HADMÉRNÖK

X. Évfolyam 1. szám - 2015. március

JÉRI Tamás
jeri.tamas@bv.gov.hu

AZ ADATBÁZIS-KEZELŐK SZEREPE A KRITIKUS INTERNETES SZOLGÁLTATÁSOKBAN

Absztrakt

Az adatbázis-kezelők a kritikus internetes szolgáltatások nélkülözhetetlen alrendszerei, amelyek egyaránt biztosíthatják az adatfeldolgozás tárgyát, vagy a szolgáltatások működéséhez szükséges kulcs adatokat. Jelen írás arra keresi a választ, hogy milyen formában töltik be szerepüket, illetve hol foglalják el helyüket az adatbázis-kezelők a kritikus internetes szolgáltatásokban.

The database systems are essential subsystems of critical internet services, which could provide the subject of data processing, or the key data for operation of the services. This paper examines the database management systems' roles and purposes in the critical Internet services.

Kulcsszavak: *Internet, szolgáltatás, adatbázis-kezelő, adatbázis, alrendszer ~ Internet, service, database management, database, subsystem*

BEVEZETÉS

"Már a 60-as évek elején a számítógépek alkalmazásának nagyobbik részét az un. *adatfeldolgozás* tette ki.

Korán rájöttek a szakemberek arra, hogy az 'egyszerű' adatfeldolgozás is jobban 'gépesíthető', ha az adatok közötti akár egyszerű kapcsolatokat struktúrának tekintjük, és adatmodellekben, adatsémákban gondolkodunk.

Az olyan adathalmazokat, amelyeket modellbe foglalva kezeltek, adatbankoknak, később pedig adatbázisoknak nevezték el." [1]

Az adatfeldolgozás napjainkban is az informatika kimagasló jelentőségű szakága, amelyben a technikai fejlődés épp úgy fellelhető, mint a többi területen. Az adatokat feldolgozni és értelmezni szándékozó embereknek és az adatbázis-kezelő rendszereknek egészen más kihívásokkal kell szembenézniük, mint 1-2 évtizeddel ezelőtt. Az információs társadalom, a digitalizálás, s az internet elterjedése, szinte felfoghatatlan mennyiségű adat létrehozását eredményezi. Az úgynevezett "Big Data" jelenségre irányuló kutatások szerint, körülbelül 2,2 millió terra byte adat keletkezik naponta, amely mennyiséget Eric Schmidt, a Google volt elnöke úgy jellemezte, hogy "ennyi adat keletkezett a civilizáció hajnala és 2003 között összesen." [2] Ezen adatmennyiség tárolására és feldolgozására elsősorban az új generációs, úgynevezett befogadó-, vagy host típusú, - azaz másik programozási nyelvvel együtt használható, - hálózati interfésszel rendelkező, SQL[1] szintaktikát ismerő adatbázis-kezelő rendszerek alkalmasak. Az önálló programozási nyelvvel ugyan rendelkező, de mára elavult, elsősorban egy felhasználós, limitált rekordszámot kezelő, xBase[2] rendszerek egyre kevésbé játszanak szerepet napjaink adatbázisainak kezelésében. A kritikus internetes szolgáltatások (továbbiakban: KRISZ) működtetésében - szinte - megkerülhetetlen az adatkezelés problematikája, melynek egyenes következménye a KRISZ-hez illesztett, hálózati adatbázis kezelést biztosító rendszerek üzemeltetése, a bizalmasság, a sértetlenség, és az állandó rendelkezésre állás teljesítésével. Kérdésként merül fel, hogy az interneten megjelenő adatok kezelése mennyiben tér el a zárt rendszerben tároltakétól, egyáltalán milyen specialitások jellemzik a hálózati adatbázis kezelést, és milyen jelentőséggel bírnak az internetes szolgáltatások mögött rejlő adatok? Leszögezve azt a tényt, hogy az internetes szolgáltatást támogató adatbázis-kezelőnek állandó elérhetőséggel kell működnie, továbbá hogy a KRISZ felé biztosítani kell az adatfeldolgozás alap funkcióit, látszik, hogy a szolgáltatást igénybe vevő (felhasználó) és az adatbázis-kezelő közvetett kapcsolatban állnak egymással. A KRISZ-nek tehát az ügyfél és az adatbázis között egyaránt kell transzparenciát biztosítania a jogos adatok, információk kinyerésére, valamint gátat szabnia az adatok korlátlan, illetéktelen felhasználásának. A szolgáltatók az - akár érzékeny - adatok jogosultsághoz kötött rendelkezésre bocsátásával, állandó veszélynek teszik ki magukat az illegális adatszerzést célként kitűző emberekkel szemben, melyet versenyhelyzet, jogszabály, vagy csak az internet adta lehetőségek egyaránt indukálhatnak.

Fontos leszögezni, hogy mindegyik adatbázis-kezelőnek kell rendelkeznie olyan interfésszel/programmal amely a hozzáférések, a jogosultsági szintek, s az adatbázisban tárolt adatok módosítását lehetővé teszi. A gyakorlat azt mutatja, hogy előbb-utóbb, - az alkalmazói program megkerülésével, - szinte minden adatbázisban valamely adat manuális módosítása, korrigálása, továbbá az adatbázis-kezelő, mint bármely más szerverprogram karbantartása, frissítése szükséges. Ezeknek a funkcióknak a biztosítására hozzáférési felületet, vagy más értelmezésben lehetséges támadási pontot kell állandóan, vagy ideiglenesen fenntartani, s egyben a rendszer karbantarthatóságát biztosítani.

---

[1] SQL - Structured Query Language (strukturált lekérdezőnyelv)

[2] Általános kifejezése a dBASE programnyelvből és adatbázis struktúrából származó programozási nyelveknek

Publikációm fő célja a KRISZ-t kiszolgáló adatbázis-kezelő rendszerek szerepének feltérképezése, elhelyezkedés- és előfordulás szerinti vizsgálata.

AZ ADATBÁZIS-KEZELŐK HELYE A KRITIKUS INTERNETES SZOLGÁLTATÁSOKBAN

A kritikus internetes szolgáltatások egyik leggyakoribb háttérkiszolgálója az adatbázis-kezelő szerverprogram, amely az alábbi ismertebb internetes szolgáltatásokban rendszerint fellelhető:

- Web[3]
- Email[4]
- FTP[5]

Használatával a tartalom előállítás, vagy a szolgáltatások authentikációját biztosító felhasználó-kezelés egyaránt lehetséges, praktikus és legfőképpen szükséges. Tekintettel arra, hogy a KRISZ-nek és az adatbázis-kezelőnek állandó on-line kapcsolatban kell állnia egymással, a biztonsági szempontokat is figyelembe véve, eldöntendő, hogy a KRISZ-hez képest milyen elhelyezkedéssel működjön az adatbázis-kezelő? Az elhelyezkedést befolyásolja az adatbázis-kezelő jellege, a hálózati interfész rendelkezésre állása, az adatbázisok száma, illetve az adatbázis kiszolgálást igénybe vevő - egyéb - alkalmazások rendeltetése.

A KRISZ és az adatbázis-kezelő egymáshoz viszonyított lehetséges elhelyezkedéseiből meghatározhatók a kapcsolódási formák és a megvalósítási módok. Az adatbázis-kezelő KRISZ-en belüli alrendszeri funkciója, a két szerverprogram egymáshoz viszonyított elhelyezkedése, kapcsolódása, valamint a tárolt adatok érzékenységének együttese, meghatározza a rendszer kritikusságát.

Elhelyezkedés

Tekintettel arra, hogy a KRISZ mindenképpen egy interneten elérhető szolgáltatás, leszögezhető, hogy a rendelkezésre állásnak internet-tartományba tartozó IP címmel[6] rendelkező szerveren, vagy szervereken kell megvalósulnia. A KRISZ jellegéből, illetve a származtatott adatok további felhasználásából adódóan, mérvadó az adatbázis-kezelő KRISZ-hez viszonyított elhelyezkedése.

Operációs rendszer szerint

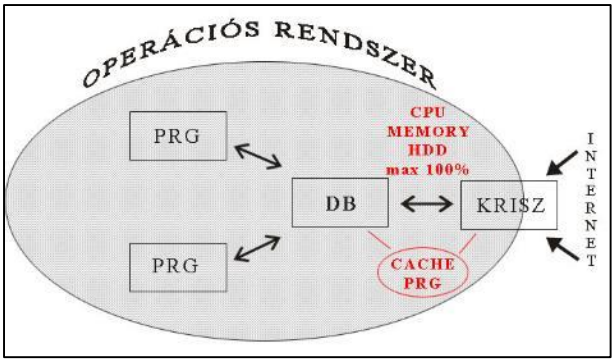
Egyazon operációs rendszeren:

Napjaink - kiszolgálásra fejlesztett - operációs rendszerei a megfelelő hardver-, és erőforrás kapacitás rendelkezésre állása esetén, könnyedén képesek több szolgáltató program együttes futtatására és kezelésére.

Technikailag tehát viszonylag egyszerűen megvalósítható és nagy rendelkezésre állással - is - üzemeltethető egyazon operációs rendszeren több szolgáltatás (1. ábra), azonban ha közöttük van KRISZ és vele függőségi viszonyban álló adatbázis-kezelő is, akkor természetesen mindkettő szerverprogram kiemelt figyelmet érdemel. Fontos, hogy egyik szolgáltatás sem emésztheti fel úgy a rendelkezésére álló erőforrásokat, hogy a másik működésképtelenné váljon, hisz az közvetlenül, vagy közvetetten a KRISZ üzemképtelenségéhez vezet. Ezért elengedhetetlen a rendszerparaméterek folyamatos monitorozása, a finomhangolások elvégzése, és szükség esetén további erőforrás kímélő szolgáltatások üzembe helyezése. A

[3] World Wide Web - világháló
[4] elektronikus üzenet
[5] File Transfer Protocol - állomány átviteli protokoll
[6] Internet protokoll cím, egyedi hálózati azonosító

sikeres erőforrás-gazdálkodás érdekében szinte elkerülhetetlen cache[7] szerver operációs rendszer és/vagy funkcionális program szintű üzemeltetése. A cache használata amellett, hogy nagy leterhelés esetén is képes megfelelő szinten tartani az erőforrásokat, egyben további kockázatot is jelent, hisz a KRISZ alrendszereként [3], üzemképtelensége egyes esetekben a rendszer túlterheléséhez vezethet. Az egyazon operációs rendszeren működő KRISZ és adatbázis-kezelő bármelyikének szolgáltatás/kapacitás bővítését megfontoltan kell végrehajtani, főleg, ha a rendszer erőforrásainak felhasználása előzetesen, átlagos terhelés esetén is eléri a 25 %-os szintet. Miután bármely szolgáltatás működtetése az operációs rendszer támadhatóságának szempontjából is egyfajta kockázatot jelent, a rendszer - bármely szerverprogramon keresztül történő - sikeres birtokba vétele (Owned[8]), megteremti az összes szolgáltatás, köztük a KRISZ leállításának, használhatatlanná tételének a lehetőségét is.

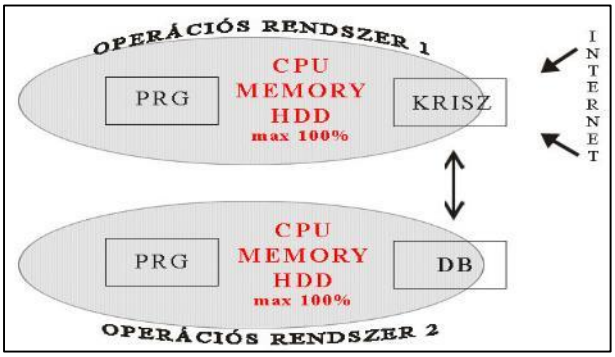


1. ábra. Közös operációs rendszeren

A KRISZ üzemeltetése - mindamellett, hogy kockázatosabb, - természetesen költséghatékonyabb az adatbázis-kezelővel egyazon operációs rendszeren, hisz a fenntartási költségek mind az energia felhasználás, mind az internet elérés szempontjából jelentősen kisebbek.

Különböző operációs rendszeren

A KRISZ-t és az azt kiszolgáló adatbázis-kezelőt - lehetőség szerint - bölcs döntés külön operációs rendszerre telepíteni és úgy üzemeltetni. Fontos megjegyezni, hogy az operációs rendszerek a virtualizációs[9] technológiáknak köszönhetően, akár egyazon hardveren is működhetnek, de az erőforrás felhasználás szempontjából önállóak maradnak. A KRISZ-t vagy az adatbázis-kezelőt célzó támadás az egyenkénti rendelkezésre állás szempontjából közvetlenül nem hat ki a másikra, a KRISZ sikeres működése ugyanakkor feltételezi az adatbázis-kezelő megfelelő rendelkezésre állását.



2. ábra. Különböző operációs rendszeren

[7] gyorsító tár

[8] A hackerek által használt, a rendszer birtokbavételére utaló szleng

[9] "...virtualization is a smorgasbord of technologies that offer organizations many advantages..." [4] - a virtualizáció a technológiák svédasztala, amely számos előnyt nyújt a szevezetek számára

Biztonsági szempontból tehát indokolt a KRISZ és az adatbázis-kezelő külön operációs rendszeren (2. ábra) történő üzemeltetése, azonban a konstrukcióban megoldandó feladat, az operációs rendszerek állandó on-line kapcsolatban tartása és az átvitelre kerülő adatmennyiség függvényében, a szükséges sávszélesség biztosítása. A megfelelő kapcsolat és sávszélesség megteremtése esetén viszont, a két operációs rendszer- és vele együtt a szolgáltatások közötti távolság, a minimálistól a végletekig növelhető. Az összeköttetési kényszerből adódik, hogy a KRISZ-t és az adatbázis-kezelőt működtető operációs rendszerek IP cím-tartományát hálózati konfigurációval összhangban és szinkronban kell tartani. Függetlenül attól, hogy belső-, vagy külső (internetes) címtartományban valósul meg az egységesítés, leszögezhető, hogy a KRISZ alap rendeltetéséből adódóan, az adatbázis-kezelő pedig a KRISZ kiszolgálása miatt nyitott hálózati porttal rendelkezik, tehát hálózaton elérhető, támadható, ezáltal védendő. A KRISZ és az adatbázis-kezelő operációs rendszer szintű szétválasztása esetén lehetséges, hogy az adatbázis szerver másik funkcionális információs rendszert is kiszolgáljon, sőt a gyakorlatban előfordul, hogy a KRISZ egy már működő IT rendszerre kerül illesztésre és kiterjesztésre.

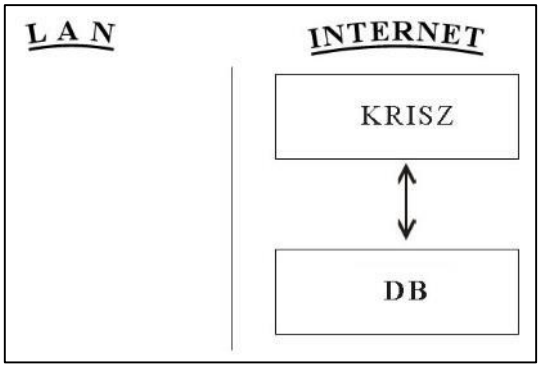
Mivel tehát ebben a megközelítésben több operációs rendszer üzemeltetése szükséges, a vele járó folyamatos - szolgáltatásra is kiterjedő - karbantartási, frissítési és adminisztrációs teendőket egyszerre, az operációs rendszer számának megfelelően több helyen is el kell végezni, valamit az összeköttetést biztosító kapcsolat rendelkezésre állását is gyakran ellenőrizni szükséges.

Hálózat szerinti elhelyezkedés

Napjaink professzionális adatbázis-kezelői hálózati interfésszel rendelkező szerverprogramok, s a KRISZ támogatása - néhány kivételtől eltekintve - szinte csak ezen adatbázis-kezelőkkel valósul meg. A hálózati adatbázis-kezelők üzemeltethetők internet tartományon belüli-, vagy kívüli IP címen, továbbá "localhost"[10]-on, azaz a visszahurkoló - hálózati - interfészen, amely tényleges, a működtető szerveren kívüli hozzáférést nem tesz lehetővé.

Internet tartományon belüli IP címen

Ebben az esetben, a KRISZ mellett az adatbázis-kezelő szolgáltatás is a világháló tartományába tartozó IP címen üzemel (3. ábra). Elsősorban akkor lehet szükség erre a megvalósításra, ha az adatbázis szerver az internet különböző pontjairól, akár nagy távolságokról érkező kéréseket is ki kell, hogy szolgáljon.

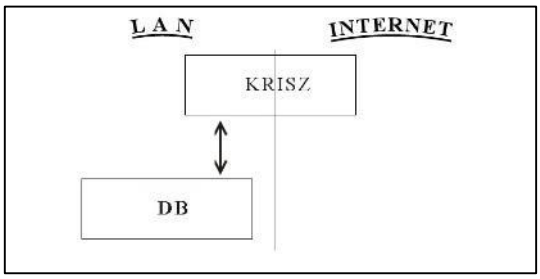


3. ábra. Interneten működő szolgáltatások

Az adatbázis(ok)ban tárolt adatok érzékenysége alapvetően meghatározza egy internetről elérhető adatbázis-kezelő működtetésének kockázatát, azonban érdemes leszögezni, hogy a közvetlen internetes elérhetőség, valamint a nyitott adatbázis-kezelő port, a tárolt adatoktól függetlenül csábítja a rossz szándékkal kapcsolódni vágyókat. Kiindulva abból, hogy a KRISZ nyílt IP címről kerül kiszolgálásra - akár igen magas kapcsolódási számmal is, - a biztonság

[10] A számítógép hálózatokban az egyes munkaállomások saját magukra mutató neve.

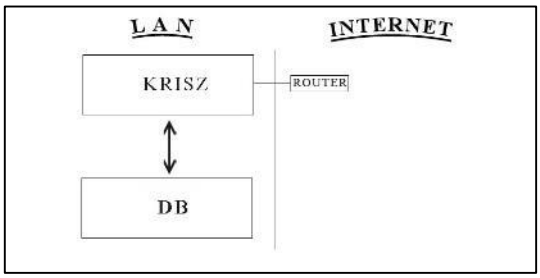
fenntartása érdekében szinte alapkövetelmény a titkosítás megvalósításának minden formája (kapcsolódás, adat-továbbítás), továbbá fontos az adatbázis-kezelő authentikációjának és a megfelelő jelszavak használatának a kikényszerítése. Az adatbázis-kezelő közvetlen internetes elérhetősége komoly kockázattal jár, nyomós érvként csupán a nagy távolságok áthidalásával elérhető költségtakarékosság, valamint egyéb feloldhatatlan kötöttségek, úgymint a szerver hozzáférésből adódó korlátozás hozhatók fel. A gyakorlat sajnos azt mutatja, hogy rossz, vagy figyelmetlen konfiguráció eredményeként is működnek nyitott port-tal adatbázis-kezelők az interneten, gyakran az üzemeltető tudta nélkül is.



4. ábra. LAN-ba rejtett adatbázis-kezelő

Internet tartományon kívüli - privát - IP címen

Az internet mögötti, "belső" LAN[11] hálózatban működő szolgáltatások alkalmazásának létjogosultsága pontosan az, hogy a külvilág elől rejtve működjenek, az internetről közvetlen hálózati porton ne legyenek elérhetők (5. ábra).



5. ábra. LAN-ba rejtett szolgáltatások

Ahhoz azonban, hogy egy internet tartományban üzemelő KRISZ kapcsolatba léphessen egy belső hálózatba rejtett adatbázis-kezelővel, a hálózati szinkronizációt meg kell oldani, azaz a KRISZ-t működtető operációs rendszernek olyan hálózati interfésszel - is - kell rendelkeznie, amely rálátással bír az adatbázis-kezelőhöz rendelt hálózati pontra. A megoldásra több lehetőség is kínálkozik, hisz a KRISZ szerverét akár több hálózati interfésszel is lehet konfigurálni, melyek közül egyik az internet, a másik pedig a belső hálózati kapcsolatot biztosíthatja (4. ábra). Megoldást jelenthet a KRISZ és az adatbázis-kezelő együttes LAN-ba "rejtése", amely biztonságos(abb) környezetben, egyszerűbb hálózati szinkronizációval megvalósítható működést biztosít, ugyanakkor a KRISZ internetes elérhetősége miatt forgalomirányítási kényszert jelent.

IP cím nélkül

Tekintettel arra, hogy a kizárólag "localhost"-on figyelő és a hálózati támogatással nem rendelkező adatbázis-kezelők elérhetősége hálózati pontról egyaránt kizárt, őket a hálózati elhelyezkedés szempontjából egy kategóriába sorolom, ugyanakkor megjegyzem, hogy működésük és a KRISZ-hez történő kapcsolódásuk teljesen eltérő. Amíg előző esetben a

[11] Local Area Network - helyi hálózat

"localhost"-on hálózati jellegű a kapcsolat, addig utóbbi esetben a kapcsolódás file-rendszer szintű. Az IP cím nélküli adatbázis-kezelő és a KRISZ biztosan egy operációs rendszeren fut és az adatbázis-kezelő hálózati kapcsolat hiányában, közvetlenül csak és kizárólag a lokálisan futó programokat tudja kiszolgálni. Ebben a konstrukcióban a fentiekben az "azonos operációs rendszer" témakörben már taglalt problémák szintén fennállnak, azzal a kitétellel, hogy az adatbázis-kezelő szolgáltatás csak közvetlenül - a KRISZ-en keresztül - érhető el és esetleg támadható.

Kapcsolódás, megvalósítás

Az adatbázis-kezelőnek és a KRISZ-nek egyaránt kapcsolódási képességgel kell rendelkeznie ahhoz, hogy egymás irányába adatokat tudjanak küldeni és fogadni, amely képesség szükségszerűen az egymáshoz viszonyított - fentiekben taglalt - elhelyezkedéstől függ.

Adatbázis-kezelő ——> "KAPCSOLÓDÁSI KÉPESSÉG" <—— KRISZ

A "KAPCSOLÓDÁSI KÉPESSÉG" lehet mindkét oldal binárisan kódolt-, vagy moduláris fejlesztés eredményeként ki-be kapcsolható funkciója, amelynek aktivizálásával a kapcsolat az alábbiak szerint jöhet létre.

Hálózati porton keresztül

Az adatbázis-kezelő hálózati port-on fogadja a kéréseket, amelyhez a KRISZ - a rálátási képesség függvényében, - általában valamelyik modulján keresztül kapcsolódást kezdeményez, majd a megfelelő jogosultság esetén a hálózati kapcsolat létrejöhet. A különböző adatbázis-kezelőkhöz eltérő a kapcsolódás és a kommunikáció protokollja, ezért a gyártók általában biztosítják a megvalósításhoz szükséges fejlesztői környezetet, vagy az előre megírt programokat, könyvtárakat, függvényeket.

Operációs rendszer közös pontján keresztül (socket[12], memória, file rendszer)

Az adatbázis-kezelő az operációs rendszer valamely KRISZ által is elérhető pontján keresztül biztosítja a kapcsolódás lehetőségét, amelyhez a KRISZ az adatbázis-kezelő specifikációjának megfelelően modulja segítségével kapcsolódást kezdeményez. Ez a közös pont lehet egyszerűen file, vagy a rendelkezésre álló memória egy bizonyos lefoglalt, fenntartott területe.

A feltételek rendelkezésre állása esetén tehát, a megfelelő konfiguráció alkalmazásával, a KRISZ és az adatbázis-kezelő kapcsolata létrejöhet. Ez a metódus általában még csak a kapcsolódás lehetőségét biztosítja, az adatbázis-kezelőben tárolt adatokhoz történő tényleges hozzáférés rendszerint további eredményes authentikációt követően valósulhat meg. A modern adatbázis-kezelők jogosultsági szintje rétegesen szabályozott

- a kapcsolat létrehozására,
- az adatbázishoz történő hozzáférésre,
- az adott adatbázis tábláihoz történő hozzáférésre,
- az adatbázisban tárolt adatok kezelésére (lekérdezés, módosítás, törlés, stb..),
- az adatbázis, a táblák és a mezők struktúrájának, szerkezetének módosítására,
- a rendelkezésre álló jogok továbbadására vonatkozóan.

A jogosultságok beállítására a fentiek rendelkezésre állása esetén viszonylag nagy a mozgástér, amely feladat általában az adatbázis-kezelőt üzemeltető rendszeradminisztrátorra hárul. Fontos megjegyezni, hogy a gyakorlatban az adatbázis-kezelő rendszeradminisztrátora - a felsőbb szintű jogosultságok beállításával - adott adatbázisra vonatkozóan rendszerint tovább delegálja a felhasználók kezelését és egyúttal a felelősséget is a KRISZ üzemeltetőjének.

[12] "Egy gyakran alkalmazott szállítási réteg interfész a Berkeley-csatlakozók (sockets) által nyújtott interfész." [5]

Amennyiben az adatbázisokra, táblákra, oszlopokra vonatkozóan nem történik további hozzáférés szűkítés vagy pontosítás, azaz a KRISZ minden tranzakciót ugyanannak a túlzottan sok jogosultsággal rendelkező felhasználónak a nevében végez(tet), úgy a KRISZ - esetleges - gyenge pontjain keresztül az adatbázisokban tárolt adatok védtelenné válhatnak.

A sikeres kapcsolódást követően, a KRISZ - általában az adatbázis kezelést biztosító modulján keresztül - a rendelkezésre álló jogosultságoknak megfelelő tranzakciókat képes végrehajtani.

Kritikusság

Az online magyar értelmező szótár definíciója alapján, a kritikusság egyik melléknévi definíciója "Kétséges kimenetelű (helyzet, állapot, időszak, időpont), amely egy fennálló helyzetben, állapotban sorsdöntő fordulatot hozhat, egy folyamat menetét, sorsát döntően alakíthatja, befolyásolhatja, megszabhatja; válságos." [6]; míg a Révai Nagylexikon szerint "döntő, válságos, veszélyes" [7] a szó jelentése.

A "kritikus internetes szolgáltatás" fogalom fentiek szerinti értelmezése egy olyan interneten megjelenő szolgáltatás, amelynek működése kétes kimenetelű is lehet, magában hordozza a veszélyt, megvan az esélye a kedvezőtlen állapotváltozásnak, ami akár válságos helyzet kialakulásához is vezethet.

Kérdésként merül fel, hogy az adatbázis-kezelő és a KRISZ közötti kapcsolat megszakadása, vagy az adatbázisban tárolt adatok kiszivárgása, esetleg az adatok kompromittálódása, mennyire idézi elő a kedvezőtlen - esetleg válságos - állapotot?

Figyelemmel arra, hogy a KRISZ alrendszereként működő adatbázis-kezelőben akár a szolgáltatáshoz szükséges összes információ is eltárolható függetlenül annak végső formájától (kép, hang, állomány stb..), megállapítható, hogy az adatbázis-kezelő olyan mértékben kritikus pontja a rendszernek, amennyire a benne tárolt adatok befolyásolják a szolgáltatás sikerességét.

AZ ADATBÁZIS-KEZELŐK ELŐFORDULÁSA A RENDVÉDELEM KRITIKUS INTERNETES SZOLGÁLTATÁSAIBAN

Napjainkban a rendvédelmet irányító kormányzatban, annak háttérintézményeiben és magában a rendvédelemben is egyre nagyobb hangsúlyt kapnak azok az interneten elérhető szolgáltatások, amelyek bevezetését követően a használat kötelező érvényűvé válhat a bevont szervek, vagy akár a társadalom szélesebb körű szereplői részére egyaránt.

Az internetes megjelenés természetesen lehet védett, például virtuális magánhálózatba, vagy szolgáltatók által - garantáltan - szegmentált hálózatba rejtett, vagy bárki által elérhető, teljesen nyilvános. A kritikus internetes szolgáltatások ismérveiben [8] megfogalmazott feltételek teljesülése, azaz a szolgáltatás szükségessé, kritikussá válása esetén, egyrészt teljesülnie kell(ene) az állandó rendelkezésre állás követelményeinek, másrészt az adatbázis-kezelő - mint háttérszolgáltató alrendszer - jelenléte további védelmi intézkedések bevezetését követeli meg.

A teljesség igénye nélkül bemutatásra kerülő alábbi internetes szolgáltatások mindegyike a rendvédelemhez tartozik, működésük elvárt, hisz társadalmi és/vagy kormányzati célt szolgál.

Elektronikus levelező rendszerek

A rendvédelemben - és a kormányzatban - használt elektronikus levelező rendszerek többnyire a „gov.hu” domain tartomány részeként, a szervezetre vonatkozó sub-domain alkalmazásával működnek, a kiosztott email címek pedig több esetben a postafiókot használó személyek vezeték-, és keresztneveiből származtatódnak.

A Microsoft platformon biztosított levelezés eredményeként, a végfelhasználók az OWA[13] webmail rendszeren keresztül képesek leveleket küldeni és fogadni, postafiókjaikat kezelni. A rendszer elérhetősége a szervezetek intranet hálózatából és a világhálóról egyaránt lehetséges, ami magában foglalja az állandó rendelkezésre állás-, és az internet irányából bekövetkező támadások elleni védekezés szükségességét.

A levelező felhasználók accountjai Active Directory[14] címtár adatbázisban tárolódnak, ami ugyan nem egy klasszikus adatbázis-kezelő rendszer, de egy speciális adatbázis, amit maga a Microsoft is megerősít: "Active Directory is a special-purpose database — it is not a registry replacement." [9]

Tényként fogadható el, hogy a rendvédelem feladat-meghatározó és jelentési rendszere leginkább az elektronikus levelezésre támaszkodik, amely önmagában is kritikus információs infrastruktúra, hisz leállásával a szervezeti kommunikáció "lefagy". Azzal azonban, hogy az elektronikus levelezés interneten megjelenő, háttér adatbázissal rendelkező webmail alapú rendszer, azt kritikus internetes szolgáltatásnak tekinthetjük. Rövid - nyilvános - keresés után, az alábbi interneten elérhető, rendvédelemi webmail rendszerek címeit lehet megtalálni:

- https://webmail.katved.gov.hu/owa/ (Katasztrófavédelem)
- http://webmail.police.hu/ (átirányítva az alábbira)
- https://amids.police.hu/nidp/app (Országos Rendőr Főkapitányság)
- https://webmail.tek.hu (Terror Elhárítási Központ)
- https://webmail.bm.com/owa (Belügyminisztérium)
- https://mail.bv.gov.hu/owa (Büntetés-végrehajtás)
- https://mail.hm.gov.hu/owa (Honvédelmi Minisztérium)

A webmail szolgáltatásokat különböző - azonban hasonló IP tartományban üzemelő - szerverek biztosítják, amelyet az URL[15]-ek névfeloldása bizonyít. A szerverek hálózati IP címének scennelése azt mutatja, hogy a Web és az Email szolgáltatások mellett - nagy valószínűséggel - egyéb hálózati kiszolgálás nem üzemel, ami azt jelzi, hogy a felhasználói adatbázis a nyilvánosság elöl rejtett, tehát közvetlenül nem érhető el.

Adatbázis alapú egyéb rendszerek

A rendvédelmi portálokon végzett rövid böngészés után, az alábbi adatbázis alapú, kritikusnak tekinthető weboldalak voltak megtalálhatók[16]:

- https://kozigbirsag.police.hu/

Jogszabály alapján, tájékoztató az objektív felelősség hatálya alá tartozó szabályszegések elkövetése miatt folytatott közigazgatási eljárás adatairól.

- http://kirportal.police.hu/koral-1.0/page/szemelydetails.xhtml

Kőrözési al-portál.

- https://www.etdr.gov.hu/

Építésügyi hatósági engedélyezési eljárásokat támogató elektronikus dokumentációs rendszer, az e-közigazgatás szolgáltatása.

- http://rvv-rvki.hu

Rendészeti Vezetőképzési, Továbbképzési és Vizsgaportál; Rendészeti feladatokat ellátók képzése és vizsgáztatása (2014.01.30-án 14.621, 2014.11.17-én 22.479 regisztrált felhasználóval)

- https://monitoringadatszolgaltatas.bm.hu/default.aspx

Pályázatokkal kapcsolatos, kötelező érvényű adatszolgáltatási rendszer.

---

[13] http://en.wikipedia.org/wiki/Outlook_Web_App - Outlook Web Access / Outlook Web App
[14] http://hu.wikipedia.org/wiki/Active_Directory
[15] http://hu.wikipedia.org/wiki/URL - **U**niform **R**esource **L**ocator - egységes erőforrás-azonosító
[16] 2014.11.17-i állapot

– https://www.parbeszed.hm.gov.hu/
Honvédelmi Minisztérium - Párbeszéd Portál

A weboldalak mindegyike valamilyen felhasználó-, vagy jogosultság-azonosításhoz kötött, adatbázisból dolgozik, ugyanakkor a fenti webmail rendszerekhez hasonlóan az adatbázis-kezelő rejtett, tehát közvetlenül nem érhető el.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Dolgozatomban kísérletet tettem annak bemutatására, hogy az adatbázis-kezelő rendszerek nélkülözhetetlen "kellékei" korunk információs társadalmának és vele együtt annak eredményeként, valamint következményeként, a kritikus internetes szolgáltatásoknak is. Bemutattam, hogy milyen relációban alkalmazhatók az adatbázis-kezelők a KRISZ mellett és azoknak milyen előnyei, vagy hátrányai vannak. A felkutatott URL-ek bizonyítják, hogy számos adatbázis alapú kritikus internetes szolgáltatás működik a rendvédelemben, amelyek a társadalom és a kormányzat szereplőinek egyaránt rendelkezésre állnak. Látszik, hogy az internet adta lehetőségeket a rendvédelem is egyre inkább (ki)használja, ugyanakkor megállapítható, hogy a rendelkezésre álló szolgáltatások egymástól elszigeteltek, azonban összefüggés közöttük, hogy a szerverek hasonló IP tartományba tartoznak, amely központosított információbiztonsági háttérre, azaz kormányzati hálózati felügyeletre utal. A centralizálásnak előnye az egységesített védelmi intézkedések alkalmazása, ugyanakkor hátránya lehet, hogy az érintett rendvédelmi szervek bízva a hozzáértőkben, a helyi (kiber)biztonsági intézkedéseket elodázzák.

Felhasznált irodalom

[1] Szelezsán János - Adatbázisok, LSI Oktatóközpont ISBN 963 577 189 4

[2] http://www.portfolio.hu/vallalatok/it/elkepeszto_mennyi_adat_letezik_mire_lehet_felhasznalni.186053.html - letöltve 2013.11.23

[3] Jéri Tamás - A kritikus internetes szolgáltatások alrendszerei Társadalom és Honvédelem, 2013/3-4. szám, NKE Budapest, ISSN 1417-7293

[4] Dan Kusnetzky: Virtualization: A Manager's Guide, ISBN 978-1-449-30645-8 O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472 United States of America, 2011.

[5] Andrew S. Tanenbaum: Számítógép-hálózatok, ISBN 963 545 384 1 Panem Könyvkiadó Kft., Budapest 2004.

[6] WikiSzótár.hu magyar értelmező szótár http://wikiszotar.hu/wiki/magyar_ertelmezo_szotar/Kritikus - letöltve 2014.01.25

[7] Révai nagy lexikona - pdf változat http://mek.oszk.hu/06700/06758/pdf/revai12.pdf - letöltve 2014.01.25

[8] Jéri Tamás - Kritikus Internetes Szolgáltatások Hadmérnök, VIII. Évfolyam 1. szám 2013. március, NKE Budapest, ISSN 1788- 1919 http://hadmernok.hu/2013_1_jerit.pdf - letöltve 2014.01.25

[9] http://msdn.microsoft.com/en-us/library/windows/desktop/aa746492%28v=vs.85%29.aspx - letöltve 2014.01.29