

## **Az IT biztonság új kihívásai: napjaink biztonsági fejlesztéseinek motorja az előírásoknak való megfelelés és annak tanúsítása**

Napjainkban új biztonsági kihívásokkal néznek szembe a vállalatok. A biztonsági fejlesztések motorja sokszor mégsem az üzletmenet diktálta racionális fejlesztési igény, hanem a szervezettekkel szemben kívülről támasztott elvárás, a szabályoknak való megfelelés, és e megfelelés tanúsítása. Ezek a követelmények olyan biztonsági megoldások bevezetését várják el a cégektől, amelyek számos más, korábban is fennálló problémára adnak választ, így a szervezetek használatukkal végső soron több legyet ütnek egy csapásra.

### **A hagyományos rendszerek problémái**

Az IT biztonság körébe tartozó feladatok hosszú múltra vezethetők vissza, és egyben jelentős változásokon is keresztülmentek az elmúlt időszakban. A hagyományos biztonsági modell konzervatív megközelítésű, rendszerint alkalmazás szintű. E rendszerekben minden alkalmazásban egyenként implementálják a hozzáférési szabályozást ahelyett, hogy központosítva oldaná meg a problémát. Ez védelmet jelent a statikus kockázatok ellen, de *nehezen alkalmazkodik a változásokhoz*, így gátja az üzleti élet által diktált rugalmasságnak, akadálya a szervezetek és üzletágak gyors növekedésének.

A fentiekből kifolyólag mára számos olyan biztonsági kérdés merül fel, amelyre a cégek nem tudnak választ adni, vagy a válasz nem kedvező a biztonság szempontjából. Például:

- Minden esetben tudomást szerez róla, ha kialakul egy biztonságilag veszélyes helyzet?
- Hány volt alkalmazottnak és volt szerződéses partnernek van még hozzáférése az Önök rendszereihez?
- Nem kizárt, hogy előbb tudhatja meg egy rendszergazda a cég pénzügyi eredményeit, mint az ügyvezető?
- Garantálni tudják Önöknél az alkalmazotti- és ügyfeladatok védelmét?
- A jogszabályi megfelelési vizsgálatok egyedi, manuális lefolytatása mekkora költségeket ró az Önök szervezetére?

### **Biztonság – kényszer hatására**

Ebben az egyre nehezebben tartható helyzetben mégsem a belső folyamatok, *hanem egy külső kényszer megjelenése hozott változást*. 2002-2003 körül világszerte számos tőzsdei gazdálkodó szervezetnél találtak olyan visszaéléseket, amelyek az adatkezelés hiányosságaira voltak visszavezethetők, ezért elsőként az Egyesült Államokban majd az Európai Unióban is olyan jogi kényszerek jelentek meg, amelyek részletesen szabályozzák a tőzsdei cégek adatkezelésének módját. (SOX, GLB, EU 8. direktíva). Ezekben az IT biztonsági terület, a rendszerekben dolgozók jogosultságainak kezelése is jelentős hangsúlyt kapott.

Az előírások a hazai cégek egyre szélesebb körét érintik így minden, a Sarbanes-Oxley törvény alá eső amerikai vállalat magyarországi leányvállalatait. Az általános tőzsdei terület mellett megemlíthetők azok a gazdasági vertikumok, amelyekben a cégeknek külön szabályzóknak kell megfelelni. Ilyen például a pénzügyi szektorban a Basel II, (1992. évi LXIII. tv), a Hitelintézeti Törvény a hitelintézetekről és a pénzügyi vállalkozásokról szóló 1996. évi CXII. törvény 2003-as 13/B. §-al illetett kiegészítése: "Informatikai rendszer védelme", a tőkepiacról szóló 2001. évi CXX. törvény 2003-as 101. §-al illetett kiegészítése: Informatikai rendszer védelme, a Pénzügyi Törvény, a BIT (Biztosítókrol és biztosítási tevékenységről szóló 1995. XCVI. tv.), az ÖPT (Önkéntes kölcsönös biztosítópénztárakról szóló 1993. évi XCVI tv.), a NYPT (Nyugdíjpénztári 1999. évi CXXIV trv.), vagy éppen garantálni kell a személyes adatok sérthetlenségét a Magyar Adatvédelmi Törvény törvény szerint. Ezen előírások teljesülését állami vagy a szektorban illetékes szervek (például a PSZÁF) ellenőrzik.

Az előírásoknak való megfelelés – szemben a biztonsági kockázatok csökkentése érdekében tett lépésekkel – nem tartozik a cégek saját mérlegelési körébe, hanem olyan külső kényszer, amelyhez alkalmazkodni kell, a megfelelést pedig bizonyítani kell a vizsgálatok során.

### **Új megoldások**

Az új kihívásokra új megoldásokat kellett keresni lehetőleg úgy, hogy orvosolja a fent említett problémákat, azaz legyen rugalmas, csökkentse a költségeket, biztosítson átláthatóságot („governance”) és ezen keresztül csökkentse a biztonsági kockázatokat is („risk management”).

A cégek részéről számos többletforrást és többletenergát igénylő helyzet érdekessége, hogy az előírásoknak megfelelő rendszerek kiépítésénél éppen azok a biztonsági megoldások kerülnek előtérbe, amelyek egyben megoldást jelentenek a korábban említett problémákra – rugalmatlanság, megosztottság, rossz alkalmazkodóképesség, átláthatatlanság – is. A cégek számára olyan technológiák váltak tehát vonzóvá, amelyek a jó audit-képességek mellett

- központosítják az IT biztonság adminisztrációját,
- csökkentik a belső helpdesk tevékenységeket,
- kézbentarthatóságot kínálnak, és
- a változások olcsóbban, újabb kockázatok generálása nélkül kezelhetők le.

Ilyenek például a központi felhasználó, jogosultság adminisztrációs rendszerek (identity provisioning), amelyeknek vannak önkiszolgáló, vagy delegált adminisztrációs lehetőségeik, de emellett mindent naplóznak, kitűnő audit képességekkel teljes áttekintést tudnak nyújtani a pillanatnyi és a historikus jogosultsági térképről. Adatbázis szinten ide sorolhatjuk azokat a megoldásokat, amelyek garantálják az előírásokban megfogalmazott felelősségi körök szétválasztását. De ide tartoznak a központi hozzáférés kezelési megoldások is, például az egykapus bejelentkezés (single sign-on) vagy elosztott (federation) keretrendszerek.

### **A biztonság nem csupán egyetlen rendszer, hanem vállalati szemléletmód**

Az új megoldások mindegyike azt célozza, hogy az IT biztonság ne csak a különböző heterogén informatikai rendszerekben kezelt különféle jogosultságok halmaza legyen, hanem a szervezetben tevékenykedő személyek szintjére lebontott jogosultságkezelés, a személyek különféle végponti rendszerekben játszott szerepétől függetlenül, azok felett állva.

A szervezethez és az abban dolgozó személyekhez való alkalmazkodás a HR rendszerrel, illetve a partner- és ügyfélkezelő rendszerrel való integrálással valósulhat meg. Ezek a rendszerek a biztonsági

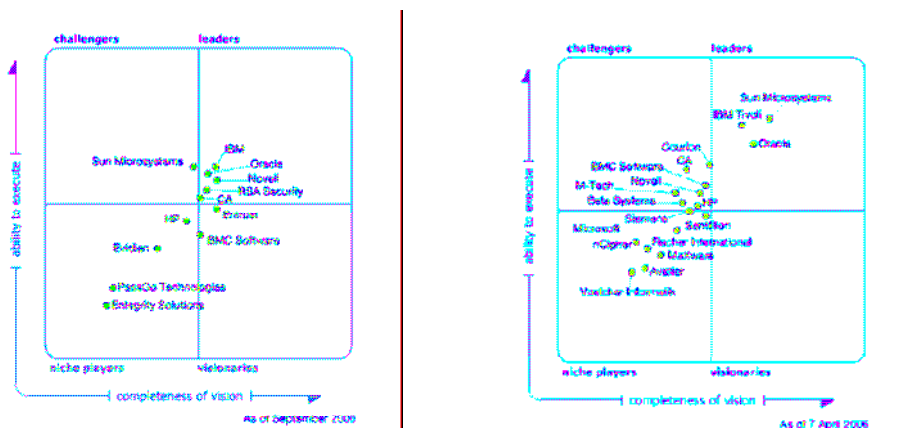
szempontból kezelendő személyekről szervezetenként mindig naprakész információkkal rendelkeznek, nagyszerű kiindulási alapjai egy automatizálható jogosultság adminisztrációnak, ami nem hagy kiskapukat, és mentes az emberi hibáktól.

A személy (munkakör) és az informatikai jogosultság között azonban egy olyan absztrakciós szintet is ki kell alakítani, ami egyszerűvé és automatizálhatóvá teszi a jogosultsági megfeleltetéseket. A munkaköröket elemi szerepkörökre (role) bontjuk, ezekhez pedig az egyes IT alrendszerekben ottani jogosultságokat rendelhetünk. A szervezetek feladata tehát egy ilyen IT biztonsági megoldás bevezetésénél (vagy azt megelőzően) az, hogy kialakítsák a szerepköröket, minimalizálják és konszolidálják azokat. Ez a feladat hasonló a más jellegű IT projekteket is kísérő „szervezeti és működési szabályzat (SZMSZ)” jellegű megfontolásokhoz, és kritikus sikertényező.

### Az Oracle megoldásai – hagyományos és új kihívásokra

Az Oracle IT biztonsági megoldásai két lábon állnak. Az egyik a negyed évszázados múltú visszatekintő Oracle technológiai termékcsalád, ezen belül is a piacvezető szerepet betöltő adatbáziskezelő, amelynek jó hírneve többek közt az adatbáziskezelésben elengedhetetlen biztonságban és megbízhatóságban gyökeredzik.

A másik pillér egy olyan felhasználó-, jogosultság és hozzáférés-kezelési termékportfólió, amellyel az Oracle a fent említett „governance, risk- & compliance management” igényekre ad megoldást, nem csak Oracle, hanem bármilyen heterogén IT környezetben. Ezt a portfóliót az Oracle kisebb, de piacvezető cégek felvásárlásával építette fel, majd kovácsolta egységessé. Mindezeknek köszönhetően a Gartner két idei elemzésében is (identity provisioning illetve web access management) az Oracle „vezető” besorolást ért el.



### Megoldások a kézben tarthatóság növelésére (governance)

A kézben tarthatóság jellegű kihívások közt az egyik legfontosabb a magas **működési költségek problémája**. A cégvezetők részéről folyamatos a nyomás a költségcsökkentésre, ezzel szemben a nagy belső leterheltség miatt egyre nőnek a helpdesk költségek, (minden helpdesk hívás akár 10-15 euróba kerülhet a cégeknek!), illetve nő az IT adminisztrátorok száma és az ezzel járó többletkiadások. A minden feladatot egyedi vagy szigetszerű megoldásként ellátó rendszerek karbantartása drága.

Az Oracle komplex biztonsági rendszerének elemei kiküszöbölik ezeket a problémákat. Az *Oracle Identity Manager* automatikusan követi a személyzeti változásokat és érvényesíti azokat az IT rendszerekben, támogatja az önkiszolgáló és delegált adminisztrációt, és nem utolsósorban a minimumon tartja az IT rendszerekben szükséges felhasználószámot. Az *Oracle Access Manager*

egyesített automatikus bejelentkezést biztosít az összes webes rendszer felett, szintén támogatja az önkiszolgáló és delegált adminisztrációt, korszerű jelszó menedzsmentet és visszaállítást tesz lehetővé, illetve támogatja a heterogén, azaz több gyártótól származó rendszereket. Az *Oracle Label Security* ugyanazon adatbázis használatát teszi lehetővé a különböző felhasználói körök számára, miközben automatikusan és alacsony szinten választja szét a biztonsági szinteket és az adatokat.

A single sign-on, a jelszó visszaállítás, a delegált adminisztráció, az önkiszolgálás támogatás és az automatikus provisioning mind kitűnő ROI jellemzőkkel bírnak, a felhasználónkénti költségmegtakarítás csak a helpdesk költségeken elérheti az évi 330 eurót, automatizált adminisztráció (provisioning) bevezetésével pedig a felhasználónkénti költségmegtakarítás akár évi 1000 euró is lehet. Mindemellett eltűnnek a manuális auditok költségei, az IT adminisztrátorok számát nem kell növelni, illetve csökken az IT infrastruktúra komplexitása, és ezáltal a fejlesztés és fenntartás költsége.

A kézmentarthatóság másik fontos kihívása a **növekvő üzletvitel támogatásának képessége**. A cégeknek fejlődésük közben meg kell oldani, hogy biztonságosan és gyorsan kezelhessék akár több ezer / tízezer új ügyfél és a hozzájuk tartozó megfelelő jogosultságok kezelését úgy, hogy ezzel párhuzamosan az ügyfelek és üzleti partnerek elégedettsége is nőjön.

E kérdésekre is az Oracle több biztonsági megoldásának együttese ad választ. A már említett *Oracle Access Manager* mellett az *Oracle Enterprise Single Sign-On Suite* kiterjeszti az egyszeri bejelentkezést a webes alkalmazásokon túl vastag klienses alkalmazásokra, desktop operációs rendszerekre is, hatékony jelszó-menedzsment és visszaállítási lehetőségek mellett. Az *Oracle Label Security* az alkalmazástól független jogosultság-szabályozást nyújt a cégeknek, használatával biztonságossá válnak az ad-hoc lekérdezések és az üzleti intelligencia alkalmazások, valamint a belső adatbázisok egyszerűen megnyithatóvá válnak a partnereket és az ügyfeleket kiszolgáló rendszerek felé.

A kézmentarthatóság harmadik jellemző kihívása a **felhasználók változásmenedzsmentje**, azaz hogy informatikai rendszereik milyen gyorsan képesek követni a belépő és a kilépő alkalmazottakkal járó adminisztrációt. Amikor egy alkalmazott belép vagy munkakört vált, az automatizált rendszerek hiányában sokszor rengeteg munkaidő vész kárba, mire az alkalmazott a megfelelő jogosultságok és hozzáférések birtokában teljes értékű munkát tud végezni.

Az Oracle válasza erre szintén az *Oracle Identity Manager*, amely automatikus felhasználói jogosultság adminisztrációs funkciókra képes, beépített kérelmezési és elbírálási szolgáltatásokat nyújt, kifinomult forrás analízis (reconciliation), munkafolyamat és provisioning mechanizmusokkal rendelkezik, és kimagasló megfeleléségi tanúsítási szolgáltatásokat biztosít. Az *Oracle Virtual Directory* a meglévő felhasználó-nyilvántartások (címtárak) egyesítését oldja meg nagyon rövid üzembe állítási és bevezetési idővel úgy, hogy közben nincs szükség új nyilvántartások létrehozására, az adatok másolására vagy szinkronizálására.

E rendszerek használatával megszűnik az elszórt, decentralizált címtárakban tárolt redundáns adatok problémaköre, és minden alkalmazás pontos felhasználói adatokkal dolgozhat. Csökkenek az adminisztrációs költségek, nő az előírásoknak való megfelelés képessége, az áttekinthetőség, az auditálhatóság.

#### Megoldások a kockázatok csökkentésére (risk management)

A biztonsági kockázatok terén a cégek számos megoldandó problémával találkoznak, amelyek közül a legfontosabb a jogosultságok kezelése és nyilvántartása. Például az adatbázis-konzolidációk eredményeként több olyan személy is lehet a szervezetben, akik adminisztrátori jogokat gyakorolnak

egy adatbázisban. Szintén jellemző, hogy nem állapítható meg, hogy ki fér hozzá az érzékeny alkalmazásokhoz és adatokhoz. A jelszavak nem kezelhetők biztonságosan, ha egy felhasználónak akár 8 jelszava is lehet különböző rendszerekben, vagy éppen a régi alkalmazottnak és volt szerződéses partnernek is van még hozzáférése a rendszerekhez. A Gartner adatai szerint a volt alkalmazottak 30%-ának még van hozzáférése a cég rendszeréhez, és ez a CIO-k 43%-ának a legnagyobb félelme.

Az Oracle megoldása e problémákra egyrészt az *Oracle Database Vault*, amely a felelősségi körök mentén szétválasztja a menedzsment szintű joggal bíró felhasználókat, másrészt az *Oracle Advanced Security / Oracle Secure Backup*, amely az adatok tárolása, továbbítása és mentése idején is biztonságot nyújt, és a már említett *Oracle Identity Manager / Oracle Access Manager*, amely jól kézben tartható, egyponos felhasználó adminisztráció és egyponos hozzáférés-kezelést biztosít. Alkalmazásukkal automatizálttá válik a felhasználó-követés (belépés, változások, kilépés), a változások azonnal átvezetésre kerülnek a nyilvántartásba, a nyilvántartott jogosultságok azonnal érvényre jutnak, és mód nyílik erős azonosítási technikák (certificate, chipkártya, biomertikus, stb.) használatára is. Mindemellett napjaink egyre népszerűbb szolgáltatás-orientált alkalmazási modelljében (SOA) kiemelkedő fontosságú a webes szolgáltatások (Web Services) védelme és menedzsmentje, amely megoldja a hozzáférés ellenőrzést, az azonosítást és az adatkódolást is. Az Oracle terméke erre a feladatra az *Oracle Web Services Manager*.

#### Megoldások az előírásoknak való megfelelésre (compliance)

Az előírásoknak való megfelelés a nyilvános tőzsdei cégek számára azt jelenti, hogy meg kell felelniük az auditorok által megkövetelt jelentési feltételeknek, de számos nem tőzsdei cég is hasonló helyzetbe kerülhet egyes iparágakban. A megfelelés és a belső előírások miatt is a szervezeteknek el kell határolniuk a feladatokat (pl. Purchasing és Payments hozzáférések elválasztása), és ha ezekre nincs bevezetett informatikai eszköz, akkor a felügyeletet és annak riportálását kézzel kell végezni.

Az *Oracle Audit Vault* szétválasztja a kiváltságos felhasználók hagyományos üzemeltetésre és biztonsági esemény naplózásra vonatkozó felelősségi köreit. Specializált adattárházban tárolja az összegyűjtött, védett audit adatokat. A szoftver emellett képes jelentést készíteni a szabályoknak való megfelelésről. Az *Oracle Identity Manager*, az *Oracle Access Manager*, az *Oracle Identity Federation* és az *Oracle Web Services Manager* pedig összes korábban említett funkcióját maximális naplózási és audit szolgáltatással egészíti ki, teljes áttekintést tudnak nyújtani a pillanatnyi és a historikus jogosultsági helyzetről.

Ezek használatával a cégek képessé válnak arra, hogy megfeleljenek a velük szemben támasztott előírásoknak. Az adatbázis-biztonsági és identity management eszközök megoldják a feladatellátást, külön lehet feljogosítani például a fejlesztőket, az adatbázis-adminisztrátorokat és a Security Officer-eket. A termékekbe épített szolgáltatásoknak köszönhetően az audit automatizálható és alacsony költségek mellett hajtható végre.

#### **Költségek, ROI**

A jogszabályoknak való megfelelés költségei magasak, a CIO Insight magazin tanulmánya szerint a cégek átlagosan az IT munkaerő 12 %-át, az IT budget 8%-át költik erre évente. Az AMR Research szerint a teljes összeg 2005-ben elérte a 15.5 milliárd dollárt. A lehetséges költségek között nem csupán a megfelelő rendszerek, jelentések/beszámolók kialakítását kell számításba venni, hanem ezen felül az esetleges bírságokat, valamint a jó hírnéven esett csorbát, amennyiben a cégnél a felügyeleti szervek hibát találnak.

A korábban már említett költségek leszorításában is nagy szerepet játszik egy felhasználó-, jogosultság és hozzáférés-kezelési projekt. Bár nyilván egy ilyen megoldásnak vannak licenz és bevezetési költségei, de a nagy megtakarítások miatt kiemelkedő az ilyen projektek megtérülése (ROI). Felmérések szerint évente a felhasználónkénti költségmegtakarítás 330 euró csak a helpdesk költségeket tekintve, illetve 1000 euró évente a felhasználónkénti költségmegtakarítás az identity provisioning bevezetésével.

### **Várható trendek**

Az Oracle és a piac többi résztvevője is stratégiai területként kezeli a biztonságot. Termékfejlesztései, a portfólióban végrehajtott egységesítései is ezt támasztják alá.

A gazdálkodó szervezetek fokozódó kontrollja (pl. az adatkezelési előírások kiterjesztése a hazai tőzsdei cégekre is) várhatóan a jövőben csak erősíteni fogja a megfelelési és audit törekvéseket, amelyek egyre több szektorban és egyre kisebb szervezeteknél is integrált felhasználó-, jogosultság és hozzáféréskezelési rendszerek bevezetését fogják indukálni.

\* \* \*

### **Néhány szóban az Oracle cégről**

Az Oracle Corporation a vállalati szoftverek legnagyobb szállítója a világon. A cégről az Oracle weblapjain kaphat bővebb felvilágosítást: [www.oracle.com](http://www.oracle.com).

### **Védjegyek**

*Az Oracle, a JD Edwards, a PeopleSoft és a Siebel az Oracle Corporation és/vagy társult vállalatainak bejegyzett védjegye.*

### **További információ:**

Kerekes Anita  
PR menedzser  
Oracle Hungary Kft.  
tel: 224 1783  
mobil: 30 436 2702  
anita.kerekes@oracle.com

Markovits Péter  
Műszaki tanácsadó  
Oracle Hungary Kft.  
Tel: 224 1744  
Mobil: 30 914 6612  
peter.markovits@oracle.com

Mosolygó Ferenc  
Műszaki tanácsadó  
Oracle Hungary Kft.  
Tel: 224 1735  
Mobil: 30 966 5997  
ferenc.mosolygo@oracle.com