Adatvédelmi incidens kezelés gyakorlata

Dr. Dósa Imre

Amiről érdemes szót ejteni

- Felkészülés
- Monitoring
- Esettanulmányok – mit jelentsek, mit nem
- A bejelentés tartalma, kellékei
- Korrekciós intézkedések
- Adatvédelmi gyakorlat figyelése

Felkészülés

Cél: az adatvédelmi incidens felismerése

- Incidens észlelő szervezeti egységek kiválasztása
  - Panaszkezelés, ügyfélszolgálat
  - IT incidens kezelés, információbiztonsági terület
- Teljes dolgozói állomány oktatása
  - Adathordozó, mobiltelefon notebook elvesztése
  - Tiszta asztal elv
  - Jelszavak biztonságos kezelése, social engineering
- Belső adatvédelmi incidens nyilvántartás kialakítása
  - Incidens jelentési folyamat szabályozása, tesztelése

Monitoring

Jelentések, riportok, naplók böngészése

- Panaszok, ügyfélszolgálati hangfelvételek vizsgálata adatvédelmi szemmel
- Hibajegyek adatvédelmi kontrollja
- Adatvédelmi bajnokok (kapcsolattartók) a szervezetben
- Eszköz elvesztések figyelése
- Együttműködés információbiztonsággal
  - DLP rendszerek naplói

Esettanulmányokból kiérlelt gyakorlat

Mit jelentsek, mit nem – magas a tét! Nem jelentem a NAIH-nak:

- Személyes adat nem érintett – az incidens nem adatvédelmi
  - Pl. leltárív elveszett, céges adat érintett csupán
- Nem a biztonság sérül – így működünk
  - Szerződéses jogvita
  - Ügyintézői hiba (Kivéve: hiányos kontrollok)
- Gyanú és nem bizonyosság
- Nem volt veszélyes érintett jogaira
  - Pl. jogosulatlan 3. együttműködő vagy hivatal
- Egy érintett, orvosolt hiba

A bejelentés tartalma, kellékei

NAIH felületén, elektronikusan aláírt e-mail-ben

- Bejelentés
- Belső incidens nyilvántartás kivonata
- Incidensre okot adó hatósági, vizsgálati eljárás anyaga
- Belső vizsgálat dokumentumai
- Elhárítási intézkedések dokumentumai

Korrekciós intézkedések

Jogszerű állapot helyreállítása

- Okozott hátrányok felszámolása
  - Érintettek értesítése – aktivizálása
  - Hibajavítás
- Gyökér-ok felkutatása, felszámolása
  - Jövőben hasonló eset ne fordulhasson elő
  - Gyakran szervezési intézkedés, kontroll bevezetése
  - Oktatás: bekövetkezési valószínűség csökkentése
- Szakaszos bejelentésben közlendő NAIH-al

Adatvédelmi gyakorlat figyelése

Panaszok vizsgálata – incidensek hatósági ellenőrzése - határozatok

- Hazai példák, külföldi gyakorlat tapasztalatai:
  - Legsúlyosabb: incidens felismerés(i képesség) hiánya
  - Bejelentés elmaradása önálló büntetési ok
  - Nem az incidens, hanem a kezelés hatékonysága súlyosabb
- Állandóság és változás a hatósági szemléletben
  - Érintetti érdekek hangsúlyos képviselete
  - Tisztességesség zsinórmértéke
  - Adatvédelmi szempontok kizárólagossága
  - Adatkezelői őszinteség méltánylása
  - Adatkezelő dokumentációja iránti igény

Köszönöm a figyelmet!

Adatvédelmi incidens fogalma

GDPR 4. cikk 12. pont:

- „adatvédelmi incidens”:
  a **biztonság** olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok **véletlen** vagy **jogellenes megsemmisítését, elvesztését, megváltoztatását**, jogosulatlan **közlését** vagy az azokhoz való jogosulatlan **hozzáférést** eredményezi;

Rendelkezésre állás
Sértetlenség
Bizalmasság

Adatvédelmi incidens bejelentése

GDPR. 33. cikk (1)

- **72 órával** azután, hogy az adatvédelmi incidens a tudomására jutott
- kivéve, ha az adatvédelmi incidens valószínűsíthetően **nem jár kockázattal** a természetes személyek jogaira és szabadságaira nézve