MILTON FRIEDMAN EGYETEM

PROGRAMOZÁSI TECHNOLÓGIÁK

4. óra - Kockázatmenedzsment

2024.04.05

Szalai Patrik

szalai.patrik@uni-milton.hu

TÉMAKÖRÖK:

4, Risk Management

- Bevezetés
- Miért szükséges
- Lépések
- Kapcsolódó fogalmak
  - ORM
  - Kibervédelem
  - BCP
- COBIT – ISACA
- CC
- ITB, IBK
- NIS2 és CER

5, Gyakorlás

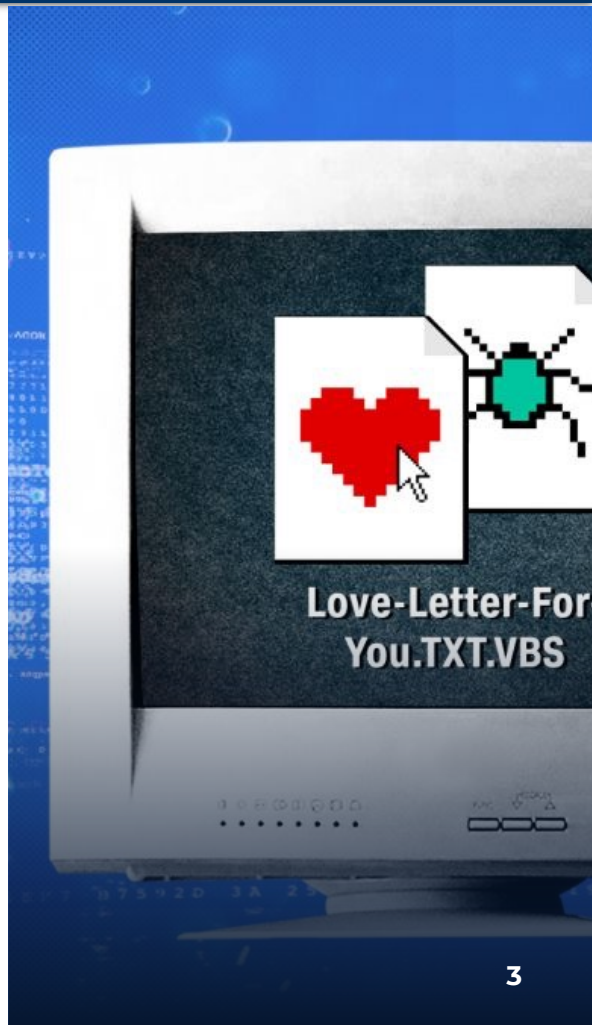
- Mátrixok
  - Veszélyforrások
  - Valószínűség
  - Kár kategóriák
  - Kockázat kategóriák
  - Szorzótábla
  - Elviselhetetlen kockázatok
  - Alternatív védelmi intézkedések
  - Javasolt védelmi intézkedések

RISK MANAGEMENT

Bevezetés | **Lépések** | **Fogalmak**

ISMÉTLÉS – KOCKÁZATKEZELÉS

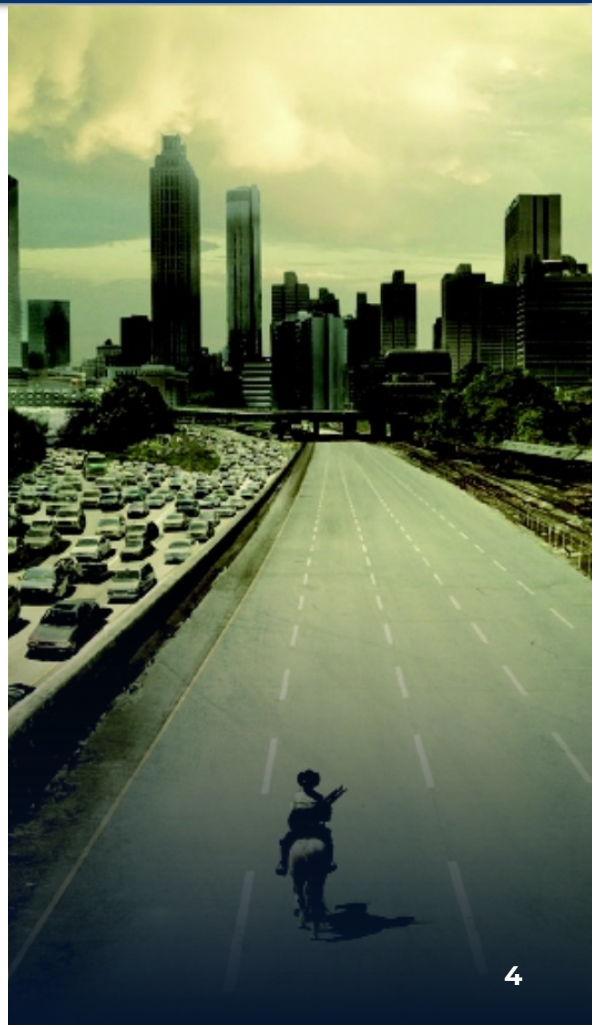
- **Az informatika szerepe napjainkban**
  - A kezdetekben csak apró változások
  - Majd a mindennapok része
  - Mára már civilizációnk alappillére
- **A felhasználással a rendszerek is nőnek**
  - Nő a komplexitás
  - Nő a függőség
  - Nő a kitettség
  - **Nő a kockázat**
- **Az okozott károk**
  - „Melissa” (1999) $ 80 000 000
  - „ILOVEYOU” (2000) $ 10 000 000 000
  - „Mydoom” (2004) $ 38 000 000 000+



ISMÉTLÉS – KOCKÁZATKEZELÉS

- **A kockázat management 4 fő lépése:**
  - A kockázatok azonosítása
  - Értékelése
  - Csökkentése
  - Kommunikációja

- **A kockázat mérőszámai**
  - **A:** Valószínűség
  - **B:** Okozott kár mértéke
  - Kockázat súlyossága **= A x B**



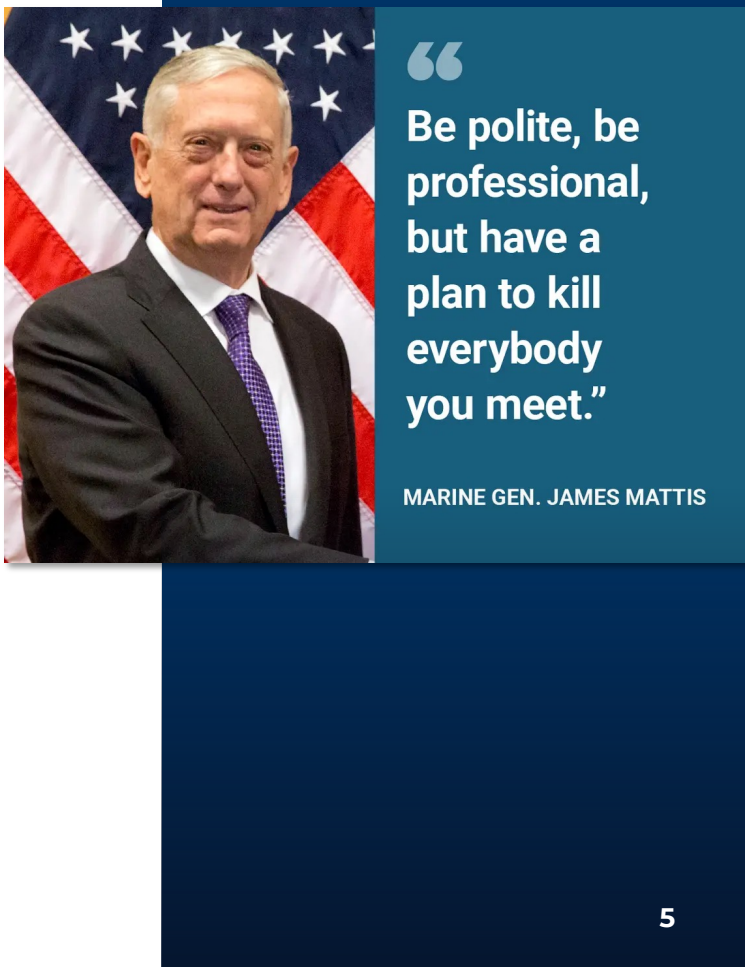
KIHÍVÁSOK

- **Minden eset más és más**
  - Államigazgatás
  - Pénzügy
  - Kutatás
  - Harcászat
  - Energetika
  - Stb...
  - **KKV-k esetében is van kockázat!**

- **DE!** Nem kell paranoidnak lenni!

- **Kockázatok jellege**
  - Fizikai biztonságot veszélyeztető
  - Információbiztonságot veszélyeztető
  - Üzletfolytonosságot veszélyeztető

Soroljunk még párat!

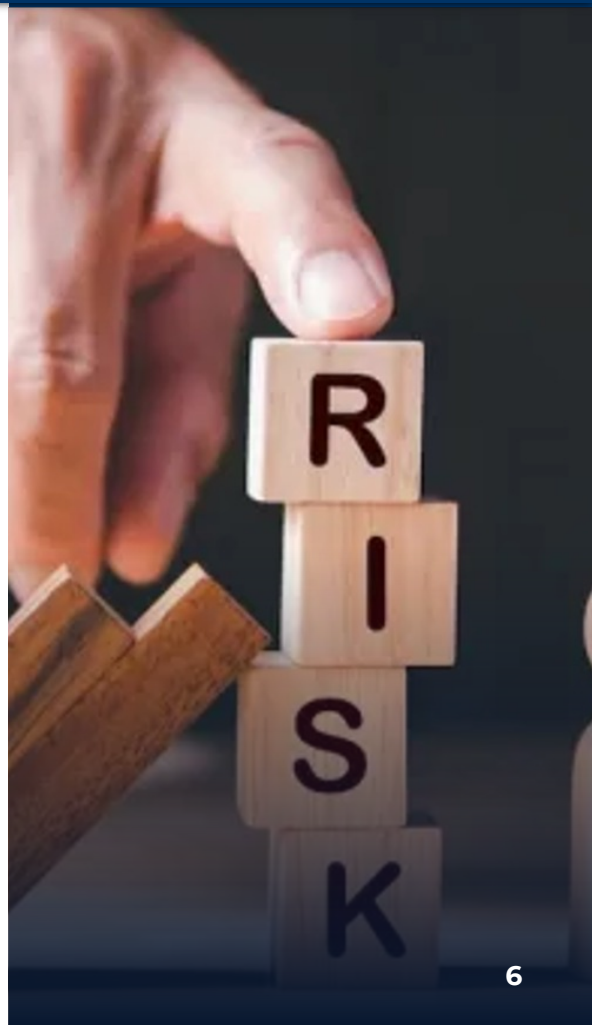


KOCKÁZAT KATEGÓRIÁK

- Pénzügyi Kockázat
- Opeational Risk
- Piaci Kockázat
- Hitelkockázat
- PR Kockázat - "Arcvesztés”
- Jogi Kockázat
- Compliance Kockázat
- Környezeti Kockázat
- Ellátási lánc Kockázat

Főként hármat fogunk vizsgálni:

- **Fizikai biztonságot veszélyeztető kockázat**
- **Információbiztonságot veszélyeztető kockázat**
- **Üzletfolytonosságot veszélyeztető kockázat**



KOCKÁZAT KATEGÓRIÁK

Fizikai biztonságot veszélyeztető kockázatok

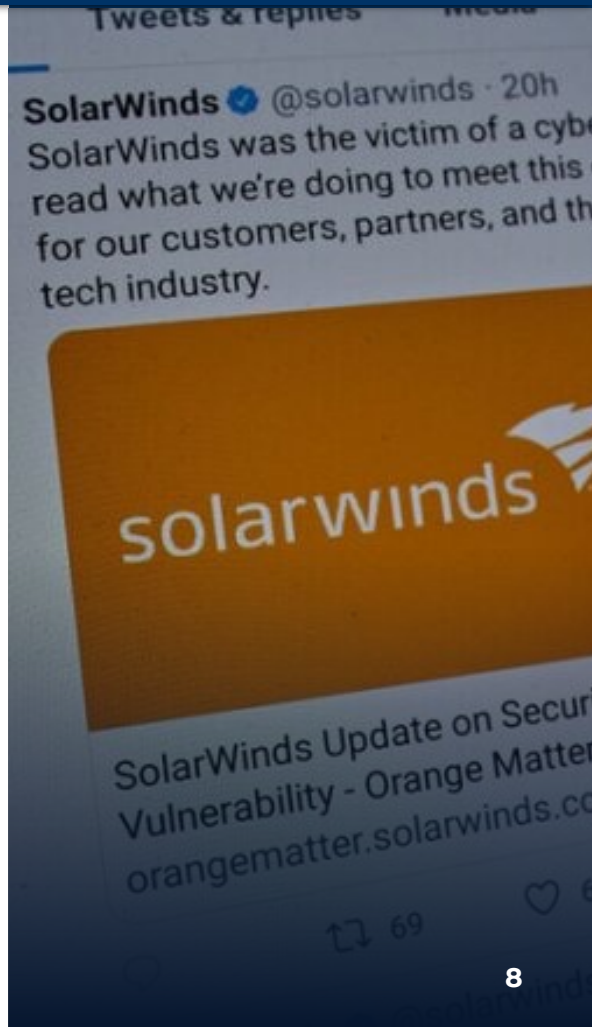
- Fizikai károk, akár tárgyi- akár emberi sértettel
- Ide tartoznak a:
  - Balesetek
  - Lopás (tulajdon ellopásából eredő vagyonszerzési céllal)
  - Rongálás
  - Szabotázs
  - Terrorizmus
  - Vis maior helyzetek
    - Természet által előidézett
    - Ember által előidézett
- Kezelése, megelőzése általában fizikai úton történik.

KOCKÁZAT KATEGÓRIÁK

Információbiztonságot veszélyeztető kockázatok

- Sokrétű károk, pénzügyitől az emberéletekig terjedhetnek
- Ide tartoznak a:
  - Adatvesztés
  - Adatszivárgás/Lopás
  - Adatokkal való visszaélés
  - Kibertámadások
  - Insider Threat
  - IT Incidensek

- Kezelésükhöz kiforrott információbiztonsági tervekre és folyamatokra, megoldásokra van szükség.

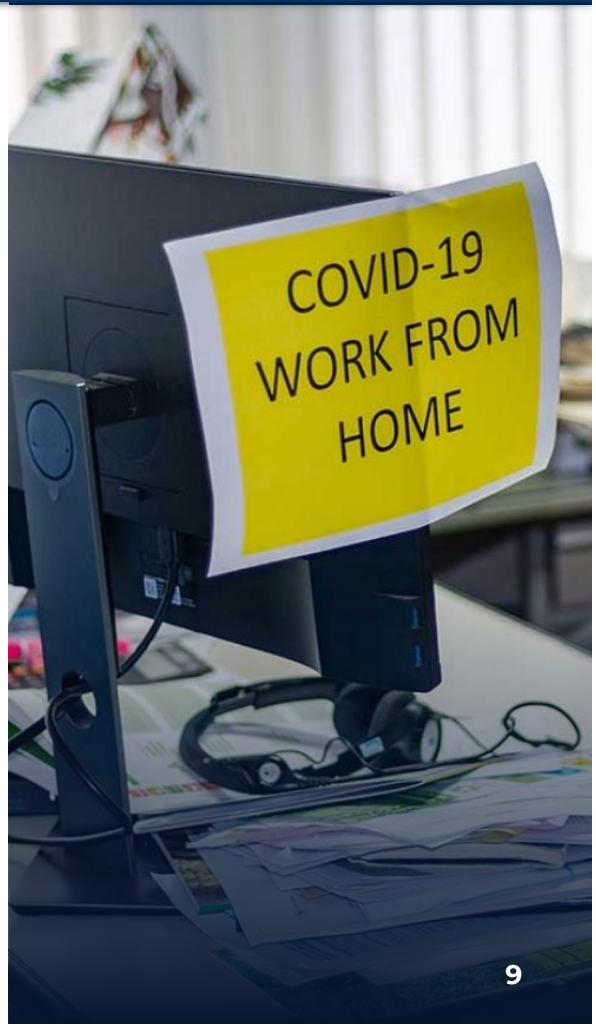


KOCKÁZAT KATEGÓRIÁK

Üzletfolytonosságot veszélyeztető kockázatok

- Adatvesztéstől a pénzügyi károkig
- Ide tartoznak a:
  - Rendundancia hiánya
  - Erőforrások hiánya
  - Dependenciák
  - BCP hiányosságok
  - Hiányos Kommunikáció és Koordináció

- Kezelésükhöz tervezésre, felügyeletre és megfelelően rugalmas folyamatokra van szükség.



A CIA TRIÁD

Az információbiztonság 3 alappillére

- Confidentiality
- Integrity
- Availability

Feladat: Próbáljuk meg definiálni őket!

A CIA TRIÁD

Az információbiztonság 3 alappillére

- **Confidentiality** – Az erőforráshoz csak a felhatalmazott felek férnek hozzá.

Jó ha mindenki hozzáfér? Árthat az integritynek?

- **Integrity** – Az erőforrás tartalma ép, megbízható és nem megmásított.

Megbízhatok az adatban? Garantáltam az épségét?

- **Availability** – Az erőforrást a felhatalmazott felek el tudják érni amikor kell.

Az adat védett és ép, de semmit nem ér, ha nem férek hozzá amikor kell!

A COBIT

Az ISACA management terve

- **COBIT –** Control Objectives for Information and related Technologies
- Ajánlás gyűjtemény
- Best Practices
- IT Managerek számára
- Kockázatmenedzsment akcióterv fejezet

Nem fogunk COBIT vizsgát tenni most, de a lépéseit érdemes megismerni!

A COBIT RISK MANAGEMENT LÉPÉSEI

A kockázatelemző munkájának lépései

1. Veszélyforrások feltérképezése
2. Valószínűségi kategóriák meghatározása
3. Veszélyforrások bekövetkezésének becslése
4. Kárkategóriák meghatározása
5. Okozott kár becslése
6. Kockázatkategórák meghatározása
7. Szorzótábla meghatározása
8. Elviselhetetlen kockázatok meghatározása
9. Alternatív védelmi intézkedések felderítése
10. Javasolt védelmi intézkedések meghatározása

COBIT® 5
AN ISACA® FRAMEWORK

ISACA®

GYAKORLAT – KOCKÁZATELEMZÉS

Tegyük fel, hogy:

- Önök egy tanácsadó cégben dolgoznak kockázatelemzőként
- Ügyfelük egy hazai nagyvállalat
- Az IT infrastruktúra veszélyforrásait kell felmérniük és tanácsot adni a kockázatkezelésre

Kérdés: Mikre kell gondolni a kezdéshez?

1. VESZÉLYFORRÁSOK FELTÉRKÉPEZÉSE

Az egyszerűség kedvéért szűkítsük a scope-ot!

- Áramszünet
- Alaplapi meghibásodás
- Adathordozó-meghibásodás
- Betöréses lopás
- Lehallgatás
- Jogosulatlan módosítás
- Más nevében adott utasítás
- Számítógépes betörés
- Vírusfertőzés
- Tűzvész

Feladat: Készítsünk gyűjtőkategóriákat!

1. VESZÉLYFORRÁSOK FELTÉRKÉPEZÉSE

Gyűjtőkategóriák

- **SZ** – Szervezési gyengeségek (servezési hiányosságokból eredó veszélyek) - Szl, Sz2 ...
- **T** – Természeti veszélyforrások (pl. túz, csótörés, árvíz, villám, földrengés) - T1, T2 ...
- **F** – Fizikai veszélyek (pl. betörés, lopás, rongálás) - F1, F2 ...
- **L** – Logikai fenyegetések (pl. informatikai csalás, halózati betörés, lehallgatás) - L1, L2 ...
- **H** – Humán veszélyforrások (belsó munkatársak gondatlansága, visszaélések) - H1, H2

2. VALÓSZÍNŰSÉG MEGHATÁROZÁSA

Bekövetkezési valószínűség

P = Probability

Jelölés	Megnevezés	Előfordulások száma	Leírás
PVS	Very Small	**0.0 - 0.1 / év**	Eseti előfordulás
PS	Small	**0.1 - 0.2 / év**	Ritka előfordulás
PL	Large	**0.2 – 1.0 / év**	Évente előfordul
PVL	Very Large	**1.0+ / év**	Évente többször előfordul

2. VALÓSZÍNŰSÉG MEGHATÁROZÁSA

Bekövetkezési valószínűség

- **P = Probability**

Definíciók:

- **PVS** – Ritkán, kb/max 10 évente egyszer várható az előfordulása
- **PS** – Kb. 5-10 évente előforduló, vagy csak profi támadó által kihasználható gyengeség
- **PL** – Kb. évente egyszer előforduló vagy átlagos szakember által is végrehajtható visszaélés
- **PVL** – Évente többször is előforduló vagy BÁRKI által kihasználható gyengeség

3. VESZÉLYFORRÁSOK BEKÖVETKEZÉSÉNEK BECSLÉSE – ÓRAI MUNKA

ID	Veszélyforrás	P
F1	Áramszünet	
F2	Alaplapi meghibásodás	
F3	Adathordozó meghibásodás	
H1	Betöréses lopás	
L1	Lehallgatás	
L2	Jogosulatlan módosítás	
L3	Más nevében adott utasítás	
L4	Számítógépes betörés	
L5	Vírusfertőzés	
T1	Tűzvész	

3. VESZÉLYFORRÁSOK BEKÖVETKEZÉSÉNEK BECSLÉSE - PÉLDA

ID	Veszélyforrás	P
F1	Áramszünet	PVL
F2	Alaplapi meghibásodás	PL
F3	Adathordozó meghibásodás	PL
H1	Betöréses lopás	PL
L1	Lehallgatás	PS
L2	Jogosulatlan módosítás	PS
L3	Más nevében adott utasítás	PL
L4	Számítógépes betörés	PS
L5	Vírusfertőzés	PVL
T1	Tűzvész	PVS

4. KÁRKATEGÓRIÁK MEGHATÁROZÁSA

D = Damage

Jelölés	Megnevezés	Anyagi kár	Emberi kár
DVS	Very Small	**10 000.- HUF**	**-**
DS	Small	**100 000.- HUF**	**-**
DA	Average	**1 000 000.- HUF**	**könnyű**
DL	Large	**10 000 000.- HUF**	**súlyos**
DVL	Very Large	**Üzletmenet időszakos megszakadása**	**halálos**
DD	Disaster	**Üzletmenet hosszabb, teljes megszakadása**	**Tömeges**

4. KÁRKATEGÓRIÁK MEGHATÁROZÁSA

Definíciók

- **D – Damage – Kár**
- **DVS** – Elsődleges, kis összegű kár
- **DS** – Másodlagos, nagyobb összegű kár
- **DA** – Fennakadás az alkalmazói rendszerekben vagy könnyű emberi sérülés
- **DL** – Komoly fennakadás az üzleti folyamatokban vagy súlyos emberi sérülés
- **DVL** – Az üzletmenet hosszabb megszakadása, ügyfélkörben is érezhető változás vagy haláleset
- **DD** – Az üzletmenet hosszabb megszakadása, mely az egész cég csődjét okozhatja, vagy kihatással lehet a cég részvényeire vagy tömeges és súlyos emberi sérüléseket, haláleseteket okozhat

5. OKOZOTT KÁR BECSLÉSE – ÓRAI MUNKA

Alkalmazzuk a CIA triádot!

ID	Veszélyforrás	P	C	I	A
F1	Áramszünet	**PVL**			
F2	Alaplapi meghibásodás	**PL**			
F3	Adathordozó meghibásodás	**PL**			
H1	Betöréses lopás	**PL**			
L1	Lehallgatás	**PS**			
L2	Jogosulatlan módosítás	**PS**			
L3	Más nevében adott utasítás	**PL**			
L4	Számítógépes betörés	**PS**			
L5	Vírusfertőzés	**PVL**			
T1	Tűzvész	**PVS**			

5. OKOZOTT KÁR BECSLÉSE - PÉLDA

Alkalmazzuk a CIA triádot! (Figyelem, a könyvben található példán változtattam!)

ID	Veszélyforrás	P	C	I	A
F1	Áramszünet	PVL	-	DS	DA
F2	Alaplapi meghibásodás	PL	-	-	DA
F3	Adathordozó meghibásodás	PL	DS	DA	DL
H1	Betöréses lopás	PL	DL	-	DL
L1	Lehallgatás	PS	DL	-	-
L2	Jogosulatlan módosítás	PS	-	DA	-
L3	Más nevében adott utasítás	PL	DA	DA	-
L4	Számítógépes betörés	PS	DVL	DVL	DS
L5	Vírusfertőzés	PVL	DL	DL	DL
T1	Tűzvész	PVS	-	DD	DD

6. KOCKÁZATKATEGÓRIÁK MEGHATÁROZÁSA

R = Risk

Jelölés	Megnevezés	Kár várható értékének nagyságrendje
RVS	Very Small	**10 000.- HUF / év**
RS	Small	**100 000.- HUF / év**
RA	Average	**1 000 000.- HUF / év**
RL	Large	**10 000 000.- HUF / év**
RVL	Very Large	**Beláthatatlan (nem korlátos)**

7. SZORZÓTÁBLA MEGHATÁROZÁSA

R = P x D

P/D	DVS	DS	DA	DL	DVL	DD
PVS	RVS	RVS	RS	RA	RL	RVL
PS	RVS	RS	RA	RL	RVL	RVL
PL	RVS	RS	RA	RL	RVL	RVL
PVL	RS	RS	RL	RVL	RVL	RVL

7. SZORZÓTÁBLA MEGHATÁROZÁSA

Színkódokkal egyszerűbb az áttekintés és a szemléltetés.

P/D	DVS	DS	DA	DL	DVL	DD
PVS	RVS	RVS	RS	RA	RL	RVL
PS	RVS	RS	RA	RL	RVL	RVL
PL	RVS	RS	RA	RL	RVL	RVL
PVL	RS	RS	RL	RVL	RVL	RVL

7. SZORZÓTÁBLA ALKALMAZÁSA – ÓRAI MUNKA

Kiegészítjük a táblát az R értékkel. Mindig a legnagyobb D értéket alkalmazva, a legrosszabb eshetőséget!

ID	Veszélyforrás	P	C	I	A	R
F1	Áramszünet					
F2	Alaplapi meghibásodás					
F3	Adathordozó meghibásodás					
H1	Betöréses lopás					
L1	Lehallgatás					
L2	Jogosulatlan módosítás					
L3	Más nevében adott utasítás					
L4	Számítógépes betörés					
L5	Vírusfertőzés					
T1	Tűzvész					

7. SZORZÓTÁBLA ALKALMAZÁSA - PÉLDA

Kiegészítjük a táblát az R értékkel. Mindig a legnagyobb D értéket alkalmazva, a legrosszabb eshetőséget!

ID	Veszélyforrás	P	C	I	A	R
F1	Áramszünet	PVL	-	DS	DA	RL
F2	Alaplapi meghibásodás	PL	-	-	DA	RA
F3	Adathordozó meghibásodás	PL	DS	DA	DL	RL
H1	Betöréses lopás	PL	DL	-	DL	RL
L1	Lehallgatás	PS	DL	-	-	RL
L2	Jogosulatlan módosítás	PS	-	DA	-	RA
L3	Más nevében adott utasítás	PL	DA	DA	-	RA
L4	Számítógépes betörés	PS	DVL	DVL	DS	RVL
L5	Vírusfertőzés	PVL	DL	DL	DL	RVL
T1	Tűzvész	PVS	-	DD	DD	RVL

8. ELVISELHETETLEN KOCKÁZATOK MEGHATÁROZÁSA

Ezeket külön jelöljük a többitől, fontos, hogy ezek nem csak RVL értékek!

P/D	DVS	DS	DA	DL	DVL	DD
PVS	RVS	RVS	RS	RA	RL	RVL
PS	RVS	RS	RA	RL	RVL	RVL
PL	RVS	RS	RA	RL	RVL	RVL
PVL	RS	RS	RL	RVL	RVL	RVL

8. ELVISELHETETLEN KOCKÁZATOK MEGHATÁROZÁSA – ÓRAI MUNKA

A táblázat alapján elviselhetetlen kockázatok:

ID	Veszélyforrás	P	C	I	A	R
F1	Áramszünet					
F2	Alaplapi meghibásodás					
F3	Adathordozó meghibásodás					
H1	Betöréses lopás					
L1	Lehallgatás					
L2	Jogosulatlan módosítás					
L3	Más nevében adott utasítás					
L4	Számítógépes betörés					
L5	Vírusfertőzés					
T1	Tűzvész					

8. ELVISELHETETLEN KOCKÁZATOK MEGHATÁROZÁSA - PÉLDA

A táblázat alapján elviselhetetlen kockázatok:

ID	Veszélyforrás	P	C	I	A	R
F3	Adathordozó meghibásodás	PL	DS	DA	DL	RL
H1	Betöréses lopás	PL	DL	-	DL	RL
L4	Számítógépes betörés	PS	DVL	DVL	DS	RVL
L5	Vírusfertőzés	PVL	DL	DL	DL	RVL
T1	Tűzvész	PVS	-	DD	DD	RVL

9. ALTERNATÍV VÉDELMI INTÉZKEDÉSEK FELDERÍTÉSE

Lehetséges védelmi megoldások és hatásuk:

- **D –** Okozott kár kategóriáját csökkenti 1-el
- **DD** – Okozott kár kategóriáját csökkenti 2-vel
- **P** – A bekövetkezési valószínűség kategóriát csökkenti 1-el
- **PP** – A bekövetkezési valószínűség kategóriát csökkenti 2-vel
- **E** – Megszűnteti a veszélyforrás kockázatát

9. ALTERNATÍV VÉDELMI INTÉZKEDÉSEK FELDERÍTÉSE – ÓRAI MUNKA

V = Védelmi intézkedés

ID	Védelmi intézkedés	Beruházás (CAPEX)	Éves költség (OPEX)	Hatás
V1				
V2				
V3				
V4				
V5				
V6				
V7				
V8				
V9				
V10				

9. ALTERNATÍV VÉDELMI INTÉZKEDÉSEK FELDERÍTÉSE - PÉLDA

V = Védelmi intézkedés

ID	Védelmi intézkedés	Beruházás (CAPEX)	Éves költség (OPEX)	Hatás
V1	Szünetmentes táp	5 000 000.- HUF	50 000.- HUF	F1-D, F1-P
V2	Áramfejlesztő	10 000 000.- HUF	200 000.- HUF	F1-E
V3	Poroltók	1 000 000.- HUF	200 000.- HUF	T1-DD, T1-PP
V4	Duplikálás	5 000 000.- HUF	200 000.- HUF	F2-PP, F3-PP
V5	Hibatűrő rendszer	30 000 000.- HUF	2 000 000.- HUF	F2-PP, F3-PP
V6	Biztonsági mentések	2 000 000.- HUF	2 000 000.- HUF	F3-D, L5-D
V7	Riasztórendszer	20 000 000.- HUF	2 000 000.- HUF	H1-DD, H1-P
V8	Biztonsági őrség	2 000 000.- HUF	30 000 000.- HUF	H1-E
V9	Biztosítás	0	10 000 000.- HUF	H1-D
V10	Adatkommunikáció titkosítása	2 000 000.- HUF	0	L1-E
V11	Hozzáférés-védelem	500 000.- HUF	0	L2-P, L4-P
V12	Digitális aláírás	500 000.- HUF	0	L3-E
V13	Vírusvédelem	500 000.- HUF	200 000.- HUF	L5-PP, L5-D

10. JAVASOLT VÉDELMI INTÉZKEDÉSEK MEGHATÁROZÁSA

A lehető legideálisabb intézkedések csoportja

- Lehető legkisebb beruházással
- Lehető legkisebb éves költséggel
- Effektíven megszüntetni az összes elviselhetetlen kockázatot
- Elviselhetetlen kategória alá szorítani nem kötelező teljesen **E – Eliminálni**, ha az a fenti 2 szempontot sérti

Súlyozott költségek:

- Az éves költség 3x szorzóval számolandó a beruházással szemben

Végül: Nézzük át, nem becsültünk-e valamilyen intézkedést túl!

10. JAVASOLT VÉDELMI INTÉZKEDÉSEK MEGHATÁROZÁSA – PÉLDA

Szóba jövő intézkedések:

ID	Veszélyforrás	Védelmi intézkedések
F3	Adathordozó meghibásodás	**V4, V5, V6**
H1	Betöréses lopás	**V7, V8, V9**
L4	Számítógépes betörés	**V11**
L5	Vírusfertőzés	**V6, V13**
T1	Tűzvész	**V3**

10. JAVASOLT VÉDELMI INTÉZKEDÉSEK MEGHATÁROZÁSA – ÓRAI MUNKA

V = Védelmi intézkedés

ID	Védelmi intézkedés	Beruházás (CAPEX)	Éves költség (OPEX)	Hatás
V1	Szünetmentes táp	5 000 000.- HUF	50 000.- HUF	
V2	Áramfejlesztő	10 000 000.- HUF	200 000.- HUF	
V3	Poroltók	1 000 000.- HUF	200 000.- HUF	
V4	Duplikálás	5 000 000.- HUF	200 000.- HUF	
V5	Hibatűrő rendszer	30 000 000.- HUF	2 000 000.- HUF	
V6	Biztonsági mentések	2 000 000.- HUF	2 000 000.- HUF	
V7	Riasztórendszer	20 000 000.- HUF	2 000 000.- HUF	
V8	Biztonsági őrség	2 000 000.- HUF	30 000 000.- HUF	
V9	Biztosítás	0	10 000 000.- HUF	
V10	Adatkommunikáció titkosítása	2 000 000.- HUF	0	
V11	Hozzáférés-védelem	500 000.- HUF	0	
V12	Digitális aláírás	500 000.- HUF	0	
V13	Vírusvédelem	500 000.- HUF	200 000.- HUF	

10. JAVASOLT VÉDELMI INTÉZKEDÉSEK MEGHATÁROZÁSA – PÉLDA

V = Védelmi intézkedés

ID	Védelmi intézkedés	Beruházás (CAPEX)	Éves költség (OPEX) X 3	Hatás
V3	**Poroltók**	1 000 000.- HUF	600 000.- HUF	**T1-DD, T1-PP**
V6	**Biztonsági mentések**	2 000 000.- HUF	6 000 000.- HUF	**F3-D, L5-D**
V7	**Riasztórendszer**	20 000 000.- HUF	6 000 000.- HUF	**H1-DD, H1-P**
V11	**Hozzáférés-védelem**	500 000.- HUF	0	**L2-P, L4-P**
V13	**Vírusvédelem**	500 000.- HUF	600 000.- HUF	**L5-PP, L5-D**

AJÁNLÁSOK

ITB	IBK	COBIT, CC

ITB

Hazai legfontosabb ajánlások egyike

- Informatikai Tárcaközi Bizottság 8. sz. Ajánlása
- Ajánlás az IBK elkészítéséhez
- Felsorol sok kockázatot, mint fenyegetettség
- Kockázat = Valószínűség x Okozott kár
- Felsorol biztonsági intézkedéseket is
- Megadja, hogy mely intézkedés mely fenyegetésre van hatással
- Segít meghatározni az elviselhetetlen kockázatokat
  - Gyakoriság és Károk 0-4 pontozás (4 legmagasabb)
  - 2 szám összege >= 5 vagy szorzatuk > 4

IBK

Informatikai Biztonsági Koncepció

Tartalmazza:

- Az adott szervezet informatikai biztonságának követelményeit,
- Az informatikai biztonság megteremtése érdekében szükséges intézkedéseket,
- Ezek kölcsönhatásait és következményeit

Fő tartalmi összetevői:

- A védelmi igény leírása (meglévő állapot, fenyegetettségek, fennálló kockázatok),
- Az intézkedések fő irányai (kockázat-menedzselés),
- A feladatok és felelősségek megosztása (az intézkedések megvalósítása során),
- Időterv (megvalósítási ütemekre és az IBK felülvizsgálatára).

EU ELLÁTÁSI LÁNC

NIS2 | CER | ZERO TRUST

MILTON FRIEDMAN EGYETEM

KÖSZÖNÖM A FIGYELMET!

4. óra - Kockázatmenedzsment

2024.04.05

Szalai Patrik

szalai.patrik@uni-milton.hu