ALVERAD
TECHNOLOGY FOCUS

NIS2

az ipari kibervédelem szemszögéből

2024. 06. 12.

Hinkel Attila

- Partner
- IT biztonsági szakértő

Akkreditált kiberbiztonsági vizsgálólaboratórium

- Informatikai rendszerek
- Szoftvertermékek
- Ipari rendszerek

Jogi háttér

2019/881 (EU) rendelet (2019.04.17.)
az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról

2022/2555 (EU) irányelv – NIS 2 (2022.12.14.)
az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről

2023. évi XXIII. Törvény
(Kibertantörvény)
a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről

10/2023. (V. 15.) SZTFH rendelet
az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról

23/2023. (XII.19.) SZTFH rendelet
az érintett szervezetek kiberbiztonsági felügyeleti hatósági nyilvántartásáról

XX/2024. (X.X.) SZTFH rendelet
auditorokról

Jogi háttér – kijelölés - felügyelet

2022/2557 (EU) irányelv – CER (2022.12.14.)
a kritikus szervezetek rezilienciájáról

2022/2555 (EU) irányelv – NIS 2 (2022.12.14.)
az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről

Hazai implementáció folyamatban
BM - Országos Katasztrófavédelmi Főigazgatóság

2023. évi XXIII. Törvény
(Kibertan trv.)
a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről

Rendszer

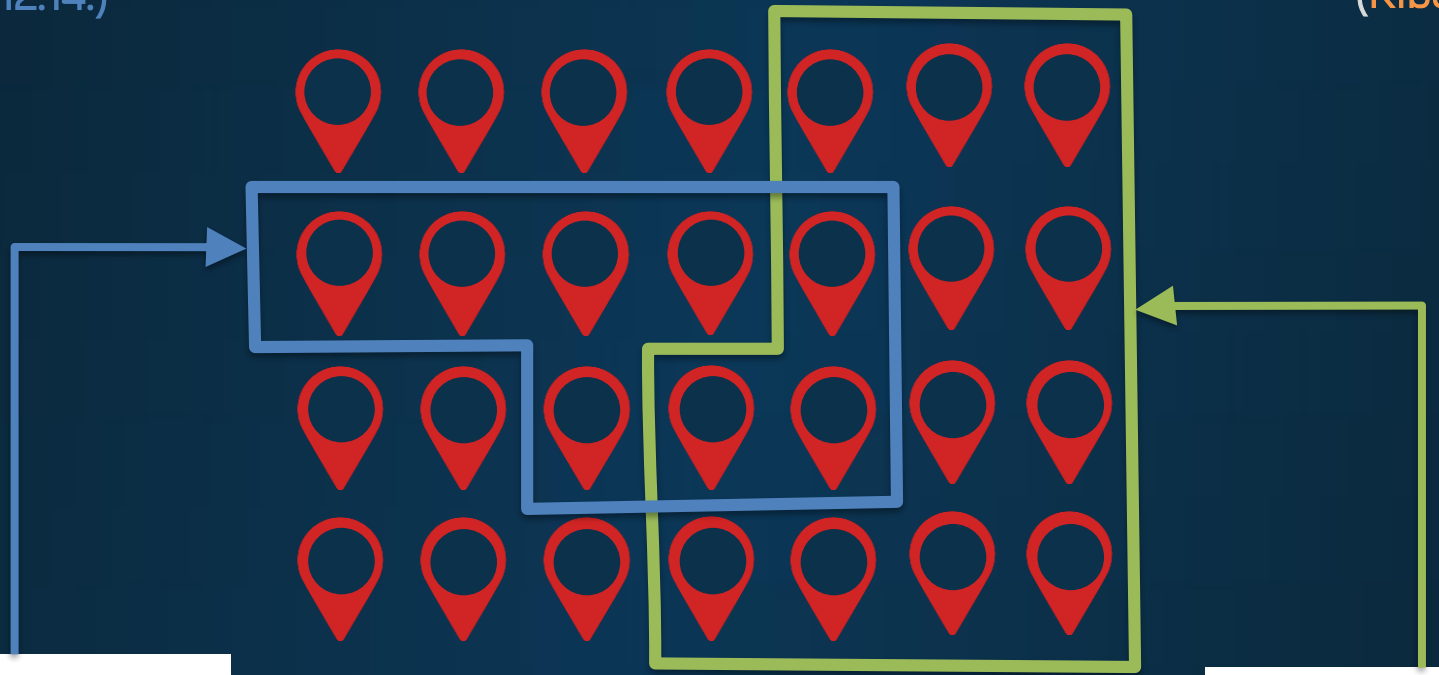
Kijelölés

Szervezet

Kiberbiztonsági felügyelet

2022/2557 (EU) irányelv
CER (2022.12.14.)
Fontosság

2023. évi XXIII. Törvény
(Kibertan trv.)
Méret



NEMZETI KIBERVÉDELMI INTÉZET

SZTFH

Elektronikus Információs Rendszer – OT rendszer (is)

2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről

17. § (1) Az e fejezetben foglaltakat

….az érintett szervezet elektronikus információs rendszereire kell alkalmazni.

9.elektronikus információs rendszer: az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény szerinti fogalom

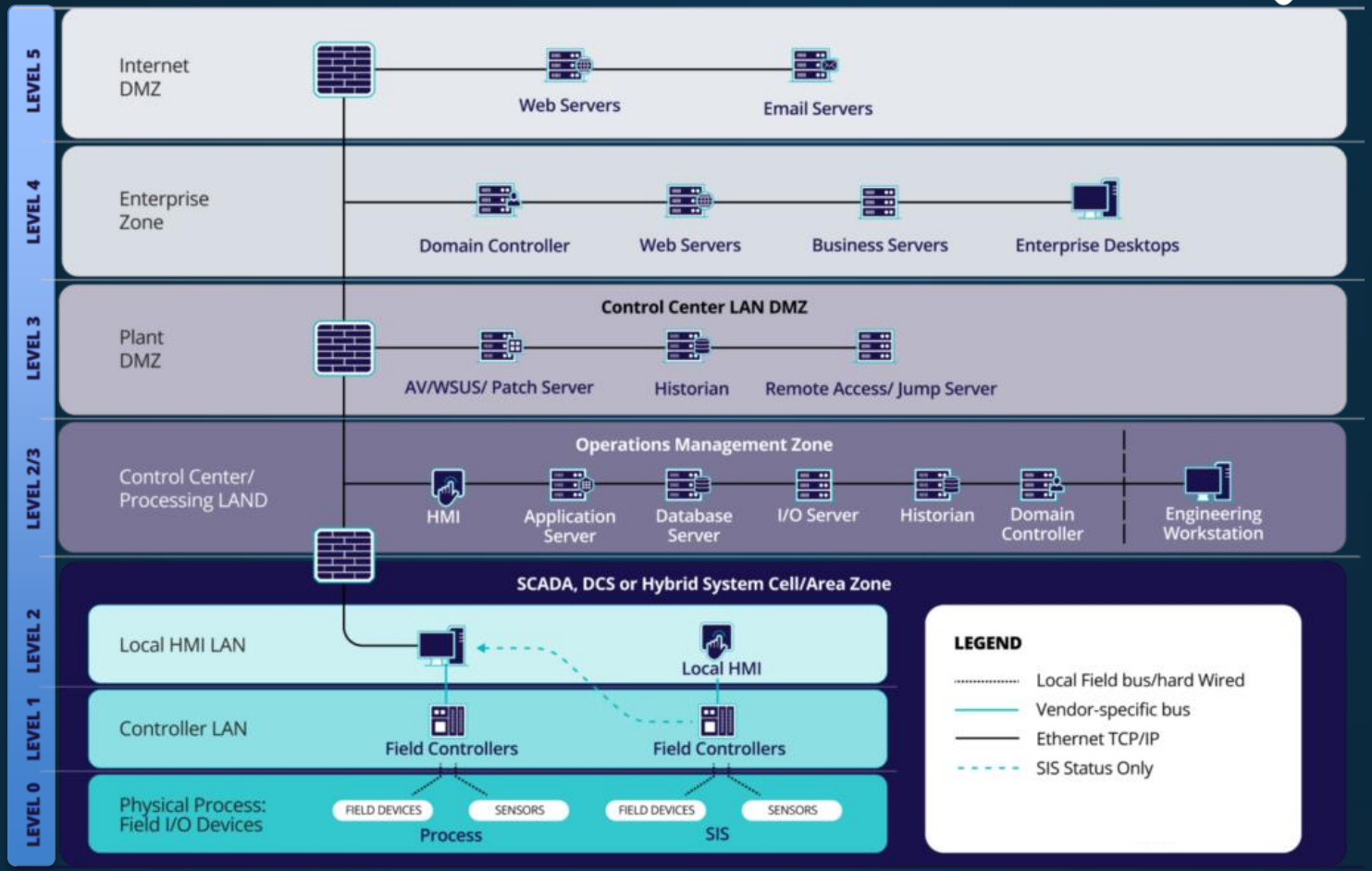
2013. évi L. törvény

14b.elektronikus információs rendszer:

b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi; vagy

c) a b) pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok;

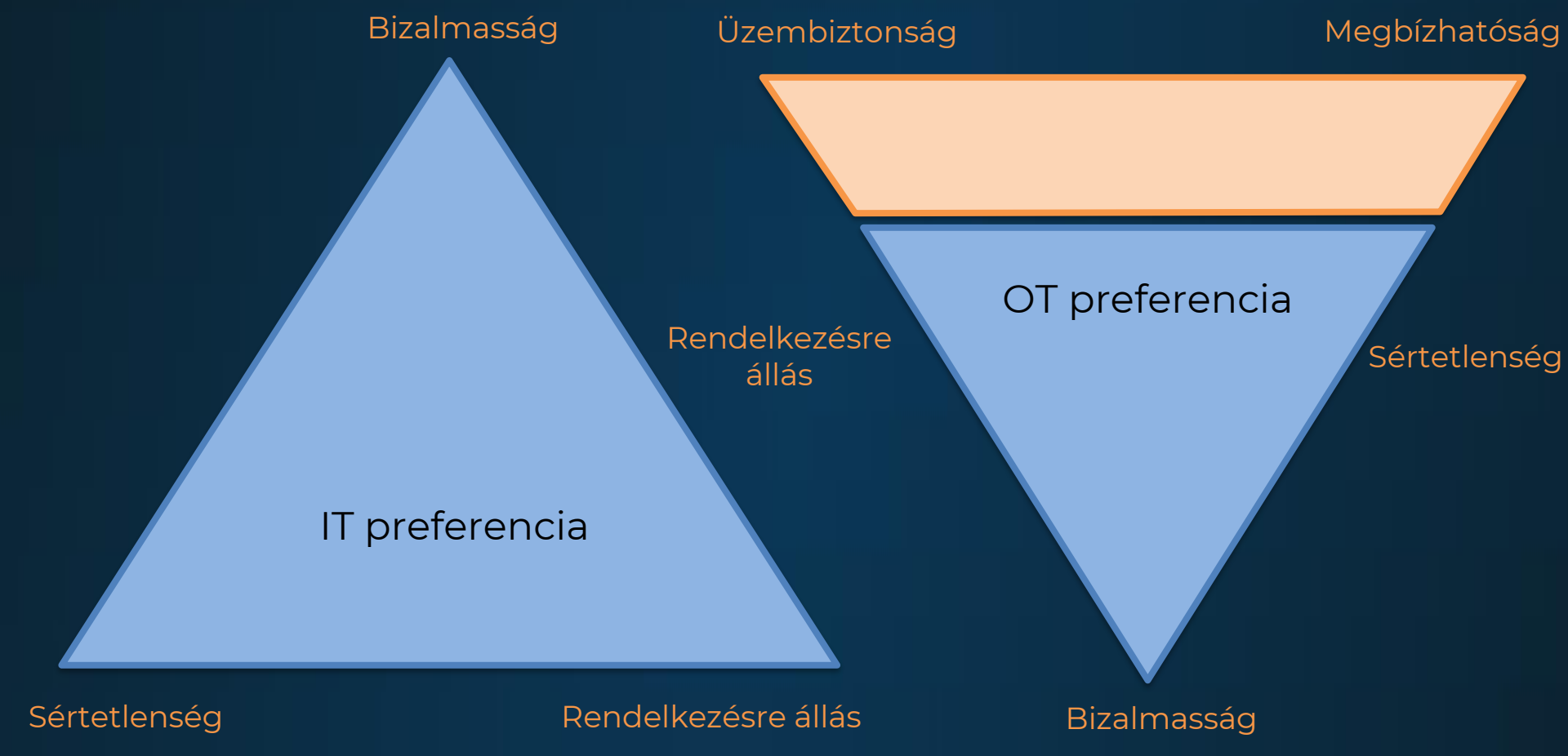
Elektronikus Információs Rendszer – OT rendszer (is)



IT = OT

ALVERAD
TECHNOLOGY FOCUS

IT ≠ OT

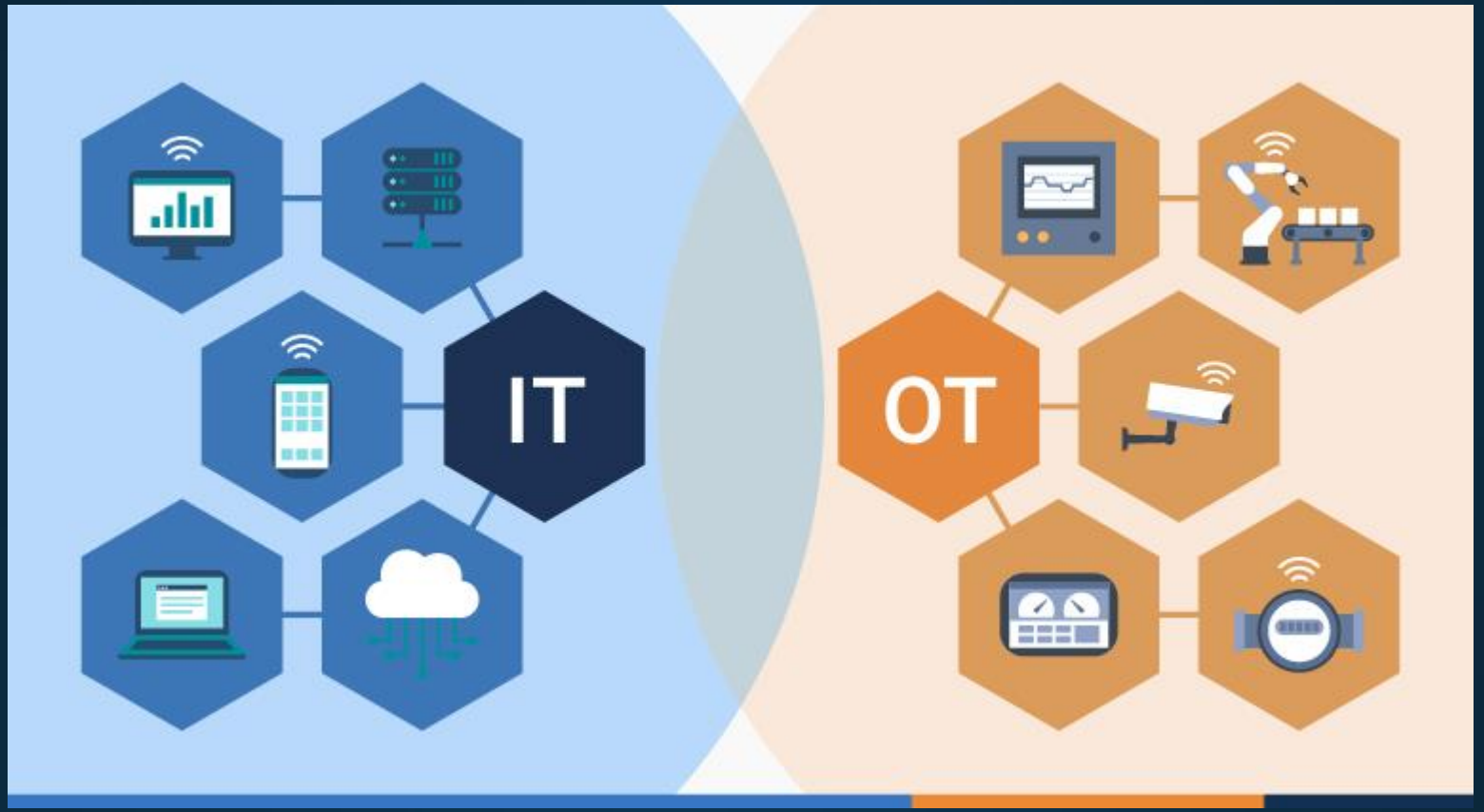

Bizalmasság
IT preferencia
Sértetlenség
Rendelkezésre állás
Üzembiztonság
Megbízhatóság
OT preferencia
Rendelkezésre állás
Sértetlenség
Bizalmasság

IT ≠ OT

	Information Technology (IT)	Operational Technology (OT)
Összetevők, komponensek	Szerverek, munkaállomások, adattárak, felhő, biztonsági eszközök, mobileszközök, webalkalmazások, hálózati eszközök.	PLC/DCS, SCADA, adatgyűjtők, szenzorok, motorok és egyéb terepi eszközök, protokollkonverterek, gyártásirányítók (MES).
Életciklus	3-5 éves életciklus, folyamatos törekvés a modernizálásra, fejlesztésre („piszkáld, hogy működjön!”).	10-25-50 éves életciklus, csak a feltétlen szükséges változások („ne piszkáld és akkor működik!”).
Működés	Eredetileg is együttműködő, összekapcsolt alkalmazások, rendszerek és hálózatok összessége.	Eredetileg szigetrendszerű, önálló működés, nem volt cél a rendszerek és eszközök hálózati összekapcsolása.
Biztonsági koncepció	„Data first”, adatközpontú szemlélet, a biztonság e köré szerveződik.	„Process first”, a biztonság a technológiai folyamatok fenntartására és a berendezés, emberélet és környezet megóvására szerveződik.
Személyzet	Rendszergazdák, IT mérnökök, biztonsági mérnökök és felhasználók. „Fehérgalléros” munkavállalók.	Operátorok, karbantartók (TMK), terepi mérnökök (field engineer), PLC programozók, folyamat- és automatizálási mérnökök. „Fehér- és kékgalléros” munkavállalók.
Üzemeltetés	Az IT rendszereket a szervezetek maguk üzemeltetik és tartják karban, illetve igénybe vehetnek alvállalkozó (outsource) partnert.	Az OT rendszereket jellemzően a szállítók, integrátorok vagy a gyártók üzemeltetik és tartják karban, akár nagyobb berendezésenként eltérő üzemeltetés és karbantartás is megjelenhet. Szervezet és iparágfüggő.
Elhelyezkedés	Centralizált rendszerek, adatközpontokban, szerverszobákban és irodahelyiségben működnek, könnyű hozzáférés és megközelítés jellemzi.	Gyakran szennyezett környezet, terepi körülmények, decentralizált és akár elszigetelt (szigetrendszerű) működés, nagy távolságok áthidalása, és a terepi viszonyokat tekintve akár nehéz megközelítés és hozzáférés jellemzi.

IT ≠ OT - egységes értékelés ?

IT: NIST 800-53



OT: NIST 800-82

IT ≠ OT - egységes értékelés !

Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

IT: NIST 800-53

- Az érintett szervezet automatikus mechanizmusokat használ a naplóbejegyzések felülvizsgálatának, elemzésének és jelentési folyamatainak integrálására.

OT: NIST 800-82

- Amennyiben az EIR nem támogatja a naplóbejegyzések gyűjtését, a naplóbejegyzések felülvizsgálatát az EIR rendszerbiztonsági tervében meghatározott rendszerességgel manuális ellenőrzéssel kell végezni.

- **Magyarázat:** A helyettesítő védelmi intézkedések magukba foglalhatják például a kézi mechanizmusokat vagy eljárásokat. Olyan eszközök esetében, ahol a naplóbejegyzések gyűjtését nem tudják megvalósítani, időszakos manuális felülvizsgálatra lehet szükség.

Eszköz zárolása

IT: NIST 800-53

- Meghatározott időtartamú inaktivitás után vagy a felhasználó erre irányuló lépése esetén, az eszköz zárolásával megakadályozza az EIR-hez való további hozzáférést.

OT: NIST 800-82

- Abban az esetben, ha az EIR nem rendelkezik automatikus zárolási képességgel, vagy vészhelyzetben azonnali kezelői reakcióra van szükség, ezért zárolással nem lehet megakadályozni az EIR-hez való hozzáférést, a szervezet kockázatértékelés alapján helyettesítő intézkedést vezet be, amelyet dokumentál az EIR rendszerbiztonsági tervében.

Az elektronikus információs rendszer helyreállítása és újraindítása

IT: NIST 800-53

- Az érintett szervezet a meghatározott helyreállítási idővel és helyreállítási ponttal kapcsolatos célkitűzésekkel összhangban lévő időtartam alatt gondoskodik az EIR utolsó ismert, üzembiztos állapotba történő helyreállításáról és újraindításáról egy összeomlást, kompromittálódást vagy hibát követően.

OT: NIST 800-82

- Az érintett szervezet a meghatározott helyreállítási idővel és helyreállítási ponttal kapcsolatos célkitűzésekkel összhangban lévő időtartam alatt gondoskodik az EIR utolsó ismert, üzembiztos állapotba történő helyreállításáról és újraindításáról egy összeomlást, kompromittálódást vagy hibát követően.
- **Magyarázat:** Az érintett szervezet megvizsgálja, hogy az EIR utolsó ismert, üzembiztos állapotba történő helyreállításakor a felmerülő kockázatok figyelembevételével a rendszer állapotváltozóit vissza kell-e állítani a kezdeti értékekre vagy az üzemszünet előtti értékekre.

Behatolásvizsgálat (penetration testing)

IT: NIST 800-53

- Az érintett szervezet behatolásvizsgálatot végez a szervezet által meghatározott gyakorisággal a meghatározott EIR-eken vagy rendszerelemeken

OT: NIST 800-82

- Az érintett szervezet az OT funkciók zavartalanságának biztosításával behatolásvizsgálatot végez a szervezet által meghatározott gyakorisággal a meghatározott EIR-eken vagy rendszerelemeken.
- **Magyarázat:** A behatolásvizsgálatokat megfontoltan alkalmazzák az OT-hálózatokon, hogy az ellenőrzési folyamat ne befolyásolja hátrányosan az OT-funkciókat. Az OT-rendszerek általában nagyon érzékenyek az időzítési korlátokra, és korlátozott erőforrásokkal rendelkeznek. A helyettesítő ellenőrzések közé tartozik például a replikált, virtualizált vagy szimulált rendszer alkalmazása a behatolásvizsgálat elvégzéséhez. Előfordulhat, hogy a tesztelés elvégzése előtt le kell állítani a gyártás alatt álló OT rendszert. Ha az OT-rendszereket tesztelés céljából lekapcsolják, a teszteket lehetőség szerint a tervezett OT leállások idejére kell ütemezni. Ha a behatolásvizsgálatot nem OT-hálózatokon végzik, fokozottan ügyelni kell, hogy a tesztek ne terjedjenek át az OT-hálózatra.

10 – 25 év

Kerülő megoldások

- Architektúrák
- Komponensek képességei
- Szemléletmód
- Fehér és kék galléros párbeszéd

Beépített biztoság

Köszönöm a figyelmet!

- Hinkel Attila
- +36.20.928.9449
- hinkel.attila@alverad.hu