



Nemzeti Közzolgálati Egyetem (NKE):

Információs rendszerek és hálózatok biztonsága,

Pénzüntézeti információs rendszerek védelme.

Hírközlési és Informatikai Tudományos Egyesület (HTE):

Információbiztonsági Szakosztály-EIVOK, alelnök <https://www.hte.hu/eivok>

eivok@hte.hu





A Kiberhónap.

The screenshot shows the website's header with navigation links: INCIDENS JELENTÉS, Friss NKI riasztás jelent meg, INTÉZET, HATÓSÁG, HÍREK, TUDÁSKÖZPONT, FIGYELMEZTETÉSEK. The main content area features the '10th EUROPEAN CYBER SECURITY MONTH' logo and the text 'EURÓPAI KIBERBIZTONSÁGI HÓNAP'. Below the logo are buttons for 'Regisztráció', 'Események', and 'Archívum'. A paragraph of text explains the event's significance and mentions that Hungary has participated since 2016.

<https://nki.gov.hu/rendezvenyek/kiberhonap22/>

Információbiztonság aktuális kérdései – EIVOK-28 Tudományos – Szakmai Konferencia



- 2022-09-22
- 09:00 - 13:00
- Nyíregyházi Egyetem
- Európai Kiberbiztonsági Hónap

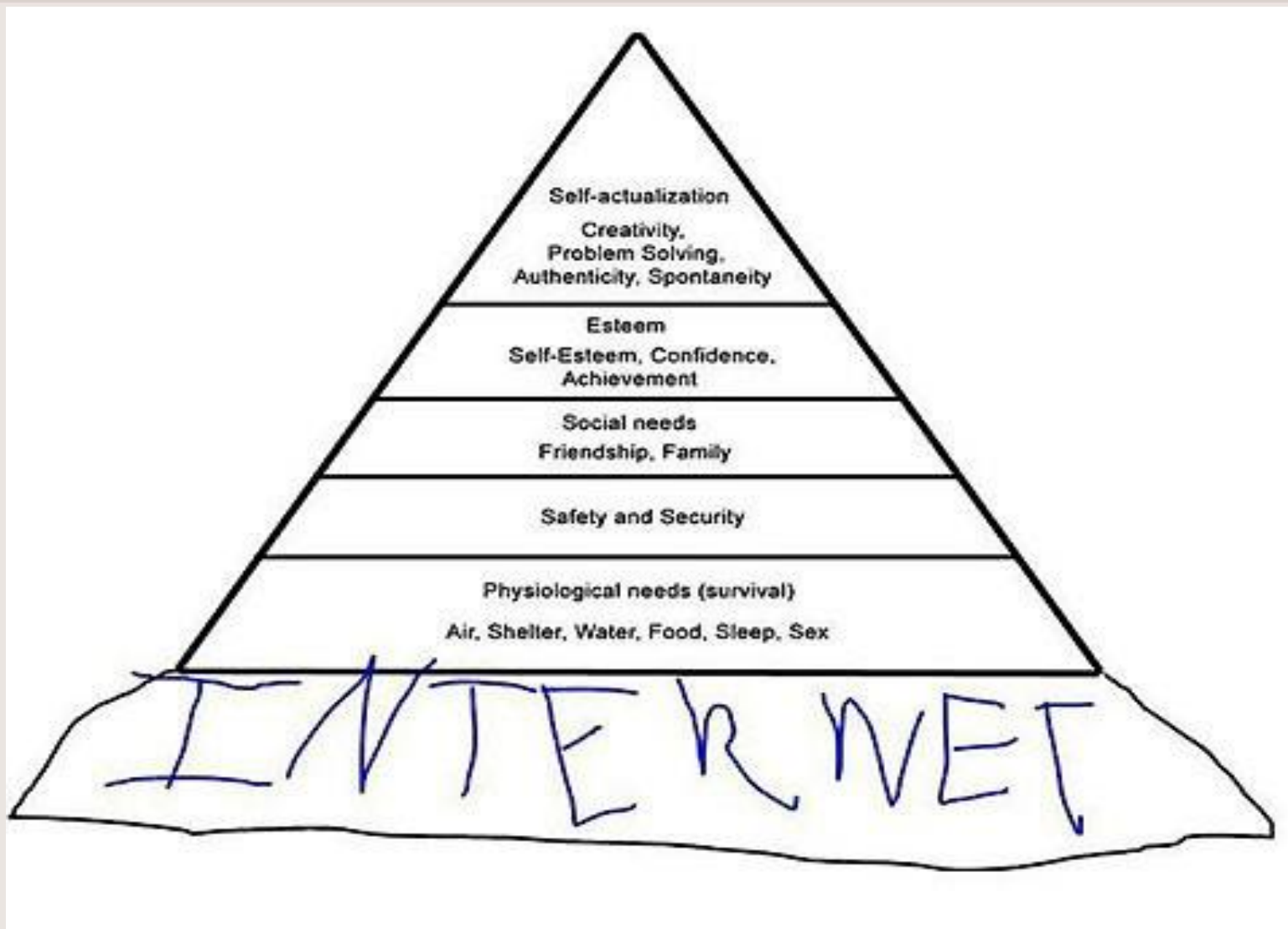
Konferencia betekintést nyújt az aktuális információbiztonság területének számos kérdésébe, amely most Nyíregyházán kerül lefolytatásra. [icon name="user" prefix="fas"] IT biztonsági szakemberek. A téma iránt érdeklődő [...]

TOVÁBBI INFORMÁCIÓ

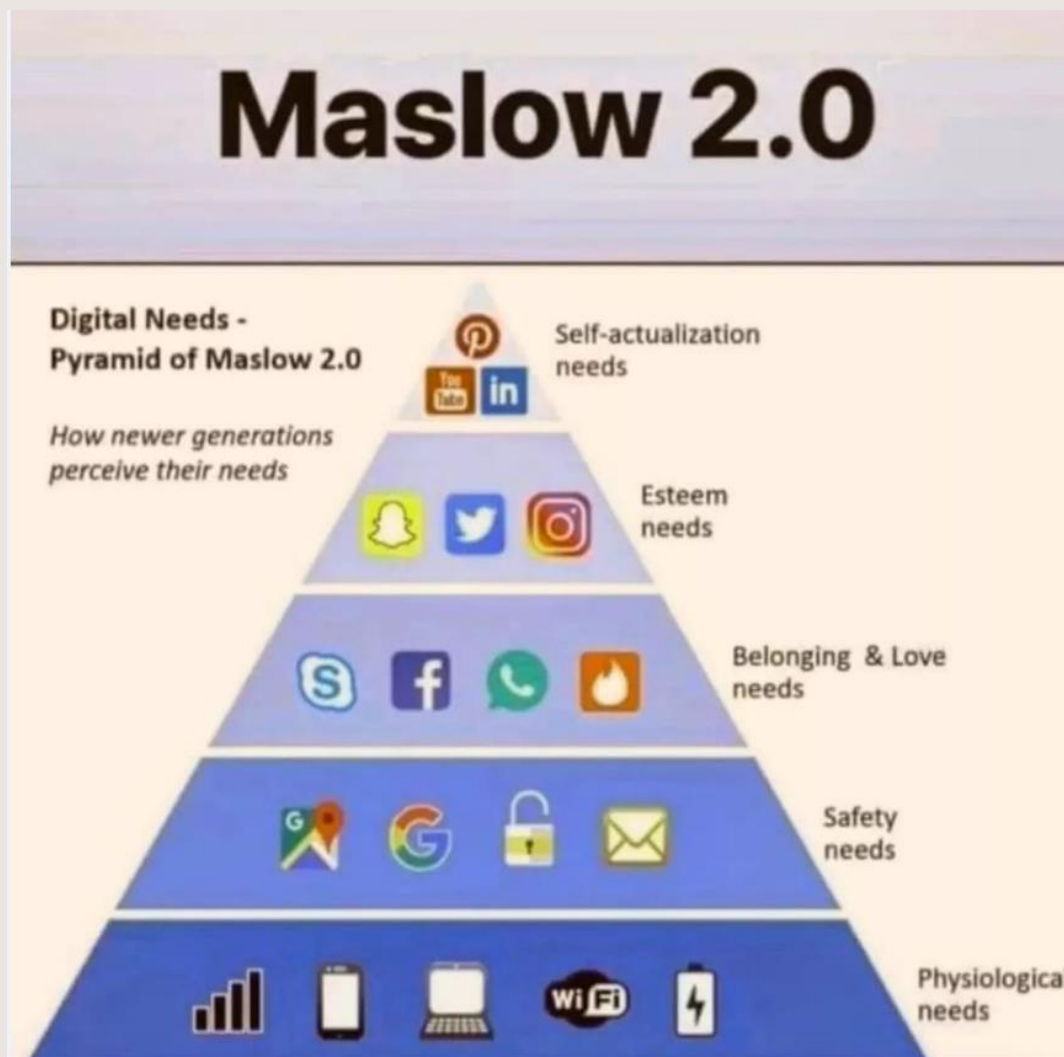


European Union Agency for
Network and Information Security



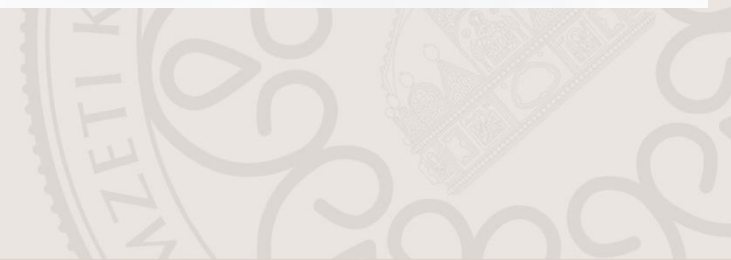


A Digitális Maslow.





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, családukról, ismerőseinkről, munkahelyünkről, etc. minden adat megtalálható rajtuk, vagy rajtuk keresztül, ma egy közepes közösségi szolgáltató is többet tud rólunk mint bárki más, milyen jogalappal?**
- **Tárgyi eszközök, adatvagyon probléma a számvitelben, és a mindennapokban,**
- **Veszélyforrások,**
-



提高信息化素养
培养高科技人才

提高一线部队信息化作战能力
打赢未来信息化战争



Mi történik éppen?



• <http://map.norsecorp.com/#/>



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 / családjunkat / munkahelyünket,
- Hazai, és nemzetközi szakmai portálok, hírlevelek, vásárolható információk, elemzések, és az NKI:



SAJTÓSZEMLE – 2022. 37. HÉT

tegnap 11:37

A 2022. 37. hetére vonatkozó hírvélotás, amely az NBSZ NKI által 2022.09.09. és 2022.09.15. között kezelt incidensek statisztikai adatait...



SAJTÓSZEMLE – 2022. 36. HÉT

szeptember 9. 12:37

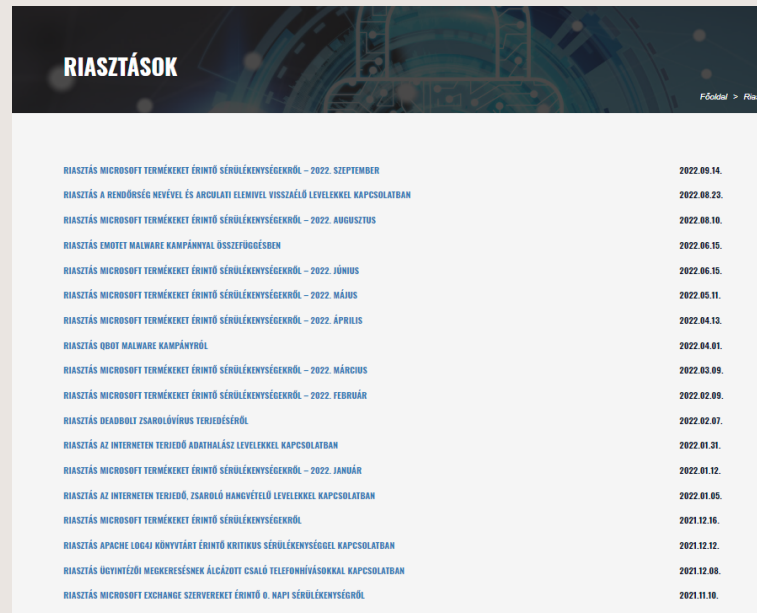
A 2022. 36. hetére vonatkozó hírvélotás, amely az NBSZ NKI által 2022.09.02. és 2022.09.08. között kezelt incidensek statisztikai adatait...



SAJTÓSZEMLE – 2022. 35. HÉT

szeptember 2. 08:29

A 2022. 35. hetére vonatkozó hírvélotás, amely az NBSZ NKI által 2022.08.26. és 2022.09.01. között kezelt incidensek statisztikai adatait...





Stratégiai szint.

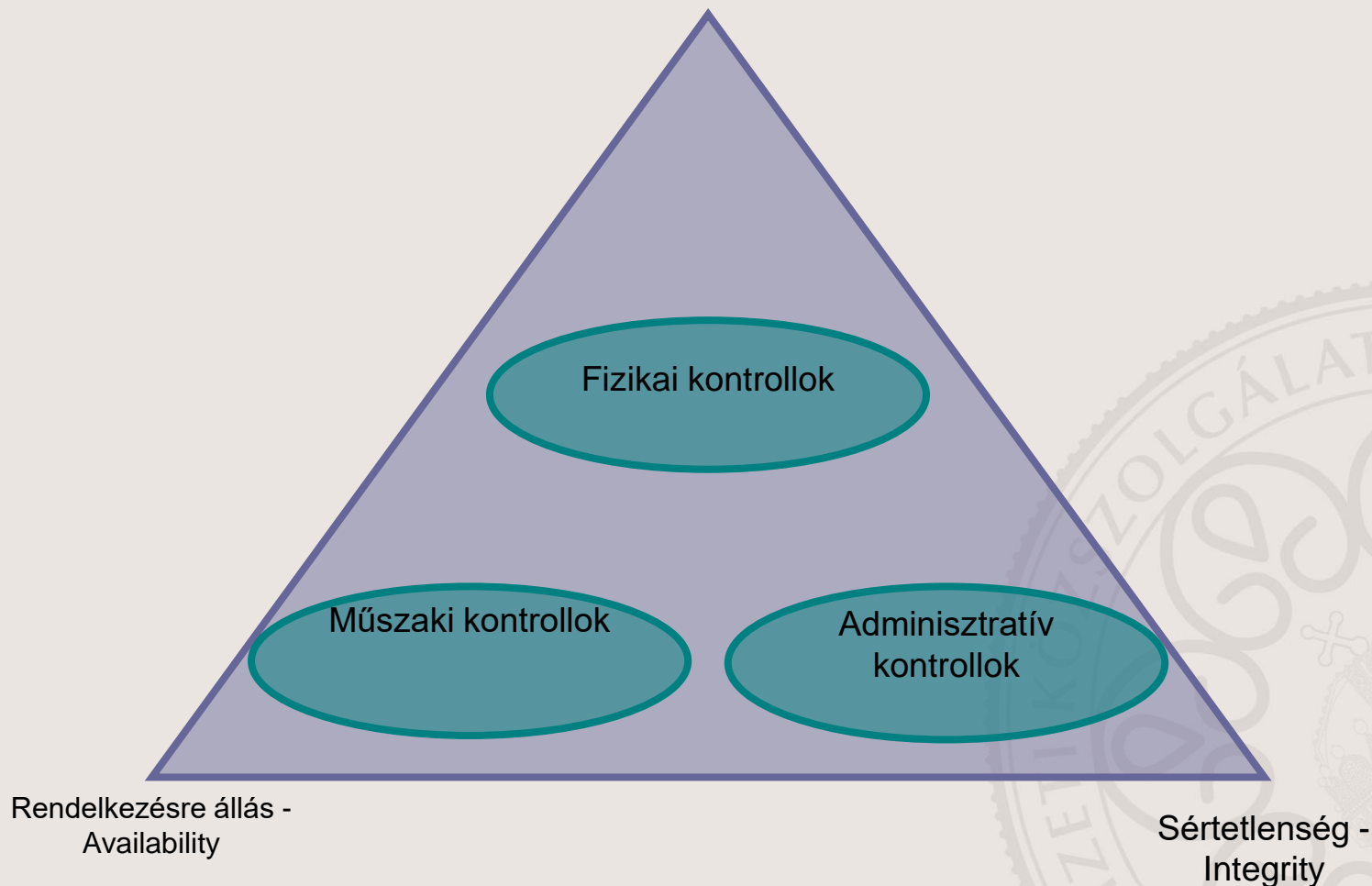
A Kormány 1163/2020. (IV. 21.) Korm. Határozat Magyarország Nemzet Biztonsági Stratégiájáról

159. A kibertérben jelentkező kihívások, kockázatok és fenyegetések kezelésére, a megfelelő szintű kiberbiztonság garantálására, a kibervédelmi feladatok ellátására, a nemzeti létfontosságú **információs infrastruktúra zavartalan működésének biztosítására Magyarországnak készen kell állnia.** Elsődleges feladat a kibertérben ténylegesen jelentkező vagy potenciális kihívások, kockázatok és fenyegetések azonosítása és nyomon követése, a kormányzati koordináció erősítése, a kibertér jogi szabályozásának fejlesztése, **a felhasználók biztonságtudatos viselkedésének elősegítése**, a kormányzati infokommunikációs rendszerek, a nemzeti létfontosságú információs infrastruktúra, a minősített információk és a nemzeti adatvagyon védelmének erősítése, valamint a kiberbiztonsággal kapcsolatos nemzetközi együttműködés bővítése.



3 szó.. BSR (CIA), 3 fajta kontroll.

Bizalmasság -Confidentiality





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

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





Incidens relációk.

- IT üzemi \neq szolgáltatáskiesés, de lehet ilyen hatás is,
- IT üzemi \neq IT biztonsági, de lehet ilyen hatás is,
- IT üzemi \neq adatbiztonsági, de lehet ilyen hatás is,
- IT üzemi \neq épületüzemi, de lehet ilyen hatás is,
- IT biztonsági \neq adatbiztonsági, de lehet ilyen hatás is,
-
- **Minden esetben incidens típusonként kell értékelni!!!**



Ibtv. vonatkozik e ránk?

- **2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról**
- A nemzet érdekében kiemelten fontos – napjaink információs társadalmát érő fenyegetések miatt – a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága.
Társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmosságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerlemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme.
 Mindezekre figyelemmel az Országgyűlés a következő törvényt alkotja:



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

A) 3.1. ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK

1.	A Sorszám	B Intézkedés típusa	C	D	E	F	G
			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 mérőföldkövei	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

Osztályba sorolás és védelmi intézkedés űrlap

Rendszer: Adatgazdó: Adatkezelő: Adatfeldolgozó: Üzemeltető: Fejlesztő projekt:	rövid neve: törzsszáma: törzsszáma: törzsszáma: felhívás száma:	Az elektronikus információs rendszer létfontosságú létesítmény része: Nem nemzeti adatvagyonot dolgoz fel: Nem	
Verzió: 4.60 Kiadva: 2017.08.22 Forrás: 41/2015. (VII. 15.) BM rendelet 1., 3. és 4. melléklete Szerzők: Seilárd Zoltán, Benyő Pál, Juhász György, Simonyi Gyula	Kitöltés dátuma:	Biztonsági osztály: Nincs adat Sértetlenség: Nincs adat Rendelkezésre állás: Nincs adat 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
3.3. LOGIKAI VÉDELMI INTÉZKEDÉSEK	Nem	1	Nincs adat
3.3.1. Általános védelmi intézkedések	Nem		Nincs adat
3.3.2. Tervezés	Nem		Nincs adat
3.3.3. Rendszer és szolgáltatás beszerzés	Nem		Nincs adat
3.3.4. Biztonsági elemzés	Nem		Nincs adat
3.3.5. Tesztelés, képzés és felülvizlet	Nem		Nincs adat
3.3.6. Konfigurációkezelés	Nem		Nincs adat
3.3.7. Karbantartás	Nem		Nincs adat
3.3.8. Adathordozók védelme	Nem		Nincs adat
3.3.9. Azonosítás és hitelesítés	Nem		Nincs adat
3.3.10. Hozzáférés ellenőrzése	Nem		Nincs adat
3.3.11. Rendszer- és információvédelem	Nem		Nincs adat
3.3.12. Hálózati és elszámoltathatóság	Nem		Nincs adat
3.3.13. Rendszer- és kommunikációvédelem	Nem		Nincs adat



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 ökoszisztéma összes eleme is értelemezhető adatként, azaz IT környezeteket (fejlesztői, teszt, oktatási, éles, etc.) ugyanúgy mentjük 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, készletléti tartalék rendszer, élesben folyamatosan rendelkezésre álló tartalék,
- Egy incidens (sokféle 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!

eivok@hte.hu

