Digitális nyomelemző rendszer

Probléma felvetés

„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…”

Az informatikai eszközökkel támogatott üzleti rendszerekre egyre több fenyegetés irányul, ezek kapcsán egyre nagyobbak a kockázatok, és egyre több kár keletkezik. A vállalat informatikai és informatikai biztonsági vezetésének kihívásai hatalmasak. Botok, férgek és hackerek kívülről, adatlopási, lopási, csalási kísérletek pedig belülről fenyegetik a rendszereket. A gazdasági válság pedig erősíti ezeket a fenyegetéseket.

Másik oldalról viszont a központi és helyi szabályozások javítása, finomítása csökkenti a kockázatokat, és segít megelőzni a káros események megvalósulását. A fentiek miatt egyre nagyobb kihívás az üzleti folyamatok, és az üzleti adatok, információk védelme. Ezt a kihívást automatizált biztonsági és megfelelőségi ellenőrzésekkel lehet hatékonyan támogatni.

Alapkoncepció

A különböző vállalati rendszerek naplóadatai egyre szélesebb körben állnak rendelkezésre. Megfelelő feldolgozással és elemzéssel hatékonyan állíthatók elő ezekből jelzések/figyelmeztetések/riasztások a külső/belső támadásoktól a visszaéléseken keresztül a csalások felderítéséig, illetve gyűjthetők információk a törvényi, biztonsági és egyéb szabályozási megfelelőségről.

A rendszer kialakításakor egy olyan szemléletet kell követni, amely szerint a különböző — akár nem informatikai jellegű — rendszerek releváns eseményeit egy közös eseménytérben képezzük le, amelyet aztán automatikus, informatikai módszerekkel is lehet értelmezni, és a kapott eredményeket a felhasználók által értelmezhető és tovább feldolgozható formában is meg lehet jeleníteni.

Az általánosan elterjedt megközelítéssel ellentétben nemcsak az informatikai rendszerekben keletkező napló (log) rekordokat kell feldolgozni, hanem minden egyéb olyan adatot is, amelyekből egy adott folyamat összes lépése megbízhatóan visszakövethető, rekonstruálható. Meghatározásunk szerint ez a ***digitális nyom***. Tehát a digitális nyom gyűjtőfogalmába, a hagyományos napló bejegyzések mellett a felhasználói rendszerek operatív adatait is beleértjük, sőt ide tartozóként határoztuk meg az egyedileg képzett — akár kézzel rögzített — adatokat, kiegészítő információkat is. Így a rendszer komplexitásában tudja vizsgálni az időben elhúzódó és/vagy térben is elkülönülő rendszerekben futó folyamatokat.
A digitális nyomok keresését az üzletileg kritikus folyamatok mentén érdemes végezni, ezért egy ilyen rendszer kiépítését célszerűen kockázatelemzéssel kell kezdeni. A kockázatelemzés során meghatározzuk a biztonsági és/vagy üzleti szempontból legérzékenyebb rendszereket és folyamatokat, és az ezek mentén gyűjtendő naplóadatok/operatív adatok körét, melyeket első körben javasolt bekötni a nyomelemző rendszerbe.

A külső és/vagy belső visszaélések elleni küzdelem több szervezeti funkcionális terület együttműködését is feltételezheti. Az IT, az IT biztonság, a vállalati biztonsági felügyelet, és az audit

szervezet saját, vagy közös céljaik elérése, és a kapcsolódó feladataik megoldása céljából egymástól függetlenül, vagy szorosan együttműködve is alkalmazhatják a rendszert. Összefoglalva:

A nyomelemző rendszer feladata a különböző informatikai rendszerek által rögzített „digitális nyomok" összegyűjtése, a nyomgyűjtés felügyelete és ellenőrzése, majd a forrásadatok feldolgozásával a rendellenességek feltárása, esetleges fenyegetések, visszaélések felderítése, az ilyen típusú események megelőzésének támogatása a rendszerek használata során felderíthető rejtett összefüggések elemzésével, az időben elhúzódó folyamatok összetett vizsgálatával.

A rendszer működése

A rendszer – természetesen - moduláris felépítésű. Az egyes főbb funkciókat külön rendszerkomponensek reprezentálják, amelyeket igény esetén mind fizikailag, mind logikailag külön helyre (külön helyszín, kiszolgáló, operációs rendszer, stb.) lehet telepíteni. A moduláris felépítésből eredő másik előny, hogy a rendszer rugalmasan illeszthető már meglévő információbiztonsági rendszerekhez, eszközökhöz akár input, akár output oldalon. Működését/funkcióit az alábbi szintekre lehet osztani:

- **Nyomgyűjtés (technológiai szint)**
  - Intelligens nyomgyűjtés
  - Előszűrés, időpecsét,
  - Ütemezett, titkosított kommunikáció
  - Végpont/központ kiesés kezelése
  - Azonnali riasztás külön csatornán
  - Koncentrátor/Interfész/3rd party kezelés

- **Feldolgozás (technológiai szint)**
  - Adattisztítás, konszolidálás
  - Egységesítés
  - Központi struktúrába töltés
  - Dimenzionálás
  - Adatpiac frissítés

- **Felderítés/Elemzés (operatív szint)**

- Szabálymenedzselés
- Riasztás
- Jelentésgenerálás
- Elemzés
- Biztonsági naplózás

- **Mesterséges Intelligencia (kiemelt szakértői szint)**
  - Adatbányászat/Hasonlóságelemzés
  - Automatikus szabályfelismerés
  - Előrejelzés (predikció)
  - Trendanalízis
  - Szakértői vélemény generálás

Bevezetés feltételei

Minden rendszer használati értéke nagyban függ a benne lévő adatok minőségétől és mennyiségétől. Ez kiemelten igaz egy digitális nyomelemző rendszerre, mely más alkalmazások/eszközök adataiból építkezik. Tehát mindenekelőtt a forrásrendszerekre vonatkozóan a digitális nyomoknak:

- léteznie kell abban a mélységben és tartalomban, amely a figyelés szempontjából elvárt
- vezetődnie kell abban a frekvenciában, megbízhatósággal és következetességgel, amely a figyelés szempontjából elvárt
- hozzáférhetőnek kell lennie: direkt, vagy közvetett módon importálható formátumú és tartalmú legyen

A fentiek figyelembevételével könnyen belátható, hogy az ilyen típusú rendszereket nem egy projekt, hanem egy projekt láncolat vagy inkább cselekvési program keretében kell bevezetni lehetőleg az alábbi lépések szerint:

- **Projekt1 (vertikális implementáció)**
  - Nyomelemző keretrendszer technológiai implementálása
  - Kommunikációs csatornák kialakítása (rendszerek, üzenetküldő szerverek, koncentrátorok között)
  - Testre szabás (interfészek készítése, adatkonvertáló eljárások kialakítása, esemény figyelési logika kidolgozása)
  - Próbaüzem/döntés a továbblépésről

- Javaslat: max. 3-5 rendszer első lépésben!

- **Projekt 2…n (horizontális kiterjesztés)**
  - Előkészített rendszerek folyamatos bekötése

Több lépcsős fejlődési/tanulási lehetőségek

A felhasználók betanulása szempontjából nagyon előnyös, hogy a rendszerben található funkciók és modulok – a bevezetéssel szinkronban - biztosítják a több lépcsős, folyamatos fejlődést:

- A kezdeti „egyszerű” log elemzésből kiindulva eljuthat a felhasználó arra a szintre, hogy összetett szabályok alapján ne csak az egyes rendszerek rekordjait vizsgálja, hanem egymástól logikailag távol lévő és látszólag össze nem függő rendszerek között átívelő eseményeket, gyanús összefüggéseket vizsgáljon. Ezek rendszeres figyelését fejlesztői közreműködés nélkül is beállíthatják a felhasználók.

- A kezdeti „egyszerű” riasztáson túllépve a felhasználó definiálhat egy olyan speciális munkafolyamatot (workflow), melynek mind a lépései, mind a felmerülő adatigényei (akár bizonyítékképzési szinten) 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 kihasználásával kialakíthat egy olyan biztonsági BSC (BalancedScorecard) alkalmazást, mely az előírt belső folyamataira illeszkedve mind a felső vezetés információ igényét, mind a külső adatszolgáltatási kötelezettségeket kielégíti.

- A szakértői szint bevezetésével különböző Üzleti Intelligencia alkalmazások használata lehetséges. A tranzakciós adatbázishoz illeszthetők olyan BI csomagok, amelyekkel az ad-hoc elemzési szolgáltatásokat bővíteni lehet.