

Sealog

HOGY AZ INFORMÁCIÓ VÉDVE LEGYEN!

„Egy cég információvagyonát érintő károkozás az esetek többségében jóval a bekövetkezés időpontja után jut a károsult tudomásra. Utólag az események bizonyítása körülményes, az elkövető(k) személye, az okozott kár mértéke pedig nehezen meghatározható...”

VISSZAÉLÉSEK, CSALÁSOK

Az információ: hatalom, mellyel lehet élni és visszaélni; más megfogalmazásban áru, amit adnak-vesznek. Egy vállalat feladatainak hatékony végrehajtása egyre növekvő mértékben függ az informatikai és információs rendszerek zavartalan működésétől. Kulcskérdéssé vált az adatok, információk hitelességének, bizalmasságának, és sértetlenségének, vagyis összességében ezek rendelkezésre állásának megőrzése. Ugyanakkor mára a korrupció és a visszaélések az üzleti életben mindennaposakká váltak. Az elhúzódó válság egyik hatásaként a romló gazdasági környezetben a csalások, visszaélések is elszaporodtak. Az ACFE (Association of Certified Fraud Examiners) egy tanulmánya szerint a vállalatok árbevételeinek 6 százaléka eshet áldozatul a visszaéléseknek. Ez az arány igen jelentős, tehát a cégvezetőknek kiemelt figyelmet kell fordítaniuk a probléma kezelésére, és ezzel együtt a csalások megelőzésére is. Nemzetközi tapasztalatok szerint az információk kiszivárogtatását 70%-ban az alkalmazottak, vagy helyismerettel rendelkező munkatársak (vagy volt munkatársak) követik el.

Néhány lehetséges károkozási forma:

- ▶ a bizonylati fegyelem, a normatív rendelkezések kijátszása ellenőrizhetetlen adatkezelési műveletek végrehajtása visszaélés, csalás, jogtalan előnyyszerzés céljából;
- ▶ üzleti titkok kiszolgáltatása, jogosulatlan adatszolgáltatás, szándékos károkozás imázs rombolás céljából;
- ▶ közreműködés szolgáltatások jogosulatlan igénybevitelében;
- ▶ szolgáltatók, outsourcing partnerek szabálytalan információ szerzése/kezelése;
- ▶ döntés-előkészítési, döntési tevékenysé-

gek ellenőrizetlenségére építő, üzleti etikát sértő cselekedetek;

- ▶ informatikai rendszerekbe, hálózatokba történő behatolás károkozási céllal (adatrombolás, adatok megváltoztatása);

A visszaélések megakadályozására nem elég a megszokott módokon védekezni, a fizikai védelmen túl a rendszerek minden elemére ki kell dolgozni védelmi eljárásokat.

FELDERÍTÉS, MEGELŐZÉS

A visszaélések elleni küzdelem egyik legfontosabb eleme a megfelelő tervezés, de egyelőre még nagyon kevés olyan cég van, ahol létezik, és hatékonyan működik visszaélés elleni védekezést támogató irányítási rendszer. Egy ilyen irányítási rendszer legfontosabb elemeit a szabályozások és szabályzatok (például pénzmosás elleni, illetve a biztonsági), valamint a rendszerek működtetését szolgáló képzések és gyakorlatok jelentik. Ezek kialakítása a legtöbb cégnél megtörténik, de ha hiányzanak a csalásellenes fellépést szolgáló eszközök és hiányoznak a működtetési-eljárási tervek, akkor kisebb az esélye a felderítésének. A csalások hatékony megelőzéséhez nélkülözhetetlenek a megfelelően működő, függetlenített belső ellenőrzés, a csalás megelőzési vállalati programok, továbbá olyan informatikai támogató rendszer, amely a feladatok végrehajtását hatékonyra teszi.

A FELADAT MEGOLDÁSA A SEALOG LOGELEMZŐ RENDSZERREL

A **Sealog** feladata a különböző informatikai rendszerek használatának felügyelete és ellenőrzése, az informatikai eszközökkel megvalósítható visszaélések felderítésének, a visszaélések megelőzésének támogatása az egyedi rendszerek használata során felderíthető rejtett összefüggések elemzésével, az időben elhúzódó folyamatok összetett vizsgálatával.

A **Sealog** egy adatpiac alapú megoldás, amely a cég által alkalmazott informatikai/információs rendszerek közül kiválaszthatóan a belső audit szempontjából fontos rendszerek napló adatait jól strukturált módon, elemzésre alkalmas formában tárolja. A **Sealog** működése során nem csak a különböző rendszerekből átvett adatokat tisztítja, rendszerezi, hanem speciális üzleti logika alkalmazásával a(z esetlegesen) visszaélés-

re gyanút adó adatkombinációk esetén automatikus riasztást is küld a biztonsági menedzserek felé. Újabb és újabb szolgáltatások beépítésével és az elérési ponton bekövetkezett történések tipizált feldolgozásával átfogó információt tudunk nyújtani magának a szolgáltatásnak az igénybevételéről és felhasználási módjáról is. Biztosítjuk a rendellenes beavatkozások kiszűrését, a gyanús hozzáférések folyamatos figyelését.

Megoldásunk előnye, hogy a gyorsan változó környezeti adottságokhoz könnyen adaptálható. Nemcsak előzetes ismeretek, dokumentációk alapján lehet a figyelendő eseményeket meghatározni, hanem támogatást nyújt ahhoz is, hogy a felhasználók – akik akár az informatika azon területén nem is jártasak – a rendszerezett és áttekinthetővé tett logok elemzésével maguk is felfedezzenek gyanús, vagy rendellenes eseményeket. Ezek rendszeres figyelését fejlesztői közreműködés nélkül is beállíthatják.

Erőssége, hogy egy „előre mutató” megoldást kap kezébe a megrendelő, melyben a keretrendszer olyan szintre képes kinőni magát, hogy a belső biztonságért felelős szervezetek központi támogató alkalmazásává lépjen elő. A **Sealogba** beépített funkciók és modulok biztosítják a többlépcsős, folyamatos fejlődés lehetőségét:

- ▶ A kezdeti „egyszerű” log elemzésből kiindulva eljuthat a felhasználó arra a szintre, hogy összetett szabályok alapján egymástól logikailag távol lévő és látszólag össze nem függő rendszerek között átvívelő eseményeket, gyanús összefüggéseket vizsgáljon.
- ▶ A kezdeti „egyszerű” riasztáson túllépve a felhasználó definiálhat egy olyan speciális munkafolyamatot (workflow), melynek mind a lépései, mind a felmerülő adatigényei a rendszer által támogatottak.
- ▶ A kezdeti „egyszerű” heti jelentéseken túl a rendszer adattárházi/adatpiaci felépítését kihasználva a felhasználó komplex mérő- és mutatószám rendszer kialakítására kap lehetőséget, melynek segítségével kialakíthat egy olyan biztonsági BSC (Balanced Scorecard) alkalmazást, mely mind a felső vezetés információ igényét, mind a külső adatszolgáltatási kötelezettségeket kielégíti.

Pókó István,

üzletfejlesztési igazgató
Seacon Europe Kft.