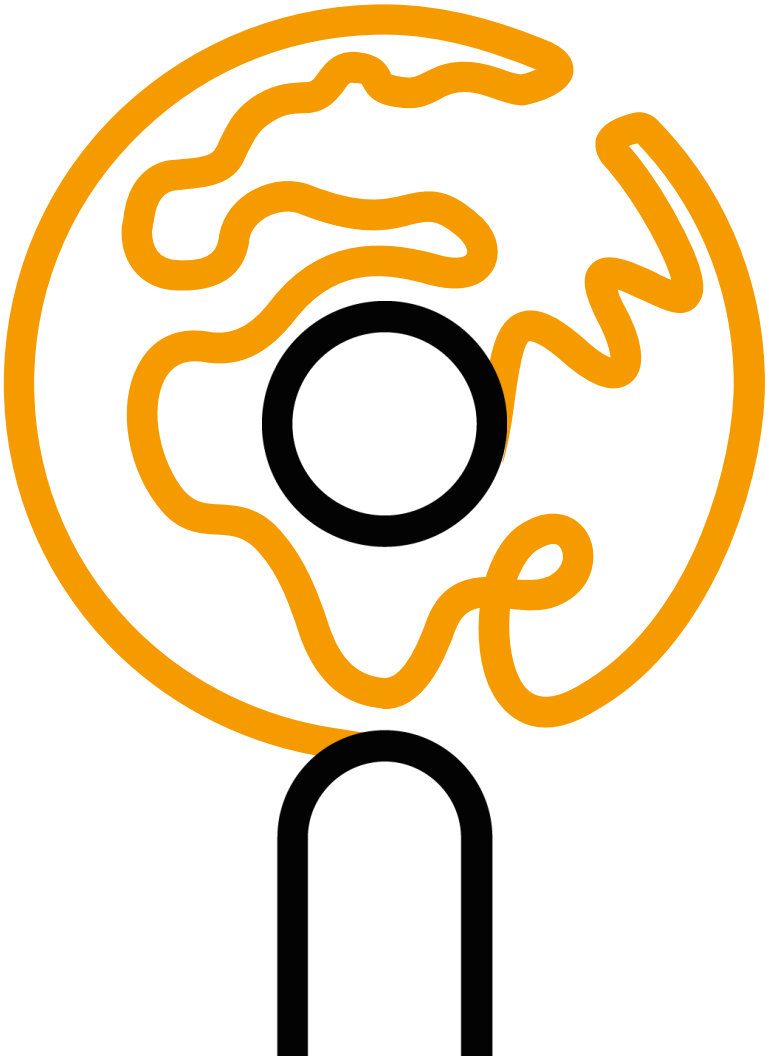
Part of innogy



elmű·émász

Szoftverrel támogatott információbiztonsági rendszer bevezetés az ELMŰ-nél

ELMŰ-ÉMÁSZ · Dénes Sándor · 2017.03.08.

0

Bevezetés

1

Az eszközleltár naprakészen tartása

2

Működőképesség megőrzése
2.1 A folyamatok értékelésének felülvizsgálata
2.2 Helyreállítási képesség
2.3 Folytonossági tervek elkészítése

3

Információbiztonság
3.1 Információ biztonság vizsgálata
3.2 Adatvagyon felülvizsgálata

4

Mindennapi munka támogatása

0.
Bemutatkozunk

- Az ELMÜ - ÉMÁSZ
  - 2,3 millió fogyasztó
  - 2800 munkatárs
  - 12 TWh (12 000 000 000 kWh, 43 PJ) értékesített villamosenergia
  - 250 000 000 m^3 értékesített földgáz
  - 110 alállomás
  - 2 300 km, 18 800 km, 26 000 km vezeték hosszak
  - 17 TWh fuvarozott villamosenergia.

- A Security Puzzle
  - információbiztonság
  - üzletfolytonosság
  - krízis menedzsment
  - utazásbiztonság
  - rendezvény biztonság
  - vagyonvédelem
  - fizikai biztonság
  - külső kapcsolatok.

0.
Helyzetértékelés 2015 végén

Informatikai szolgáltató váltás IBM → T-Systems

- Alkalmazások „selejtezése”
- Informatikai szolgáltatások migrációja (néhol duplikálása)
- Eszközpark áttelepítése

Küszöbön áll a cég szervezeti átalakítása

- Egyetemes szolgáltatás,
- Versenypiaci szolgáltatás,
- Elosztói tevékenység,
- Ügyfélszolgálati tevékenység területén.

„Ami elromolhat, az el is romlik”

E. Murphy

0.
Mi legyen a kockázat minimalizálás módja?

- A villamosenergia (gazdaságosan) nem tárolható, ezért a folyamatos rendelkezésre állás az egyik legfontosabb jellemzőnk illetve elvárásunk.

Az információbiztonsági kritériumok közül az egyik éppen a rendelkezésre állás.

- A „szolgáltatásunk” során nagy mennyiségű adatot használunk, kezelünk. Ezen adatok léte az üzletfolytonosságunk alapja.

Az információbiztonság az üzletfolytonosság feltétele.

- Olyan eszközre volt szükségünk, amely ezt a két területet egységesen kezeli. A meglévő szoftvereink között volt olyan, ami alkalmas erre, az

ADAPTO

1.
Eszközleltár napra készen tartása

- Alkalmazói rendszerek
  - folyamat modellezési rendszerből kiindulva (ARIS)
  - az átadás jó alkalmat kínált a szolgáltatások átvizsgálására → selejtezés, alkalmazás gazdák adatainak frissítése
  - közben: SPECTRUM→IDCS rendszer csere
- Hardverek listája
  - a kiszervezett IT tevékenység átadási listájából (IBM→IT) kiindulva készült
  - közben: eszközpark felújítása
  - jelenleg élő változáskezelési rend → havi frissítés
  - célkitűzés: a fontos folyamatok erőforrásai real-time frissüljenek

2. Működőképesség megőrzése

2.1 Hatáselemzés - Üzletmenet folytonosság

- Kiindulási feltételek:
  - a folyamat szabályozási rendszer adataiból (ARIS) kiindulva
  - a normál működés során végrehajtott átszervezéseket figyelembe véve
- Eredmények
  - szerepköri anomáliák kiszűrése: ADAPTO → ARIS
  - kritikus folyamatok meghatározásának kritériumai:
  - max. 1 napos eltűrt kiesés (MAD)
  - meghatározott összegnél nagyobb okozott kár
  - nem pénzügyi hatások nagysága
  - a kritikus folyamatok minden alkalmazása kritikus

A kritikus folyamatokra kell BCP!

2. Működőképesség megőrzése
2.2 Üzletmenet-folytonosság tervezés

- Szemléletváltás
  - a szervezeti egységekre szabott tervek helyett folyamatalapú tervezés
  - előnye: a módszertan kikényszeríti a strukturált gondolkozást
- Folyamatgazdák, kulcsemberek bevonása a tervezésbe
  - folyamatok értékelése
  - áthidalási tervek kidolgozása
- Szabályzatok készítése a tervekből
  - folyamatszabályozási terület → egy kézben összpontosul a szabályozás
  - ISO 22301 Üzletmenet folytonosság szabvány szerint

2. Működőképesség megőrzése

2.3 Kritikus alkalmazások helyreállításának képessége

- Kétféle okból lehetnek kritikus alkalmazások:
  - fontos folyamatban vesz részt
  - fontos adatot kezel → az adatvagyon értékelését külső tanácsadó bevonásával végeztük, interjú módszerrel
- Elvárható gondosság:
  - a megrendelőnek meg kell győződnie a kiszervezett szolgáltatások helyreállításának képességéről
  - evidenciák gyűjtése

3. Információbiztonság

3.1 Információ biztonság vizsgálata

- A működés nem tanúsított, de ISO 27001 szabvány szerint történik
  - erős anyavállalati szabályozás és
  - regulációs elvárás mellett
- Új szabályozás honosítása a vállalatra (folyamatban)
- Kockázatelemzés

3. Információbiztonság

3.2 Adatvagyon felülvizsgálata

- Mivel a legfontosabb védendő objektum az adat, ezért az információbiztonság az adatvagyon értékéből indul ki.
- Adatvagyon értékelését, beárazását külső konzulens végezte.

4.
Mindennapi munka támogatása

- Hatásvizsgálat
  - Mi történik ha elveszítünk egy rendszert?
  - Mi történik, ha kikapcsolunk egy berendezést, milyen szoftverek állnak le?
- Felkészültség a vészhelyzetekre: gyors reagáló készség
  - Folytonossági tervek kiküldése az érintetteknek.
  - Tervszerű kommunikáció.

+1

Fizikai biztonság

- Alállomások adatai
  - alaprajz alapján zónák meghatározása
  - zónában elhelyezett értékek meghatározása
  - védelmi berendezések rögzítése

Part of innogy

elmű·émász

Dénes Sándor
biztonsági vezető
Tel: + 36 1 238 1229
sandor.denes @elmu.hu