HADMÉRNÖK

IV. Évfolyam 2. szám - 2009. június

Fleiner Rita
Budapesti Műszaki Főiskola
fleiner.rita@nik.bmf.hu

ADATBÁZISOK SZEREPE KRITIKUS INFRASTRUKTÚRÁK BIZTONSÁGÁBAN

Absztrakt

A kritikus infrastruktúrák működése napjainkban már szinte elképzelhetetlen az informatika eszközeinek, rendszereinek, alkalmazásainak támogatása nélkül. A támogató informatikai rendszerek jelentős részének működésében lényeges, esetenként kiemelt szerepet játszanak különböző adatbázisok is. Jelen publikáció alapvető célja – egy kutatás folytatásaként - az adatbázis-biztonság helyének, szerepének bemutatása két konkrét, nevezetesen a pénzügyi és a közigazgatási kritikus infrastruktúra szektorokban, a kapcsolódó szolgáltatások és informatikai rendszerek vizsgálatán keresztül.

The operation of critical infrastructures nowadays is practically impossible without the support of IT systems, IT applications. In the operation of most of the supporting IT systems databases play a significant, occasionally crucial role. The aim of this publication – as a continuation of a research – is to demonstrate the place and the role of database security in the area of two specific, namely financial and civil service critical infrastructure sectors through the examination of the contributing services and information systems.

Kulcsszavak: *adatbázisok, kritikus infrastruktúra, kritikus infrastruktúra szektorok, közhiteles nyilvántartások, fenyegetettség ~ databases, critical infrastructure, critical infrastructure sectors, public registers, threats*

BEVEZETÉS

A fejlett XXI. századi társadalmak egyre nagyobb mértékben függenek a különböző infrastruktúráktól, melyek egymással is szoros kapcsolatban, kölcsönös függésben állnak. A társadalmi, gazdasági és hétköznapi élet működési folyamatai egyre inkább veszélyeztetettek a kritikus, más szóval létfontosságú infrastruktúrák működésének, szolgáltatásainak megszakadása esetén.

A kritikus infrastruktúrák általános fogalma alatt olyan infrastruktúrákat (működtető személyzet, folyamatok, rendszerek, szolgáltatások, létesítmények, és eszközök összessége) értünk, amelyek megsemmisülése, szolgáltatásaik vagy elérhetőségük csökkenése egy adott felhasználói kör létére, lét- és működési feltételeire jelentős negatív hatással jár. A kritikus infrastruktúra ezen általános fogalmán belül az érintett felhasználói körtől függően meg kell különböztetnünk a nemzeti, európai, védelmi/katonai, szövetségi, vagy szervezeti kritikus infrastruktúrákat. [1]

A szakirodalomban gyakorlatilag teljes körűen elfogadott a kritikus infrastruktúrák egymástól való kölcsönös függése (ún. interdependenciája). Az összekapcsolódó, összetett függési viszonyokban álló infrastruktúrák a közvetett veszélyeztetéseken keresztül így természetesen sérülékenyebbek is. Napjainkban ezek között is kiemelt jelentőséggel bír a különböző infrastruktúrák egyre növekvő mértékű függősége a tágabb értelemben vett informatikai hálózatok, rendszerek, eszközök szolgáltatásaitól.

A kritikus infrastruktúrák működése napjainkban már szinte elképzelhetetlen az informatika eszközeinek, rendszereinek, alkalmazásainak támogatása nélkül. Ez az informatikai támogatás részben önálló információs infrastruktúrák révén, részben azokat támogató, kiszolgáló összetevők révén jelenik meg. A támogató informatikai rendszerek jelentős részének működésében lényeges, esetenként kiemelt szerepet játszanak különböző adatbázisok is. Az adatbázis adatoknak számítógépekben tárolt, valamely adatmodell szerint strukturált gyűjteménye. Az adatbázisokban tárolt adatok kezelését speciális alkalmazások, az úgynevezett adatbázis-kezelő rendszerek biztosítják.

A kritikus információs infrastruktúrának nevezzük az információs tevékenységeket támogató rendszerek, eszközök olyan összességét, amely önmagában kritikus infrastruktúra, vagy lényeges szerepet játszik más kritikus infrastruktúrák működésében. Az előbbieket a szakirodalomban funkcionális információs infrastruktúráknak is nevezik. Ezek azok az "információs közművek", amelyek a társadalom alapvető információs szolgáltatásigényeit elégítik ki. [2]

A kritikus információs infrastruktúrákat számos fenyegetés veszélyezteti, melyek a rendszerek különböző elemeit érintik. Egy lehetséges fenyegetési pont az infrastruktúrák részét képező lényeges adatbázisok támadása, mely különösen veszélyes azokban az esetekben, ahol az adatbázisok az infrastruktúra központi elemét képezik. A publikációban olyan kritikus infrastruktúra szektorokat, azon belül informatikai rendszereket vizsgálunk meg, ahol az adatbázisok szerepe, így biztonsága is központi helyet foglal el.

A kritikus infrastruktúrák osztályozására, szektorokba sorolására több hasonló felépítésű, de egymástól szemléletbeli eltéréseket tartalmazó munka született. Ezt Muha Lajos részletesen elemzi PhD értekezésében [3], ahol EU, NATO és nemzeti osztályozásokat mutat be. A hazai kritikus infrastruktúravédelem nemzeti programjáról szóló kormányhatározat [4] a következő felosztást javasolja: energiaellátás; közlekedés; vízellátás; élelmiszerellátás; egészségügy; pénzügy; ipar; jogrend, kormányzat; közbiztonság, védelem; és végül az infokommunikációs szolgáltatások. A továbbiakban az állampolgárok által mindennapi szinten használt szolgáltatásokra koncentrálva, a pénzügyi és a kormányzati szektorokban mutatjuk be az adatbázisok helyét, szerepét.

Jelen publikáció alapvető célja – az adatbázis-biztonság és a kritikus infrastruktúrák biztonsága összefüggéseinek alapjait tárgyaló publikációhoz [5] kapcsolódóan – az adatbázis-biztonság helyének, szerepének részletesebb bemutatása a pénzügyi és a kormányzati

(közigazgatási) kritikus infrastruktúra szektorokban. Ennek kapcsán a kapcsolódó szolgáltatásokat és informatikai rendszereket is megvizsgáljuk. A publikáció tehát a kiválasztott kritikus infrastruktúra szektorokban részletesebben bemutatja, elemzi az adatbázisok felhasználását, helyét és szerepét; illetve meghatározza az adatbázisok biztonsága sérülésének következményeit, hatását az adott kritikus infrastruktúra biztonságára vonatkozóan.

ADATBÁZISOK HELYE, SZEREPE, FŐBB JELLEMZŐI EGYES KRITIKUS INFRASTRUKTÚRA SZEKTOROKBAN

Publikációnk ezen fejezetében néhány olyan kritikus infrastruktúrabeli szolgáltatás részletesebb vizsgálatát folytatjuk le, melyek az állampolgárok hétköznapjainak szerves részét képezik és ezeket vagy aktívan (pl. internetes bankolás) vagy passzívan (pl. orvosi ellátás kapcsán elektronikus TAJ szám ellenőrzés) gyakorolják is. Vizsgálataink középpontjában a szolgáltatások szempontjából létfontosságú adatbázisok állnak, de ehhez a kapcsolódó, komplexebb környezetet biztosító informatikai folyamatokat is meg kell ismernünk. A kiválasztott szolgáltatások a pénzügyi és közigazgatási területek alá tartoznak, az utóbbi esetében az országos szintű rendszerek adatbázisaira, a közhiteles nyilvántartásokra fogunk koncentrálni.

A két terület (pénzügy és közigazgatás) vizsgálatát az alábbi szempontok tanulmányozásával végezzük el. Először nagyvonalakban megvizsgáljuk az adott szolgáltatási ágazat informatikai fejlettségét, történetét, jogi szabályozottságát. Utána röviden felvázoljuk az adatbázisokat tartalmazó informatikai rendszereket, majd részletesebben leírjuk a bennük szereplő adatbázisok helyét, szerepét, a tárolt adatok jellemzőit és az adatbázisok elérésének módjait. Végül pedig az adott ágazatban megtalálható adatbázisok kritikusságát vizsgáljuk meg.

Pénzügy

A kritikus infrastruktúrák osztályozásában [4] a Pénzügyi ágazat alatt két alágazat megjelölését találjuk, nevezetesen:

1. fizetési, értékpapírklíring- és elszámolási infrastruktúrák és rendszerek
2. bank és hitelintézeti biztonság

A köznapi életben pénzügyi intézménynek általában a bankokat gondoljuk, a magyar jogszabály azonban a hitelintézeteket és pénzügyi vállalkozásokat definiálja alatta. A bank a hitelintézetek egy fajtája, jelen dolgozatunkban ezzel foglalkozunk részletesebben. (A második alágazat esetén szerencsésebb lenne a bank és hitelintézeti rendszerek elnevezés, hisz a biztonság egy állapot és nem infrastruktúra elem.)

A pénzintézetek, ezen belül a bankok szolgáltatásaikhoz, működési folyamataikhoz, adataik nyilvántartásához már évtizedek óta intenzíven használnak informatikai rendszereket, melyek köre, mértéke az információs technológia fejlődésével folyamatosan bővül. Mivel a pénzintézetek, bankok erősen profit orientált szervezetek, általánosságban kijelenthető, hogy rendelkeznek elég anyagi háttérrel és motivációval ahhoz, hogy informatikai szintű szolgáltatásaikat folyamatosan fejlesszék és használják a legújabb technológiai megoldásokat.

Informatikai rendszereikre, ezen belül adatbázisaikra és azok biztonságára vonatkozó hazai törvények és jogszabályok (melyekbe nemzetközi normákat, mint például Bázel II.[1] is adaptálni kellett) erős szabályozottságot jelentenek, ezek betartását Magyarországon a PSZÁF[2] ellenőrzi.

A következőkben röviden ismertetjük a pénzügyi szektor első alágazatához tartozó három hazai jelentős pénzügyi elszámolási rendszert, nevezetesen a GIRO, VIBER és KELER rendszereket, majd terjedelmi okok miatt egyet (VIBER) kiemelve részletesebben is megvizsgálunk.

A bankközi zsírórendszer a bankok közötti fizetési forgalmat (bankközi átutalásokat) lebonyolító, nem valós idejű, kötegelt feldolgozás szerint működő elszámolási rendszer, melyet Magyarországon a GIRO Zrt. működtet és közvetve vagy közvetlenül minden bank a tagja. A Valós Idejű Bruttó Elszámolási Rendszer (VIBER) a GIRO rendszer mellett működő, annál gyorsabb elszámolási (átutalási) rendszer. Azonnali, valós időben történő tranzakciókra nyújt lehetőséget. Az átutalás gyakorlatilag azonnal megjelenik a partner bankjánál és a fogadó bank köteles azt még aznap ügyfele rendelkezésére bocsátani. A VIBER megbízás a bankban történő rögzítést követően visszavonhatatlan. A tranzakciók díja igen magas, általában 0,5 % (min 10 eFt max. 100 eFt). Az értékpapírok elszámolási rendszerét Magyarországon a KELER Zrt. látja el, mely a VIBER rendszernek kiemelt jelentőségű tagja. Lehetővé teszi a piaci szereplők egymással kötött értékpapír ügyleteinek kockázatmentes és gyors elszámolását. Közvetlen partnerei a befektetési szolgáltatók, brókercégek, bankok és értékpapírt kibocsátó vállalatok

A VIBER rendszert a Magyar Nemzeti Bank (MNB) üzemelteti, tagjai hitelintézetek (bankok), a Magyar Államkincstár, a Magyar Posta, a KELER és az MNB. A rendszeren keresztül megvalósított pénzügyi ügyletek a következőkből állnak össze 6. Egyrészt a VIBER tagok ügyfelei által kezdeményezett kifizetések (például egy magánszemély banki átutalását valós időben szeretné elvégezni), másrészt a KELER-hez kötődő, VIBER tag bankok értékpapír ügyleteinek pénzoldali teljesítése, harmadrészt a bankközi tranzkciók (két VIBER tag számlája közötti terhelés és jóváírás), végül pedig a bankok hitelfedezetének törlesztése.

A VIBER tagok és az MNB között a SWIFT nemzetközi hálózat biztosít rejtjelzett, saját szabványra épülő kommunikációt, mely a SWIFT központon keresztül bonyolódik le. (Tehát a VIBER tag üzenete először a nemzetközi központba jut el, majd onnan az MNB-be.) A VIBER rendszer lényeges része az MNB által vezetett központi számlavezető rendszer (CAS, Central Accounting System), mely a fizetési megbízásokat teljesíti végleges és visszavonhatatlan módon. Ebben a rendszerben találhatóak a VIBER-hez kötődő fontos adatbázisok, melyek egyrészt a VIBER tagok pénzügyi egyenlegét, számlaszámát, egyedi kódját, nevét tartalmazzák, másrészt a pénzügyi tranzakciókhoz tartozó információkat. A VIBER üzemidején kívül a CAS és az MNB-ben vezetett analitikus ügyfélszámla-vezető rendszer (hitelintézetek pénzforgalmi számlái, hitel- és betétszámlái, forint- és devizaszámlái) között adatharmonizáció történik.

A pénzügyi szektor második alágazatához a bankok önálló rendszerei tartoznak, ezen belül mi a banki informatikai rendszerekre koncentrálunk. Egy banki informatikai rendszer a következő részekből épül fel. Egyrészt áll az ügyfél oldalon megjelenő, az ügyfelek felé

[1] Az Európa Tanács által 2004-ben elfogadott, hitelintézetek és befektetési vállalkozások tőkemegfeleltetési előírásainak direktívája, mely jogi, pénzügyi és informatikai elvárásokat fogalmaz meg pénzintézetek számára.
[2] Pénzügyi Szervezetek Állami Felügyelete

interfészt biztosító alrendszerből, ami a pénzügyi tranzakciók bank felé történő elindításáért felel. Ma már többféle csatornán keresztül lehet ezt a folyamatot végrehajtani, például bankfiókon, telefonon, interneten, ATM (Automated Teller Machine, bankjegykiadó automata) vagy POS (Point of Sale, a vásárlás helye)[3] terminálon keresztül. A tranzakciók véglegesítése a másik fontos egységen, a központi rendszerben történik, ahol a banki szintű nagy adatbázisok is találhatók, melyek a mi vizsgálatunk szempontjából kiemelkedő fontosságúak. A két egység között az általános tranzakció továbbító rendszer teremti meg a kapcsolatot, tehát ez az a réteg, mely például a bankfiókban elindított számlanyitási kérelmet a központi rendszerbe elektronikus úton eljuttatja. A bankfiókokban is találhatóak helyi adatbázisok, de a pénzügyi szolgáltatások adatainak lényeges része a központi banki rendszer adatbázisaiban található.

Egy bank központi informatikai rendszere több, egymással különböző kapcsolatban álló alrendszerből épül fel, melyek mögött saját adatbázisok állnak. A számlavezető rendszer adatbázisában nyilvántartják az ügyféltörzs adatait (vállalati és lakossági egyaránt), a különböző számlákhoz tartozó adatokat (számlatörzs), a kamatozás adatait, illetve néhány hónapra visszamenőleg a tranzakciók adatait, mely ennek a rendszernek a legnagyobb és leggyakrabban módosuló adattábláját (tízmilliós nagyságrendű sorból áll) jelenti. A főkönyvi rendszerben a bank összvagyonával kapcsolatos adatokat tárolják, mely naponta kap adatokat a számlavezető rendszertől. Az átutalási rendszerben nyilvántartják az ügyfelek más bankszámlákra történő, rendszeres átutalásainak adatait, ez a rendszer külön bérelt vonalakon keresztül kapcsolódik a zsíró-, illetve VIBER elszámolási rendszerekhez. A hitelelbíráló rendszer adatbázisában a hitelekről és az ügyfelek minősítéséről, kockázatairól tárolnak adatokat. A KELER Zrt.-vel kapcsolatban álló értékpapír rendszer részvények és befektetési jegyek adatait tartalmazza. Az elektronikus csatornák rendszere végzi a kapcsolattartást az internet-, és mobil bank felhasználóival, tehát külső (bankon kívüli) hozzáféréssel is tud kapcsolatokat fogadni. Saját adatbázissal rendelkezik, amihez az adatok egy részét, például az ügyfelek és számláik adatait a számlavezető rendszerből tölti fel egy inicializáció keretében, majd a tranzakciók során on-line kommunikációt is folytatnak ezek a rendszerek egymással. A kártya rendszer feladatköre és adatbázis rendszere kettős feladatot lát el. Egyrészt az ATM és POS terminálokról kezdeményezett tranzakciókat fogadja és kommunikálja le a számlavezető rendszerrel, ehhez persze megfelelő adattáblákkal kell, hogy rendelkezzen a kártyák és hozzá tartozó ügyfelek adataival kapcsolatban. Másrészt a kártya-, és PIN gyártás folyamatához szükséges adatokat tárolja. Az utóbbi néhány évben lezajlott adatbázis kezelő rendszerek fejlesztésének köszönhetően bankokban a különböző adatbázisok adatait hatalmas méretű adattárházakba vonják össze, melyekből adatbányászati módszerekkel, beépített összefüggések felhasználásával a bank folyamatairól jelentéseket generálnak például a PSZÁF, MNB és az APEH felé.

A fizetési és elszámolási rendszereket kritikus infrastruktúrának tekinthetjük, a rendszerek nem megfelelő működése veszélyeztetheti a pénzügyi szektor hatékony működését, és szélsőséges esetben a rendszer egészének stabilitást is [7]. Mivel a pénzügyi elszámolási rendszerek működése erőteljesen függ a mögöttük álló adatbázis kezelő rendszerek és azon belüli adattartalom biztonságától, ezek szerepe szintén kritikusnak minősíthető.

A banki, hitelintézeti informatikai rendszerek kritikusságának vizsgálatát szolgáltatásaik kritikusságának felmérésével kell kezdeni. Ehhez meg kell határozni a létfontosságú banki szolgáltatásokat és azokat a paramétereket, melyek a különböző bankok konkrét

[3] Kereskedőknél található eszköz, mely a bankkártyás fizetésnél megteremti a bankkal létesített kapcsolatot.

szolgáltatásait kritikusság szerint kategorizálják. Egy kritikusnak ítélt banki szolgáltatás mögött pedig meg kell határozni a kritikus adatbázisokat is. Egy banki szolgáltatás esetén fontos és figyelembe veendő szempont az is, hogy a fizetési és elszámolási rendszerekben egy szereplő (pl. egy bank) működőképességének sérülése veszélyeztetheti a rendszer többi tagjának a helyes működését is, ezáltal pedig a teljes pénzügyi rendszert. [7]

Kormányzat, közigazgatás

A közigazgatás olyan közhatalommal rendelkező igazgatási tevékenység, illetve szervezetrendszer, amely a hatalommegosztás elvéből eredően önálló hatalmi ágként funkcionálva biztosítja a jogállamiság követelményeinek érvényesülését. (A civil közigazgatás az államigazgatási szervek rendszeréből és önkormányzati szervek rendszeréből áll) [8] A kritikus infrastruktúrák védelmére vonatkozó hazai Zöld könyv besorolása szerint a Jogrend – Kormányzat szektor alá tartozik a közigazgatási szolgáltatások alágazata. Ha ezt a fogalmat átfogóan kezeljük (mint a jelen írás), akkor más kritikus infrastruktúra szektorok szolgáltatásaival (pl. egészségügy, közbiztonság – védelem) bizonyos átfedéseket találhatunk.

A közigazgatási szolgáltatások informatikai támogatása két jól elkülöníthető, területre bontható: a közszolgálati intézmények belső működésének támogatására (back office) és a lakosság, valamint a gazdálkodó szervezetek ezen intézményekkel történő kapcsolattartására (front office) [5]. A magyar közigazgatásban az informatika évtizedek óta jelen van, és folyamatosan fejlődik, az elmúlt években jutott el arra a szintre, hogy az egymástól különálló, elszigetelt rendszerek összehangolása, összekapcsolása elkezdődhessen. Ezt a célt szolgálja a Központi Elektronikus Szolgáltató Rendszer, mely magába foglalja az összeköttetést biztosító Elektronikus Kormányzati Gerinchálózatot, az egykapus ügyintézést megvalósító és a központi tájékoztató szerepet betöltő Kormányzati Portált, az egyes ügyek intézésében a tájékozódást segítő, és az állampolgárok és vállalkozások számára információt szolgáltató Kormányzati Ügyféltájékoztató Központot, az elektronikus ügyintézést igénybe vevők azonosítását biztosító Ügyfélkaput, valamint a központi rendszer elemein megjelenő szolgáltatásokat és ügyintézési lehetőségeket. Magyarországon az elektronikus közigazgatás megvalósításának, fejlesztésének koordinálását a 1026/2007. (IV. 11.) Korm. határozattal létrejött Közigazgatási Informatikai Bizottság látja el.

Az elektronikus közigazgatás alapvető feltétele a tevékenység során felhasznált, naprakészen tartott elektronikus nyilvántartások, adatbázisok megléte, elérhetősége. Ezek egyik csoportját az alapnyilvántartások alkotják, amelyek az adott területen (vagy az ország területén) élő személyek, szervezetek, események adatait tárolják el. A másik csoportba az ágazati, vagy szakági rendszerek tartoznak, amelyek az adott szakterület (tárca) funkcióihoz igazodnak, a szakterületi informatikai rendszerek szerves részét képezik [5]. A közigazgatásban jelenlévő nyilvántartások egyik fontos típusa a közhiteles nyilvántartás, azaz olyan, hatóság által vezetett nyilvántartás, melynek tartalmát, az abban szereplő adatok valódiságát az ellenkező bizonyításig mindenki köteles elfogadni.

Az alapnyilvántartásokról, illetve ezek biztonságos és védett elektronikus tárolásáról (adatbázisokban) hazánkban a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala (KEK KH) gondoskodik. Ide tartoznak a teljesség igénye nélkül, többek között a polgárok személyi adatainak és lakcímének nyilvántartása, a bűnügyi nyilvántartás, a közúti közlekedési nyilvántartás, az úti okmányok nyilvántartása, az idegenrendészeti nyilvántartás és a választásokhoz kapcsolódó nyilvántartások. Az alapnyilvántartások adatszolgáltatási feladattal bírnak egyes ágazati nyilvántartások felé (pl. APEH, OEP, ORFK, KSH).

A személyi adat és lakcímnyilvántartás célja, hogy biztosítsa azokat az alapvető személyi és lakcímadatokat, amelyek a polgárok egymás közötti jogviszonyaiban személyazonosságuk igazolásához, illetőleg a közigazgatási és az igazságszolgáltatási szervek, a helyi önkormányzatok, valamint más szervezetek törvényen alapuló adatigényeinek kielégítéséhez szükségesek. A következő adatokat tartalmazza: név, állampolgárság, születési hely és idő, anyja neve és személyi azonosítója, elhalálozás helye és ideje, lakcím (településnév, irányítószám, közterület neve, házszám, stb.), adatszolgáltatásra vonatkozó korlátozás, családi állapot, házasságkötés helye, arckép, aláírás, szem. ig. száma, személyi azonosítója, lakcím kártya azonosítója. A nyilvántartás közhitelessége miatt szükségszerű a nyilvántartott adatok naprakészségének biztosítása. Adatváltozás esetén az esemény bekövetkezésének helyén (pl. helyi okmányirodában) az új adatok bekerülnek az adatgyűjtő rendszerbe, ahonnan távadatfeldolgozó hálózat segítségével a lehető legrövidebb időn belül elérik a központi nyilvántartást, ahol a tárolt adatokon átvezetésre kerülnek, majd az átvezetés eredményeként keletkezett aktuális adatok ugyanezen távadatfeldolgozó hálózaton keresztül eljutnak a nyilvántartás helyi szerveihez (a lakóhely szerint illetékes jegyzőhöz). [9]

A közúti közlekedési nyilvántartás tartalmazza a járművezetői okmányok adatait, járművek adatait, külföldről behozott használt járművek származás-ellenőrzés adatait, eredetiségvizsgálati adatokat, parkolási igazolványok adatait. A bűnügyi nyilvántartás - egymástól különálló nyilvántartásokként - a bűntettesek, a büntetőeljárás alatt állók, a kényszerintézkedés alatt állók, az ujj-és tenyérnyomatok, valamint fényképek és a DNS-profilok nyilvántartását foglalja magába. A választások előtt összeállított választói névjegyzéket a személyi adat- és lakcímnyilvántartás adataiból, illetve a választójoggal nem rendelkező személyek nyilvántartásából készítik el.

Az ágazati elektronikus nyilvántartások közé a rendőrségi, bírósági, oktatási, adóügyi, vámügyi, társadalombiztosítási, földhivatali, stb. adatbázisok tartoznak. Jelen publikációban a TAJ-nyilvántartást és jogviszonyadatok nyilvántartását vizsgáljuk meg részletesebben, melyeket az Országos Egészségbiztosítási Pénztár (OEP) felügyel [10]. A TAJ-nyilvántartás az 1995-ben élő személyeket, valamit az azóta nyilvántartásba került személyek adatait tartalmazza, egy személyre vonatkozóan tárolja a személyi adatokat (név, leánykori név, anyja neve, születési hely és idő), nemet, családi állapotot, állampolgárságot, lakóhelyet (tartózkodási hely) és a TAJ-számot. A nyilvántartás célja a személyek egészségbiztosítási ellátásának igénybe vételéhez szükséges Társadalombiztosítási Azonosító Jel-lel történő azonosítása, az ellátás jogosultságának eldöntése nem tartozik a feladatkörébe. Ezt a funkciót a Bejelentett személyek jogviszonyadatainak nyilvántartása látja el, mely a személy munkaviszonyával kapcsolatos adatokat (pl. foglalkoztató neve, székhelye, nyilvántartási száma, jogviszony jogcíme, jogviszony időtartama, heti munkaidő, magánnyugdíjpénztári tagság) is tartalmazza a név és TAJ szám tárolása mellett. A fenti két nyilvántartás külső elérése több módon is lehetséges. Az állampolgároknak az ügyfélkapun keresztül lehetőségük van betegéletút-lekérdezésre, biztosítási jogviszony lekérdezésre és TAJ-szám érvényességének ellenőrzésére. 2007. április 1-től az egészségügyi szolgáltatás (orvosi ellátás, gyógyszer vásárlás) igénybevételét megelőzően az egészségügyi szolgáltató köteles a betegnél előzetes jogviszony-ellenőrzést végezni. A gyógyszertárak a gyógyszer kiadásakor a VIREP rendszer segítségével lépnek on-line kaocsolatba az OEP nyilvántartásával abból a célból, hogy a betegek közgyógyellátásra való jogosultságát ellenőrizzék [11]. Az egészségügyi szolgáltatók (háziorvosok, kórházak) szintén on-line módon ellenőrzik a páciens jogosultságát a számukra fejlesztett OJOTE rendszerrel [12].

Összefoglalásul kijelenthetjük, hogy a közigazgatásban megtalálható számos, kulcsfontosságú szerepet betöltő adatbázis, melyek sérülése, meghamisítása alapvető

közigazgatási szolgáltatásokat hiúsít meg, vagy tesz megbízhatatlanná. Számos szolgáltatás hiánya a mindennapi és a gazdasági élet lényeges folyamatainak megvalósulását országos szinten akadályozza. Hasonlóan a pénzügyi szektorhoz, a közigazgatásban is fel kell mérni, hogy melyek a kritikusnak minősíthető szolgáltatások és mögöttük milyen létfontosságú adatbázisok állnak, melyek védelméről megfelelően gondoskodni kell.

Az előbbi két szakterület áttekintése, értékelése alapján is megállapíthatjuk, hogy a kritikus infrastruktúrákban vannak olyan adatbázisok, amelyek biztonsága az adott kritikus infrastruktúra biztonságának alapvető összetevője. Ezen adatbázisok megnevezésére – legalábbis a kritikus infrastruktúra védelem vonatkozásában – javasoljuk bevezetni a kritikus adatbázisok kifejezést. Az ebbe a csoportba tartozó adatbázisok meghatározásához először az érintett infrastruktúra által nyújtott szolgáltatás kritikus jellegét, majd ezen belül az adott adatbázis működéskritikus jellegét kell meghatározni. A kritikusnak ítélt adatbázisok védelmére pedig sajátos biztonsági szabályozást célszerű alkalmazni.

KRITIKUS INFRASTRUKTÚRÁK FENYEGETETTSÉGE ADATBÁZISOKON KERESZTÜL EGYES SZEKTOROKBAN

A kritikus infrastruktúrák működése számos módon, különböző összetevőiken keresztül veszélyeztethető, gátolható. A veszélyeztetések lehetnek fizikai (anyagi) és információs jellegűek. Ez utóbbiak sajátossága, hogy a veszélyeztetett rendszerbe általa értelmezhető, feldolgozható információt juttat be, vagy a rendszer által kezelt információt, megvalósított információs tevékenységet módosít, töröl az adott rendszer saját folyamatai, résztevékenységei útján [5].

Kritikus infrastruktúrákat ért támadások közül kiemelendő az Észtország ellen 2007 tavaszán végrehajtott akció, melyben pont az általunk tárgyalt két ágazat, a pénzügyi és a kormányzati szektorok szolgáltatásait érte a legjelentősebb veszteség. A fejlett információs infrastruktúrával rendelkező, és az e-kormányzat területén komoly sikereket elért Észtország, a több mint kéthetes DDoS támadás során komoly anyagi károkat szenvedett, mert számos kormányzati, minisztériumi és több bank internetes oldala elérhetetlenné vált a támadások következtében. A támadások a tallinni orosz emlékmű elmozdítása után kezdődtek, és nagy részük többé-kevésbé beazonosíthatóan Oroszországban működtetett szerverekről indult. [13]

A kritikus infrastruktúrák adatbázisokon keresztüli fenyegetettségének vizsgálata kapcsán érdemes tisztázni az adatbázis biztonság fogalmát, illetve azokat a tulajdonságokat, melyeket a fenyegető hatások ellen a megkívánt mértékben védeni kell. Adatbázis biztonság alatt az adatbázisokban tárolt adatok biztonságát, illetve az adatbázis kezelő rendszer biztonságos működését értjük. Az adatok biztonságához a bizalmasság, sértetlenség és rendelkezésre állás, az adatbázis kezelő rendszerek biztonságához pedig a sértetlenség és rendelkezésre állás tulajdonságainak fenntartása tartozik. Bizalmasság annak biztosítása, hogy az információ csak az arra jogosultak számára érhető el, sértetlenség alatt az információk és az erőforrás teljességének és pontosságának megőrzését értjük, végül a rendelkezésre állás, annak biztosítása, hogy a felhatalmazott felhasználók hozzáférjenek a szükséges információkhoz. [14]

Az adatbázisok fenyegetettségeit két fő csoportra oszthatjuk aszerint, hogy az a szervezeten belülről vagy kívülről érheti az adott adatbázist. A belső támadás (szándékos vagy véletlen) a szervezeten belülről történik például egy belső munkatárs által, és általánosan jellemez minden informatikai rendszert, illetve szektort, ezért az ágazati elemzésekben ezt a típust nem említjük külön. A belső fenyegetések, közé kell sorolni a hardver, szoftver vagy

véletlen emberi hiba által okozott adatbázis sérüléseket is, melyek ellen rendszeres mentések, adatbázis replikációk készítésével lehet védekezni. A jól működő rendszerek újabb verzióinak telepítése is kockázatot hordoz, az új programok váratlan hibákat rejthetnek magukban, ezeket gondos, az eredeti környezetet lehető legjobban szimuláló tesztelés kell, hogy megelőzze. A belső fenyegetések elleni fegyverek közül nagyon fontos a megelőzés, a dolgozóknak megfelelő biztonsági oktatásban, továbbképzésekben kell részesülniük. Fontos feladat az adatokhoz való hozzáférés naplózása és a naplóbejegyzések folyamatos figyelése a visszaélések kiszűrése érdekében. Bizonyos szektorokban törvényi kötelezettségeknek is köszönhetően elterjedt a megfelelőség, angolul compliance monitorozása, mely a belső visszaélések kiszűrésében jelentős előrelépést jelent.

Külső támadások abban az esetben fenyegetnek, ha az adatbázisok tartalma külső hozzáféréssel, például webes szolgáltatások által elérhető. A támadás következménye lehet jogosulatlan adatszerzés, adatbázisban tárolt adatok, objektumok, jogosultságok megváltoztatása vagy az adatbázis kezelő rendszert futtató számítógép megzavarása, irányításának átvétele. Egy adott szolgáltatáshoz tartozó adatbázisok fenyegetéseinek vizsgálatakor fontos szempont az adott informatikai rendszer és azon belül az adatbázisok elérésének különböző módjai. A következőkben megvizsgáljuk a kiválasztott szektorokban az adatbázisok elleni támadások lehetséges módjait, motivációját, ágazatban használt védekezéseket, majd elemezzük a támadás következményeit a kritikusság szempontjából.

Pénzügy

A pénzügyi szektor adatbázis fenyegetéseinek vizsgálatánál is az egyik kiinduló pont az adatbázist tartalmazó informatikai rendszer és azon belül az adatbázisok elérésének különböző módjainak feltérképezése. A pénzügyi fizetési rendszereknél ismét a VIBER-t vizsgáljuk részletesebben. A VIBER rendszert kívülről a SWIFT hálózaton keresztül lehet elérni, ezáltal támadni is, amit egy webes alkalmazás támadásával összehasonlítva sokkal keményebb célpontnak kell minősíteni, kizárni viszont nem lehet. Az ameriakai titkosszolgálat például 2001. szeptember 11-i után titkos művelet keretében sikeresen behatolt a belgiumi székhelyű SWIFT banki adatbázisba (melyben a világ több mint 200 országában található mintegy 7800 bank és hitelintézet összes folyószámlájának, illetve azokon átmenő tranzakcióknak adatait tárolják) annak érdekében, hogy feltételezett terroristák nemzetközi pénzügyi átutalásait ellenőrizze [15].

A bankok adatbázisainak biztonságát külső és belső forrásból származó veszélyek fenyegetik. Külső támadások azon adatbázisok ellen lehetségesek, melyek a szervezeten kívülről, például internetes hozzáféréssel is elérhetők, ezáltal megszerezhetők. A támadás motivációja mögött húzódhat anyagi haszonszerzés, vagy akár összetettebb gazdasági-, politikai célok elérése. A támadás következménye lehet jogosulatlan adatszerzés, adatbázisban tárolt adatok, objektumok, jogosultságok megváltoztatása vagy az adatbázis kezelő rendszert futtató számítógép megzavarása, irányításának átvétele. Adatok illetéktelen kiszivárgása, esetleg nyilvánosságra kerülése a bankok számára rendkívül kellemetlen esemény, melynek jelentős anyagi, jogi és reputációs következményei lehetnek. Ügyfél adatok, bankkártya információk, számlaszámok, hitelminősítési adatok megszerzése hackerek, bűnözői körök, gazdasági hírszerzők kiemelt célpontjai közé tartoznak, de a banki infrastruktúra kritikussága szempontjából nem meghatározóak, ugyanis ezáltal a pénzügyi szektor működését nem lehetetlenítik el. A második típusú következmény, az adatbázis tartalmának megváltozása már lehet olyan mértékű, mely veszélyeztetheti a bank informatikai rendszerének működését, de hatással lehet még a fizetési rendszerek helyes működésére is (például tranzakciók adatainak szisztematikus megváltoztatása). A pénzügyi rendszer

kritikussága sérülhet, melynek helyreállítását az adatbázis egy korábbi, még helyes verziójának visszaállítása tudja megoldani. Itt egy lényeges szempont annak megállapítása, hogy mikor is történt a támadás, tehát melyik időpillanatban lévő verzióra kell az adatbázist visszagörgetni. A harmadik típusú következmény, mely a adatbázis kezelő rendszer mögötti infrastruktúrát zavarja meg, szintén kihat a kritikusság megsértésére. Ilyen típusú támadás esetén megoldás lehet a tartalék szerverre való átállás, mely egy bizonyos időkiesés után visszaállítja a helyes működést.

Kormányzat, közigazgatás

A magyar közigazgatás informatikai rendszereinek biztonságával más nézőpontból már többen foglalkoztak. Ki kell emelni Krasznay Csaba publikációját [16], melyben az e-közigazgatás fenyegetéseit támadási vektorok szerint rendszerezi, meghatározván három fő csoportot, a kliens oldali, a struktúra szintű és a protokoll szintű támadási pontokat. Póserné Oláh Valéria publikációjában [17] két szempontból vizsgálja a magyar közigazgatás informatikai rendszereinek biztonságának hiányosságait, nevezetesen a szabályozás oldaláról, illetve a hazai informatika biztonsági kultúrának fejlettsége felől. Jelen publikáció sajátossága az előzőekhez képest, hogy a közigazgatás létfontosságú adatbázisainak biztonsága szempontjából vizsgálja a helyzetet.

A közigazgatás adatbázisaira is érvényes a belső támadás, belső károkozás lehetősége, melyre kellően védettnek és felkészültnek kell lenni. A külső támadás felületét a rendszerek külső elérései biztosítják, a közigazgatás esetében számos adatbázist az állampolgárok az ügyfélkapun keresztül tudnak lekérdezni, illetve módosítani. Az ügyfélkapu biztonságos működésének egyik korlátja az egylépcsős bejelentkezés (azonosító és jelszó megadásával) [18], mely viszonylag könnyen támadható. 2009. februárjában súlyos incidens történt az ügyfélkapu használatában. Az üzemzavar következtében az oldalra belépő ügyfelek más személyek és cégek fiókjaiba lettek irányítva, ezáltal mások adatait, APEH-től érkező leveleit látták a sajátjuk helyett [19]. Ez egy igen súlyos biztonsági incidensnek számít, mivel nemcsak a tárolt adatok bizalmasságának kritériuma sérült, hanem mód volt mások adatainak, tehát adatbázisok tartalmának módosítására is, mely az adatok sértetlenségének kritériumát szegi meg, sőt ilyen esetben kijelenthető, hogy kritikus infrastruktúrát ért veszélyeztetés lépett fel.

A közigazgatás adatbázisait kívülről nemcsak az ügyfélkapun keresztül lehet elérni, a nyilvántartások egyéni vizsgálatával más módokat is találunk. Az előzőekben már vizsgált, OEP által vezetett TAJ-nyilvántartást és jogviszonyadatok nyilvántartását az ügyfélkapun kívül az egészségügyi szolgáltatók és gyógyszertárak a VIREP és OJOTE online elérést biztosító rendszerekkel tudják lekérdezni, melyek szintén rejthetnek sebezhetőségeket magukban. 2009. januárjában (hivatalos közlemény szerint szoftver hiba miatt) az OEP jogviszony-nyilvántartási adatbázisa megsérült és jelentős számú lekérdezés esetében hibás jelzést küldött a biztosított jogállásáról, vagyis a rendezett jogviszonyú biztosítottak is helytelen igazolást kaphattak, amikor háziorvosuknál, patikákban vagy más egészségügyi ellátónál jelentkeztek. Az adatbázis helyreállításáig a jogosultság ellenőrzést szüneteltették. A hiba miatt sérült a jogviszony-nyilvántartási adatbázis tartalma, de pár napos munkával (feltehetőleg előző mentések visszaállításával) a hibát korrigálni tudták [20]. Ebben az esetben is kijelenthető, hogy kritikus adatbázist ért veszélyeztetés. Az előző példák is mutatják, hogy a kritikus információs infrastruktúrák, ezen belül pedig a kritikus adatbázisok védelme a mai világban egy kiemelt feladat.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

A publikációban tárgyalt kritikus infrastruktúra szektorok (pénzügy, kormányzat) esetében – mint valószínűleg az összesben – elmondható, hogy rendszereik, folyamataik, szolgáltatásaik erősen (a jövőben várhatólag még intenzívebben) támaszkodnak informatikai rendszerek, eszközök támogatására. Az informatikai szolgáltatások nélkül az alapfolyamatok teljesen, vagy nagyrészt működésképtelenné, a szolgáltatások elérhetetlenné, vagy jelentős mértékben csökkentett színvonalúvá válnak. A növekvő informatika-függőségből következik, hogy a tárgyalt kritikus infrastruktúra szektorokban találhatóak olyan adatbázisok, amelyek szerepe jelentős, sértetlensége, hitelessége az adott alkalmazási terület alapvető működési feltételei közé tartozik.

Az előzőekben szereplő szakterületi áttekintések alapján megállapítható, hogy a kritikus infrastruktúrákban vannak olyan adatbázisok, amelyek biztonsága az adott kritikus infrastruktúra biztonságának alapvető összetevője. Ezen adatbázisok megnevezésére – legalábbis a kritikus infrastruktúra védelem vonatkozásában – javasoljuk bevezetni a kritikus adatbázisok kifejezést. Az ebbe a csoportba tartozó adatbázisok meghatározásához először az érintett infrastruktúra szolgáltatásának kritikus jellegét, majd ezen belül az adott adatbázis működés szempontjából vett kritikusságát kell meghatározni. Ez a feladat az adott szakterület szakértőinek kompetenciájába tartozik. A kritikusnak ítélt adatbázisok védelmére célszerű speciális biztonsági előírásokat, technológiákat meghatározni, ami pedig az informatikai biztonság szakterület feladatkörének a része.

FELHASZNÁLT IRODALOM

[1] Munk Sándor: A kritikus információs infrastruktúrák védelme információs támadások ellen. – Hadtudomány, 2008/1-2. (95-106.o.)

[2] Haig Zsolt-Várhegyi István: Hadviselés az információs hadszíntéren. – Zrínyi Kiadó, Budapest, 2005.

[3] Muha Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme. Doktori (PhD) értekezés. – Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2007.

[4] 2080/2008. (VI.30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról.

[5] Munk Sándor, Fleiner Rita: Adatbázisok kritikus infrastruktúrákban Hadmérnök, 2009 (IV.)/1. (225-234.o.), http://www.hadmernok.hu/2009_1_fleiner.pdf (2009.03.09.)

[6] VIBER rendszerleírás, 3.4 változat http://www.mnb.hu/Resource.aspx?ResourceID=mnbfile&resourcename=1szmellVIBERrendszerleiras20081117 (2009.01.20.)

[7] Lublóy Ágnes–Tanai Eszter: A működési kockázat és a hazai nagy összegű fizetési rendszer (VIBER), Hitelintézeti szemle 2007. hatodik évfolyam 4. szám 324-357o.

[8] http://www.kszk.gov.hu/data/cms13430/Allamigazgatas_diasor.ppt (2009.05.25.)

[9]http://www.nyilvantarto.hu/kekkh/kozos/index.php?k=adatszolgaltatas_hu_a_nyilvantartott_adatok_kore_szemelyi (2009.02.09.)

[10]http://www.oep.hu/portal/page?_pageid=34,12980076&_dad=portal&_schema=PORTAL (2009.02.09.)

[11] http://www.pointer.hu/files/virepmienk0515_final.doc (2009.02.09.)

[12] https://jogviszony.oep.hu/ojote/docs/ojote_felhasznaloi_kezikonyv.pdf (2009.02.09.)

[13] Kovács László: Az információs terrorizmus elleni tevékenység kormányzati feladatai, Hadmérnök, 2008 (III.)/2. (138-148.o.), http://www.zmne.hu/hadmernok/2008_2_kovacsl.php (2009.02.05.)

[14] Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana, Robothadviselés 8. Tudományos Konferencia, Budapest, 2008.11.27. (In. Bolyai Szemle 2008. XVII. évf. 4. szám, 137-156.o.)

[15] Banki adatokba tekintett be az USA http://www.sg.hu/cikkek/45511 (2009.02.09.)

[16] Krasznay Csaba: A magyar elektronikus közigazgatás biztonságának elemzése és továbblépési lehetőségei. Hadmérnök, 2009 (IV.)/1. (197-207.o.), http://hadmernok.hu/2009_1_krasznay.pdf (2009.03.09.)

[17] Póserné Oláh Valéria:. A magyar közigazgatás az informatikai biztonság szemszögéből, Robothadviselés 8. Tudományos Konferencia, Budapest, 2008.11.27. (In. Bolyai Szemle 2008. XVII. évf. 4. szám, 157-166.o.)

[18] Krasznay Csaba, Szigeti Szabolcs: A magyar elektronikus közigazgatási rendszer biztonsági analízise, Networkshop 2006 Konferencia, Miskolc, http://www.krasznay.hu/presentation/nws2006_krasznay.doc (2009.02.09.)

[19] http://itcafe.hu/hir/ugyfelkapu_uzemzavar_meh.html (2009.02.09.)

[20] http://itcafe.hu/hir/oep_szoftverhiba.html (2009.02.09.)