

Közvetlenül módosított adatok

Korlátlan jogosultsággal lehet közvetlenül is módosítani az adatokat az adatbázisban, nem árt tehát, ha kontrolláljuk az ilyen tevékenységet.

A működő informatikai rendszerekben különböző okoknál fogva szükség lehet az adatbázisok adatainak közvetlen módosítására, ez az úgynevezett direkt adatmódosítás (dam). Azért direkt, mert az, aki végzi, megkerüli az alkalmazásokba épített üzleti logikát és jogosultsági rendszert. Erre azért van szükség, mert a módosítások az üzleti folyamatokban nem ott történnek, ahol történniük kellene – magyarázza *Tim Zoltán*, a Stratis tanácsadója.

Megkérjük a rendszeradminisztrátort

Ezeket a módosításokat jellemzően magas jogosultságú rendszerüzemeltetők és adatbázis-adminisztrátorok végzik el abban az esetben, ha egy alkalmazás hibájának következtében adatbázis-inkonzisztencia lép fel, vagy ha nincs funkció egy feladat elvégzésére. Például új telephelyet kell felvenni a rendszerbe, de nincs „új telephely” funkció – ilyenkor ezt a rendszeradminisztrátor viszi be a megfelelő helyre.

Ugyancsak dam-ra kerül sor, ha a felhasználónak nem áll rendelkezésre megfelelő felület az adatmódosításhoz. Szabályozás hiányában a felhasználók közvetlenül a rendszergazdákhöz fordulnak, akik „kisegítik” őket.

Az adatmódosításokra valamilyen üzemeltetési incidens keretében kerül sor, azaz miután a hibát, a problémát regisztrálják a helpdesken. Az incidenskezelési folyamat keretében jutnak a rendszer-

üzemeltetők arra a következtetésre, hogy dam-ra van szükség.

Számon kérhetőség

A dam egyik problémája az, hogy viszonylag nehéz nyomon követni a rendszerüzemeltetők tevékenységét, mivel korlátlan hozzáférési jogokkal rendelkeznek feladataik ellátásához. Ha valaki mégis megpróbálja nyomon követni, nagyon gyakran emberi ellenállásba ütközik a jogosultság-megvonástól való félelem miatt. Ilyenkor célszerű elbeszélgetni a rendszeradminisztrátorokkal és meggyőzni őket, hogy a monitorozás egyrészt a szervezet érdeke, másrészt saját érdekük is.

Ha ugyanis az adatmódosítások nem követhetők nyomon, akkor egy esetleges visszaélés esetén nem lehet megállapítani az elkövetőt. Ha pedig nem lehet megállapítani az elkövetőt, akkor mindenkit elővesznek, akinek jogosultsága van a direkt adatmódosításra.

Ma úgy üzemeltetnek nagy üzleti rendszereket, hogy peremfeltételnek tekintik a rendszer- és adatbázis-adminisztrátorok megbízható voltát, és hogy az üzemelési környezet jóindulatú. Pedig a dam révén az adatok sértetlensége van veszélyben. Ugyanakkor számolni kell külső támadással is, különösen rosszul védett informatikai hálózat esetében.

Naplózás

További probléma a dam-mal, hogy nehezen lehet ellenőrzés alatt tartani, mivel a normál működés keretében is szükség lehet rá valamilyen hibaelhárítási célból. Ennek gyakorisága, persze, az informatikai rendszer megbízhatóságától függ; ha hibával teli alkalmazást futtatnak, akkor bizony gyakran kell közvetlenül adatot módosítani. Így a szervezeteknek törekedniük kell arra, hogy a dam szigorúan szabályozott körülmények között menjen végbe, s ebbe beletartozik a nem jogszerű módosítások felfedése is.



Tim Zoltán, Stratis
Veszélyben a sértetlenség

A dam-ellenőrzés többretegű, a szabályozás mellett az egyik fő elem például a naplózás. Azonban ez sem problémamentes, mivel nagy mennyiségű bejegyzés keletkezik, amelyeket nehéz feldolgozni, továbbá korrelációt kell találni az események között. A bejegyzésből meg kell tudni mondani azt is, hogy ki végezte. A dolgokat megkönnyíti viszont, ha az informatikai rendszert – az alkalmazásokat, az infrastruktúrát – úgy tervezik és konfigurálják, hogy a rendszerben végzett valamennyi tevékenység személyhez köthető legyen.

A lényeg, hogy minden adatmódosításhoz felhasználói azonosítót kell tudni kapcsolni, s ha a rendszerek ezt nem támogatják, vagy elveszik valahol ez az információ, akkor nem lehet megállapítani, melyik adatmódosítást ki végezte.

Külső tényezők

A dam és ellenőrzésének területe egyébként most kezd az érdeklődés középpontjába kerülni amiatt, hogy a szervezeteket különféle külső tényezők – elvárások, megfelelések, fokozódó hackertámadások – adatvédő biztonsági intézkedésekre kényszerítik. Az adatmódosítások nyomon követéséhez már léteznek eszközök, amelyek az alkalmazások tranzakciós naplóbejegyzéseit pásztázzák, s kiolvassák, melyik tranzakció során mi történt.

Ezt a fajta monitorozást egyébként Magyarországon még kevés helyen alkalmazzák, s a Gartner szerint Nyugaton is csak a potenciális piac 1 százaléka használ ilyen eszközöket.

Horváth András

Nem programmódosítás!

Ma már sok alkalmazás üzleti logikája is adatbázisban tárolódik. Ilyen például egy tárolt eljárás, paraméter stb. Ezeknek a módosítása közvetlenül az adatbázisokban nem direkt adatmódosítás, hanem programmódosítás.