MCC-EIVOK 43 Információbiztonsági tudományos-szakmai konferencia

Gondolatok a kiberbiztonság alapjairól

Oláh István
EIVOK alelnök

Nemzeti Közszolgálati Egyetem (NKE):

Információs rendszerek és hálózatok biztonsága,

Pénzintézeti információs rendszerek védelme,

Szoftverfejlesztés biztonsági kérdései egy aktuális sebezhetőség tükrében,

Bizalom a kiberbiztonságban.

Óbudai Egyetem (ÓE):

IT rendszerek üzemeltetésének logikai biztonsági követelményei.

Hírközlési és Informatikai Tudományos Egyesület (HTE):

Információbiztonsági Szakosztály-EIVOK, alelnök

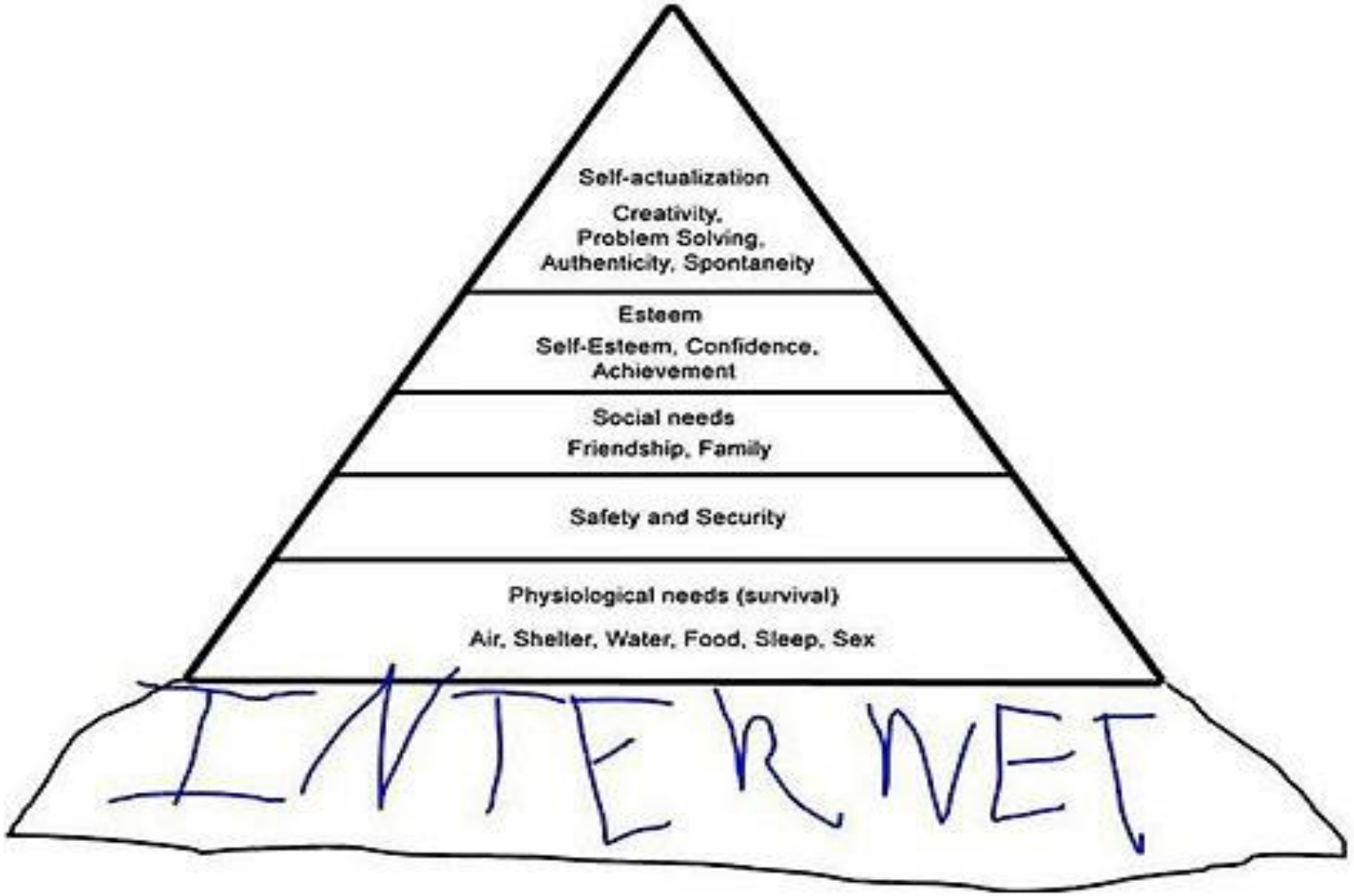
https://www.hte.hu/eivok

eivok@hte.hu

Istvan.olah@hte.hu

olah.istvan@uni-obuda.hu

?


Self-actualization
Creativity,
Problem Solving,
Authenticity, Spontaneity
Esteem
Self-Esteem, Confidence,
Achievement
Social needs
Friendship, Family
Safety and Security
Physiological needs (survival)
Air, Shelter, Water, Food, Sleep, Sex
INTERNET

A Digitális Maslow.

MIK EZEK?

A lehetséges válaszok.

- Kütyük, izék, masinák,
- Játékok,
- **Testrészeink, végtag kiegészítők,**
- Amikkel fekszünk, kelünk,
- **Amiket egész nap nézünk, avagy ki ural kit?** A használó a képernyőt, vagy a képernyő a használót, de ki is vezérli a képernyő tartalmát?
- Amiket már minden gyerek, unoka tud jól használni, de ez nem így van, mert a **használni és tudatosan használni nem ugyanaz!**
- **Munkaeszközök,**
- **Adathordozók,** rólunk, családunkról, ismerőseinkről, munkahelyünkről, etc. minden adat megtalálható rajtuk, vagy rajtuk keresztül, ma egy közepes közösségi szolgálató is többet tud rólunk mint bárki más, milyen jogalappal?
- **Tárgyi eszközök, adatvagyon probléma a számvitelben, és a mindennapokban,**
- **Veszélyforrások,**
- **……**


www.china-defense-mashup.com

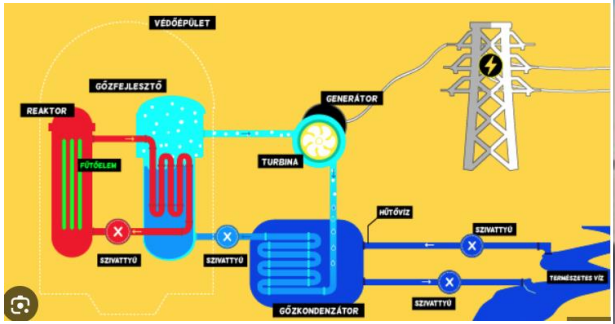
Hol lehet csatát vívni?

- Föld,
- Víz,
- Levegő,
- Világűr,

- KIBERTÉR!!!!!

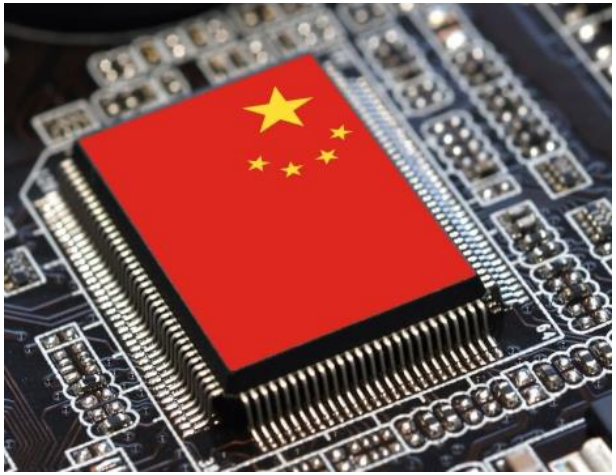
MIK EZEK?

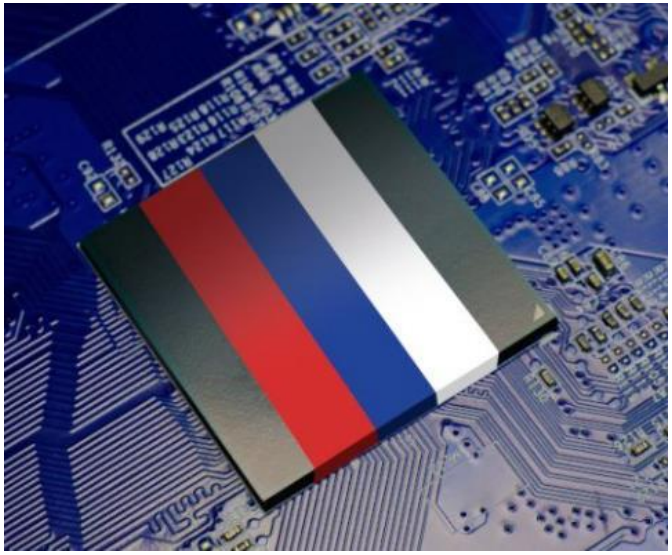

56

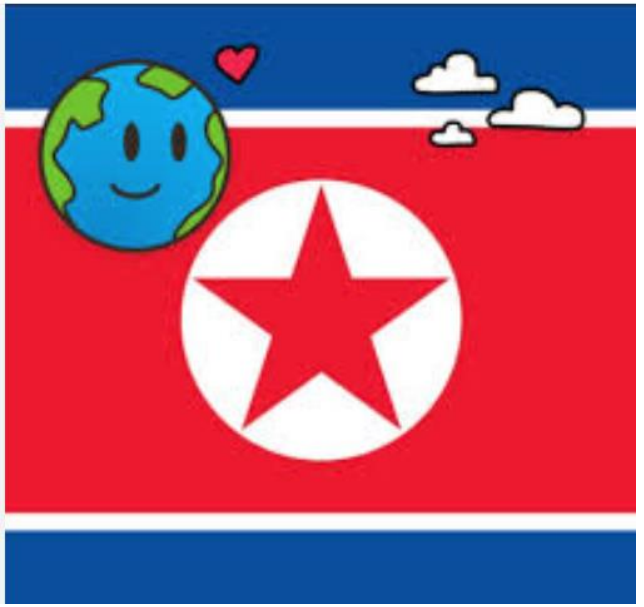

VEDŐÉPÜLET
GŐZFEJLESZTŐ
REAKTOR
FŰTŐELEM
GENERÁTOR
TURBINA
HŰTŐVÍZ
SZIVATTYÚ
SZIVATTYÚ
SZIVATTYÚ
SZIVATTYÚ
TERMÉSZETES VÍZ
GŐZKONDENZÁTOR


WED
12:02
ROOM TEMP
16.0 °C
SET
22 °C
M

Benne van mindenben..??







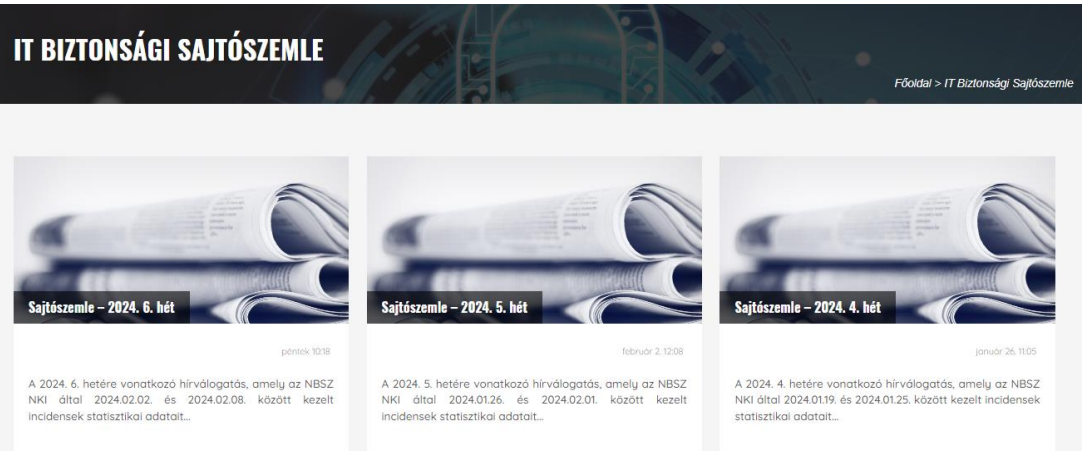
Mi van benne, mint képesség?

- Megfigyelés,
- Lehallgatás,
- Befolyásolás,
- Kémkedés,
- …
- Kik által birtokolva a képességek?
- Milyen jogszabályi, társadalmi, szervezeti, egyéni felhatalmazás alapján?
- A használat első pillanatától, okos-e mindent tiltani taktika?
- **A TUDATOS használat, mint TANULHATÓ KÉPESSÉG kiemelten fontos minden felhasználó esetében! A szervezetek vezetőinek a feladatai közt TOP1 szinten szükséges szerepeljen.**
- **Általános iskola 3. osztálytól: Digitális Kultúra tárgy (15 év múlva látjuk a hatást majd), lesz-e ECDL+ = IT-KIBERJOGSI?**

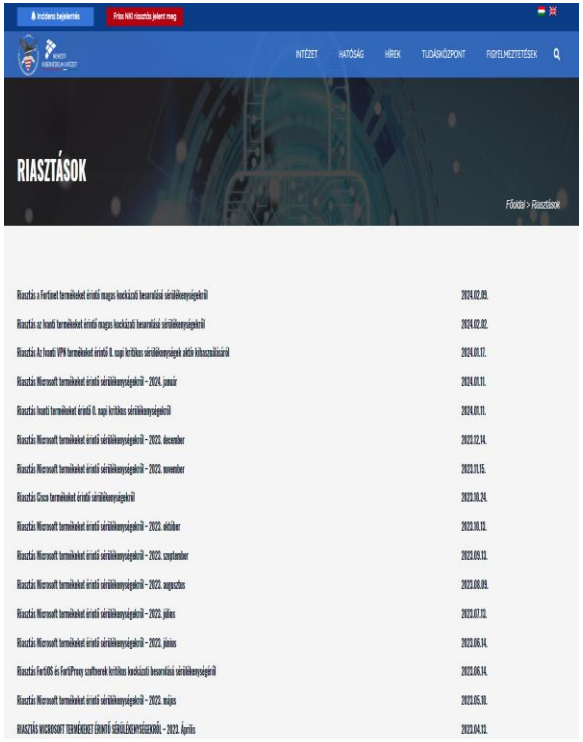
Honnan tudhatunk a fenyegetettségekről?

- Napi sajtó, minden nap 1–2 hír magyarul is, **de tegyük fel a kérdést**, hogy ez érint–e minket / családunkat / munkahelyünket,
- Hazai, és nemzetközi szakmai portálok, hírlevek, vásárolható információk, elemzések, és az NKI:

- NKI weboldala:

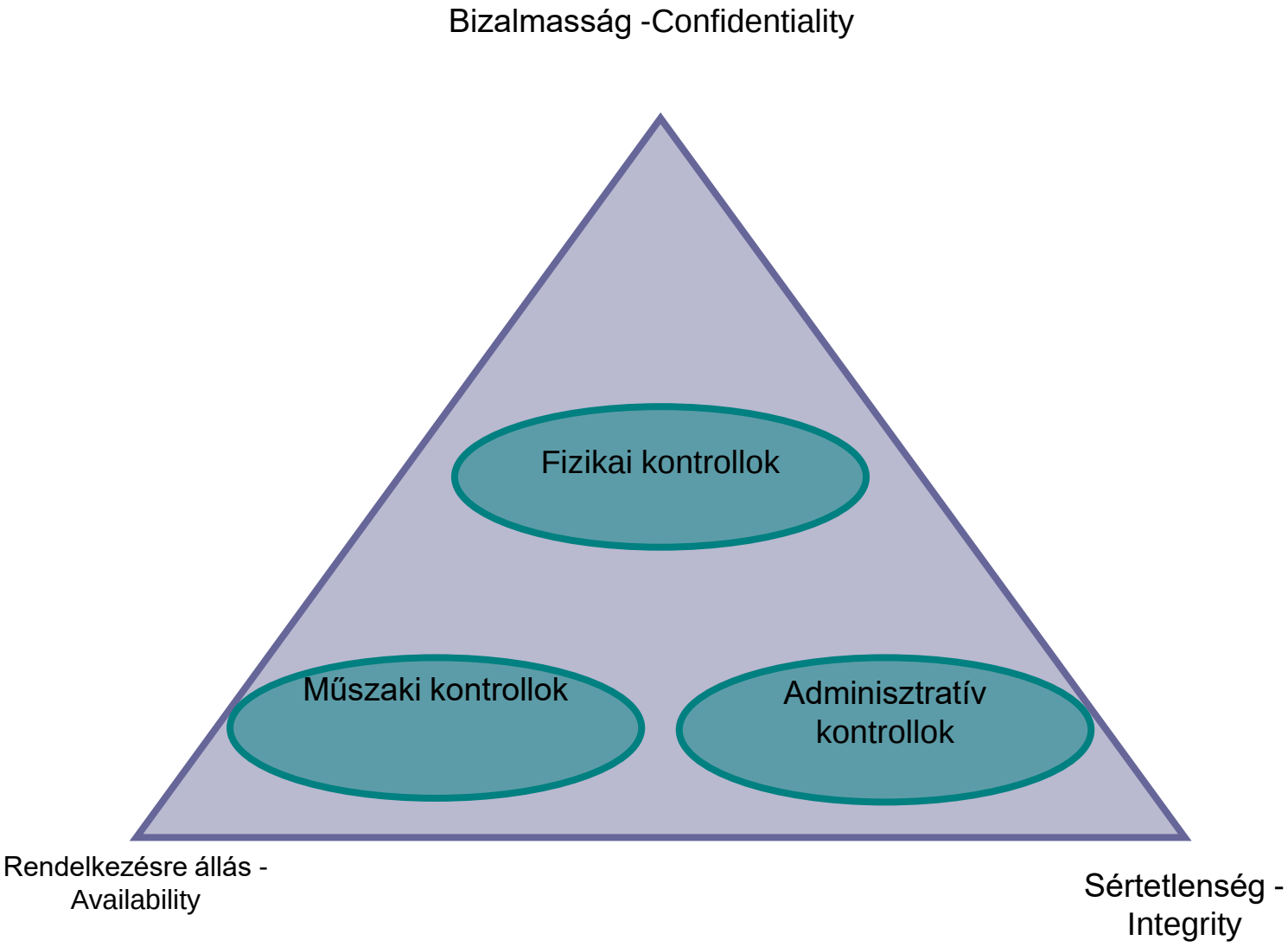


https://nki.gov.hu/it-biztonsag/kiadvanyok/sajtoszemle/



https://nki.gov.hu/figyelmeztetesek/riasztas//

3 szó.. BSR (CIA), 3 fajta kontroll.



A A A ! a klasszikus Ki, Mikor, Mit?

- Authentication: felhasználó azonosítás
- Authorization: jogosultságkezelés
- Accounting: naplózás

Melyek a kapcsolatos módszertanok, kontrollok ?

- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről (módszertani útmutató is egyben!)
- Osztályba sorolás példa:
  - 2.4. A 3. biztonsági osztály esetében közepes káresemény következhet be, mivel
  - 2.4.1. különleges személyes adat sérülhet, személyes adatok nagy mennyiségben sérülhetnek;
  - 2.4.2. az érintett szervezet üzlet–, vagy ügymenete szempontjából érzékeny folyamatokat kezelő elektronikus információs rendszer, információt képező adat, vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok, stb.) védett adat sérülhet;
  - 2.4.3. a lehetséges társadalmi–politikai hatás: bizalomvesztés állhat elő az érintett szervezeten belül, vagy szervezeti szabályokban foglalt kötelezettségek sérülhetnek;
  - 2.4.4. a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 5%–át.

Melyek a kontrollok, pl. az ovi-tábla, egy „okos-excel”?

- https://nki.gov.hu/hatosag/tartalom/urlapok/

ovi460.xltm 2022.09.17. 8:44

A NBSZ-IBF és NBSZ-IBD űrlapokat JAR fájlokban lehet letölteni: ezek futtatásával telepíthetők a kívánt űrlapok az Általános Nyomtatványkitöltő alkalmazáshoz. Ehhez a művelethez telepített Java futtatókörnyezet szükséges.

A NEIH-BKSZ, NEIH-OVI és NEIH-SZVI űrlap használatához Microsoft Office Excel alkalmazás szükséges.

Letöltés:

[NEIH-BKSZ] Bejelentés-köteles szolgáltatók regisztrációs űrlapja (v1.00, MS Office)
[NBSZ-IBF] Információbiztonsági felelős regisztrációs űrlapja
[NBSZ-IBD] Információbiztonsági dokumentációk leíró űrlapja
[NBSZ-SZVI] Szintbe sorolás és védelmi intézkedés űrlap (v2.10, MS Office)
Kitöltési útmutató az NBSZ-SZVI űrlap 2.10 változatához
[NEIH-OVI] Osztályba sorolás és védelmi intézkedés űrlap (v4.60, MS Office)
Kitöltési útmutató a NEIH-OVI űrlap 4.60-as változatához

Osztályba sorolás és védelmi intézkedés űrlap

Rendszer:		rövid neve:		Az elektronikus információs rendszer	
Adatgazda:		törzsszáma:		létfontosságú létesítmény része:	
Adatkezelő:		törzsszáma:			Nem
Adatfeldolgozó:		törzsszáma:		nemzeti adatvagyont dolgoz fel:	
Üzemeltető:		törzsszáma:			Nem
Fejl. projekt:		felhívás száma:		Bizalmasság:	Nincs adat
Verzió:	4.60			Sértetlenség:	Nincs adat
Kiadva:	2017.08.22	Kitöltő neve:		Rendelkezésre állás:	Nincs adat
Forrás:	41/2015. (VII. 15.) BM rendelet 1., 3. és 4. melléklete	Kitöltés dátuma:		Biztonsági osztály:	Nincs adat
Szerzők:	Szilárd Zoltán, Benyó Pál, Juhász György, Simonyi Gyula			Teljesített osztály:	0
3.1.5.	A biztonsági események kezelése	Nem		Nincs adat	Nincs adat
3.1.6.	Emberi tényezőket figyelembe vevő - személy - biztonság	Nem		Nincs adat	Nincs adat
3.1.7.	Tudatosság és képzés	Nem		Nincs adat	Nincs adat
3.2.	FIZIKAI VÉDELMI INTÉZKEDÉSEK	Nem	1	Nincs adat	Nincs adat
3.3.	LOGIKAI VÉDELMI INTÉZKEDÉSEK	Nem	1	Nincs adat	Nincs adat
3.3.1.	Általános védelmi intézkedések	Nem		Nincs adat	Nincs adat
3.3.2.	Tervezés	Nem		Nincs adat	Nincs adat
3.3.3.	Rendszer és szolgáltatás beszerzés	Nem		Nincs adat	Nincs adat
3.3.4.	Biztonsági elemzés	Nem		Nincs adat	Nincs adat
3.3.5.	Tesztelés, képzés és felügyelet	Nem		Nincs adat	Nincs adat
3.3.6.	Konfigurációkezelés	Nem		Nincs adat	Nincs adat
3.3.7.	Karbantartás	Nem		Nincs adat	Nincs adat
3.3.8.	Adathordozók védelme	Nem		Nincs adat	Nincs adat
3.3.9.	Azonosítás és hitelesítés	Nem		Nincs adat	Nincs adat
3.3.10.	Hozzáférés ellenőrzése	Nem		Nincs adat	Nincs adat
3.3.11.	Rendszer- és információsértetlenség	Nem		Nincs adat	Nincs adat
3.3.12.	Naplózás és elszámoltathatóság	Nem		Nincs adat	Nincs adat
3.3.13.	Rendszer- és kommunikációvédelem	Nem		Nincs adat	Nincs adat

A) 3.1. ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK

	A	B	C	D	E	F	G
1.	Sorszám	Intézkedés típusa	Biztonsági osztály				
2.			1	2	3	4	5
3.	3.1.1.	Szervezeti szintű alapfeladatok					
4.	3.1.1.1.	Informatikai biztonsági szabályzat	X	X	X	X	X
5.	3.1.1.2.	Az elektronikus információs rendszerek biztonságáért felelős személy	X	X	X	X	X
6.	3.1.1.3.	Az intézkedési terv és mérföldkövei	0	X	X	X	X
7.	3.1.1.4.	Az elektronikus információs rendszerek nyilvántartása	X	X	X	X	X
8.	3.1.1.5.	Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás	X	X	X	X	X
9.	3.1.2.	Kockázatelemzés					
10.	3.1.2.1.	Kockázatelemzési és kockázatkezelési eljárásrend	X	X	X	X	X
11.	3.1.2.2.	Biztonsági osztályba sorolás	X	X	X	X	X
12.	3.1.2.3.	Kockázatelemzés	X	X	X	X	X
13.	3.1.3.	Rendszer és szolgáltatás beszerzés					
14.	3.1.3.1.	Beszerzési eljárásrend	0	0	X	X	X
15.	3.1.3.2.	Erőforrás igény felmérés	0	0	X	X	X
16.	3.1.3.3.	Beszerzések	0	0	X	X	X
17.	3.1.3.3.2.	A védelem szempontjainak érvényesítése a beszerzés során	0	0	0	X	X
18.	3.1.3.3.3.	A védelmi intézkedések terv-, és megvalósítási dokumentációi	0	0	0	X	X
19.	3.1.3.3.4.	Funkciók - protokollok - szolgáltatások	0	0	0	X	X
20.	3.1.3.4.	Az elektronikus információs rendszerre vonatkozó dokumentáció	0	0	X	X	X
21.	3.1.3.5.	Biztonságtervezési elvek	0	0	0	X	X
22.	3.1.3.6.	Külső elektronikus információs rendszerek szolgáltatásai	0	X	X	X	X
23.	3.1.3.7.	Független értékelők	0	0	0	X	X
24.	3.1.3.8.	Folyamatos ellenőrzés	0	0	X	X	X
25.	3.1.3.8.2.	Független értékelés	0	0	0	X	X

Az adatvagyon.

- Mérjük fel a szervezet adatait, soroljuk be az adatokat biztonsági osztályba!
- Hol érhetők el, hogy kezelhetők?
- Minden tárolási helyet gyűjtsünk össze, e-form, papír, fénykép, stb.!
- Kik férhetnek hozzájuk, szabályozzuk, és ezt mint elvárást érvényesítsük az IT rendszerekben és ne fordítva:
  - Szervezet munkavállalói, kiemelt figyelem a rendszergazdákra!
  - Szervezet partnereinek munkavállalói, külső üzemeltető,
  - Ügyfelek,
  - Hatóságok,
  - Köznyilvános adatok,
  - Akikre nem szoktak gondolni, távközlési cégek, felhő szolgáltatók, etc.,
- Mit nem lehet egy embernek, azaz a kizáró szerepkörök (SOD mátrix)?
- Az IT ökösziszténa összes eleme is értelemezhető adatként, azaz IT környezeteket (fejlesztői, teszt, oktatási, éles, etc.) ugyanúgy mentsük mint az adatokat,
- Az adatok mentéséről, archiválásáról úgy gondoskodjuk, ezeket ellenőrizzük, pl. hogy ne csupa nulla legyen a mentett állomány,
- Életciklus-menedzsment: létrehozás, használat, archív állapot, törlés,
- **Mindent naplózzunk, és a naplók BSR elemeiről gondoskodjuk, mert bizonyítékok!**
- Mindezeket a PDCA (tervezd, csináld, ellenőrizd, cselekedj, és kezd újra) elv szerint.

A Működés biztonsága.

- Mérjük fel a szervezet működési folyamatait, soroljuk be a folyamatokat! pl. BIA módszertan,
- A besorolás szerint döntsünk arról, hogy szükséges-e egy incidens esetén a folyamatot fenntartani!
- Amennyiben igen, akkor erre legyen kész forgatókönyvünk, BCP,
- A forgatókönyveket teszteljük legalább évente!
- Egy BCP-hez határozzuk meg a szükséges IT-rendszereket és ne fordítva!
- Az IT-rendszereket e szerint soroljuk be a **rendelkezésre állás** szempontjából is (pl. SLA, OLA szintek),
- A besorolás alapján döntsünk arról, hogy szükséges-e többleterőforrás a rendszerben, készenléti tartalék rendszer, élesben folyamatosan rendelkezésre álló tartalék,
- Egy incidens (sok féle és fajta lehet) esetében legyen döntési szempontrendszerünk, **szereplőink,** és folyamatunk arra, hogy kell-e a tartalékra átállni,
- Az átállásra legyen kész és tesztet forgatókönyvünk (DR), amelyet a szervezetben minden szereplő begyakorolt,
- Rendelkezzünk naprakész kommunikációs tervvel és folyamattal (BCP itt is),
- Ha minta szükséges: „Az információszolgáltatásról szóló 54/2021. (XI. 23.) MNB rendelet 3. sz. mellékletében felsorolt technikai segédletek 2022,” **P-58**, **P-64**
- Mindezeket a PDCA (tervezd, csináld, ellenőrizd, cselekedj) elv szerint.

Tudásmenedzsment, emberek.

- Mérjük fel a szervezet érettségi szintjét, abból kiindulva készítsünk szervezeti és egyéni képzési terveket!
- Folyamatosan képezzük a legnagyobb kockázati forrást a FELHASZNÁLÓKAT, azaz saját magunkat, családtagjainkat, kollegáinkat,…., legalább évente egy alkalommal a munkaszervezetben!
- **A védelem feladatai során ne az IT-üzemeltetőkre, IT és információbiztonsági szakemberekre, hanem mindenkire gondoljunk, mert csakis a közös védelem lehet eredményes!** (leggyengébb láncszem),
- Időszakonként végezzünk próbát, ahogy pl. tűzriadó próba is van,
- A vezetőket külön készítsük fel az incidensek kezelésére,
- Mindezeket a PDCA szerint.

Köszönöm a figyelmet!

www.hte.hu/eivok

eivok@hte.hu