QUADRON RENDSZER Információvédelmi Kft. // 1051 Budapest, Sas u. 10-12.
Fax: +36 (1) 796 3253 // e-mail: info@quadron.hu // www.quadron.hu

A QUADRON RENDSZER Kft. az általa kínált termékekkel és szolgáltatásokkal felkészült, és tapasztalt szakembereivel képes kialakítani azt a komplex megoldásrendszert, amivel **2013. évi L. törvény** előírásait az állami szervek teljesíteni tudják.

Mit tartalmaz az 2013. évi L. törvény?

A jogalkotók 2013-ban törvényt hoztak az államigazgatási szervek elektronikus információbiztonsági követelményeiről. Ez az új jogszabály egy olyan modern, nemzetközi szabványokon alapuló, komplex biztonsági rendszer kialakítását és működtetését írja elő, amivel az államigaztatási folyamatokat befolyásoló számítástechnikai kockázatok hatékonyan csökkenthetők.

A törvény zárt, teljes körű, folytonos és a kockázatokkal arányos védelmet ír elő, amelyet az elektronikus információs rendszer minden elemére és azok teljes életciklusában meg kell valósítani. A kezelt adatok bizalmasságát, sértetlenségét és rendelkezésre állását biztonsági besorolásuknak megfelelő módon kell garantálni. Ennek érdekében védelmi intézkedések összefüggő rendszerét kell kialakítani, ami adminisztratív, fizikai és logikai elemekből épül fel. Ezeknek támogatniuk kell azt, hogy a biztonsági incindensek észlelhetőek legyenek, azokra megfelelően reagálhasson a szervezet, valamint képes legyen akár ezek megelőzésére vagy korai felismerésére is.

A törvény előírásainak megfelelő zárt, teljes körű és folytonos adatbiztonsági rendszer szabályozási elemekből, időszakos vagy rendszeres, folyamatokba épülő, manuális, vagy számítástechnikai eszközökkel támogatott ellenőrzési lépésekből, teljesen automatizált biztonsági céleszközökből és a biztonsági tudatosságot javító oktatásokból kell, hogy felépüljön. A törvény betartásáért a szervezet vezetője felel, neki kell kijelölnie vagy megbíznia azt a személyt, aki az elektronikus információs rendszerek biztonságáért felelős.

A biztonsági rendszer kockázatokkal arányos kialakításának alapját egy besorolási rendszer adja:

A szervezetben kezelt adatokat az azokat kezelő információs rendszerenként 1-től 5-ig tartó skálán kell értékelni három szempont alapján: bizalmasság, sértetlenség és rendelkezésre állás. A magasabb számozás magasabb védelmi igényt is kell, hogy jelentsen. A biztonsági osztályokba sorolást és az azokhoz tartozó, egyre szigorúbb védelmi intézkedéseket a szervezet információbiztonsági szabályzatában kell rögzíteni.

A biztonsági szabályzatoknak a következőkből kell legalább állnia:

- Informatikai Biztonsági Politika,
- Informatikai Biztonsági Stratégia,
- Informatikai Biztonsági Szabályzat,
- az információs rendszerek védelmének felelőseire, azok feladataira, hatáskörére, felhasználóira vonatkozó szabályok.

QUADRON RENDSZER Információvédelmi Kft. // 1051 Budapest, Sas u. 10-12.
Fax: +36 (1) 796 3253 // e-mail: info@quadron.hu // www.quadron.hu

A biztonsági osztályokba sorolást követően feltárulnak azok az eltérések, amelyek a meglévő és biztonsági osztálynak megfelelő védelmi intézkedések között vannak. A hiányzó védelmi intézkedések kialakítására cselekvési tervet kell előírni. Amennyiben jelentős eltérés van a jelenlegi és a kívánt állapot között, akkor a törvény lehetőséget ad arra, hogy a szervezet úgy alakítsa ki a cselekvési tervét, hogy legfeljebb két éven belül képes legyen a jelenleg meglévőnél legalább egy biztonsági osztállyal magasabban megkövetelt védelmi szint elérésére. Ezáltal kétévente léphet eggyel feljebb, amíg el nem éri a besorolás szerint elvárt biztonsági osztályt.

A biztonsági osztályokba sorolást szükség szerint (a kezelt adatvagyonban történő változás vagy új elektronikus információs rendszer bevezetése esetén), de legalább háromévente, dokumentált módon újra el kell végezni.

A törvény előírásai alapán a biztonsági osztályba sorolást követően a következő feladatok merülhetnek fel a megfelelőség teljesítésére:

Feladatok, amelyek részben vagy teljes mértékben adminisztratív úton megvalósíthatóak:

- Informatikai Biztonsági Politika kiadása (vagy a meglévő frissítése)
- Az elektronikusan tárolt információk és a rendszerek biztonsági osztályba sorolása
- A biztonsági osztályba sorolás követelményének rögzítése az Információ Biztonsági Szabályzatban (vagy az IBSZ létrehozása)
- Szabályzati hierarchia kialakítása (IBP – IBSZ – belső, alacsonyabb szintű utasítások)
- Az IBSZ-ben és az alacsonyabb szintű utasításokban kialakítani az elektronikus információs rendszerek biztonságával kapcsolatos feladatok, felelősségek rendszerét
- Informatikai biztonsági stratégia kialakítása
- A szervezet folytonos működését, az adatvagyon rendelkezésre állását maximalizáló folyamatok, szabályozás kialakítása
- A felhasználók információbiztonsági tudatossági szintjének emelése, oktatási feladatok
- Amennyiben vannak kiszervezett biztonsági tevékenységek, akkor a szerződések kiegészítése a 2013. évi L. törvénynek való megfelelés kötelezettségével

Feladatok, amelyek részben vagy teljes mértékben technológiai megoldásokkal megvalósíthatóak:

- Rendszeresen végre kell hajtani biztonsági auditokat
- Gondoskodni kell az elektronikusan tárolt információk és a rendszerek eseményeinek nyomon követhetőségéről
- A biztonsági eseményeknél gondoskodni kell a gyors és hatékony reagálásról
- A biztonsági események és feltárt kockázatokról való tájékoztatás módjának kidolgozása (országos szintű szervezeteknek is)
- Az elektronikus rendszerek biztonságáért felelős személy jelentésének, riportálási módszerének kialakítása a szervezet vezetője számára

QUADRON RENDSZER Információvédelmi Kft. // 1051 Budapest, Sas u. 10-12.
Fax: +36 (1) 796 3253 // e-mail: info@quadron.hu // www.quadron.hu

Feladatok, amelyek a törvény általános, az elektronikus információs rendszerek bizalmassági, sértetlenségi és rendelkezésre állási előírásaiból, illetve magas biztonsági osztályokra vonatkozó esetleges további előírásokból következhetnek:

- A szerverek és munkaállomások teljes körű végpontvédelme
- A szervereken tárolt adatok biztonságos mentése, a mentések visszaállíthatósága
- A szervezet külső kommunikációs pontjain a határvédelem megvalósítása
- A szervezet adatvagyon elemeihez való hozzáférési, jogosultságkezelési folyamatainak kialakítása
- Az információk minősítése alapján azok titkosítása (belső és idegen hálózaton átmenő adatokra egyaránt)
- Az adatszivárgás megelőzése (akár mobil eszközökre vonatkozóan is)
- A weben elérhető tartalom hitelességének biztosítása