Biró Gabriella | főosztályvezető

Hétpecsét | 2023.01.25.

A MAGYAR PÉNZÜGYI SZEKTOR KIBERFENYEGETETTSÉGI TÉRKÉPE 2022

MNB FELÜGYELETI STRATÉGIA 2020-2025

KÜLDETÉS: A pénzügyi rendszer stabilitásának támogatása és mélyítése, kiemelt fókusszal a **fogyasztóvédelemre, digitalizációra és fenntarthatóságra**

JÖVŐKÉP: Fejlődő, versenyző, **egészséges** pénzügyi szektor – **támogató,** formáló, **hatékonyan** felügyelő MNB

KIEMELT ÉRTÉK: Stabilitás és bizalom

Jogszerűség, integritás, fogyasztó-központúság, innováció, fenntarthatóság, következetesség, fair verseny

PIACI FÓKUSZÚ CÉLOK

1. Sokkellenálló-képesség biztosítása

1.1. Megbízhatóan működő, egészséges mérlegszerkezettel, biztonságos tőkehelyzettel és megfelelő veszteségviselő képességgel rendelkező piaci szereplők

1.2. A pénzügyi szektor védelme, kiemelt fókusszal a pénzügyi visszaélésekre és a piacfelügyeletre

1.3. Intézmények ellenállóképességének növelése a pénzmosási és terrorizmusfinanszírozási kockázatok kapcsán

1.4. A szektor kiberbiztonsági ellenállóképességének biztosítása

2. Egészséges verseny prudens és fogyasztóközpontú termékekkel

2.1. Transzparencia megkövetelése, kiemelt fókusszal az árazásra

2.2. A pénzügyi termékek prudens és fogyasztóközpontú értékesítése

2.3. Ügyfél igénynek folyamatosan megfelelő termékek

2.4. Megtakarítási rendszerek fejlesztése

3. Technológiai fejlődés támogatása, kockázatok kezelése

3.1. Technológiai innováció támogatása minden szektorban

3.2. Új technológiák prudens bevezetésének biztosítása

3.3. Digitális pénzügyek biztonságtudatosságának erősítése

4. A pénzügyi rendszer környezeti fenntarthatóságának elősegítése

4.1. Megfelelő felkészülés a környezeti anomáliák következtében megjelenő kockázatokra

4.2. Intézményi támogatás a zöld átállásban

4.3. Környezeti fenntarthatósági tudatosság erősítése

SZERVEZETI FÓKUSZÚ CÉLOK

5. Erőteljes fogyasztóvédelem

5.1. Tisztességes szolgáltatói magatartás szektorszintű és egyedi elvárásának összehangolása

5.2. Termékfókuszú fogyasztóvédelem erősítése

6. Kockázat alapú felügyelet

6.1. Kockázat alapú felügyelési tevékenység továbbfejlesztése, a korai beavatkozást lehetővé tevő felügyelési eszközök alkalmazása

6.2. Nemzetközi együttműködés erősítése, különös tekintettel a home-host felügyelési együttműködésekre és a határon átnyúló tevékenységekre

7. Határozott, időbeni fellépés, beavatkozás

7.1. Adatvezérelt működés

7.2. Proaktív, kockázatokra fókuszáló felügyeleti kommunikáció és jogérvényesítés, a hatékony válságkezelési eszköztár erősítése

8. Folyamatos fejlődés – Támogató felügyelet

8.1. Hasznos innovációk támogatása, felhasználása, károsak kiszűrése, megelőzése

8.2. Pénzügyi tudatosság támogatása

8.3. Támogató, ügyfélbarát engedélyezési folyamatok a kapuőri szerep fenntartása mellett

9. Aktív nemzetközi és hazai szabályozói szerepvállalás

9.1. Felügyeleti tapasztalatokra építő jogfejlesztés

9.2. Aktív szerepvállalás az európai uniós jogalkotásban és a hazai jogba való átültetésben

9.3. Proaktív együttműködés erősítése a hazai és külföldi társhatóságokkal, társfelügyeletekkel, érdekvédelmi szervezetekkel

MNB KIBERFENYEGETETTSÉGI TÉRKÉP PROJEKT

Az Európai Unió támogatásával

A projekt háttere: *A magyar pénzügyi szektor kiberfenyegetettségi térképe 2022* című kiadvány az **MNB Informatikai felügyeleti főosztály** munkája révén jött létre.

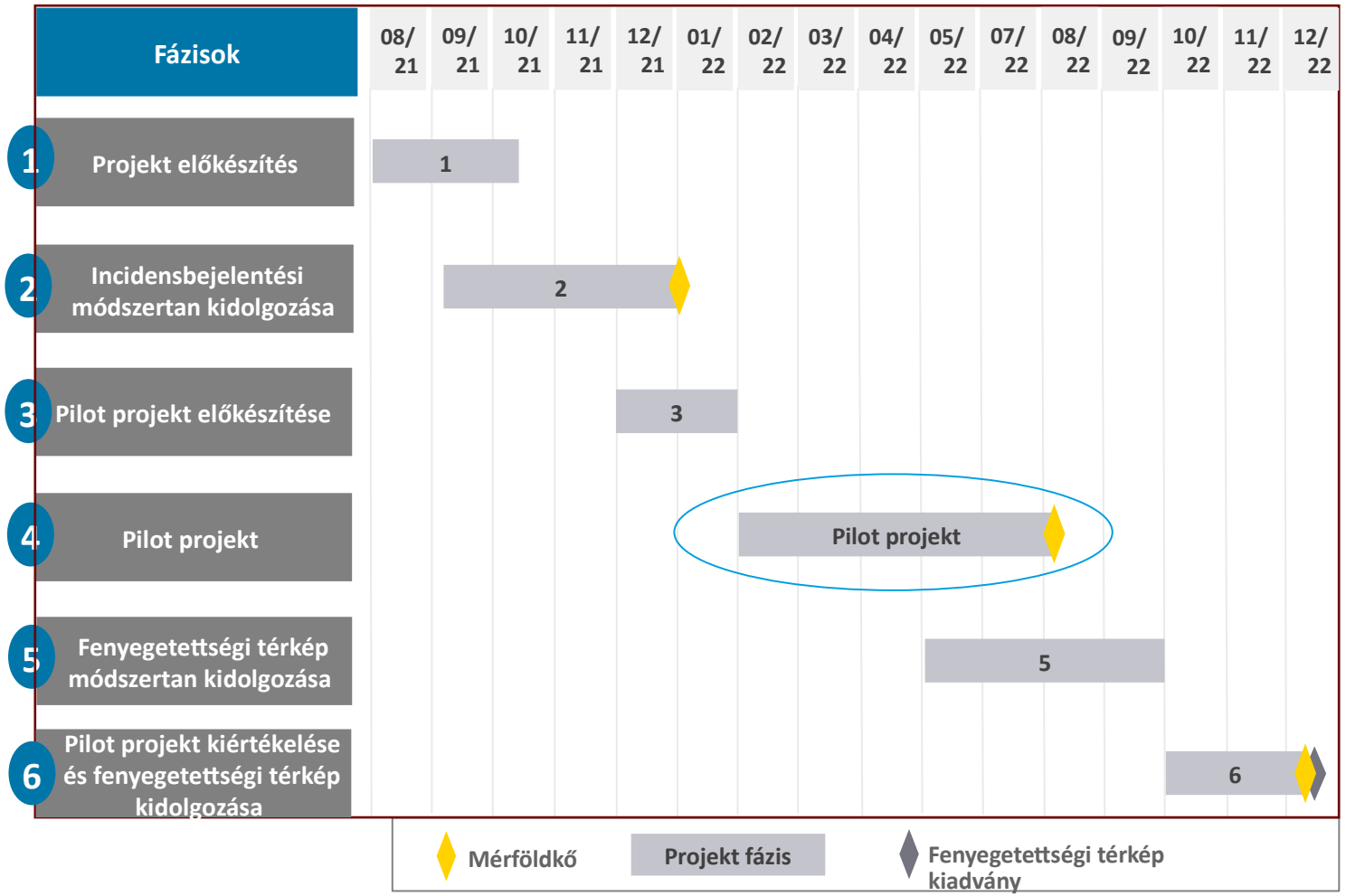
A projekt az Európai Bizottság Strukturálisreform-támogatás Főigazgatósága (DG REFORM) 2021. évre vonatkozó Technikai Támogatási Eszköz támogatásával és finanszírozásával valósult meg. A feladatokban a Bizottság döntése alapján az Ernst & Young Consulting Ltd. magyarországi irodája segítette az MNB-t.

A projekt fő célkitűzései:

1. Új **incidens jelzésre vonatkozó módszertan**, valamint rendszeres **fenyegetettségi térkép elkészítéséhez szükséges módszertan** elkészítése. A módszertani munkák során kiemelt figyelmet kapott a DORA rendeletre való felkészülés.
2. A módszertanok tesztelése egy **6 hónapos Pilot Projekt** keretében, melynek eredményeként a keletkezett adatokból elkészíthető az első magyar pénzügyi szektorra vonatkozó fenyegetettségi térkép.
3. A fenyegetettségi térképnek köszönhetően az MNB és a felügyelt intézmények is pontosabb képet kaphatnak a pénzügyi szektorban megjelenő kiberbiztonsági fenyegetésekről.

Forrás | MNB

A PROJEKT EGYSZERŰSÍTETT IDŐVONALA



PROJEKTTERV

A projekt 2021. szeptemberé-ben vette kezdetét és az eredeti terv szerint 2022. december végén zárult volna.

Leszállítandók:

- Incidensbejelentési módszertan
- Fenyegetettségi térkép módszertan
- A magyar pénzügyi szektor kiberfenyegetettségi térképe 2022

2021. július – 2022. december

Forrás | EY

A PILOT IDŐTARTALMA ÉS SZEREPE

A pilot projekt célja kettős volt:

- A kialakított incidensbejelentő és fenyegetettségi elemzésre vonatkozó módszertanok tesztelése
- A fenyegetettségi térkép módszertan hatékonyságának és alkalmazhatóságának kipróbálása

A pilot projekt résztvevői:

- A pilot projekthez csatlakozó 39 felügyelt intézmény (5 bank, 12 biztosító, 10 pénztár)
- MNB Informatikai felügyeleti főosztály
- EY magyarországi tanácsadói

A PILOT PROJEKT LEGFONTOSABB ISMÉRVEI

- A projekt pilot fázisa **február 1. és július 31.** között zajlott
- A pilot során gyűjtött adatok felhasználásával készült el a fenyegetettségi térkép
- A pilot tanulságai alapján került kialakításra a végleges és később bevezetésre kerülő incidensbejelentési módszer-tan

Forrás | MNB

A PILOT PROJEKTBEN GYŰJTÖTT JELZÉSEK

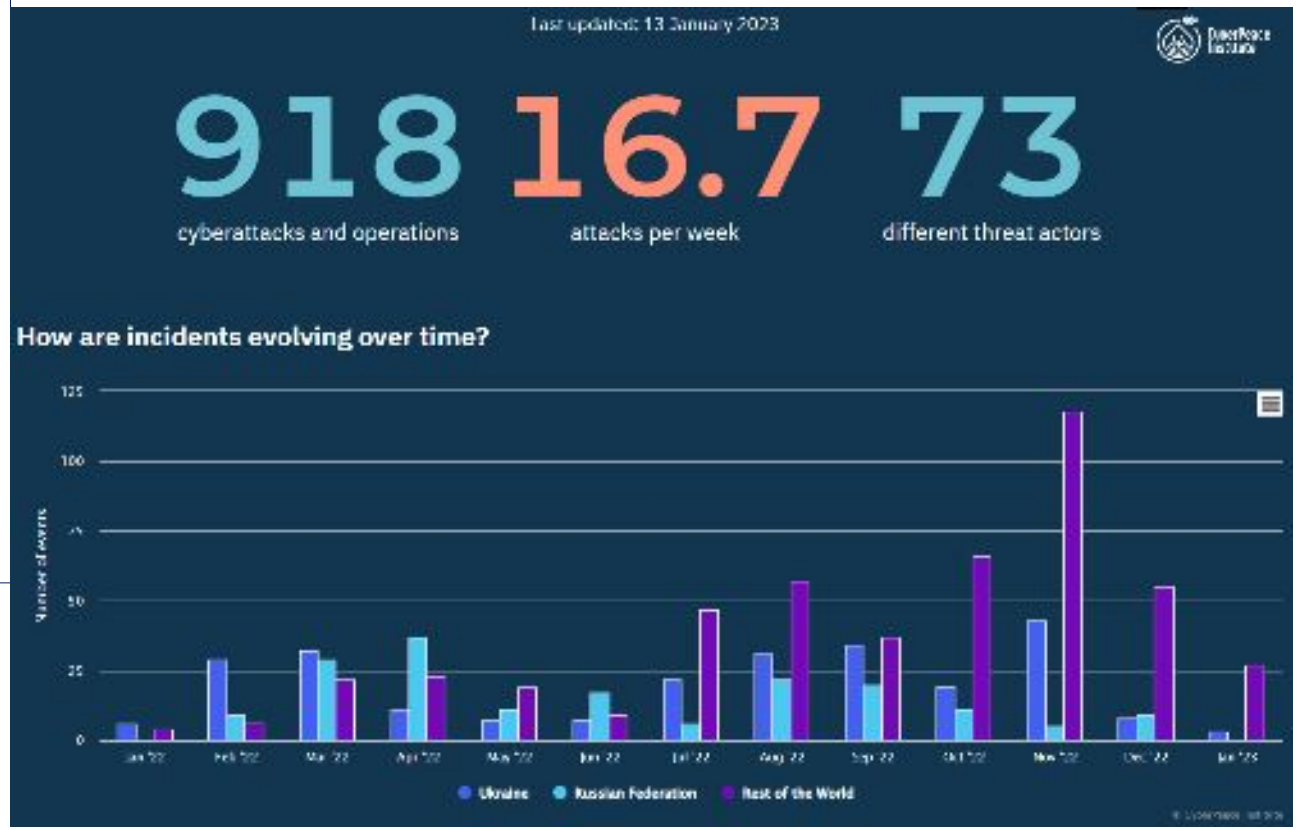
1. Havi összegző bejelentések a hónap történéseiről – kritikus és nem kritikus incidensek
2. Kritikus incidensek esetében 90 percen belül kezdeti jelzés, majd időközi jelzés(ek), végül záró jelzés – hasonlóan az eddigi gyakorlathoz

A JELENTÉSEK TÍPUSAI ÉS AZOK ELEMEI

Havi bejelentések vs. Kritikus incidensek jelzései

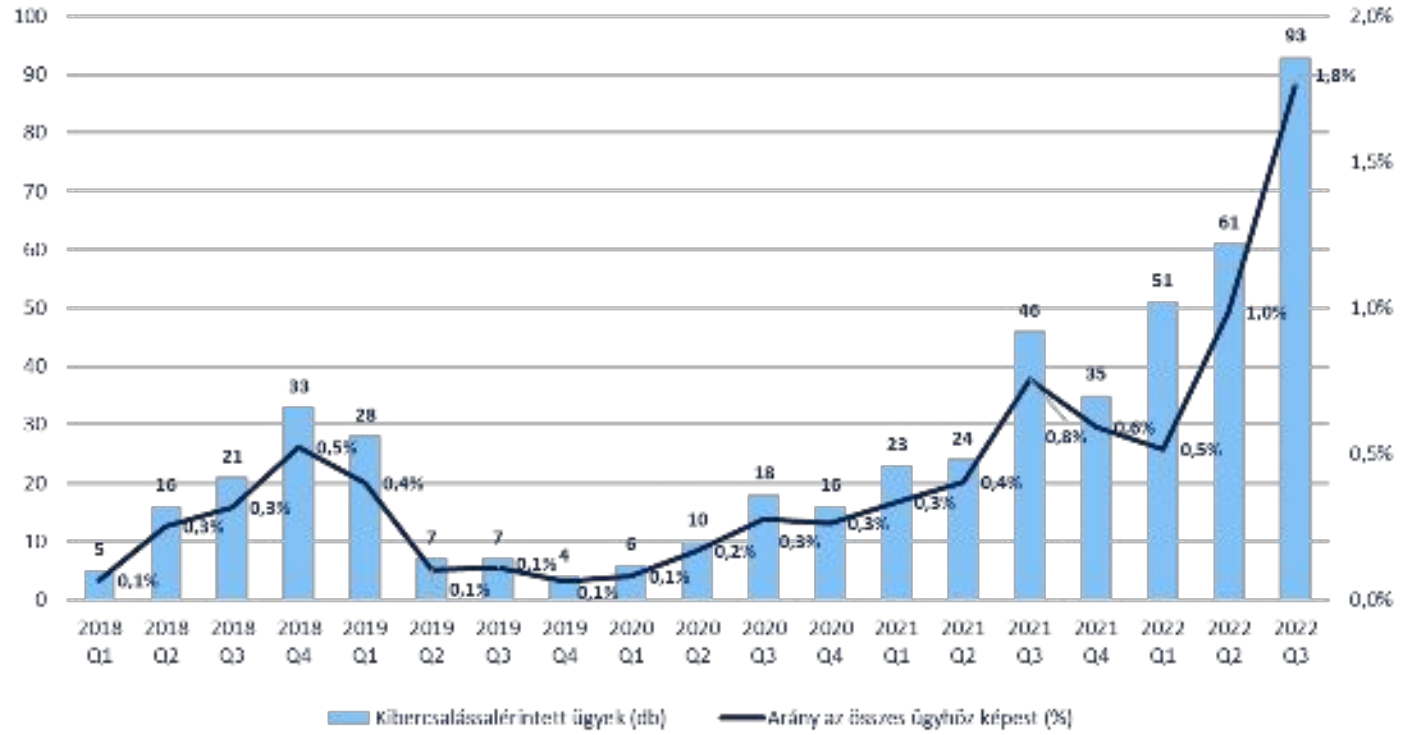
Forrás | MNB

ÁLTALÁNOS KIBERBIZTONSÁGI KITEKINTÉS



ENISA & CyberPeace Institute

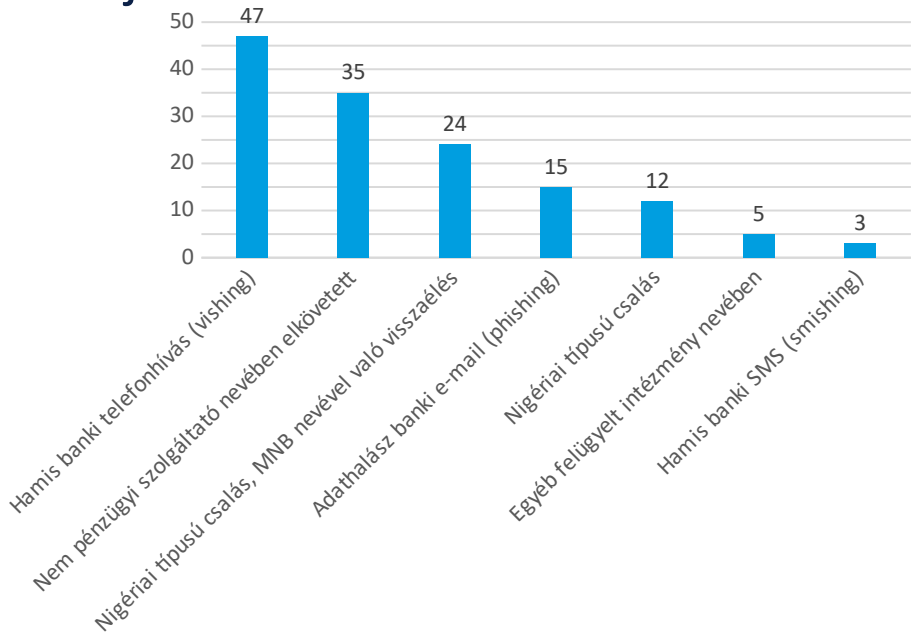
KIBERVISSZAÉLÉSI TENDENCIÁK AZ MNB ADATOK ALAPJÁN



KIBERVISSZAÉLÉS TÉMÁJÚ ÜGYFÉLJELZÉSEK

számának alakulása az MNB ügyfélszolgálaton

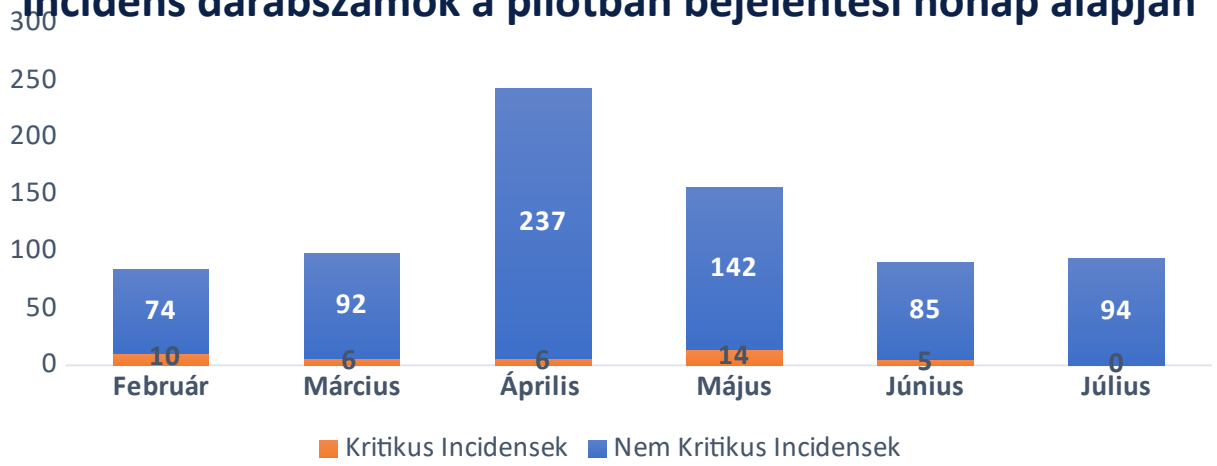
Kibervisszaélések típusai az MNB Ügyfélszolgálati Információs Központja által rendelkezésünkre bocsátott adatok alapján a pilot ideje alatt



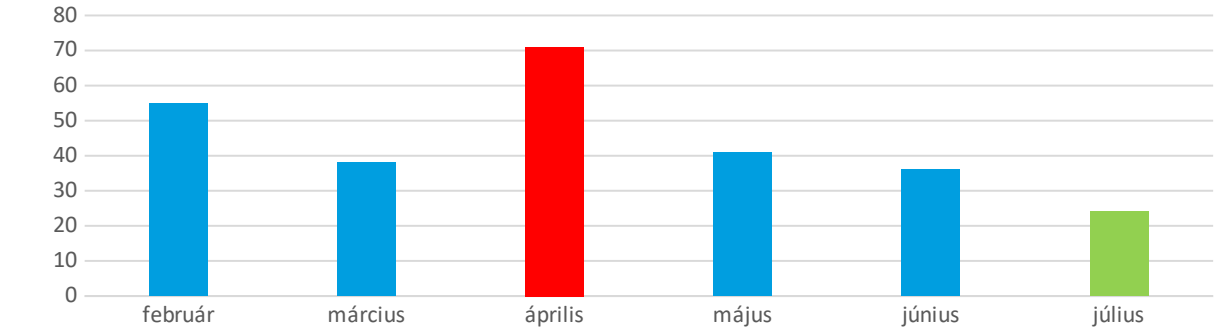
Forrás | MNB

AZ INCIDENS ELOSZLÁS KONZISZTENS MINTÁZATOT MUTAT

Incidens darabszámok a pilotban bejelentési hónap alapján



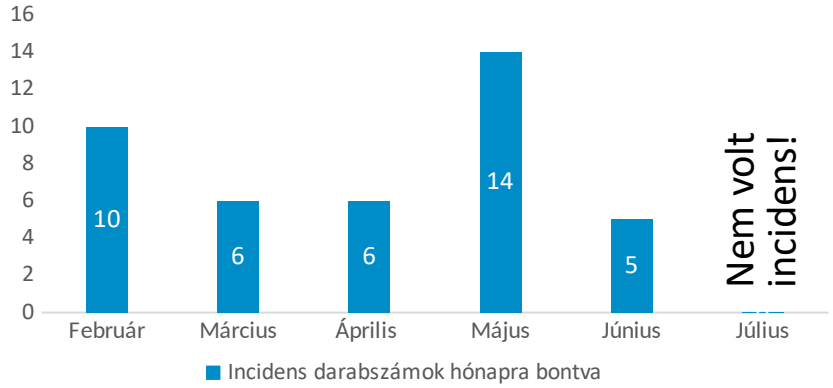
A pénzforgalmi szolgáltatást érintő üzemzavarok havi eloszlása (P58 MNB azonosító kódú adatszolgáltatás alapján)



AZ INCIDENSEK HAVI ELOSZLÁSA A PILOTBAN

A nyári hónapokban kevesebb az incidens mind a pilot adatai, mind a pénzforgalmi adatszolgáltatás alapján – nyáron az IT rendszerekben végrehajtott változások száma is alacsonyabb.

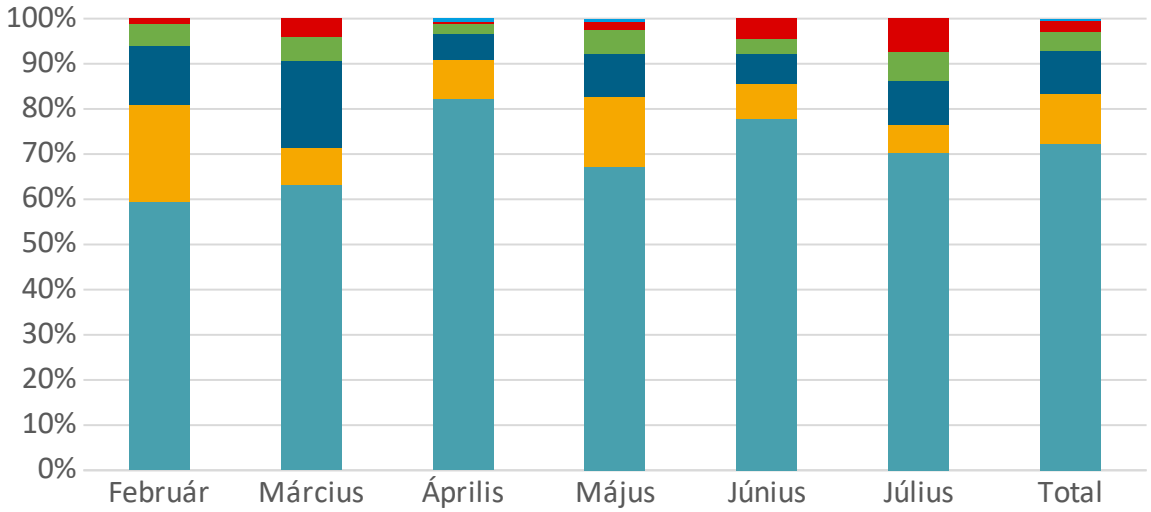
Incidens darabszámok bejelentési hónap alapján (kritikus incidensek esetén)



2022. február - augusztus

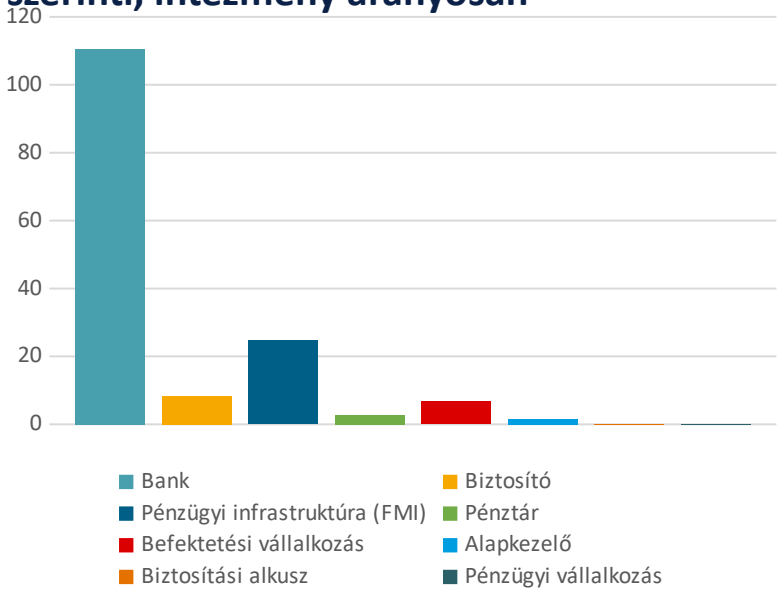
Forrás | MNB

A BANKOK JELENTETTÉK A LEGTÖBB INCIDENST



A különböző típusú intézmények nagyon eltérő mennyiségű incidenst tapasztaltak és jelentettek – legtöbbet a bankok.

Incidens darabszámok intézménytípusok szerinti, intézmény arányosan

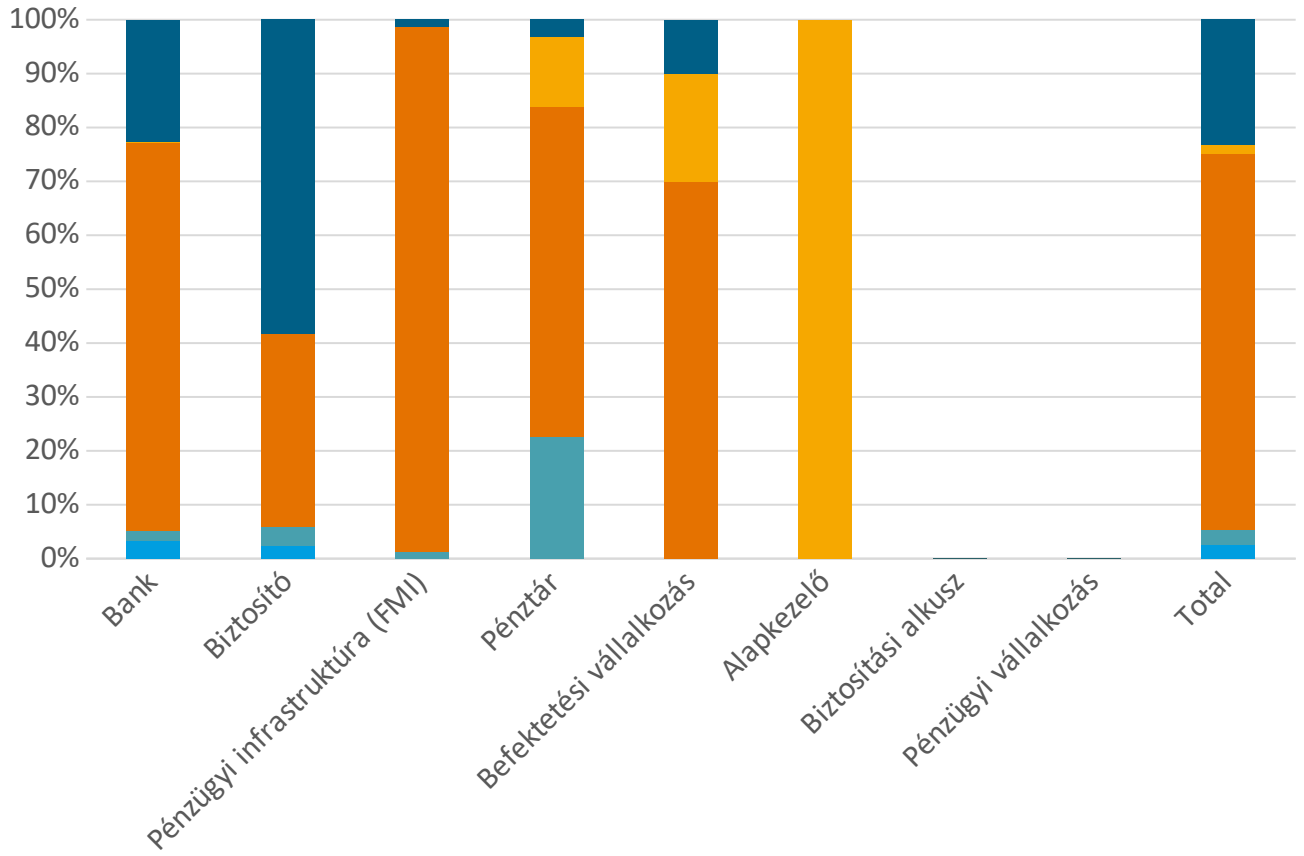


INCIDENS BEJELENTÉSEK

intézménytípusok szerinti havi bontásban

Forrás | MNB

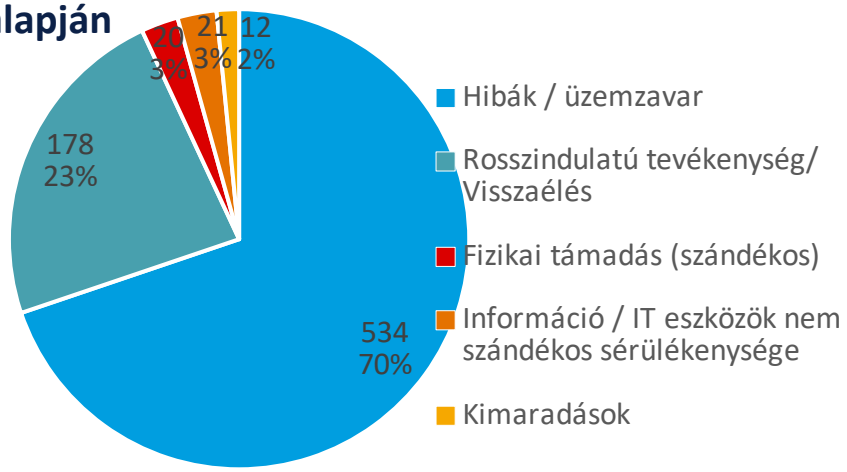
AZ INCIDENSEK NAGY RÉSZÉNEK OKA ÜZEMZAVAR



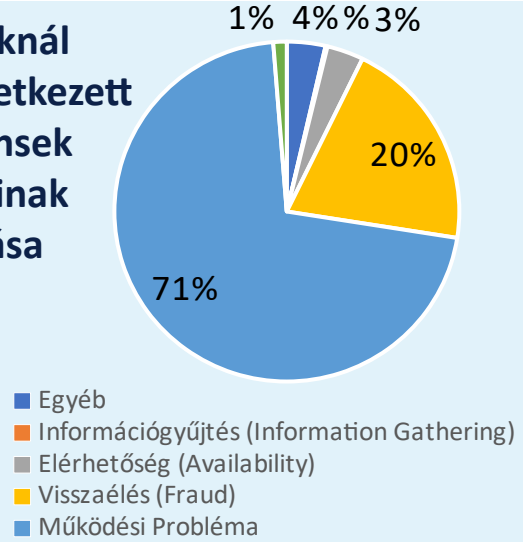
GYÖKÉROKOK MEGOSZLÁSA

intézménytípus és bejelentési hónap alapján

Gyökérokok megoszlása fő kategóriák alapján

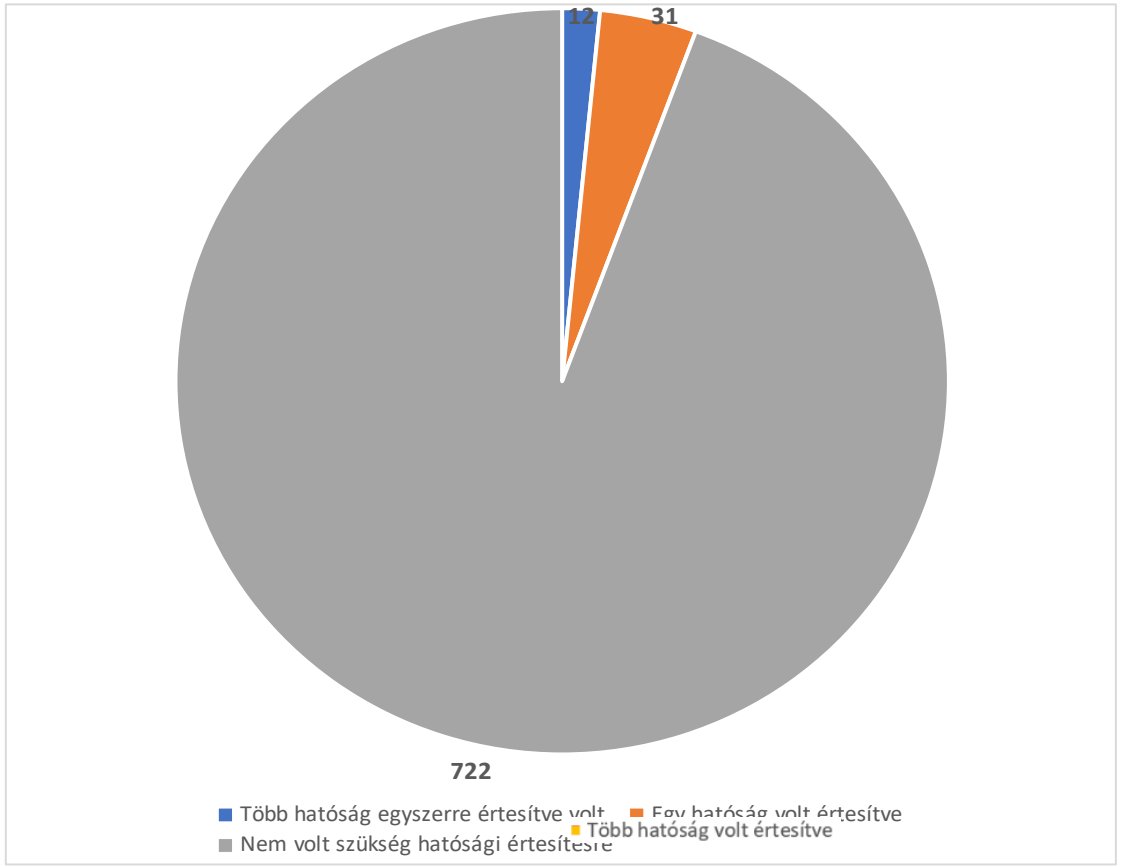


Bankoknál bekövetkezett incidensek típusainak eloszlása



Forrás | MNB

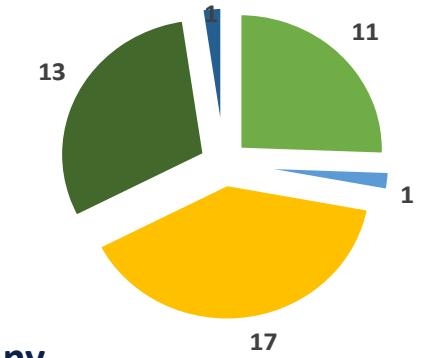
HATÓSÁGOK ÉRTESÍTÉSE AZ INCIDENSEKRŐL



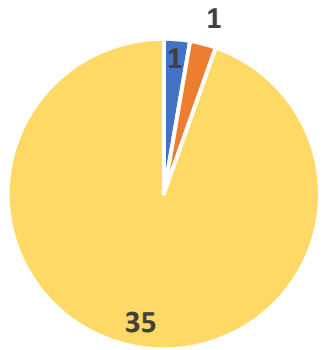
INCIDENS DARABSZÁMOK

a hatóság értesítések függvényében

Hatósági értesítési arány

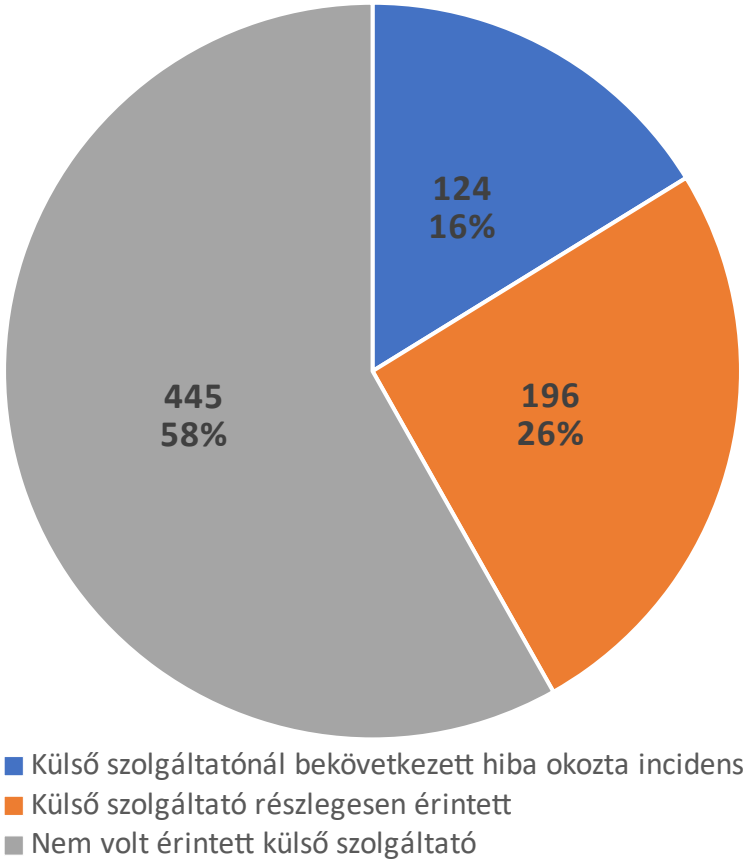


Kritikus incidens darabszám, a hatóság értesítések függvényében



Forrás | MNB

KÜLSŐ SZOLGÁLTATÓK ÉRINTETTSÉGE AZ INCIDENSEKBEN

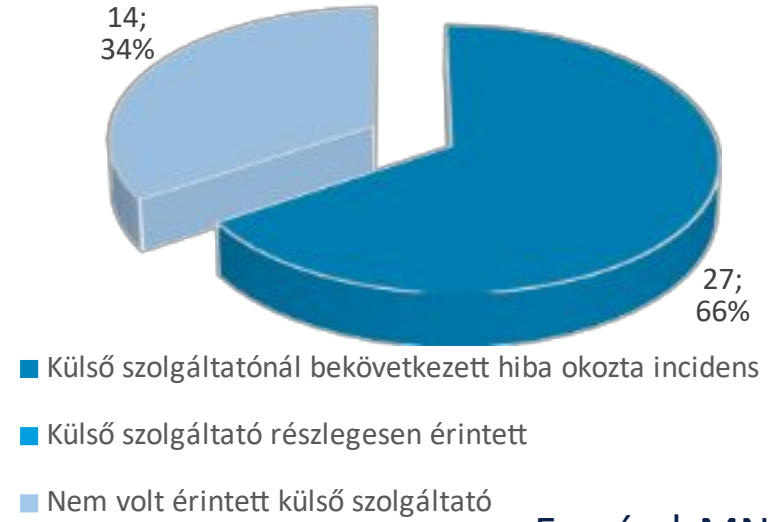


KÜLSŐ SZOLGÁLTATÓI ÉRINTETTSÉG ARÁNYA

a pilot során jelentett incidensekben

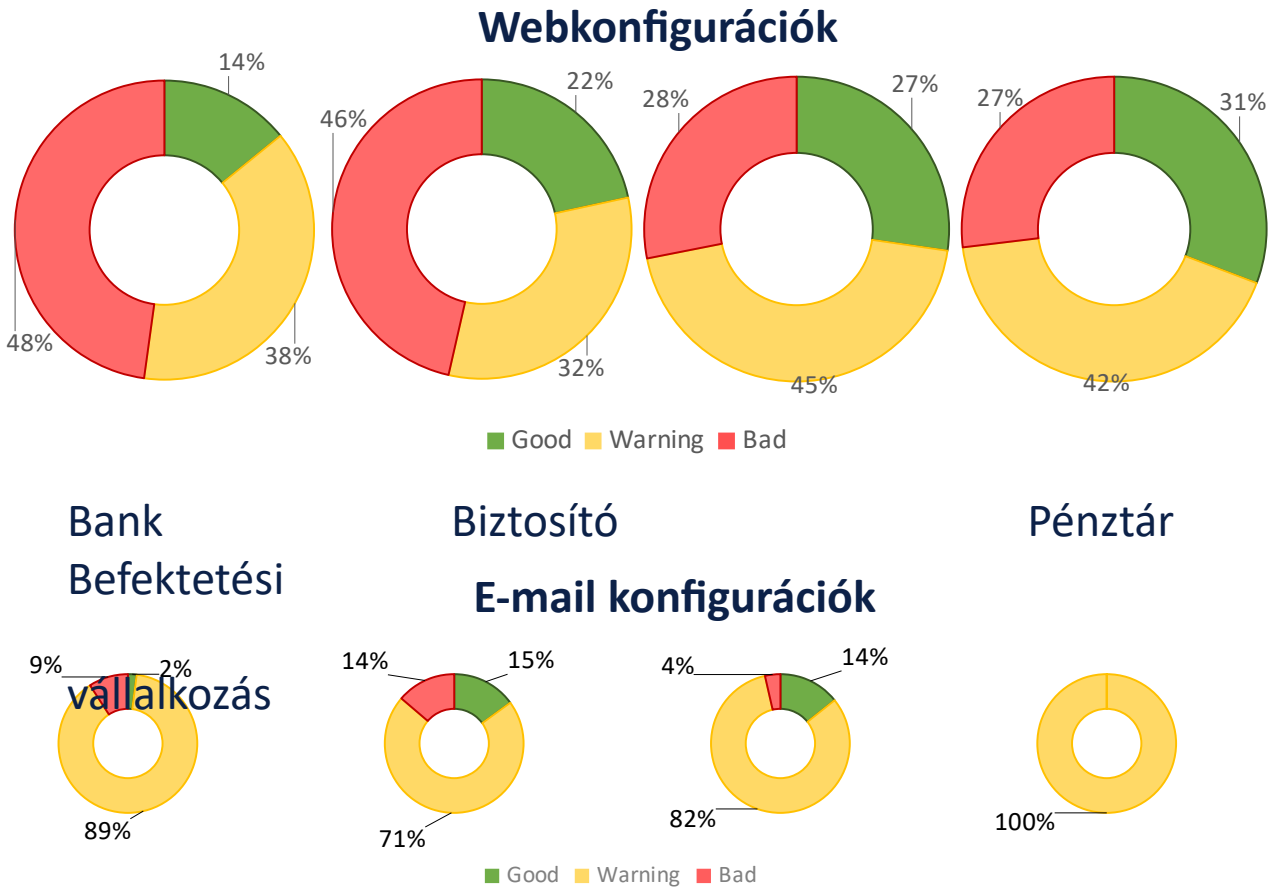
Az incidensek többsége nem érintett külső szolgáltatót – bár a szolgáltatók biztonsága az utóbbi években kiemelt figyelmet kapott.

Kritikus incidens darabszám és arány, ahol volt külső szolgáltatói érintettség



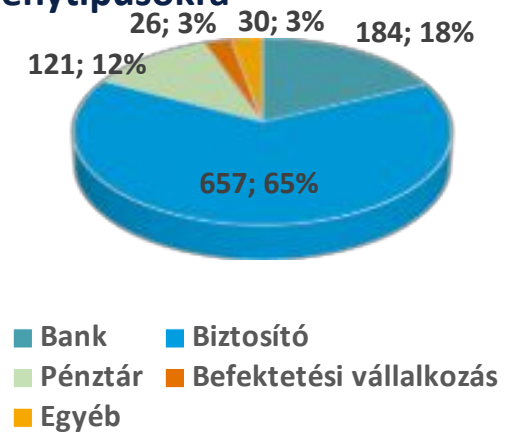
Forrás | MNB

AZ INTÉZMÉNYEK INTERNETES TECHNIKAI BEÁLLÍTÁSAI



Az internet felől látható technikai beállítások gyengeségei nem mutattak összefüggést a bejelentett incidensekkel, ugyanakkor a beállítások sok esetben nem követik a szakmai ajánlásokat.

A domainek száma és aránya az egyes intézménytípusokra



WEB ÉS E-MAIL KONFIGURÁCIÓK

A legtöbb domainnel rendelkező intézménytípusnál

Forrás | MNB & NBSZ-NKI

ÖSSZEFOGLALÓ

- A **nemzetközi trendek** kisebb (néhány hónapos) késéssel Magyarországon is megjelennek.
- A pilotban gyűjtött incidensek döntő többsége (70%) hagyományos értelemben vett **üzemzavar** volt.
- A **nyári hónapokban**, különösen azokban az időszakokban, mikor kevesebb az IT rendszereket érintő változás/frissítés, látványosan **kevesebb** az IT rendszerek működését érintő incidens.
- **A tényleges kibertámadások** – jellemzően az adathalászat különböző formái – **főként az ügyfeleket célozzák**, ezért fontos az ügyfelek biztonságtudatosságának erősítése.
- A pilot során sokkal jobb minőségű incidensadatok érkeztek az MNB-hez, mint a kötelező felügyeleti adatszolgáltatás keretében, és a projektben részt vevő intézmények is pozitív visszajelzést adtak a bejelentések módjáról.
- Nincs kimutatható összefüggés a pilot során gyűjtött incidensek és az intézmények kívülről elérhető internetes biztonsági beállításai közt.

Forrás | MNB

KÖSZÖNÖM A FIGYELMET!

MNB Informatikai Felügyelet aloldal, ajánlások, szakmai anyagok:
https://www.mnb.hu/felugyelet/szabalyozas/informatikai-felugyelet

Forrás | MNB