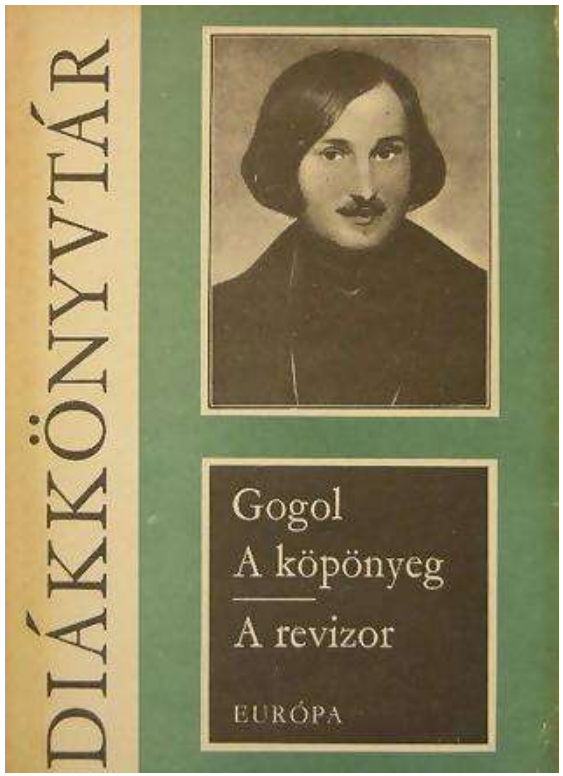


TSM / ISP auditra felkészülés Fundamenta módra

2017. november 9.

„Uraim! Azért kérettem önöket ide, mert egy igen kellemetlen hírt kell közölnöm: revizor jön hozzánk.”

Fundamenta Lakáskassza Alap, amelyre építhet

Tartalom

- Fundamenta-Lakáskassza bemutatása
- Kik jönnek és miért jönnek?
- A revizor / auditor is ember
- Mit kérhet és mit nem? Mihez nyúlhat és mihez nem?
- Nyilvántartások vezetése
- Tesztelések
- Fizikai biztonság – DR
- Szoftveres biztonság – hardening
- Megállapítások kezelése

A Fundamenta-Lakáskassza

Szakosított pénzintézet

- Banki szoftverek, banki biztonsági előírások. Készpénz forgalom nincs.
- 2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról szabályozza a működés feltételeit.

Kezelt adattípusok

-Oracle DB - RMAN,
-MS SQL DB TSM for SQL,
-MS Exchange – TSM for Exchange,
-VM környezet – TSM for VE
-File rendszer – BA kliensek, FlashCopy Manager
-Sharepoint 2010 & Project Server 2007 - DocAve for Sharepoint

A mentések biztonságos működtetése alapvető fontosságú!
Minden audit során kisebb vagy nagyobb intenzitással, de ránéznek

Kik jönnek és miért jönnek? Mire fókuszálnak?

- **Fundamenta belső ellenőr:** tervezett és alkalmi (konkrét kérdésekhez kapcsolódó) vizsgálatok
- **Anyacég (Schwäbisch Hall):** évente minimum egy alkalommal, változó fókusszal, német nyelven – biztonsági protokollok betartása, tesztelések
- **MNB:** – ügyfél adatok védelme
- **HunGuard:** évente – informatikai rendszerek zártságának vizsgálata
- **Könyvvizsgáló cég (Ernst&Young):** évente - adatok sérthetetlenségének védelme – Disaster Recovery
- **IBM** – eseti – személyes kiszállás nincs (eddig nem volt) - licenc compliance

A revizor is ember! (?)

- Pozitív attitűd: ne abból induljunk ki, hogy „szívatni” jönnek, hanem javítani a folyamatainkon.
- 15 év tapasztalata: Mindent észrevesznek! Mindent elolvasnak!
- Nem a szakmai részre fókuszálnak, hanem általában „tételesen” fésülik át a dokumentációt (ha a licenc nyilvántartásban ott egy mentési NODE, de a mentett adatok listájában nincs rá utalás, biztosan rákérdeznek)
- Fontos a magabiztos hozzáállás! Megjelenés. Pontosság!
- Előzetes adatbekérések határidőre történő teljesítése

Mit kérhet és mit nem? Mihez nyúlhat és mihez nem?

Mit kérhet? - Nyilvántartásokat, naplózási adatokat, tesztelési jegyzőkönyveket. Felhasználói ill. üzemeltetői interjúk. Ügyfél adatokat nem – csak betekintést végezhetnek

Mihez nyúlhat? - Semmihez! Fontos! Megmondhatja, hogy milyen parancsot adj ki (és ha nem egy format c:\, te be is kell írd), de ő nem adhatja ki! Próbáluk minimalizálni az „akkor és ott” megmutatást. Javasoljunk képernyőképeket, logokat betekintésre. Behatolási teszt kizárólag előre egyeztetett idősávban és targetekkel!

Nyilvántartások naprakész vezetése

Szalag nyilván-tartás

Naprakész, elektronikus nyilvántartás. Ha eltérést találnak (pl. páncélszekrényben van, ami a nyilvántartás szerint a Tape Libraryben), megjegyzés lesz belőle.

Felhasz-náló kezelés

Identity Management használata
Administrator: NO
Nevesített userek (felelősség) Operator: NO OperatorSanyi: OK AdminBellas: OK

Adatvissza-töltési kérések

Elektronikus (Sharepoint alapú) űrlapon, vezetői engedélyezéssel. A visszatöltés ne eredeti helyre történjen, hanem ideiglenes tárhelyen kerüljön átadásra, vagy teszt környezetben. Élesbe visszatöltés: megjegyzés

Megsemmi-sítési procedúra

Adathordozó megsemmisítési jegyzőkönyv. Roncsolás, nyilvántartásból kivezetés

Tesztelések

- Általában elég a rendszeresen vezetett jegyzőkönyvek bemutatása. A megtörtént, de nem teljeskörűen dokumentált jegyzőkönyvek pótlása

- Ritkábban: ad-hoc teszt: konkrét rendszer helyreállítása **teszt** rendszerbe – jegyzőkönyvezve

- DR forgatókönyv: katasztrófa eljárás megléte „nulláról” – csak a páncélszekrényben lévő szalagok vannak.

Fizikai biztonság – DR

- Saját géptermek biztonsága
  - belépés biztonsága (kód, kártya), naplózása
  - tűzvédelmi előírások betartása
  - gépteremben éghető anyag tilos
- Hosting megfelelőség
  - minősített hosting szolgáltatók:
    - T-Systems Adatpark
    - Invitech DC10

- Szalagok biztonságos tárolása, szállítása:
  - tűzvédelem – páncélszekrény 30 perc tűzállósággal
  - másodpéldányok fizikai távolsága a fő telephelytől
  - backup példányok szállítása: gépjármű, két fő, jegyzőkönyv

Szoftveres biztonság – hardening

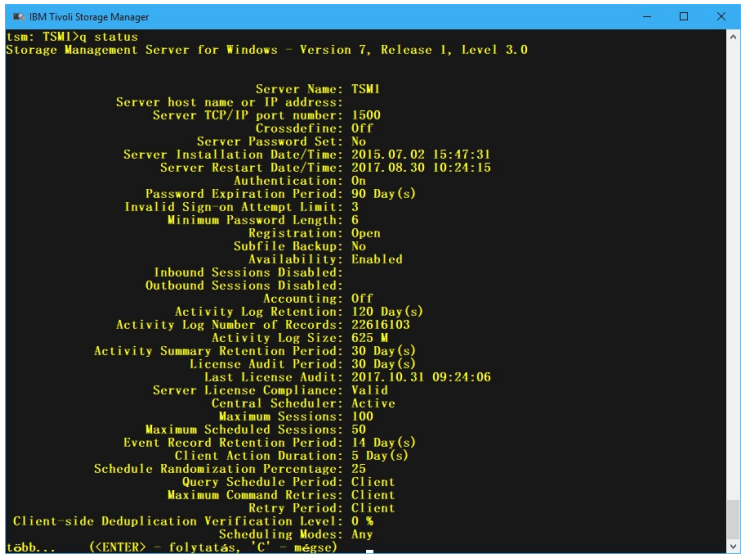
Windows 2012 R2 – rendszeres patchelések – negyedévente

TSM Server 7.1.3 – 8.1 upgrade tervezés alatt

Kliensek vírusvédelme (automatikusan frissülő)

Kliensek (operációs rendszer) patch szintje: 90 napos frissesség az elvárás – komoly patch menedzsment bevezetését követeli meg.

Tűzfal beállítások ellenőrzése – szükséges minimális



Megállapítások kezelése

- Minden megállapításra reagáljunk!
  - Elfogadjuk a megállapítást és
    - Az abban foglalt változtatásokat már végrehajtottuk
    - Ismert hiba, folyamatban a javítás, pótlás, módosítás
    - Be van tervezve a javítás, módosítás, változtatás
    - Változtatást megtervezzük, bevezetjük (határidő!)
    - Egyéb kapcsolódó okból, üzleti érdekből a módosítás nem végrehajható – de megvizsgáljuk a komplex változtatás lehetőségét
  - Nem fogadjuk el (mert):
    - formai, alaki hibákat találtunk
    - A megállapítás hibás feltetélezésen, tévesen értelmezett adatokon alapul, küldjük a módosított információkat, kérjük felülvizsgálni.
- A következő audit során kiemelten fogják nézni az előző során tett észrevételekre adott válaszokat, megoldásokat! Csak olyat ígérjünk be, amit végre is tudunk hajtani.

Köszönöm szépen! Ha kérdésed van:

Belső László

belso.laszlo@fundamenta.hu

RENDŐRKAPITÁNY HANGJA
Kedves egészségére, nagyságos uram!
BOBCSINSZKIJ HANGJA
Adjon isten száz esztendőt, meg egy zsák aranyat!
DOBCSINSZKIJ HANGJA
Isten éltesse sokáig!
ARTYEMIJ FILIPPOVICS HANGJA
Dögölj meg!
KOROBKINNÉ HANGJA
A nyavalya essen beléd!
POLGÁRMESTER
Alázatosan köszönöm! Viszont kívánom!