Bankbiztonság

Kiss Péter
Információbiztonsági szakértő, tanácsadó. Rendszeresen tart szervezett képzéseket információbiztonsági témában. Független szakértőként nagyvállalatoknál segít az ISO27001:2005 szabvány kialakításában, bevezetésében. Rendelkezik ITIL-F, Információbiztonsági auditori képesítéssel, ISACA tag. Szakmai tapasztalatát többek között az Állami Nyomda Nyrt.-nél, illetve a pénzügyi és banki szektorban szerezte.

Érdekes kifejezés. A legtöbb ember számára a bankbiztonság nem jelent mást, mint a bankfiókban található riasztórendszereket, rácsokat, nagy zárakat, fegyveres vagyonőröket és páncélszekrényeket.

Valójában a bankbiztonság sokkal összetettebb és bonyolultabb szakterület, mintsem a megfelelő zárak, riasztórendszerek és egyéb vagyonvédelmi berendezések „gyűjteménye". Itt is, mint egyéb más biztonsági területeken, csakis komplex, egyen-szilárd biztonsági rendszerek, intézkedések összességével érhető el egy-egy bank (pénzintézet) esetében a megfelelő biztonsági szint.

A szemléletesség kedvéért, hiába van egy pénzintézetnél (banknál) a világ legjobb és legkorszerűbb informatikai biztonsági rendszere, ha az adott bankba bárki ellenőrzés nélkül bejuthat, illetve ha a kritikus területek fizikai védelme nem megfelelő. Nyilvánvaló, hogy ilyen esetben az információt nem az informatikai rendszeren keresztül, komoly szakértelmet és erőfeszítést igénylő betöréssel fogja az elkövető megszerezni, hanem egyszerűen besétál, és elhozza a számára releváns információt adathordozón vagy dokumentum formájában. A helyzet fordítva is igaz, ha nem lehet fizikailag hozzáférni egy adott információhoz, de informatikai módszerekkel gyerekjáték megszerezni, akkor az informatikai rendszert fogják támadni.

Szerencsére és remélhetőleg a példában leírt körülmények nem jellemzők a pénzintézetekre. A megfelelő biztonság (bankbiztonság) kialakítására és működtetésére megfelelő garancia lehet a jogszabályi követelményeknek való megfelelési kényszer, illetve a különböző felügyeleti szervek folyamatos tevékenysége.

Sokkal jellemzőbb, és általános az a gyakorlat, hogy a biztonsági területeket külön-külön szervezeti egységekre bontják, ezért előfordulhat, hogy a párhuzamosságok, a nem egyértelmű hatás- és jogkörök, illetve a nem megfelelő belső kommunikáció miatt egy-egy esetben nem a kellő időben figyelnek fel az intő jelekre.

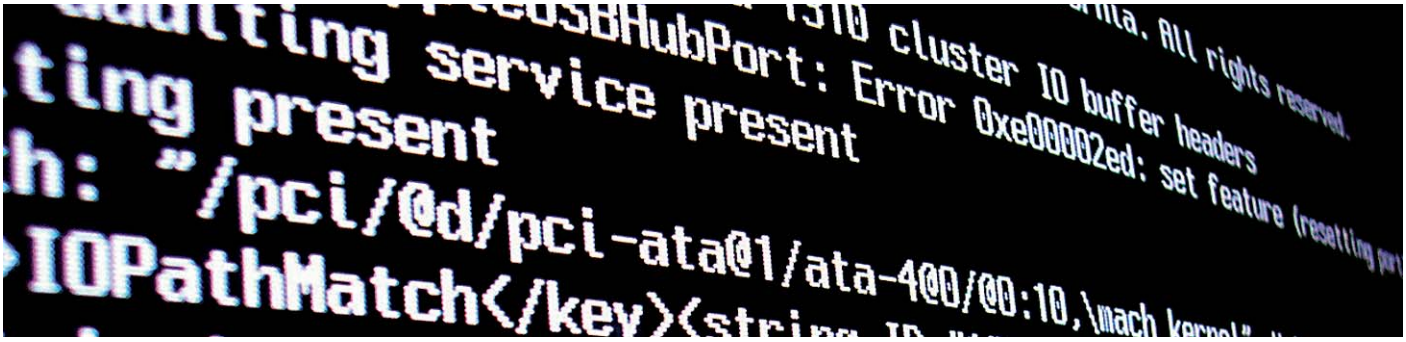
Biztonsági területek

A teljesség igénye nélkül tekintsük át a bankbiztonság fogalomkörébe tartozó biztonsági területeket: compliance tevékenység, fraud management, humánbiztonság, információbiztonság, IT biztonság, logikai biztonság, mind azok a területek, amelyek egy adott bank biztonságát hívatottak szolgálni.

Egy példa a bankbiztonsági tevékenység és az emberi erőforrás terület együttműködésére a humánbiztonsági feladatok kezelése során: ennek az együttműködésnek érdekessége, hogy a humánbiztonsági feladatok – speciális, bizalmi munkakörök esetén történő biztonsági szempontú ellenőrzések – legtöbbször nem az adott bank (pénzintézet) emberi erőforrás szervezeténél valósulnak meg, hanem a bankbiztonság munkatársai végzik el az ellenőrzést.

Egy másik példa – szakmai szempontból az egyik legérdekesebb - a bankbiztonsági tevékenység során kialakult együttműködésről az informatikai terület és a bankbiztonsági terület között: az egyik legáltalánosabb szervezeti megosztás, hogy a bankbiztonság, mint önálló szervezeti egység végzi a hagyományos vagyonvédelmi feladatokat, és egyéb biztonsági területekkel (informatikai biztonság, családkezelés stb.) – ideális esetben – szorosan együtt működik.

Szintén jellemző, hogy az informatikai biztonság az IT szervezeten belül valósul meg, ami viszont szakmailag kifogásolható, mivel a függetlenség alapkövetelmény a biztonsági munka kapcsán, ezért könnyen belátható, hogy az az informatikai biztonsági szervezet, amely az IT szervezetbe van integrálva, nem lehet független. Régebben, illetve történelmi okokból egy-egy informatikai rendszer esetében (sokszor egy egész gazdasági szervezetnél) a rendszergazda „élet-halál" ura volt. Aki jóban volt vele, mindent elérhetett az informatikai rendszeren vagy azt felhasználta (például internet), aki nem ápolt baráti viszonyt a rendszergazdával, az pedig azt használta, amit kapott. Mára ez a helyzet is megváltozott, az informatika kezd a helyére kerülni, és ez a hely, akár tetszik, akár nem, az adott gazdasági társaság üzemeltetési területe. Az informatika feladata a megfelelő szintű, folyamatos és stabil rendelkezésre állás biztosítása annak érdekében, hogy az adott bank, pénzintézet vagy gaz-



dálkodó szervezet megfelelő színvonalon, hatékonyan és nem utolsósorban a szektorra vonatkozó jogszabályi és nemzetközi elvárásoknak megfelelően nyújthassa szolgáltatásait az ügyfeleinek. Éppen ezért célszerű létrehozni egy információbiztonsági szervezetet, ahol egyéb feladatok mellett az IT terület független, megfelelő szakmai színvonalú biztonsági felügyelete is megoldható. Ugyanakkor érdekes megfigyelni, hogy az információbiztonsági feladatokat a mai napig gyakran az informatikai biztonság fogalmával azonosítják, pedig a két szakterület nem egy és ugyanaz. A biztonsági kérdések vitathatatlan módon az információbiztonsági terület hatáskörébe tartoznak, amikor is az információbiztonsági terület jogosult meghatározni, hogy a különböző informatikai rendszereknek milyen biztonsági szempontoknak kell megfelelniük, hogyan kell biztonságosan működniük és nem utolsósorban milyen biztonsági szabályozás vonatkozik a felhasználókra.

Adathalászat

Konkrét példán keresztül szeretném bemutatni, hogy a bankbiztonság miért és mennyiben több, mint a bevezetőben leírt vélekedés. Vélhetően sokan hallottak Önök közül az adathalász (phishing) támadásokról. Ezek a támadások informatikai rendszereken keresztül valósulnak meg, ahol is a támadó célja az, hogy hozzáférjen az áldozat (azaz a banki ügyfél) személyes adataihoz, majd a megszerzett adatok segítségével az áldozat bankszámlájáról (internetes bankolás), minél gyorsabban, minél több pénzt szerezzen meg.

Nézzük a folyamatot[1] röviden:

- A támadás során látszólag a támadott bank nevében, véletlenszerűen e-maileket küldenek szét a felhasználóknak. Ez az adathalász levél valamilyen ürüggyel arra próbálja meg rávenni a címzettet, hogy lépjen be az internetes banki rendszerébe, és ellenőrizze, hogy számlájával minden rendben van. A levél szövege minden esetben tartalmaz egy linket, amelyre kattintva az áldozat elérheti az internetes banki felületet. Anélkül, hogy teljes részletességgel kitárgyalnánk a csalás menetét, még annyit fontos megjegyezni, hogy a levélben megadott link a csalás kulcsa. Ugyanis a link nem az adott bank hivatalos internetes banki oldalára mutat, hanem a csalók által létrehozott ál-honlapra. A megnyitott hamis honlap megtévesztésig hasonlít az igazi banki honlapra, de nem teljesen egyformák. Mindig vannak eltérések. Amennyiben az áldozat lépre megy (márpedig a nagy számok statisztikájából kiindulva ezt a felhasználók egy része meg is teszi), és a hamis honlapon keresztül próbál meg belépni a számlájához, máris hibázott. A megadott azonosító adatai ugyanis nem fogják beléptetni a banki rendszerbe (hiszen egy hamis honlapon van), viszont a támadók abban a pillanatban megszerezték az áldozat belépéshez szükséges adatait.
- Az így megszerzett adatokkal a támadó belép az áldozat nevében az internetes banki rendszerbe, és az áldozat pénzét máris továbbutalja a saját számlájára.
- Az elutalt pénzt vagy a támadó saját maga vagy egy megbízott közvetítő veszi fel a bankfiókban és juttatja el támadóhoz.

A fenti példán keresztül is érzékelhető, hogy egy adathalász-támadás során legalább három különböző biztonsági terület érintett a fenyegetés megelőzésében, elhárításában. Érintett az informatika, akik a rendszert üzemeltetik, érintett az információbiztonság (informatikai rendszerek biztonsága) és érintett a csalásfelderítés (fraud). Az előbbi három területen túl érintett lehet egyéb más biztonsági terület, attól függően, hogy az adott bank biztonsági szervezete milyen rendszerben épül fel.

Amíg a csalás elektronikus csatornákon zajlik, elsősorban az informatikai biztonság és az információbiztonsági terület érintett. Attól a pillanattól kezdve, hogy a megszerzett adatokkal a támadó visszaél, és jogosulatlanul elutalja a pénzt, érintetté válik a csaláskezelés és esetleg a bankbiztonsági terület. És akkor még nem említettem a rendőrséget, hiszen megalapozott gyanú esetén a bank részéről általában feljelentést von maga után a cselekmény.

A bankbiztonsági terület a bankok azon belső szervezete, amely feladata biztosítani azt, hogy illetéktelenek a bank ügyfeleinek, a bank bizalmas információihoz, legyen szó akár banktitokról, értékpapírtitokról, üzleti titokról vagy személyes adatokról, illetéktelenül és/vagy jogosulatlanul ne férhessenek hozzá. Szintén a bankbiztonsági terület feladata biztosítani, hogy a bank vagyonvédelmi szempontjai maradéktalanul érvényesüljenek a bank területén, illetve a különböző visszaélések (csalás, lopás, hamísítás, bennfentes kereskedelem stb.) megelőzése és felderítése. Remélem, a cikk elolvasása után egyetért velem az Olvasó, hogy a bankbiztonság – függetlenül attól, hogy több különböző elnevezésű szervezeti egység tevékenykedik a szakterületen – sokkal több és összetettebb tevékenységet takar annál, mint amit a bevezetőben írtam. Ahhoz, hogy egy bank bankbiztonsági tevékenysége megfeleljen a banki és a hazai jogszabályi elvárásoknak, a tevékenységben részt vevő valamennyi szervezeti egység között megfelelő belső kommunikációt és együttműködést kell kialakítani.

Ne feledjük, hogy minden biztonsági rendszer csak annyira erős, mint az adott biztonsági rendszer leggyengébb eleme!

[1] A leírás a példa kedvéért leegyszerűsített, és elsősorban a cikk témáját képező biztonsági területek közötti együttműködés fontosságát hívatott támogatni.