NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

Egy előadás margójára: azaz Digitális Mohács 2.0. a szakértők véleménye szerint

Kovács László – Krasznay Csaba

Nemzeti Közszolgálati Egyetem
Kiberbiztonsági Kutatóműhely

NEMZETI
KÖZSZOLGÁLATI
EGYETEM
A HAZA SZOLGÁLATÁBAN

Digitális Mohács 2.0

Kérdőíves felmérés eredményei

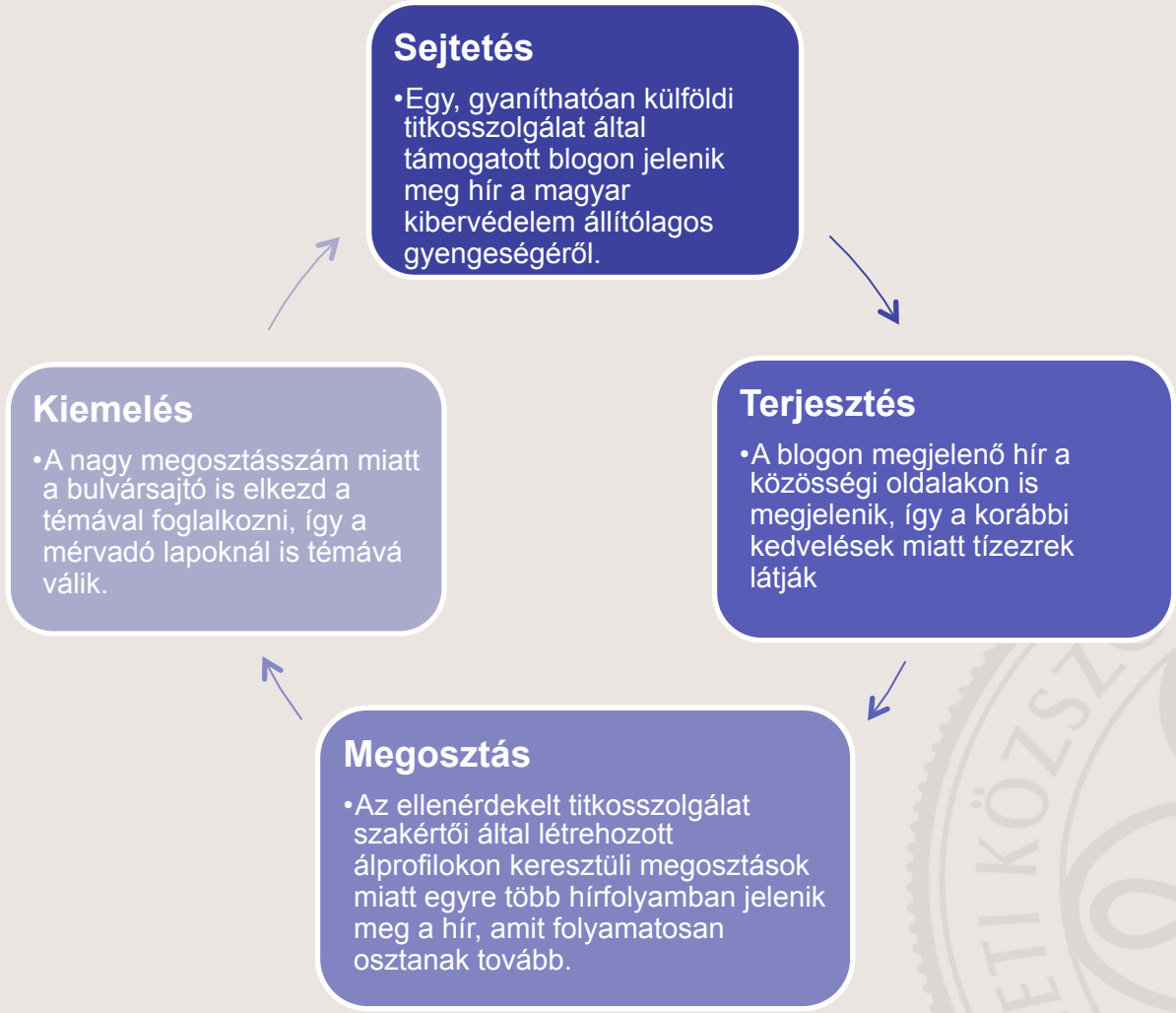
NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

Digitális Mohács 2.0 forgatókönyv

- 2016 szeptemberében a Hétpecsét szakmai fórumán került bemutatásra a Digitális Mohács 2.0 előadásunk.
- A felvázolt forgatókönyv az ún. Tabletop Exercise (TTX) mintáját követte.
- A forgatókönyvben egy, napjainkban teljesen elképzelhető eszkalációs folyamatot mutattunk be.
- Nem tértünk ki arra, hogy milyen stratégiai cél érdekében történnek a támadások, valamint nem foglalkoztunk a lehetséges védelmi műveletekkel.
- De kíváncsiak voltunk, **Önök mit gondolnak, mit reagálnának!**
- Ezért kértük, hogy az előre kiadott űrlapon jelezzék válaszaikat.
- Az előadást követően 70 kitöltött kérdőívet kaptunk vissza.
- Jelen előadás a kapott válaszokat elemzi röviden. A mélyebb tudományos elemzést tudományos cikkben fogjuk hamarosan publikálni.

NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

Digitális Mohács 2.0 forgatókönyv
1. felvonás: Pszichológiai műveletek



NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

Digitális Mohács 2.0 forgatókönyv
2. felvonás: Látványos támadások

DDoS támadások

Bizonyos kormányzati weboldalak és az NTG ellen túlterheléses támadások indulnak, mely miatt egyes szolgáltatások órákra elérhetetlenné válnak.

Defacement támadások

Egyes önkormányzati és háttérintézményi weboldalakat feltörnek, a kezdőlapokon Magyarországot fenyegető üzenetek jelennek meg.

Tömeges adatszivárgás

Olyan adatbázisok jelennek meg az interneten, melyek állításuk szerint több tízezer magyar állampolgár személyes adatait tartalmazzák.

NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

Digitális Mohács 2.0 forgatókönyv
3. felvonás: A politika befolyásolása

Wikileaks szivárogtatás

- Kormányzati e-mailek kerülnek napvilágra
- #HunLeaks címmel a nemzetközi sajtó is elkezdi ezeket elemezni

A „magyar Snowden”

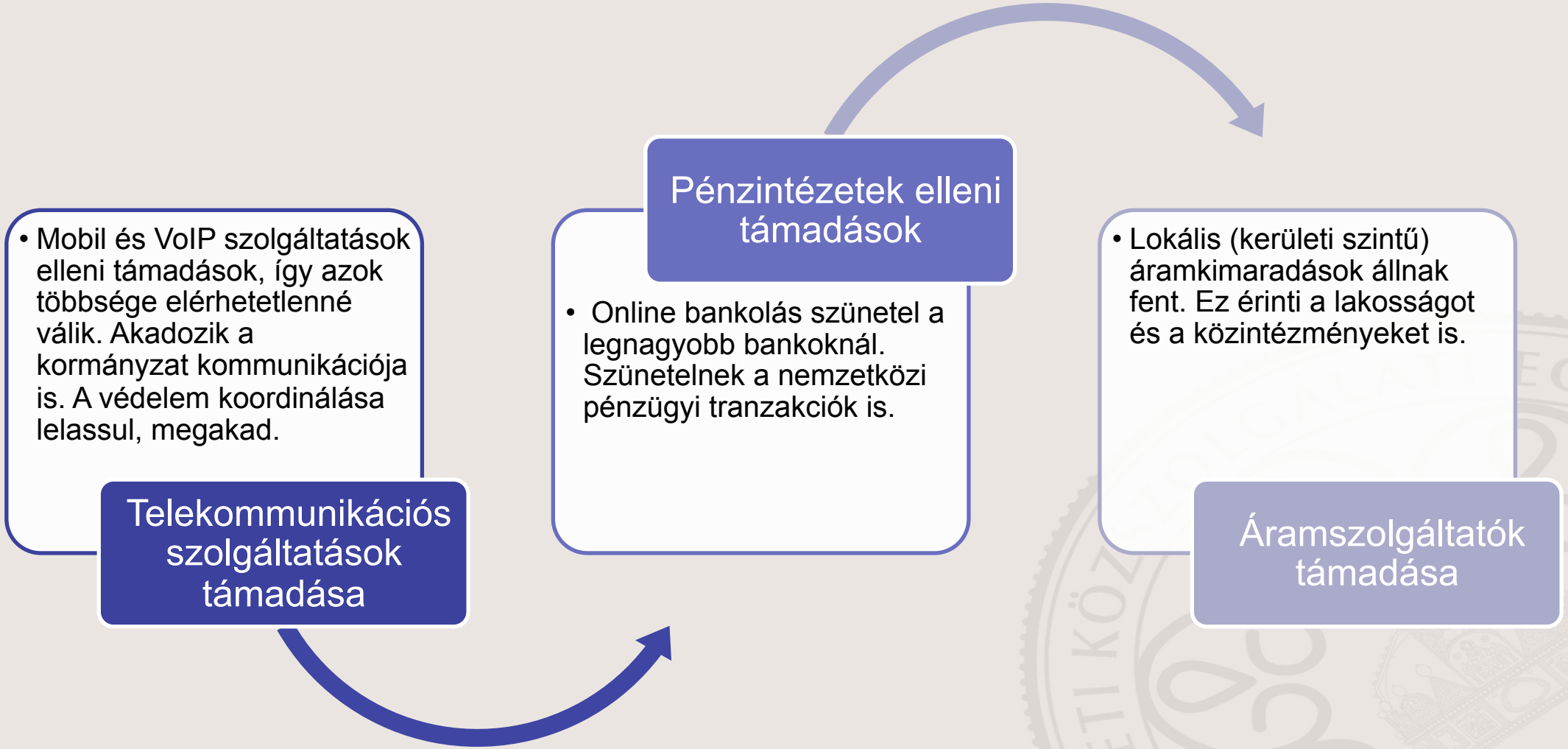
- Egy szivárogtató jelentős mennyiségű minősített iratot ad át egy oknyomozó újságírónak
- Ezt a csomagot egy nemzetközi újságírócsapat elemzi

APT egy létfontosságú rendszerelemnél

- A korábbi támadások hatására elrendelt vizsgálat egy kifinomult malware-t talál egy közműszolgáltatónál
- A malware célja adatszerzés
- A vizsgálat szerint legalább 2 éve fut

NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

Digitális Mohács 2.0 forgatókönyv
4. felvonás: Infrastruktúra támadások

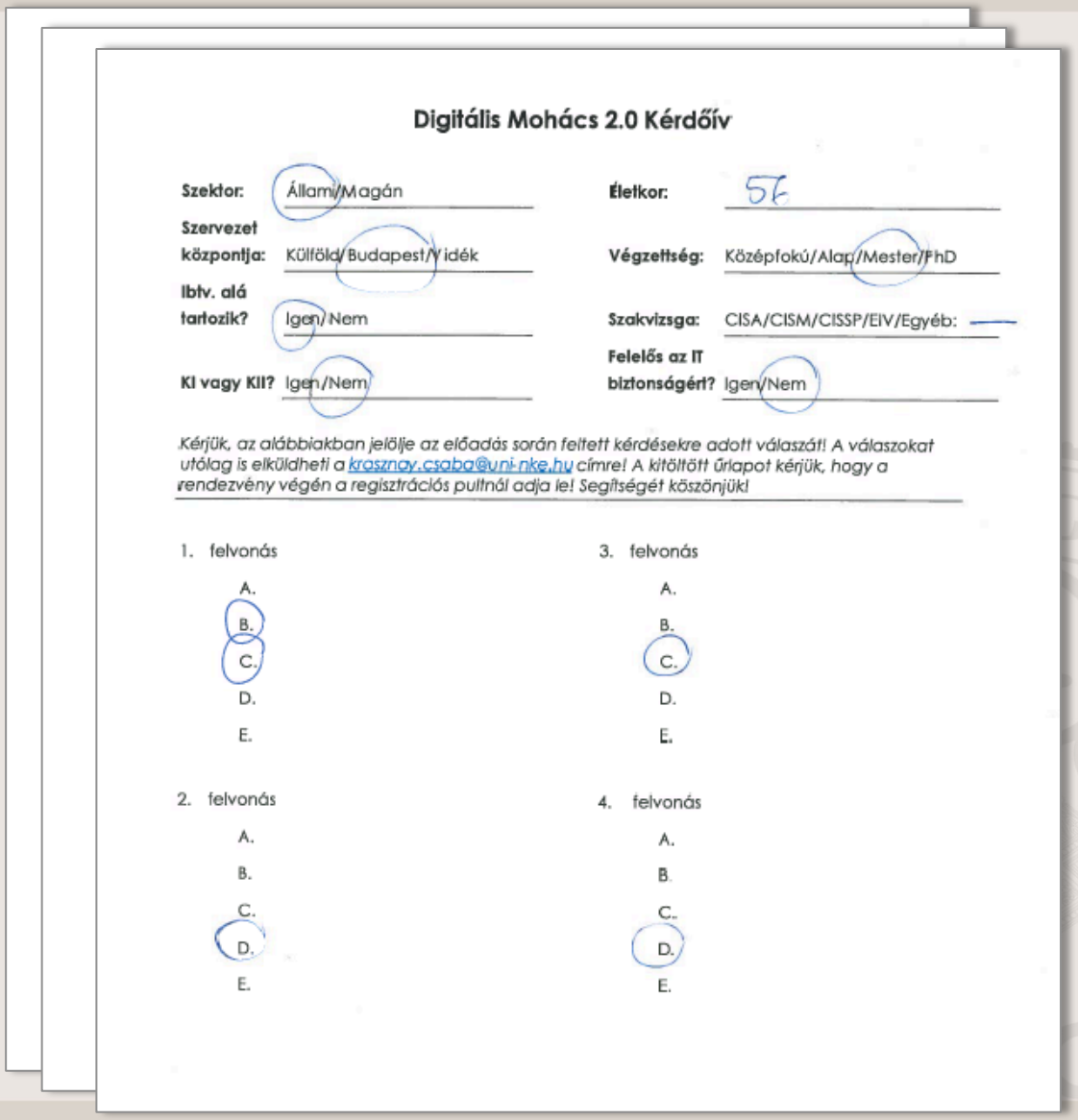


A kérdőíves felmérés eredményei

NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

A kérdőíves felmérés

- **70 kitöltött és visszajuttatott kérdőív**
- **kérdőívenkénti adatok:**
  - Szektor: magán/állami
  - Ibtv. alá tartozik: Igen/Nem
  - Életkor
  - Végzettség
  - Szakvizsga
  - IT felelős: Igen/Nem
  - 4 felvonás: a, b, c, d, egyéb válasz lehetőség



Digitális Mohács 2.0 Kérdőív

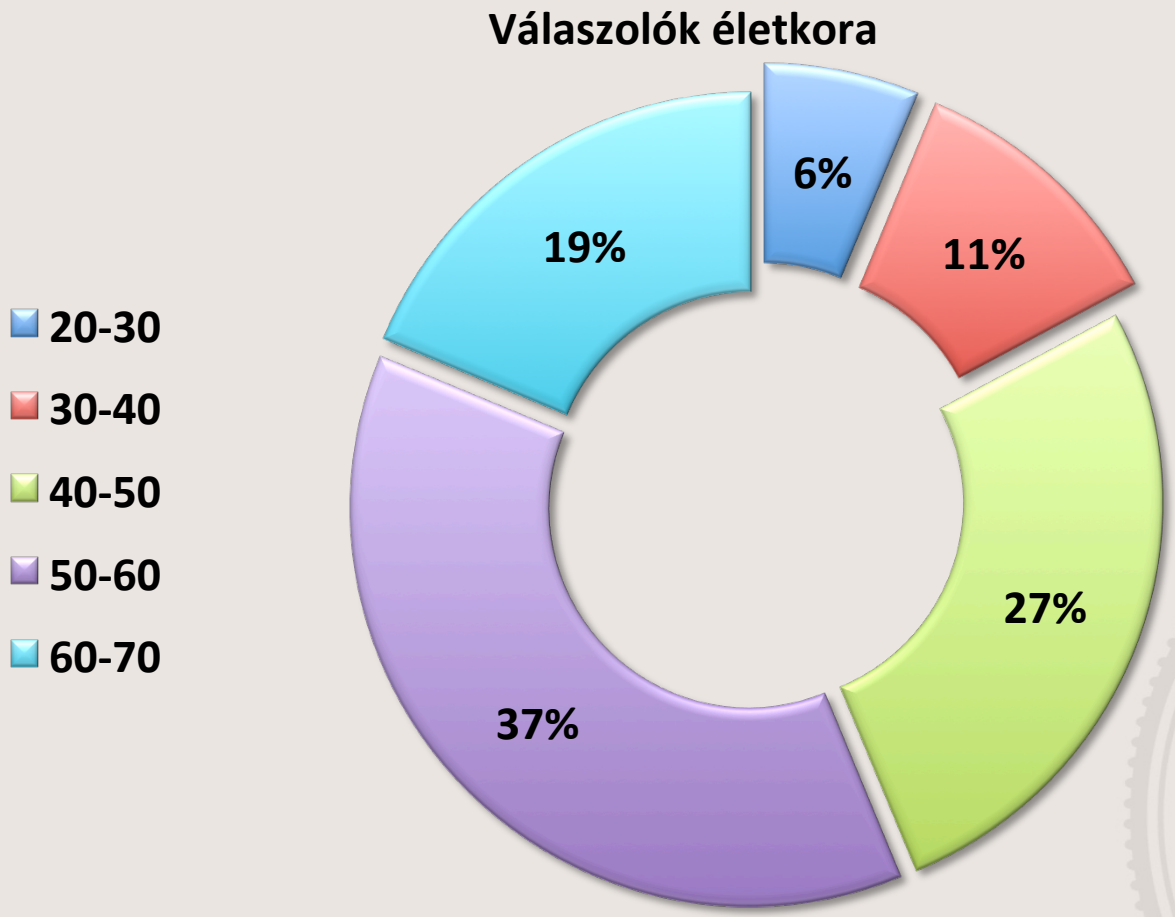
Szektor: Állami/Magán
Életkor: 57
Szervezet központja: Külföld/Budapest/Vidék
Végzettség: Középfokú/Alap/Mester/PhD
Ibtv. alá tartozik? Igen/Nem
Szakvizsga: CISA/CISM/CISSP/EIV/Egyéb: —
KI vagy KII? Igen/Nem
Felelős az IT biztonságért? Igen/Nem

Kérjük, az alábbiakban jelölje az előadás során feltett kérdésekre adott válaszát! A válaszokat utólag is elküldheti a krasznay.csaba@uni-nke.hu címre! A kitöltött űrlapot kérjük, hogy a rendezvény végén a regisztrációs pultnál adja le! Segítségét köszönjük!

1. felvonás: A. B. C. D. E.
2. felvonás: A. B. C. D. E.
3. felvonás: A. B. C. D. E.
4. felvonás: A. B. C. D. E.

NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

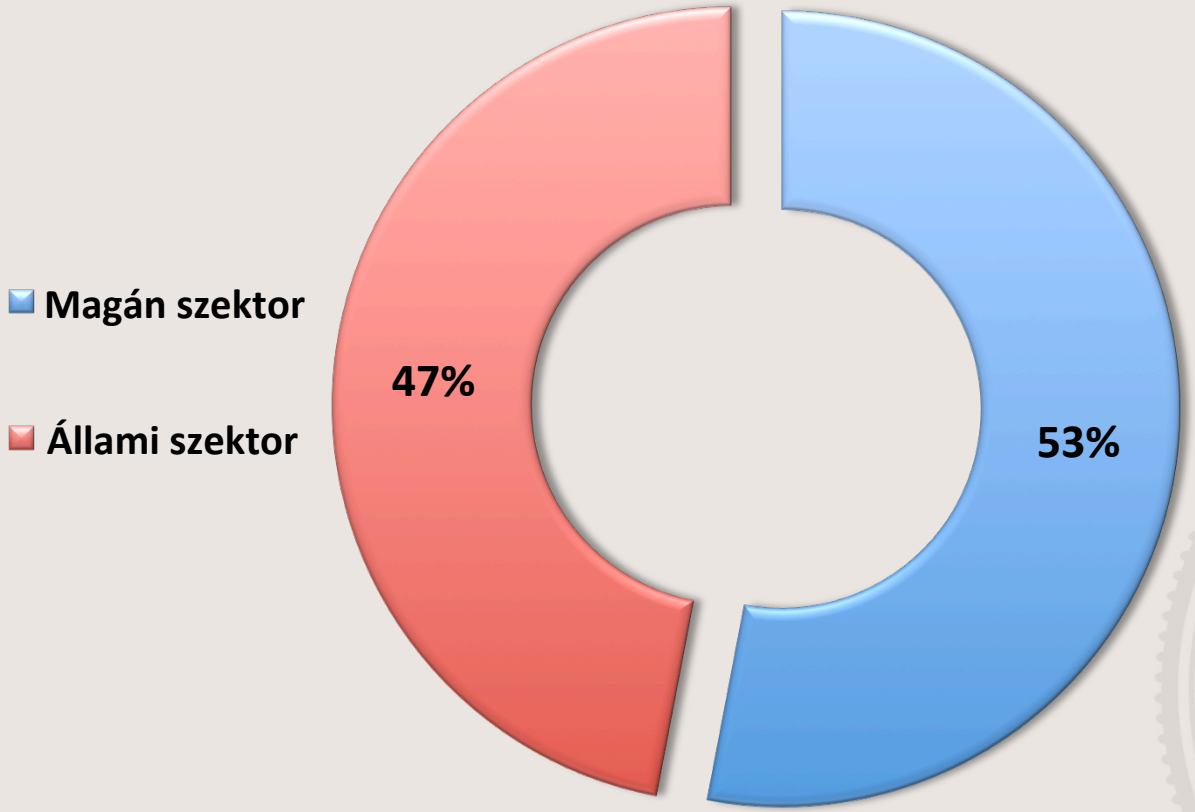
A kérdőíves felmérés



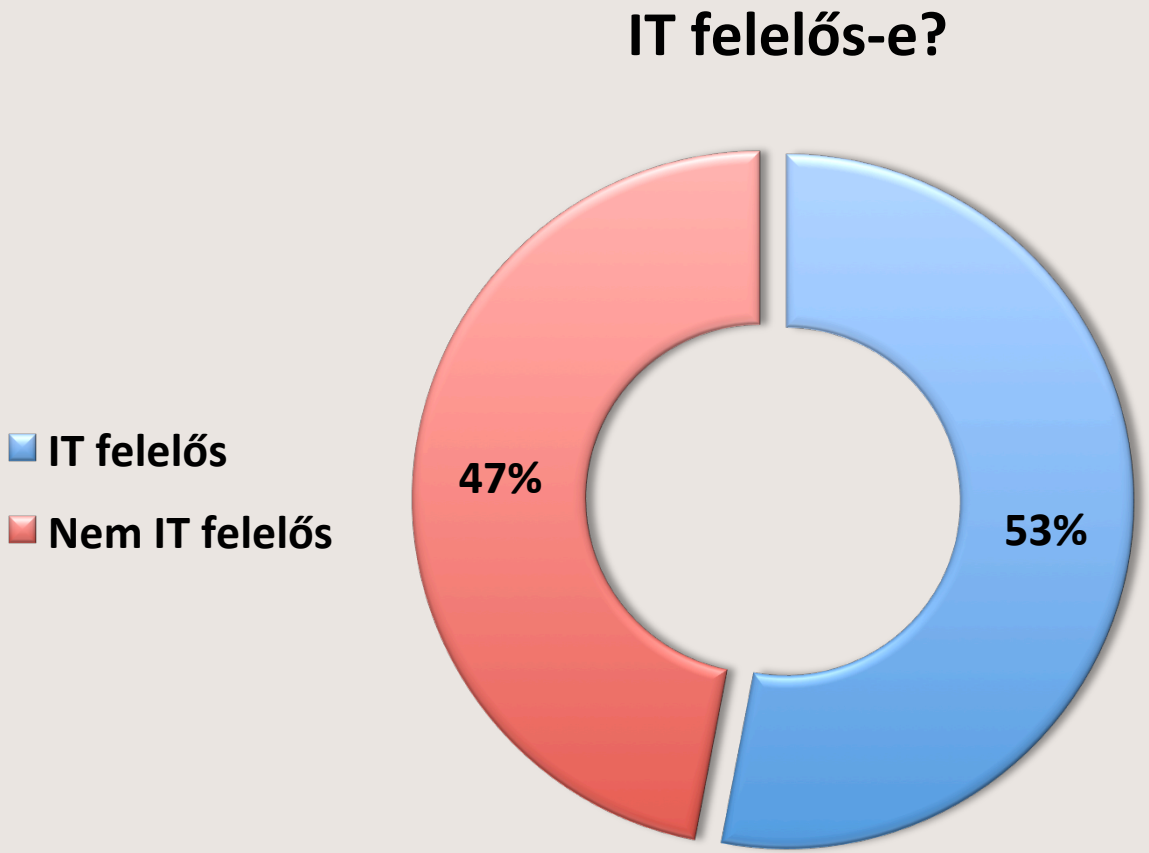
NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

A kérdőíves felmérés

Válaszadók szektor szerinti eloszlása

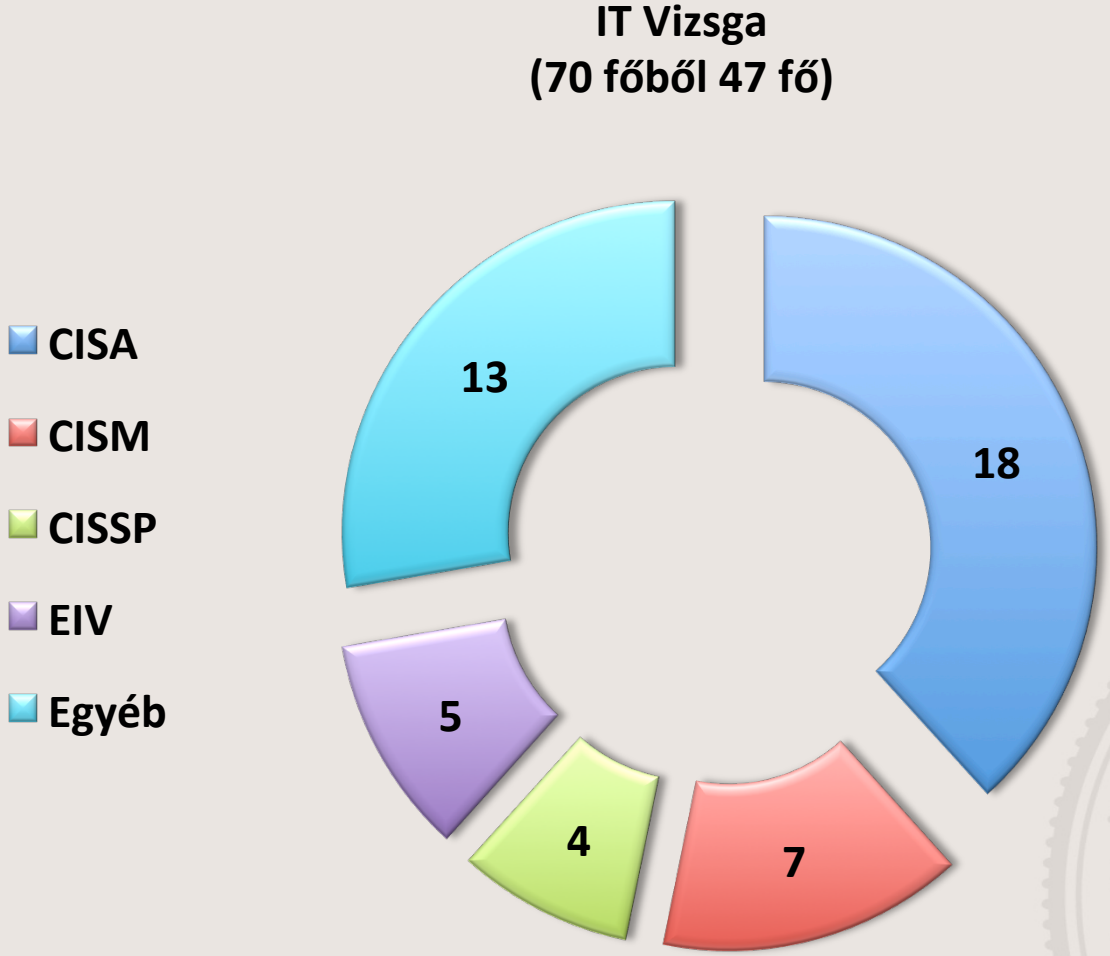


A kérdőíves felmérés



NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

A kérdőíves felmérés



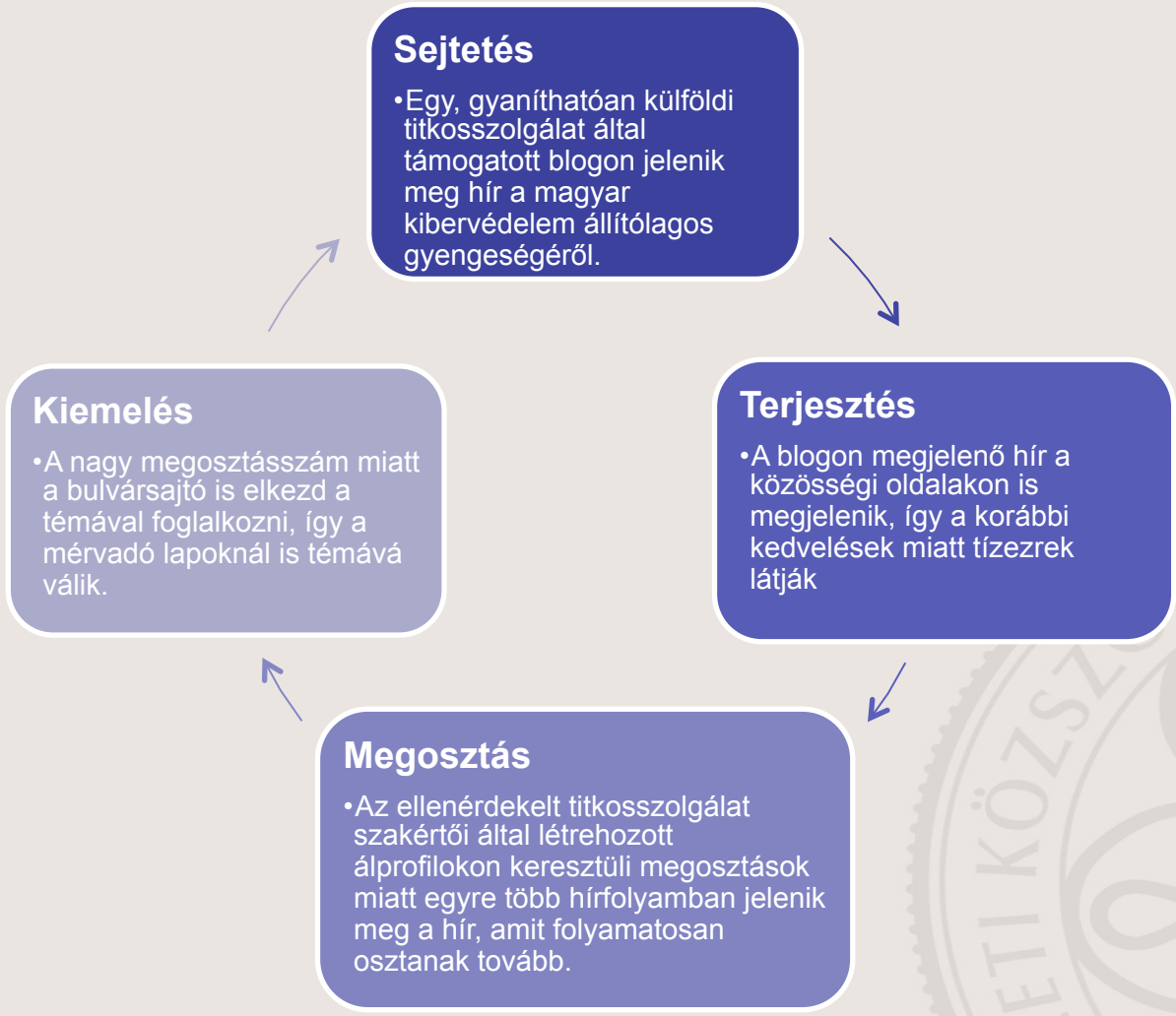
NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

A kérdőíves felmérés

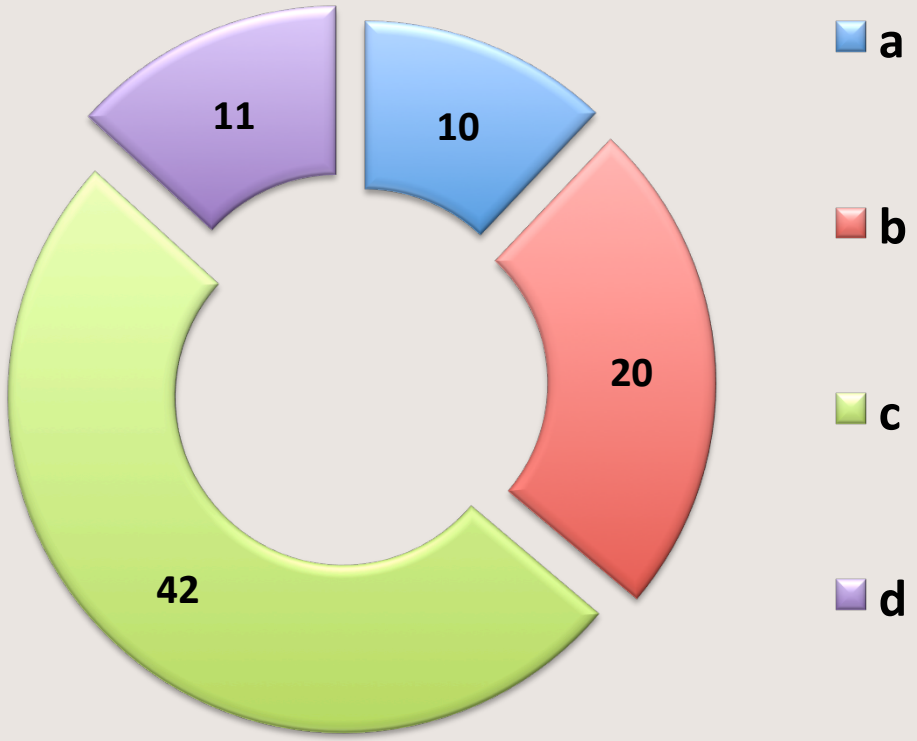
ÖN MIT TENNE?

NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

1. felvonás: Pszichológiai műveletek



Ön mit tenne?



A) Ilyen mendemondákkal nem kell törődni, semmilyen válaszlépést nem tennék.

B) A kormánnyal szimpatizáló blogokon és internetezőkön keresztül hasonló módszerekkel élő ellenkampányba kezdenék.

C) A Nemzeti Kibervédelmi Intézet nevében kiadnék egy közleményt, melyben cáfolnám az állításokat.

D) A Magyar Kormány nevében cáfolnám a híresztelést, egyben diplomáciai úton jelezném a gyanús nagyhatalom felé ellenérzéseimet.

NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

2. felvonás: Látványos támadások

DDoS támadások

Bizonyos kormányzati weboldalak és az NTG ellen túlterheléses támadások indulnak, mely miatt egyes szolgáltatások órákra elérhetetlenné válnak.

Defacement támadások

Egyes önkormányzati és háttérintézményi weboldalakat feltörnek, a kezdőlapokon Magyarországot fenyegető üzenetek jelennek meg.

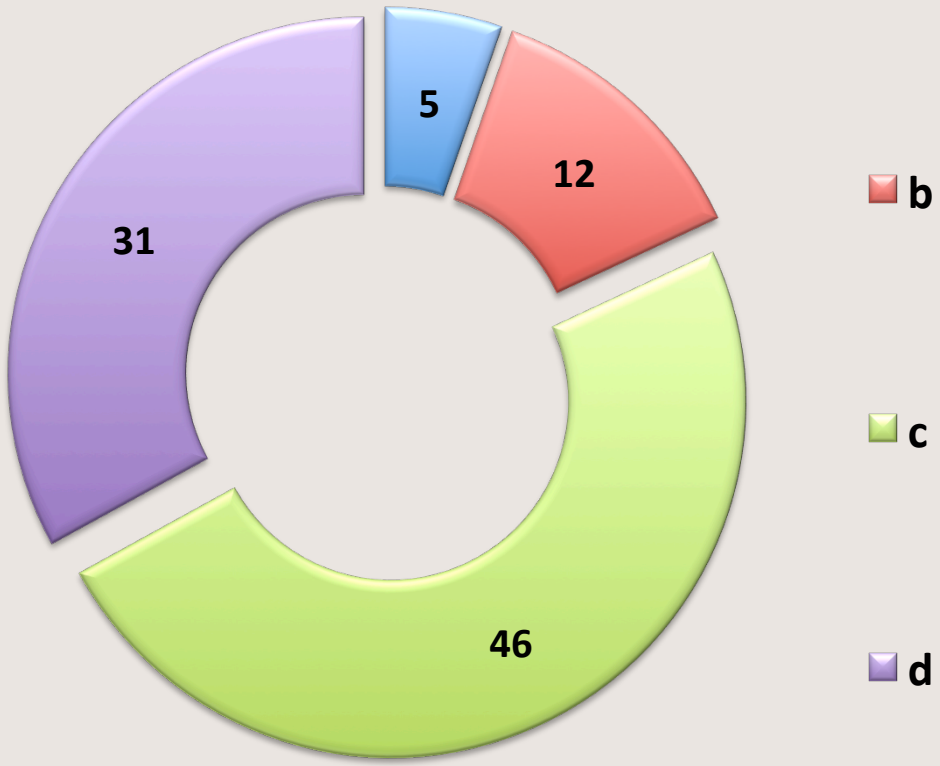
Tömeges adatszivárgás

Olyan adatbázisok jelennek meg az interneten, melyek állításuk szerint több tízezer magyar állampolgár személyes adatait tartalmazzák.

NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

Ön mit tenne?

2. Felvonás: Látványos támadások



A) Ezek jelentéktelen támadások, hatásuk ideiglenes, így semmilyen különleges intézkedést nem hoznék. A sajtóval nem foglalkoznék.

B) Decentralizáltan, a támadások által érintett szervezetekre fókuszálva elkezdeném az elhárító munkálatokat. A sajtót az érintett szervezetek kezelik.

C) A Nemzeti Kibervédelmi Intézet vezetésével végezném az elhárítást, egyben bizonyos műszaki intézkedések mentén kiterjedtebben kezdenék el a további potenciális támadásokra figyelni. A sajtót az NKI kezeli.

D) Összehívnám a Nemzetbiztonsági Kabinetet, ahol egy műveleti törzset állítanék fel, így a műszaki intézkedések mellett egyéb hírszerzési és belbiztonsági tevékenység folytatása is lehetővé válik. A sajtót a kormányszóvivőre bíznám, egyben megnevezném a gyanítható elkövető országot.

NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

3. felvonás: A politika befolyásolása

Wikileaks szivárogtatás

- Kormányzati e-mailek kerülnek napvilágra
- #HunLeaks címmel a nemzetközi sajtó is elkezdi ezeket elemezni

A „magyar Snowden”

- Egy szivárogtató jelentős mennyiségű minősített iratot ad át egy oknyomozó újságírónak
- Ezt a csomagot egy nemzetközi újságírócsapat elemzi

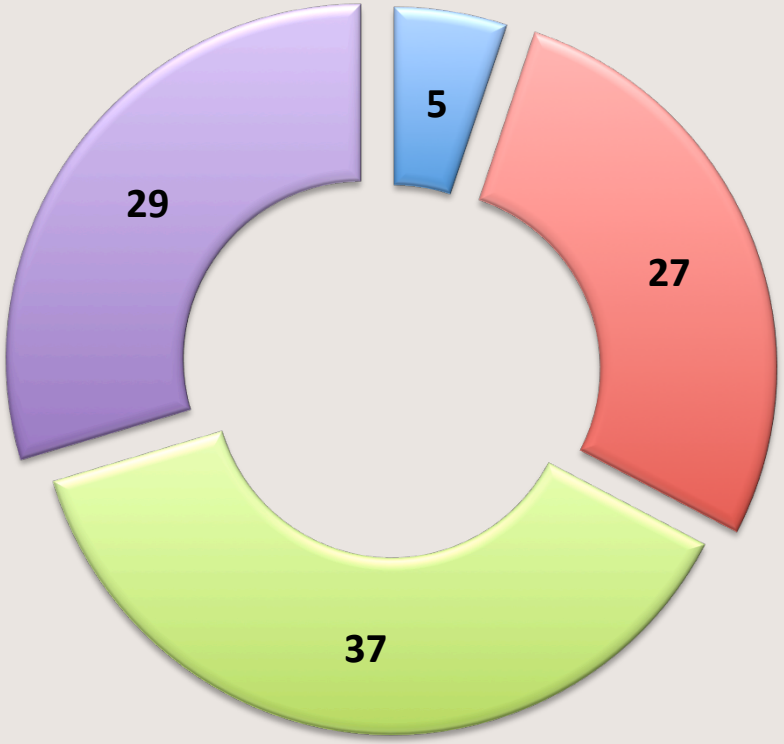
APT egy létfontosságú rendszerelemnél

- A korábbi támadások hatására elrendelt vizsgálat egy kifinomult malware-t talál egy közműszolgáltatónál
- A malware célja adatszerzés
- A vizsgálat szerint legalább 2 éve fut

NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

Ön mit tenne?

3. Felvonás: A politika befolyásolása



A) Mivel az incidensek valószínűleg egymástól függetlenek, egyedi, testreszabott választ adnék rájuk.

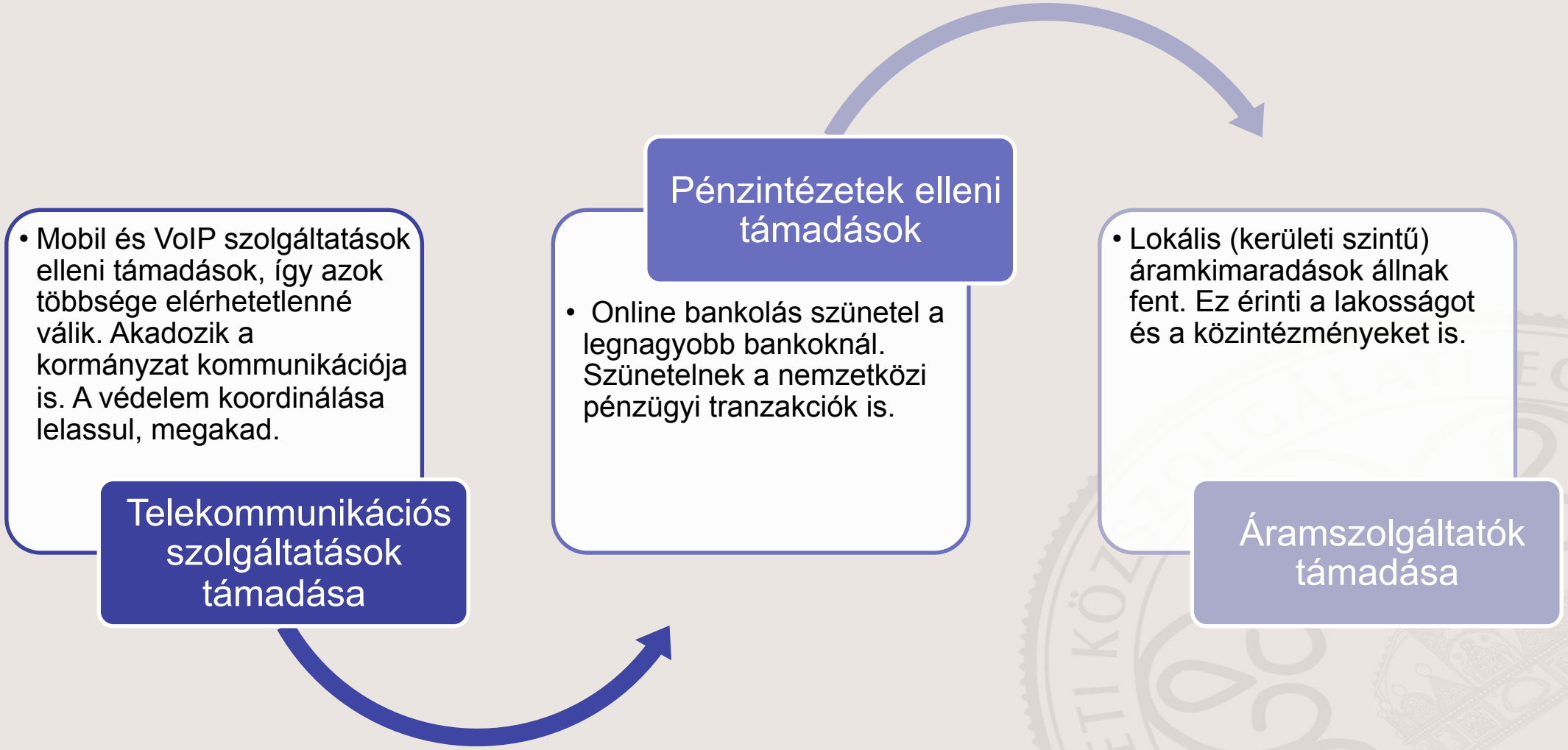
B) Az esetek valószínűleg összefüggnek, titkosszolgálati tevékenységgel próbálnám megoldani a kialakult helyzetet. A sajtó kezelését a szakértőkre és az NKI-ra bíznám.

C) Mivel az esetek egyértelműen összefüggnek, a Nemzetbiztonsági Kabineten belül működő operatív törzs hangolja össze a válaszlépéseket. A sajtóban nevesíteném az elkövető államot.

D) Mivel jelen támadássorozat aláássa Magyarország biztonságát, az Európai Unió és a NATO diplomáciai és szakértői segítségét kérném!

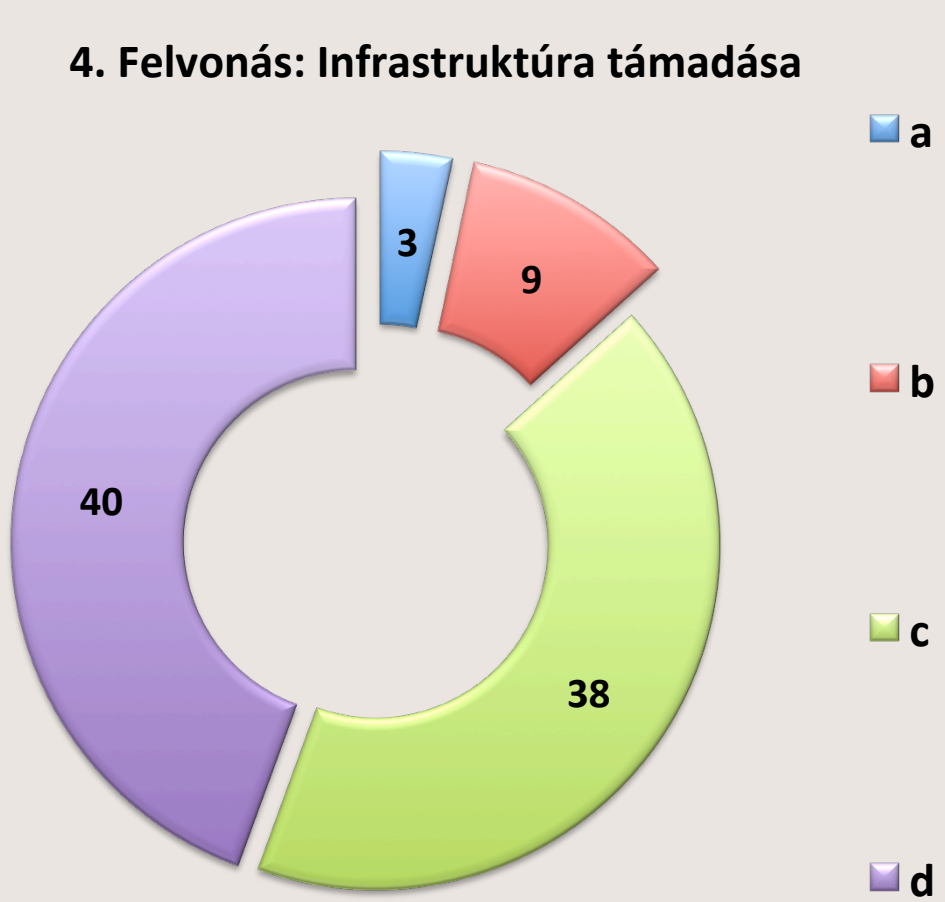
NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

4. felvonás: Infrastruktúra támadások



NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

Ön mit tenne?



A) Ezek elszigetelt támadások, de lehet hogy csak a rendszerek egymástól független, véletlen meghibásodásai, hatásuk ideiglenes és csak korlátozott lehet, így semmilyen különleges intézkedést nem hoznék.

B) Decentralizáltan, a támadások által érintett szervezetekre fókuszálva elkezdeném az elhárító munkálatokat és a szolgáltatások minimális szintű visszaállítását. A sajtót az érintett szervezetek kezelik.

C) Mivel egyértelmű, hogy a korábban talált malware-hez kapcsolódó célzott támadásokat látunk, a Nemzeti Kibervédelmi Intézet vezetésével végezném az elhárítást, egyben bizonyos műszaki intézkedések mentén kiterjedtebben kezdenék el a további potenciális támadásokra figyelni. A sajtót az NKI kezeli.

D) A Nemzetbiztonsági Kabineten belül működő műveleti törzs kezelné a helyzetet, így a műszaki intézkedések mellett egyéb hírszerzési és belbiztonsági tevékenység folytatása is lehetővé válik. A sajtót a kormányszóvivőre bíznám. EU és NATO segítséget kérnék diplomáciai és szakértői szinten.

NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

Ön mit tenne?

Szöveges válaszadási lehetőséget is biztosítottunk mind a 4 felvonásban. Számos szakmailag nagyon fontos választ kaptunk. Ugyanakkor, volt néhány feszültségoldó válasz is:

„Beküldeném Krasznayt az m1-be ☺”

„Nem szolgált az előadás némi propaganda célt, hogy népszerűsítse a központi kibervédelmet, mint egyedüli üdvözítő megoldást?”

Következtetések

- A forgatókönyvben szereplő támadások reálisak, potenciálisan bekövetkezhetnek.
- A felvázolt forgatókönyvben szereplő támadások intenzitásával növekszik a szakemberek igénye a központi (állami) incidenskezelésre.
- A különböző támadások kezelésében a szakma a Nemzeti Kibervédelmi Intézetet kiemelt jelentőségűnek látja.

NEMZETI
KÖZSZOLGÁLATI
EGYETEM
A HAZA SZOLGÁLATÁBAN

Prof. Dr. Kovács László kovacs.laszlo@uni-nke.hu
Dr. Krasznay Csaba krasznay.csaba@uni-nke.hu

KÖSZÖNJÜK SEGÍTSÉGÜKET ÉS FIGYELMÜKET!