Információbiztonság lépésről lépésre az egészségügyben

Információbiztonság – miről is beszélünk?

Milyen adatokat kell védeni?

- **betegek** egészségügyi és személyes adatait
- **egészségügyi dolgozók**, beszállítók, stb. adatait
- **gyógyszerek, vizsgálati eszközök és eljárások**, stb. adatait
- **minőségirányítási dokumentációt** és gyűjtött indikátorokat
- **kórházi gazdasági / finanszírozási / ügyviteli** adatokat

Kitől – mitől?

- **Adatszivárgástól** – jogosulatlanok hozzáférése az adatokhoz
- **Adatok hibás felhasználásától** – hibás információk a gyógyításban, menedzsmentben
- **„Nem az előírt célnak megfelelő" adatkezeléstől** – adatok illetéktelen célú felhasználása (gyógyszercégek piaci versenyelőnyéhez)
- **Adatok rendelkezésre állásának hiányától** – üzemszünet az informatikai rendszerben

Példák betegadatok fenyegetettségeire

Adatszivárgás:

- illetékteleneknek (szándékosan vagy véletlenül) kiadott betegadatok, majd azokkal való visszaélés

Hibás felhasználás:

- „elnézett, vagy elcserélt vizsgálati eredmények (vagy kórlapok) alapján döntés a kezelésről
- gondatlanul rögzített adatok alapján készült betegdokumentáció
- gondatlanul rögzített vagy szándékosan „kozmetikázott” adatok alapján készült finanszírozási adatszolgáltatás

„Nem az előírt célú” felhasználás:

- Szakdolgozatokban, tudományos munkákban nem megfelelően kezelt adatok közzététele

Adatok rendelkezésre állásának hiánya:

- Diagnosztikához, beavatkozáshoz, gyógyításhoz nem, vagy késve (vagy hibásan) állnak rendelkezésre a szükséges információk

Elvárások a biztonság fejlesztésére az egészségügyi intézmények oldaláról

- Ne jelentsen nagy terhet a munkatársaknak (egyszerű és átlátható működés)
- Ne legyen drága
- Valóban növelje a biztonságot
- Ne csak adatvédelmet, hanem információ-biztonságot jelentsen

Együttműködés a Szent-Györgyi Albert Klinikai Központ és az INFOBIZ Kft között.

Az INFOBIZ Kft. megoldása egészségügyi intézmények (kórházak) számára

Az **INFOBIZ Kft.** kialakított egy többlépcsős programot:

- A komplett információbiztonsági irányítási rendszer kiépítése több, egymást követő és egymásra épülő önálló lépésben valósul meg.
- Az egyes lépések önálló projektekként önállóan is végrehajthatók, azok beruházás igénye kisebb.
- Lépésenként önálló, a biztonságot tovább javító eredményeket produkálnak - az eredményekhez viszonyított olcsó áron.

Együttműködés programja lépésről-lépésre

- ✓ **1. lépés: Önértékelő kérdőíves felmérés** *... és a kapcsolódó intézkedési javaslatok a statisztikailag feltárt problémák pótlására*
- ➢ **2. lépés: Szakértői informatikai és információbiztonsági kezdeti állapotfelmérés** *... és a kapcsolódó intézkedési javaslatok a feltárt gyenge pontok, problémák javítására*
- ➢ **3. lépés: Adatvagyon, információs vagyon és fenyegetettségeinek, kockázatainak felmérése** *... és a kapcsolódó intézkedési javaslatok az el nem fogadható kockázatok kezelésére*
- ➢ **4. lépés: Folyamatos kockázatkezelésen alapuló biztonsági intézkedések beemelése az irányítási rendszerbe** *(→ integrált irányítási rendszer ezzel tartalmazza az információbiztonsági irányítási rendszert is)*

Az első lépés feladatai

Célok:

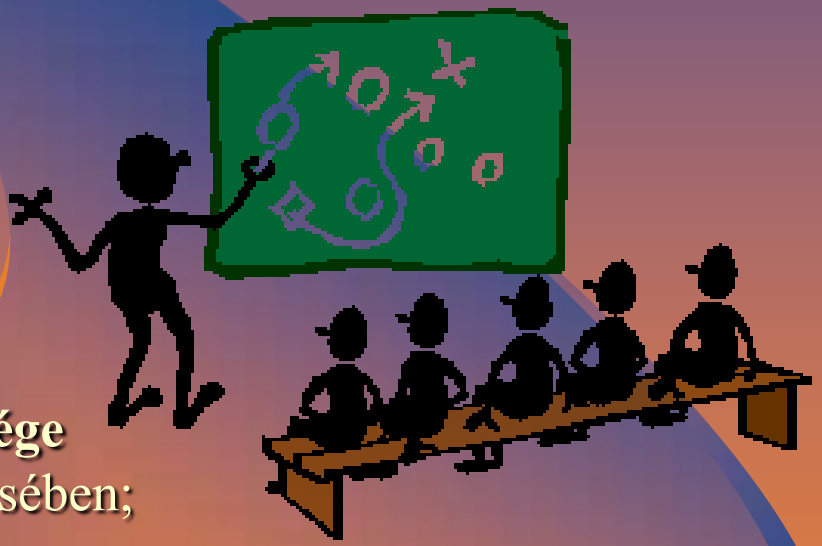
- a felső vezetésnek bemutatni az információbiztonság jelentőségét,
- gyors és költséghatékony módon az adatvédelem / információbiztonság állapotát nagyságrendileg jellemezni
- főbb problémákra rámutatni

Tevékenységek:

- **Képzés**: Információbiztonsági tájékoztató, ismeretfrissítő és tudatosságnövelő alapképzés
- **Önértékelés**: Egy széles körű, általános célú önértékelési kérdőív az információbiztonság és adatvédelem gyakorlati alkalmazási szintjének meghatározása, valamint egy az informatikai üzemeltetés körben
- **Kiértékelések, következtetések**

A bevezető információbiztonsági témájú képzés

Képzés célja: *az adatvédelmi felelősök és a középvezetők számára ismeretfrissítés, az adatbiztonsági tudatosság erősítése, valamint a figyelem felhívása az információbiztonság és informatikai üzemeltetés hatásának jelentőségére a Klinika működési - és adatbiztonságára.*



A képzés főbb témái:

- **„Csapdás" esetek**, előre nem számított negatív események és ezek tapasztalatai a betegek adatvédelmével kapcsolatban;
- Az **információbiztonság szerepe és jelentősége** egészségügyi szolgáltató szervezetek működésében;
- A **kórházi információtechnológiai** (IT) **adatvédelem** főbb gyakorlati szempontjai;
- Az **informatikai üzemeltetés**, mint szolgáltatás megbízhatóságának kritériumai, mutatói.

Az önértékelés módszere

	Általános célú	Informatikai célú
Célja	A teljes szervezetet átfogóan, felhasználói körben az adatvédelem gyakorlatának és tudatosságának (előzetes) felmérése.	Az informatikai rendszer fenyegetettségi és védelmi profiljának (előzetes) felmérése.
Módszere	A teljes szervezetet átfogóan, felhasználói körben az adatvédelem gyakorlatának és tudatosságának (előzetes) felmérése.	Egy 8 – 10 oldalas kérdőív, az informatikai és informatikai biztonsági rendszer kulcselemei.
Résztvevők köre	Minél szélesebb körben, minden betegellátó és adminisztratív egységből több dolgozó.	Szervezet informatikai vezetése.
Kiértékelés módja	IT alapú statisztikai kiértékelés, majd az eredmények alapján a kimutatható gyenge pontok.	Szakértői verbális kiértékelés a kulcselemekre adott válaszok és összefüggéseik alapján.

Az önértékelés témakörei

Általános célú önértékelés témái: az egyes betegellátó és adminisztratív szervezeti egységek mindennapi gyakorlatában

- a **papíralapú dokumentációk** biztonságos / bizalmas kezelése,
- az **adatvédelmi szabályok** és előírások megléte, ismerete és betartása,
- az **informatikai biztonsági szabályozások** megléte, ismerete és betartása.

Informatikai célú önértékelés témái: informatikai infrastruktúra, alkalmazások, üzemeltetés, felhasználói állomány, működési környezet …

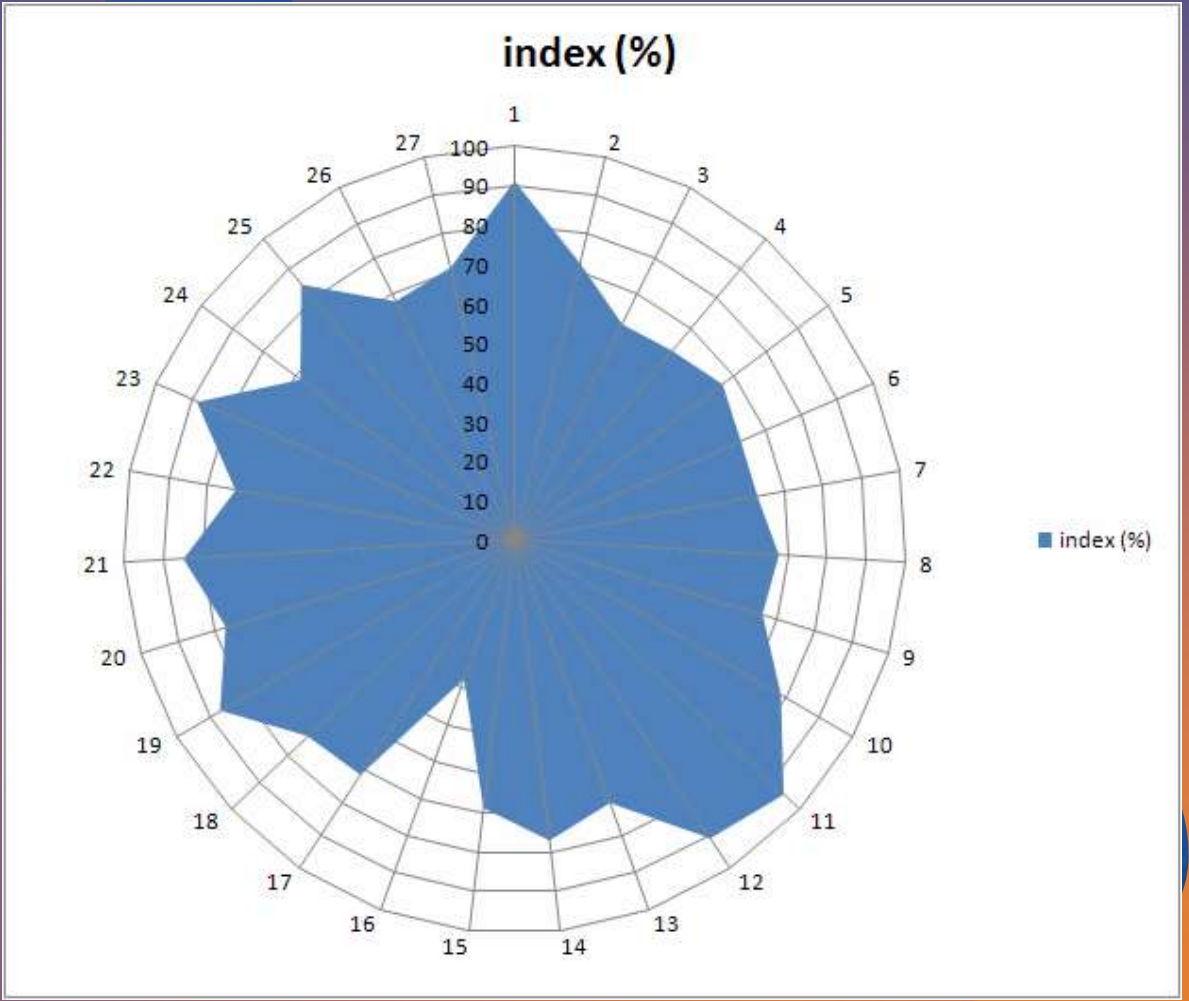
- kereteinek, működésének jellemzése (**fenyegetettségi profil**)
- üzemeltetése meglévő védelmi elemeinek jellemzése (**védelmi profil**)

Az önértékelés eredményei

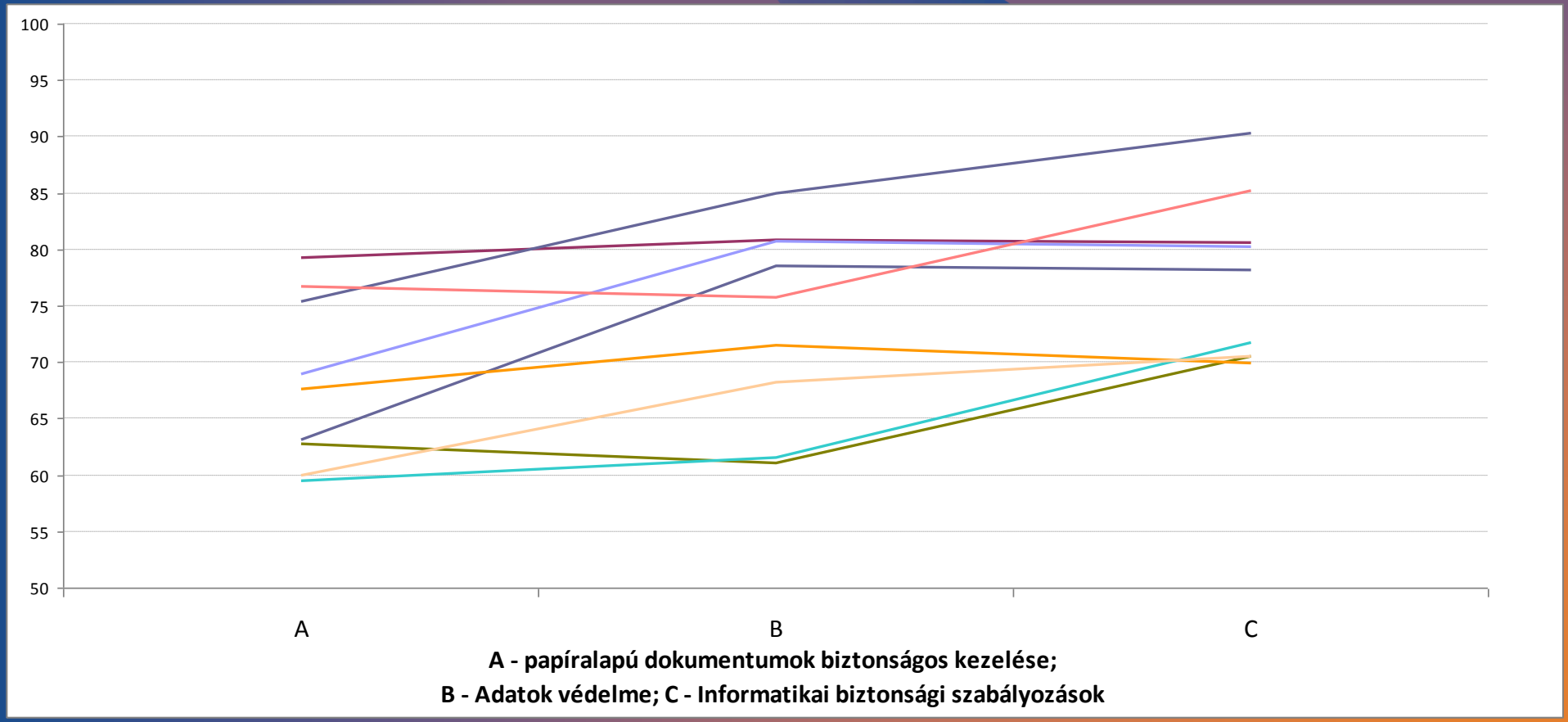
Az általános, 27 kérdést tartalmazó kérdőív kérdésenkénti összesített eredményei

- **Teljes intézményre** vonatkoztatva
- **Vizsgált szervezeti egységekre**

(9 egység - klinika, labor, intézet)



Az önértékelés eredményei



A - papíralapú dokumentumok biztonságos kezelése;
B - Adatok védelme; C - Informatikai biztonsági szabályozások

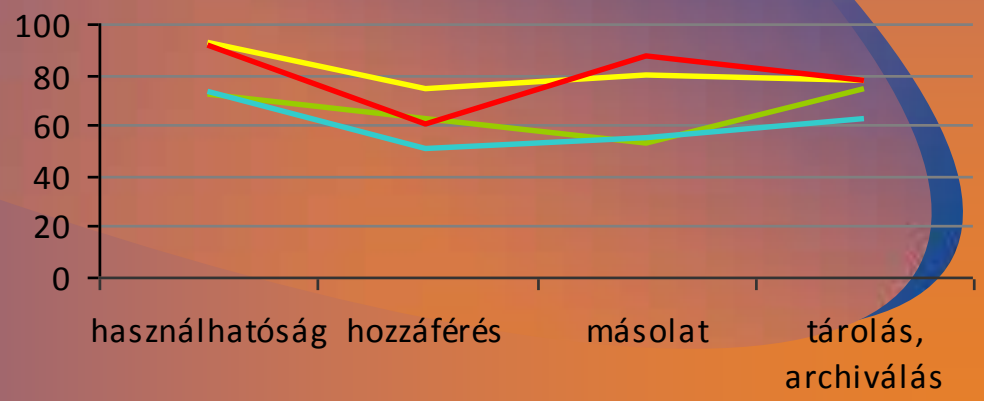
Az önértékelés eredményei

Az **egyes témakörök értékelése külön-külön**,

vélhető **erősségek és fejlesztendő területek** kimutatásával

- **teljes intézményi szinten**, illetve
- **szervezeti egységenként**

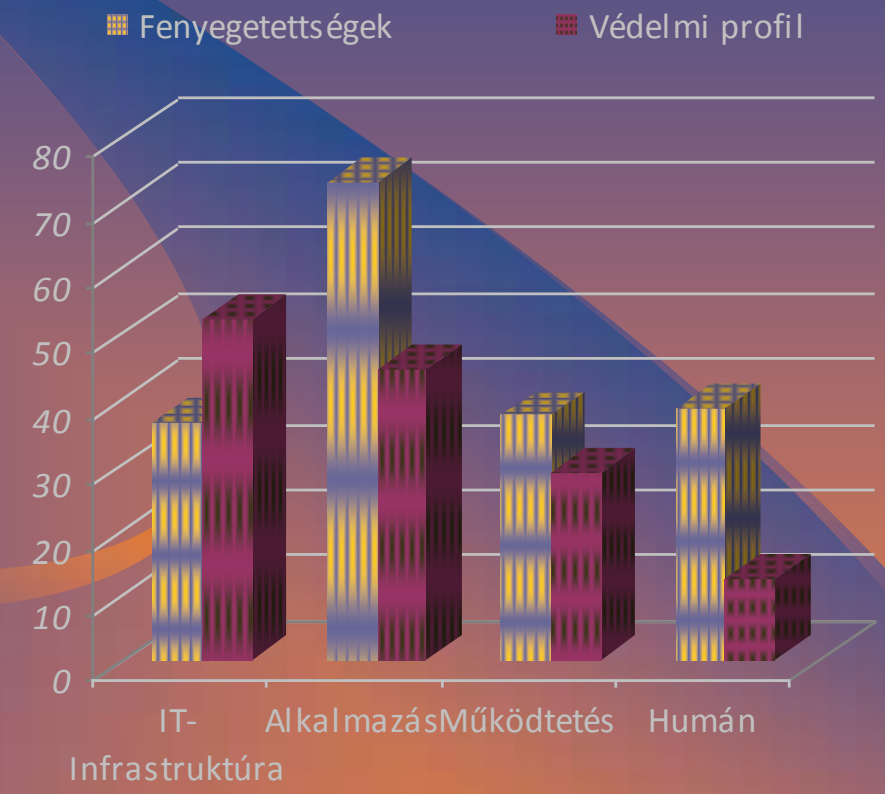
is külön-külön és egymáshoz viszonyítottan is.



Az IT önértékelés eredményei

Az intézményi informatikai rendszer

- **átfogó jellemzése,**
- **fenyegetettségi és védelmi profilja,**
- a biztonság szempontjából az **erős és a fejlesztendő területei,**
- **kiindulási alap** és információ egy részletes informatikai / informatikai biztonsági felméréshez



Az eredmények haszna

Belső intézkedési tervre javaslattétel,
az információbiztonság állapotának javítására:

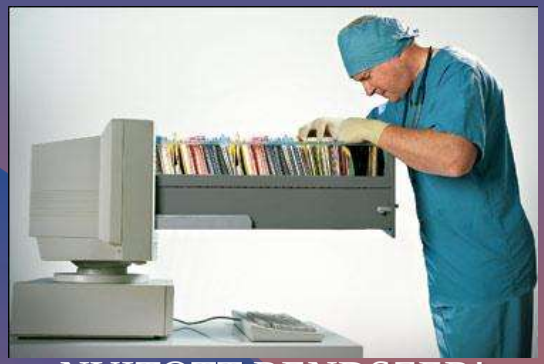
- Belső biztonsági tudatosítási program elindítása,
- Belső dokumentum-kezelés, iratkezelés gyakorlatának javítására
- Az elektronikus betegadat-kezelés gyakorlatának javítására
- Információbiztonsági rendszer kialakítása feltételeinek megteremtésére.

Az IBIR bevezetés második lépésének előkészítése.

Tudatosítási program
1. lépés (?)

Figyelmeztető táblák:

Vigyázat!
Adatszivárgás
lehetséges!



NYITOTT RENDSZER!

VIGYÁZZ AZ INFORMÁCIÓRA!

Vigyázat!
A közelben idegenek
előfordulása lehetséges

Köszönjük megtisztelő figyelmüket!

Fábián Zoltán
fabian.zoltan@med.u-szeged.hu
http://www.klinikaikozpont.u-szeged.hu

Dr. Horváth Zsolt
horvathzs@infobiz.hu
http://www.infobiz.hu