BalaBit IT Security

Megfelelés a BSZT és a BAT IT biztonsági előírásainak

befektetési vállalkozások számára

Szigorú törvényi előírások, kötelező IT audit

A befektetési vállalkozásokról és az árutőzsdei szolgáltatókról szóló 2007. évi CXXXVIII. törvény (Bszt.) 12.§-a kötelezően előírja a fenti szolgáltatóknak IT rendszereik *kockázatokkal arányos védelmét*. A törvény értelmében a szolgáltatóknak IT rendszerük biztonságos működését felügyelő **informatikai ellenőrző rendszert** kell kiépíteniük és üzemeltetniük. Ennek keretében gondoskodniuk kell többek között a biztonsági rendszerük zártságáról, a kritikus rendszerelemek (eszközök, folyamatok, személyek) azonosításáról, a felhasználók szabályozott hozzáférés-kezeléséről, a kritikus események naplózásáról, a távadatátvitel biztonságáról, illetve a rendszereik vírusvédelméről is.

A Bszt. 2012. január 1-től kiegészült a befektetési alapkezelőkről és a kollektív befektetési formákról szóló 2011. évi CXCIII. (Bat.) törvénnyel. A Bat. **további szigorításokat** tartalmaz az alapkezelők IT rendszereivel kapcsolatban:

§ A befektetési alapkezelő olyan nyilvántartási rendszert köteles fenntartani, amely biztosítja a nyilvántartási adatok **8 évig történő megőrzését és visszakereshetőségét**, mindezt az adat-manipulációval szemben történő védelemmel ellátva (CXCIII. tv. 15.§).

§ A befektetési alapkezelőnek rendelkeznie kell az elektronikus adatfeldolgozásra vonatkozó **ellenőrzési és biztonsági eljárásokkal**; az információk biztonságának, integritásának és bizalmas jellegének megőrzésére alkalmas rendszerekkel, és a megfelelő belső ellenőrzési mechanizmussal, beleértve különösen az alkalmazottai által lebonyolított személyes ügyleteket (20.§).

§ 2012. április 30-ig **könyvvizsgálói igazolást** kell a Felügyelet felé bemutatni arról, hogy a befektetési alapkezelő informatikai, nyilvántartási rendszere a törvény rendelkezéseinek megfelel (154.§).

A törvény rendelkezéseinek figyelmen kívül hagyása súlyos anyagi és/vagy személyi következményekkel járhat, sőt a hatóságok akár a tevékenység végzésére jogosító engedélyt is felfüggeszthetik!

Az audit arra is kiterjed, hogy az üzemeltetett IT rendszer *biztonság, illetve ellenőrizhetőség szempontjából megfelel-e a törvény rendelkezéseinek*. Az IT auditorok szigorú biztonsági követelményeket támasztanak az érintett vállalkozásokkal szemben, és a megfelelés jelentősen megterhelheti e cégek informatikai büdzséjét. Jogosan merülhet fel a kérdés, hogy miként lehet a vonatkozó rendelkezéseknek - és a közelgő auditnak - a lehető legkisebb emberi és anyagi ráfordítással megfelelni.

Hogy tud a BalaBit a költséghatékony megfelelésben segíteni?

Shell Control Box – Független audit eszköz

A Shell Control Box (SCB) egy **tevékenység-felügyeleti megoldás**, amely az adminisztrátorok és felhasználók IT rendszerekhez való távoli hozzáférését szabályozza és auditálja. A Bat. 20.§-a előírja megfelelő belső ellenőrzési mechanizmusok kiépítését, beleértve különösen az alkalmazottak által lebonyolított személyes ügyletek ellenőrzését. Az SCB-vel rögzíthető és filmszerűen visszanézhető, hogy ki, mikor és mihez fért hozzá a kritikus adatokat tároló pénzügyi rendszerekben. Az SCB-vel részletes, felhasználói szintű hozzáférési házirend alakítható ki, amely kikényszeríti, hogy csak az arra jogosult felhasználók érjék el az érzékeny pénzügyi adatbázisokat. Az adatvesztés, adatmanipulálás kockázata is csökken, hiszen a felhasználói tevékenység korlátozása és rögzítése révén nemcsak technikai, de pszichológiai gátat is jelent a rossz szándékú hozzáférések ellen.

Pénzügyi szolgáltatóknál tipikus, nagy kockázattal járó probléma, hogy a pénzügyi rendszerüket (pl. az értékpapír BackOffice alkalmazást) sokszor a külső szállító távolról menedzseli. Az SCB a külső IT szolgáltató adminisztrátorainak tevékenységét is auditálja, és mivel az eszköz független az adminisztrátortól és az adminisztrált szerverektől is, egyedi lehetőséget nyújt a pénzügyi alkalmazások naplóinak és jelentéseinek kiegészítésére. Az SCB a teljes adminisztratív forgalmat (beleértve a konfigurációk módosításait, paraméterezést, végrehajtott parancsokat, verzióváltást, stb.) titkosított, időpecséttel ellátott és digitálisan aláírt állományokban tárolja, meggátolva a felvételek utólagos manipulálását. Az SCB-vel testreszabott jelentéseket is készíthet a felhasználók tevékenységéről, mellyel felgyorsítható az audit folyamata. Tipikus felhasználási területek:

- Iparági szabványoknak (PCI-DSS, Bazel II/III, stb.) és törvényeknek (Hpt., Bszt., stb.) való megfelelés,
- Privilegizált felhasználók (pl. rendszer-adminisztrátorok, vezetők) hozzáférésének szabályozása,
- Külső IT szolgáltató partnerek ellenőrzése (SLA control),
- Vékonykliens felhasználók (pl. brókerek, ügyfélszolgálati munkatársak) tevékenység-felügyelete.

syslog-ng termékcsalád - Megbízható naplózó-infrastruktúra

A Bszt. 12§ (6)/d. pontja előírja kritikus folyamatok eseményeinek naplózását, a naplózás rendszeres értékelését, és a nem rendszeres események kezelését. A BalaBit syslog-ng alkalmazása **teljes körű naplómenedzsment** eszközként használható: az operációs rendszerek, alkalmazások naplóüzeneteit a jogszabályi előírások szerint gyűjti, osztályozza, szűri, tárolja, és hosszú távon archiválja. A rendszer egy hatékony platformot kínál, amely üzenetek tízezreit képes valós időben osztályozni, hogy kiszűrje a megszokottól eltérő eseményeket, és szükség esetén azonnal riasszon.

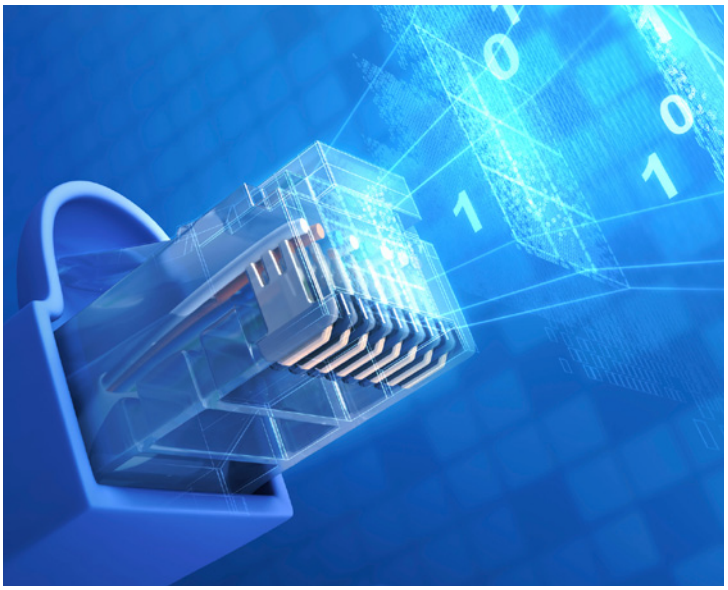
A syslog-ng alkalmazás segít a naplózó rendszer biztonságossá tételében is, mivel a naplóadatokat titkosítva, aláírva és időpecséttel ellátva tárolja, meggátolva ezzel a naplók utólagos manipulálását. Képes tehát teljesíteni azokat a törvényi követelményeket is, amelyek az információk biztonságával, integritásával és bizalmasságával összefüggésben merülnek fel. A Bat. előírja, hogy a nyilvántartási adatokat 8 évig meg kell őrizni – ezt a folyamatot a BalaBit megoldása leegyszerűsíti, mivel a fontos naplóüzeneteket egy központi helyen tárolja, és rendszeres időközönként archiválja. A syslog-ng segít a megfelelőségi auditok és belső ellenőrzések zökkenőmentes levezénylésében, és egyszerűsíti a bizonyítékok feltárását a forensics vizsgálatok során.

Tipikus felhasználási területek:

- Iparági szabványoknak (PCI-DSS, Bazel II/III, stb.) és törvényeknek (Hpt., Bszt., stb.) való megfelelés,
- Rendszer-felügyelet és biztonság menedzsment,
- IT audit és forensics vizsgálatok,
- SIEM optimalizáció.

Zorp - Hálózati határvédelem

A BalaBit Zorp egy **robusztus határvédelmi megoldás**, melyet kiterjedt informatikai hálózattal rendelkező nagyvállalatok és más, magas biztonsági igényű intézmények számára fejlesztettek ki. A Bszt. 12.§-a rendelkezik a távadatátvitel bizalmasságáról, hitelességéről, és a rendszer biztonsági kockázattal arányos vírusvédelméről. A Zorp a hálózati forgalom aprólékos elemzéséből nyert információk alapján lehetőséget ad, hogy kompromisszumok nélkül implementálja a jogszabályok hálózatokra vonatkozó biztonsági előírásait. Beépülő vírusszűrő modulja biztosítja az elvárt szintű vírusvédelmet. Az alkalmazásszintű határvédelmi technológia által nyújtott védelem alkalmas egyedi, speciális IT biztonságtechnikai problémák megoldására is. Éppen ezért tipikus felhasználói az államigazgatási és a pénzügyi szektorból kerülnek ki.



BalaBit IT Security

A BalaBit a világ egyik vezető IT-biztonsági szoftverfejlesztő vállalata a magas jogosultságú felhasználók monitorozása, a naplógyűjtés és -tárolás valamint az egyedülálló proxy technológián alapuló tűzfal megoldások területén. Innovatív technológiai megoldásaival a külső és belső fenyegetések megelőzésében, valamint az IT-biztonsági és megfelelőségi előírások betartásában támogatja ügyfeleit. A nyílt forráskódú közösség elkötelezett tagjaként a vállalat megoldásai minden főbb platformot támogatnak az összetett és heterogén IT rendszerekben, fizikai, virtuális és felhő alapú környezetekben egyaránt. A teljes mértékben magyar tulajdonú BalaBit 2009-ben és 2010-ben is felkerült a régió leggyorsabban növekvő technológiai vállalatait rangsorba állító Deloitte Technology Fast 50 listára. A vállalat képviselettel rendelkezik Franciaországban, Németországban, Olaszországban, Oroszországban és az Egyesült Államokban, ügyfelei és partnerei világszerte valamennyi lakott kontinensen megtalálhatók.

- Bövebben: www.balabit.hu

További információ

2007. évi CXXXVIII. törvény (Bszt.)

2011. évi CXCIII. törvény (Bat.)

Shell Control Box audit eszköz

syslog-ng naplózó termékcsalád

Zorp határvédelmi rendszer

Kérjen visszahívást