BalaBit IT Security

MEGFELELÉS AZ ÚJ ADATVÉDELMI TÖRVÉNY ELŐÍRÁSAINAK

Szolgáltató vállalatok számára

Szigorú törvényi követelmények

2012. január 1-jén hatályba lépett az **Információs önrendelkezési jogról és az információszabadságról szóló (2011. évi CXII.) törvény**, rövidebb nevén az új adatvédelmi törvény.

A korábbi, gyakorlatilag szankciókat nem tartalmazó szabályozást egy jóval rigorózusabb gyakorlat váltotta fel. A változások nagymértékben érintik az adatkezelést vagy adatfeldolgozást végző szolgáltató cégek működését is, különös tekintettel a tömeges ügyfélkapcsolat-kezelést végző cégekre, mint például a pénzügyi, távközlési, közüzemi szolgáltatók vagy az online áruházak. A törvény 7.§-a ugyanis kimondja, hogy az adatkezelő **köteles teljes körűen gondoskodni** az általa kezelt **személyes adatok biztonságáról**, köteles továbbá megtenni az ehhez szükséges technikai és szervezési intézkedéseket! A 7.§ (5) pontja értelmében a személyes adatok automatizált feldolgozása során az adatkezelőnek biztosítania kell:

- a jogosulatlan adatbevitel megakadályozását;
- az automatikus adatfeldolgozó rendszerek jogosulatlan személyek általi használatának megakadályozását;
- annak ellenőrizhetőségét, hogy a személyes adatokat adatátviteli berendezés alkalmazásával mely szerveknek továbbították;
- annak ellenőrizhetőségét, hogy mely személyes adatokat, mikor és ki vitte be az adatfeldolgozó rendszerekbe;
- a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát, és
- azt, hogy az automatizált feldolgozás során fellépő hibákról jelentés készüljön.

Hatósági szankciók, adatvédelmi audit

A törvény létrehozta a **Nemzeti Adatvédelmi és Információszabadság Hatóság**ot, melynek jogköre - autonóm államigazgatási szervként - jelentősen kiszélesedett a korábbi Adatvédelmi Biztos intézményéhez képest. Az új hatóság ugyanis már szabálysértési-, büntető-, sőt akár bírósági eljárást is kezdeményezhet a törvény rendelkezéseit megszegő szolgáltatókkal szemben, megtilthatja a további adatkezelést, és - akár többször is - 10 millió forintig terjedő bírságot szabhat ki!

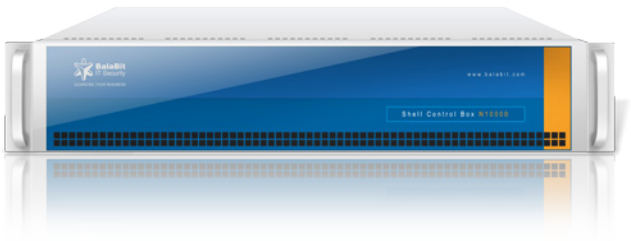
Az Hatóság az adatkezelő kérelmére 2013. január 1-től **adatvédelmi auditot** is lefolytathat. Az audit célja az adatkezelési műveletek hatósági értékelésén keresztül a **magas szintű** adatvédelem és adatbiztonság megvalósítása. Az adatvédelmi audit eredményét a Hatóság az auditról készített értékelésben rögzíti, mely értékelés alapesetben nyilvános. Az adatvédelmi audit a Hatóság egyéb hatásköreinek gyakorlását azonban nem korlátozza!

Hogyan segíti a BalaBit a törvényi megfelelést?

Shell Control Box

FELHASZNÁLÓK TEVÉKENYSÉG-FELÜGYELETE

Mint fent is látható, az adatvédelmi tv. előírja a személyes adatok bevitelének és továbbításának ellenőrizhetőségét. A BalaBit Shell Control Box (SCB) egy tevékenység-felügyeleti berendezés, amely a szerverekhez való távoli hozzáférést ellenőrzi, és a rendszerekhez csatlakozó felhasználók munkafolyamatait rögzíti. Rögzítheti például a központi ügyfél-adatbázishoz hozzáférő munkatársak tevékenységét, vagy az SAP szerveren dolgozó adatrögzítők munkáját. A rögzített audit állományok filmszerűen visszajátszhatóak, így az események pontosan úgy tekinthetők meg, ahogy azok megtörténtek. Ez által megvalósítható a törvény által előírt ellenőrizhetőség. Az SCB segítségével tehát bármikor megállapítható, hogy ki, mikor, mit csinált az adatfeldolgozó rendszerben, így egyfajta pszichológiai gátat is jelent a rosszindulatú adatmanipulációval, adatlopással, stb. szemben.



Minden munkafolyamat titkosított, időpecséttel ellátott és digitálisan aláírt audit állományokban kerül tárolásra, biztosítva a személyes adatok bizalmasságát és az ellenőrzés hitelességét.

Gyors jelentések és hibaelhárítás

A törvény megköveteli, hogy a fellépő hibákról jelentés készüljön (7.§/(5)/f). Az audit állományok tartalma kereshető, és az eredményekből automatikus riportok készíthetők. A rögzített audit állományok teljes körű dokumentációt nyújtanak egy esetleges hiba esetén. Bármilyen hiba (pl. jogosulatlan adatbázis módosítás, váratlan leállás) lép fel, az esemény körülményei rögtön hozzáférhetőek ezekben az állományokban, így az incidens oka könnyedén megállapítható. Ez által üzemzavar esetén a helyreállítás is látványosan felgyorsítható, segítve ezzel a törvény katasztrófa utáni helyreállíthatóságára vonatkozó rendelkezését (7.§/(5)/e).

Részletes hozzáférés-vezérlés

Az SCB a kritikus adatfeldolgozó szerverekhez történő hozzáféréseket részletesen szabályozza, azaz képes megakadályozni, hogy jogosulatlan személyek érjenek el erőforrásokat a védett szervereken. Ez által kielégíthető a törvény jogosulatlan rendszer-használat megakadályozását előíró pontja (7.§/(5)/b).

Auditok támogatása

Független audit eszközként az SCB segít az adatvédelmi auditok levezénylésében is, hiszen teljes körű és hiteles bizonyítékként szolgál az adatkezelők tevékenységéről, gyors keresési és részletes jelentéskészítési funkciói révén pedig felgyorsítja az audit folyamatot.

syslog-ng

MEGBÍZHATÓ NAPLÓ-KEZELÉS

A törvény sokat idézett 7.§-a megköveteli a személyes adatok feldolgozásának ellenőrizhetőségét, valamint az üzemzavar utáni helyreállíthatóságot. 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 naplóbejegyzések eredeti bizonylatként is felfoghatók az IT környezetben, melyek az adatfeldolgozó rendszerekben történt eseményeket (pl. a személyes adatokkal kapcsolatos tranzakciókat) is részletesen gyűjtik és tárolják. Üzemzavar esetén egyszerűbben megtalálja a hiba körülményeire vonatkozó bizonyítékokat, hiszen a központilag gyűjtött naplóüzenetek könnyedén szűrhetők és kereshetők. A megoldás közel 50 különböző platformról képes gyűjteni az üzeneteket, így a legtöbb nagyvállalati és intézményi környezetbe könnyen integrálható.

Hiteles jelentések

A syslog-ng alkalmazás segít az ellenőrző 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, amelyek a személyes adatok biztonságával és bizalmasságával összefüggésben merülnek fel.

A hiteles naplók alapján testre szabható jelentések is készíthetők, kielégítve ezzel a vonatkozó törvényi előírást, és támogatva ezzel az IT üzemeltetést és az auditokat egyaránt.

Zorp Gateway

ADATFELDOLGOZÓ SZERVEREK SPECIÁLIS VÉDELME

A BalaBit Zorp egy robusztus határvédelmi megoldás, melyet kiterjedt informatikai hálózattal rendelkező nagyvállalatok és más, magas biztonsági igényű intézmények számára fejlesztettek ki. A Zorp a hálózati forgalom aprólékos elemzéséből nyert információk alapján lehetőséget ad, hogy kompromisszumok nélkül implementálja a hazai jogszabályok hálózati biztonsági előírásait. Nem csak általános tűzfalként, de az adatfeldolgozó szerverek védelmére is használható, hiszen az alkalmazás-kiszolgáló elé telepítve protokollellenőrzésre és a szerver biztonsági hiányosságainak kiküszöbölésére is alkalmas.

Single Sign On autentikáció

Az adatvédelmi törvény 7.§-a előírja az adatfeldolgozó rendszerek jogosulatlan használatának megakadályozását. A Zorp segítségével lehetővé válik a hálózati átjárón átmenő összes kapcsolat autentikálása. A hálózati autentikáció célja a felhasználók által kezdeményezett kapcsolatok hitelesítése, annak érdekében, hogy csak a megfelelő személyek érhessenek el bizonyos szolgáltatásokat. A Zorp nyújtotta megoldással a teljes hálózati forgalom a felhasználók szintjén azonosítható és auditálható. A jelszavas és erős autentikációs metódusokat (S/Key, SecureID, X.509, stb.) egyaránt támogatja, biztosítva ezzel, hogy a jogosulatlan munkatársak ne érjék el a személyes adatokat tároló adatfeldolgozó rendszereket.

Konklúzió

A BalaBit megoldásai nagymértékben elősegítik az új adatvédelmi törvény adatbiztonsági előírásainak való megfelelést, melyet az alábbi táblázatban foglaltunk össze:

Törvényi előírás	Javasolt BalaBit termék
7.§/(5)/a. Jogosulatlan adatbevitel megakadályozása	**SCB, Zorp**
7.§/(5)/b. Jogosulatlan személyek hozzáférésének megakadályozása	**SCB, Zorp**
7.§/(5)/c. Személyes adatok továbbításának ellenőrizhetősége	**SCB, syslog-ng**
7.§/(5)/d. Személyes adatok felvitelének ellenőrizhetősége	**SCB, syslog-ng**
7.§/(5)/e. Üzemzavar esetén történő helyreállíthatóság	**SCB, syslog-ng**
7.§/(5)/f. Hibajelentések	**SCB, syslog-ng**

A BalaBit az egyik legnagyobb hazai IT biztonsági gyártóként rendkívül erős terméktámogatást kínál ügyfeleinek.

További információ: www.balabit.hu