HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Cser Orsolya

PÉNZÜGYI BIZTONSÁG ÉS KIBERBIZTONSÁG A BANKI RENDSZEREK TERÜLETÉN

Absztrakt

A biztonság az egyik legalapvetőbb emberi szükséglet, amely sohasem önmagában, hanem mindig a veszélyhelyzetre történő reagálásként jelenik meg. Egy állam belső biztonságát jelenti a politikai, társadalmi, gazdasági rend megóvása, a veszélyek elhárítása, mint például a gazdasági terrorizmus eszköze, a kibertámadás. A modern hadviselés egyik legfontosabb színtere a kibertér. Ennek támadása a banki rendszerek esetében fontossá tette azt, hogy az informatikai rendszerek a lehető leginkább biztonságos módon kerüljenek kialakításra a szervezeten kívül és belül. A pénzügyi szolgáltatási tevékenység csak a működési kockázatok csökkentését szolgáló információs és ellenőrzési rendszer, valamint a rendkívüli helyzetek kezelésére vonatkozó terv megléte esetén kezdhető meg, illetve folytatható. Ennek érdekében a jövőre vonatkozóan érdemes kidolgozni egy olyan gyakorlati szabályozást – a többféle területen használt Legjobb Gyakorlatok (Best Practises) módszerével -, amely által a pénzügyi szervek (bankszektor) összehangoltan és azonnali reagálással képesek fellépni az őket ért támadások ellen.

Security is one of the most basic human needs, which is never alone, but always in the emergency response as shown. Internal security of a state is the political, social and economic order to preserve or eliminate hazards, such as instrument of economic terrorism, cyber attack. Cyberspace is a major arena of modern warfare. This attack has made it important for the banking system, the IT systems in the most secure manner are developed inside and outside the organization. Financial service activities must be initiated in the event of an intention to information and control systems to reduce operational risks and to manage emergency situations or continued. To this end, you may want to develop a practical scheme for the future - in a number of ways for Best Practices (Best Practises) method - which is coordinated by the financial authorities (banking) and are capable of immediate response to counteract the attacks against them.

Kulcsszavak: *kibertámadás, informatikai rendszer, elektronikus szolgáltatás, bankbiztonság ~ cyber attack, IT system, electronic service, bank security*

A BIZTONSÁG ÉS A KRITIKUS INFRASTRUKTÚRÁK

A biztonság [1] az egyik legalapvetőbb emberi szükséglet, amely sohasem önmagában, hanem mindig a veszélyhelyzetre történő reagálásként jelenik meg. Egy állam belső biztonsága [2] a politikai, társadalmi és a gazdasági rend megóvását, a veszélyek elhárítását jelenti. Kérdéskörébe tartozik a gazdasági terrorizmus egyik eszköze, a kibertámadás elleni védelem is. Ez utóbbi veszélyhelyzet fontos kérdés, mivel annak célja a pénzügyi válságok kezelése, az ezzel kapcsolatos banki feladatok.

A biztonság alapfeltétele a gazdaság zavartalan működése és a fejlődés feltételeinek biztosítottsága, melynek gazdasági szempontjai:

- gazdasági stabilitás biztosítottsága: hatékony gazdasági szerkezet, biztonságos külgazdasági kapcsolatok, szabad verseny;
- stabil pénzügyi feltételek megteremtése: mérsékelt infláció, rendezhető adósság és hitelállomány, ösztönző kamatrendszer.

A pénzügyi válságok témakörének és azok kezelésének szorosan kapcsolódó területe a pénzintézeteknél történő értékmegőrzés. A védelem- és hadigazdaságtan fogalmi rendszere, szemléletmódja alkalmazható egy látszólag távoli területen, mint a bankszféra, amely értékeink védelmében tevékenykedik.

A banki biztonság kiemelt jelentőségű, hiszen egy bankrendszert adott esetben kibertámadás érhet. Így szükségszerű, hogy a bankok tekintetében a megfelelően biztonságos környezet biztosítva legyen, ezért a biztonságot be kell építeni az információs rendszerekbe. A rendkívüli események bekövetkezésének okai lehetnek szándékos vagy óvatlan magatartás, mint pl. egy információs rendszereket érő kibertámadás, illetve váratlan események összessége, mint például egy természeti csapás. Az adott magatartás, esemény következtében az élet és vagyonbiztonság súlyos veszélybe kerül, amely akadályozza, vagy megbénítja a bank normális működését. A rendkívüli események megelőzése, megakadályozása, a keletkezett hátrány mértékének csökkentése érdekében a helyi katonai és rendőri szervekkel szoros együttműködést kell kialakítani.

A modern társadalmak nagymértékben függenek a különböző infrastruktúráktól (energiaellátás, ivóvíz ellátás, informatikai és banki hálózatok stb.), amelyek komplex rendszerét is egymástól való függőségek jellemzik. E rendszerek működési zavarai, illetve egyes elemeinek ideiglenes kiesése, vagy megsemmisülése jelentős kihatással vannak mindennapi életünkre, a gazdaság és a kormányzat hatékony működésére. Az állam, a gazdaság szereplői, valamint a lakosság részéről elvárás, hogy ezen alapvető létfontosságú, vagy kritikus infrastruktúrák lehető legnagyobb biztonsággal [3] működjenek.

A kritikus infrastruktúra elemek terrorcselekményekkel, természeti katasztrófákkal és balesetekkel szembeni védelme érdekében fontos, hogy az infrastruktúrák működésének megzavarása vagy manipulálása megelőzhető, kivédhető, illetve lehetséges mértékben rövid, kivételes és kezelhető legyen.

A kritikus, vagy létfontosságú infrastruktúrák [4] az általános definíció szerint "létesítmény vagy rendszer olyan rendszereleme, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához –, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt következményekkel járna."

Ezen infrastruktúrák részben az állam, részben a magánszféra tulajdonában vannak, illetve azokat az állam vagy a magánszféra működteti.

A létfontosságú infrastruktúrákat kár érheti, működésükben zavar keletkezhet vagy azok meg is semmisülhetnek terrorcselekmény, természeti katasztrófa, hanyagság, baleset, számítógépes hackertevékenység, bűncselekmény vagy rosszhiszemű magatartás

következtében. Az infrastruktúrák biztonságának növelése ezért elsőrendű kérdéssé vált a fejlett országok biztonságpolitikájában.

Az infrastruktúrák biztonságnövelésének fő területei, az egyének, közösségek védelmének és a kritikus infrastruktúrák biztonságának magasabb szintre emelése. Mindhárom területen a veszélyek és fenyegetettségek fizikai, informatikai eredetűek vagy a rendszerek komplexitásból adódnak.

A megoldást az új fenyegetettségek és kockázatok fizikai, informatikai és pszichológiai szintű okainak felderítése, összefüggéseik megértése és kezelése jelenti.

Összességében a Kritikus Infrastruktúrák (KI) [5]:

- azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotó részei;
- amelyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése;
- közvetlenül vagy közvetetten, átmenetileg vagy hosszútávon súlyos hatást gyakorolhat;
- az állampolgárok gazdasági, szociális jólétére, a közegészségre, közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére.

A létfontosságú infrastruktúrák *több gazdasági ágazatra kiterjednek*, többek között a bankügyletekre és pénzügyekre, a szállításra és forgalmazásra, az energiaiparra, a közművekre, az egészségügyre, az élelmiszerellátásra és tájékoztatásra, valamint a kulcsfontosságú állami szolgáltatásokra. Ezen ágazatok néhány létfontosságú eleme nem tartozik a szigorúan vett „infrastruktúra" fogalmába, de valójában olyan hálózatok vagy ellátási láncok, amelyek valamely alapvető termék vagy szolgáltatás biztosítását támogatják.

A létfontosságú infrastruktúrákat fenyegető katasztrofális *terrortámadások lehetősége egyre nő*. A létfontosságú infrastruktúrák ipari ellenőrző rendszerei elleni támadás következményei rendkívül eltérőek lehetnek.

Az infrastruktúrák katasztrofális meghibásodásának egyik típusa, amikor az infrastruktúra egy részének meghibásodása a többi meghibásodásához vezet, ami *dominóhatást* válthat ki. Ilyen meghibásodás az infrastrukturális ágazatok egymásra gyakorolt szinergikus hatása következtében alakulhat ki. Ennek egy egyszerű példája lehet a villamosenergia-szolgáltató közüzemek elleni támadás, ahol megszakad a villamosenergia-szolgáltatás, és ezáltal más elektromos készülékek – így a banki rendszerek is - leállhatnak. Az egymást követő események láncolata szintén nagy károkat okozhat, és a közüzemeken keresztül is a bank-, pénzügyi rendszerek leállását idézheti elő.

A KIBERTÉR

A modern hadviselés egyik legfontosabb színtere a kibertér [6], amely egy olyan tartomány, ahol hálózatos rendszerekben működő elektronikai eszközöket és az elektromágneses spektrumot használják fel az adatok tárolására, cseréjére és módosítására, kiterjesztve azon hálózatokra is, melyek elemei nem rádiócsatornán, hanem vezetéken (rézvezeték, optikai kábel stb.) vannak egymáshoz kapcsolva.

A kibervédelem ennek alapján arra irányul, hogy fenntartsa a saját hálózatos információs rendszereinkben a hozzáférhetőséget az információkhoz, információalapú folyamatokhoz, és biztosítsa ezen rendszerek hatékony használatát békeidőben, válság vagy konfliktus idején egyaránt.

A kiberhadviselés [7] az információs dimenzióban megvalósuló hálózati hadviselést jelenti. Leegyszerűsítve a kritikus információs infrastruktúrák bizalmasságának, sértetlenségének és rendelkezésre állásának befolyásolására irányuló tevékenység informatikai, fizikai és emberi eszközökkel.

A kibertámadás észlelésének igénye szoros együttműködést és összehangolt cselekvést kíván az információs rendszerek tervezői, gyártói, forgalmazói, adminisztrátorai, felhasználói, valamint a szolgáltatásokat biztosító, jogalkotó és hírszerző szervezetek között. Az információs rendszereket támadók műveleti sebessége meghaladhatja a humánmegoldásokat tartalmazó észlelési és válaszadási képességeket. A hatékony kibervédelem érdekében elsődleges fontosságú automatizált módszerekkel felbecsülni az esemény súlyosságát (a rendszer sérülése, kompromittálódás, rosszindulatú program bejutása a rendszerbe) és csökkenteni azok negatív hatásait.

A helyreállítás megkezdéséhez és a szükséges válaszlépések megtételéhez a támadások időbeni felderítése alapvető feltétel.

Általánosan elfogadott, hogy egy sikeres kibertámadás legrosszabb esetben is csupán kevés sérüléssel járna, de a létfontosságú infrastrukturális szolgáltatások szempontjából veszteséget eredményezhet. Például a banki hálózat elleni sikeres kibertámadás miatt az ügyfelek nélkülöznék a banki szolgáltatásokat mindaddig, míg a szakemberek elvégzik a hálózat helyreállítását és javítását.

A kibertér támadása – informatikai vagy más módon – a bankok esetében fontossá tette azt, hogy az informatikai rendszerek a lehető leginkább biztonságos módon kerüljenek kifejlesztésre a szervezeten kívül és belül. A pénzügyi rendszerek kiemelt szerepet töltenek be, hiszen ezek megfelelő működése nélkül a pénzügyi folyamatok egy része vagy egésze működésképtelenné, de legalábbis jelentősen akadályozottá válik.

INFORMÁCIÓS HADVISELÉS [8]

Napjaink új típusú társadalmában a különféle információs tevékenységek az un. információs környezetben, vagy más néven az információs színtéren zajlanak. Ennek következtében a katonai műveletek működési területei és tartományai tovább bővültek, kiegészültek az információs hadszíntérrel.

Az információs hadviselés során alkalmazható fenyegetések négy kategóriára [9] bonthatók: "kompromittálás, megtévesztés, szolgáltatás akadályozása/megszakítása, fizikai megsemmisítés. Mind a négy kategória kockázatot jelent azokra az önálló, vagy hálózatba szervezett fegyverekre és támogató rendszerekre (banki rendszerek), amelyek nagymértékben támaszkodnak információs rendszerekre. A fenyegetés származhat szervezett erőktől (államok) vagy strukturálatlan ellenfelektől (hacker)."

A kompromittálásnak többféle formája [10] lehet, így például a technológia illetéktelen megszerzése vagy szoftverhiba, a rendszerbe történő illetéktelen behatolás, rosszindulatú szoftver használata, felderítő szervezet adatgyűjtése vagy egy pszichológiai művelet.

Ahhoz, hogy az automatizált információs rendszereket megvédjük, első lépésben meg kell érteni az ellenük irányuló fenyegetéseket, mint pl. az adatok és információk kompromittálása, a szolgáltatások részleges vagy teljes akadályozása, rongálása. Ennek legjobb eszköze a képzés és a szoros együttműködés az operátorok és a felhasználók között.

Az előzetes vizsgálatként össze kell gyűjteni a minimális információkat, jelezni kell a várható fegyelmi lépéseket, javaslatot tenni a további vizsgálatra. A kompromittálás utáni veszteségek felbecsülését egy központilag irányított rendszernek kell végeznie, mely egy központi adatbázisból és célirányosan kialakított programokból és projektekből áll.

Az információs rendszerek biztonsági monitorozása a saját hivatalos távközlés lehallgatása, olvasása, másolása vagy rögzítése, amelynek célja anyagot biztosítani az analízishez, amely lehetővé teszi az automatizált banki információs rendszerek biztonsági fokának pontos megállapítását. Ebben az információs környezetben az információs műveletek [11] a fizikai-, az információs- és a tudati dimenzióban érvényesülő, koordinált tevékenységet jelentik, amelyek a szembenálló fél információira, információalapú folyamataira és infokommunikációs

rendszereire gyakorolt hatásokkal képesek befolyásolni az ellenfelet. Az információs műveletek célja az információs fölény, uralom és végül a vezetési fölény kivívása.

Az információs műveletek elsődleges fenyegetései: kompromittálás, adatsérülés vagy információs művelet megszakadása. A biztonsági problémák esetében a megelőzés, a gyors reagálás és a károk csökkentése tekinthető kiemelt feladatnak. E feladatok mindegyikénél egyre nagyobb súllyal jelentkezik a számítástechnikai megoldások elterjedt használata.

A különböző szempontok szerinti megfogalmazások sokszínűsége bizonyítja az információs műveletek védelme érdekében a széles körű együttműködés szükségességét, a kockázathoz kötött védelmi feladatokat és a minden részletre kiterjedő képzést.

A PÉNZÜGYI ÉS BANKRENDSZEREK

A pénzügyi rendszerek [12] működésében – mint az élet más területein is - egyre hangsúlyosabb szerep jut az elektronikus szolgáltatásoknak, melyek a gyorsabb és költségtakarékosabb kiszolgálást jelentik a bankok részéről. Törvényileg, központosítva, jogszabályok által kívánják a banki szolgáltatások biztonságát garantálni, azonban meglátásom szerint az információbiztonság tekintetében jelenleg nincs olyan egységes szabályozás, amely a szolgáltatások bizalmasságának, sértetlenségének és rendelkezésre állásának követelményeit meghatározzák. Ugyan tökéletes védelmet nyújtani talán lehetetlen, de mégis törekedni kell rá, hogy a szükséges biztonságos környezet kifejlesztésre kerüljön.

Ezáltal a biztonsági gondolkodásnak [13] az új alkalmazások, rendszerek kialakításánál, tervezésénél meg kell jelennie ahhoz, hogy a pénzügyi rendszerek kiberterébe a lehető legkevesebb veszélyforrás juthasson be. Elsődleges szempont a biztonságos fizikai környezet kialakítása és a további biztonsági követelmények megállapítása.

Célszerű a bankrendszerek területén olyan szabályozások általi megoldások létrehozása, amelyek felhasználásával a banki szolgáltatások biztonsági szintje jelentősen növelhető, valamint a felmerülő pénzügyi, gazdasági, nemzetbiztonsági kockázatok nagymértékben csökkenthetők. A pénzügyi rendszer biztonságát folyamatosan fenyegetések érik, mint például a katasztrófa és háborús helyzetek, valamint a csalók és rablók tevékenységei. Ezen problémák ellen kell felkészíteni a felsőszintű igazgatást, és azután együttesen fellépni a fenyegetettség megszűntetése és a biztonságos körülmények visszaállítása céljából.

A kibertér ma Magyarországon a legtöbb fejlett infrastruktúrával rendelkező országhoz hasonlóan védtelennek tekinthető. Bár az informatikai rendszerek támadásával emberéletekben nem vagy csekély kár eshet (közvetett hatásként), de a gazdasági, és ennek következményeként a politikai károk felbecsülhetetlenek.

Észtország kritikus információs infrastruktúráit [14] 2007. április 27-én külső, elosztott túlterheléses (Distributed Denial of Service – DDoS) támadás érte, amelyet tömeges levélküldés (spammelés) és weboldalak megváltoztatása (deface) egészített ki. A főbb célpontok az észt parlament számítógépei, valamint a *bankok,* minisztériumok, napilapok és elektronikus hírközlő szervezetek voltak. A támadás mind Észtországot, mind pedig a NATO-t felkészületlenül érte, pedig kivitelezéséhez csekély erőforrásokra volt szükség.

Magyarországon [15] egyelőre nem került napvilágra olyan incidens, mely külső támadás eredménye lett volna, de 2009-ben több olyan informatikai hiba is bekövetkezett, amely az adott kritikus információs infrastruktúra működését megakasztotta. Ez emberek tíz- és százezreinek okozott nehézséget, a sajtó kiemelten foglalkozott velük és jelentős presztízsveszteséget jelentett az üzemeltető intézménynek.

Magyarországnak is van tehát keserű tapasztalata az IT rendszerek leállásának következményeivel kapcsolatban, de a direkt, összehangolt támadások hatása egyelőre elképzelhetetlen. A bankügyi tranzakciók működésében hazánkban is egyre hangsúlyosabb szerep jut az elektronikus szolgáltatásoknak. Ezen szolgáltatások biztonságos működése

nemzetbiztonsági szempontból kritikus kérdés, hiszen ezek nélkül az ország gazdasági és pénzügyi működése jelentős akadályokba ütközne.

A szolgáltatások biztonságát a jogalkotók jogszabályokkal próbálják garantálni, azonban bizonyos területeken jelenleg nincsenek olyan egységes műszaki ajánlások, melyek a szolgáltatások bizalmasságának, sértetlenségének és rendelkezésre állásának követelményeit meghatároznák. A nemzetközi trendek és a hazai tapasztalatok is azt mutatják, hogy az elektronikus banki szolgáltatások állandó célpontjai a szervezett bűnözésnek, a hackereknek és más államok hivatalos szerveinek.

Tökéletes védelmet nyújtani aránytalanul magas költséget jelentene, azonban az elvárható gondosság elve alapján szükséges a nyilvánosan elérhető szolgáltatásokat biztonságosan kifejleszteni. Ez azt jelenti, hogy a biztonsági gondolkodásnak már az új alkalmazások tervezésénél meg kell jelennie. A banki szolgáltatásokba biztonsági megoldásokat fejleszteni több szinten lehet.

A bankok biztonsági szintje jelentősen növelhető, és így a felmerült nemzetbiztonsági kockázatok nagymértékben csökkenthetők. A legjobb gyakorlatok (best practice, azaz széles körű tapasztalaton alapuló, több szervezetnél is sikeresen bevált gyakorlat) felhasználásával és továbbfejlesztésével, valamint az elektronikus banki ügyletek védelmi igényeihez történő hozzáigazításával lehet elérni.

A PÉNZÜGYI REÁLFOLYAMATOK BIZTONSÁGA

A tapasztalatok a közös katonai-civil [16] együttműködésről az alábbiak:

- A makrogazdasági körforgásnak folyamatosan kell működnie ahhoz, hogy a pénzellátás, és a reálfolyamatok (termelés) folytonossága biztosítva legyen.
- A pénzügyi rendszer biztonságát folyamatosan fenyegetések érik, mint például a katasztrófa és háborús helyzetek, valamint a csalók és rablók tevékenységei.
- Ezen problémák ellen kell felkészíteni a felsőszintű igazgatást (CMX gyakorlatok), és azután együttesen fellépni a fenyegetettség megszűntetése és a biztonságos körülmények visszaállítása céljából.
- A modern aszimmetrikus hadviselésbe főszerepben a terrorizmus és kiberbiztonság van, mint napjaink kiemelt biztonsági feladatai.
- Elterjedőben vannak a potenciális támadások kritikus infrastruktúrák ellen, (ebben az esetben a bankszektor).
- A bankok tekintetében biztosítani kell a megfelelően biztonságos környezetet, a biztonságot be kell építeni az információs rendszerekbe.

A bankbiztonsági tevékenység mindazon tervezési, szervezési, irányítási, végrehajtási és ellenőrzési feltételekről való intézményes gondolkodás, amely a pénzintézet saját tulajdonú tárgyainak, értékeinek, valamint az alkalmazottak és az ügyfelek biztonságának védelmét szolgálja.

A Nemzeti Biztonsági Stratégia [17] (NBS) célja, hogy iránymutatást nyújtson a kormányzati szektor számára biztonságpolitikai – azon belül pénzügyi - kérdésekben. Filozófiájában ezért átfogó és összkormányzati megközelítést követ. Az ország biztonsága azonban mindenekelőtt közügy, ezért a stratégia egyik feladata, hogy a szakmai körökön túl a mindennapi életben is hasznosítható támpontot nyújtson a hazai biztonságpolitikai gondolkodásban.

Az NBS-ben szerepelnek azon biztonsági elemek is, melyek egy pénzügyi krízis esetében – mint például kibertámadás az ország bankrendszere ellen – fontos szempontok annak érdekében, hogy a veszélyhelyzetet megszűntessék.

Megfogalmazásra kerültek mindazon tényezők, melyek a pénzügyi biztonságot meghatározzák az egyes nemzetállamok gazdaságának működése tekintetében:

- pénzellátás – bankválság esetén a készpénzellátás korlátozása;
- azonnali betét kivétel pánik – pl. Postabank-botrány (1997. február);
- pénzügyi tartalék – a krízishelyzetek esetére;
- pénzügyi moratórium – pénzintézetekből történő pénzkivétel korlátozása.

A NBS 30. pontja a pénzügyi biztonságról szól, iránymutatást nyújt a kormányzati szektor számára egy pénzügyi krízis (pl. a kibertámadás) problémáinak kezeléséről és megszűntetéséről.

A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI törvény 2. számú mellékletében a nemzeti létfontosságú rendszerelemek kijelölése alapján a pénzügy is egy kritikus infrastruktúra ágazatnak tekintendő [18]:

	A	B
	Ágazat	Alágazat
17	pénzügy	pénzügyi eszközök kereskedelmi, fizetési, valamint klíring- és elszámolási infrastruktúrái és rendszerei
18		bank- és hitelintézeti biztonság
19		készpénzellátás

A NATO CMX GYAKORLATA – 2012. NOVEMBER [19]

Kritikus infrastruktúráink sérülékenyek és támadhatók. A szakemberek nem látnak olyan határozott lépéseket, amelyek ezen hálózatok – mint például a banki és pénzügyi számítógépes hálózatok – megfelelő, komplex védelmét erősítenék. Mindez azt jelenti, hogy a kritikus infrastruktúrák rendkívül sebezhetőek.

A fejlett hadi- és informatikai kultúrával rendelkező országok a 21. század elejének egyik legkomolyabb kihívásaként kezelik a kritikus információs infrastruktúrák védelmét. Magyarországon mindeddig nem készült olyan tanulmány, amely számításba venné, hogy milyen láncreakciót válthat ki egy kritikus információs rendszereket érintő átfogó, informatikai támadásokat is magába foglaló cselekménysorozat, mint például a bankrendszerünk ellen történő kibertámadás - ahogyan azt 2012 novemberében a CMX 2012 gyakorlatban szimulálták.

Egy, az információs infrastruktúrákat célzó támadás akár napokig tartó működési zavarokat okozhat az országban. A NATO 2012. évi CMX válságkezelő és egyben kibervédelmi (támadás érte a bankrendszert) gyakorlatának fő célja a jelen kor kihívásai elleni egységes fellépéshez szükséges döntések konszenzusos meghozatala volt:

- NATO-szerződés 5. cikkelyének érvényesítése – a tagországok közösen léptek fel a támadás elhárításáért és a rendszerek helyreállításáért;
- A hazai válságkezelési rendszer döntés-előkészítő és döntéshozatali folyamatainak, valamint a NATO-központtal és a tagországokkal való együttműködés gyakorlása;
- A Gyakorlathoz a 2007-es, Észtország elleni kibertámadást vették mintául (ma már nincsen „valódi” háború kibertámadások nélkül).

A szakemberek felhívták a figyelmet, hogy az ilyen típusú támadásoknál elsősorban a megelőzésre kell törekedni, mivel a más szervezetek által előre tervezett és célzott támadásra szinte lehetetlen felkészülni.

BANKBIZTONSÁGI TEVÉKENYSÉG

Egy bankrendszer [20] tekintetében a legfontosabb kritériumok:

1. A pénzügyi szolgáltatási tevékenység csak a működési kockázatok csökkentését szolgáló információs és ellenőrzési rendszer, valamint a rendkívüli helyzetek kezelésére vonatkozó terv megléte esetén kezdhető meg.
2. A pénzügyi intézménynek ki kell alakítania a pénzügyi, kiegészítő pénzügyi szolgáltatási tevékenységének ellátásához használt informatikai rendszer biztonságával kapcsolatos szabályozási rendszerét és gondoskodnia kell az informatikai rendszer kockázatokkal arányos védelméről.
3. A szabályozási rendszerben ki kell térni az információtechnológiával szemben támasztott követelményekre, a használatából adódó biztonsági kockázatok felmérésére és kezelésére a tervezés, a beszerzés, az üzemeltetés és az ellenőrzés területén.
4. A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell legalább az informatikai biztonsági rendszer önvédelmét, kritikus elemei védelmének zártságát és teljeskörűségét biztosító ellenőrzésekről, eljárásokról, valamint olyan biztonsági környezetről, amely az informatikai rendszer működése szempontjából kritikus folyamatok eseményeit naplózza, és alkalmas e naplózás rendszeres (esetleg önműködő) és érdemi értékelésére, illetve lehetőséget nyújt a nem rendszeres események kezelésére.
5. A pénzügyi intézménynek [21] tevékenysége ellátásához, nyilvántartásai naprakész és biztonságos vezetéséhez meg kell valósítania a biztonsági kockázatelemzés alapján indokolt védelmi intézkedéseket és rendelkeznie kell legalább a következőkkel:
    a) a szolgáltatások ellátásához szükséges informatikai rendszerrel, valamint a szolgáltatások folytonosságát biztosító tartalék berendezésekkel, illetve e berendezések hiányában az ezeket helyettesítő egyéb - a tevékenységek, illetve szolgáltatások folytonosságát biztosító – megoldásokkal;
    b) az informatikai rendszer szoftver elemeiről (alkalmazások, adatok, operációs rendszer és környezetük) olyan biztonsági mentésekkel és mentési renddel (mentések típusa, módja, visszatöltési és helyreállítási tesztek, eljárási rend), amelyek az adott rendszer helyreállíthatóságát a rendszer által nyújtott szolgáltatás kritikus helyreállítási idején belül lehetővé teszik. Ezen mentéseket kockázati szempontból elkülönítetten és tűzbiztos módon kell tárolni, valamint gondoskodni kell a mentések forrásrendszerrel azonos szintű hozzáférés védelméről;
    c) a szolgáltatásai folyamatosságát akadályozó rendkívüli események kezelésére szolgáló tervvel.

A rendkívüli helyzetek kezelésének módjára az alábbiak fogalmazhatóak meg:

1. A pénzintézetnek a mérete, az általa végzett pénzügyi, kiegészítő pénzügyi szolgáltatási tevékenysége jellege, nagyságrendje, összetettsége arányában megbízható irányítási rendszerrel kell rendelkeznie, és ennek keretén belül köteles a felmerülő kockázatok azonosítására, mérésére, kezelésére, nyomon követésére és jelentésére szolgáló hatékony eljárásokat alkalmazni.
2. Emellett írásban rögzített eljárásrendekkel, szabályzatokkal kell rendelkeznie a működési kockázatok mérésére, kezelésére, valamint vészhelyzeti és üzletmenet-folytonossági tervvel a folyamatos működés fenntartása, továbbá a súlyos üzletviteli fennakadásokból következő esetleges veszteségek mérséklése érdekében.

A Magyar Nemzeti Bank (MNB) alapfeladata a fizetési és elszámolási rendszerek felvigyázása, e rendszerek biztonságos és hatékony működése, továbbá a pénzforgalom zavartalan lebonyolítása érdekében. A 2012. július 14. napjától az MNB [22] alapvető és egyéb feladatai az alábbiakban foglalható össze:

- Az MNB más felelős hatóságokkal együttműködve feltárja a pénzügyi közvetítőrendszer egészét fenyegető üzleti és gazdasági kockázatokat, elősegíti a rendszerszintű kockázatok kialakulásának megelőzését, valamint a már kialakult rendszerszintű kockázatok csökkentését vagy megszüntetését.
- Feltárja a pénzügyi közvetítőrendszer egészét fenyegető üzleti és gazdasági kockázatokat, elősegíti a rendszerszintű kockázatok kialakulásának megelőzését, valamint a már kialakult rendszerszintű kockázatok csökkentését vagy megszüntetését.
- Az MNB elnöke a rendszerszintű kockázatok felépülésének megakadályozása vagy a kockázatok csökkentése érdekében rendeletet adhat ki.
- Amennyiben olyan körülmény áll fenn, amely miatt a hitelintézet működése a pénzügyi rendszer stabilitását veszélyezteti, az MNB a hitelintézetnek rendkívüli hitelt nyújthat.
- Az MNB sürgős, rendkívüli, a pénzügyi rendszer egészének stabilitását és a pénzforgalom zavartalanságát veszélyeztető esetben hitelt nyújthat, amelynek lejárata legfeljebb három hónap lehet.

A Magyar Nemzeti Bank elnöke rendeletben szabályozza, hogy a rendszerkockázatok felépülésének megakadályozása vagy a kockázatok csökkentése érdekében szükséges intézkedéseket: a túlzott hitelkiáramlást megakadályozó előírásokat, a rendszerszintű likviditási kockázatok felépülését megakadályozó likviditási követelményeket, felépítésének és működésének feltételeit, a rendszerszinten jelentős intézmények csődvalószínűségét csökkentő többletkövetelményeket.

Mindezen – egyebekben üzleti titkot képező – eljárások, szabályzatok, intézkedési tervek megfelelőségét a Pénzügyi Szervezetek Állami Felügyelete (PSZÁF) köteles ellenőrizni. A jogalkotó 2013. szeptember 16.-ai döntésével 2013. október 1.-jei hatállyal összevonta a PSZÁF-ot az MNB-vel [23]. Ennek alapján az MNB új szervezetében már megjelennek a pénzügyi biztonság eléréséhez javasolt feladatok.

Megállapítható, hogy az NGM csak a szabályozás elméleti oldaláról érintett, a gyakorlati tennivalók tekintetében MNB (magába foglalva a PSZÁF-ot), esetleg a Magyar Államkincstár (MÁK) bizonyul illetékes szervnek.

KÖVETKEZTETÉSEK

A pénzügyi szolgáltatási tevékenység végzéséhez szükséges egy a működési kockázatok csökkenését szolgáló információs és ellenőrzési rendszer, valamint a rendkívüli helyzetek kezelésére vonatkozó intézkedési terv.

A biztonsági kockázatelemzés eredményei alapján gondoskodni kell az informatikai biztonsági rendszer önvédelmét, kritikus elemei védelmének zártságát és teljeskörűségét biztosító ellenőrzésekről, eljárásokról, valamint a rendszeres biztonsági mentésről és a kritikus folyamatok eseményeit naplózó biztonsági környezetről.

A rendkívüli helyzetek kezelésének eljárásait, szabályzatait, intézkedési terveik megfelelősségét a PSZÁF köteles ellenőrizni, ezért célszerű a bevonása.

Az MNB alapfeladata a fizetési és elszámolási rendszerek felvigyázása, azok biztonságos és hatékony működése, a pénzforgalom zavartalan lebonyolítása érdekében.
Összességében az NGM csak a szabályozás elméleti oldaláról érintett, a gyakorlati tennivalók érdekében a PSZÁF, az MNB és a MÁK az illetékes szervek.

Mindezek érdekében a jövőre vonatkozóan érdemes kidolgozni egy olyan gyakorlati szabályozást – a többféle területen használt Legjobb Gyakorlatok (Best Practises) módszerével –, amely által az állami és pénzügyi (bankszektor) szervek összehangoltan, azonnali reagálással képesek fellépni az őket ért támadások ellen.

Kulcsfontosságú szereppel bír az NGM-en kívül a 2 állami, pénzügyi felügyeleti szervünk, úgymint az MNB (PSZÁF!) és a MÁK. Minden pozitívan előremutató eredmény, megoldás eléréséhez az általuk közösen megfontolt és kimunkált tevékenységre van szükség a jövőben a bankokat fenyegető kibertámadások ellen.

Felhasznált irodalom

[1] Gazdag Ferenc, Tálas Péter: A biztonság fogalmának határairól, Nemzet és Biztonság, 2008/1. szám (3-9. o.)

[2] Gazdag Ferenc: Biztonsági tanulmányok – Biztonságpolitika, ZMNE, Budapest, 2011. 37-46. o. ISBN 978-615-5057-23-6

[3] A Kormány 1139/2013. (III.21.) Korm. határozata Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

[4] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

[5] Sík Zoltán Nándor: A kritikus információs infrastruktúra védelem kormányzati feladatai az információs hadviselés korában http://old.ivsz.hu/resource.aspx?ResourceID=GetDocStoreFile&EntryID=3353 (2013.december 17.)

[6] Haig Zsolt, Várhegyi István: A cybertér és cyberhadviselés értelmezése Hadtudomány 2008. elektronikus szám 1-12. o. ISSN 1215-4121 http://mhtt.eu/hadtudomany/2008/2008_elektronikus/2008_e_2.pdf (2014. január 16.)

[7] Haig-Kovács-Ványa: Az elektronikai hadviselés, SIGINT és a Cyberhadviselés kapcsolata Felderítő Szemle X. évf. 1-2. sz. 2011. 183-209. o. http://www.kfh.hu/hu/letoltes/fsz/2011-1-2.pdf (2014. január 16.)

[8] Haig Zs.: Az információs hadviselés kialakulása, értelmezése. Hadtudomány XXI. évf. 1-2. szám 2011. (12-28. o.) http://mhtt.eu/hadtudomany/2011/1/HT-2011_1-2_4.pdf (2014. január 16.)

[9] Kassai Károly: A minősített információk és adatok védelme http://www.zmne.hu/kulso/mhtt/hadtudomany/2002/1/z-05/chapter1.htm, (2013. december 12.)

[10] Kassai Károly: A minősített információk és adatok védelme http://www.zmne.hu/kulso/mhtt/hadtudomany/2002/1/z-05/chapter1.htm, (2013. december 12.)

[11] Haig-Kovács-Munk-Ványa: Az infokommunikációs technológia hatása a hadtudományokra, NKE, Budapest (2013. 173 o.) ISBN: 978-615-5305-02-3

[12] Vígvári András: Pénzügy(rendszer)tan Akadémiai Kiadó, Budapest 2009. (192-194. o.) ISBN 978-963-05-8595-8

[13] Vígvári András: Pénzügy(rendszer)tan Akadémiai Kiadó, Budapest 2009. (414-417. o.) ISBN 978-963-05-8595-8

[14] Dr. Haig Zsolt – Dr. Kovács László: Fenyegetések a cybertérből http://www.nemzetesbiztonsag.hu/letoltes.php?letolt=57 (2013. december 17.)

[15] Dr. Kovács László – Dr. Krasznay Csaba: Digitális Mohács - kibertámadási forgatókönyv Magyarország ellen http://www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo__krasznay_csaba-digitalis_mohacs_.pdf 2013. december 10.

[16] Cser Orsolya: Biztonságunk egyik záloga a hatékony civil-katonai együttműködés http://mhtt.eu/hadtudomany/Hadtudomany_2013_3-4_10.pdf (2013. november 29.)

[17] A Kormány 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról

[18] A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI törvény 2. számú melléklete

[19] A NATO kibervédelmi gyakorlatán is jól vizsgáztunk (CMX 12 NATO Válságkezelési gyakorlat nemzeti feladatai) http://bitport.hu/biztonsag/a-nato-kibervedelmi-gyakorlatan-is-jol-vizsgaztunk (2013. december 2.)

[20] A hitelintézetekről és a pénzügyi vállalkozásokról szóló 1996.évi CXII. törvény

[21] Jakab Péter: Egy működő vállalati komplex biztonsági rendszer felépítése, működése http://regi.hte.hu/data/upload/File/HTE_Forum_JakabP_080902.ppt (2013. december 19.)

[22] A Magyar Nemzeti Bankról szóló 2011. évi CCVIII. törvény

[23] Cser Orsolya: A pénzügyi rendszer, mint kritikus infrastruktúra ágazat – avagy a pénzellátás folyamatosságának védelme „Szervezeti, szabályozási és innovatív változások a létfontosságú rendszerek védelmében” tudományos-szakmai konferencia 2013.11.14. – elektronikus megjelenés 2014. március végén a konferencia külön kiadványában