2013 L. - tapasztalatok

Antidotum – 2015

Tőzsér és Máriás

SZOFTVER IRODA

Jogszabály

- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)
  - A törvényt az Országgyűlés a 2013. április 15-i ülésnapján fogadta el. A kihirdetés napja: 2013. április 25.
  - „25. § Ez a törvény 2013. július 1-jén lép hatályba”
  - „6. § (1) … rendszerei biztonsági osztályba sorolását első alkalommal az e törvény hatálybalépését követő egy éven belül el kell végezni.”
  - (2) … a szervezet biztonsági szintbe sorolását első alkalommal az e törvény hatálybalépését követő egy éven belül el kell végezni.
  - (3) … adatokat az e törvény hatálybalépésétől számított 60 napon belül, a … (IBSZ) szabályzatot az e törvény hatálybalépésétől számított 90 napon belül nyilvántartásba vétel céljából köteles bejelenteni a hatóságnak.
  - (4) … az előírt képzési követelményeknek a hatálybalépést követő öt éven belül kell eleget tenniük.”

2013 L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

„(1) E törvény rendelkezéseit kell alkalmazni:

a) a központi államigazgatási szervekre, a Kormány és a kormánybizottságok kivételével,

…

e) az Országos Bírósági Hivatalra és a bíróságokra,

f) az ügyészségekre,

…

k) a helyi és a nemzetiségi önkormányzatok képviselő-testületének hivatalaira, a hatósági igazgatási társulásokra,…”

+

„a jogszabályban meghatározott, a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói,

az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt rendszerelemek elektronikus információs rendszereinek védelmére”

2013 L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

„A szervezet vezetője köteles gondoskodni az elektronikus információs rendszerek védelméről a következők szerint:”

16 pont (!!), többek között:

- h) rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik arról, hogy a szervezet elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak
- n) megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket.

Tőzsér és Máriás
SZOFTVER IRODA

Rendeletek

- 73/2013. (XII. 4.) NFM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági **nyilvántartásba vételének**, valamint **a biztonsági események jelentésének** és közzétételének rendjéről
- 77/2013. (XII. 19.) NFM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint **a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről**
- 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek **képzésének és továbbképzésének tartalmáról**

Jogszabályok

- 26/2013. (X. 21.) KIM rendelet (… az elektronikus információs rendszer biztonságáért felelős személyek **képzésének és továbbképzésének tartalmáról)**
  - **7. § (2)** Az Ibtv. 13. § (10) bekezdése alapján nem kell a 4. § (1) bekezdése szerinti végzettséget megszereznie annak a személynek, aki rendelkezik:
    - a) az Information Systems Audit and Controll Association (ISACA) által kiadott:
      - aa) Certified Information System Auditor (CISA), vagy
      - ab) Certified Information Security Manager (CISM), vagy
      - ac) Certified in Risk and Information Systems Control (CRISC),
    - b) az International Information Systems Security Certification Consortium Inc. által kiadott Certified Information Systems Security Professional (CISSP)

    érvényes oklevéllel.

Jogszabályok

- 2011. évi CCIX. Törvény (a víziközmű-szolgáltatásról)
- 2008. évi XL. törvény a földgázellátásról
- 2007. évi LXXXVI. törvény a villamos energiáról
- 2003. évi C. törvény az elektronikus hírközlésről

A műszaki rész mindenhol szó szerint ugyanaz…

Tőzsér és Máriás
SZOFTVER IRODA

Jogszabályok

- 2011. évi CCIX. Törvény (a víziközmű-szolgáltatásról):
  - 5)93 Számla kiállítására csak olyan informatikai rendszer felhasználásával kerülhet sor, amely biztosítja a díjak hibátlan kiszámítását végző rendszerelemek zártságát, és megakadályozza a számlázási rendszerhez történő jogosulatlan hozzáférést, valamint a számlázási információk észrevétlen módosítását.
  - (6)94 Az (5) bekezdésben meghatározott követelményeknek való megfelelést tanúsító szervezet által történő, a számlázási informatikai rendszerre vonatkozó **tanúsítással kell igazolni**. A számlázási rendszerre vonatkozó követelmények teljesülése kizárólag informatikai biztonsági funkciókat megvalósító szoftvertermékek és -rendszerek **elfogadott hazai vagy nemzetközi informatikai biztonsági módszertanon alapuló** tanúsítására akkreditált tanúsító szervezet által kiállított tanúsítvánnyal igazolható.

Jogszabály - változás

- „7. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény módosítása”
- (4) Az Ibtv. 1. § (1) bekezdése a következő 49 - 51. ponttal egészül ki:

  „50. adatgazda: annak a szervezeti egységnek a vezetője, ahová jogszabály vagy közjogi szervezet szabályozó eszköz az adat kezelését rendeli, illetve ahol az adat keletkezik,”
- (20) Az Ibtv. 9. alcíme helyébe a következő alcím lép:

  „9. Sérülékenységvizsgálat, biztonsági esemény vizsgálata”

  „18. § (1) A hatóság … az érintett szervet kötelezheti arra, hogy az sérülékenységvizsgálatot végeztessen, valamint a biztonsági eseményt kivizsgáltassa.”

Tőzsér és Máriás
SZOFTVER IRODA

MIÉRT van erre szükség?

- A kiberháború intenzíven zajlik,
  akár tudomásul vesszük ezt, akár nem!

- **Második helyezés nincs!**

Tőzsér és Máriás
SZOFTVER IRODA

MIÉRT van erre szükség?

- Jogs
  - ,
    i
  - -
- Elle
- EU-s pályázatok, előírások
- Projektek
- …

Saját,
jól felfogott
ÉRDEK!

szervek elektronikus

Tőzsér és Máriás
SZOFTVER IRODA

Tapasztalatok – hozzáállás

- Nagyon sok helyen még „sehol semmi”
- Nagyon sok helyen most írják ki a pályázatokat…

- Kisebb, vidéki polgármesteri hivatalok (közös önkormányzati hivatal)
- Budapest, kerületi polgármesteri hivatalok

PH: JEGYZŐ!

- Érintett intézmények, szervezetek: kijelölt közreműködők
- Érintett gazdasági társaságok is vannak!

Tőzsér és Máriás
SZOFTVER IRODA

Tapasztalatok

- Fontosság, figyelem
- HW/SW környezet
- Szabályozás
- Képzés, tréningek

Tőzsér és Máriás
SZOFTVER IRODA

Cél

Meg kell teremteni a szervezet biztonsági szintjének megfelelő

- logikai
- fizikai
- adminisztratív
  - elektronikus

biztonsági feltételeket a

megelőzés – észlelés – reagálás - kezelés

érdekében.

Tőzsér és Máriás
SZOFTVER IRODA

Folyamat

- IBF bejelentés (erkölcsi, abevjava)
- Biztonsági szintbe sorolás
  - 77/2013. NFM rendelet szerinti NEIH XLS segédlet
  - Kockázatelemzés alapján!
- Informatikai biztonsági szabályzat beküldése (abevjava)
- Cselekvési terv
  - Hiányosságok pótlása
  - IB politika
  - IB stratégia
  - Kockázatelemzés
  - BCP/DRP
  - Audit
  - Képzések
  - …

Nyilvánosság!
X% nyilvános adat
100-X%=védeni

Tőzsér és Máriás
Szoftver Iroda

Költségek-eredmények

- Alapok
  - Hozzáférés, jogosultság-ellenőrzés
  - Feladatok és felelősségek megosztása
  - Biztonsági képzés
  - Patch management
  - Kockázatelemzés/kockázatkelezés
- Erősítés
  - Etikus hack, behatolás-vizsgálat
  - Konfiguráció erősítés
  - SIEM (Security information and event management)
- Fejlett
  - IDM (Identity and Access Management)
  - Fejlett fenyegetettség érzékelés
  - (Hálózati) viselkedés-elemzés
  - Hálózatvizsgálat (forensics)

Kérdés?

zoltan.tozser@tmsi.hu

Tőzsér és Máriás

SZOFTVER IRODA