HADMÉRNÖK

IV. Évfolyam 4. szám - 2009. december

Fleiner Rita
fleiner.rita@nik.bmf.hu

ADATBÁZISOK ELLENI FENYEGETÉSEK RENDSZEREZÉSE

Absztrakt

A publikáció az adatbázisok biztonságát fenyegető támadások rendszerezésével foglalkozik. Az adatbázis-biztonság alapfogalmainak értelmezése után különböző rendszerezési kategóriák kerülnek ismertetésre, majd a támadási pontok szerint jellegzetes adatbázis fenyegetések bemutatása történik meg.

The publication studies the taxonomies of the database security threats. After discussing the basic terms of database security, we present different methods for the classificaton of the database security threats, then according to the point of the attack we present typical database attack methods.

***Kulcsszavak**: adatbázis-kezelő rendszer, adatbázis fenyegetés, adatbázis-biztonság ~ database management system, database security threat, database security*

Bevezetés

Napjainkban az informatikai rendszerek jelentős részének működésében lényeges szerepet játszanak különböző adatbázisok. Az adatbázis adatoknak számítógépekben tárolt, valamely adatmodell szerint strukturált gyűjteménye. Az adatbázisokban tárolt adatok kezelését speciális alkalmazások, az úgynevezett adatbázis-kezelő rendszerek biztosítják, melyek több felhasználós, hálózatos környezetben működnek. Adatbázis szervernek nevezzük az egy vagy több adatbázis-kezelő rendszert futtató számítógépet.

Az adatbázisok biztonságának megsértése (működésképtelenné tétele, meghamisítása, a tárolt adatok jogtalan megismerése) az adott informatikai rendszer és az általa nyújtott szolgáltatás

biztonságát fenyegeti. Ebből következően lényeges kérdés az adatbázisok megfelelő védelme, melyhez ismernünk kell az adatbázisok biztonságát veszélyeztető fenyegetések különböző formáit.

Jelen publikáció értelmezi az adatbázis-biztonság alapfogalmait, különböző kategorizálási szempontrendszert ad meg az adatbázis fenyegetéseinek osztályozásához, majd a támadási pontok szerint jellegzetes adatbázis fenyegetéseket gyűjt össze.

Adatbázis-biztonság alapfogalmai

Általános értelemben a fenyegetés olyan potenciálisan káros, vagy meg nem engedett hatás, amely a védendő objektumot károsan, egy megengedett mértéknél jobban befolyásolja. A fenyegetés érintheti a védendő objektum létét, érdekeit, állapotát, működését, vagy valamely tulajdonságát. A fenyegetések bekövetkezését a különböző sebezhetőségek teszik lehetővé. A sebezhetőség a biztonság alanyának egy olyan tulajdonsága, hiányossága, vagy gyengesége, amely lehetőséget teremt egy fenyegetés megvalósulására. [1]

A publikációban az adatbázisok információs jellegű fenyegetésit vizsgáljuk. Ehhez szükséges az adatbázis-biztonság fogalmának tisztázása, ezen belül az adatbázis-biztonság alanyának és ennek védendő tulajdonságainak meghatározása. Az adatbázis-biztonságot az informatikai biztonság részének tekintjük.

Az adatbázis-biztonság fogalmának nincs széleskörűen elfogadott értelmezése. Az egyik típusú értelmezés szerint az adatbázis-biztonságot a tárolt adatok biztonsága jelenti, ezen belül az adatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása, az adatbázis-kezelő rendszerekről ez a hozzáállás nem tesz említést. Ezt a szemléletmódot tükrözik a több kiadást megélt, felsőoktatásban is használt adatbázis témájú szakkönyvek [2, 3]. A másik típusú értelmezés a tárolt adatokat és az ezeket kezelő adatbázis-kezelő rendszert tekinti a biztonság védendő objektumának, ezt a hozzáállást megtalálhatjuk például az USA Védelmi Minisztériuma által kiadott Adatbázis-biztonság Technikai Megvalósítási Útmutatóban [4]. Mivel a témát a kritikus infrastruktúra védelem, illetve az informatika biztonság megvalósítása oldaláról is tanulmányozom, az adatbázis-biztonság fogalmába mind a tárolt adatok, mind az azokat kezelő adatbázis-kezelő rendszerek biztonságát is beleértem.

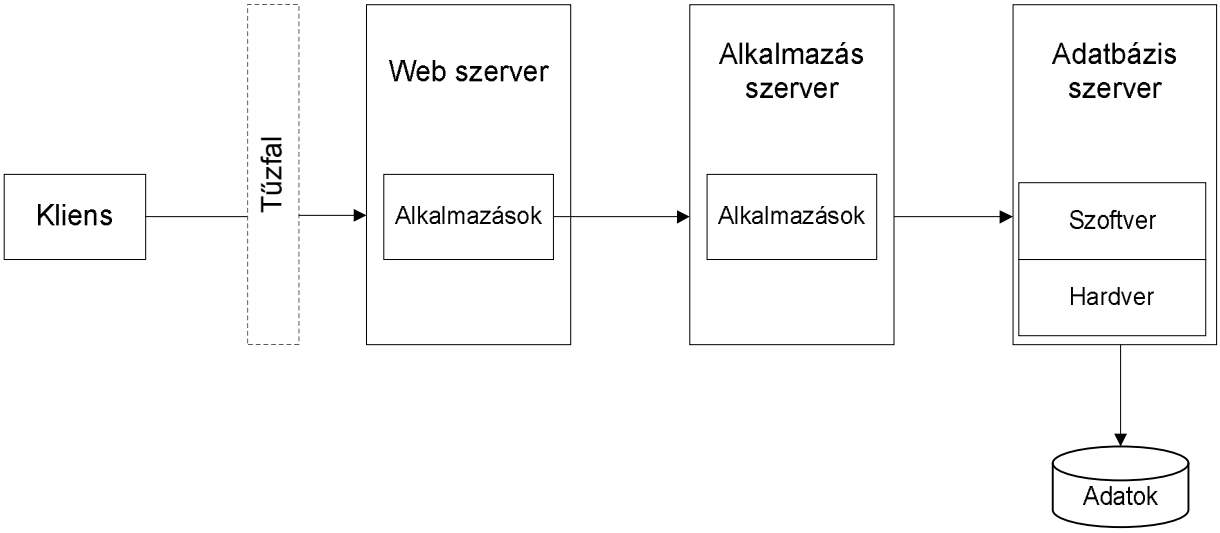
A biztonság alanyának meghatározása mellett szólni kell a védendő tulajdonságok halmazáról is, amik természetesen konkrét alkalmazások és környezetek esetén eltérőek lehetnek. Az adatbázisok védelme szempontjából a bizalmasság, sértetlenség és rendelkezésre állás biztosításának követelménye jelenhet meg. [5]

Adatbázisok nézőpontjából a bizalmasság: annak biztosítása, hogy az adatok csak az arra jogosultak számára legyenek elérhetőek, a bizalmasság elvesztése az információ illetéktelenek általi hozzáférését, megismerését jelenti. A sértetlenség azt jelenti, hogy a tárolt adatot, illetve az adatbázis-kezelő rendszert csak az arra jogosultak változtathatják meg, azok észrevétlenül nem módosulhatnak és nem törölhetők. A rendelkezésre állás annak biztosítása, hogy a felhatalmazott felhasználók hozzáférjenek a szükséges adatokhoz. A rendelkezésre állás megsértése azt jelenti, hogy az adatokhoz, illetve az adatbázis-kezelő rendszerhez való hozzáférés egy adott időtartamra

nézve ellehetetlenül vagy teljes mértékben megszűnik.

A letagadhatatlanság és a hitelesség biztonsági kritériumait adatbázisokkal kapcsolatban ritkán említik, ezek a sértetlenség biztonsági tulajdonság részének tekinthetők. A letagadhatatlanság az a biztonsági tulajdonság, amely megfelelő bizonyítékokkal szolgál az adatbázis-kezelő rendszerben végrehajtott tevékenységek későbbi ellenőrizhetőségét illetően, ezt auditálhatóságnak is szokták hívni. A hitelesség az adat forrásának, eredetének a valódiságát jelenti.

Az adatbázisokat tartalmazó rendszerek felépítése nagyon összetett és változatos lehet. Az alábbi ábra egy olyan részstruktúrát mutat be, mely bonyolultabb rendszerekben is építő elem lehet. Ezt a struktúrát is szem előtt tartva fogjuk a fenyegetések rendszerezését elvégezni.



1. ábra: Adatbázisokat tartalmazó rendszerek architektúrája

Az architektúrában a kliens nem közvetlenül fordul az adatbázis-kezelő rendszerhez, hanem egy alkalmazást használ, ami az adatbázis adataihoz való hozzáférést is elvégzi. Az ábrán egy tűzfal látható a web szerver előtt, a gyakorlatban azonban az architektúra több pontján is előfordulhat. Gyakran az adatbázis-kezelő rendszereket futtató számítógépeket is tűzfal védelemmel látják el. A kliens tehát a web szerveren, alkalmazás szerveren és adatbázis szerveren keresztül éri el az adatokat. Az adatbázis szerver esetén berajzoltuk a hozzá tartozó platformot is, amit hardver és szoftver részekre osztottunk fel. Ezt persze a többi komponensre is bejelölhetnénk, de az adatbázis támadások szempontjából ennek van különösebb jelentősége.

A struktúra persze módosulhat, ha például több adatbázis szerver kommunikál egymással, gondoljunk az osztott adatbázis rendszerekre, vagy a magas rendelkezésre állás biztosítására kiépített fürtözött vagy tükrözött struktúrákra.

Szempontrendszerek az adatbázis fenyegetések osztályozásához

Mivel az adatbázisokban koncentráltan található érzékeny, kritikus információ, az adatbázisok védelme fontos feladattá vált. Az adatbázisok az architektúra legutolsó pontján, tűzfalak védelmével ellátva helyezkednek el, ezért sokáig ezek védelme az informatika biztonsági feladatok között nem szerepelt prioritásként. Mára a helyzet megváltozott. Egyrészt a webes alkalmazások elterjedtével támadásuk könnyebbé vált, a behatolók ellen kevésbé vannak elrejtve, másrészt integritásuk megsértése bizonyos esetekben helyreállíthatatlan vagy nagyon problémásan helyreállítható helyzetet teremtene, illetve törvényi előírások is létrejöttek az adatok védelme érdekében. Egyre elterjedtebb igény, szükség jelentkezik vállalati szinten adatbázis biztonsági terv készítésére az adatvagyon védelme érdekében. A védelem megtervezéséhez fontos ismerni, hogy milyen veszélyek ellen lehetnek az adatbázisokat kitéve.

Az adatbázis fenyegetések rendszerezésével a célunk olyan rendszerezési kategóriák felállítása, melyek segítségével számbavehetők, áttekinthetők az általunk vizsgált fenyegetések. Olyan kategorizálási szempontokat keresünk, melyek egyértelmű besorolást tesznek lehetővé.

Osztályozni lehet a fenyegetéseket a támadó adatbázishoz való viszonya szerint. Adatbázis fenyegetések esetén vizsgálható, hogy külső vagy belső támadás zajlott-e le. Komoly felmérések, tanulmányok készültek annak kimutatására, hogy ezek közül melyik a gyakoribb probléma egy szervezet esetében. Több tanulmány egész magas százalékot hoz ki a belső fenyegetések javára. A belső-külső kategóriák jelentésének meghatározása nem is olyan egyszerű, mint első ránézésre hinnénk. Belső támadásnak definiálhatjuk az adatbázist üzemeltető személyek által elkövetett támadást, melyben a támadó a számára megadott jogosultsággal él vissza, azokat nem rendeltetésszerűen használja.

Kategorizálhatunk egy támadást az elkövető indíttatása szerint, azaz a kivitelezője elkövetheti ezt szándékosan vagy véletlen folytán.

A támadásokat kategorizálhatjuk aszerint, hogy mely biztonsági tulajdonság sérülését okozhatja. Azaz a bizalmasság, a sértetlenség vagy a rendelkezésre állás biztonságát veszélyezteti-e. A sértetlenség és rendelkezésre állás esetén megvizsgálható, hogy az adatokon történt meg a negatív kölcsönhatás vagy pedig az adatbázis-kezelő rendszert érintette. Például a rendelkezésre állás megsértése esetén az adatok megsemmisítése miatt vagy pedig az adatbázis-kezelő rendszer megváltoztatása miatt vált az adatbázis elérhetetlenné. A sértetlenség megsértésekor szintén megvizsgálható, hogy az adatokon vagy az informatikai rendszerben történt meg az illetéktelen módosítás. Egy fenyegetés több biztonsági tulajdonság megsértését kiválthatja, így egyszerre több kategóriához is hozzárendelhető.

Végül vizsgálhatjuk az adatbázis fenyegetéseket a lehetséges támadás architektúrában elfoglalt helye szerint is. Szem előtt kell tartanunk, hogy csak azokat a fenyegetéseket rendszerezzük, vesszük számba, melyek az adatbázisban tárolt adatokat vagy az adatbázis-kezelő rendszer működését veszélyeztetik.

Az adatbázis-biztonság helyzetét mérő kockázat elemzések egyik célja annak azonosítása, hogy a szervezet adatvagyonát hol veszélyeztetik a támadások leginkább. Ebből a nézőpontból tekintve ennek a csoportosításnak a jelentősége nagy. Az adatbázisokat veszélyeztető fenyegetések az architektúra négy pontjáról indulhatnak. Ennek alapján megkülönböztethetőek a

hálózat, az alkalmazások, a platform és az adatbázisok sérülékenységeire építő fenyegetések.

Hálózati fenyegetésének tekintjük azokat a lehetséges támadási módokat, melyek az adatbázis szerverek, illetve adatbázis állományokat tartalmazó háttértárak közötti kommunikáció támadására alapulnak, vagy pedig a hálózat tetszőleges pontján lépnek fel és az adatbázisok rendelkezésre állását vagy sértetlenségét támadják meg. Az adatok bizalmasságának hálózati úton való támadása már nem tartozik a rendszerezésünk tárgyába.

Az alkalmazásokban rejlő sebezhetőségek, programozási hiányosságok az adatbázis fenyegetések egy fontos csoportját jelentik, ebbe a kategóriába eső támadások különös tekintettel a webes alkalmazások használatának elterjedésével váltak gyakorivá.

A platform fenyegetései alatt a hálózatba kötött szerverek és felhasználói számítógépek hardver és szoftver komponenseinek sebezhetőségeit értjük. Mivel csak az információs úton történő támadásokat vizsgáljuk, az operációs rendszer és egyéb rendszerprogramok hibáit kihasználó fenyegetések tartoznak ebbe a kategóriába, különös tekintettel az adatbázis szervereket futtató platformok sebezhetőségeire.

Az adatbázisok felőli támadási pont az adatbázis-kezelő rendszerben, illetve a tárolt adatokban rejlő sérülékenységeket kihasználó fenyegetések induló pontja. A következő fejezetben a támadási pontok szerinti jellegzetes fenyegetéseket vizsgáljuk meg.

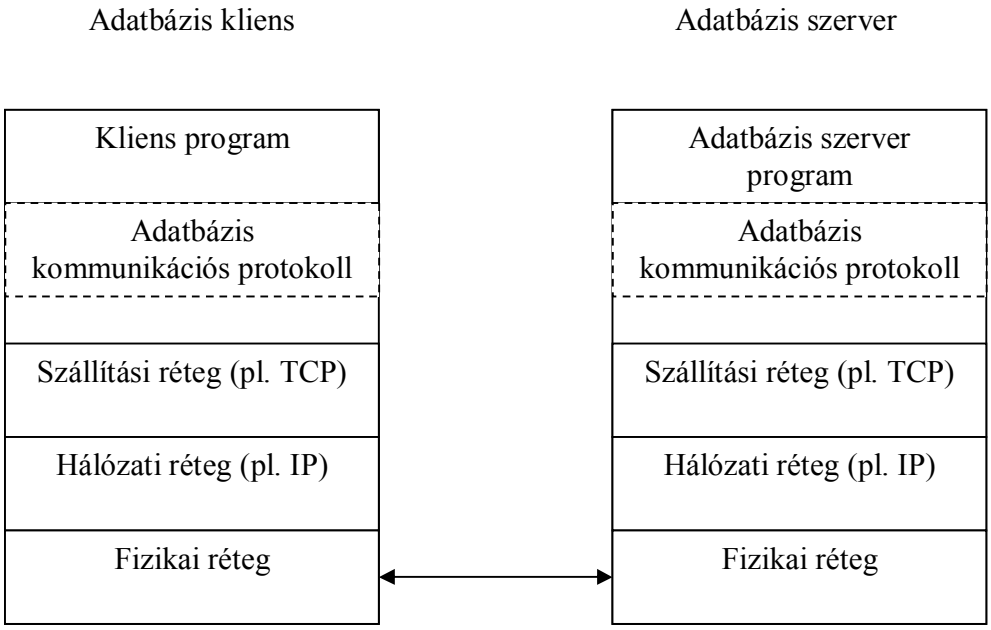
Jellegzetes adatbázis fenyegetések a támadás pontja szerint

Hálózati infrastruktúra sebezhetőségei

A hálózati fenyegetések kategóriájába tartoznak az OSI modell szerinti hálózati-szállítási réteg lehetséges támadásai, illetve az adatbázis-kezelő rendszer hálózati protokolljának támadásai. A támadások technikái épülhetnek a hálózati adatforgalom lehallgatására, beékelődéses (man in the middle) támadási módszerre (melyet például a forráscím meghamisításával lehet megvalósítani), szolgáltatás megtagadása típusú támadásra (például a SYN csomagok elárasztásának módszerével), de akár a puffer túlcsordulásos hiba kihasználására is.

A hálózati adatforgalom lehallgatásának veszélye megjelenik az adatbázisok magas rendelkezésre állásának megvalósításánál (adatbázis tükrözés, fürtözés), ahol adatbázis szerverek kapcsolódnak hálózaton keresztül. Az adatbázis szerverek közötti adatforgalom titkosítás nélkül (vagy gyenge titkosítással) áramlása esetén az adatok lehallgathatóak, ezzel pedig adatbázisok tartalma kerülhet illetéktelenül támadók birtokába.

Pár évvel ezelőtt az adatbázis szerverek elleni új támadási vektor jelent meg, méghozzá az adatbázisok kommunikációs protokolljában rejlő sebezhetőségekre építve [6]. A támadás mindhárom biztonsági tulajdonság megsértését okozhatja. Az adatbázisok kommunikációs (vagy más néven hálózati) protokolljai az OSI modellben a hálózati-szállítási réteg és az alkalmazás réteg között helyezkednek el az alábbi ábra szerint:



2. ábra: Az adatbázis kommunikációs protokoll elhelyezkedése

Az SQL adatbázis lekérdező nyelv a kliens-szerver kommunikációhoz szükséges folyamatokat nem definiálja, ezeket az adatbázis-kezelő rendszer hálózati protokollja látja el. Például a kliens kapcsolat (client session) létrehozása, a parancsok (autentikációs, lekérdezés, kontroll információ) klienstől szerverhez való eljuttatása, az adatok és a lekérdezés státuszának klienshez való eljuttatása az adatbázis hálózati szoftverének a feladata.

Az adatbázisok hálózati szoftvereit (nem szükségszerűen, de a gyakorlat alapján) az adatbázis-kezelő rendszerek gyártói fejlesztik (például Oracle esetében Oracle Net-nek hívják), kódjaik általában nem nyilvánosak és számos sebezhetőséget hordoznak magukban. Bejelentett kommunikációs protokoll sebezhetőségek alapultak az üzenet struktúrájának elrontására, mező méret megváltoztatására, mező tartalmának manipulálására, illetve üzenet sorszámának meghamisítására.

A támadás kivitelezéséhez a támadónak vagy egy saját programot kell írnia, amivel a manipulált üzeneteit elküldi a szervernek és feldolgozza a kapott választ addig a pontig, amíg a káros hatás bekövetkezik vagy pedig egy TCP proxy segítségével be kell ékelődnie a kliens és a szerver közé, és ebben a pozícióban az elkapott üzeneteket megfelelően módosítva kell továbbítania. TCP proxy: a kliens-szerver kommunikációba ékelődik be, a TCP csomagokat megjeleníti, változtatás nélkül továbbítja, illetve szükség esetén módosítva küldi tovább.

Alkalmazások sebezhetőségei

Az alkalmazásokban rejlő sebezhetőségek, programozási hiányosságok az adatbázis támadások egy fontos csoportját jelentik, melyek mögött elsősorban a felhasználói inputok ellenőrzésének hiánya áll. Sérülékenységet jelent még a hibaüzenetek nem megfelelő kezelése, az adatbázis elérések nem megfelelő megvalósítása és a naplózás hiánya is.

A felhasználói inputok ellenőrzésének hiánya puffer túlcsordulásos, SQL injekciós, illetve XSS (cross-site scripting) támadásra adhat lehetőséget. Mindhárom támadási módszerrel kiváltható a rendelkezésre állás, a sértetlenség illetve a bizalmasság megsértése.

Alkalmazások a felhasználók számára megjelenített hibaüzeneteikben adatbázisra, illetve az adatbázis szerverre jellemző információkat fedhetnek fel, ami támadások felépítéséhez ad segítséget, ezáltal sérülékenységi pontot jelent.

Egy adott alkalmazás az adatbázis szervert mindig egy (esetleg több) adatbázis felhasználó nevében éri el. Ha az alkalmazás tulajdonosként vagy superuserként csatlakozik az adatbázishoz, sérülékenységet jelent, mivel bármilyen utasítást és lekérdezést lefuttathat, pl. a szerkezeti módosítást (táblák megszüntetése) vagy táblák komplett törlése. Mindig a lehető legkevesebb jogosultsággal rendelkező, az alkalmazás számára önálló és testreszabott felhasználókat kell használni. Ekkor, ha a behatoló meg is szerez valamilyen jogosultságot (hitelesítési információt), akkor is csak akkora változást tud okozni, mint az alkalmazás maga.

Az alkalmazás szintjén történő adatbázis lekérdezések, hozzáférések naplózásának hiánya szintén sérülékenységet okozhat a rendszerben, hisz az adatbázis szerver naplóiban az alkalmazás számára az adatbázis elérésre létrehozott felhasználók jelennek csak meg (általában ezek száma a tényleges felhasználók számának töredéke). Nyilvánvalóan a naplózás nem tud megakadályozni egyetlen ártalmas próbálkozást sem, de segítséget nyújthat annak felderítésében, hogy melyik alkalmazás és ki által lett kijátszva.

A puffer túlcsordulásnál a program egy fix hosszúságú tömböt (puffert) foglal le a memóriában, majd a tömb írásakor nem ellenőrzi annak határait. A támadó a lefoglalt tömböt túlírva (túl hosszú bemenet segítségével) felülírhat a program működése szempontjából lényeges memóriarészeket, így kártékony kódokat futtathat le. Puffer túlcsordulást kiváltó sérülékenység felléphet az alkalmazás szintjén például az SQL kérések túlméretezésével, vagy a dinamikus SQL lekérdezés számára túlméretezett input megadásával.[7]

Az adatbázisokat érintő fenyegetések közül az SQL injekciós technika mindenképp az egyik vezető helyet foglalja el. A támadásnál az alkalmazás által előállítandó, tervezett tartalmú, dinamikusan szerkesztett SQL utasításba illesztenek káros tevékenységeket megvalósító kódot. Az alkalmazás a felhasználótól bekért paraméterek segítségével állítja elő az SQL szerverhez eljuttatandó lekérdezést. A támadó a paraméter értékének olyan kártékony karaktersorozatot ad meg, ami megváltoztatja az eredeti lekérdezés szintaktikáját, ezáltal az egészen más feladatot valósít meg, mint az eredeti elképzelés. [8]

XSS támadás jelenti napjainkban a webes alkalmazások leggyakoribb megsértését. A támadó a felhasználó böngészőjében futtathat le tetszőleges kódot (például javaszkriptet), miközben a felhasználó egy megbízható webhelyhez kapcsolódik. Igazából a felhasználót sebzi meg a támadás, a web alkalmazás, mint közvetítő közeg segítségével. A támadó munkafolyamat (session) azonosítókat tud a felhasználó gépéről megszerezni, ezáltal a felhasználó nevében be tud lépni az alkalmazáson keresztül az adatbázis rendszerbe. A session azonosítók megszerzésére építő támadást munkamenet-eltérítésnek (session hijacking) nevezik. Az XSS támadás különösen veszélyes az adatbázis rétegre nézve, ha a támadáshoz használt web alkalmazás a felhasználó által megadott adatokat az adatbázis rétegen belül tárolja, ekkor a támadó az adatbázisba tud illetéktelenül beleírni. [9]

Platformok sebezhetőségei

A platformok fenyegetéseihez hozzájárulnak a hálózatba kötött szerver és felhasználói számítógépek szoftver komponenseinek sebezhetőségei. Az adatbázisok biztonságára nézve az adatbázis-kezelő rendszert futtató számítógép operációs rendszerének és az itt található állományoknak a nem megfelelő védelme biztonsági rést jelent.

A Blaster féreg például a Windows XP, Windows 2000 operációs rendszerek puffer túlcsordulásra épülő sérülékenységét használta ki, amivel megfertőzött gépeket, köztük adatbázis szervereket is elérhetetlenné tett. [10]

Az adatbázis-kezelő rendszer gépén lévő állományok megfelelő védelméről is gondoskodni kell. Titkosítatlanul tárolt adatbázis mentések és futtatható állományok jogosulatlan hozzáférése is biztonsági rést jelent.

Gyakori példa, hogy felhasználók adatbázis-kezelő rendszerbe való belépésekor lefut egy login szkript, mely a rendszer szükséges beállításait elvégzi. Ha ezt a login fájlt illetéktelenek elérik és módosítani tudják, akkor teljes hozzáférést szerezhetnek az adatbázishoz, amit az alábbi példa szemléltet:

```
----------login.sql----------

set term off

create user hacker identified by hacker;

grant dba to hacker;

set term on

----------login.sql----------
```

Adatbázisok sebezhetőségei

Az adatbázis-kezelő rendszer szoftverei és a tárolt adatok is hordozhatnak sérülékenységeket. A biztonságos működéshez elsődleges feladat az adatbázis-kezelő rendszer biztonságos telepítése, megerősítése és folyamatos felügyelete, ezt angolul „database hardening”-nek nevezik. Az adatbázis-kezelő rendszerek telepítésekor gyakran, automatikus módon, ismert nevű felhasználók jönnek létre, mely a támadás számára egy jó kiindulási pont. Ugyanis a felhasználónév birtokában a támadónak „csak” a jelszót kell kitalálnia (ami gyakorta nem erős, azaz könnyen megfejthető). A telepítéskor automatikusan létrejövő táblák, tárolt eljárások is sérülékenységi pontot jelenthetnek. Célszerű ezeket törölni, és szükség esetén más névvel magunknak létrehozni.

A szerverekre vagy anonim kapcsolattal vagy autentikáció után lehet kapcsolódni. A támadó a hitelesítési mechanizmus és információk lehallgatásával, megszerzésével illetéktelenül tud az adatbázis szerverre bejutni.

Gyenge konfigurációs paraméterek használata, szoftver hibák, az adatbázis tárolt eljárásaiban található puffer túlcsordulásra, illetve SQL injekcióra épülő sérülékenységek, felhasználói hibák,

elavult verziójú programok használata és biztonsági frissítések feltöltésének hiánya kártékony kód lefuttatását, vírusok, trójaiak és férgek rendszerbe való bejutását eredményezheti, illetve szolgáltatás megtagadása típusú támadásra ad lehetőséget. Például az SQL Slammer féreg a Microsoft SQL szerverének puffer túlcsordulásra épülő sérülékenységét használta ki és okozott az adatbázis-kezelő rendszer biztonságában rendelkezésre állás megsértést. A kártékony kód olyan rendszereket tudott megfertőzni, melyek a már bejelentett sérülékenységet javító biztonsági frissítést nem alkalmazták. [11]

Összefoglalás

A publikációban az adatbázisok fenyegetések különböző formáit mutattuk be. Először értelmeztük az adatbázis-biztonság alapfogalmait, többek közt az adatbázis-biztonság alanyát és a védendő tulajdonságait, majd különböző rendszerezési kategóriákat állítottunk fel az adatbázis fenyegetések rendszerezéséhez. A támadási pontok szerint négy csoportra osztottuk az adatbázis fenyegetéseket, ezek a hálózat, alkalmazások, platform és adatbázis rendszerek sebezhetőségeire épülő támadási lehetőségek. A támadási pontok kategóriái szerint jellegzetes adatbázis fenyegetéseket gyűjtöttünk össze. Egy szervezet adatbázisainak biztonságát mérő kockázat elemzések fő célja a veszélyek felvázolása és rangsorolása, ezt a folyamatot segíti az, ha ismerjük a lehetséges támadásokat és ezek megvalósulásának helyeit.

Felhasznált irodalom

[1] MUNK Sándor: Információbiztonság vs. informatikai biztonság. – Robothadviselés 7 tudományos szakmai konferencia anyaga (2007.11.27.), Hadmérnök különszám

[2] Ramez Elmasri , Shamkant B. Navathe: Fundamentals of Database Systems, 5th Edition, Addison Wesley 2007

[3] C. J. Date: An Introduction to Database Systems, 8th Edition, Addison Wesley 2004

[4] Database Secrity Technical Implementation Guide, Version 8, Release 1, 19 September 2007, Developed by DISA for the DoD

[5] Útmutató az IT biztonsági szintek meghatározásához http://www.ekk.gov.hu/hu/emo/ekozigkeretrendszer/ek3-itbiztonsag/EKK_ekozig_ITbiztonsagiszintekmeghatarozasa_080822_V101.doc (2009.12.10.)

[6] Amichai Shulman: Danger From Below: The Untold Tale of Database Communication Protocol Vulnerabilities http://www.imperva.com/resources/adc/db_comm_protocol.html (2009. 12.10.)

[7] Bucsay Balázs: MySQL and SQL Column Truncation Vulnerabilities http://rycon.hu/papers/02mysqlcolumntruncation.pdf (2009.12.10.)

[8] Fleiner Rita: SQL injekcióra épülő támadások és védekezési lehetőségek, Hadmérnök, 2008 (III.)/4. (117-128.o.) http://hadmernok.hu/archivum/2008/4/2008_4_fleiner.html (2009.12.10.)

[9] Simon Whatley: What is a SQL Injection Attack http://www.simonwhatley.co.uk/what-is-a-sql-injection-attack (2009.12.10.)

[10] CERT® Advisory CA-2003-20 W32/Blaster worm http://www.cert.org/advisories/CA-2003-20.html

[11] SQL slammer (computer worm) http://en.wikipedia.org/wiki/Slammer_%28computer_worm%29 (2009.12.10.)