diesel-villamos gépcsoportokkal (Diesel aggregátor) oldjuk meg.** A fixen telepített megoldások többnyire automatikus vezérlésűek és az áramkimaradást követően általában 1 percen belül elindulnak és képesek a teljes terhelés átvételére. Az elindulásukhoz szükséges időt akkumulátoros UPS-ek hidalják át. A nagyteljesítményű és nagy-megbízhatóságú központi számítógépeket kivétel nélkül redundáns tápegységekkel gyártják. Ezen duál-tápegységek elektromos megtáplálását célszerű független áramforrásoktól (kétsínes elektromos hálózat) biztosítani.

Egy pénzintézet informatikai rendszer biztonsági menedzsmentjének kialakításakor a fenti követelményeken túl fontos, hogy a biztonsági rendszerben **egyszerűen legyen leképezhető és ellenőrizhető a pénzintézet biztonságpolitikájának megvalósítása.** A biztonsági menedzsmentnek legyen szerves része, illetve legyen szoros kapcsolata a hálózat, felhasználó, és szoftver

menedzsmenttel, szoftver disztribúcióval, tűzfal-mendzsmenttel, a levelező rendszer tartalomszűrésével, illetve a vírusvédelemmel.

Ma több jogszabály, egyebek között a hitelintézeti és tőkepiaci törvény és egy kormányrendelet, valamint MABISZ és PSZÁF ajánlás jelenti a bankok működésére vonatkozó, legfontosabb, személyi és tárgyi feltételeket előíró szabályozott környezetet. A móri események után kormánykezdeményezésre és a Pénzügyminisztérium koordinálásában kidolgozó munka indult egy egységes, magas szintű bankbiztonsági jogszabály kidolgozására. A munkában jelentős szerepet vállalt a Magyar Bankszövetség, illetve Bankbiztonsági Munkabizottsága. A kormányrendelet-tervezet tartalmában végül is megegyeztek az érintettek, egyebek között a PM, a BM, a IM, a PSZÁF, a Magyar Bankszövetség, a MABISZ, a SZVMSZK, a Takarékszövetkezetek és a Posta. Ez utóbbiakra a tervezet több éves moratóriumot léptetett volna életbe, a követelmények kötelező teljesítését illetően.

A tervezet a kormány Gazdasági Bizottsága elé került, ahonnan már nem jutott tovább. Az indoklásról a Magyar Bankszövetség a mai napig sem kapott hivatalos értesítést. Időről időre felbukkan az a legenda, miszerint a „banki lobby fúrta” meg a tervezetet. Ennek az állításnak azért több tény is ellentmond: egyrészt a kérdéses kormányrendelet- tervezet alapját mindenféle kényszer nélkül, a móri eseményeket évekkel megelőzve a „megfúrással” vádolt bankok bankbiztonsági szakemberei alkották meg, másrészt a nagy kereskedelmi bankok egy jelentős része már akkor is megfelelt a tervezetben foglalt követelményeknek. Mára ezeknek egy jelentős részét túl is teljesítik.

**Felhasznált irodalom:**

1. Bob Rosberg (Mosler Anti-Crime Bureau): Előadás az ORFK Bűnmegelőzési Osztályán (jelentés)

2. Christian Grandjean: Fegyveres támadások a svájci pénzintézetek ellen és a biztonsági intézkedések
3. "A pénzintézetek és ezek dolgozói ... sérelmére elkövetett rablások és betöréses lopások jellemzői, a felderítés tapasztalatai, javaslatok, ajánlások": Az ORFK Bűnmegelőzési Osztályának jelentése
4. "Pénzt vagy életet?!": Az ORFK Bűnmegelőzési Osztály kiadványa
5. Ted G. Lewis , Rudy Darken : Potholes and Detours in the Road to Critical Infrastructure Protection Policy. Homeland Security Affairs 1/2 2 2005 Article 1, 2005 www.comw.org/tct/fulltext/05lewis.pdf
6. Neumann, J. von, Morgenstern, O.: Theory of Games and Economic Behavior. Princeton University Press, Princeton, 1953.
7. Gadó János: Előadás az MTA 1999. évi közgyűlésén. Fizikai Szemle 1999/9. 322.o. http://www.kfki.hu/fszemle/archivum/fsz9909/gado.html