Jogosultságmonitorozó rendszer kialakítása

Jogosultságkezelés problematikája

Az egyre kifinomultabb fenyegetettségek, az iparági szabályozások folyamatos szigorításai felerősítették azt az igényt, hogy a vállalatvezetők minden pillanatban tudják: ki, mikor, milyen bizalmas adatokhoz férhet hozzá. A felhasználók személyazonosságának és vállalati erőforrás elérésüknek felügyelete egyre fontosabb szemponttá és egyre nagyobb kihívássá válik napjainkban. Növekszik azon vásárlók, alkalmazottak, partnerek és beszállítók száma, akik jogosultak hozzáférni egy adott szervezet kritikus fontosságú információs erőforrásaihoz.

A hozzáférési jogosultságok meghatározása egyrészt a szervezeti hierarchia, másrészt a személyes tevékenységet meghatározó feladatkör függvénye Az azonosság- és hozzáférés kezelési megoldások feladata a folyamatot támogató funkciók szolgáltatása, ami technikailag segíti a vezetői elképzelés kompetenciafüggő, összehangolt érvényre jutását, és ellenőrzött fennmaradását.

Egy vállalat biztonsága a mai világban az informatikai rendszereken keresztül sebezhető a legnagyobb mértékben. Rengeteget foglalkozik a média is a vállalatok informatikai biztonságával. Nagyon sok informatikai vállalkozás szakosodott a IT biztonság felderítésére, védelmére, megelőzősére.

Egy átlagos vállalkozás, aki informatikai eszközökkel végzi a napi munkáját, igen sok információt halmozott fel és digitalizált informatikai eszközök segítségével, amikre üzleti vagyonként kell tekinteni. A felhalmozott tudást és az üzleti vagyont védeni kell, méghozzá nem csak a külső támadásokkal szemben, hanem a belső kockázatokkal szemben is. Nagyon sok informatikai és cégvezető megbízik saját alkalmazottaiban, pedig az esetek nagy részében az információk kiszivárogtatása belső alkalmazott közreműködésével történik. Ennek a gyanúja a legtöbb esetben fel sem merül, illetve nem szereznek róla tudomást az érintettek.
A visszaélési lehetőségeknek több oka is lehet:

- Bizonyos alkalmazottak több jogosultsággal rendelkeznek, mint ami a munkavégzésükhöz szükségesek, azáltal olyan adatokhoz férhetnek hozzá, melyekhez papírforma szerint nem lenne joguk. Ez nem feltétlenül szándékosságból eredhet, egy egyszerű véletlenből is alakulhatnak ilyen helyzetek, de ez a fajta anomália melegágya lehet a visszaélési, csalási kísérleteknek.

- Sok esetben ideiglenesen kapnak a belső felhasználók engedélyeket egy bizonyos időszakra, mert a munkájuk ezt megköveteli, majd ezeket a jogokat nem szüntetik meg.

- A dolgozó leszámolása után elfelejtik visszavonni a jogosultságait. Ez főleg abban az esetben jelent nagy kockázatot, ha az illetőt valós, vagy vélt sérelem éri a vállalat részéről.

- Bekerülnek a rendszerbe olyan külső felhasználók, akik csak ideiglenes jogot kapnak, pl.: tesztelési célból, majd később ezeket sem szüntetik meg.

- Egy új alkalmazás vásárlását követően a beszállító cég a telepítés idejére hozzáférést kap bizonyos informatikai erőforrásokhoz, majd később még több jogosultságra lesz szüksége, a végén már senki nem tudja megmondani, hogy mennyi jogosultsággal rendelkezik, a legvégén pedig nem szüntetik meg a jogosultságokat, így egy óriási észrevehetetlen biztonsági rés keletkezik a vállalkozás informatikai rendszerében.

- Az erős jogkörrel rendelkező alkalmazottak (rendszergazdák, alkalmazás gazdák) önhatalmúlag jogosultságot módosíthatnak alkalmazottaknak, illetve visszaélhetnek vele.

A példák felsorolását a végtelenségig tudnánk folytatni, sajnos ezek mindennapi esetek, melyekről sok esetben nem is szerzünk tudomást.

Az informatikai jogosultságot igen felületesen vagyunk képesek kezelni: van joga, nincs joga. Ez egy kicsit sarkítottnak tűnhet, de ez a valóság. Nagyrészt nem törődnek részletekkel, amit sok dologgal lehet magyarázni:

- Nincsen elég kapacitás a pontos jogosultság kezelésére.
- Nincsen igény a jogosultság igénylési folyamat betartására.
- Túl gyorsan növekedett a vállalkozás és az informatika nem tudta kellőképpen tartani a fejlődés ütemét.
- Nincsenek szigorú informatikai szabályozások

A sort itt is a végtelenségig lehetne fojtatni, de térjünk vissza a részletekhez.

Mit értünk részleteken?

A legtöbb vállalkozás még mindig nagyon egyszerű eszközöket használ a napi informatikában, excel – word dokumentumokat. Nagyrészt rendelkeznek vásárolt vagy egyedi fejlesztésű informatikai alkalmazásokkal is, melyek valamilyen adatbázis kezelő rendszer segítségével tárolják az információkat. Egy dokumentum és a hozzá tartozó felhasználók jogai egy apró részlet az informatikai rendszerben. A valós világban viszont egy óriási értékű információ halmaz, amely egy pillanat alatt kikerülhet a kezünk közül.

Egy dokumentum a sok ezer között! Így vélekedik az akinek nem fontos a dokumentum tartalma és nem foglalkozik azzal, hogy megvédje a dokumentum tartalmát az illetéktelen személyektől. Ha ez a dokumentum a konkurencia kezére jut, akkor máris felértékelődik a benne rejlő tartalom.

Egy másik példa, ha van egy adatbázis szerverünk, akkor abban rengeteg információt tárolnak az alkalmazásaink, ezek az információk szintén nagyon fontosak és bizalmasak. Azt viszont, hogy ki férhet hozzá egy adatbázishoz közvetlenül, azt gyakran nem is sejtjük, mivel mindig az alkalmazáson keresztül, felhasználói bejelentkezéssel és jogosultságkezeléssel védjük az információinkat.

- Ha egy vezető az alkalmazottjainak (rendszergazdáknak) felteszi ezeket a kérdéseket:
- Ki milyen fájlokhoz és rendszerekhez férhet hozzá és milyen jogosultsági szinttel?
- Egy felhasználó mikor használt utoljára egy bizonyos fájlt, fájlokat?
- Egy fájlhoz milyen felhasználók, csoportok milyen jogosultsággal férhetnek hozzá?
- Egy felhasználó vagy csoport hány darab „n” típusú fájlnak tulajdonosa, mekkora helyet foglalnak ezek, stb…?
- Milyen fájlokkal dolgozik egy adott felhasználó egy adott idő intervallumban?
- Ki milyen adatbázis szerverekhez férhet hozzá és milyen jogosultsággal?
- Ki milyen alkalmazás szerverekhez férhet hozzá és milyen jogosultsággal?
- Mikor használta egy felhasználó utoljára a vállalat egyik „erőforrását”?

- Egy felhasználó vagy egy rendszergazda hány szerverre tud bejelentkezni és ott milyen jogokkal rendelkezik?
- Milyen elfekvő, nem használt felhasználók léteznek az informatikai rendszerekben?
- Milyen felhasználók, login-ok rendelkeznek bizonyos rendszereken teljes adminisztrációs jogkörrel?
- Mit, és milyen szinten „láthatnak" a rendszergazdák? …

Az esetek nagy részében azt a választ kapja, hogy nem tudjuk. Néhány estben pedig: ezeket az információkat több hetes munka összeszedni, vagy lehetetlen. Pedig nem az.

Ismert megoldások

Egy jól működő jogosultságmenedzsment rendszer alapfeladata jól menedzselhetővé - ellenőrizhetővé és átláthatóvá – tenni a jogosultságkezelési munkát.

Mint szinte minden problémára, erre is számos megoldás létezik.

Ezek egy része viszonylag komplex módon közelít a problémához, áruk ennek megfelelően igen jelentős, míg mások egy-egy részproblémára fókuszálnak, egymással integrálatlan megoldás halmazt nyújtva.

- Az egyedi, manuális jogosultságkezelés leginkább a kis cégek körében elterjedt. Saját tapasztalatból mondhatom, hogy egy kis cégnél is igen könnyen elérheti a jogosultsági rendszer azt a bonyolultsági szintet, amit nem lehet manuálisan kezelni.
- A központi jogosultságkezelés olyan megoldás, amely egyre inkább elterjedőben van. Más kérdés hogy ennek is sokféle megközelítésével találkozunk, mindenki mást ért központi jogosultságkezelés alatt. A legtöbb helyen csak annyit jelent a központi jogosultságkezelés, hogy központi szabályozás van kiadva a jogosultságkezelés folyamatára, de a ténylegesen kiosztott jogosultságok visszaellenőrzésére nincs mód.
- A teljes körű, elektronikus megoldás, ami a kiosztást és a visszaellenőrzést is tartalmazza, általában rendkívül drága, és nagyon nehezen implementálható a jellemzően inhomogén informatikai struktúrákba.

Általánosságban elmondható, hogy a legtöbb megoldás nem a tényleges jogosultságok felolvasására helyezi a hangsúlyt, pedig meglátásunk szerint ezzel a megközelítéssel lehet a legpontosabb képet kapni a jogosultsági helyzetről, így lehet a leghatékonyabban csökkenteni az adatvagyont érintő kockázatokat.

Megoldási javaslat

Az általunk javasolt megközelítési mód az, hogy a pillanatnyilag ténylegesen kiosztott jogosultságokat kell összegyűjteni a vállalat különböző rendszereiből, és ezeket az összegyűjtött jogosultsági adatokat adattárházban kell tárolni a későbbi elemezhetőség érdekében.

A rendszernek képesnek kell lennie:

- A pillanatnyi jogosultságok föltérképezésére (monitorozására) ütemezetten, vagy közvetlen indítással aktiválható „felderítő robotok" alkalmazásával.
- A beállított jogosultságok védett adatbázisban történő tárolására
- Standard és adhoc jellegű riportok készítésére a belső összefüggések feltárására

A jogosultságmonitorozó rendszert célszerű modulárisan és skálázhatóan kialakítani annak érdekében, hogy megfeleljen a különböző cégek, szervezetek különböző szintű igényeinek. Az így kialakított moduláris rendszer, önállóan is alkalmazható komponensei révén képes biztonságosabbá tenni a néhány fős, kis cégek működését is, de teljes kiépítettségében a közepes, vagy akár nagyobb méretű szervezetek esetén is ellenőrizhetővé és átláthatóvá teszi a jogosultság menedzselési munkát azzal, hogy „megmutatja", kinek mihez van jogosultsága.

A tényleges jogosultságok begyűjtésén alapuló jogosultságmenedzsment rendszer képes arra, hogy feltárja a különbséget a vezetői szándék és a tényleges helyzet között, ezzel egy hatékony eszközt adva mind az informatikai üzemeltetés, mind a vállalatvezetés kezébe.

A jogosultsági adatok adattárházban történő tárolása lehetőséget biztosít egyrészt a jogosultsági adatok monitorozására, másrészt elemzések készítésére a bonyolult összefüggések feltárása érdekében, a jogosultság-beállítási anomáliák felderítésére. A rendszernek képesnek kell lennie megmutatni különféle grafikus és táblázatos jelentések formájában, hogy egy adott felhasználó vagy csoport milyen informatikai jogosultságokkal bír a vállalat egészét, vagy egy részterületét illetően.

A rendszer specifikációja:

SecurityDiscoverer (Adatgyűjtő modul)

Feladata a jogosultsági adatok felderítése, begyűjtése a különböző rendszerekből. Távolról konfigurálható, felügyelhető. Új kiszolgálóra való telepítése a központi modulból végezhető. Az adatokat lokálisan is képes tárolni (hálózat kiesési puffer), majd lehetőség szerint továbbítani a központi szervernek (SecurityStore). Az adattovábbításnak titkosított csatornán kell történnie.

SecurityStore (Adattároló modul)

Input oldali feladata a gyűjtőmodulokból érkező adatok fogadása titkosított csatornán keresztül. Érkeztetés után rendszerezi, csoportosítja és eltárolja őket az adatbázisba, ideértve a SecurityDiscoverer programok konfigurációs bejegyzéseit is. Az adatok összefüggéseinek ellenőrzését végző üzleti logika réteg is ebben a program modulban helyezkedik el. Output oldalon kiszolgálja a SecurityMonitor adatkéréseit is, amik a lekérdezések és riportok alapjául szolgálnak.

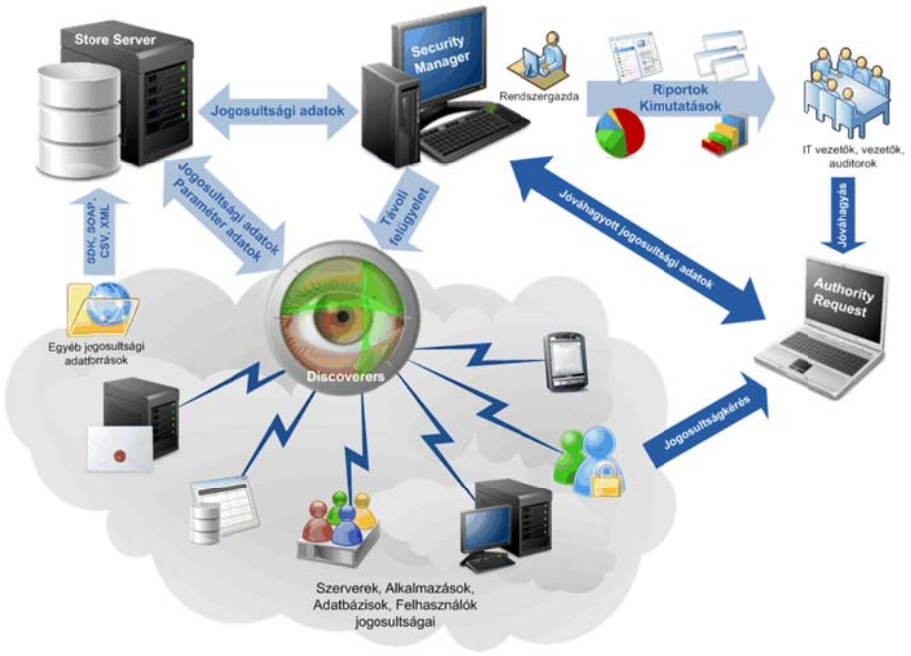
SecurityMonitor (Adatmegjelenítő modul)

A modul feladata a klasszikus felhasználói funkciók biztosítása, úgymint: lekérdezések, elemzések, riportok futtatása, OLAP megjelenítés, figyelmeztetések menedzselése, rendszergazdai felület, belső jogosultságkezelés, SecurityDiscoverer programok távmenedzselése. A különböző rendszerek adatainak egyesítését végzi, így egy felületen látható a megfigyelt felhasználó összes jogosultsága, amit a program kezelője néhány kattintással meg tud jeleníteni.

Authority Request (Jogosultságigénylő modul)

A modul feladata, hogy a felhasználók a jogosultsági igényeiket egy webes felületen keresztül fel tudják adni, majd az illetékesek jóváhagyása után a jóváhagyott igények a rendszergazdához kerülnek mint elvégzendő feladat, illetve bekerülnek az igényelt jogosultságok adatbázisba, annak érdekében, hogy később össze lehessen hasonlítani az igényelt és a ténylegesen beállított jogosultságokat.

A rendszer felépítése



A rendszer felhasználói köre

Egy valós jogosultság-beállítási adatokra épülő monitor rendszer nagyon nagy segítség a **rendszerüzemeltetők, rendszergazdák** számára. Használatával elemzéseket tudnak készíteni a jogosultsági anomáliák felderítésére, rendszeres és adhoc riportokat tudnak generálni a vezetőség felé az aktuális jogosultsági állapotról, illetve a vezetői szándék és a tényleges helyzet könnyen áttekinthető összehasonlításával napi listát tudnak maguknak készíteni az elvégzendő feladatokról.

Az **IT vezetők, vezetők** az előre definiált, illetve adhoc módon előállított jelentések, statisztikák áttekintésével tiszta képet kaphatnak az adatvagyont érintő jogosultsági kockázatokról, illetve kontrollt gyakorolhatnak az IT üzemeltetés fölött.

Az **ISO Auditorok, belső ellenőrök** a megfelelőségi riportok felhasználásával megkönnyíthetik az auditálási folyamatokat, illetve bizonyítékokat tudnak generálni a megfelelőség elbírálásához.

Bevezetési alapelvek

Alapvető elvárás, hogy minden hasonló rendszert az adott vállalatnál érvényben lévő informatikai stratégiával, ezen belül az IT biztonsági politikával összhangban kell bevezetni. Nagyon fontos, hogy nagyon nagy mennyiségű adat keletkezik már egy konkrét jogosultsági rendszer megfigyelésével is, ezért nem célszerű minden alrendszerre beállítani a figyelést, inkább ki kell választani azokat az üzletileg kritikus rendszereket, amelyeket a kockázatkezelési folyamat kritikusnak minősített.

A jogosultságmonitorozó rendszer önmagában csak egy eszköz, ahhoz hogy hatékonyan szolgálja a vállalat érdekeit, integrálni kell a vállalat működési és szabályozási folyamataiba.

szabályzási rendszerbe kell