# Minimális elvárások egy komplex ICT projekt keretein belül a résztvevő felek részéről (Mit tegyünk, ha beüt a krach, avagy a Felelősségteljes Nyilvánosságra Hozatal)

Hirsch Gábor, IVSZ

IVSZ

# Miért?

- Megváltozott külső környezet
- Szabályozási trendek
  - General Data Protection Regulation (GDPR)
  - NIS irányelv
  - L. törvény
- Hazai események (pl BKK story)

# Responsible Disclosure

- Felelősségteljes Nyilvánosságra Hozatal (FNYH)
  - A Kormányzat teremtse meg a feltételeit
- Jó példa: Hollandia
  - több éves egyeztetés
  - társadalmi és szakmai (beleértve a hacker közösséget)
- Bug Bounty  - Hibavadász Program
- Best Case - Legjobb Gyakorlat Elve

# Érintetti kör

- Kormányzat, törvényhozás, államigazgatás
- Megrendelők
- Szolgáltatók, szállítók
- Sajtó, média
- Társadalom, szakmai szervezetek

# Álltalános elvárások

- Egységes és világos biztonsági követelményrendszer alkalmazása/megkövetelése a fejlesztendő alkalmazásokra
- A webes alkalmazások esetében a minimális elvárás az OWASP Top 10
- Biztonsági forráskód elemző megoldások alkalmazása/megkövetelése
- Biztonságos fejlesztési módszertanok alkalmazása/megkövetelése
- A biztonsági részletek, követelmények teljesülésére kiterjedő teljes dokumentációs rendszer elkészítése /megkövetelése
- Fejlesztési projekt során etikus hacker szolgáltatás alkalmazása/megkövetelése
- Az alkalmazás biztonságos közvetlen futtató környezetének létrehozása/megkövetelése
- Felelősségteljes Nyilvánosságra Hozatal (Responsible Disclosure), Hibavadász (Bug Bounty) programok alkalmazása/megkövetelése

# Sajtó, média

- Hitelesség ellenőrzése!!!!!!!!
- Kiegyensúlyozott, szakmai alapokon nyugvó tájékoztatás
- Felelősségteljes Nyilvánosságra Hozatal beépítése a kommunikációba

# Társadalom, szakmai közösségek

- Etikus hackerek, független tesztelők
  - tartsák be az adott rendszer hibavadász program és felelősségteljes nyilvánosságra hozatal szabályait
  - ne másoljanak, módosítsanak vagy töröljenek adatokat a vizsgált rendszerben
  - ha nem tudják pontosan megállapítani, hogy ki a rendszer tulajdonosa, csak saját felelősségükre jelentsék a hibát (a vélt tulajdonosnak)
  - a média bevonását a legnagyobb elővigyázatossággal kezeljék
  - használjanak olyan anonimizáló proxy, VPN, ideiglenes email címeket és egyéb szolgáltatásokat, amikkel név nélküli módon tudják megtenni bejelentéseiket,

# A biztonságos fejlesztés 13 szabálya (KIBEV)

1. Bevitel ellenőrzés (input validálás): ellenőrizni, érvényesíteni (ha kell tisztítani, átformázni, átalakítani)
2. Biztonsági kódelemző program. Fordítóprogram. Figyeljen oda a figyelmeztetéseire.
3. Építés és Tervezés: igazodjon a biztonsági eljárásokhoz (Security by Design)
4. KISS (Keep It Simple and Stupid): egyszerű a nagyszerű
5. Jogosultságok: alaphelyzet a tiltás.
6. Beállítások: igazodjon a legkevesebb jogosultság felé.
7. Adattisztítás: tisztítsa meg minden felesleges vagy érzékeny tartalomtól a más rendszer felé küldendő adatokat.
8. Védekezés: alkalmazzon mélységi és többszintű védekezést és megfelelő üzemeltetést
9. Minőség: használjon hatékony minőségbiztosítási technikákat
10. Szabványok: alkalmazz biztonságos fejlesztés szabványt vagy szabályokat.
11. Biztonsági szint: határozzon meg biztonsági követelményeket.
12. Támadások ellen: modellezzen lehetséges támadásokat.
13. Bizalmasság, sértetlenség: védje az információ épségét és hitelességét

+1

14. Dokumentáció

# Köszönöm a figyelmet!