MINDEN KIBERÜL

#podcast

SZTFH

Szabályozott Tevékenységek
Felügyeleti Hatósága

Fáj vagy nem fáj, és ha nem, akkor miért nagyon?

Avagy szabályozással egy biztonságosabb kibertérért

Bor Olivér

kiberbiztonsági és kommunikációs szakértő

egyetemi vendégoktató

SZTFH

Szabályozott Tevékenységek
Felügyeleti Hatósága

Szabályozott Tevékenységek Felügyeleti Hatósága

Stabil, kiszámítható működési és szabályozási környezet biztosítása a kiemelt ágazatok számára

2021. október 1-től:

- Szerencsejáték Felügyelet,
- Nemzeti Dohánykereskedelmi Nonprofit Zrt.,
- Felszámolók Névjegyzékét Vezető Hatóság,
- IM Bírósági végrehajtói felügyelet.

2022. január 1-től:

- Magyar Bányászati és Földtani Szolgálat, Kormányhivatalok bányakapitányságai
- Kiberbiztonsági feladatok

Szabályozott Tevékenységek Felügyeleti Hatósága

milliárd forint 2000

Az iparági szereplők éves szinten több mint 2000 milliárd forintos árbevételt realizálnak.

ezer ember 50

Az ágazati szereplők mintegy 50 ezer főnek kínálnak munkahelyet.

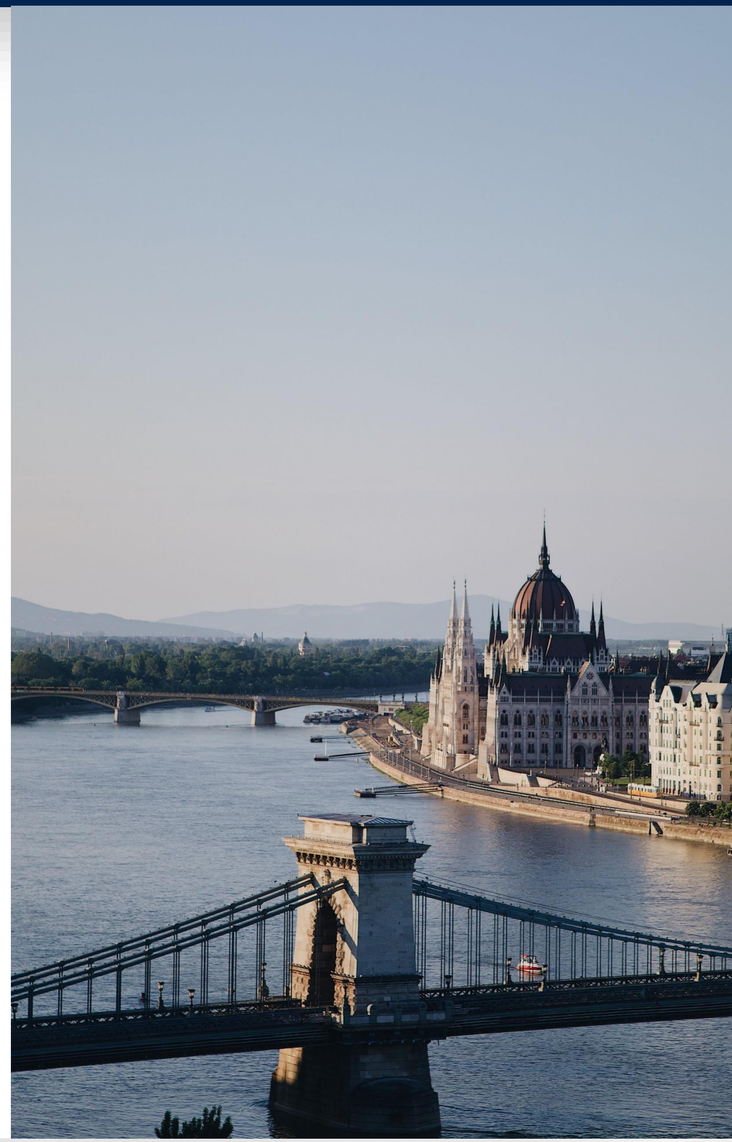
ezer család 150

Az ágazatok közvetve és közvetetten 100-150 ezer ember megélhetését biztosítják.

milliárd forint 700

A felügyelt tevékenységekből évi 700 milliárd forint adó és járulékbevétel származik.

Kiemelkedő jelentőség és felelősség, hatékony hatósági mozgástérrel párosítva



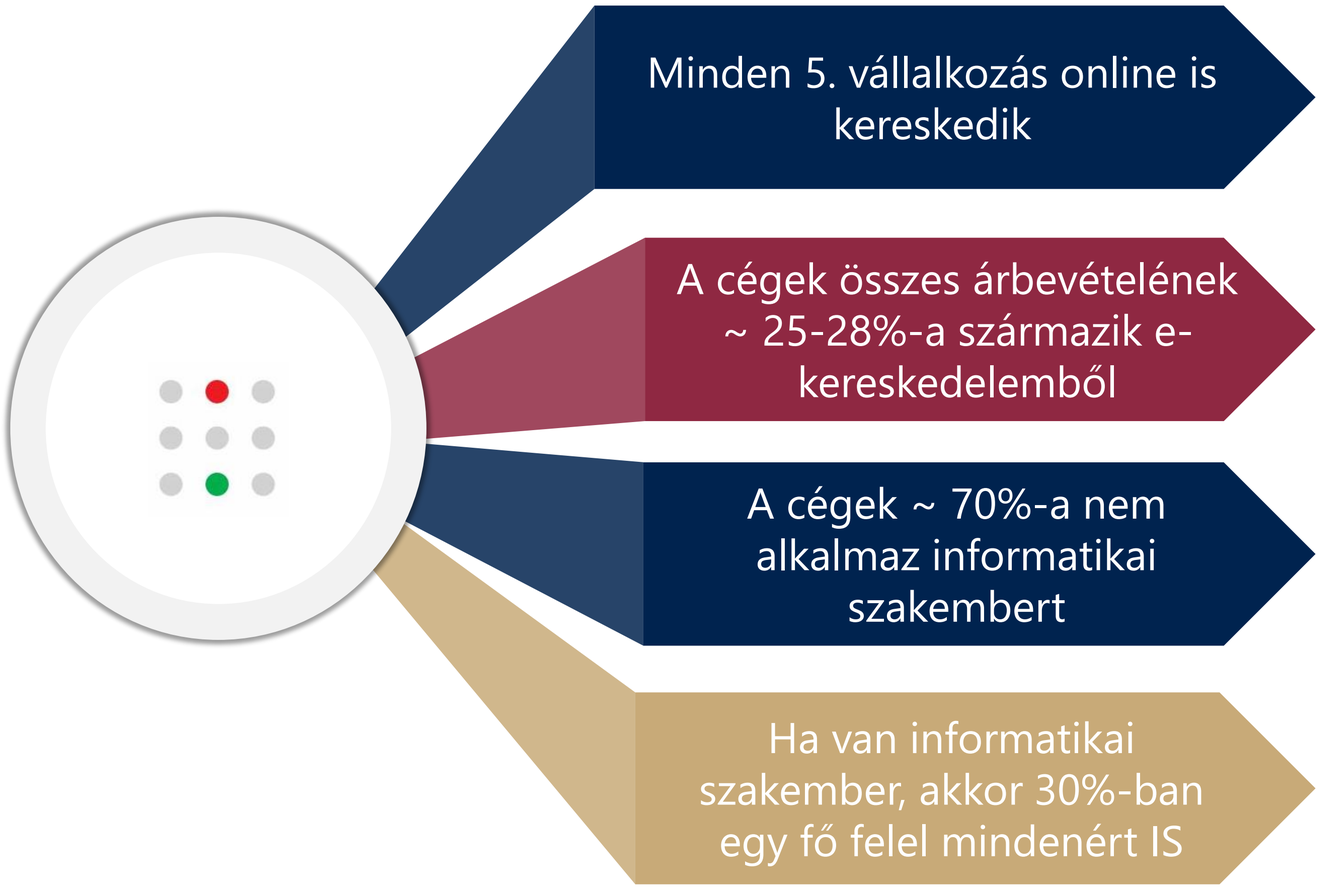
Két féle szervezet…

2012 **ROBERT MUELLER, FBI**

There are only two types of companies:
those that **have been hacked**,
and those that **will be**.

Vállalati digitalizáció Magyarországon

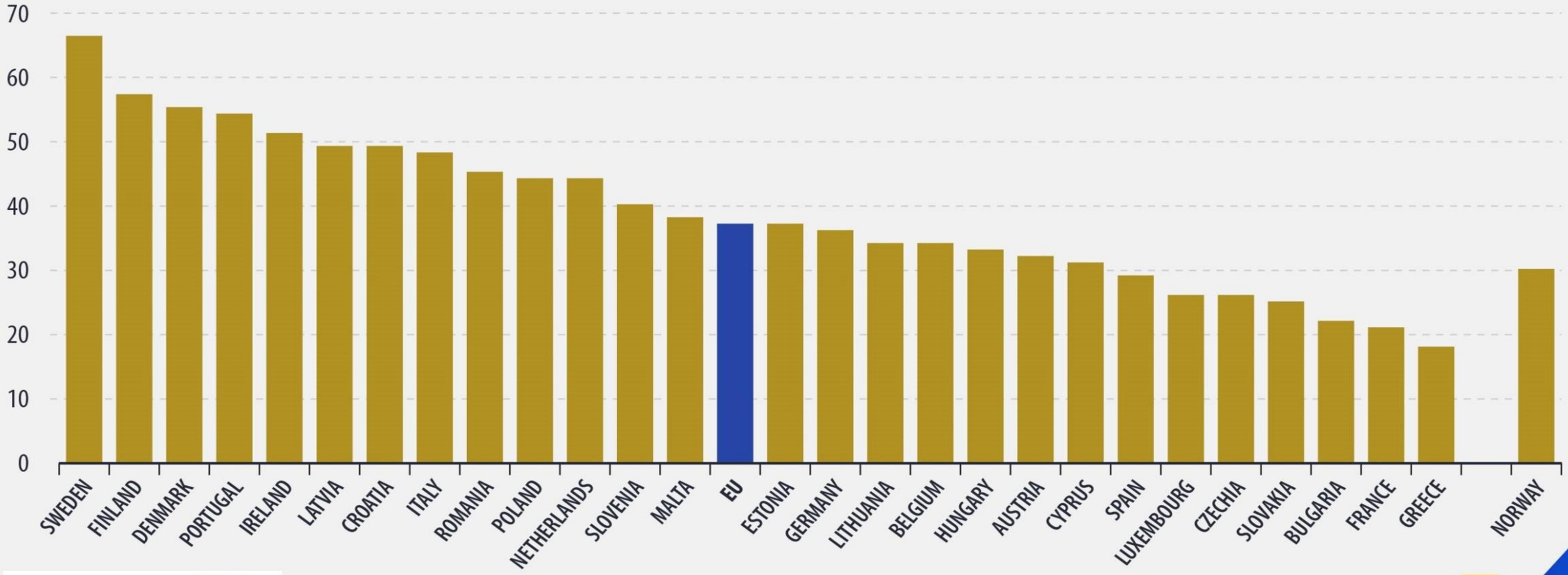
A hazai cégek ~70%-a rendelkezik saját weboldallal



Ne legyenek magányos hősök!

Vállalatok biztonsági felkészültsége

VÁLLALATI IKT BIZTONSÁGRA VONATKOZÓ INTÉZKEDÉSI CSOMAGOK, ELJÁRÁSRENDEK (%-OS ARÁNY)



eurostat

Milyen biztonságos a rendszerem?

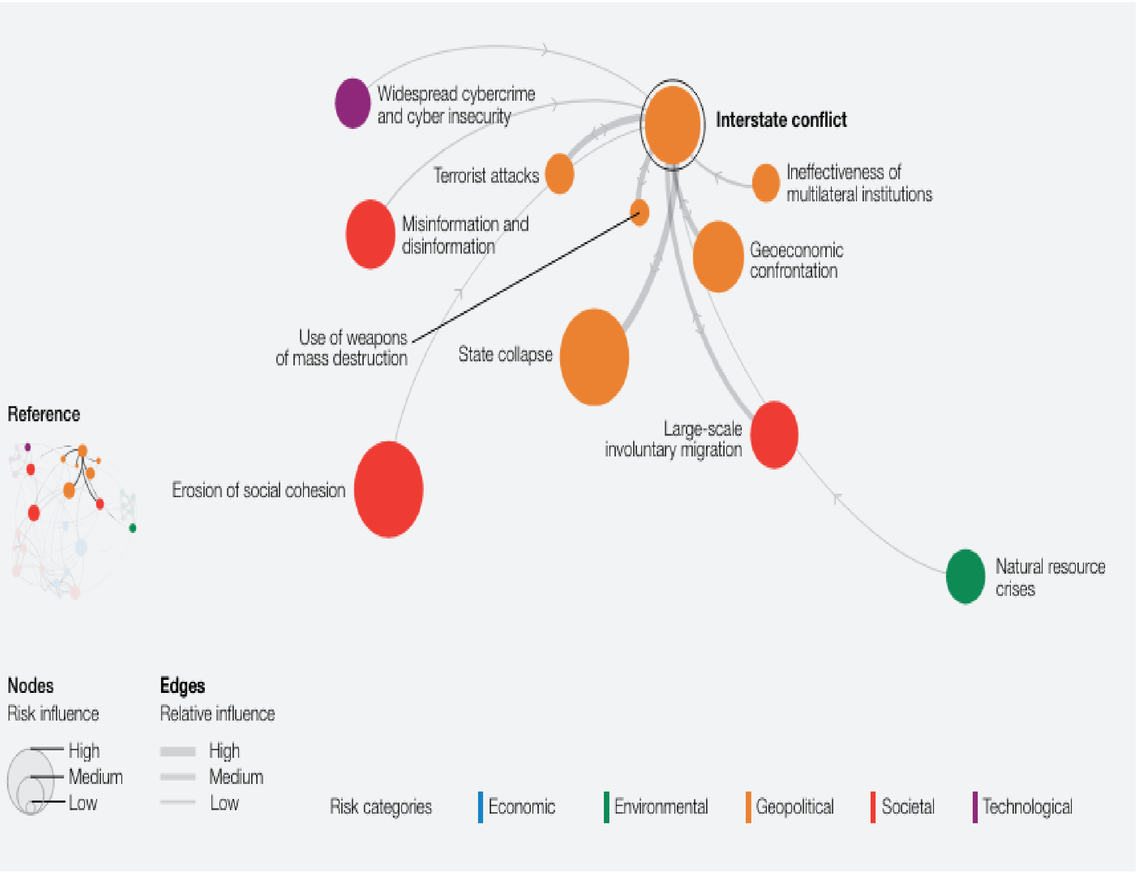
Milyen biztonságos a rendszerem?

VALÓSÁG

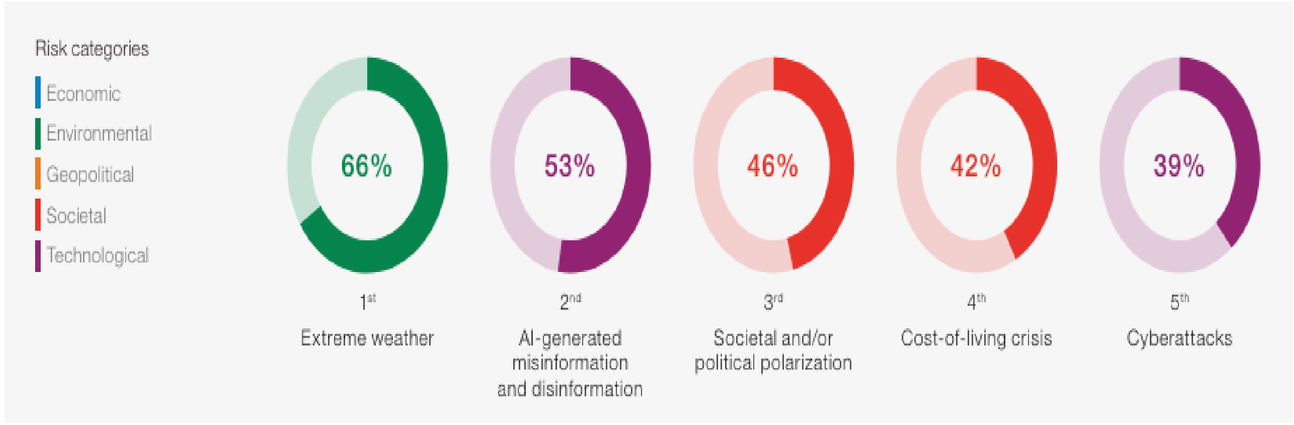
Global Risk Report 2023 (WEF)

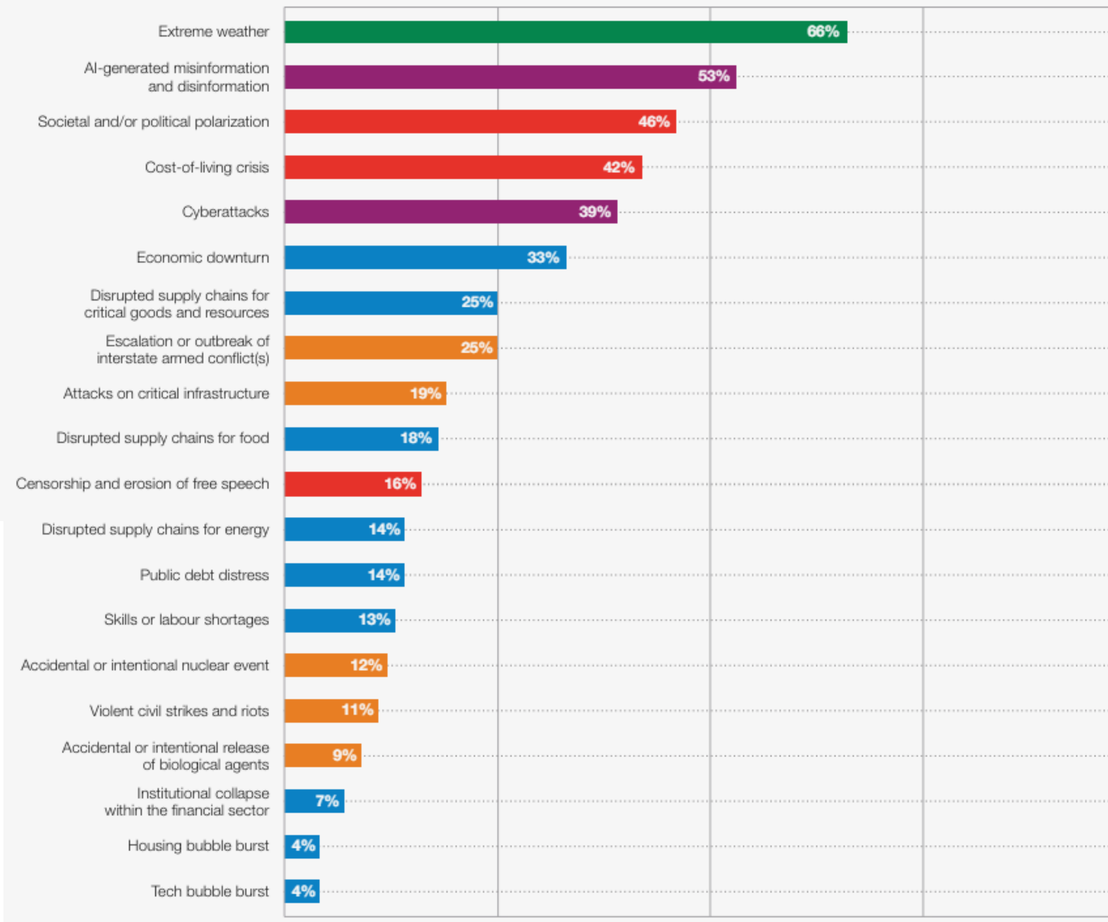
	2 years	10 years
1	Cost-of-living crisis	Failure to mitigate climate change
2	Natural disasters and extreme weather events	Failure of climate-change adaptation
3	Geoeconomic confrontation	Natural disasters and extreme weather events
4	Failure to mitigate climate change	Biodiversity loss and ecosystem collapse
5	Erosion of social cohesion and societal polarization	Large-scale involuntary migration
6	Large-scale environmental damage incidents	Natural resource crises
7	Failure of climate change adaptation	Erosion of social cohesion and societal polarization
8	Widespread cybercrime and cyber insecurity	Widespread cybercrime and cyber insecurity
9	Natural resource crises	Geoeconomic confrontation
10	Large-scale involuntary migration	Large-scale environmental damage incidents

Risk categories: Economic, Environmental, Geopolitical, Societal, Technological



Global Risk Report 2024 (WEF)





Fenyegetések (ENISA 2023-es jelentése alapján)

Ransomware

Az érintett szervezetek ~40%-a fizetett

Internet infrastruktúra elleni támadás

Leállás, aktív cenzúra, forgalomátirányítás

Dezinformáció

Ellátási lánc elleni támadás

2020-ban < 1%, 2021-ben >17%

2022-ben 61%

Malware

Egyre több 0.day, egyre több mobilos kártevő

Social engineering

BEC, Spear-phising, whaling, smishing, vishing

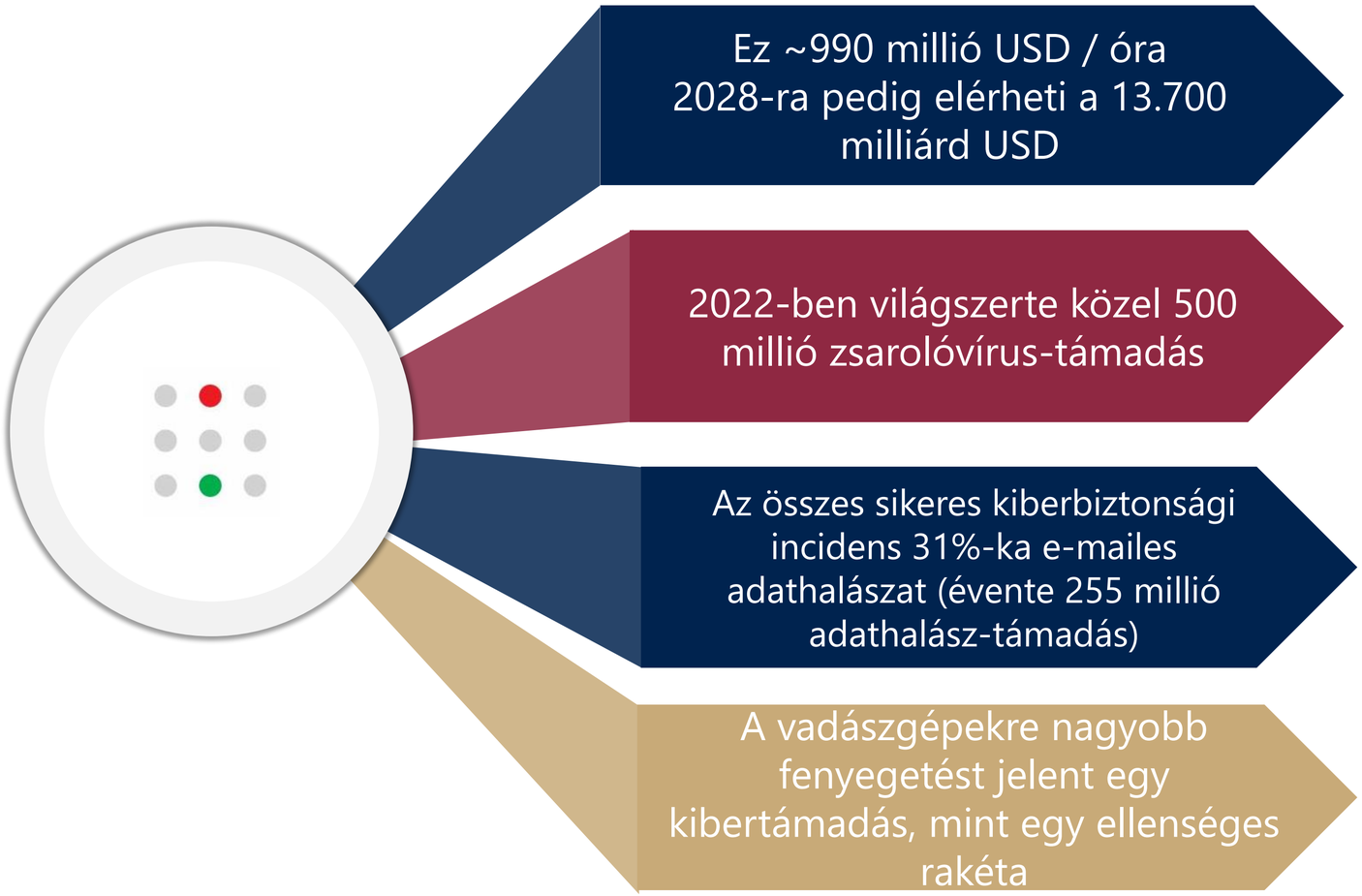
Adatokkal kapcsolatos fenyegetés

Szolgáltatásmegtagadásos támadás

Orosz-ukrán konfliktus óta nem látott mértékben növekszik…

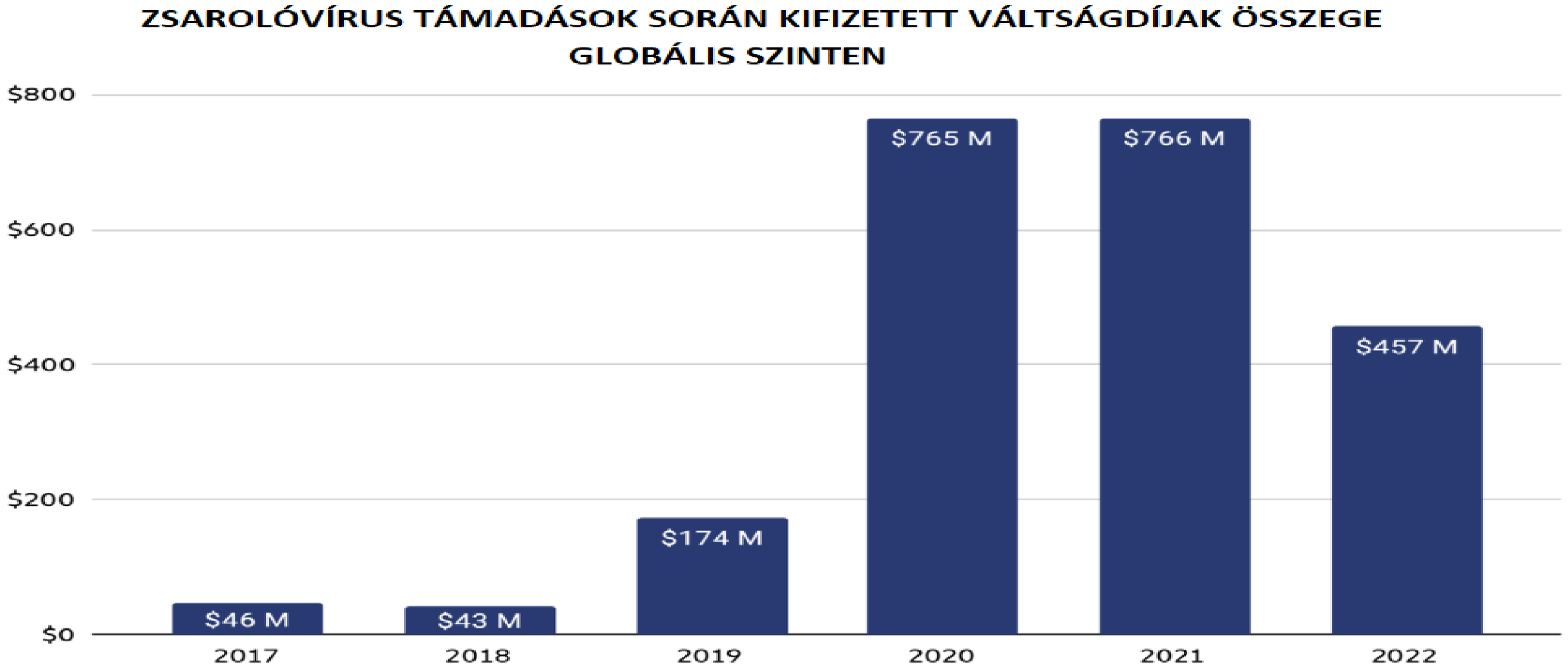
Nincs kegyelem – tényleg fáj

A kiberbűnözők által elkövetett támadások globális kárértéke 2023-ban: kb. 8000 milliárd USD

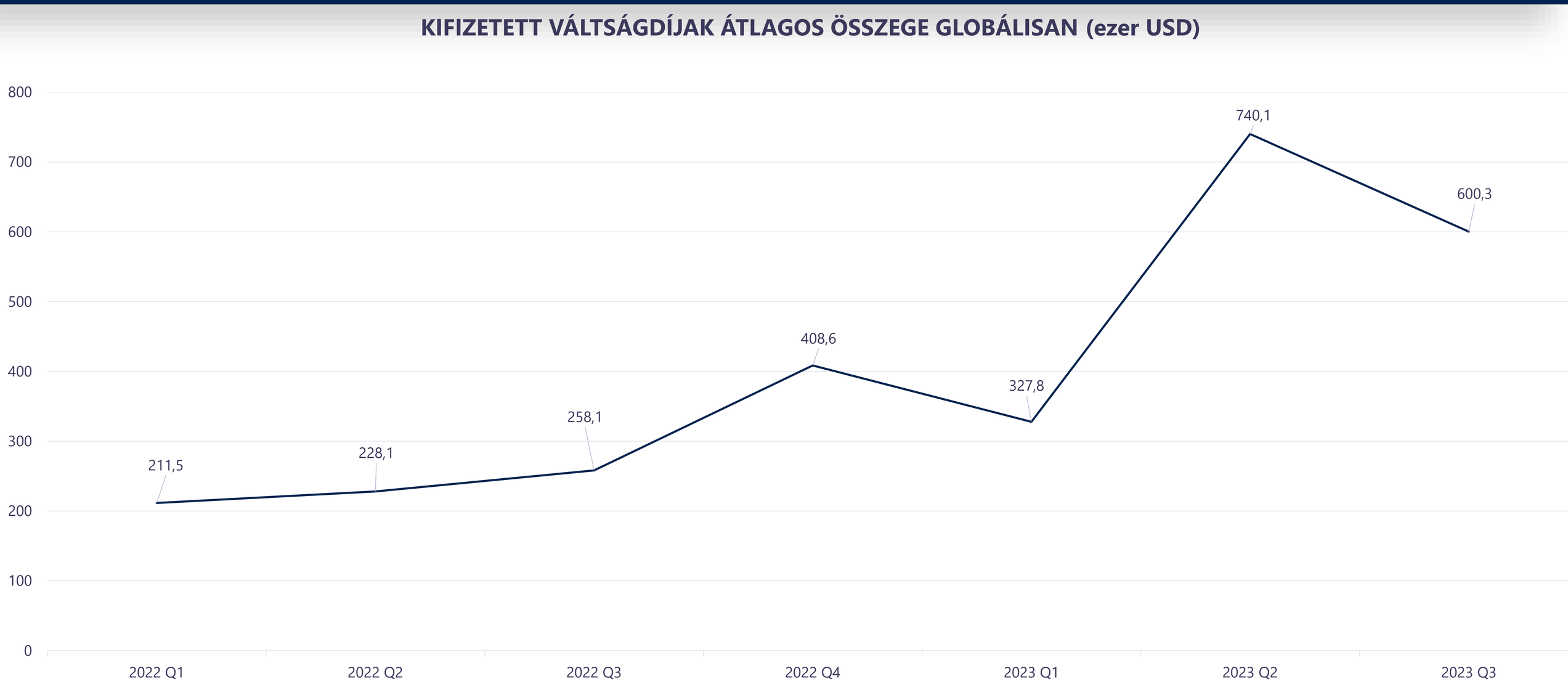


- Pénzügyi szféra
- IKT szektor
- Digitális szolgáltatások

Nincs kegyelem – zsarolóvírusok (globálisan)



Nincs kegyelem – zsarolóvírusok (globálisan)



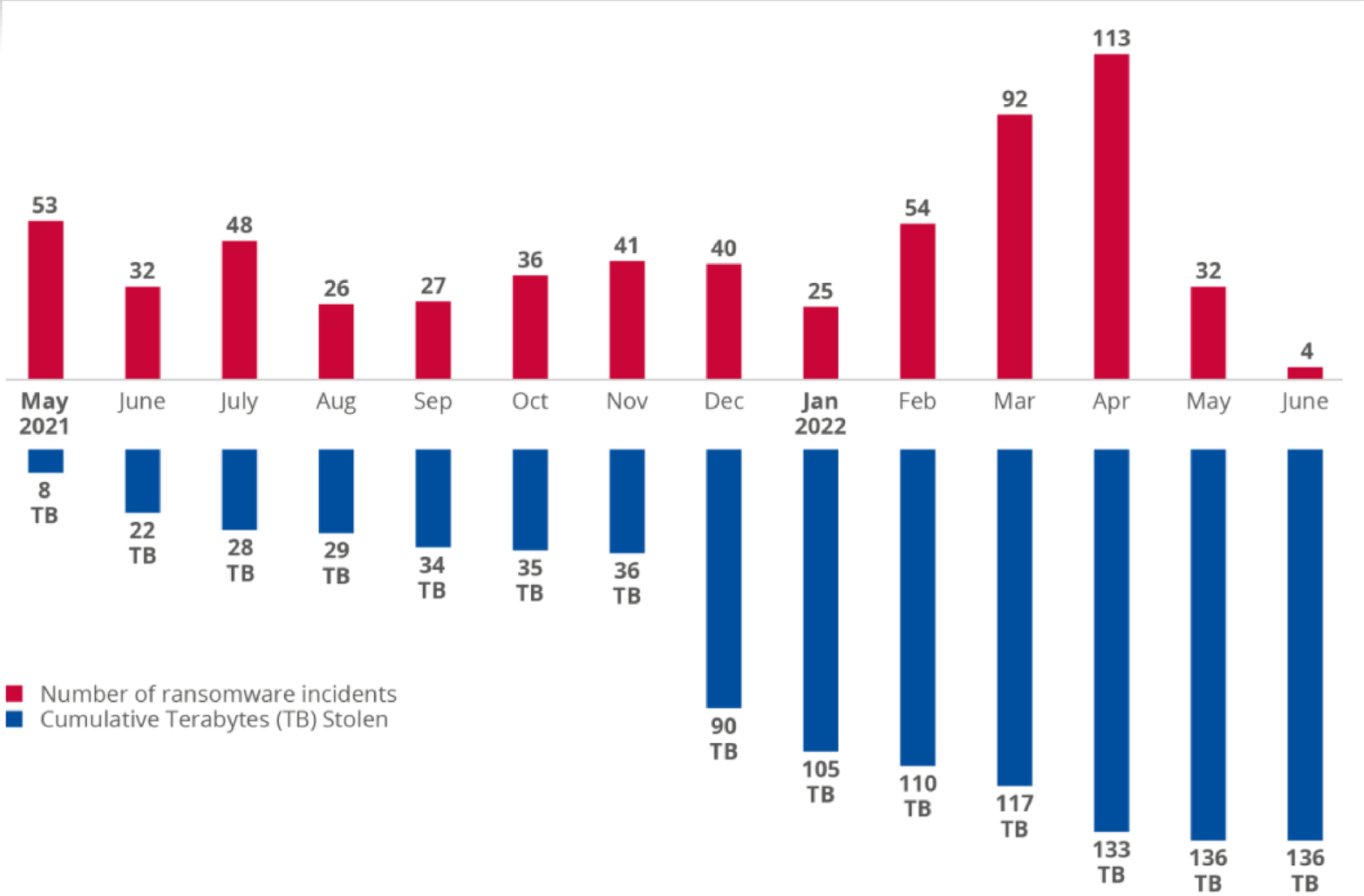
Nincs kegyelem – zsarolóvírusok (Magyarországon)

Kifizetett váltságdíj 2021-ben Mo-n

~ 250M forint

Helyreállításra fordított összeg 2021-ben Mo-n

~ 540M forint



Nincs kegyelem - adathalászat

Feladó: **Nemzeti Egészségügyi Központ Magyarország** <Muller.Cecilia@nnk.gov.hu>
Date: 2020. jún. 12., P, 9:28
Subject: A Covid-19 védőfelszerelés ingyenes forgalmazása (Nemzeti Egészségügyi Központ Magyarország) 2020
To:

NEMZETI NÉPEGÉSZSÉGÜGYI KÖZPONT

Állami Népegészségügyi és Tisztiorvosi Szolgálat

Kedves mindenkinek,

A magyar kormány által kiadott covid-19 válaszadási utasítások szerint mi, a Magyar Nemzeti Egészségügyi Központ a covid-19 védőeszközöket ingyenesen kívánjuk eljuttatni a magyarországi összes regisztrált vállalathoz és iparághoz. Kérjük, töltse ki egyértelműen a mellékelt űrlapot. győződjön meg arról, hogy az alkalmazottak száma és a cég címe egyértelműen meg van írva ebben a formában.

Töltse ki a mellékelt űrlapot, és a mai bezárás előtt küldje vissza nekünk a másolatot, várva a gyors választ.

Az összes kitöltött nyomtatványt erre az e-mailre kell küldeni: Müller.Cecília@nnk.gov.hu

Szia

- Dr. Müller Cecília
  osztályvezető
- Országos Tisztifőorvos
- NEMZETI NÉPEGÉSZSÉGÜGYI KÖZPONT
- 1097 Budapest, Albert Flórián út 2-6.
- Müller.Cecília@nnk.gov.hu

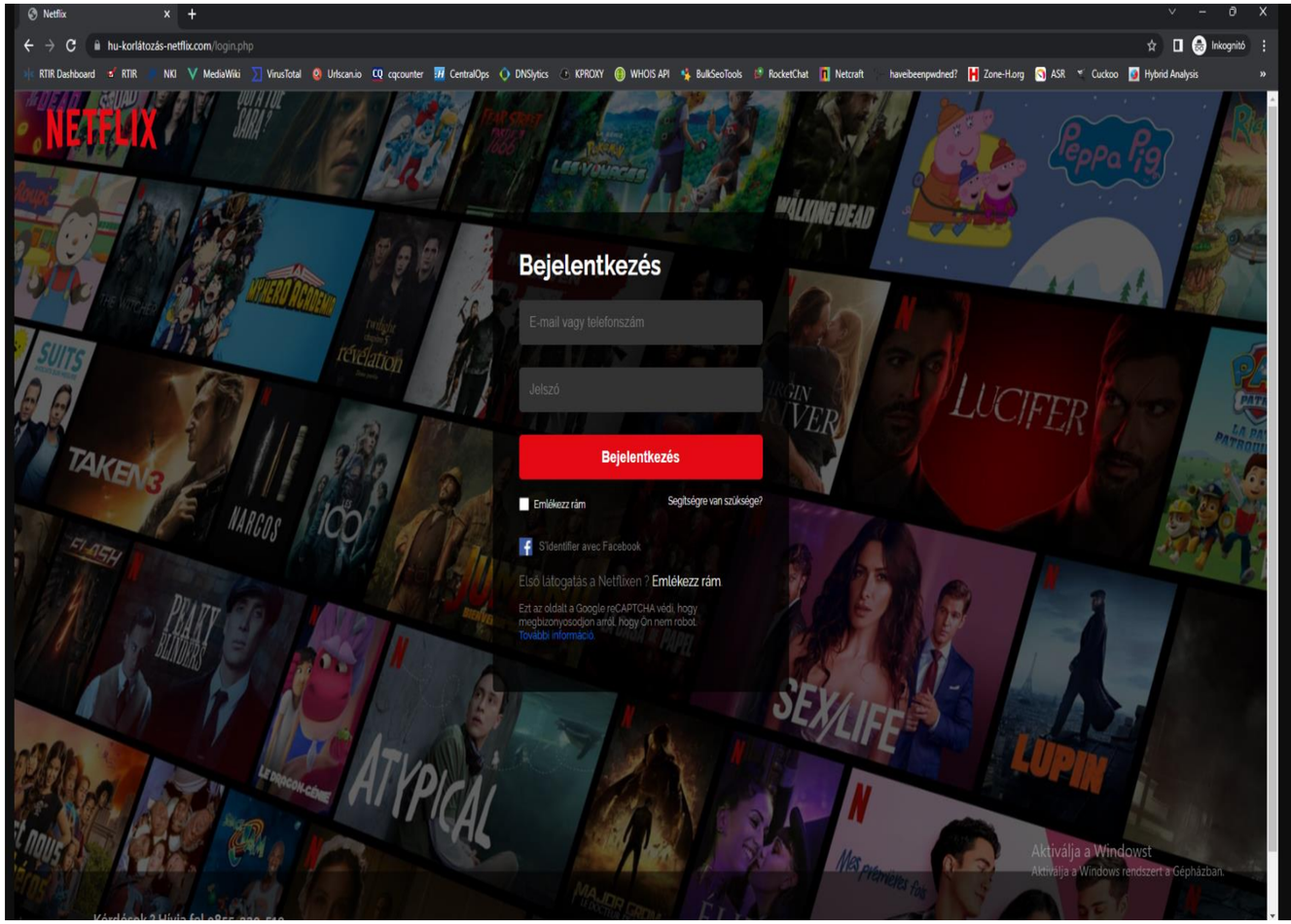
Nincs kegyelem – a nagy klasszikus újragondolva

NETFLIX : Utolsó figyelmeztetés a fiókjának korlátozása előtt, kérjük, erősítse meg adatait 24 órán belül : netflix-korlátozás.net

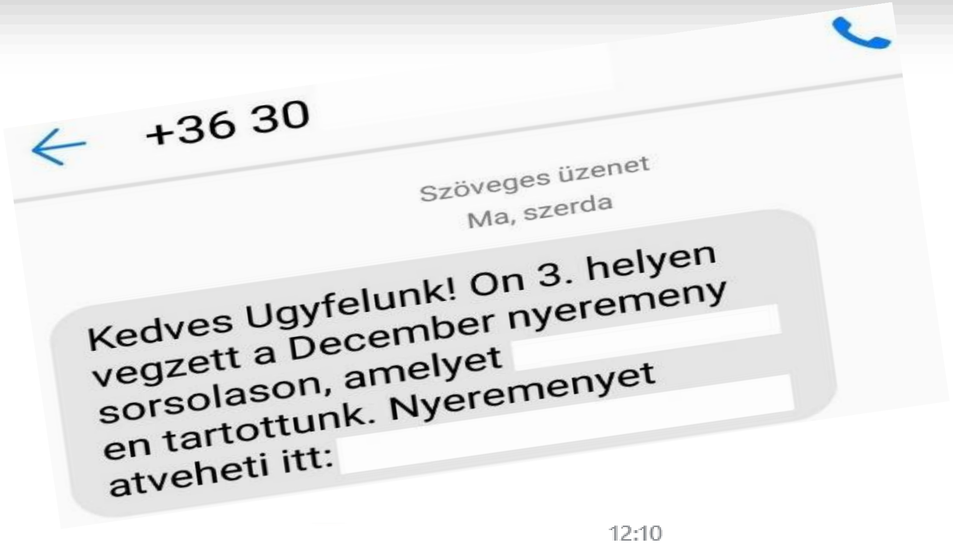
Legutobbi befizetését elutasitottak,kérjük, er sitse meg fizetési adatait, különben fiokjat felfüggesztjük: netflix.renew-hu.net

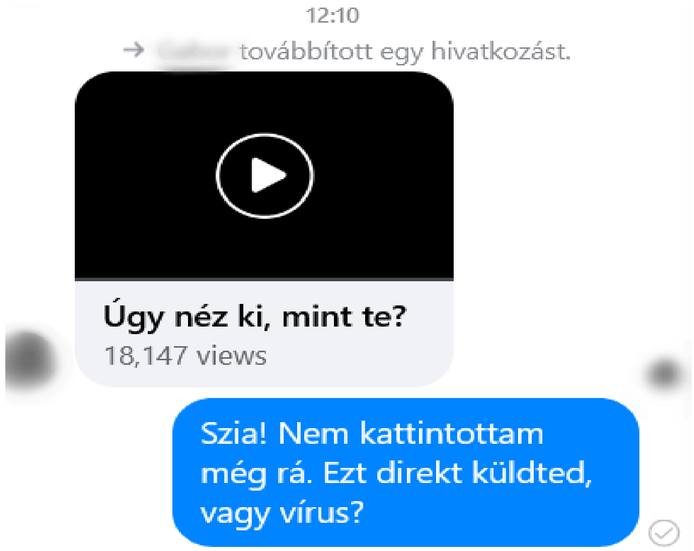
NETFLIX
Utolsó figyelmeztetés a fiókjának korlátozása előtt, kérjük, erősítse meg adatait 24 órán belül : hu-korlátozás-netflix.com

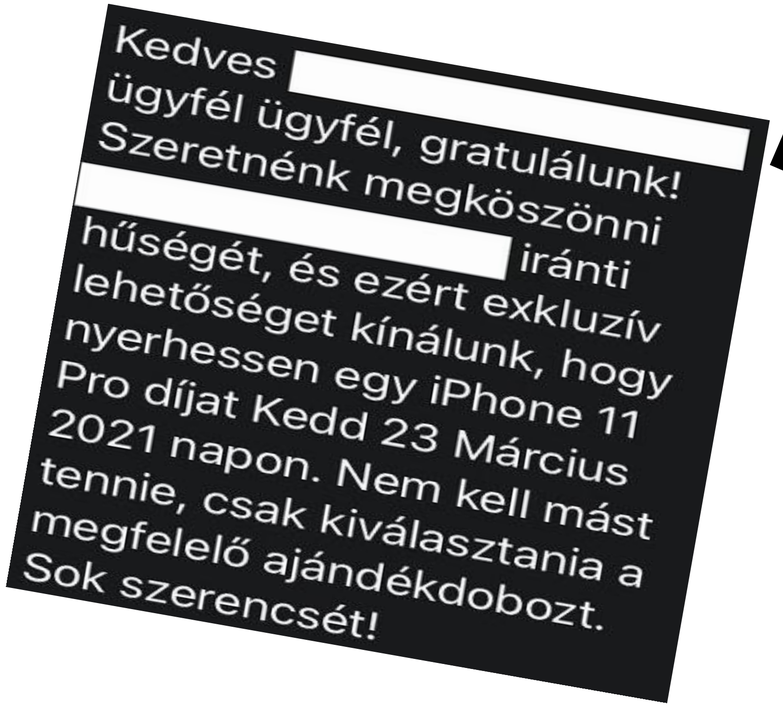
Netflix : Legutobbi befizetését elutasitottak,kérjük, er sitse meg fizetési adatait, különben fiokjat felfüggesztjük: https://hongria-my-account.com

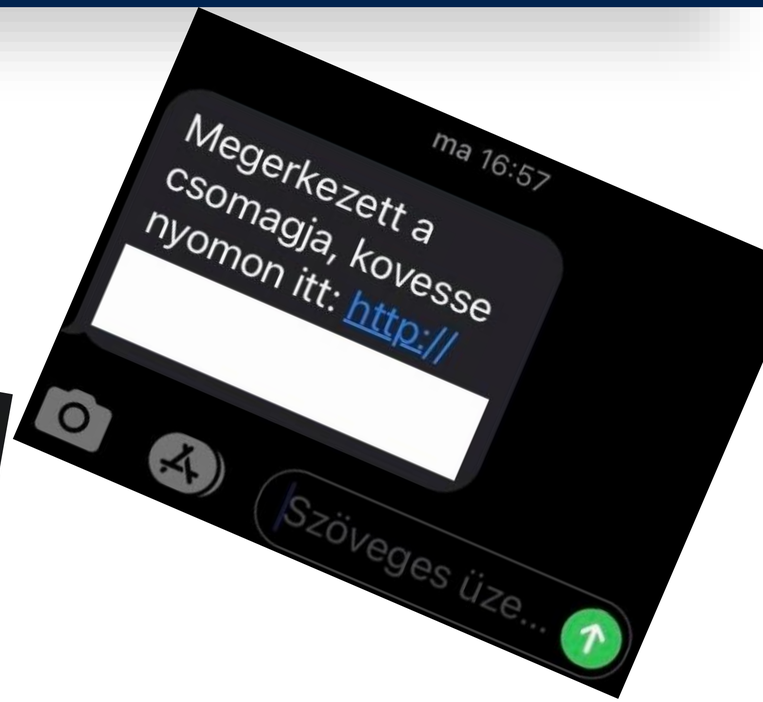


NINCS KEGYELEM – pszichológiai manipuláció



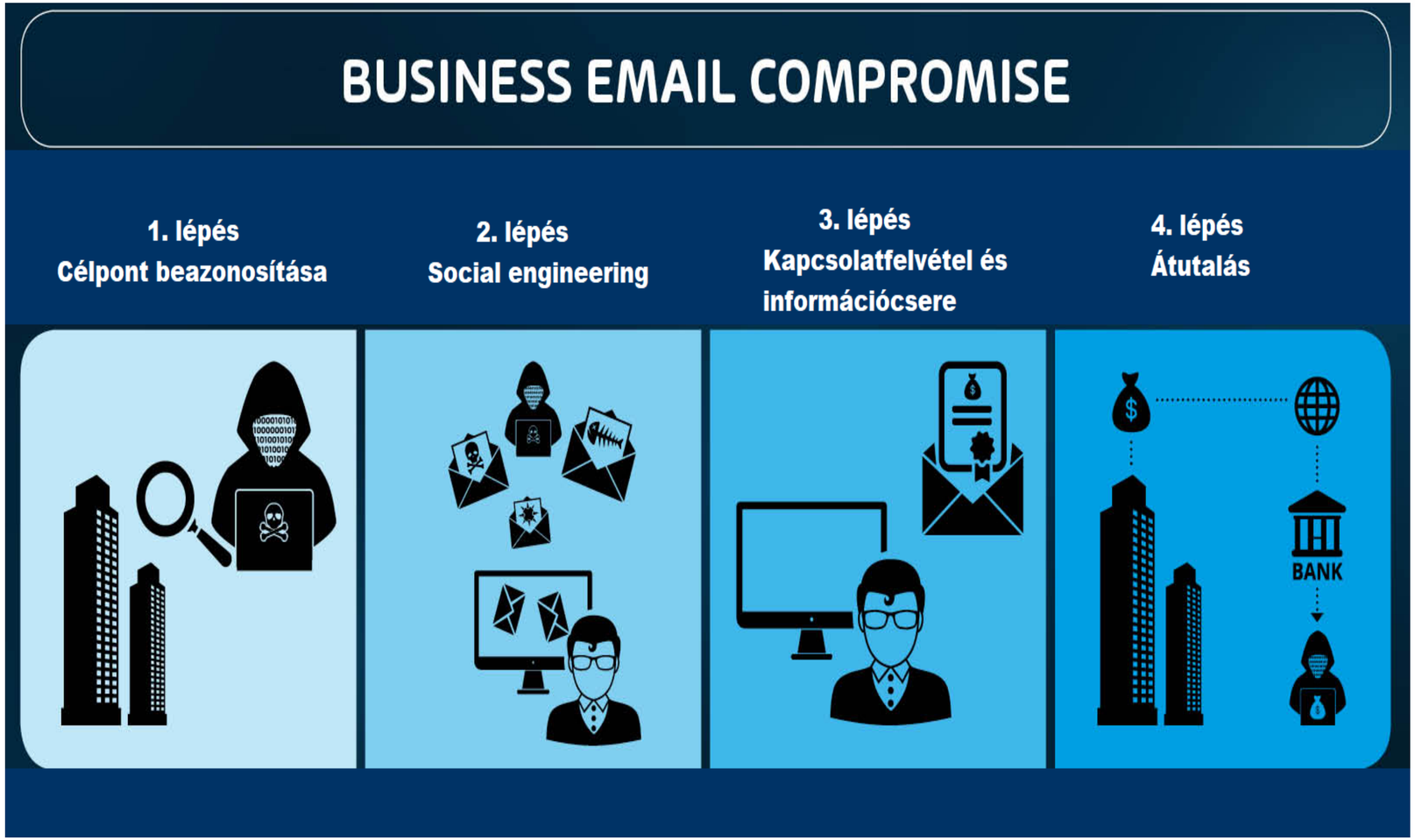






NINCS KEGYELEM – BEC / CEO csalások

Money
Money
Money



NINCS KEGYELEM – AI: Deep fake, LLM és társaik

Az első deepfake audio scam (vishing) 2019-ben történt: egy CEO hangján kértek utalást. Kár értéke: 243.000 USD

Első deep fake videókat 2017-2018-ban celebpornóra használták

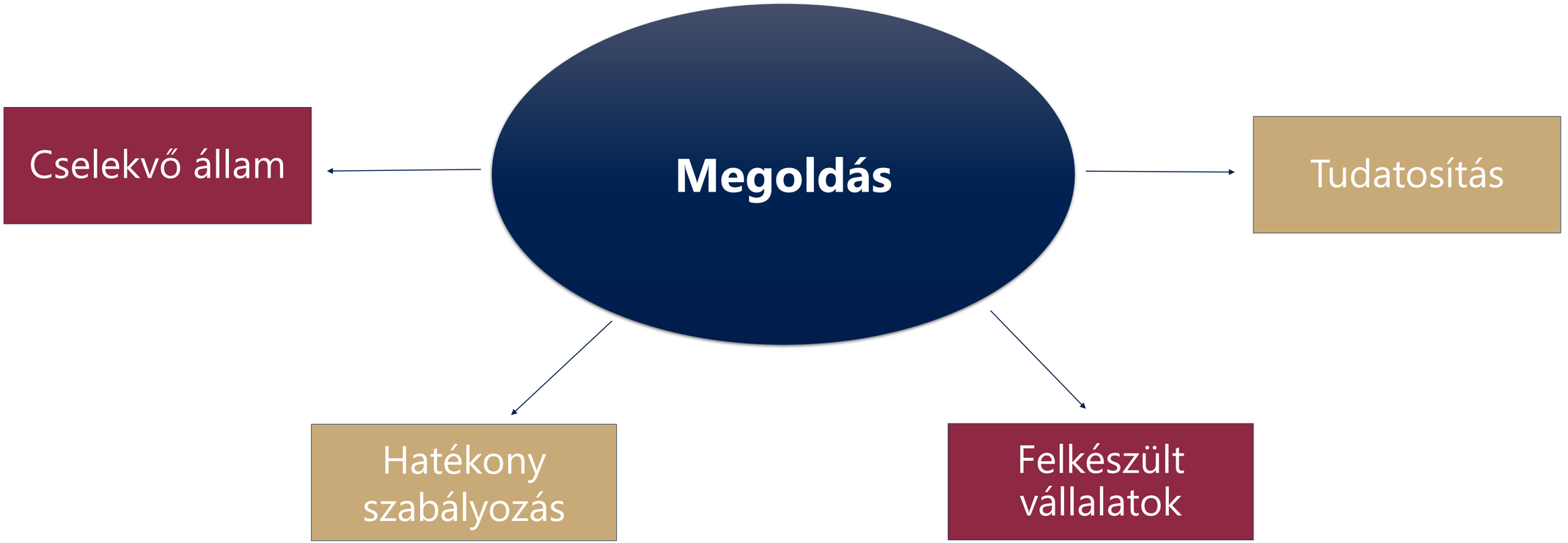
A 2018-as amerikai félidős választásokon már reális támadási formának tartották a deep fake-et

A máig egyik leghíresebb deep fake videó 2018-ban készült Barack Obama-ról.

2023: az AI éve…ChatGPT

2023: Tinder és az AI esete Ázsiában, eljegyzés lett belőle

Kihívások és válaszok



Köszönöm a figyelmet!

kiberbiztonsag@sztfh.hu

SZTFH

Szabályozott Tevékenységek
Felügyeleti Hatósága

Kiberbiztonsági szabályozás

Dr. Bencsik Balázs

SZTFH

Szabályozott Tevékenységek
Felügyeleti Hatósága

Európai Uniós jogszabályi környezet

Kibertan.tv – 2023. évi XXIII. törvény

a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló törvény

ÉRTELMEZŐ RENDELKEZÉSEK

KIBERBIZTONSÁGI TANÚSÍTÁS

2019/881 (EU) rendelet

Nemzeti tanúsítási keretrendszer

KIBERBIZTONSÁGI FELÜGYELET

2022/2555 (EU) irányelv – NIS2

Kiberbiztonsági felügyelet – érintett szervezetek

Kiberbiztonsági felügyelet – érintett feladatai

Vezetői feladatok

Biztonságért felelős személy

Szervezeti szabályozások

Tudatosító oktatások és szinten tartás

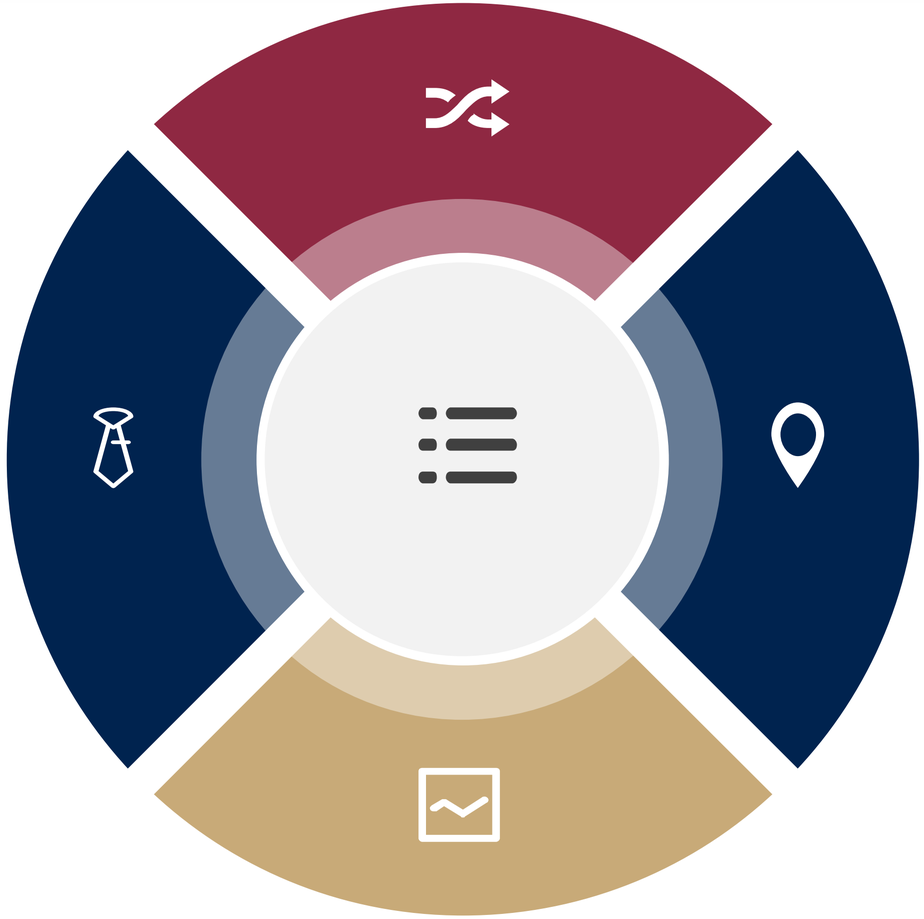
Kiberbiztonsági audit megrendelése

Biztonsági osztályba sorolás

alap

jelentős

magas



Védelem - mit

Hálózati és információs rendszerek + fizikai környezetük

Adatok/információk

Szolgáltatások

Célok

IBIR

Kockázatelemzés

Védelmi intézkedések

Incidensek megelőzése, kezelése, hatásának csökkentése

BC

Életciklus egészében megvalósuló védelem

Kiberbiztonsági felügyelet és ellenőrzés

SZTFH

- Hatósági felügyelet – díj:
  - előző évi árbevétel 0,015 %-a, de max. 10M Ft.
- Nyilvántartás
- Hatósági ellenőrzés
- Rendkívüli ellenőrzés elrendelése
- Figyelmeztetés
- Eltiltás (egyéb hatóságokkal együttműködve)
- Bírság
- 10 000 000 EUR, de legfeljebb éves árbevétel 2%-a

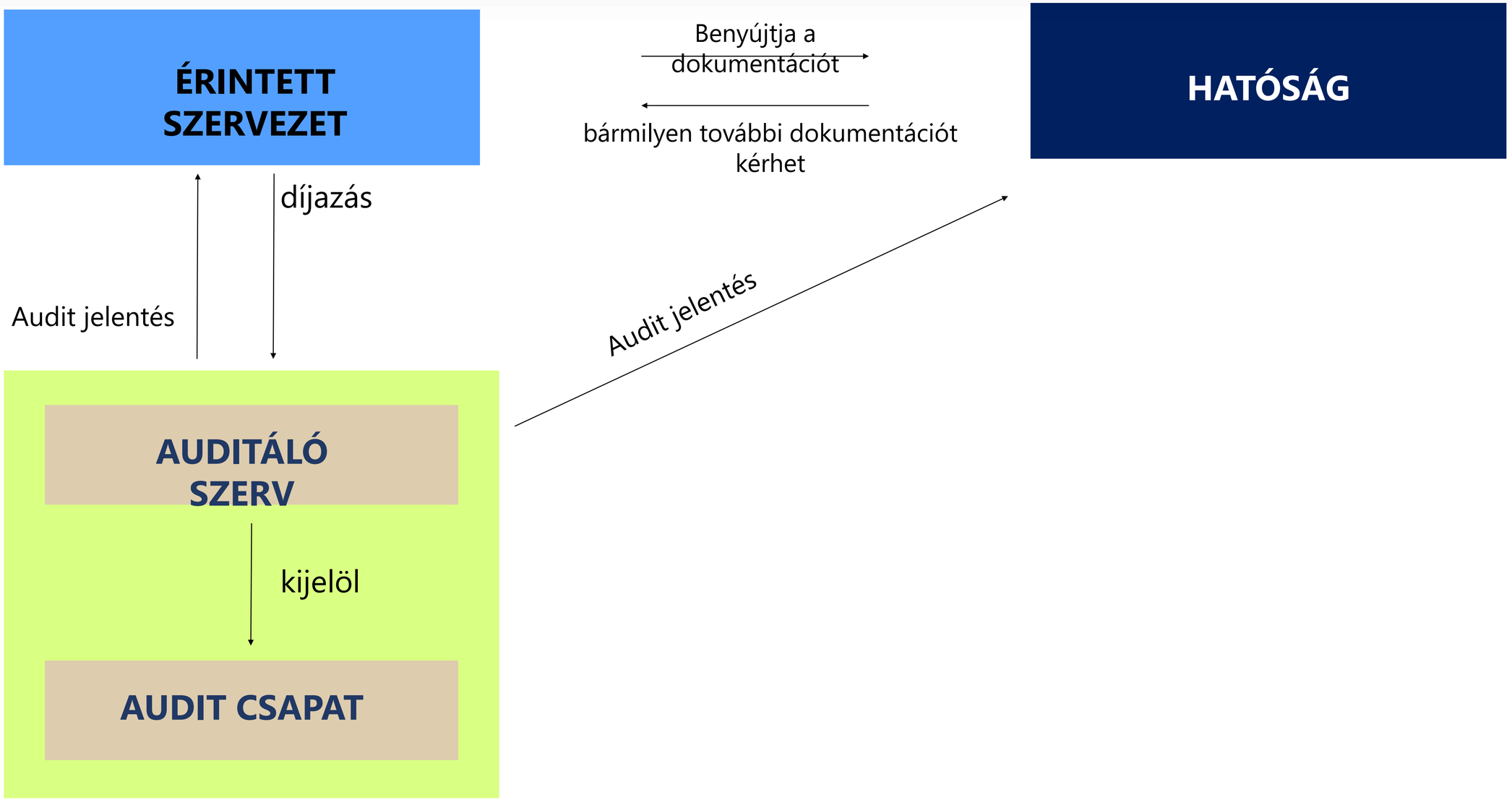
Auditorok

- Érintett szervezet felkérésére
- Kiberbiztonsági audit
  - Biztonsági osztályba sorolás
  - Védelmi intézkedések
  - Sérülékenység- és behatolásvizsgálat
  - Kriptográfiai megfelelőség
  - Forráskód-vizsgálat
- Kétévente kötelező
- Eredmény

Kontrollszett

Követelménycsoport	Követelmény szövege	alap	jelentős	magas
Sikertelen bejelentkezési kísérletek	Az érintett szervezet: - Az általa meghatározott esetszám korlátot alkalmazza a felhasználó meghatározott időtartamon belül egymást követő sikertelen bejelentkezési kísérleteire. - EIR-je automatikusan zárolja a felhasználói fiókot vagy csomópontot a meghatározott időtartamra, vagy ameddig a rendszergazda fel nem oldja annak zárolását, vagy késlelteti a következő bejelentkezési lehetőséget a meghatározott algoritmus szerint. Továbbá értesíti a rendszergazdát, ha a sikertelen próbálkozások maximális számát túllépték.	X	X	X
Eszköz zárolása	Az érintett szervezet: - Meghatározott időtartamú inaktivitás után vagy a felhasználó erre irányuló lépése esetén, az eszköz zárolásával megakadályozza az EIR-hez való további hozzáférést. - Fenntartja az eszköz zárolását mindaddig, amíg a felhasználó a megfelelő azonosítási és hitelesítési eljárásokat el nem végzi.	-	X	X
Munkaszakasz megszakítása – Megszakítási üzenet	Az EIR egyértelmű kijelentkezési üzenetet jelenít meg a felhasználók számára, amely jelzi a hitelesített kommunikációs munkaszakaszok befejezését.	-	-	-

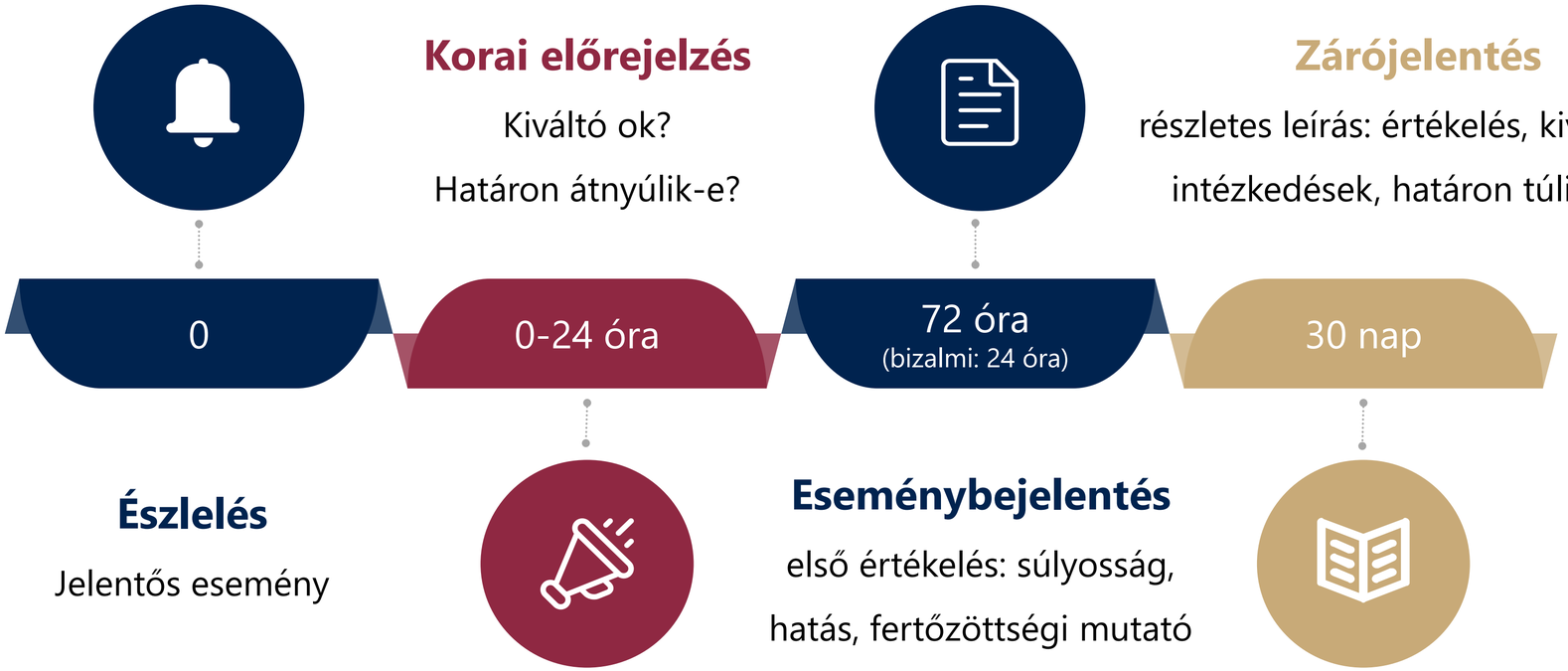
Feladatok és felelősségek



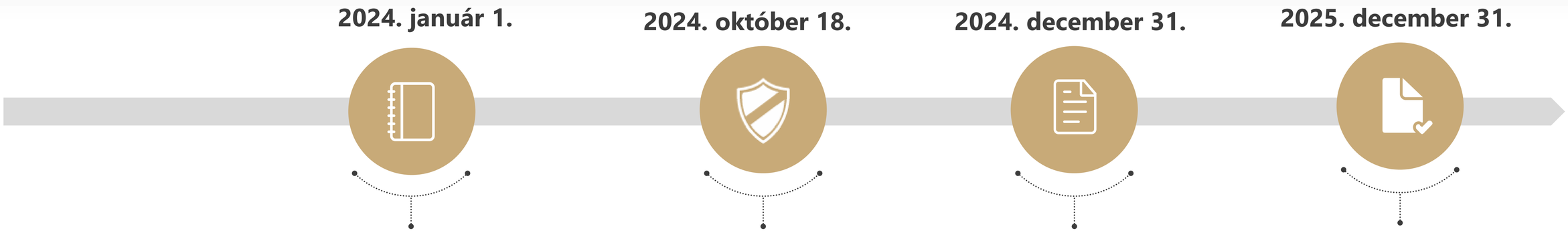
Biztonsági események jelentése

NIS1 olyan esemény, amely **ténylegesen** kedvezőtlen hatást gyakorol a hálózati és információs rendszerek biztonságára

NIS2 olyan esemény, amely **veszélyezteti** a hálózati és információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét vagy bizalmasságát



Kiberbiztonsági felügyelet - ütemezés



SZTFH	• Érintett szervezetek nyilvántartásba vétele • Auditorok nyilvántartásba vétele	• Felügyeleti tevékenység • Ellenőrzési tevékenység		
Érintett szervezet	• Önazonosítás, nyilvántartásba vételre bejelentkezés 2024. június 30-ig • Biztonsági osztályba sorolás • Elektronikus információs rendszerek biztonságáért felelős személy feladatköre és kijelölése	• Védelmi intézkedések alkalmazása • Felügyeleti díj megfizetése	• Első kiberbiztonsági audit vonatkozásában szerződéskötés az auditorral	• Első kiberbiztonsági audit lefolytatásának határideje

Kiberbiztonsági szabályozás

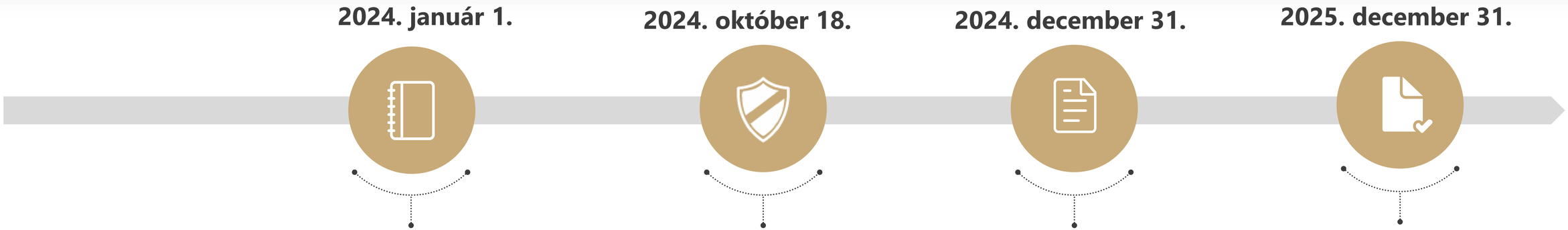
Király Anna

kiberbiztonsági szakértő

SZTFH

Szabályozott Tevékenységek
Felügyeleti Hatósága

Kiberbiztonsági felügyelet - ütemezés



SZTFH	• Érintett szervezetek nyilvántartásba vétele • Auditorok nyilvántartásba vétele	• Felügyeleti tevékenység • Ellenőrzési tevékenység		
Érintett szervezet	• Önazonosítás, nyilvántartásba vételre bejelentkezés 2024. június 30-ig • Biztonsági osztályba sorolás • Elektronikus információs rendszerek biztonságáért felelős személy feladatköre és kijelölése	• Védelmi intézkedések alkalmazása • Felügyeleti díj megfizetése	• Első kiberbiztonsági audit vonatkozásában szerződéskötés az auditorral	• Első kiberbiztonsági audit lefolytatásának határideje

Kiberbiztonsági felügyelet és vhr-ei

23/2023. (XII. 19.) SZTFH rendelet

(ÖN)AZONOSÍTÁS | **FELELŐS** | **TECHNIKAI ADATOK** | **PARTNER ADATOK** | **KÉRELEM**

A1

Szervezet mérete (Kkvtv.)

	mikro-	kis-	közép-	nagyvállalkozás	
foglalkoztatotti létszám	<10	<50	<250	≥250	fő
	és	és	és	vagy	
előző évi bevétel	≤ 2	≤10	≤ 50	>50	millió€
			vagy	vagy	
mérlegfőösszeg			≤ 43	> 43	millió€

Kiberbiztonsági felügyelet és vhr-ei

23/2023. (XII. 19.) SZTFH rendelet

(ÖN)AZONOSÍTÁS | **FELELŐS** | **TECHNIKAI ADATOK** | **PARTNER ADATOK** | **KÉRELEM**

A2

Tevékenység

Szervezet mérete?

Közép- vagy nagyvállalkozás

Vizsgálandó tevékenységek:
- ✓ Kibertantv. 1 melléklet
- ✓ Kibertantv. 2. melléklet

Mikro- vagy kisvállalkozás

Vizsgálandó tevékenységek:
- ✓ elektronikus hírközlési szolgáltató
- ✓ bizalmi szolgáltató
- ✓ DNS-szolgáltatást nyújtó szolgáltató
- ✓ legfelső szintű domainnév-nyilvántartó
- ✓ domainnév-regisztrációt végző szolgáltató

Végzi valamely tevékenységet?

nem

igen

érintett szervezet

Kiberbiztonsági felügyelet és vhr-ei

23/2023. (XII. 19.) SZTFH rendelet

(ÖN)AZONOSÍTÁS | **FELELŐS** | TECHNIKAI ADATOK | PARTNER ADATOK | KÉRELEM

F

Ki láthatja el a feladatot?

A Kibertantv. nem szab feltételeket.

GYIK

Vegyünk fel plusz egy munkavállalót?

A szervezet mérlegelésén múlik...

Milyen tv-i kötelezettség van a kijelöléshez kapcsolódóan?

Kibertantv. 19. § (6) bekezdés a) pont

Külsőst bíznék meg, mire figyeljek?

Szakmai háttér, megbízhatóság, egyéb vállalt feladatai stb.

Megbízott jogi entitás esetén a szerződésben javasolt rögzíteni, hogy személy szerint ki fogja a feladatot ellátni!

Szükséges adatok

megbízott jogi entitás esetén:

- cég neve
- adószám
- cégjegyzékszám
- székhely

+

személy

- 4T adata
- telefonszáma (amin elérhető!)
- mail címe

Kiberbiztonsági felügyelet és vhr-ei

23/2023. (XII. 19.) SZTFH rendelet

(ÖN)AZONOSÍTÁS | FELELŐS | **TECHNIKAI ADATOK** | PARTNER ADATOK | KÉRELEM

T

A szervezet nevére bejegyzett és általa használt domain nevek. (nem csak .hu!)

Domain nevek

IP-címek

FIX IP-címek (= dinamikus ✕), melyek a szervezethez rendeltek:

- egyedi IP-címként
- IP-tartományként (tól-ig)
- alhálózattal (/xx)

Olyan **informatikai hátterű szolgáltatás**, amely **széles körben elérhető**, pl:

- ✓ Telefonos ügyfélszolgálat
- ✓ Ügyfélportál
- ✓ Weboldal
- ✓ Online ügyfélszolgálat

Nyilvános szolgáltatások

Kiberbiztonsági felügyelet és vhr-ei

23/2023. (XII. 19.) SZTFH rendelet

(ÖN)AZONOSÍTÁS | FELELŐS | TECHNIKAI ADATOK | **PARTNER ADATOK** | KÉRELEM

P

Szolgáltatás:

általában **ellenszolgáltatásért** … nyújtott szolgáltatás, amely [kivételekkel] magában foglalja
a) az **internet-hozzáférési szolgáltatás**t;
b) a **személyközi hírközlési szolgáltatás**t; és
c) … **jelek**nek elektronikus hírközlő hálózatokon történő **átvitelé**ből, … **irányítás**ából álló szolgáltatást, ideértve a **gépek közötti szolgáltatás**t és a **műsorterjesztésre használt átviteli szolgáltatás**t is.

Eht. 188. § 17. pont = **elektronikus hírközlési szolgáltató**

Ekertv. 2. § *l)* pont = közvetítő szolgáltató

- egyszerű adatátvitel és hozzáférés-biztosítás
- gyorsítótárolás
- tárhelyszolgáltatás
- keresőszolgáltatás
- alkalmazásszolgáltató
- videómegosztóplatform-szolgáltató

Kibertantv. 19. § (4) bekezdés = közreműködő

… **elektronikus információs rendszer létrehozás**ában, **üzemeltetés**ében, **karbantartás**ában vagy **javítás**ában közreműködő …

Partner

Kiberbiztonsági felügyelet és vhr-ei

23/2023. (XII. 19.) SZTFH rendelet

(ÖN)AZONOSÍTÁS | FELELŐS | TECHNIKAI ADATOK | PARTNER ADATOK | **KÉRELEM**

K

Ki indíthatja?

az **érintett szervezet cégkapujához meghatalmazás**sal rendelkező természetes személy

Honnan indítható?

- magyarorszag.hu-ról kereséssel: **SZTFH 420 Érintett szervezet nyilvántartásba vételére irányuló kérelem**
- **SZTFH honlapjáról** (sztfh.hu): Ügyintézés/Nyomtatványok és űrlapok/ Kiberbiztonsági Ügyek/SZTFH 420/Részletek

Köszönöm a figyelmet!

kiberbiztonsag@sztfh.hu

SZTFH

Szabályozott Tevékenységek
Felügyeleti Hatósága

MINDEN KIBERÜL

#podcast

SZTFH

Szabályozott Tevékenységek
Felügyeleti Hatósága