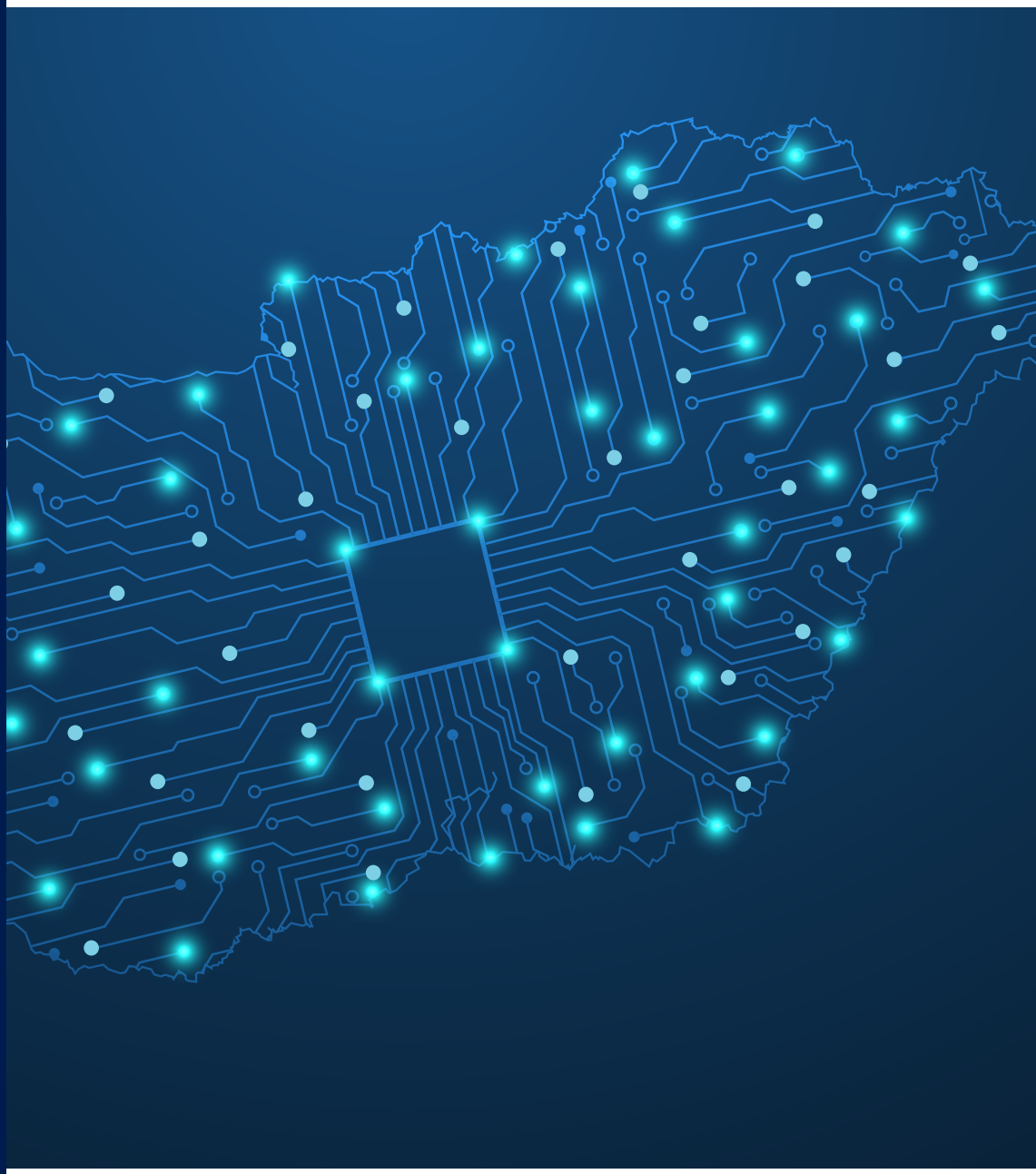
A MAGYAR PÉNZÜGYI SZEKTOR KIBERFENYEGETETTSÉGI TÉRKÉPE 2022



2022
DECEMBER

„A totális biztonság sosem volt elérhető senki számára. Ezt elvárni nem reális; azt képzelni, hogy létezhet ilyesmi, könnyen katasztrófához vezethet.”

Teller Ede

A MAGYAR PÉNZÜGYI SZEKTOR KIBERFENYEGETETTSÉGI TÉRKÉPE 2022

2022
DECEMBER

A magyar pénzügyi szektor kiberfenyegetettségi térképe 2022

(2022. december)

A kiadványt jóváhagyta: Pénzügyi Stabilitási Tanács

Az Európai Unió támogatásával

Kiadja: Magyar Nemzeti Bank

Felelős kiadó: Hergár Eszter

Szerkesztő: Biró Gabriella

1013 Budapest, Krisztina körút 55.

www.mnb.hu

ISSN 2939-7308 (nyomtatott)

ISSN 2939-7383 (on-line)

A Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvény, az árstabilitás elérését és fenntartását tűzte ki a Magyar Nemzeti Bank elsődleges és mindenkori céljaként. A Magyar Nemzeti Bank ezen cél veszélyeztetése nélkül támogatja a pénzügyi közvetítőrendszer stabilitásának fenntartását, ellenállóképességének növelését, a gazdasági növekedéshez való fenntartható hozzájárulásának biztosítását és a rendelkezésére álló eszközökkel a Kormány gazdaságpolitikáját.

A Magyar Nemzeti Bank Felügyeleti stratégiája, a Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvényben megfogalmazott célkitűzést erősítve, a pénzügyi rendszer stabilitásának támogatását és mélyítését jelölte ki 2025-ig fő célkitűzésének. A digitalizációnak köszönhetően az IKT-megoldások és a digitális szolgáltatások jelentősége és az azoktól való függés mértéke folyamatosan növekszik a pénzügyi szektorban, így a pénzügyi rendszer ellenállóképességének megvalósításához kiemelt figyelmet kell szentelni a digitalizációs folyamatokra, azok biztonságára, fenyegetettségeire.

A Magyar Nemzeti Bank e kiadvány keretein belül ismerteti a magyarországi pénzügyi szektor kiberbiztonsági fenyegetettségi helyzetét a 2022. február és augusztus közötti időszakra vonatkozóan. A jelentés célja, hogy megfelelő és átfogó képet kapjunk a jelenlegi fenyegetettségekről és azonosítsuk a főbb trendeket, ezzel is támogatva a pénzügyi szektor szereplőit a számukra releváns fenyegetettségek azonosításában és az azokra való megfelelő felkészülésben. E kiadvánnyal az MNB hozzájárul a pénzügyi szektor és a felügyelt intézmények kiberbiztonsági ellenállóképességének fejlesztéséhez, biztosításához, valamint általánosságban fejleszti a kiberbiztonsági tudatosságot és felkészültséget.

A magyar pénzügyi szektor kiberfenyegetettségi térképe 2022 jelentés az Európai Bizottság (Bizottság) Strukturálisreform-támogatás Főigazgatósága (DG REFORM) által támogatott, „módszertan kidolgozása a pénzügyi szektorban megjelenő kiber fenyegetettségek elemzésére és a fenyegetettségi helyzetkép készítéséhez” című projekt keretében készült. Az elemzést a MNB Informatikai felügyeleti főosztálya készítette.

A jelentésben az MNB szakértői elsősorban a 2022. február 1. és július 31. közötti időszakra vonatkozó információkat használtak fel, különös tekintettel a pénzügyi szektorban megjelenő kiberfenyegetettségek elemzésére és a fenyegetettségi helyzetkép készítéséről szóló projekt keretében megvalósuló pilot projekt során beérkezett incidensadatokra.

Tartalom

I. Vezetői összefoglaló

Jelen kiadvány, a Magyar Nemzeti Bank (a továbbiakban: MNB) **A magyar pénzügyi szektor kiberfenyegetettségi térképe 2022 (Cyber Threat Landscape Report of the Hungarian Financial Sector 2022) című jelentése**, mely összefoglaló képet ad a magyar pénzintézeti szektort érintő főbb kiberbiztonsági fenyegetésekről, az azokkal kapcsolatosan megfigyelhető főbb trendekről, valamint magas szinten bemutatja a hazai pénzügyi szektorban tapasztalt incidenseket.

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

A projekt 2021 szeptemberében vette kezdetét, a pénzügyi szektorban nemzeti szinten található incidensbejelentési kötelezettségek felmérésével, valamint nemzetközi kitekintéssel. Ezek figyelembevételével az incidensek bejelentésére vonatkozó módszertan kidolgozására került sor, majd 39 intézmény (többek közt 12 biztosító, 5 bank, 10 pénztár) részvételével 2022. február 1. és július 31. közt egy hat hónapos pilot projekt keretében megtörtént a részletes incidensadatok összegyűjtése és elemzése, melyekre a jelentés – néhány egyéb adattal kiegészítve – épül.

A jelentés a teljes projekt bemutatása után négy fő részre tagolódik: az általános – nemzetközi és hazai, más szektorokat is érintő – kitekintés után az összes incidens és kiemelten a kritikus incidensek adatai alapján azonosított fenyegetettségi trendek kerülnek bemutatásra, majd a projektben résztvevő intézmények internet felől látható potenciális támadási felületeihez tartozó technikai adatainak vizsgálata és kívülről elérhető biztonsági beállításainak elemzése következik, végül pedig az olvasó módszertani áttekintést kap a pilot során alkalmazott eszközökről és megközelítésekről.

A jelentés főbb tanulságai az alábbiakban összegezhetők:

- a nemzetközi trendek kisebb (néhány hónapos) késéssel Magyarországon is megjelennek, a kockázatok és fenyegetések gyakorlatilag azonosak, vagyis érdemes figyelni különösen az európai eseményeket és azok alapján alakítani a hazai védekezési prioritásokat;
- a pilotban gyűjtött incidensek döntő többsége (70%) hagyományos értelemben vett üzemzavar volt, tehát jelenleg ezek megelőzése és mielőbbi elhárítása hatékonyabb módja a kiberbiztonság fenntartásának, mint a kibertámadásokra összpontosító védelmi intézkedések;
- több forrásból származó adatok alapján a nyári hónapokban, különösen azokban az időszakokban, mikor kevesebb az IT rendszereket érintő változás/frissítés, látványosan kevesebb a rendszerek működését érintő incidens, azaz a körültekintőbb változásmenedzsment fontos eszköz lehet az üzemzavarok megelőzésében;
- a tényleges kibertámadások – jellemzően az adathalászat különböző formái – főként az ügyfeleket célozzák, ezért a védekezés és a károk megelőzése során a technikai védelmi intézkedések mellett fontos az ügyfelek biztonságtudatosságának erősítése;
- a pilot során sokkal részletesebb és jobb minőségű incidensadatok érkeztek az MNB-hez, mint a kötelező felügyeleti adatszolgáltatás keretében és maguk a projektben résztvevő 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.

A magyar pénzügyi szektor kiberfenyegetettségi térképe 2022 jelentés kiadásával maga a projekt még nem zárul le, a módszertani munka folytatódik és várhatóan az incidensbejelentési eljárásrend finomítása után az MNB rendszeresen, évente készít majd hasonló elemzést a rendelkezésre álló adatokból.

II. Bevezetés

A pénzügyi szektort kiemelten érinti a globális digitális transzformációs nyomás, az online és papírmentes megoldásokra való áttérés szükségszerűsége. Az MNB 2022. évi FinTech és Digitalizációs jelentése is rámutatott, hogy *„2021-ben új lendületre kapott a pénzügyi szektor digitális transzformációja. A COVID-19 járványhelyzet, illetve a vele járó ugrásszerű digitalizáció a bővülő pénzügyi szolgáltatási kör mellett az ügyfelek oldalán is egyre nagyobb nyitottságot eredményezett – és egyre több esetben növekvő elvárásokat is – a digitális megoldások igénybevételének lehetőségére*". Mindezek alapján megállapítható, hogy a pénzügyi szolgáltatások terén a szolgáltató, amely nem képes a változó ügyféligényekre kellő gyorsasággal reagálni, az behozhatatlan hátrányt szenvedhet el. A kiélezett versenyben az üzleti célok elérése érdekében az évtizedek óta alkalmazott informatikai megoldások mellett folyamatosan fejlesztésekre, innovációra és új megoldások bevezetésére van szükség. Az eltérő és sokszínű ügyféligények megfelelő kiszolgálása érdekében a hagyományos megoldások mind szélesebb körű alkalmazása, valamint az innovatív technológiák gyors integrációja miatt kiemelten fontossá válik a kiberkockázatok és kiberbiztonság kérdésköre, továbbá a felgyorsult digitalizációs fejlesztések okán az intézményeknek és IT biztonsági szakértőiknek is nagyobb számú és és komplexebb információbiztonsági kockázattal és fenyegetéssel kell szembenézniük.

A hatékony védelmi rendszerek kialakítását és működtetését egyértelműen támogatja, ha az intézmény tudja, hogy szolgáltatásai és tevékenysége alapján melyek aktuálisan azon főbb fenyegetettségek, amelyek ellen biztosan védekeznie kell. Ehhez az elmúlt időszakban tapasztalt incidensek és főbb azonosított fenyegetések összevetése és összegzése nagy segítséget nyújthat. A pénzügyi szektorban ma már általános elvárás, hogy az intézmények monitorozzák, időben észleljék, kezeljék és tartsák nyilván az incidenseiket, sőt az Európai Unió (a továbbiakban: EU), tovább mélyíti és szigorítja ezt a követelményrendszert az általa kidolgozott digitális ellenállóképességi rendelet, ún. DORA rendelet (Digital Operational Resilience Act) segítségével, annak érdekében, hogy a pénzügyi szektor intézményei minél nagyobb digitális ellenállóképességre tegyenek szert egységesen EU-szerte.

Az észlelt incidensekhez köthető információt azonban – többek között azok bizalmas jellege miatt – a legtöbb intézmény házon belül dolgozza fel. Ennek eredményeként a szektorban intézményi szinten kiváló mikro-tudásközpontok jöhetnek létre. Ugyanakkor a szigetszerű működési modell miatt a szektoriális szintű fenyegetettségi adatok összevetésére, elemzésére, megosztására és az esetleges összefüggések kimutatására a magyarországi pénzügyi szektor szereplőinek a gyakorlatban korlátozott lehetőségeik vannak.

Ezt a hiányosságot, valamint az intézményeknél elszórtan rendelkezésre álló tudásbázis kiaknázásának lehetőségét az MNB azonosította és kezdeményezte a „*Módszertan kidolgozása a pénzügyi szektorban megjelenő kiber fenyegetettségek elemzésére és a fenyegetettségi helyzetkép készítéséhez*" című EU-s támogatású projektet.

A projekt keretében az MNB építve a meglévő incidens és fenyegetettségi információkra, valamint az EU által a DORA rendeletben megfogalmazott törekvésére, miszerint a pénzügy szektorban előforduló incidenseket és esetleges fenyegetéseket a tagállami hatóságok fogják gyűjteni, kezdeményezte egy olyan módszertan kidolgozását, mely ezen adatok felhasználását és a pénzügyi szektor intézményeinek való visszamutatását lehetővé teszi. Azaz a rendelkezésre álló adatok felhasználásával az MNB célja, hogy hiánypótló kiadványként létrehozza Magyarország első szektorspecifikus kiberfenyegetettségi térképét. A fenyegetettségi térkép létrehozásával és publikálásával az MNB határozott célja, hogy a teljes hazai pénzügyi szektort támogatni tudja átfogó, valós, egy meghatározott időszakra vonatkozó szektorspecifikus fenyegetettségi elemzéssel. Az MNB véleménye szerint mindez hozzásegíti az intézményeket a mind hatékonyabb védekezési és kockázatmenedzsment feladatok megtervezéséhez, működtetéséhez és finomhangolásához, valamint a kiberbiztonsági prioritások megfelelő meghatározásához. Az aktuális fenyegetések megelőzése és az azokra való felkészülés támogatja a pénzügyi szolgáltatások hatékony működését, stabilitását és integritását, valamint segíti az intézményeket, hogy meg tudják előzni az események miatt bekövetkező veszteségeket, károkat vagy szolgáltatáskimaradásokat.

A projekt részfeladata volt hat hónapos időtartamban a projekthez csatlakozó intézmények részéről beküldött incidensbejelentések befogadása és feldolgozása. A kiadványban bemutatott elemzések alapját a pénzügyi szektorban működő szereplők napi éles működése során azonosított incidensek adatai biztosították. Ennek köszönhetően a projekt során olyan adatstruktúra került felépítésre, mely korábban Magyarországon nem állt rendelkezésre. Az adatok feldolgozása során lehetőség nyílt mélyebb, szektorszintű összefüggések megkeresésére, melyek a IV. fejezetben (Azonosított fenyegetettségi trendek bemutatása) kerülnek részletesen kifejtésre.

A kiberfenyegetettségi térkép összefoglalva megmutatja a pénzügyi szektorban tapasztalható incidensek jellemzőit, azok különböző tulajdonságaikat, illetve bizonyos esetekben a kezelésük módját.

A kiadvány széles célközönséget igyekszik megszólítani:

Elsődlegesen a pénzügyi szektor intézményeinek felső vezetői, döntéshozói és IT biztonsággal foglalkozó szakértői számára tartalmaz fontos és hasznos információkat, adatokat. A felsővezetők számára a kiadvány egy átfogó kiberfenyegetettségi helyzetképet mutat be, mely segít megérteni és általánosságban átlátni, hogy milyen fenyegetettségekkel nézhet szembe az intézmény. A döntéshozók számára megfelelő rálátást biztosíthat az adott időszak (előző év vagy félév) főbb fenyegetettségeiről és incidenseiről a szektorban, mely alapján azonosítani tudják, hogy a trendek (és saját fejlettségük) figyelembevételével mely területekre kell nagyobb hangsúly fektetniük (akár már a kockázatelemzés keretében). Az IT biztonsággal foglalkozó szakemberek pedig a kiadvány és annak a kérdéseket is bemutató V. fejezete alapján a védelmi megoldások megtervezése, előkészítése vagy módosítása során tudják a bemutatott információkat alkalmazni.

Másrészt pedig a kiadvány a pénzügyi szektor intézményei számára szolgáltatásokat nyújtó szolgáltatókat is tudja orientálni, hasznos információkkal ellátni, hogy mik a jellemzőbb incidensek az adott szektorban vagy intézményi típusnál.

1. AZ MNB KIBERFENYEGETETTSÉGI TÉRKÉP PROJEKT BEMUTATÁSA

A fentiek alapján az MNB, az EU digitális ellenállóképesség növelésére vonatkozó céljaival összhangban, felismerte annak jelentőségét és szükségességét, hogy megfelelő és átfogó kép kialakítása szükséges a pénzügyi szektor aktuális fenyegetettségeiről, hogy azonosíthatóvá váljanak a főbb trendek, és ezekre fókuszálva az MNB-nek lehetősége legyen segíteni és támogatni az intézményeket a főbb fenyegetettségekre való felkészülésben.

Sajnos jelenleg Magyarországon a pénzügyi szektort ért támadásokról, incidensekről és főbb fenyegetettségekről csak részleges információk állnak az érintettek rendelkezésére, hiszen jelenleg nincs átfogó, minden intézményre kötelező incidensbejelentési kötelezettség megfogalmazva (sem az MNB, sem pedig a pénzügyi szektor eseménykezelését támogató Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (a továbbiakban: NBSZ-NKI) Számítógép-biztonsági és Incidenskezelő Csoportja (NBSZ-NKI CSIRT) részéről).

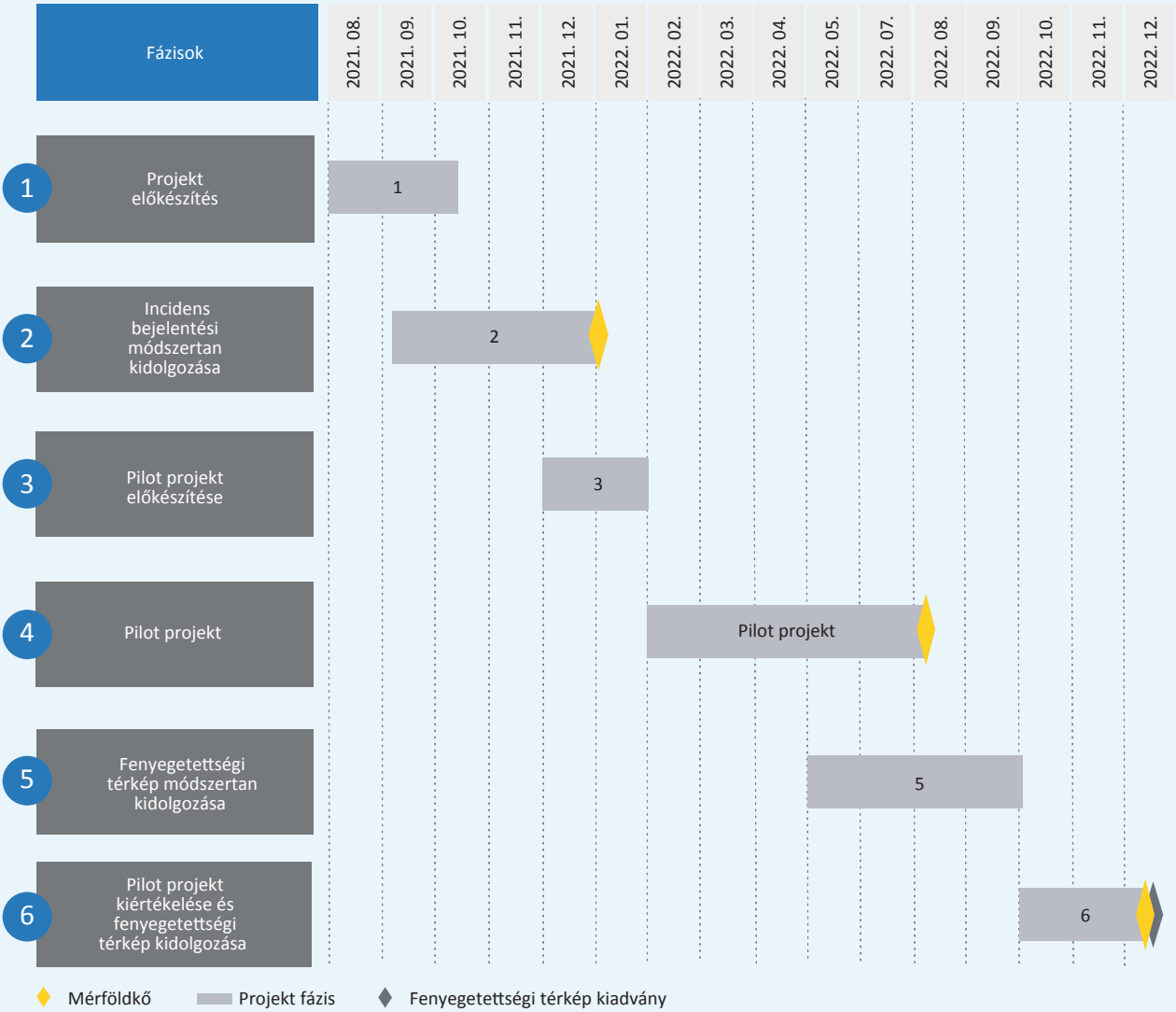
Az MNB a már létező és kialakítás alatt álló EU-s és nemzeti jogszabályi elvárások, valamint a nemzetközi jó gyakorlatok figyelembevételével olyan módszertan kidolgozását tűzte ki célul, mely megfelelő képet ad a pénzügyi szektort ért kibertámadásokról, incidensekről és főbb fenyegetettségekről. Így a jelentős fenyegetések kezelésére az MNB a rendelkezésére álló eszközökkel nagyobb hangsúlyt tud fektetni. Az általános főbb kiberkockázatok és fenyegetések áttekintése, valamint az ágazatspecifikus trendek azonosítása támogatni tudja az intézmény szintű kockázatkezelési akciótervek megfogalmazását, melyek segítségével a piaci szereplők hatékonyabban reagálhatnak a kibertér eseményeinek alakulására.

A fenti célkitűzés megvalósítására az MNB elhatározta a pénzügyi szektor kiberfenyegetettségi térképének elkészítését, mely projektje a Bizottság Strukturálisreform-támogatás Főigazgatósága (DG REFORM) által meghirdetett Technikai Támogatási Eszköz 2021. évre vonatkozó pályázaton támogatást nyert. A projekt végrehajtásában a Bizottság döntése alapján az Ernst & Young Consulting Ltd. magyarországi irodája segítette az MNB-t. A projekt 2021 szeptemberében vette kezdetét, a pénzügyi szektorban nemzeti szinten található incidensbejelentési kötelezettségek felmérésével, valamint nemzetközi kitekintéssel. A három hónapos előkészítő fázis alatt számos európai hatósággal történt egyeztetés. A tapasztalatok alapján levonható volt az a következtetés, hogy a tervezett szektorális kiberfenyegetettségi térképhez egy új alapokra helyezett incidens jelentési keretrendszer kialakítására lesz szükség. Az előzetes információs követelmények számos létező és tervezett jelentési keretrendszert figyelembe véve, a nemzetközi tapasztalatok és legjobb gyakorlatok alapján kerültek

meghatározásra. Ezt követően az MNB kialakított egy új, szélesebb hatókörű incidensbejelentési keretrendszert, amelyet egy pilot projekt (a továbbiakban: Pilot) keretében tesztelt.

A Pilot projekt fontos célja, volt, hogy az intézmények minél szélesebb köre tudjon csatlakozni a programhoz. Cél volt továbbá, hogy minél több formalizált adat kerülhessen összegyűjtésre, rendszerezésre és elemzésre. Ezért egy hat hónapos pilot időszak (2022. február 1. – 2022. július 31.) került meghatározásra, mely során a Pilot projektben részt vevő intézmények az újonnan kialakított módszertan szerint tájékoztatták az MNB-t az incidenseikről és azok részleteiről. A Pilot projekthez 39 intézmény csatlakozott önkéntes alapon, amelyek különféle pénzügyi szolgáltatásokat nyújtanak. Öt bank, tizenkét biztosító, pénzügyi infrastruktúrák, befektetési vállalkozások, alapkezelők, biztosítási alkuszok, valamint pénztárak is szerepet vállaltak a Pilot projektben. A 39 intézmény vezetői szinten megállapodást írt alá az MNB-vel, majd szakértői szinten módszertani oktatást kapott az incidensbejelentési folyamatról.

1. ábra
Az MNB kiberfenyegetettségi térkép kiadvány projektterve



A Pilot projekthez csatlakozó intézmények – a külön erre a célra kifejlesztett bejelentési űrlapok segítségével – kétféle jelentési feladatot vállaltak magukra: egyrészt havonta küldtek havi bejelentéseket, amelyek minden, az adott hónapban történt kritikus és nem kritikus incidenseik összefoglalására szolgáltak, másrészt a havi jelentéseken túl a kritikus incidensek kapcsán azonnali, részletes jelzéseket is küldtek. Ez az incidensbejelentési keretrendszer, amelynek részét képezték

külön erre a célra kifejlesztett bejelentési űrlapok, tette lehetővé a jelen kiadvány legfőbb részét képező adatvezérelt következtetések levonását.

2. ábra
A jelentések típusai és azok elemei

Az intézményeknek a havi jelentésekben minden olyan informatikai biztonsági incidensről jelenteniük kellett, amely egy előre nem látható esemény következtében kedvezőtlen hatással volt az informatikai hálózatára vagy az információs rendszerekre, és a bennük tárolt vagy általuk kezelt adatokra. Továbbá az incidensek egy része az MNB által kidolgozott szempontrendszer alapján (kritikus funkciót támogató rendszerek érintettsége, ügyféladatok, pénzügyi ágazati titok, például banktitok vagy értékpapírtitok nyilvánosságra kerülése) kritikusnak minősülhet, amelyekhez részletesebb jelentési kötelezettség társult. A kritikus incidensekhez három szintű jelzési kötelezettség tartozott: a kezdeti jelzés, az időközi jelzések és a záró jelzés. Az alábbi esetekben biztosan kritikusnak volt tekinthető az incidens:

- a sajtó érdeklődésének homlokterébe kerülő események esetén;
- több ügyfelet érintő banktitoknak, fizetési titoknak, biztosítási titoknak, értékpapírtitoknak, pénztártitoknak minősülő személyes adat illetéktelen személyhez kerülésekor (például adatszivárgás, sikeres adathalászat);
- az informatikai rendszerben több ügyfelet érintő adatmódosítást eredményező jogosulatlan tevékenység esetén (például külső vagy belső visszaélés);
- az intézmény üzleti hatáselemzése (Business Impact Analysis – BIA) alapján kritikusnak tekintett szolgáltatásokra az előreláthatólag 1 órát meghaladó kiesésről vagy a normál szolgáltatási szinttől elmaradó szolgáltatások esetén, külön kiemelve az alábbi területeket:
  - elektronikus csatornák (online értékesítési csatornák, fizetési kártya, internetbank és elektronikus fizetések)
  - hitelintézetek, befektetési vállalkozások és befektetési alapok esetén számlavezetés.

A projekt kifejezett célja volt, hogy az új struktúrában és szélesebb körben történő incidensbejelentések során begyűjtött és feldolgozott adatok elemzésének eredménye minél pontosabb képet tudjon adni olyan fenyegetettségi területekről és trendekről, melyekről a megelőző időszakban nem állt rendelkezésre kellő mennyiségű információ. További célkitűzés volt, hogy a bejelentés folyamatának új formáját tesztelni lehessen éles környezetben. Így „valós terepen" szerzett értékes gyakorlati tapasztalatokkal lehet majd támogatni a jövőbeli, incidensbejelentéseket támogató rendszerek és folyamatok fejlesztésére irányuló törekvéseket, kezdeményezéseket. A Pilot projekt során új struktúrában és széles körben jelentettek incidenseket a résztvevő intézmények. A Pilot projekt végével a kiberfenyegetettségi térkép kiadvány projekt következő fázisa jelen riport kidolgozása volt.

III. Általános kitekintés

2020-ban a COVID-19 okozta járványhelyzet világszerte elősegítette a digitalizációs folyamatok felgyorsulását a pénzügyi szektorban is. A transzformációs folyamatok 2021-ben tovább erősödtek, mivel a hatóságok által elrendelt lakhelyelhagyási tilalmak és az üzleti folyamatokat megnehezítő bizonytalanság rugalmasságra és innovációra ösztönözte a pénzügyi szolgáltatókat. A pandémiával kapcsolatos kiberbiztonsági fenyegetések és az „új normális" kihasználására tett kísérletek általánossá váltak. Ahogy az MNB FinTech és Digitalizációs jelentése is rámutat, ennek ellenére 2021-ben a pénzforgalmi folyamatok sok tekintetben visszatértek a koronavírus-járvány előtti mederbe, és bár a COVID-19 továbbra is jelen volt a mindennapokban, a pénzforgalmi szolgáltatók[1] megtanulták folyamataikban kezelni a pandémiás helyzet utóhatásait[2]. Elmondható, hogy az összes pénzügyi szolgáltató a pénzforgalmi szolgáltatókhoz hasonlóan viselkedett, vagyis a pandémia után kezdtek visszatérni a járvány előtti megszokott folyamatokhoz. A pénzforgalmi szolgáltatók közül a banki pénzforgalmi szolgáltatók számossága a legnagyobb, ezért a banki pénzforgalmi szolgáltatók digitalizációra vonatkozó magatartása előre jelezheti az egész pénzügyi szektor alkalmazkodási folyamatait.

1. ÁLTALÁNOS FENYEGETETTSÉGI TRENDEK

1. táblázat
ENISA legfőbb fenyegetések listája 2021-ben

Rangsor	Fenyegetések	Trend
1	Zsarolóvírusok	↑
2	Rosszindulatú programok	↓
3	Cryptojacking	↑
4	E-mailekkel kapcsolatos fenyegetések	↑
5	Az adatokkal szembeni fenyegetések	↑
6	A rendelkezésre állás és az integritás elleni fenyegetések	↑
7	Dezinformáció	↑
8	Nem rosszindulatú fenyegetések	↑
9	Ellátási láncok elleni fenyegetések	↑

Az Európai Uniós Kiberbiztonsági Ügynökség (a továbbiakban: ENISA) által készített Fenyegetettségi térkép (ENISA Threat Landscape – a továbbiakban: ETL) fő célja, hogy bemutassa az adott tárgyévre vonatkozó kiberbiztonsági környezetet. Az ETL azonosítja az elsődleges fenyegetéseket, a fenyegetésekkel kapcsolatban megfigyelt főbb trendeket, támadókat és támadási technikákat. Az ETL-ben korlátozott információ és adat áll rendelkezésünkre a korábbi pénzügyi szektort érintő trendekről és eseményekről, általános (nem ágazatspecifikus és nem átfogó) fenyegetettségi elemzéseket mutat be.

A korábbi ENISA ETL kiadványok[3] szerint 2017-ben, 2018-ban és 2020-ban a leggyakoribb fenyegetések a rosszindulatú programok (úgynevezett malware támadások), a web alapú támadások, valamint a webalkalmazásokat ért támadások voltak. A jól ismert elosztott szolgáltatásmegtagadás (DDoS – Distributed Denial of Service, elosztott szolgáltatásmegtagadás) és adathalász támadások egyaránt megjelentek a hat leggyakoribb fenyegetés között. 2019-ben nem készült ETL, azonban az adatokat a következő évi jelentés tartalmazza.

[1] A hatályos szabályozás alapján pénzforgalmi szolgáltatónak minősülnek – a fenyegetettségi térkép szempontjából releváns intézmények közül – a bankok, a pénzforgalmi intézmények és az elektronikuspénz-kibocsátó intézmények.
[2] MNB – FinTech és Digitalizációs jelentés 2022. június (Elérhető: https://www.mnb.hu/letoltes/fintech-es-digitalizacios-jelentes-2022.pdf)
[3] ENISA Threat Landscape through the years (Elérhető: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape) és ENISA Threat Landscape 2021 (Elérhető: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021)

Az ETL 2021-es kiadványa a 2020 áprilisa és 2021 júliusa között keletkezett fenyegetettségi információkat vette figyelembe, amely során az ENISA ETL munkacsoport kollégái kilenc fő fenyegetést azonosítottak (1. táblázat). Első helyen szerepel 2021-ben a zsarolóvírusok kategória, amelyet az év legfőbb fenyegetésének tekinti az ETL. Új elem a toplistán az ellátási láncok ellen irányuló fenyegetések, amely az ENISA véleménye szerint különös jelentőséggel bír a 2021-es évre vonatkozóan. Indoklásuk szerint a külső szolgáltatók rendkívül nagy értékű célpontokat képviselnek a kiberbűnözők számára. Az ENISA egy külön jelentésben[4] is elemezte ezt a fenyegetést, ezzel is hangsúlyozva jelentőségét. Az ENISA szerint a következő évek meghatározó kiberbiztonsági kockázatait az ellátási láncokban kell keresnünk, mely jóslat igaznak bizonyult, hiszen a fenyegetés a következő évi ETL-ben is a legfontosabbak közt szerepel.

Az ENISA 2022-es Fenyegetettségi térkép kiadványa[5] a 2021 júliusa és 2022 júliusa között keletkezett fenyegetettségi információkra épít a globális és európai fenyegetettségi trendek elemzésénél. A 2022-es kiadvány alapján továbbra is a zsarolóvírusok és a rosszindulatú programok voltak a legelterjedtebb fenyegetések (2. táblázat), azonban 2022-ben újdonságként a megtévesztésen alapuló támadás vagy pszichológiai manipuláció (social engineering) immár a fenyegetettségi toplista 3. helyén szerepelt.

2. táblázat
ENISA legfőbb fenyegetések listája 2022-ben

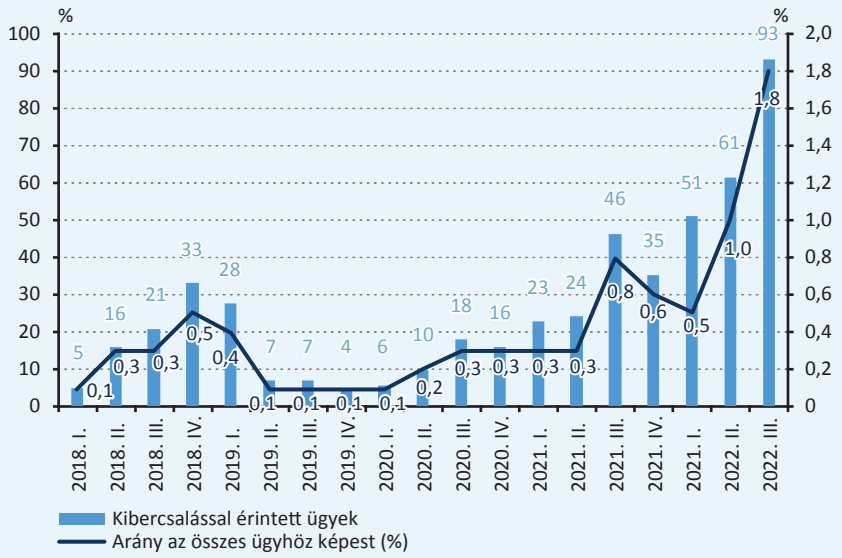
Rangsor	Fenyegetések	Trend
1	Zsarolóvírusok	→
2	Rosszindulatú programok	→
3	Megtévesztésen alapuló támadás	↑
4	Az adatokkal szembeni fenyegetések	↑
5	A rendelkezésre állás elleni fenyegetések: DDoS	↑
6	A rendelkezésre állás elleni fenyegetések: internetes fenyegetések	→
7	Dezinformáció	→
8	Ellátási láncok elleni fenyegetések	↑

Ami a fenyegetettségi trendek alakulását illeti, a jelentési időszakra vonatkozóan az ENISA kiemeli, hogy a támadók továbbra is egyre szofisztikáltabban és célzottan hajtják végre támadásaikat. Egyre inkább jellemző a kritikus infrastruktúrák támadása, vagy érintettsége és a mesterséges intelligencia használata. Ezért a kormányzati szervek nemzeti és nemzetközi szinten is fokozták szerepüket, együttműködésüket és védekezési kapacitásaikat.

A kiberbűnözőket gyakran motiválja tevékenységük pénzzé tétele, például zsarolóvírusok használatával. 2018-ban, amikor az ún. kriptovaluták (például BTC, ETH) kezdtek elterjedni az egész világban, megjelent az ezeket érintő új fenyegetés, a cryptojacking, amely engedély nélküli kriptovaluta bányászatot jelent, mások informatikai eszközeinek felhasználásával. 2018-ban máris a 13. helyen állt a 15 legjelentősebb fenyegetés listáján, és 2020-ban is a lista 15. helyén szerepelt. A kriptovaluta továbbra is a leggyakoribb kifizetési mód a kiberbűnözők számára, rekordmagasságot ért el 2021-es évben a cryptojacking támadások száma és a fenyegetettségi toplista 3. helyén állt, azonban 2022-ben már nem jutott be a legfőbb fenyegetések listájába. Az egyre nagyobb médiavisszhangnak örvendő sikeres támadások, és a „zsarolóvírus mint szolgáltatás" (Ransomware-as-a-Service – RaaS) elterjedése miatt 2021 júniusára közel duplájára nőtt a támadások havi értéke és ez a tendencia 2022-ben is töretlen. A zsarolóvírus támadások hirtelen megugrása mögött több tényező is állhat. Kiemelt kockázatot jelent, hogy a rosszindulatú kódkomponensek viszonylag könnyen hozzáférhetők, megvásárolhatók, így a kiberbűnözés technikai belépési akadálya nagy mértékben csökkent az elmúlt években. Ilyen lehet például a zsarolóvírus, szolgáltatásmegtagadás, adathalászat és félretájékoztatás szolgáltatása. A bűnöző magas technikai tudás nélkül is sikeresen megtámadhat személyeket vagy akár intézményeket is. Háromból kettő zsarolóvírus támadás „zsarolóvírus mint szolgáltatás" igénybevételével történik.

[4] Threat Landscape for Supply Chain Attacks (Elérhető: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks)
[5] ENISA Threat Landscape 2022 (Elérhető: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022)

3. ábra
Kibervisszaélés témájú ügyféljelzések számának alakulása az MNB ügyfélszolgálaton



A kibervisszaélések (3. ábra), az adathalász fenyegetések, valamint a megtévesztésen alapuló visszaélések egyre inkább elterjedtek, és megfigyelhető, hogy a csalók egyre szofisztikáltabb megoldásokat alkalmaznak annak érdekében, hogy elrejtsék a visszaélési kísérleteket. A támadások egyre hitelesebbé válnak, a visszaélések egyre jobban igazodtak a különböző elkövetési csatornák kontextusához, és az egy adott hónapban jelentett adathalász támadások száma 2020 eleje és 2021 vége között megháromszorozódott, a 2022-es ETL szerint pedig az adathalászat a legelterjedtebb támadási vektor – akár más típusú támadások kiindulópontjaként is. A támadók gyakran kihasználják, hogy a felhasználók mostanra belefáradtak a megnövekedett arányú távmunkába (user fatigue). A célpontok gyakran a pénzügyi szektor tagjai, illetve ügyfelei[6]. Az MNB kibervisszaéléssel kapcsolatos tapasztalatai (19. ábra) azt mutatják, hogy 2022 első felére a legelterjedtebb támadási forma a hamis banki telefonhívás, más szóval az úgynevezett vishing (voice phishing – hang- (telefonhívás) alapú adathalászat támadás. Mindezzel egybevágnak az NBSZ-NKI, alapvető szoltáltatást nyújtó pénzügyi intézményeket érintő tapasztalatai (3. táblázat). Ezek alapján a Pilot projekt alatt azonosított 19 incidens között van megszemélyesítés típusú előrehaladott adathalász támadás. A COVID-19 továbbra is domináns téma az adathalász támadásokkal kapcsolatos kampányokban, valamint az üzleti e-mail visszaélés (business- e-mail compromise – BEC) és CEO típusú, vagyis a vezetői vagy üzleti e-mail címmel elkövetett visszaélések is megsokasodtak, kifinomultabbak lettek és egyre szélesebb kört céloztak a 2021-es és 2022-es év során. Ezen visszaélések során az áldozatot hamis beszállítói vagy vezetői üzenetekkel próbálják rávenni, hogy nagyobb összegeket utaljanak el a bűnözők által megadott számlákra[7].

[6] APWG – Phishing Activity Trends Report 1st Quarter 2021. (Elérhető: https://docs.apwg.org/reports/apwg_trends_report_q1_2021.pdf?_ga=2.100477661.234220476.1663894927-96135508.1660773867&_gl=1*1sfq8wd*_ga*OTYxMzU1MDguMTY2MDc3Mzg2Nw..*_ga_55RF0R-HXSR*MTY2Mzg5NDkyNy4yLjAuMTY2Mzg5NDkyNy4wLjAuMA..)

[7] Lásd például az MNB – Pénzügyi Navigátor oldalát a Hamis vezetői utasítás e-mailben vagy telefonon (Elérhető: https://www.mnb.hu/fogyasztovedelem/digitalis-biztonsag/az-adathalasz-csalasok-legjellemzobb-tipusai/hamis-vezetoi-utasitas-e-mailben-vagy-telefonon)

3. táblázat
Alapvető szoltáltatást nyújtó pénzügyi intézményeket érintő NBSZ-NKI által megfigyelt incidensek, 2022. február 1. és július 31. közötti időszak

Fenyegetések	Incidens darabszámok
DDoS	3
DoS	1
Információbiztonság (Information Security)	1
Információgyűjtés (Information Gathering)	9
Ismeretlen típusú káros kód	3
Megszemélyesítés (Masquerade)	1
SPAM	3

A 2021-es jelentés alapján 2020-ban már megfigyelhető volt a rosszindulatú programok használatának a csökkenése. Ez a tendencia 2021-ben is folytatódott, azonban érzékelhető volt egy jelentős fejlődés a kártékony kódok kifinomultságát illetően. A hagyományos DDoS kampányok 2021-ben szintén célzottabbak és sokkal kitartóbbak lettek, és egyre szélesebb felületet érintenek. A nemzetközi trendekkel összhangban Magyarországot is 2020 végén érte el az első igazán jelentősnek mondható, sajtóvisszhangot is kiváltó DDoS támadási hullám. Érdekesség, hogy 2020-ban és 2021-ben a nem rosszindulatú gyökérokhoz visszavezethető incidensek erős növekedését mutattak.

Az Intsights LLC. (a továbbiakban: Intsights) rendszeresen készít egy fenyegetési helyzetelemzést és jelentést (Banking & Financial Services CyberThreat Landscape Report) a pénzügyi szektorra vonatkozóan, amely összefoglalja a leggyakoribb támadástípusokat. A 2018-as adatokat elemző jelentésük szerint az összes az évi malware támadás 25,7 százaléka a banki és pénzügyi szolgáltatásokat vette célba (Intsights, 2019[8]) és ezen trend folyamatos növekedése figyelhető meg. Ez komoly kockázatot jelent a pénzügyi szektor számára, mivel az EU-s szintű leggyakoribb fenyegetésnek (az ENISA előző években kiadott jelentései szerint) a rosszindulatú programokat alkalmazó malware támadások számítottak.

Az Intsights 2019-es fenyegetettségi riportja szerint 129 százalékkal nőt éves szinten a felhasználói hitelesítő adatok (felhasználónév, jelszó) kiszivárgásával kapcsolatos incidensek száma, míg az ellopott hitelkártya-adatokhoz kapcsolódó esetek 212 százalékkal, a rosszindulatú alkalmazások segítségével megvalósuló mobilbanki támadások esetszáma pedig 102 százalékkal növekedett.

Az Intsights következő, 2021-es fenyegetettségi riportja[9] feltárta a kibertámadók által használt leggyakoribb támadási vektorokat. A jelentés alapján a banki és pénzügyi szolgáltató intézmények ellen irányuló sikeres kibertámadások bizonyítékot szolgáltatnak arra, hogy a hackerek egyre inkább együttműködnek a támadások kivitelezésében. Az Intsights tapasztalatai azt mutatták, hogy 2020-ban és 2021-ben a banki és pénzügyi szektort érintő legjelentősebb fenyegetések a kompromittált hitelkártyák és a banki hálózatok ellen irányuló támadások voltak, amelyeket a támadók többek között trójai vírusok használatával valósítottak meg. Az ENISA kiadvánnyal összhangban a jelentés azonosította, hogy egyre gyakoribbak a más iparágakban működő harmadik felek ellen irányuló támadások, amelyek közvetetten veszélyeztetik a pénzügyi szektort.

[8] Intsights – Banking & Financial Services Cyber Threat Landscape Report (April 2019) (Elérhető: https://intsights.com/resources/banking-financial-services-cyber-threat-landscape-report-april-2019)
[9] Insights – Banking and Financial Services Industry Cyber Threat Landscape Report 2021 (Elérhető: https://intsights.com/resources/2021-banking-and-financial-services-industry-cyber-threat-landscape-report)

A folyamatos kiberfenyegetések egyre inkább a pénzügyi szektor működésének velejárói. A különböző szolgáltatások digitális csatornákon történő igénybevételének elterjedése – amit a COVID-19 világjárvány csak felgyorsított – érdemben megnövelte az intézmények, valamint a pénzügyi szektor ügyfeleinek a kitettségét. Az ügyfelek a digitális pénzügyi szolgáltatások felhasználóiként könnyen találhatják magukat kiberfenyegetések célkeresztjében. Az egyre kifinomultabbá váló rosszindulatú támadások ezt a megnövekedett támadási felületet igyekeznek kihasználni haszonszerzés céljából, mind intézményi, mind ügyféloldalról. Ezen kockázatok ellensúlyozására fókuszálnak a nemzeti és nemzetközi szabályzói törekvések, illetve a biztonsági kontrollok folyamatos fejlődésének hatására a fenyegetettségi térkép is évről évre változik.

2. NEMZETKÖZILEG AZONOSÍTOTT TÁMADÓI CSOPORTOK

A nemzetállamok által támogatott szereplők (hírszerzés, hackercsoportok, kollektívák) már 2021-ben is a legnagyobb kiberkockázatot jelentő szereplők voltak az ENISA fenyegetettségi térkép alapján. A pandémiás helyzethez köthető hírszerzési tevékenységek (például gyógyszergyártók vagy a World Health Organization megtámadása) mellett feltételezhetően nemzetállamok által támogatott szereplők követték el a legnagyobb ellátási láncokat érintő támadásokat. Az ENISA adatai alapján különböző APT csoportok (Advanced Persistent Threat group) voltak felelősök a 2020 és 2021 között bekövetkezett ellátási láncokat érintő támadások több mint feléért. Ezeknek a szereplőknek a kibertérben kifejtett tevékenységeit állami stratégiák, geopolitikai aktualitások, és nem utolsósorban fegyveres konfliktusok határozzák meg.

A 2022-es év egy meghatározó eseménye a február 24-én kirobbant orosz-ukrán háború, amely a kibertérben is jelentős változásokat eredményezett. A kibertér az ötödik hadszíntérnek tekinthető[10], a fizikai konfliktus mellett pedig a kibertérben is jelentős, a háborúhoz köthető támadások történtek és dezinformációs műveletek zajlottak, miközben új védekezési módok – például az Amerikai Egyesült Államok által alkalmazott úgynevezett „hunt forward”[11] – is megjelentek. A különböző hackercsoportok (ideértve a bűnözői csoportokat is) jelentős része állást foglalt a háborúban és tevékenységével bevallottan az orosz vagy az ukrán felet segíti/segítette, ugyanakkor az eltelt hónapok alatt megfigyelhető egyfajta átrendeződés is: egyes csoportok kiszálltak a konfliktusból vagy teljesen eltűntek, míg újabb szereplők is megjelentek a Cyberknow portál[12] adatai szerint (4. ábra).

[10] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2017. (Elérhető: https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9)
[11] BBC: Inside a US military cyber team’s defence of Ukraine (Elérhető: https://www.bbc.com/news/uk-63328398)
[12] Elérhető: https://twitter.com/Cyberknow20

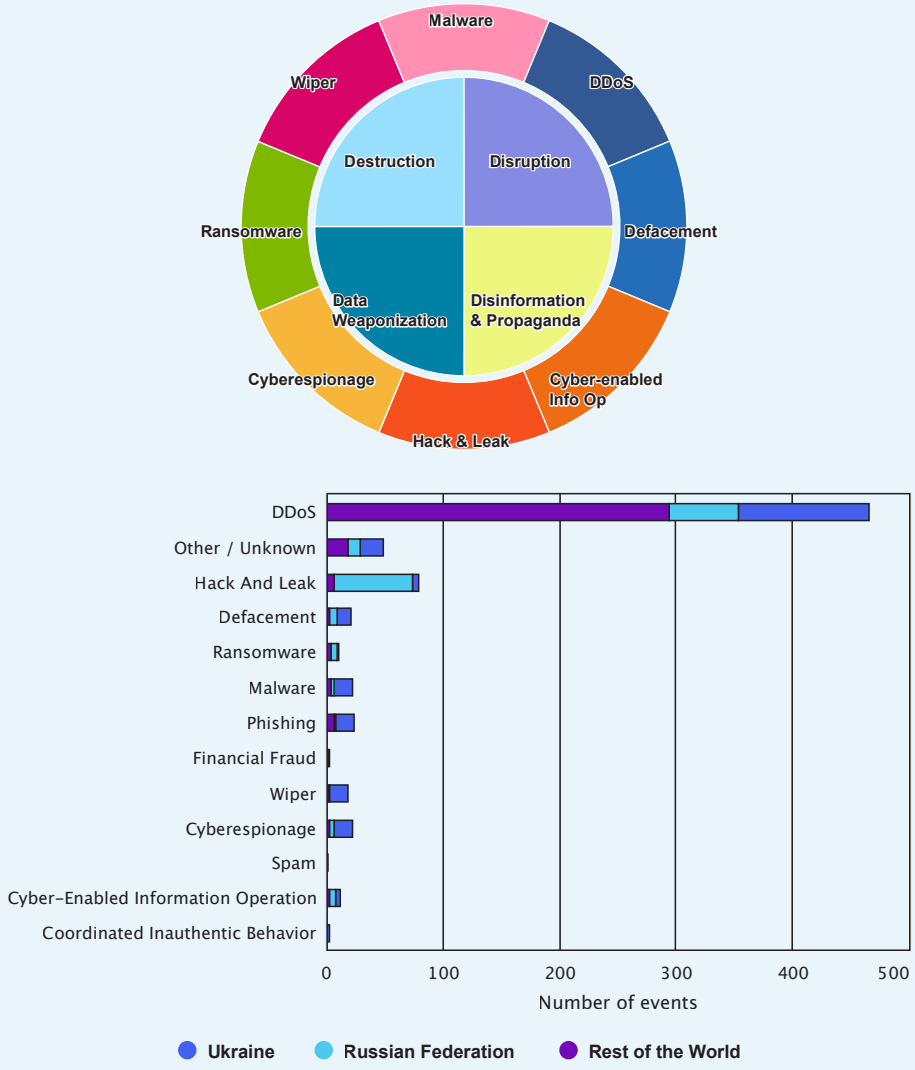
4. ábra
Oroszbarát és Ukrajna párti hackercsoportok a Cyberknow portál adatai szerint, 2022. október 12-i állapot

12 OCT 2022_CYBERKNOW_CYBERTRACKER_RUSSIA_UKRAINEWAR

Support	Name	Actions	Comms	Support	Name	Actions	Comms	Support	Name	Actions	Comms
Ukraine	SHDWSec(Anon)	Hack/DDos	Twitter	Russia	RaHDit	Hack	Telegram	UNK	Elon Musk	Psyop	Twitter
Ukraine	N3UR0515(Anon)	DDos	Twitter	Russia	Xaknet	Hack	Telegram				
Ukraine	Squad303(Anon)	DDos/SMS	Twitter	Russia	Killnet	DDos	Telegram				
Ukraine	GhostSec(Anon)	Hack	Twitter	Russia	DDoS Hacktivist Tea	DDos	Telegram	State-Sponsored			
Ukraine	RedCult(Anon)	Hack/DDos	Twitter	Russia	Zsecnet	Dox/DDos	Telegram	Russia	GhostWriter	Hack	UNK
Ukraine	KelvinSecurity Hacking Team	Hack	Twitter	Russia	DivisionZ	DDos	Telegram	Russia	SandWorm	Hack/Wiper	UNK
Ukraine	SecJuice	OSIN/Psyop	Twitter	Russia	ZOV cyber army	Hack/Psyops	Telegram	Russia	Gamaredon	Hack/Wiper	UNK
Ukraine	Belarusian Cyber-partisans	Ransomware	Twitter	Russia	Cyber Front Z	Psyop/Dox	Telegram	Russia	DEV-0586	Hack/Wiper	UNK
Ukraine	BeeHive Cybersecurity	Hack/Sec	Twitter	Russia	Info Front Z	Psyop/DDos	Telegram	Russia	DEV-0665	Hack/Wiper	UNK
Ukraine	Stand for Ukraine	Hack/DDos	Twitter	Russia	Cyber Army of Russia	DDos/psyops	Telegram	Russia	FancyBear/AOT28	Hack/Wiper	UNK
Ukraine	HackenClub	Hack/DDos	Twitter	Russia	Legion	DDos	Telegram	Ukraine	IT Army of Ukraine	DDos	Telegram
Ukraine	DumpFormus	Hack	Twitter	Russia	Beregini	Pysop/Dox	Telegram	Ukraine	Internet Forces os Ukraine	pysops	UNK
Ukraine	studentcyberarmy	DDos	Twitter	Russia	NoName057(16)	Ddos/Hack	Telegram	Ukraine	OS CyberCom	Hack	UNK
Ukraine	Onefist	Hack/DDos	Twitter	Russia	ZSNOSINT	Pysop/Dox	Telegram	UNK	MustangPanda	Hack	UNK
Ukraine	CybWar	Ddos/Leaks	Twitter	Russia	FRwLteam	Hack/DDos	Telegram	UNK	CuriousGeorge	Hack	UNK
Ukraine	KromSec	Hack/DDos	Twitter	Russia	Zarya	Hack	Telegram	Russia	TurlaAPT	Hack	UNK
Ukraine	KiraSec	Hack/DDos	Twitter	Russia	RedHackersAlliance	DDos	Telegram	Russia	SaintBear/TA471	Hack	UNK
Ukraine	CyberSoldier	DDos	Twitter	Russia	Blood Pirates	DDos	Telegram	UNK	TontoTeam	Hack	UNK
Ukraine	CyberPalyanitsa	DDos	Twitter	Russia	Wizard Spider(Trickbot Cerw)	Ransomware	Telegram	UNK	SpacePirates	Hack	UNK
Ukraine	Haydamaki	DDos	Twitter	Russia	Anonymous Russia	DDos	Telegram	UNK	Scarab	Hack	UNK
Ukraine	Ciberwars	DDos	Twitter	Russia	NBP Hackers	DDos/Hack	Telegram	Russia	Calisto	Hack	UNK
Ukraine	Ddos_saper	DDos	Twitter	Russia	Phoenix	DDos/Hack	Telegram				
Ukraine	2402Team	Hack	Twitter	Russia	KillMilk	DDos/Hack	Telegram	KEY:			
Ukraine	DarkWolf	Ddos/Deface	Twitter	Russia	Altahrea Team	DDos/Hack	Telegram	Total Groups		84	
Ukraine	Thraxman	Hack	Twitter	Russia	JokerDRP	Psyops/Dox	Telegram	Added		11	
Ukraine	NAFO	Psyop/Meme	Twitter	Russia	1877Team	DDos/Deface/Hack	Telegram	Removed		11	
Ukraine	Op Anonymous Italia Reborn	Hack	Twitter	Russia	QBotDDos(Mirai)	Ddos/Botnet	Telegram		Is for New Groups		
Ukraine	Saint Javelin	Psyops	Twitter	Russia	Osminogbotnet	Ddos/Botnet	Telegram	Pro-Russian		42	
Ukraine	National Republican Army-Cyber	Ransomware	Twitter	Russia	KoranAttack	DDos/Doxx	Telegram	Pro-Ukraine		36	
Ukraine	SUDORM-RF	Hack	Twitter	Russia	ohhackers	DDos	Telegram	UNK 6			
Ukraine	Zazu Group	DDos/Hack	Twitter	Russia	Russian Hackers Team	DDos	Telegram				
Ukraine	R00T*R4q3	Ddos/Dox	Twitter	Russia	DDos Sia Project	DDos	Telegram				
Ukraine	Altro-A	DDos	Twitter	Russia	Solaris	DDos/Forum	Telegram				

Az orosz-ukrán háború kontextusában a 2022-es év meghatározó kérdése, hogy az orosz-ukrán háború kibertérben megvalósuló eseményei hogyan hatnak ki a különböző szektorok kiberbiztonságára, milyen következményekkel, esetleges támadásokkal számolhatnak a különböző szektorok szereplői a háborús országokban, illetve világszerte. Az eseményeket elemző CyberPeace Institute[13] 2022. október 18-áig 564 kibertámadást (heti átlag 13,8 darabot) azonosított, melyhez 61 különböző elkövetőt tudtak kötni. A támadástípusok közt döntően a DDoS dominál (5. ábra), ugyanakkor feltehetően az adatlopást vagy lehallgatást célzó támadások döntő többsége nem kerül nyilvánosságra.

5. ábra
Az orosz-ukrán háború kontextusában megfigyelt fenyegetések és támadások



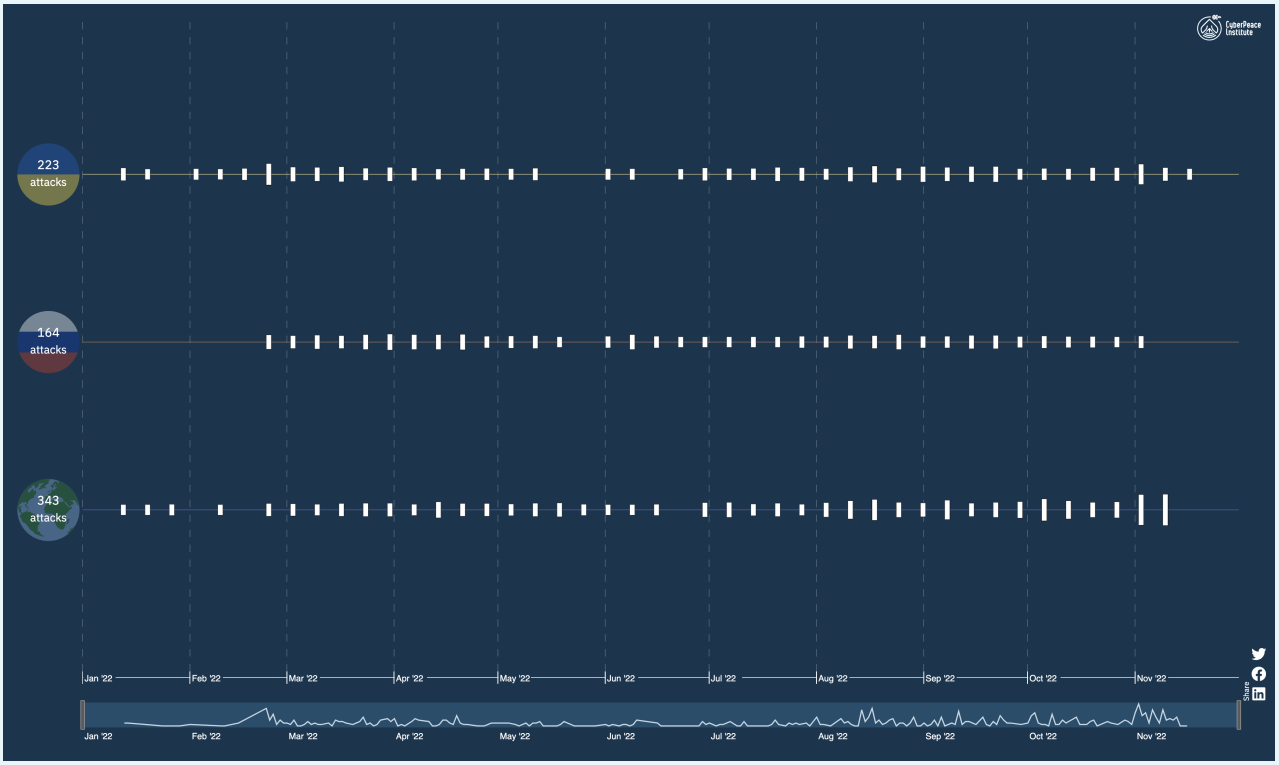
Forrás: https://cyberconflicts.cyberpeaceinstitute.org/threats

Jól látható, hogy a háború kezdete a fizikai térben egybeesik a kibertérben megnövekedett aktivitással (6. ábra). Ugyanakkor az elemzések azt is megmutatják, hogy elsősorban nem a pénzintézeti szektor került célkeresztbe sem az orosz, sem az ukrán oldalon (7. ábra), amit a 2022-es ETL adatai is megerősítenek. Európai szinten is fokozott éberségre intett a legtöbb felügyeleti hatóság, azonban tényleges kibertámadást csak viszonylag kevés szereplő szenvedett el a háború következtében, sőt az is elmondható, hogy az egyéb támadások számossága is csökkent a pénzintézeti szektorban. Ennek

[13] Elérhető: https://cyberconflicts.cyberpeaceinstitute.org/

okát nagyon nehéz egyértelműen megállapítani, de a különböző hackercsoportok aktivitását elemezve sejthető, hogy a háborús konfliktusban való önkéntes szerepvállalás a kiberbűnözésre specializálódott csoportok részéről jelentős erőforrásokat kötött le különösen a háború első heteiben.

6. ábra
Az orosz-ukrán háborúhoz köthető kibertámadások időbeli eloszlása célpontok szerint az összes szektorra



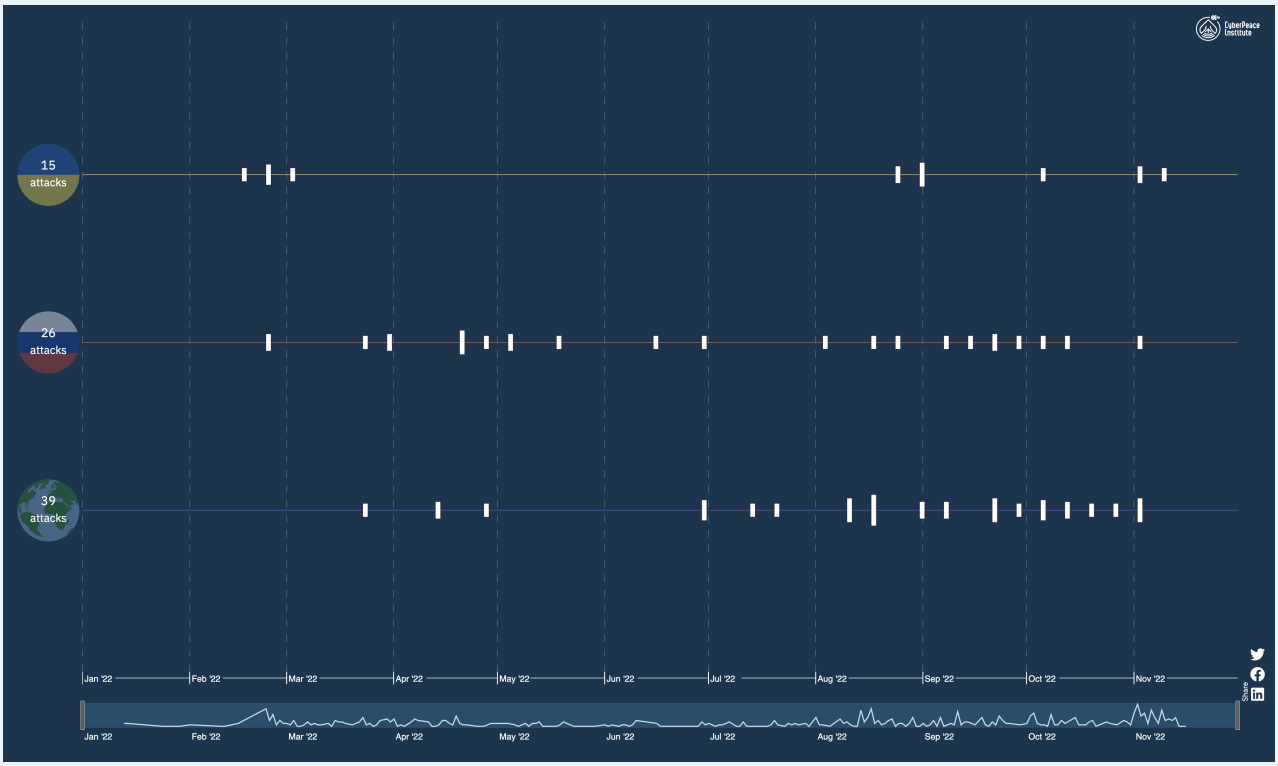
Forrás: https://cyberconflicts.cyberpeaceinstitute.org/threats/timeline.

A kiberbűnözői szereplőkkel kapcsolatos trendek, továbbá a motivációik és a célpontjaik megértése nagyban segíti a tervezést a kiberbiztonsági védelemi és kockázatcsökkentési stratégiák kidolgozásában. Az ENISA fenyegetettségi térképe a következő, kiberbiztonságot fenyegető szereplőket azonosította:

- nemzetállamok által támogatott szereplők;
- kiberbűnözők;
- szabadúszó hackerek;
- hacktivisták.

A CyberKnow és a CyberPeace intézet adatai is azt mutatják, hogy mind az Ukrajnával, mind az Oroszországgal szimpatizáló legnagyobb kibertérbeli szereplők a hacker kollektívák és a feltehetően nemzetállamok által támogatott szereplők kategóriába sorolhatóak. Ebből valószínűsíthető, hogy tevékenységüket – legalábbis a háború vonatkozásában – nem az anyagi haszonszerzés motiválja, ezért sem a pénzintézetek az elsődleges célpontjaik.

7. ábra
Az orosz-ukrán háborúhoz köthető kibertámadások időbeli eloszlása célpontok szerint a pénzügyi szektorban



Forrás: https://cyberconflicts.cyberpeaceinstitute.org/threats/timeline.

A nemzetközi kitekintés és egyéb elérhető statisztikák áttekintése, valamint a riport által felölelt időszak főbb politikai és geopolitikai értékelése, valamint a szereplők azonosítása a fenyegetésértékelés szerves részét képezi, mivel lehetővé teszi a Magyarországon azonosított trendek kontextusba helyezését, a biztonsági ellenőrzések fontossági sorrendbe állítását és egy dedikált stratégia kidolgozását a lehetséges fenyegetések és hatások bekövetkezésének megakadályozására.

3. NEMZETKÖZI SZABÁLYOZÓI KEZDEMÉNYEZÉSEK

Az intenzív digitalizációt és az abból adódó egyre több és komplexebb kiberbiztonsági kihívás jelentőségét az EU is felismerte és erre válaszul számos jogalkotási javaslatot fogalmazott meg, illetve több korábbi EU-s követelmény felülvizsgálatát és modernizációját kezdeményezte.

A Bizottság 2020. szeptember 24-én mutatta be a Digitális Pénzügyi Csomag (Digital Finance Package – DFP) javaslatát, mely magába foglal egy az innovációt és versenyt ösztönző, a fogyasztók védelmét erősítő és a kockázatokat csökkenteni kívánó Digitális pénzügyi szolgáltatási stratégiát[14], egy lakossági pénzforgalmi stratégiát az EU-s szintű teljesen integrált lakossági fizetési rendszer létrehozása érdekében, valamint a stratégiák és a teljes digitális pénzügyi csomag célkitűzéseinek megvalósítását támogató három jogalkotási javaslatot:

- A kriptoeszközök piacaira vonatkozó rendelettervezet (Markets in Crypto-assets – MICA rendelet[15]). A rendelet célja, hogy az eddigi hatályos uniós jogi normák hatálya alá nem tartozó kriptoeszközök kibocsátására és a hozzájuk tartozó szolgáltatások nyújtására vonatkozóan egységes uniós szintű követelményeket fogalmazzon meg, valamint, hogy lehetőség szerint enyhítse ezen kriptoeszközökhöz kapcsolódó felhasználói kockázatokat.

[14] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának az uniós digitális pénzügyi szolgáltatási stratégiáról (Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52020DC0591&from=EN)
[15] Európai bizottsági javaslat a kriptoeszközök piacairól és az (EU) 2019/1937 irányelv módosításáról szóló európai parlamenti és tanácsi rendeletről (Elérhető: https://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX%3A52020PC0593)

- A megosztott főkönyvi technológián (Distributed Ledger Technology – DLT) alapuló piaci infrastruktúrák kísérleti rendszeréről szóló rendelettervezet (DLT pilot rendelet)[16]. A rendelet egy kísérleti rendszert teremt meg a blokklánc alapon működő pénzügyi eszközök – ideértve az értékpapírokat is – kibocsátására és elszámolására a már működési engedéllyel rendelkező értékpapír-elszámolási rendszerek és multilaterális kereskedési rendszerek számára.

- A pénzügyi ágazat digitális működési ellenállóképességéről szóló rendelettervezet (DORA rendelet)[17]. A rendelet fő célja, hogy az innováció és a verseny tekintetében még inkább lehetővé tegye és támogassa a digitális pénzügyi szolgáltatásokban rejlő potenciál kiaknázását, ugyanakkor mérsékelje az ezekből eredő kockázatokat és erősítse a pénzügyi szektor digitális ellenállóképességét, valamint a tagállamokban jelenleg uralkodó eltérő felügyeleti gyakorlatokat harmonizálja, egységesítse. A rendelet a fenti célkitűzéseknek megfelelően részletes követelményrendszert fogalmaz meg az információs és kommunikációs technológiákhoz (IKT) kapcsolódó kockázatok kezelésére, a tesztelésre, valamint a pénzügyi intézményeknek IKT szolgáltatásokat nyújtó harmadik fél szolgáltatók kezelésére vonatkozóan. Továbbá egységes incidensbejelentési kötelezettséget és fenyegetettség riportálási lehetőséget ír elő a hatálya alá tartozó pénzügyi szektor szereplőinek, melynek segítségével a nemzeti és európai felügyeleti hatóságok megfelelő rálátást kaphatnak a pénzügyi szektorban előforduló jelentősebb incidensek körére, főbb fenyegetési és incidens trendekre.

A DORA rendelet tárgyalását és mielőbbi elfogadását kiemelt fontosságúvá tette a COVID-19 okozta járványhelyzetben tapasztalt kényszerű és gyors digitális transzformáció, az idei évben pedig az orosz-ukrán háborúból adódó számos kiberbiztonsági kihívás.

Mindeközben a pénzügyi szektor egyes kijelölt szereplőit (alapvető szolgáltatók) is érintő hálózat- és információbiztonsági irányelv (NIS irányelv) felülvizsgálata is megkezdődött, melynek köszönhetően 2022 májusában az Európai Unió Tanácsa, az Európai Parlament és a Bizottság megállapodtak a hálózat- és információbiztonsági irányelv módosításáról (NIS2 irányelv). A jogalkotók célja, hogy összehangolják a NIS2 irányelv előírásait az ágazatspecifikus jogszabályokkal, így pedig a DORA rendelettel és a kritikus fontosságú intézmények rezilienciájáról szóló irányelvvel (CER irányelv), hogy jogi egyértelműséget teremtsen, valamint garantálja a NIS2 irányelv és a többi vonatkozó jogi aktus közötti koherenciát.

Összességében elmondható, hogy az EU-s jogalkotók is reagáltak az elmúlt években megnövekedett fenyegetésekre és az újonnan megjelenő kihívásokra, így az elkövetkező években már ezen EU-s szintű szabályozások és elvárások végrehajtásával is tudjuk növelni a pénzügyi szektor kiberbiztonsági ellenállóképességét, valamint naprakészebb, pontosabb képet tudunk kapni az aktuális kihívásokról, fenyegetettségekről.

[16] Európai bizottsági javaslat a megosztott főkönyvi technológián alapuló piaci infrastruktúrák kísérleti rendszeréről szóló európai paralmaneti és tanácsi rendeletről (Elérhető: https://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX%3A52020PC0594)

[17] Európai bizottsági javaslat a pénzügyi ágazat digitális működési rezilienciájáról és az 1060/2009/EK rendelet, a 648/2012/EU rendelet, a 600/2014/EU rendelet, valamint a 909/2014/EU rendelet módosításáról szóló európai parlamenti és tanácsi rendeletről (Elérhető: https://eur-lex.europa.eu/legal-content/hu/TXT/PDF/?uri=COM:2020:595:FIN&rid=1)

IV. Azonosított fenyegetettségi trendek bemutatása

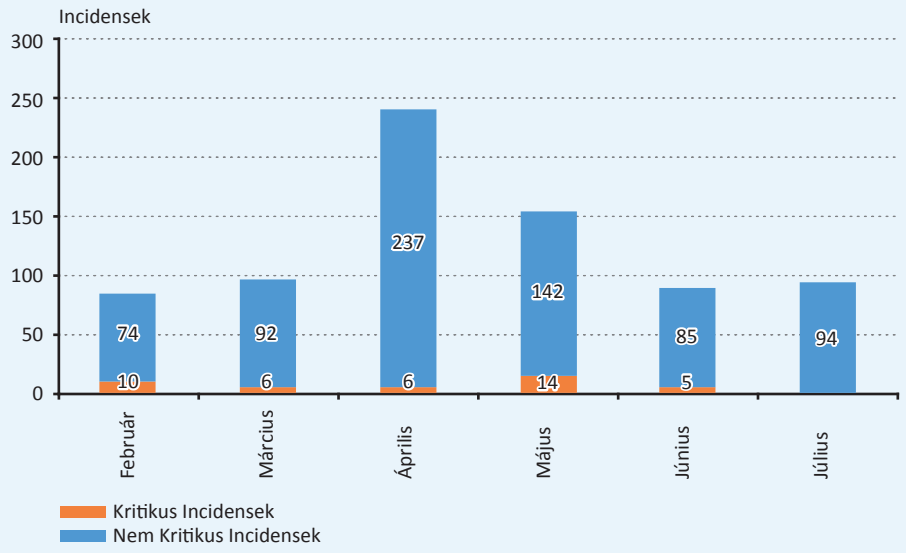
A kiberfenyegetettségi térképet létrehozó projekt előkészítési szakaszában meghatározásra került, hogy incidensbejelentés esetén milyen adatokat kell az intézményeknek rögzíteniük az incidensbejelentő űrlap segítségével. Egyrészt cél volt az, hogy az érintett intézmények az incidens elhárítása alatt minél egyszerűbb adatszolgáltatási folyamattal találkozzanak, ezért az űrlap adatstruktúrájának kialakítása során kiemelt figyelmet kellett fordítani arra, hogy csak a legszükségesebb adatokra kérdezzen rá. Ugyanakkor fontos volt az is, hogy a szolgáltatott adatokból az utólagos követéshez, feldolgozáshoz és a jövőbeli tanulságok levonásához elégséges adat álljon rendelkezésre.

A pilot projekt időszakában összegyűjtött adatok alapján elvégzett elemzések eredményei a következő alfejezetekben kerülnek bemutatásra. Az incidensek adatait kiegészítettük más forrásból – az MNB Ügyfélszolgálati Információs Központja által a rendelkezésünkre bocsátott, valamint a jegybanki információs rendszerhez elsődlegesen a Magyar Nemzeti Bank alapvető feladatai ellátása érdekében teljesítendő adatszolgáltatási kötelezettségekről szóló 54/2021. (XI. 23.) MNB rendeletben meghatározott P58 MNB azonosító kódú adatszolgáltatásból – származó adatokkal. Területekre lebontva külön alfejezetekben találhatóak a feldolgozott incidensbejelentések általános elemzései, az intézménytípusok incidensbejelentéseinek elemzése, a bejelentett incidensek mélységi elemzése, valamint a hatósági értesítés és külső szolgáltatói érintettség elemzése. A fejezet végén az elemzésekből azonosítható fenyegetettségi trendekre vonatkozó következtetések összefoglalása következik. Az egyes területeken belül külön elemzésre kerültek a teljes incidenspopulációra vonatkozó bejelentések, melyek tartalmaznak minden bejelentést (a kritikus és a nem kritikus incidenseket is). Ahol értelmezhető volt, ott külön elemzések készültek a kritikus incidensbejelentések adataira vonatkozóan. A könnyebb összehasonlíthatóság érdekében külön ábrákkal kerülnek bemutatásra az azonos területen elvégzett, teljes incidens populációra-, illetve csak kritikus incidenspopulációsra vonatkozó elemzések.

1. INCIDENSBEJELENTÉSEK ÁLTALÁNOS ELEMZÉSE

A fenyegetettségi térkép által felölelt hathónapos adatgyűjtési időszak alatt az MNB összességében 765 incidensről értesült a projektben részt vevő intézményektől. (8. ábra).

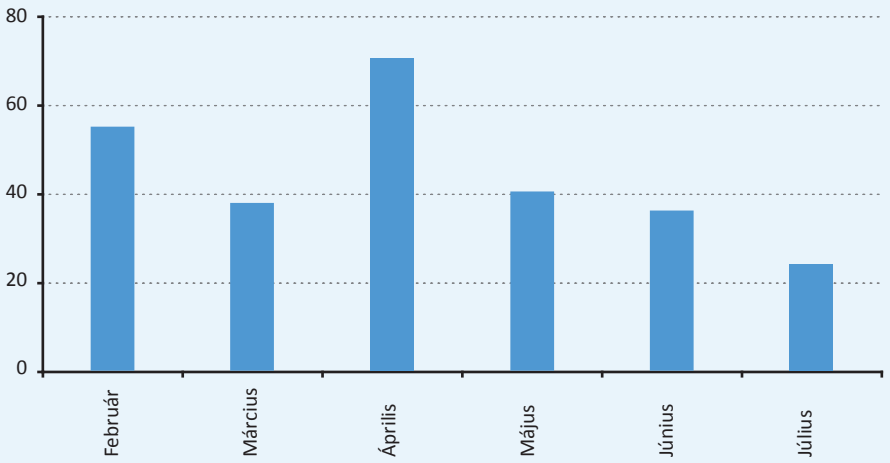
8. ábra
Incidens darabszámok bejelentési hónap alapján



Az elemzés egyik fontos célkitűzése volt, hogy megvizsgálja a februári és márciusi bevezetési időszakot követő áprilisi és májusi kiugró értékeket, ahol egy szignifikáns növekedés azonosítható a bejelentett incidensek darabszámában. Az ezt követő júniusi és júliusi időszakban újra kevesebb bejelentés érkezett.

A kiugró időszak egy lehetséges magyarázata – ami a projekt előkészítés során is azonosított kockázatként szerepelt – egy esetleges felfutási időszak, amely keretében a csatlakozott intézmények bevezetik és belső rutinná formálják az új incidensbejelentési folyamatot. Ugyanakkor a nyers adatok elemzése során kiderült, hogy csak néhány intézményhez köthető a kiugró incidensjelentési tevékenység eredményeként előálló áprilisi és májusi incidens darabszám.

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

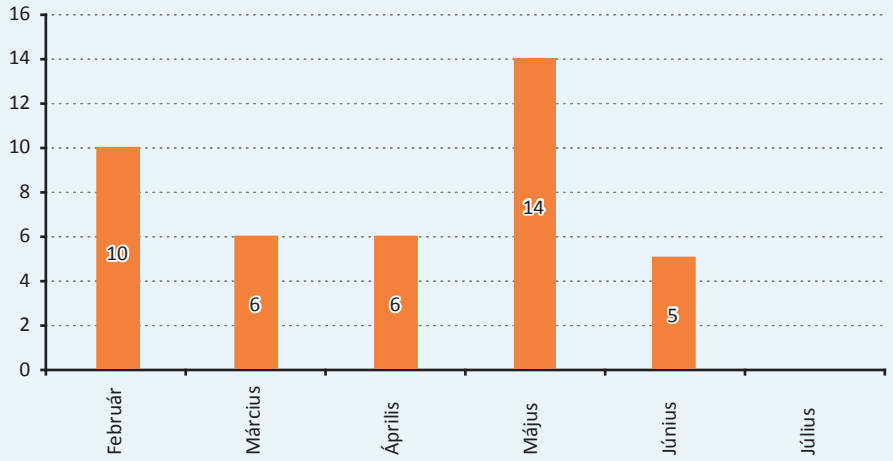


A június és július hónapok alacsonyabb eseményszámai kapcsán pedig feltételezhető, hogy a nyári szezon és szabadságolások okán a fejlesztési és a jelentősebb szoftverfrissítési feladatok száma csökkent, és a feladatok az őszi hónapokra kerültek beütemezésre. Ezt támasztják alá az Eseti nyilatkozat pénzforgalmi szolgáltatást érintő üzemzavarról szóló P58 MNB azonosító kódú adatszolgáltatás havi eloszlási adatai is (9. ábra), melyek az incidensbejelentésekhez hasonló mintázatokat mutatnak. Az áprilisi és májusi kiugró értékeket leszámítva a statisztikából a havi bejelentések átlagdarabszámát a nyári időszak nem befolyásolta jelentősen. Összességében megállapítható, hogy a felfutási időszak első két hónapjában a bejelentések nem okoztak érzékelhető nehézséget a Pilot projekthez csatlakozott intézményeknek.

A teljes bejelentett incidenspopulációhoz képest a kritikus incidensek arányát vizsgálva megállapítható, hogy összességében négy százalék alatt volt a kritikus incidensek aránya.

A kritikus incidensek darabszámainak mintázata illeszkedik az összesített havi bejelentési eredményekhez. A Pilot projekt során a kritikus incidensek esetében is megfigyelhető volt egy stabil havi bejelentési átlag darabszám (10. ábra).

10. ábra
Incidens darabszámok bejelentési hónap alapján (kritikus incidensek esetén)



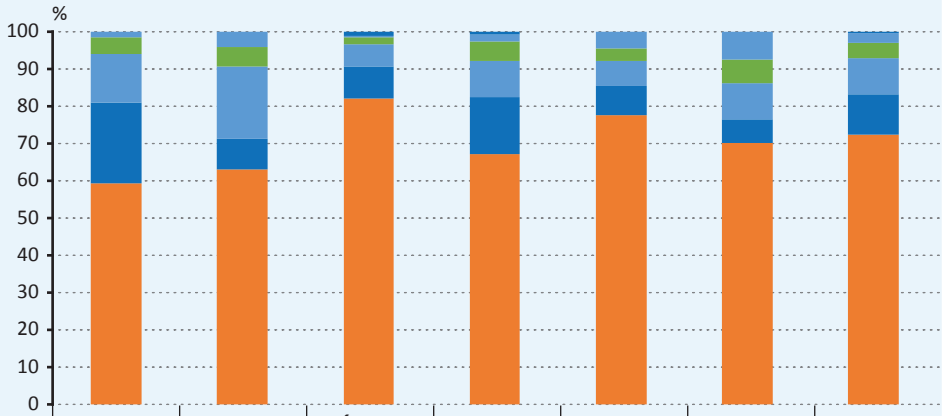
Kiemelkedő esetszám májusban tapasztalható, júliusban pedig nem került kritikus incidensbejelentésre, a többi hónapban átlagosnak nevezhető hat és tíz közötti kritikus esemény bejelentésére került sor. Az összesítésben megjelenő májusi, átlagtól jelentősen eltérő darabszám hasonlóan, mint az összesített – kritikus és nem kritikus incidensek együttes darabszámát tartalmazó – statisztika esetén, az adatok elemzése után néhány intézményhez tartozó megemelkedett bejelentési darabszámra vezethető vissza. A másik jelentős eltérést mutató érték a júliusi záró érték, ebben a hónapban nem érkezett kritikus incidensről bejelentés. Valószínűsíthetően ennek oka a nyári időszakban alacsonyabb rendszerfejlesztési aktivitás.

Összesítve a Pilot időszak során a teljes incidensbejelentési populáción és a kritikus incidenseket tartalmazó statisztikában is hasonló minta figyelhető meg. A havi stabil, jól azonosítható tartományban mozgó bejelentési darabszám jól kivehető, némileg alacsonyabb nyári értékekkel, mely kezdeti megfigyeléseket a következő évek adatelemzése fogják alátámasztani, kiegészíteni vagy korrigálni.

2. INTÉZMÉNYTÍPUSOK INCIDENSBEJELENTÉSEINEK ELEMZÉSE

Az incidensbejelentések havi szintű összesítésén jól látható (11. ábra), hogy a bankok kiugró számosságú incidenst jelentettek be, mely számszerűsítve a fenyegetettségi térkép teljes fél éves időszakában elérte a 72 százalékot a többi intézménytípussal szemben. Ez különösen annak fényében kiemelkedő, hogy a bankok a Pilot projektben résztvevő teljes intézményi körnek csak a 12 százalékát adták.

11. ábra
Incidensbejelentések intézménytípusok szerinti havi bontásban (kritikus incidensek esetén)

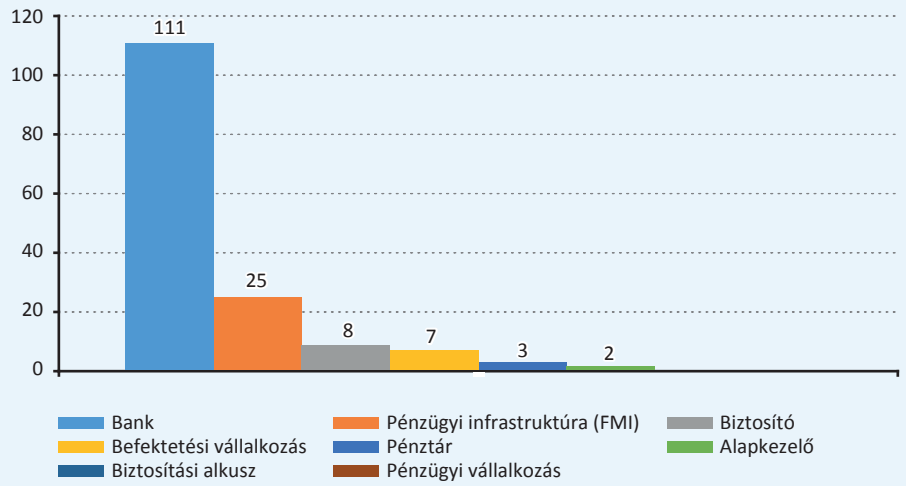


	Február	Március	Április	Május	Június	Július	Total
Bank	50	62	200	105	70	66	553
Biztosító	18	8	21	24	7	6	84
Pénzügyi infrastruktúra (FMI)	11	19	14	15	6	9	74
Pénztár	4	5	5	8	3	6	31
Befektetési vállalkozás	1	4	1	3	4	7	20
Alapkezelő	0	0	2	1	0	0	3
Biztosítási alkusz	0	0	0	0	0	0	0
Pénzügyi vállalkozás	0	0	0	0	0	0	0

Intézményarányosan a bankok által átlagosan észlelt incidensek számossága száztíz, ezzel szemben a legnagyobb részvételi arányú intézménytípus, vagyis a pénztárak esetén ez a szám csak a 2,82-es értéket érte el **(12. ábra).** A bankokat követően a biztosítók és a pénzügyi infrastruktúrák jelentettek még jelentősebb számú eseményt.

Az alapkezelők, pénztárak és befektetési vállalkozások körében kevesebb incidens történt, míg a biztosítási alkuszok és pénzügyi vállalkozások a vizsgált időszakban egyetlen incidensről sem számoltak be.

12. ábra
Átlagos incidens darabszámok intézménytípusok szerinti, intézmény arányosan



A fent említett kisebb számú incidenst bejelentő intézmények esetében nem figyelhető meg a június-júliusi nyári hónapokra vonatkozó incidensszám csökkenési tendencia, ugyanakkor meg kell jegyezni, hogy a kevesebb incidenst jelentő intézmények ügyfeleinek száma és az informatikai rendszereik komplexitása is jellemzően alacsonyabb, tehát kisebb a támadási felületük, és a kevesebb informatikai eszközt tartalmazó rendszerekben a hibák előfordulási valószínűsége is csekélyebb.

Az adatok alapján további következtetések vonhatók le az első ábrából, miszerint a bejelentések többségét nem akadályozta az első két hónap felfutási időszaka. Szándékosan bejelentések többségéről és nem intézmények többségéről beszélünk, hiszen az látszik, hogy a bejelentések többsége esetén nem volt fennakadás, és mivel a bejelentések többségét elsősorban a bankok szolgáltatták megállapítható, hogy a bankok esetén nem jelentett azonosítható nehézséget a bejelentési folyamat implementálása, míg például a biztosítási alkuszok és pénzügyi vállalkozások esetén ilyen megállapítás nem tehető. A bejelentések többségét adó bankoknak az incidensbejelentési folyamat már ismerős volt, a legtöbb esetben elegendő volt a folyamat belső finomhangolása és készen álltak arra, hogy Pilot projekt által meghatározott eljárás szerint szolgáltassanak információkat. Ezzel magyarázható az az eredmény, hogy a Pilot projekt egészét tekintve nem volt kiugróan kevesebb az első két hónapban a bejelentések száma.

Az észrevételt alátámasztja a tény, hogy a Pilot projektben résztvevő bankoknak jelenleg is van jelentési kötelezettsége a pénzforgalmi kiesésekkel kapcsolatosan. Bár a Pilot projekt és a belső piaci pénzforgalmi szolgáltatásokról szóló irányelvet (a továbbiakban: PSD2[18]) a hazai jogba átültető, a pénzforgalmi szolgáltatás nyújtásáról szóló törvény (a továbbiakban: Pft.[19]) szerinti súlyosabb működési és biztonsági eseményekhez kapcsolódó jelentési keretrendszerek olyannyira különböznek, hogy érdemi tanulságot nem tudunk levonni az összehasonlításukból, mindenképpen érdemes megvizsgálni a jelentős, a pénzforgalmi rendszereket hátrányosan érintő incidensek számát.

[18] A belső piaci pénzforgalmi szolgáltatásokról és a 2002/65/EK, a 2009/110/EK és a 2013/36/EU irányelv és a 1093/2010/EU rendelet módosításáról, valamint a 2007/64/EK irányelv hatályon kívül helyezéséről szóló 2015. november 25-i (EU) 2015/2366 európai parlamenti és tanácsi irányelv (Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A32015L2366)

[19] A pénzforgalmi szolgáltatás nyújtásáról szóló 2009. évi LXXXV. törvény (Elérhető: https://njt.hu/jogszabaly/2009-85-00-00)

A PSD2 alapján a Pft. előírja, hogy a pénzforgalmi szolgáltatók a pénzforgalmat, a pénzforgalmi szolgáltatást érintő üzemzavarokról kötelesek haladéktalanul értesíteni az MNB-t, amely jelentési kötelezettségnek a P58 MNB azonosító kódú adatszolgáltatás keretében tehetnek eleget a pénzforgalmi szolgáltatók. Ez az eseti adatszolgáltatás tartalmazza a súlyosabb működési és biztonsági eseménynek minősülő incidenseket is. Ezek a jelzések olyan incidensekről számolnak be, amelyeket a pénzforgalmi szolgáltató nem tervezett, és amelyek káros hatással vannak a pénzforgalmi rendszerek integritására, rendelkezésre állására vagy hitelességére.

1. keretes írás
Bankolás 0-24 órában: új szabályozás a bankszünnapokra

A hitelintézetekről és a pénzügyi vállalkozásokról szóló törvény[20] 2022. július 1-jén hatályba lépett módosítása alapjaiban változtatta meg a hitelintézeti szolgáltatások szüneteltetésére vonatkozó feltételeket. A korábbi szabályozással ellentétben a hitelintézetek már nemcsak munkanapokon (hétfő-péntek között), évente öt munkanap alkalmával szüneteltethetik a szolgáltatásaik nyújtását, hanem bármelyik naptári napon, bármilyen hosszúságban, ha egyébként az adott szolgáltatás vonatkozásában munkanapot tartanának. A jogalkotó célja az új szabályok bevezetésével a hitelintézetek digitalizációjának a támogatása volt. Vagyis az, hogy minden esetben legyen elegendő ideje mind a hitelintézetnek, mind pedig az ügyfeleknek felkészülni egy-egy üzemszünetre, illetve ne legyen az évi maximálisan öt nap leállási lehetőség szigorú korlátja az esetleges informatikai fejlesztéseknek.

Az új szabályozás szerint, ha a hitelintézet bármely pénzügyi vagy kiegészítő pénzügyi szolgáltatását, illetve annak bármilyen résztevékenységét tervezetten leállítja, amikor az adott szolgáltatást a vonatkozó jogszabályok vagy szerződések alapján nyújtania kellene, akkor a tervezett leállás vonatkozásában bankszünnapot kell tartania. Ezért a bankszünnap lehet akár egy kisebb hosszúságú leállás is, amely során kizárólag valamely részszolgáltatás nem érhető el (pl. egy 15 perc hosszúságú leállás, amely során a teljes hitelezési folyamaton belül csupán a hitelbírálat szünetel).

Fontos kiemelni, hogy a leállásnak tervezettnek kell lennie, tehát egy incidens miatti szolgáltatáskiesés, illetve az azt követő helyreállítás nem minősül bankszünnapnak. Jó például szolgálhatnak az azonnali átutalások, amelyek esetében a jogszabály[21] azt írja elő, hogy a hitelintézetnek 0-24 órában a hét minden napján munkanapot kell tartania. Így tehát bármilyen tervezett szolgáltatáskiesés az azonnali átutalások esetében csak bankszünnap keretében valósulhat meg. Ugyanakkor, ha egy adott szolgáltatást a hitelintézet hétvégén nem, csak hétköznap nyújt (pl. ha betétet lekötni csak hétfőtől péntekig 8 és 17 óra között lehet egy adott hitelintézetnél), akkor ezen szolgáltatás (vagy a szolgáltatás egy részének) tervezett leállása csak akkor lehet bankszünnap, ha arra a szerződésben vállalt munkanapon kerül sor (az előző példa alapján pl. egy szerda 12 és 13 óra között tervezett leállás bankszünnap keretében tehető meg, míg szombat és vasárnapi leállás esetében nincs szükség a bankszünnap szabályainak alkalmazására).

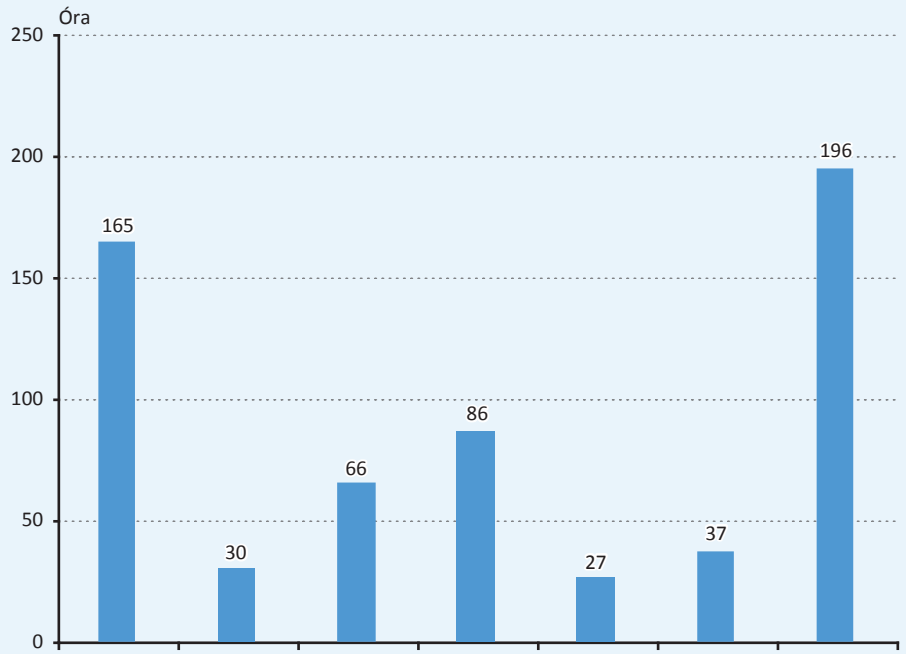
Garanciális szabály, hogy a hitelintézet a bankszünnap tartásáról 30 nappal korábban közvetlen módon (pl. push üzenet formájában) tájékoztassa az ügyfeleit, valamint az MNB részére is köteles azt bejelenteni. Az MNB kivételes intézkedések mellett továbbra is elrendelheti bankszünnap tartását, vagyis kötelezheti a hitelintézetet arra, hogy az adott szolgáltatását, vagy szolgáltatásait állítsa le. A jogértelmezést segítendő az MNB 2021. október 5-én egy vezetői körlevelet[22] is publikált honlapján a téma kapcsán. 2023. január 1-től az egyes fizetési szolgáltatókról szóló törvény[23] szintén módosul, amely szerint pénzforgalmi intézmények és elektronikuspénz-kibocsátó intézmények is a hitelintézetekhez hasonlóan tarthatnak bankszünnapot.

A kiberfenyegetettségi térkép készítése során feldolgozott incidensek, leállások nem tartoznak a bankszünnapról szóló rendelkezések hatálya alá, mivel minden esetben előre nem tervezett módon következtek be.

[20] A hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXVII. törvény (Hpt.) (Elérhető: https://njt.hu/jogszabaly/2013-237-00-00)
[21] A pénzforgalom lebonyolításáról szóló 35/2017. (XII. 14.) MNB rendelet (Elérhető: https://njt.hu/jogszabaly/2017-35-20-2C)
[22] A munkanap fogalmának a hitelintézeti bankszünnap vonatkozásában történő értelmezéséről szóló vezető körlevél (Elérhető: https://www.mnb.hu/letoltes/vezetoi-korlevel-bankszunnap-honlapra.pdf)
[23] Az egyes fizetési szolgáltatókról szóló 2013. évi CCXXXV. törvény (Fszt.) (Elérhető: https://njt.hu/jogszabaly/2013-235-00-00)

A Pilot projektben szereplő intézmények közül a kieséseket jelenteni köteles bankok (az ábrán ezek közül a nagybankok adatait jelenítettük meg) a február és augusztus közötti időszakban több mint ötven kiesést jelentettek be az MNB részére. Ezen jelentési kötelezettségeiknek eleget téve majdnem százötven órányi szolgáltatáskiesési időtartamot képviseltek (13. ábra).

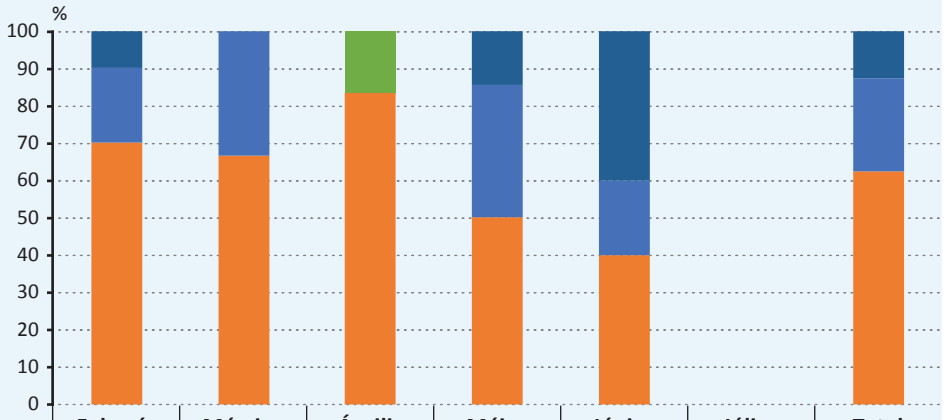
13. ábra
Pénzforgalmi rendszereket érintő kiesések a Pilot projekt időszakában a magyarországi nagybankok körében



A pilot keretében kapott jelzések és a P58 MNB azonosító kódú adatszolgáltatás eredményeinek összevetése nem vezetett értékelhető következtetésekre, azonban a részletes adatok ismeretében a vártnál kevesebb átfedést mutatott a két adathalmaz. A pilotban résztvevő pénzforgalmi szolgáltatók (jellemzően kis és nagybankok) a pénzforgalmat érintő működési incidensekről részletesebb adatokat szolgáltattak a pilotban, mint a kötelező adatszolgáltatások során. Ennek egyik lehetséges oka, hogy a pilot során jóval szűkebb időkeret (a kezdeti jelzésre 90 perc) állt rendelkezésre az MNB felé küldendő jelzésre, ezért az információk általában az incidens kezelésében közvetlenül érintett IT biztonsági és/vagy üzletmenet-folytonossági szakemberektől érkeztek, míg az adatszolgáltatásokkal különösen a nagyobb szervezetek esetében többnyire más szakterület foglalkozik.

A kritikus incidensek vonatkozásában az intézménytípusok szerinti bontásban az adatok elemzésénél szignifikáns eltérés nem tapasztalható a teljes populációhoz képest, ugyanúgy a bankok jelentették be az incidensek jelentős részét (14. ábra).

14. ábra
Incidensbejelentések intézménytípusok szerinti havi bontásban (kritikus incidensek esetén)



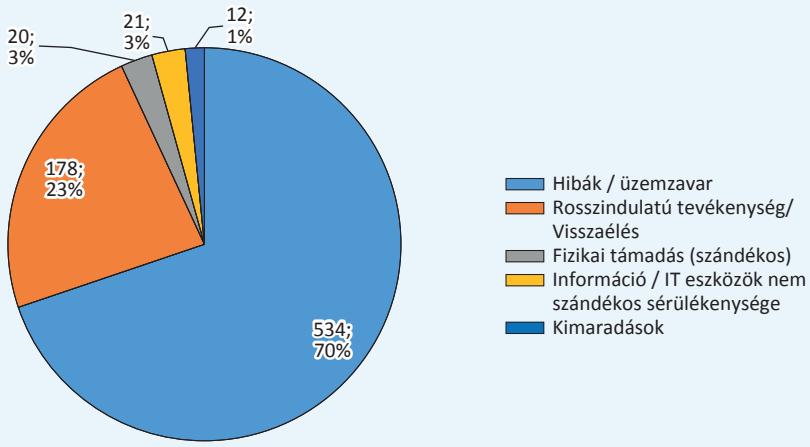
	Február	Március	Április	Május	Június	Július	Total
Alapkezelő	0	0	0	0	0	0	0
Bank	7	4	5	7	2	0	25
Befektetési vállalkozás	0	0	0	0	0	0	0
Biztosítási alkusz	0	0	0	0	0	0	0
Biztosító	2	2	0	5	1	0	10
Pénztár	0	0	1	0	0	0	1
Pénzügyi infrastruktúra (FMI)	1	0	0	2	2	0	5
Pénzügyi vállalkozás	0	0	0	0	0	0	0

Az intézménytípusokra vonatkozó incidensbejelentési adatok elemzésekor az intézmények típusa, mérete és komplexitása mellett fontos tényező lehet, hogy egy adott intézménytípus mennyire nyújt vonzó célpontot a potenciális támadók számára. A kapcsolódó elemzésre a következő fejezetben külön kitérünk, mivel elsősorban az incidensek tartalmának elemzéséből nyerhető ki további információ.

3. BEJELENTETT INCIDENSEK MÉLYSÉGI ELEMZÉSE

A leggyakrabban előforduló incidensek kiváltó okai között első helyen a hibák és üzemzavarok találhatóak, második helyen szerepelnek a rosszindulatú tevékenységek és visszaélések. (15. ábra)

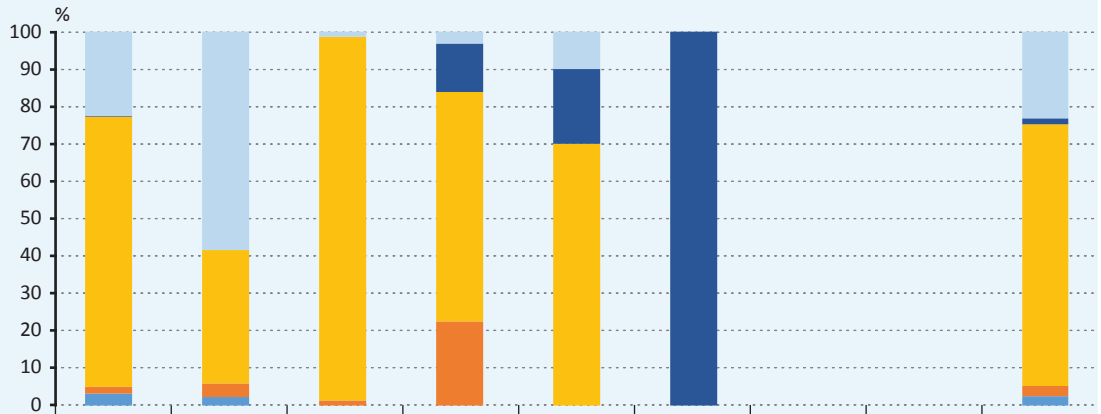
15. ábra
Gyökérokok megoszlása fő kategóriák alapján



A 15. ábráról leolvasható, hogy az MNB részére bejelentett incidensnek elsöprő többségét a hibák és üzemzavarok kategóriájába sorolható incidensek tették ki. Mindezek okán a gyökérokok elemzéséből adódik a kérdés, hogy a hiba és üzemzavar kategória miért ennyire felülreprezentált. A bejelentések technikai leírásait áttanulmányozva a kiugró érték mögött meghúzódhat az a tényező, hogy az üzemzavarok észlelése jórészt kifinomult monitoringeszközökkel történik (azaz kevésbé maradnak észrevétlenek), így állandó részhalmazát képezik az azonosított incidenseknek. Azt is érdemes figyelembe venni, hogy az adatok túlnyomó része banki környezetből érkezik, amelyek esetén a prudens működés megköveteli a fejlett monitoring és detektálási eszközök használatát, valamint a pénzforgalmat érintő kiesésekkel kapcsolatban jelenleg is van jelentési kötelezettsége az intézményeknek. Mindemellett az eredmények megerősítik azt a feltevést, hogy a magyar pénzintézeti szektor nem tartozik a visszaéléseket elkövetők legkiemelkedőbb célpontjai közé. Ennek okaival kapcsolatban csak találgathatunk, de a magyar nyelv nehézségén kívül (mely az adathalász támadások kivitelezését nehezítheti) szerepet játszhat a szektor európai összehasonlításban viszonylag kis mérete és összességében jó felkészültsége az informatikai biztonság területén. A további kategóriák elemzéséhez részletesebb ábra áll rendelkezésünkre.

Az alábbiakban részletes bontásban ábrázoljuk az incidensek kiváltó okait intézménytípusok alapján csoportosítva (16. ábra).

16. ábra
Gyökérokok megoszlása intézménytípus és bejelentési hónap alapján



	Bank	Biztosító	Pénzügyi infrastruktúra (FMI)	Pénztár	Befektetési vállalkozás	Alapkezelő	Biztosítási alkusz	Pénzügyi vállalkozás	Total
Fizikai támadás (szándékos)	18	2	0	0	0	0	0	0	20
Információ / IT eszközök nem szándékos sérülékenysége	10	3	1	7	0	0	0	0	21
Katasztrófa (természeti, környezeti)	0	0	0	0	0	0	0	0	0
Hibák / üzemzavar	399	30	72	19	14	0	0	0	534
Kimaradások	1	0	0	4	4	3	0	0	12
Lehallgatás / Eltérítés	0	0	0	0	0	0	0	0	0
Rosszindulatú tevékenység/ Visszaélés	125	49	1	1	2	0	0	0	178
Jogi	0	0	0	0	0	0	0	0	0

Az első helyen szereplő hiba és üzemzavar kategória után a második helyen a rosszindulatú tevékenység és visszaélés kategória áll, amely a bejelentett incidensek közel 25 százalékát teszi ki. A kategóriát vizsgálva fontos megjegyezni, hogy a bejelentett rosszindulatú tevékenységek jelentős része nem célzottan az intézmények ellen irányult, hanem az ügyfelek ellen, esetleg általánosnak mondható (nem célzott) rosszindulatú tevékenység volt. Az összesítésből kirajzolódik, hogy a rosszindulatú támadásokról elsősorban bankok és biztosítók számoltak be. Itt is megerősítést nyert, hogy a korábban ismertetetteknek megfelelően ezen intézménytípusokat részesítik előnyben a támadók, hiszen a támadások itt eredményezhetnek a legnagyobb valószínűséggel közvetlen anyagi hasznot.

A rosszindulatú tevékenységek kategóriájának fizikai támadások alkategóriájában a leggyakoribb fenyegetést a munkavállalói hardverek (pl. laptopok, mobiltelefonok) elvesztése vagy ellopása jelenti. Az elvesztésből és lopásból fakadó incidensek többsége rendőrségi feljelentéssel végződik. Az ilyen típusú incidensek esetén a háttértárolók titkosítása jelentősen csökkentheti a kapcsolódó kockázatokat.

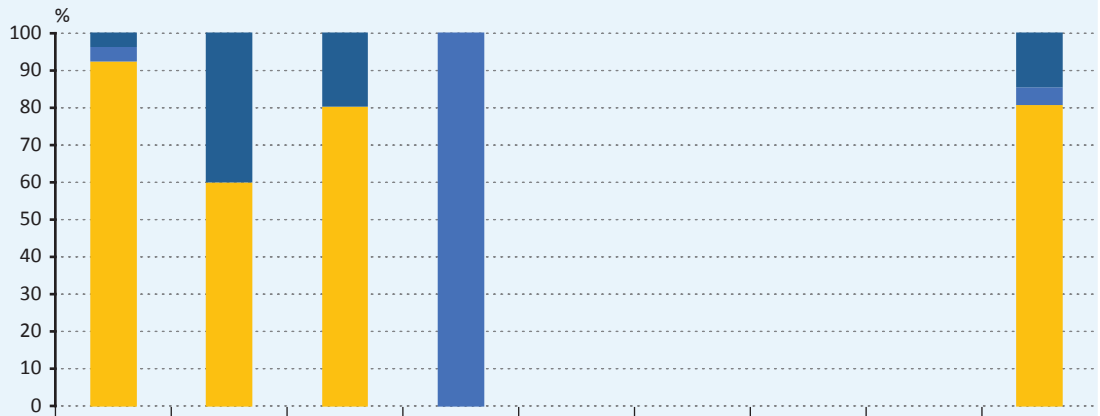
Környezeti incidens (pl. beázás, tűzeset) nem történt a résztvevő intézmények esetén. E tény magyarázható a szektorra jellemző, magas biztonsági követelményekkel (amelyek mentén az általuk használt objektumokat kialakították), de összefüggheti a Pilot időszak időjárási körülményeivel (száraz, aszályos idő) is. Nemzetközi kitekintésben például Nagy-Britanniában gondot okozott a rendkívüli melegben az adatközpontok megfelelő hűtése, ami leállásokhoz vezetett. Magyarországon még az extrém nyári melegben sem történt hasonló üzemzavar.

Három olyan kategóriát tartalmaz a Pilot projekt során meghatározott módszertan, amelyhez nem kötődik incidens. Ezek sorrendben a katasztrófák, a lehallgatás és a jogi incidensek. A projekt időszakában nem volt környezeti katasztrófa az országban. A lehallgatási incidensek pedig kiemelten érzékeny adatokhoz való hozzáférést eredményezhetnek, így a lehallgatás elleni stabil védelem jól felfogott érdeke a szektorális intézményeknek. Ugyan pontos adatok nem állnak rendelkezésre, ezért csak szakértői meglátás alapján feltételezhetjük, hogy a lehallgatási incidensek számának alakulásában a magyar nyelv speciális helyzete, valamint a megfelelő szintű védelem is szerepet játszhatott. Emellett ezekben az esetekben – amennyiben a lehallgatás célja nem a zsarolás vagy a nyilvánosságra hozatal – vélhetően sokkal nagyobb a látencia, hiszen a lehallgató nem fedi fel magát. A távadatátvitel titkosítása régóta megfogalmazott szabályozói elvárás[24]. Az előző megfontolás a jogi incidensek esetén is helytálló, jelentős anyagi és presztízsveszteségek oka lehet egy bekövetkező jogi incidens. A szigorú adatvédelmi és jogi környezet határozottan támogatja, hogy a területen minél kevesebb incidens forduljon elő.

[24] Lásd a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről szóló 42/2015. (III. 12.) Korm. rendeletet (Elérhető: https://njt.hu/jogszabaly/2015-42-20-22), valamint – többek között – az említett rendelet előírásainak értelmezését segítő az informatikai rendszer védelméről szóló 8/2020. (VI.22.) MNB ajánlást (Elérhető: https://www.mnb.hu/letoltes/8-2020-informatikai-rendsz-vedelmerol.pdf).

A bejelentett kritikus incidensek esetén a leggyakrabban előforduló incidensek kiváltó okai – hasonlóan a teljes incidens populáció mintájához – nagy többségben hibákra, üzemzavarokra vezethetők vissza (17. ábra).

17. ábra
Gyökérokok megoszlása intézménytípus és bejelentési hónap alapján (kritikus incidensek esetén)



	Bank	Biztosító	Pénzügyi infrastruktúra (FMI)	Pénztár	Befektetési vállalkozás	Alapkezelő	Biztosítási alkusz	Pénzügyi vállalkozás	Total
Fizikai támadás (szándékos)	0	0	0	0	0	0	0	0	0
Információ / IT eszközök nem szándékos sérülékenysége	0	0	0	0	0	0	0	0	0
Katasztrófa (természeti, környezeti)	0	0	0	0	0	0	0	0	0
Hibák / üzemzavar	23	6	4	0	0	0	0	0	33
Kimaradások	1	0	0	1	0	0	0	0	2
Lehallgatás / Eltérítés	0	0	0	0	0	0	0	0	0
Rosszindulatú tevékenység/ Visszaélés	1	4	1	0	0	0	0	0	6
Jogi	0	0	0	0	0	0	0	0	0

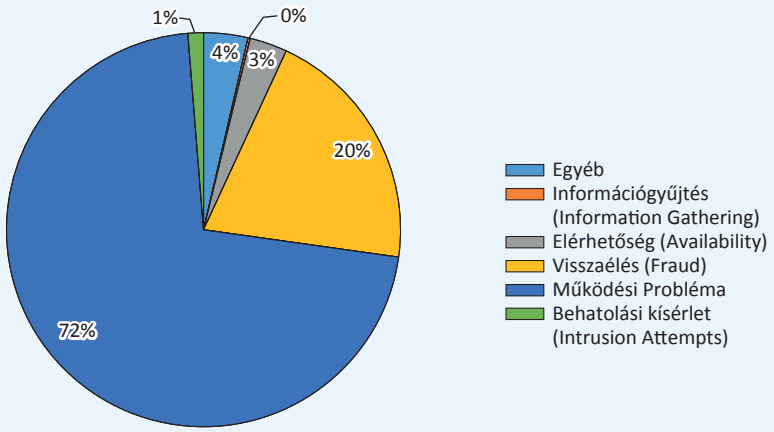
A hibák, üzemzavarok csoportja alatt találhatjuk az intézmények saját infrastruktúrájából származó hiányosságok, valamint a nekik szolgáltatást nyújtó harmadik felektől származó incidensek kategóriáját.

A kritikus incidensek esetén kisebb számosságban visszaélés adta az incidensek kiváltó okát, amely a nem frissített rendszerek hiányosságának kihasználásán alapult.

Tekintettel arra, hogy a bankok jelentették az incidensek több mint kétharmadát, erről az intézménytípusról részletesebb információval rendelkezünk, így a következő ábrákon a kizárólag banki forrásból származó incidensadatok kerülnek bemutatásra.

A következő ábrán a banki bejelentésből származó incidensek típusainak megoszlása látható (18. ábra).

18. ábra
Bankoknál bekövetkezett incidensek típusainak eloszlása



A bankok esetében is a hibákra, üzemzavarokra vezethető vissza a bejelentett működési probléma típusú incidensek jelentős többsége, mintegy 72 százaléka. A banki hibák, üzemzavarok kategóriáját tovább bontjuk, így az esetek túlnyomó többségben, 95 százalékban működési probléma okozta az incidenseket. Kisebb részben, öt százalékban egyéb a bankon kívüli ún. harmadik fél IKT szolgáltatóknál[25] bekövetkezett meghibásodás vagy zavar volt a banki hibáknak és üzemzavaroknak a kiváltó oka. A hibák és üzemzavarok kategória technikai adatait részletesebben elemezve megállapítható, hogy a rendszerek meghibásodása a banki környezetekben sokkal kevésbé jellemző, mint a teljes mintára vetítve. A kisebb meghibásodási arány a rendszerek nagyobb hibatűrésének, szigorúbb rendelkezésreállási követelményeinek tudható be. Például az azonnali fizetési rendszer esetén elvárt folyamatos rendelkezésreállást a pénzforgalmi szolgáltatók többsége két aktív telephely fenntartásával biztosítja. Érdekesség, hogy amíg a nem banki rendszerekben azonosíthatóak kommunikációs hálózatok meghibásodásával vagy megszakadásával kapcsolatos hibák, addig a banki rendszerek vonatkozásában a Pilot projekt ideje alatt nem érkezett ilyen jellegű bejelentés. Vélhetően a banki kommunikációs hálózatok magasabb hibatűrésének, fokozottabb redundanciájának tulajdonítható a kommunikációs hálózatok meghibásodásával vagy megszakadásával kapcsolatos hibák hiánya.

A rosszindulatú tevékenység a banki szegmensben is második az incidenseket kiváltó okok sorában a vizsgált időszakban, az incidensek 23 százaléka rosszindulatú tevékenységhez köthető. A rosszindulatú esetek több mint felében célzott támadások (pl. APT, DDoS stb.) álltak az incidensek hátterében. A Pilot projekt időszaka alatt nem banki szereplők is azonosítottak célzott támadást. Ez azt mutatja, hogy ha kisebb arányban is, de a pénzügyi szektor más szereplőit is célba veszik a támadók. Az információval, illetve információs rendszerekkel (beleértve a mobilalkalmazásokat) való visszaélés szintén csak a banki szereplők esetében fordult elő a vizsgált időszakban, összesen 15 esetben. Megtévesztésen alapuló támadás 25 esetben volt azonosítható a bankok esetében, míg más típusú intézményeknél ez a szám elenyésző volt. Az okokat vizsgálva feltételezhető, hogy a biztosítók vagy pénztárak esetében jóval nehezebb közvetlen anyagi előnnyel járó tranzakciót kezdeményezni. Fontos továbbá kiemelni, hogy az adathalász támadások esetén jellemzően nem a bankokat, hanem a banki ügyfeleket támadják. A rosszindulatú kód, illetve rosszindulatú szoftver kategóriában a bankoknál csak két incidenst jelentettek a résztvevők. Csak a biztosítóknál nyolcszor több esetről számoltak be az intézmények. Szolgáltatásmegtagadás (Denial-of-Service – DoS) típusú támadás 12 esetben fordult elő a bankoknál, rajtuk kívül csak a befektetési vállalkozások

[25] Ilyen szolgáltatásokra lehet példa a telekommunikációs szolgáltatások.

szenvedtek el DoS támadást a Pilot projekt időszakában. Fontos megjegyezni, hogy a bankok már évek óta a DoS, illetve DDoS támadások célkeresztjében vannak, és mostanra a többségük professzionális védelmet alakított ki. A bankok ellen irányuló támadások ezért jellemzően nem járnak tényleges kieséssel. Jogosulatlan tevékenység (nem pénzügyi, hanem az ENISA által használt értelemben) – mint elsődleges gyökérok[26] – bankok esetében csak egyszer fordult elő a Pilot projekt időszaka alatt, ugyanezen kategória viszont a pénztáraknál és a biztosítóknál is többszörösen azonosítható volt.

A fizikai támadás bár jelentős számosságúnak tűnik, ugyanakkor több esetben is bombatámadással való fenyegetésről van szó, ami szerencsére végre nem hajtott fizikai támadásokat jelent. Laptopok, mobiltelefonok különböző helyszínekről (pl. irodából, tömegközlekedési eszközről, autóból) történő ellopása a legjellemzőbb a fizikai támadás területen. Egyetlen esetben történt automata bankjegykiadó gép (ATM) rongálás a Pilot projekt időszaka alatt.

Az információs, valamint IT eszközök nem szándékos sérülése még százalékosan mérhető kategória, ide sorolhatók a következő esetek: harmadik személy által okozott kár; eszközök és rendszerek hibás használata vagy adminisztrációja; információ szivárgása, illetve információ megosztása emberi mulasztás miatt. A felsorolt incidensekre volt precedens a Pilot projektben, de számosságuk nem jelentős. A harmadik személy által okozott kár kategóriában különböző banki rendszerekbe történő behatolási kísérletek kerültek bejelentésre.

Kimaradás, erőforrások elvesztése csak egy esetben történt, ami egy géptermi áramszünetet követően a szünetmentes áramforrás műszaki problémája miatt alakulhatott ki.

A visszaélések (fraud) kategóriában adathalász (phishing) és hang alapú adathalász (vishing) kísérletek voltak jellemzőek. A phishing és vishing kísérletek alapvetően a banki ügyfelek ellen irányultak, egy-két kivételtől eltekintve. A banki intézmények a Pilot időszakban ötször annyi fraud incidenst jelentettek, mint a biztosítók és a pénztárak összesen, ami jól mutatja a bankok magasabb kitettségét az ilyen jellegű visszaéléseknek, illetve azok kísérletének.

2. keretes írás
A KiberPajzs kezdeményezés

KiberPajzs
Védelem a pénzügyekben

KiberPajzs néven közös oktatási és kommunikációs együttműködést indított 2022. november 7-én az MNB, a Magyar Bankszövetség, a Nemzeti Média- és Hírközlési Hatóság (NMHH), a Nemzetbiztonsági Szakszolgálat – Nemzeti Kibervédelmi Intézet (NBSZ-NKI), illetve az Országos Rendőr-főkapitányság (ORFK). A digitális pénzügyi bűnözők ma elsősorban a fogyasztók érzelmi manipulálásával, illetve megtévesztésével támadnak, így a résztvevők a lakossági ügyfelek pénzügyi tudatosságának erősítése, a kiberkockázatok általuk történő hatékony kezelése érdekében fognak össze.

A 2024. január 31-ig szóló – s a résztvevők igénye alapján meghosszabbítható – KiberPajzs projekt keretében az intézmények és a piaci szereplők átfogó oktatási programot indítanak az ügyfelek digitális pénzügyi tudatosságának fejlesztése érdekében. Ennek eszközeként széleskörű, összehangolt kommunikációs kampány is kezdetét veszi a kiberbiztonsági kockázatok és az ellenük való védekezési lehetőségek bemutatására.

A KiberPajzs projekt keretében zajlik emellett a hatósági és piaci folyamatok elemzése, illetve az együttműködés révén a résztvevő nyomozóhatóságok továbbfejlesztik kiberbiztonsági bűnmegelőzési és nyomozati tevékenységüket, a kibervédelmi hatóságok pedig hatékony incidenskezelési eljárásrendjüket, gyakorlatukat. A projekt kiemelten figyel a fiatalkorúakra, a fokozottan kiszolgáltatott társadalmi csoportokra (így az idősekre), de a fogyasztók mellett megelőző jellegű üzeneteket fogalmaz meg a kis- és középvállalati, illetve az egyéb céges ügyfelek felé is.

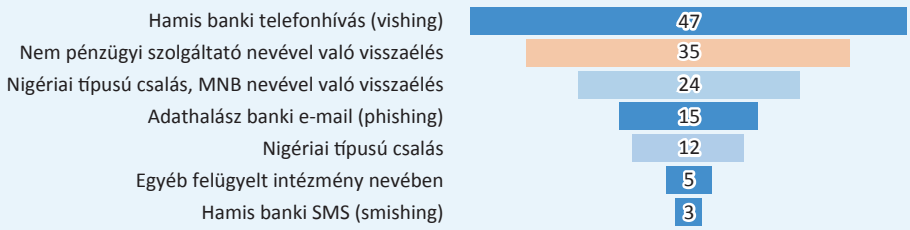
[26] Lásd pl az ENISA fenyegetettségi taxonómiáját (Elérhető: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy)

A digitalizáció révén egyre hangsúlyosabbá válik az elektronikus pénzforgalom, ezzel párhuzamosan pedig – miközben a hazai pénzügyi rendszer európai összevetésben is rendkívül biztonságosnak számít – a rajta keresztül megfigyelhető sikeres visszaélések száma és aránya is növekszik. A bűnözők nem a pénzügyi intézményeket, illetve infrastruktúrát támadják, hanem elsősorban a (gyors változásokat olykor át nem látó) fogyasztók megtévesztése, érzelmi manipulálása révén érnek célt. Ezért vált mára alapvető fontosságúvá az „elsődleges védelmi vonalnak" számító ügyfelek pénzügyi tudatosságának erősítése és felkészítésük a kiberkockázatok kezelésére.

A KiberPajzs résztvevő intézményei egységes arculatú, egyszerű üzenetekkel mutatják be a főbb csalási formákat, így az adathalászat különböző formáit, a hamis banki hívásokat vagy SMS-eket, a meghamisított banki weboldalakat, a hamis tranzakciók jóváhagyatási formáit, a csaló befektetési formákat vagy online ajánlatokat, illetve a közösségi média segítségével történő személyesadat-lopásokat. A plakátokon és üzenetekben három olyan „mindennapi példakép" személyiség birkózik meg e kockázatokkal, akik élethelyzete hasonlít a legtöbb magyarországi, digitális pénzügyi fogyasztóéhoz.

A fenti tendenciát alátámasztják az MNB ügyfélszolgálati feladatait ellátó Ügyfélkapcsolati Információs Központjának kibervisszaéléssel kapcsolatos ügyféljelzésekből származó tapasztalatai is, miszerint a vizsgált időszakra vonatkozóan az MNB-hez beérkezett ügyfélpanaszok alapján a legelterjedtebb támadási forma a hamis banki telefonhívás (vishing) volt, majd ezt követték a nem pénzügyi szolgáltató nevében elkövetett kibervisszaélések (19. ábra). Az összesítésből az is megállapítható, hogy a klasszikus banki e-mailen keresztül terjedő adathalász visszaélések csak a negyedik legelterjedtebb támadási formát képviselik. Az ügyféljelzések többségében kárt elszenvedett ügyfelektől érkeztek (62 százalék), de olyan ügyféljelzésekkel is találkozott az MNB ügyfélszolgálata, amelyben az ügyfél kibervisszaélési kísérletről adott tájékoztatást. Az ügyfelek számos esetben (20 százalék) számoltak be arról, hogy a kibervisszaélésekkel összefüggésben rendőrségi feljelentést is tettek.

19. ábra
Kibervisszaélések típusai az MNB ügyfélszolgálatához érkezett ügyféljelzések alapján, 2022. február- augusztus



Folytatva a banki rendszerek vonatkozásában bejelentett incidensek elemzését: sikeres, hálózaton keresztül kivitelezett behatolásról nem érkezett jelzés, de behatolási kísérlet számos esetben történt. A közelmúlt sérülékenységeihez és a sérülékenységeket kihasználó publikusan elérhető kódokhoz (ún. exploitokhoz) igazodva, a Log4j[27], a Spring Cloud[28] és az IIS szerverek[29] ismert sérülékenységei alapján indítottak behatolási kísérletet ismeretlenek. Ezen sérülékenységek egy részéről az MNB számára elérhető adatokból tudjuk, hogy a felügyelt intézmények a sebezhetőségek nyilvánosságra kerülése után röviddel megtették a szükséges védelmi intézkedéseket.

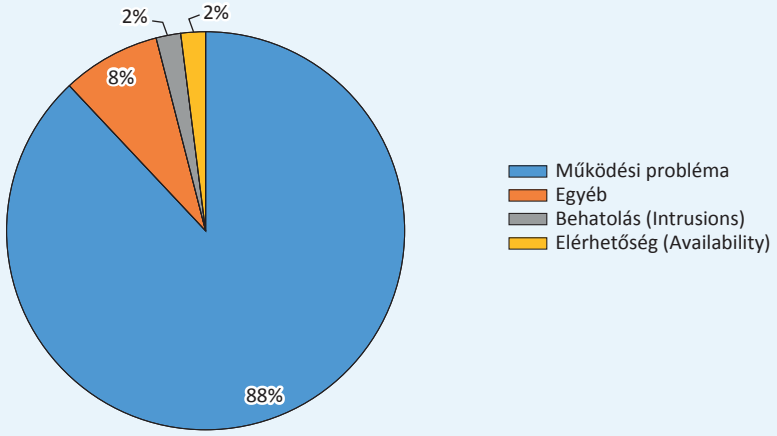
Információgyűjtési incidens típusból csak egyetlen bejelentés történt, az egyik bank ügyfelei e-mailben kaptak egy, a banki internetbank felületre emlékeztető, ám adathalász oldalra mutató hivatkozást tartalmazó levelet.

Egyéb típusú, az intézmények által nem besorolható kategóriában hozzávetőlegesen négy százaléknyi incidens került jelentésre, melyek hátterében jellemzően az információ elérhetőségét korlátozó eseményeket jelentettek.

[27] Elérhető: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2021-44228
[28] Elérhető: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22963
[29] Elérhető: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21907

A kritikus incidensek tekintetében először az incidenstípusok eloszlása kerül elemzésre (20. ábra).

20. ábra
Kritikus incidensek incidenstípusok szerinti megoszlása érintett ügyfelek alapján



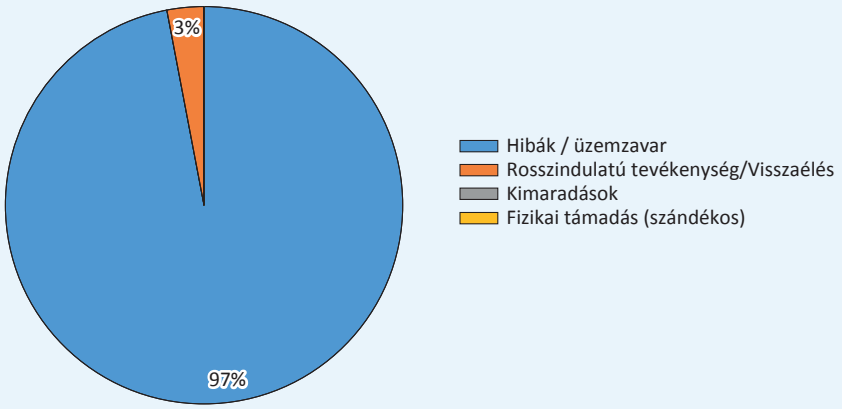
Az egyes incidensek kapcsán a felügyelt intézmények megadhatták az érintett ügyfelek számát. Amennyiben úgy tekintjük, hogy az egyes incidensekben érintett ügyfelek esetében nincs átfedés, összeadhatjuk az érintett ügyfelek számát, így megbecsülhetjük az *összes érintett ügyfelek számá*t. Az incidenstípusokat az érintett ügyfelek aránya alapján is rangsorolhatjuk: egy adott incidenstípusban érintett összes ügyfelek számát az *összes érintett ügyfelek számá*hoz viszonyítva kapott arányszámokat mutatja a 20. ábra. Itt is látható, hogy az érintett ügyfelek arányának vizsgálata alapján is a működési problémák a legjellemzőbb incidensek.

Az incidensek bejelentése során a gyökérok kategóriák alatt megjelölt alkategóriák elemzése után megállapítható, hogy mind a működési típusú problémának, mind az elérhetőségi típusú problémának, illetve egyéb kategóriának megjelölt incidensek esetén az incidenst az elérhetetlenné váló rendszerek miatt jelentették. Összesítve, a Pilot időszak hat hónapja alatt az elérhetőségi problémával érintett felhasználói hozzáférések számossága hozzávetőlegesen 150 ezer volt. Ennyi ügyfél esetében állhatott fent hosszabb-rövidebb ideig valamilyen szolgáltatás elérésével kapcsolatos probléma. Ez nem jelenti azt, hogy az incidensek valóban ilyen nagy tömegben érzékelhetőek lettek volna. Azon ügyfelek, akik a kritikus időszakban nem próbálták elérni a kérdéses rendszerkiesésekben érintett szolgáltatásokat, nem érzékelhették a problémát.

A harmadik kategória elemzése is fontos eredményeket szolgáltat: a behatolás alkategóriába sorolt incidensek mögött egyetlen pénzügyi intézmény egyetlen eseménye húzódik meg, mely több mint 3500 ügyfelet érintett. Az incidens rámutat, hogy a Pilot projektben résztvevő intézmény sikeresen elhárított egy olyan előrehaladott, súlyosabb támadást, amely rendszerbehatolással is járt. A támadás során egy alkalmazásszerver volt az elsődleges behatolási pont. Bár az esemény a belső patch management folyamatok hiányosságaival kapcsolatosan vethet fel kérdéseket, az intézményi, valamint hatósági vizsgálatokat követően megállapításra került, hogy a behatolás során több, kevésbé ismert sebezhetőséget is kihasználtak a támadók. Így arra vonatkozóan nem lehet egyértelmű következtetéseket levonni, hogy az alkalmazásszerver biztonsági frissítésével megelőzhető lett volna-e a támadás. Az incidens miatt az MNB mellett a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH) és az NBSZ-NKI is értesítést kapott. Az intézmény az incidenskezelési tervének jó gyakorlataihoz igazodva, gyorsan és hatékonyan elhárította a behatolást. Továbbá kijavította az érintett rendszert, mielőtt további negatív következményei lehettek volna a sérülékenységnek az intézmény informatikai rendszereiben. Az eset kifejezetten jól illusztrálja az incidensek észlelésének, valamint az incidenskezelési tervek meglétének fontosságát. E két elem nélkül egy sikeres támadásból fakadó incidens kezelése jelentős nehézségekbe ütközik.

A kritikus incidensek vizsgálata során elemzésre került az érintettek számossága az incidensek fő gyökérokainak függvényében (21. ábra).

21. ábra
Kritikus incidensek esetén az érintett ügyfelek számossága gyökérok szerinti bontásban



A 21. ábra – hasonlóan a 20. ábrához – az érintett ügyfelek száma alapján veti össze a gyökérokokat. Amennyiben úgy tekintjük, hogy az egyes incidensekben érintett ügyfelek közt nincs átfedés, összeadhatjuk az érintett ügyfelek számát, így megbecsülhetjük az *összes érintett ügyfelek számá*t. Az incidenseket kiváltó okokat az érintett ügyfelek aránya alapján is rangsorolhatjuk: egy adott gyökérokhoz tartozó érintett összes ügyfelek számát az *összes érintett ügyfelek számá*hoz viszonyítva kapott arányszámokat láthatjuk a 21. ábrán.

A legtöbb ügyfelet a hibák és üzemzavarok érintették. Ezen belül is a legjelentősebb érintettség az egyik legnagyobb magyarországi bank azon ügyfeleire korlátozódott, akik egy adott napon kártyás fizetési műveletet hajtottak volna végre. Az eset több tízezer ügyfélre volt hatással, ami jól példázza, hogy egy kisebb hiba potenciálisan milyen jelentős hatásokkal járhat.

Az ügyfeleket érintő incidensek jellemzően bankokhoz kötődtek: az egyéb, nem banki intézmények által jelentett, ügyfeleket érintő incidensek esetén az érintetti kör összesen 3400 fő volt, míg a banki ügyfelek esetében az érintetti kör hozzávetőlegesen 150 ezer főt tett ki.

Annak ellenére, hogy a jelen fenyegetettségi térkép alapján a vizsgált időszakban túlnyomó részben a működési problémákhoz visszavezethető gyökérokokhoz köthető incidensek történtek, továbbra is fennáll a támadások veszélye. A magyarországi pénzügyi szolgáltatók védelmi kontrolljai robusztusak, továbbá az erős szakmai háttér és támogatás közvetlenül az intézmények ellen irányuló rosszindulatú tevékenységek sikerességének esélyét csökkenti. Ennek ellenére a támadási kísérletek magas kockázatot képviselnek, mind a pénzügyi szektor intézményeire, mind a külső beszállítóikra vonatkozóan. A kritikus incidens jelzések közül kettőnél azonosítottak kiváltó okként sérülékenységet. Példaként említhetjük az egyik az MNB részére bejelentett incidenst, amely során egy szoftveres sérülékenység felfedezése miatt egy kiterjedt pénzügyi szolgáltatást nyújtó intézménynek kellett leállítania egy üzleti internetes oldalát addig, amíg a biztonsági javítócsomagok telepítésével nem szüntették meg a kockázatot. Amennyiben a sérülékenység nem került volna felderítésre, a sebezhetőség jelentős kockázatot jelenthetett volna egy potenciális célzott támadás esetén.

Továbbra is a kritikus incidenseket vizsgálva a rosszindulatú tevékenységek közt két olyan kritikus incidens volt azonosítható, mely ügyfeleket is érintett. Az egyik ezek közül a korábban említett elavult szoftver hibás konfigurációval futtatva, a másik egy elosztott túlterheléses támadás (DDoS) volt, amely szintén több mint ezer ügyfelet érintett. Rosszindulatú tevékenységek közé sorolandók továbbá az adathalász támadások, amelyek továbbra is gyakoriak és elterjedtek, különösen a pénzügyi szektor vonatkozásában. Az elmúlt évek adathalász hullámai hatására a felügyelt intézmények biztonságtudatossága sokat fejlődött ezen a téren. Ennek ellenére, a Pilot projektben azonosítható volt olyan kritikus incidens, melynek kiváltó oka adathalász támadás volt.

3. keretes írás
Kimaradást okozó kritikus incidens esettanulmánya

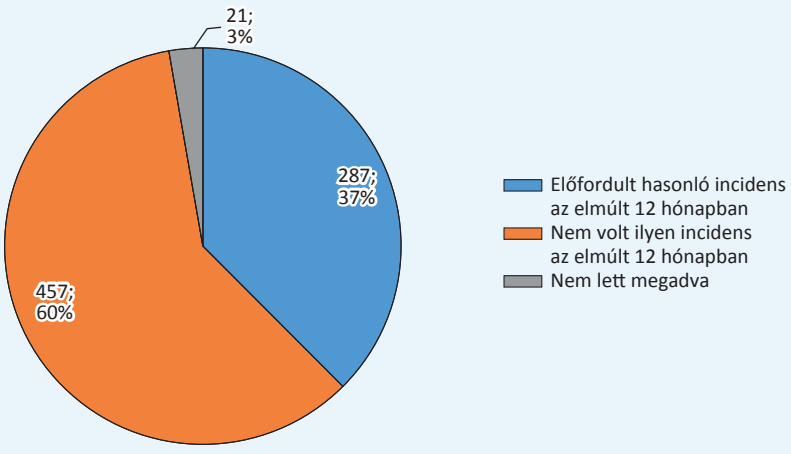
A kibereseményekkel kapcsolatos híreket olvasva, helytelen lenne azt gondolni, hogy a kritikus incidensek csak a legjelentősebb pénzügyi szolgáltatókat érintik az olyan támadások vonatkozásában, amelyeket nemzetállamok által támogatott hackercsoportok követnek el. A valóságban ehhez képest az a tapasztalat rajzolódott ki a Pilot projekt során, hogy bármelyik kiváltó ok okozhat kritikus incidenst. Az incidensek, valamint azok kiváltó okai általánosságban összefügghetnek az érintett intézmény tevékenységi körével, méretével, vagy egyéb jellemzőjével. Ehhez képest a kritikus incidensek bontásában azt tapasztaltuk, hogy ezen incidensek kevésbé igazodnak havi bejelentések alapján azonosított mintázatokhoz. Példaként egy olyan pénzügyi szolgálgatónál bekövetkezett, szolgáltatáskieséssel járó kritikus incidenst emelnénk ki, amelynél a kiváltó ok egy áramkimaradásra vezethető vissza. Az incidens kritikus jellegét egy másodlagos esemény, a szünetmentes tápegységek meghibásodása okozta. Ráadásul ez a Pilot alatt bekövetkezett esemény nem is egyedülálló, az MNB már korábban is találkozott hasonló esettel. Összehasonlítottuk azokkal az incidensekkel, amelyek azonos kiváltó ok mellett nem voltak negatív hatással a szolgáltatások rendeltetésszerű működésére, és jól látható, hogy bármilyen gyökérok, az egyszerűségétől függetlenül képes nagy hatást gyakorolni egy szervezet működésére, amikor egyszerre több tényező befolyásolja az incidens eredményes kezelését. Továbbá az incidens jól illusztrálja, hogy bármilyen incidenst kiváltó ok tud jelentős hatást gyakorolni bármekkora intézményre, amennyiben a biztonsági kontrollok nem megfelelően működnek, és ezáltal nem lehetséges kellő időben jelentősen enyhíteni az incidens hatásait. Az incidens kezelése nem zárulhat le a szolgáltatás helyreállításával, minden esetben meg kell találni az incidenst okozó gyökérokokat és meghozni azon intézkedéseket, melyek a gyökérokok kezelésével megakadályozzák az esemény újbóli előfordulását.

A kimaradások miatt kialakuló incidensek közül egyetlen volt, amely kevesebb felhasználóra volt hatással. Az egyik pénzügyi intézmény munkatársai nem érték el az Internetet a szolgáltató érintettségéből kifolyólag. Így az összesen 19 főt érintő incidens gyökérok kategória rámutat, hogy a Pilot projekt során jelzéseket szolgáltató intézmények incidensbejelentési gyakorlata nagyon eltérő volt annak értelmezésében, hogy mit jelent az ügyfélérintettség és ügyfélnek tekinti-e a belső felhasználókat.

Az incidens adatok részletes elemzése során az utolsó vizsgált terület az volt, hogy az incidensek azonosítása során mit látnak az intézmények, találkoztak-e már az adott incidenst kiváltó okkal az elmúlt 12 hónapban, vagy számukra új típusú okra visszavezethető incidens történt.

A következőkben az látható, hogy adott incidens kiváltó oka korábban már előfordult, vagy az incidenst kiváltó okot a bejelentő intézmény először azonosította az elmúlt 12 hónapban. Összefoglalva elmondható, hogy az incidensek kétharmada új, az elmúlt 12 hónapban nem tapasztalt okra vezethető vissza (22. ábra).

22. ábra
Incidensek ismételt előfordulásának aránya



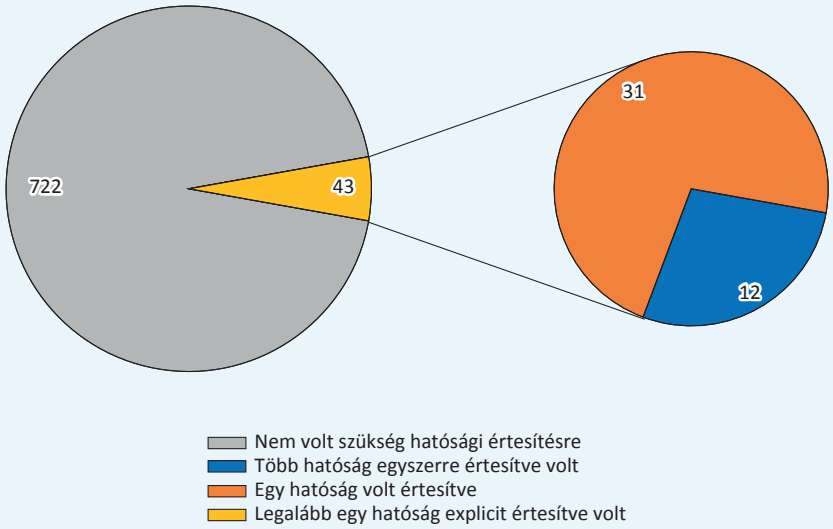
A hat hónapos jelentési időszakban új okokra visszavezethető incidensek túlnyomó többségben nem kritikus besorolású, működési típusú problémák voltak, melyek egyedi rendszereket és komponenseket érintettek. A felmerülő hibák között kiemelkednek a frissítések, a konfigurációs állományok inkompatibilitása, mint nem rosszindulatú tevékenység. Az adatok alapján elmondható, hogy az IT rendszereket érintő változásoknál kiemelten fontos a változáskezelési folyamat részeként elkészíteni a visszaállási tervet, mert ezzel minimalizálható a kiesési idő. Az új okra visszavezethető incidensek többségében üzemzavart okoztak, melyek szolgáltatáskieséssel jártak. Az incidensek megoldása során frissítések, fejlesztések, kivételek hozzáadására került sor, ezzel biztosítva, hogy a későbbiekben az adott típusú incidens ne következzen be újra.

A maradék egyharmad esetben olyan incidensek kerültek bejelentésre, ahol az incidens oka már korábban is előfordult. Két főbb területet lehetett megkülönböztetni: rosszindulatú tevékenység, illetve üzemzavar. A rosszindulatú tevékenységek túlnyomó részét DDoS, SPAM és adathalász kísérletek tették ki. Ezek a támadások általában nagy volumenűek voltak, egyszerre több rendszert vagy személyt vettek célba. A visszatérő típusú gyökérokkal azonosított incidenseknél – ellentétben az új okra visszavezethető incidensekkel – a legtöbb nem okozott szolgáltatás kiesést.

4. HATÓSÁGI ÉRTESÍTÉS ÉS KÜLSŐ SZOLGÁLTATÓI ÉRINTETTSÉG ELEMZÉSE

A Pilot projekt során az MNB részére megküldött incidensjelentések tartalmaztak olyan eseteket is, amikor további hatóság értesítésére volt szükség. Az összes bejelentett incidensekhez viszonyítva hozzávetőlegesen az esetek öt százalékában fordult elő, hogy az incidensről az érintett intézmények az MNB-n kívül más hatóságot is értesítettek (23. ábra). Ezen incidensek negyede esetében került egynél több további hatóság értesítésre.

23. ábra
Incidens darabszámok a hatóság értesítések függvényében

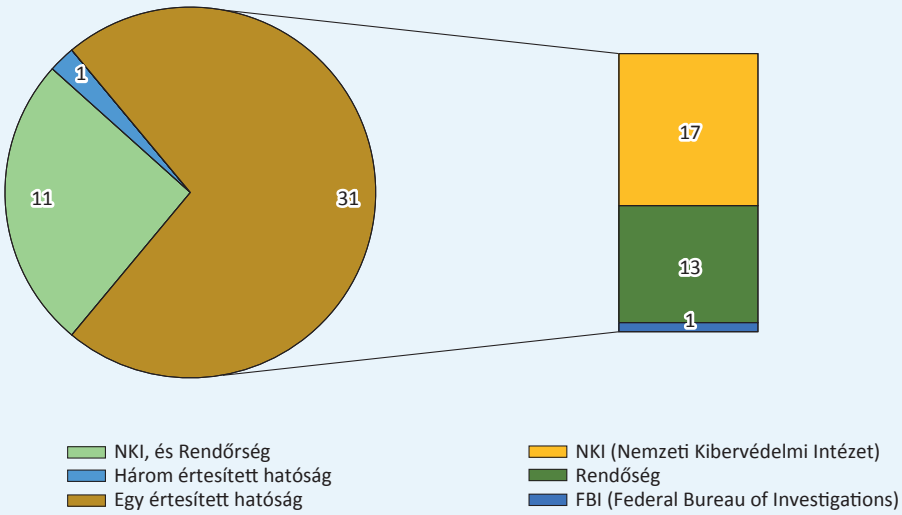


Az arányszám a jövőben több tényező függvényében is dinamikusan változhat, például ha a következő években incidensbejelentésre kötelezett intézmények érzékenysége szignifikáns módon eltér majd a Pilot projekt során tanúsított érzékenységtől, vagy ha változik a hatóságok számára kötelezően bejelentendő incidensesetek köre, például a Nemzetközi szabályozói kezdeményezések fejezetben említett új szabályozások következtében.

Ezen öt százaléknyi incidensbejelentés elemzése során, ha az incidens bejelentése az MNB-n túl további hatóságot is érintett, két esetet különböztethetünk meg. Az incidensbejelentések közel háromnegyedében elegendő volt egy hatóság értesítése az MNB-n felül. Valamivel több mint egynegyed részében több hatóság együttes értesítése történt meg. A rögzített adatok között azokban az esetekben, amikor egy incidensbejelentés során több hatóság került értesítésre, az értesített hatóságok statisztikai arányát nem az összesített incidensbejelentések számához képest mértük. A teljes incidens populációt a hatósági értesítéssel érintett esetekhez viszonyítottuk, nem az értesítések darabszámához. Számszerűsítve az érintett 43 db incidensbejelentés során összesen 56 db hatósági értesítés történt. Figyelemre méltó, hogy volt olyan bejelentett incidens, ahol az intézmény rosszul ítélte meg, hogy hatóságot értesített-e, vagy más szereplőt.

A Pilot projekt során a hatósági bejelentésre vonatkozó adatok összesítése után az MNB-n kívül három hazai és egy nemzetközi hatóság került megjelölésre, ahová incidensbejelentés történt (23. ábra): NBSZ-NKI, Rendőrség, NAIH, Federal Bureau of Investigation (a továbbiakban: FBI).

24. ábra
Hatósági értesítési arány



Az esetek közel 40 százalékában az NBSZ-NKI-t értesítették, míg 30 százalékban kizárólag a rendőrséget. A maradék 30 százalék túlnyomó részét azok az esetek jelentették, amikor az NBSZ-NKI és a rendőrség együttesen értesítést kapott. Az NBSZ-NKI-t azon intézmények értesítették, amelyeknek – kritikus infrastruktúra és/vagy alapvető szolgáltatás jellegükből adódóan – jelentési kötelezettségük van.

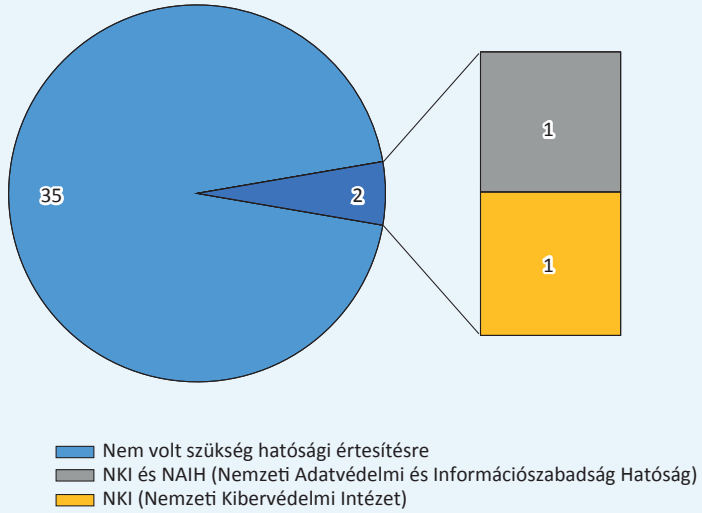
Az MNB minden fent vizsgált esetben kapott tájékoztatást, tehát egy hatóság minden incidensnél kapott értesítést és ezt akkor is megkapta volna a már meglévő adatszolgáltatási kötelezettségek okán, ha nincs Pilot projekt. Az eseteket egyenként megvizsgálva az is látható, hogy az intézmények belső eljárásrendjei jelentősen eltérnek abban a tekintetben, hogy mely esetekben tesznek rendőrségi feljelentést. Az intézmények számára előírt bejelentési kötelezettségek is jelentősen eltérhetnek egymástól az intézmények jellegétől (például bank vagy pénzügyi infrastruktúra) és kritikusságától függően.

Külföldi hatóság (FBI) értesítésére csoportszintű, átfogó DDoS támadás miatt volt szükség, mely a magyarországi intézmény mellett más országokban működő intézményeket is érintett.

Ahogyan arról már írtunk, a teljes incidenspopuláció esetében a vezető okok a hiba/üzemzavar volt, amit a rosszindulatú tevékenység követett a második helyen. Ezzel szemben a hatósági értesítések esetén a bejelentett incidensek túlnyomó többsége rosszindulatú tevékenység volt. A hatóság értesítésével járó incidensek a következők szerint tipizálhatóak: közel 40 százaléka az eseteknek adathalász incidens volt; 25 százalék bombafenyegetésként került bejelentésre; az esetek több, mint 15 százalékában valamilyen laptop fizikai ellopása történt; az esetek 12 százalékában pedig DDoS támadás áldozatává vált az intézmény. A 11 esetben elkövetett bombafenyegetés mindegyike egyetlen intézményhez volt köthető, amely intézmény az orosz és ukrán piacon is jelen van. A bombafenyegetés vélhetően az orosz-ukrán konfliktushoz köthető. A bombafenyegetéseket elektronikus levélben egy korábban használt e-mail címre küldték tört magyarsággal, cirill betűk felhasználásával.

A kritikus incidensek esetén is hasonló eloszlás figyelhető meg a hatósági értesítések tekintetében (25. ábra).

25. ábra
Kritikus incidens darabszám, a hatóság értesítések függvényében



Túlnyomó részben a bankok és a biztosítók érintettek, ahol hibákból, üzemzavarokból és rosszindulatú tevékenységekből fakadnak az incidensek. A Pilot projekt során összesen 37 kritikus incidens került hatósági bejelentésre, amely 29 hibát és üzemzavart tartalmaz.

A kritikus incidensek esetén – hasonlóan a teljes incidenspopuláció elemzésekor megállapított arányhoz – hozzávetőlegesen az esetek öt százalékban kellett az MNB-n túl egyéb hatóságot értesíteni.

A vonatkozó incidensbejelentések során két hazai hatóság került megjelölésre: NBSZ-NKI és a NAIH.

A kritikus incidensek esetén a hatósági értesítések során két kiváltó ok került azonosításra: rosszindulatú internetoldali hálózati támadás, illetve DDoS támadás.

4. keretes írás
Egy európai szintű incidens esettanulmánya

Az európai uniós nemzetközi szabályozói törekvések alapvető koncepciója, mind a pénzügyi, mind más szektorokkal kapcsolatban, hogy a gazdasági szereplők határon átnyúló szolgáltatásokkal járulnak hozzá az európai közös piac fejlődéséhez. A határon átnyúló szolgáltatások digitalizációs folyamatait lehetővé tevő globális infrastruktúrának kiemelten fontos az ellenállóképessége, annak érdekében, hogy a kommunikációs csatornák megszakítás nélkül elérhetőek legyen. A kommunikációs infrastruktúrák gerincét adó optikai kábelek vonatkozásában joggal gondolhatnánk, hogy a gazdaság tevékenységekhez elengedhetetlen kommunikációs és infrastrukturális hálózatok mára már immunisak a sikeres támadásokkal szemben.

2022. április 27-én egy ismeretlen személy vagy csoport szándékosan átvágott több, létfontosságú optikai kábelt Párizs közelében[30]. A vandalizmus sorozat Franciaország történetének egyik legjelentősebb internetes infrastruktúra ellen irányuló támadása volt, és rávilágít a kulcsfontosságú, összekapcsolt kommunikációs hálózatok sebezhetőségére.

[30] WIRED UK: The Unsolved Mystery Attack on Internet Cables in Paris (Elérhető: https://www.wired.co.uk/article/france-paris-internet-cable-cuts-attack)

Az internetes hálózat elleni támadások április 27-én a hajnali órákban kezdődtek, és az elkövetők körülbelül két óra leforgása alatt a francia főváros körül három helyszínen vágtak el kábeleket. A hatóságok szerint mindhárom incidens nagyjából ugyanabban az időben történt, ráadásul mindhármat azonos módon hajtották végre. A kábeleket úgy vágták el, hogy a lehető legnagyobb fizikai kár keletkezzen, tudatosan megnehezítve a javítási folyamatokat. Az incidenssorozat kapcsán két tény emelkedik ki, amelyek megkülönböztetik őket a távközlési tornyokhoz és az internetes infrastruktúrához kapcsolódó eddigi incidensektől. Először is a támadások összehangoltsága, a párhuzamos időbeni bekövetkezések egy szervezői hátteret sugall, illetve az okozott kár mértéke, ami arra utalhat, hogy a támadók célja a francia kommunikációs hálózatok tudatos bénítása volt. Mivel Franciaországban általában az internetes gerinchálózathoz tartozó optikai kábelek követik a már meglévő fizikai infrastrukturális elemeket, ezért annak, aki végrehajtotta a támadásokat, pontos ismeretekkel kellett rendelkeznie a kábelek nyomvonaláról.

Éppen ezért a francia hatóságok kiemelt figyelemmel kísérték az incidenst az első pillanattól fogva. A francia ügyészség nyomozást indított, amelyet a védelmi minisztérium központi hírszerzési hatósága (DGSI), valamint az igazságügyi rendőrség támogatott, mivel az incidenst követően a hatóságok fenntartották annak a lehetőségét, hogy terrortámadás történt.

Az incidens hatására Franciaország-szerte tapasztalhatóak voltak kiesések az internet elérésben, valamint a mobilhálózatok is túlterhelődtek a terheléselosztási próbálkozások következtében. A károk az eredetileg bejelentettnél sokkal nagyobb kiterjedésűek voltak, hiszen ma már tudjuk, hogy egész Európára és számos európai intézményre erős hatást gyakorolt.

Az incidensnek magyarországi érintettsége is volt, egy európai kitettséggel rendelkező pénzügyi szolgáltató tapasztalt napokkal később jelentős mértékű szolgáltatáskiesést több folyamattámogató rendszerénél. Korábban a magyar pénzforgalom történetében 2008-ban fordult elő a párizsihoz hasonló incidens, amikor ismeretlen tettesek két Határ út melletti kábelaknában rongáltak meg és tulajdonítottak el 36 telekommunikációs törzsvezetéket. A rongálás eredményeként a vezetékes internetszolgáltatás, valamint 20 ezer vezetékes telefonkapcsolat elérhetetlenné vált, amely több száz kerületi hivatalt és céget érintett. A bankközi elszámoló rendszer működését egy napra megbénította az eset. A távközléssel kapcsolatos szolgáltatások nagy része is leállt egy időre az országban.

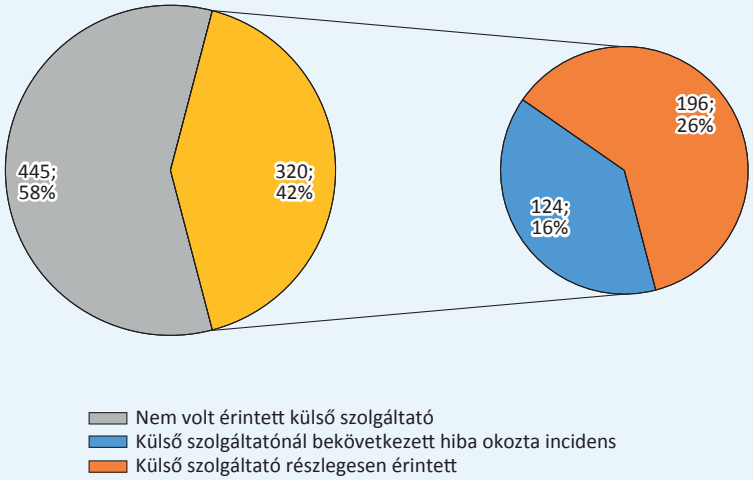
Bár a Párizsi incidenst a szolgáltató hamar elhárította, illetve az ügyfelekre gyakorolt hatása a kiesésnek elenyésző volt, az eset rávilágított, hogy egy fizikai biztonsági incidens begyűrűző hatásai határokon átívelve is kifejthetik magukat.

A Pilot projekt lezárulta után újabb nagy horderejű, kommunikációs kábelek megrongálását érintő incidens történt Európában: a német vasúthálózat egy részét bénította meg egy szabotázsakció[31]. Az eseteket nézve fel kell tennünk magunknak azt a kérdést, hogy egy újabb tendenciát látunk-e kibontakozni, vagy csupán véletlen egybeesésről van szó.

[31] POLITICO: 'Sabotage' causes major train disruption in northern Germany (Elérhető: https://www.politico.eu/article/sabotage-causes-major-train-disruption-northern-germany/)

A bejelentett incidensek során a harmadik felek érintettségét elemezve az esetek 42 százalékában külső szolgáltató is érintett volt (26. ábra). A 320 külső szolgáltatói érintettséggel rendelkező incidensek között hozzávetőlegesen 40 százalékos arányban, 124 esetben fordult elő olyan incidens, amelyeket egy, a külső szolgáltatónál bekövetkezett hiba okozott, ezért az esetek többségében a gyökérokok elemzését is annak a külső szolgáltatónak kellett elvégeznie, amelynél a hiba bekövetkezett, fellépett.

26. ábra
Külső szolgáltatói érintettség aránya



A harmadik feleket is érintő incidensekről legnagyobb számban a banki és pénzügyi infrastruktúra elemek tekintetében számoltak be az intézmények, gyakran egyedi, korábban nem tapasztalt működési problémákat azonosítva, amivel a kiszervezési tevékenységek kockázatelemzése során érdemes számolni. Az incidensek egy része működési problémákat okozott, melyek gyökérokai között előfordultak az ellátási láncban bekövetkezett meghibásodások, ezek eredménye számos esetben szolgáltatáskiesés lett. Egy másik csoportot alkottak a rosszindulatú tevékenységek, ahol az incidensek kiváltó oka legtöbbször célzott szolgáltatásmegtagadás támadás (DoS) volt. Ezekben az esetben a hibák általában kapcsolódási problémákat és lassulásokat eredményeztek.

A javító intézkedések elemzése azt mutatja, hogy további incidensek elkerülése érdekében ezekben az esetekben fejlesztések és módosítások kerültek bevezetésre, hogy a későbbiekben ugyanilyen okra visszavezethető incidens minél ritkábban forduljon elő.

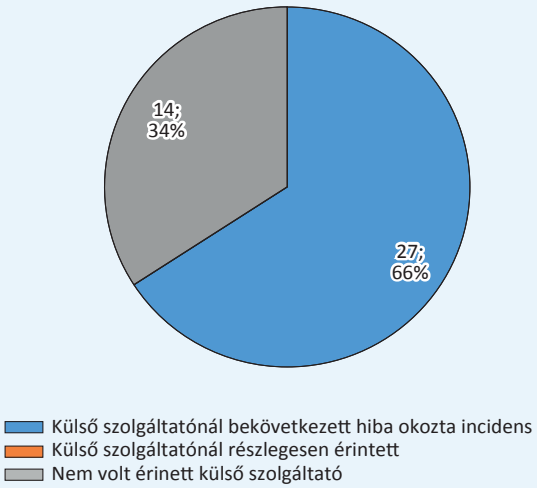
Az ENISA ellátási lánc elleni támadásokról szóló riportja [32] is rámutat, hogy évek óta tapasztalható az ellátási lánc ellen elkövetett támadások gyakoribbá válása, mivel az ellátási láncok nagyobb és adott esetben gyengébb ellenállóképességű támadási felületet biztosíthatnak, mint a pénzintézetek szigorú határvédelmi rendszerei. A támadóknak az ellátási lánc sikeres feltörése után új lehetőségei lehetnek a rendszerekbe való behatolásra, sok esetben a megbízhatónak ítélt informatikai környezetből. A magyar pénzintézeti szektorban is történt már ilyen, kiszervezett szolgáltatót érintő sikeres támadás, azonban az esetről az MNB nem a Pilot projekt keretében értesült és a támadó nem lépett tovább a szolgáltatóval kapcsolatban álló pénzintézetek irányába.

A külső szolgáltatók igénybevétele tehát továbbra is egyik oldalról lehetőség, másik oldalról megnövekedett biztonsági kockázat, amit fontos figyelembe venni már a szolgáltatások kiszervezésének tervezési fázisában csakúgy, mint folyamatosan ellenőrizni a szolgáltatási szakaszban, és körültekintően lezárni a kivezetési fázisban.

[32] Elérhető: https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks

A kritikus incidensek külső szolgáltatókhoz való kapcsolatának vizsgálata során jelentős különbség látható, hiszen a teljes incidenshalmazzal összehasonlítva, a harmadik fél érintettség aránya fordított, több mint 66 százalékos arányt mutat. Az összes olyan incidenst nézve, amelyeknél volt érintett külső szolgáltató (26. ábra), az esetek 61 százalékában a harmadik fél csak részlegesen volt érintett. Ehhez képest a kritikus incidensek esetében a 41 bejelentett kritikus incidensből 27 incidens gyökérok vezethető vissza egy harmadik félnél bekövetkezett hibára (27. ábra).

27. ábra
Kritikus incidens darabszám és arány, ahol volt külső szolgáltatói érintettség



A külső szolgáltatónál bekövetkezett hiba okozta kritikus incidensek a legnagyobb számban a banki rendszereket érintették, egyedi, korábban nem tapasztalt működési problémák miatt. Az incidensek működési problémákat okoztak, amik szolgáltatáskiesést eredményeztek. Az üzemzavar miatt keletkezett incidenseknél rendszer/szolgáltatás elérésével, SMS küldéssel, adatfelvitellel és adatküldéssel kapcsolatos hibák léptek fel, melyek megoldásához átlagosan hét óra kellett.

5. keretes írás
Külső szolgáltatói érintettségű kritikus incidensek esettanulmányai

A Pilot tanulságai alapján kiemelt célpontot képviseltek a pénzügyi szektor külső szolgáltatói a célzott támadások körében. Egyre inkább jellemző a szektorra harmadik felek érintettsége, amely megnöveli az intézmények kitettségét, hiszen nemcsak a saját digitális vagyonuk, hanem a szolgáltató harmadik feleké is célponttá válik. Jól illusztrálja a folyamatot, hogy az ügyfélszám érintettséggel ellátott kritikus incidensjelzések közül a legnagyobb, 64000 ügyfelet érintő jelzés kiváltó oka egy külső szolgáltatónál bekövetkezett működési hiba. A hiba eredményeként lakossági és vállalati ügyfelek tízezrei számára váltak elérhetetlenné bizonyos szolgáltatások, úgy, hogy az érintett intézmény az incidens technikai kezelésében ténylegesen nem tudott részt venni.

A külső beszállítók mellett a kártyaszolgáltatók is kiemelt célpontok lehetnek fejlettebb támadók körében. Így történt például, hogy az egyetlen olyan DDoS támadás, amely kritikus incidensnek minősült, egy 3D Secure Access Control Server (3DS) rendszer beszállítója ellen irányult. A kártyatulajdonosok biztonsági hitelesítésért felelős rendszer elérhetetlenné vált, komoly működésbeli gondokat okozva ezzel egy hazai pénzintézetnél. Ehhez hasonló támadásokat gyakran láttunk az elmúlt pár év során. Általánosságban, és főleg a DDoS jellegű támadásoknál fontos megjegyezni, hogy sok esetben, ha valakit támadás ér, az jelenthet figyelemelterelést vagy erőforráselvonási kísérletet is. A kártyaszolgáltatók ellen irányuló támadásokat például sok esetben követik más jellegű kártyás visszaélések, amelyek során a támadók konkrét haszonszerzés céljából próbálják meg kihasználni a 3DS elérhetetlensége esetén használt gyengébb biztonsági mechanizmusok életbe lépését egy többlépcsős támadás során.

A bemutatott kritikus incidensek továbbá felhívják a figyelmet a harmadik fél kockázatokra, egy olyan témakörre, amelyre a következő időszakban egyre nagyobb figyelem fog irányulni. Az incidensek tanulsága, hogy a felelősség nem kiszervezhető, akkor sem, ha beszállítóknál bekövetkezett problémákhoz vezethetőek vissza az incidensek.

A rosszindulatú tevékenységek vizsgálata során az incidens kiváltó ok legtöbbször elavult komponens ismert hibájának kihasználásán alapult, illetve célzott szolgáltatásmegtagadás támadás volt, ami jelentésre is került a megfelelő hatóságnál.

A már korábban előfordult incidensek vagy rosszindulatú tevékenység miatt történtek, vagy SMS küldéssel kapcsolatos fennakadások miatt következtek be.

V. Technikai adatok bemutatása

1. A PILOT PROJEKT SORÁN GYŰJTÖTT HARDENIZE ADATOK BEMUTATÁSA

A kiberbiztonságban hardeningnek nevezzük azt a folyamatot, amelynek keretében a rendszer különböző rétegeiben csökkentik a rendszer sebezhetőségét, ellenállóvá teszik az esetleges támadásokkal szemben. Történhet ez a rendszer biztonsági szempontú átkonfigurálásával vagy további eszközök beépítésével. A hardening hatékonyságát különböző eljárásokkal lehet mérni, például a konfigurációs beállítások megfelelőségének, valamint az alkalmazott védelmi technikák meglétének vizsgálatával.

A fenyegetettségi térkép projekt kidolgozása során úgy véltük, hogy ugyan a rendszereknek nagyon sokféle sérülékenysége lehet, illetve számtalan okból és felületen érhetik támadások, incidensek, de a támadások jelentős része az interneten elérhető célpontokra fókuszál, ezért az egyik fontos támadási felületet a domainek[33] jelentik.

Ezért a Pilot projekt során a NBSZ-NKI által végzett Hardenize[34] vizsgálatokkal egészítettük ki a vizsgál időszakot, hogy feltárjuk az esetleges összefüggéseket az incidensek és a domainbeállítások és védelmi megoldások között a részt vevő intézmények esetében, valamint, hogy a jelen kimutatással felhívjuk a figyelmet az egyes domainbeállítások megfelelőségére vagy az esetleges hiányosságokból adódó kockázatokra.

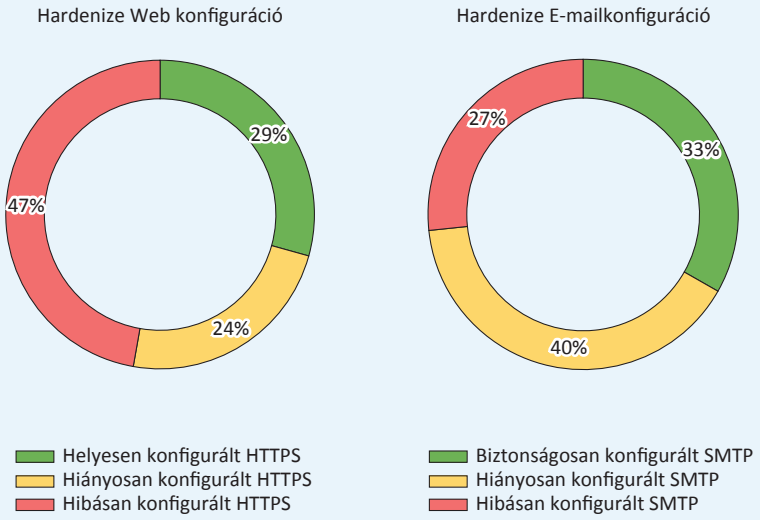
A Hardenize egy olyan webes alkalmazás, amely képes a domainbeállítások és védelmi megoldások vizsgálatára. Az alkalmazás megadott domainnév alapján lefuttat egy vizsgálatsorozatot és egy riportot ad a domain konfigurációjáról. A Hardenize külön vizsgálja a DNS (Domain Name System, névfeloldó szolgáltatás), az e-mail és a webes szolgáltatások megfelelőségét, különböző alkalmazásspecifikus szempontok alapján. Így a Hardenize vizsgálat egy átfogó biztonsági vizsgálati eszköz, ami egy rövid vizsgálati időablakban figyeli meg a domain-, e-mail- és webbeállításokat és konfigurációt. Az NBSZ-NKI a Pilot projektben részt vevő intézmények által szolgáltatott domainadatok alapján Hardenize vizsgálatokat végzett a részt vevő intézmények internet felől elérhető rendszerein, amely a publikusan elérhető rendszer konfigurációs beállításokat hivatott vizsgálni.

A kimutatások alapján, ami a Pilot projektben részt vevő intézmények által átadott domainlistákról készült, előállítottunk néhány ábrát. Ezeken az ábrákon bemutatjuk, hogy az intézmények a biztonsági beállítások terén milyen szinten állnak. A web- és e-mailkonfigurációs ábrákat úgy állítottuk össze, hogy azok egy általános és technikailag lebontott látképet adjanak vissza, ezzel könnyen megmutatva, hogy melyik területen kell erősíteni a biztonsági beállításokat az intézmények részéről, hogy szolgáltatásaik kevésbé legyenek kitettek a kiberfenyegetéseknek.

[33] „A tartománynév (angolosan domainnév, illetve doménnév) az Internet egy meghatározott részét, tartományát egyedileg leíró megnevezés. A tartománynevek kiosztása és értelmezése a Domain Name System (DNS) szabályai szerint, hierarchikusan történik.” Forrás: Wikipedia

[34] Elérhető: https://www.hardenize.com/

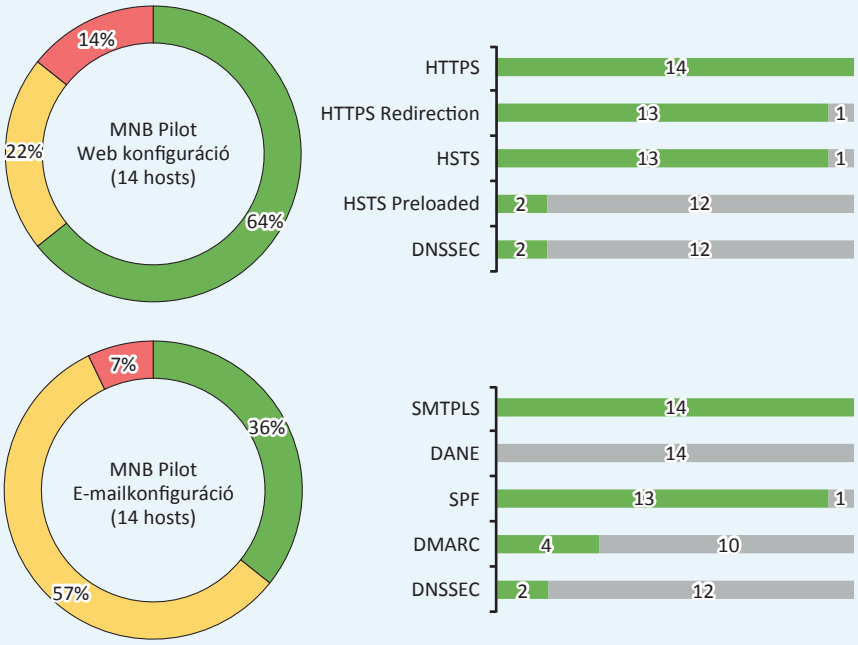
28. ábra
NBSZ-NKI Magyarországra vonatkozó Hardenize riport infrastruktúra- és e-mailbeállítás összesítés



Forrás: Hardenize, HU resilience dashboard

A Hardenize által közzétett, Magyarországra vonatkozó NBSZ-NKI Hardenize riport[35] kevesebb adatpontot mutat, mint amennyivel riportunk elemzései számolnak. A teljes magyarországi Hardenize riport 352 adatpontból áll, azon belül a riportban a kiemelten MNB Pilot projekthez kapcsolódó adatpontok száma 14. Mindeközben a Pilot projekt keretében rendelkezésünkre bocsátott adatpontok száma meghaladta az ezret. Az eltérés abból fakad, hogy az intézmények által átadott teljes domainlista intézményenként akár ötven domaint is tartalmazott.

29. ábra
NBSZ-NKI Magyarországra vonatkozó Hardenize riport Pilot projekt érintettséggel rendelkező infrastruktúra- és e-mailbeállítás összesítések



Forrás: Hardenize, HU resilience dashboard

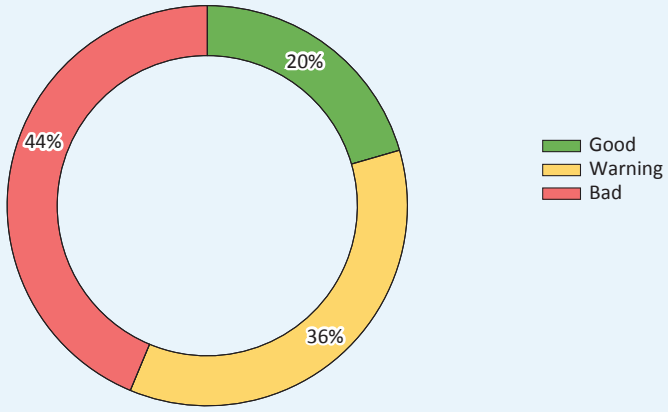
[35] Elérhető: https://www.hardenize.com/dashboards/hu-resilience/

A Hardenize dashboardon megtekinthető infrastruktúra- és e-mailbeállítás összesítések a Hardenize saját metodológiája alapján készültek el és kerültek bemutatásra. Az NBSZ-NKI Hardenize riportban bemutatott 352 magyarországi hoszt infrastruktúrabeállításainak összesítését bemutató ábra (29. ábra), hasonlóan a Pilot projekt érintettséggel rendelkező hosztok lebontásában a web, e-mail és DNS-konfigurációk összesítését és helyességét hivatott bemutatni. Az MNB kiberfenyegetettségi térkép keretében készített, NBSZ-NKI Hardenize adatokon alapuló ábrák minden esetben a beállítások és konfigurációk meglétének vagy hiányának a tényét mutatják be. Az ábrák egy átfogóbb képet adnak az intézmények eszközeinek konfigurálásáról és ezáltal az internet felől látható biztonsági helyzetükről.

2. INFRASTRUKTÚRABEÁLLÍTÁSOK

Webkonfiguráció

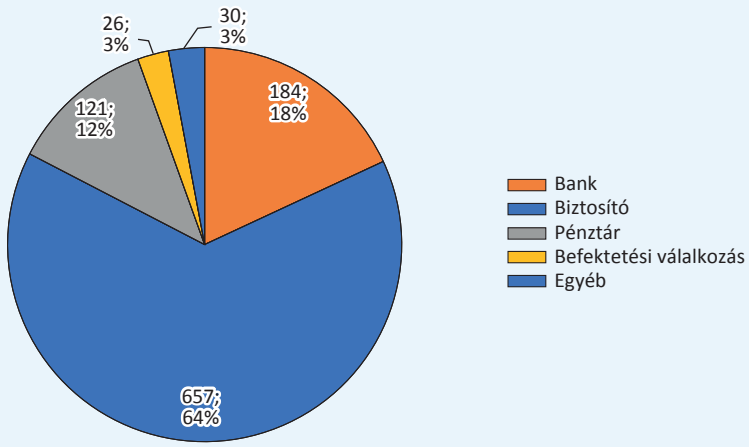
30. ábra
Összetett Webkonfiguráció teljes Pilot projekt domain adatokra nézve



A webkonfiguráció vizsgálata egy magasszintű áttekintést nyújt a domainek webes biztonsági beállításairól. A Pilot projektben résztvevő 39 intézményből 37-hez érkezett domain adat. Az összes, a résztvevők által megadott domain webkonfigurációs védettségét mutatja a 30. ábra. A webkonfiguráció áttekintése négy tulajdonságot elemez: a HTTPS, HSTS, HTTPS Redirection, valamint a HSTS Preloaded paramétereket, ezen technikai fogalmak tisztázására a későbbiekben térünk ki. „Good" értékelést kapott az a domain, amelyiknek mind a négy paramétere be volt állítva. A domainek 20 százaléka kapott „Good" értékelést. Ennek oka lehet, hogy az intézmények az összes webkonfigurációs paramétert csak a legfontosabb (kritikus) rendszereik (azokhoz tartozó domainjeik) kapcsán állítják be. Vélhetően a beállítás időigényes volta miatt a kevésbé kritikus rendszerek esetében nem minden beállítás valósult meg.

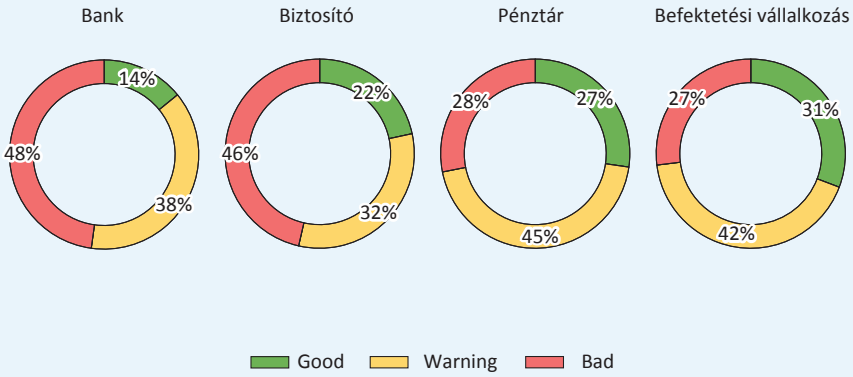
„Warning" értékelést, azaz figyelmeztető értékelést kaptak azok a domainek, amiknek a paraméterei közül a HSTS és a HSTS Preloaded nem lett beállítva. „Warning" értékelést a domainek 36 százaléka kapott, ezen beállítások fontossága, hogy HTTP protokollon keresztül egyáltalán ne legyen kommunikáció és minden forgalom legyen rákényszerítve a titkosított adatcsatornára. „Bad" értékelést azok a domainek kaptak, amiknek a paramétereiből nem került beállításra a HTTPS vagy a HTTPS Redirection, ami az intézményi domainek 44 százalékában fordult elő. A HTTPS és a HTTPS Redirection beállítása kritikus fontosságú, mivel nélkülük az üzenetek titkosítatlan kommunikációs csatornákon keresztül közvetítődnek. Ezek a beállítások azért sem megfelelőek élesüzemi rendszerek esetén, mert a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről szóló 42/2015. (III.12) Korm. rendelet (a továbbiakban: 42/2015. (III.12) Korm. rendelet) előírja az adatátvitel bizalmasságának biztosítását az intézmények számára.

31. ábra
A domainek száma és aránya az egyes intézménytípusokra



Az intézménytípusok közül a legnagyobb domain számossággal a biztosítók rendelkeznek, amely a teljes Pilot projektben résztvevő intézményi domainek több mint 60 százalékát jelenti. Amíg a biztosítókhoz köthető domainek száma 657 volt, addig a második legtöbb domainnel rendelkező bankoknál ez a szám csak 184 volt.

32. ábra
A legtöbb domainnel rendelkező négy intézménytípus webkonfigurációinak értékelése



A legtöbb domainnel rendelkező négy intézménytípus webes beállításait láthatjuk az 32. ábrán. Az ábra a HTTPS, HSTS, HSTS Preloaded és a HTTPS Redirection beállítások alapján a 30. ábrához hasonlóan „Good”, „Warning” és„Bad” értékeléseket mutatnak be. A HTTPS, HTTPS Redirection, HSTS és HSTS Preloaded technikai fogalmak tisztázására a későbbiekben térünk ki.

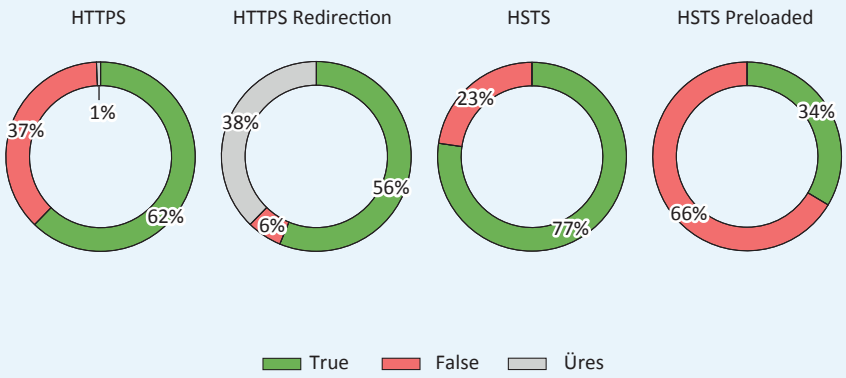
Az első ábra a bankoké, mert a kibertámadásoknak ezen intézmények vannak a legjobban kitéve. Látható, hogy a domainjeik beállítása közel 50 százalékban nem megfelelő, azaz domainjeik majdnem felénél nem állították be a HTTPS vagy a HTTPS Redirectiont. A kommunikáció titkosítatlan jellege miatt beékelődéses támadás hajtható végre. Ennek oka lehet az, hogy a domainlistában szerepelnek olyan elemek is, amelyek vagy az intézmények belső céljait szolgálják, vagy csak speciális módon lehet elérni őket, vagy használaton kívüliek és megszüntetésre várnak. A Pilot projektben részt vevő tíz darab biztosító közel háromszor több domainnel rendelkezik, mint a résztvevő bankok, a nemmegfelelőségi arányuk („bad” értékelés) közel azonos. A biztosítóknál azonban a megfelelően beállított domainek aránya szignifikánsan magasabb, mint a bankoknál: vélhetően több produktív célú domain üzemel, ahol kritikus a megfelelő beállítás.

A maradék két intézménytípusnál (pénztárak és befektetési vállalkozások) mérhető értékek eltérnek a bankok és biztosítók adataitól. A magyarázat valószínűleg az, hogy ezen intézménytípusok domainjeinek száma átlagosan jóval kevesebb, így arányaiban kevesebb a megszüntetésre váró, hibásan beállított vagy tesztcélokra, belső használatra szánt domain. A kevesebb domainnel rendelkező intézménytípusok esetében a warning kategória volt a legnagyobb. A megfelelő beállítások aránya nagyobb volt, a nem megfelelő domainek aránya pedig kisebb, mint a bankoknál vagy a biztosítóknál.

HTTPS, HTTPS Redirection

A webhelyeknek valamilyen mechanizmussal biztosítaniuk kell, hogy látogatóik tudják, a megfelelő helyen vannak. A legegyszerűbb megoldás a HTTP kapcsolat TLS (Transport Layer Security) fölé helyezése – erre HTTPS-ként hivatkozunk. A HTTPS az információ bizalmasságát, hitelességét és sértetlenségét is biztosítja. Azon rendszerek, amelyek nem támogatják a HTTPS-t, a kommunikáció során nem biztosítják ezen tulajdonságokat, az adatok módosításával és hamisításával kapcsolatosan védtelenek lesznek. Működő TLS (és HTTPS) szolgáltatáshoz szükséges egy aszimmetrikus kulcspár, a publikus kulcsból készített tanúsítvány és a tanúsítvány hitelesítése egy minősített hitelesítési szolgáltatóig visszavezethető tanúsítványlánccal. A HTTPS elérhetősége csak a webes tartalommal rendelkező (HTTP protokollal elérhető) hosztok esetében vizsgálható, tehát a bejegyzett, de tényleges weboldalt nem tartalmazó domainek esetében nem. A HTTPS elérhetősége önmagában még kevés: a megfelelő üzembe helyezéséhez a webhelyeknek minden nem biztonságos (egyszerű szöveges HTTP) forgalmat át kell irányítaniuk a titkosított kapcsolatra (HTTPS-re) a webszerver oldalán. A megközelítés biztosítja, hogy ne kerüljenek nyilvánosságra érzékeny adatok, illetve ne legyen módosítható az adattartalom egy beékelődéses támadási formában, még akkor sem, ha a támadó valamilyen módon a HTTP (titkosítatlan) kapcsolatra tereli a felhasználói forgalmat. A HTTPS Redirection csak azon hosztok esetében vizsgálható és értelmezhető, ahol HTTPS protokollon elérhető a szolgáltatás.

33. ábra
Webkonfiguráció paraméterei a teljes Pilot projekt domainadatokra nézve



A 33. ábrán látható, hogy az intézmények domainjeinek 62 százalékában elérhető a HTTPS és 56 százalékban a HTTPS Redirection, ami arra enged következtetni, hogy az intézmények azon domainjei megfelelően be vannak állítva, amelyek éles üzemet látnak el. HTTPS a megadott domainek 37 százalékára nincsen beállítva, míg a HTTPS Redirection esetén azt láthatjuk, hogy a hat százaléka nincsen beállítva. A nem vizsgálható eseteket az ábrán szürke szín jelöli, amely az üres értékeket emeli ki. Ezáltal a 38 százalékból 37 százalék az, ahol a HTTPS hiánya miatt nem vizsgálható a beállítás, és egy százalék az, ahol a vizsgált domain elérhetetlensége miatt nem határozható meg az érték. Ezen domainek nagy része vélhetően belső használatra szánt, ami nem feltétlen igényli a szigorú beállításokat. A következő két diagram csak azokra a domainekre vonatkozik, ahol a HTTPS vizsgálható volt.

HTTP Strict Transport Security (HSTS); HSTS Preloaded

A HTTP Strict Transport Security (HSTS) egy HTTPS-bővítmény, amely arra utasítja a böngészőket kliens oldalon, hogy használják a HTTPS-t a webhelyen, kényszerítsék ki a biztonságos kommunikációt. A minden böngészőben kötelezően működő HSTS megoldás HTTPS-re tereli a forgalmat. Amennyiben a böngésző az első hozzáférés során a kapott HTTPS válaszüzenetben HSTS fejlécet kap, akkor kötelezzük arra, hogy minden további kommunikációt is csak HTTPS-en keresztül hajtson végre. A megoldás dinamikus, hiszen az első válasz után kényszeríti ki a HTTPS megkerülhetetlenségét.

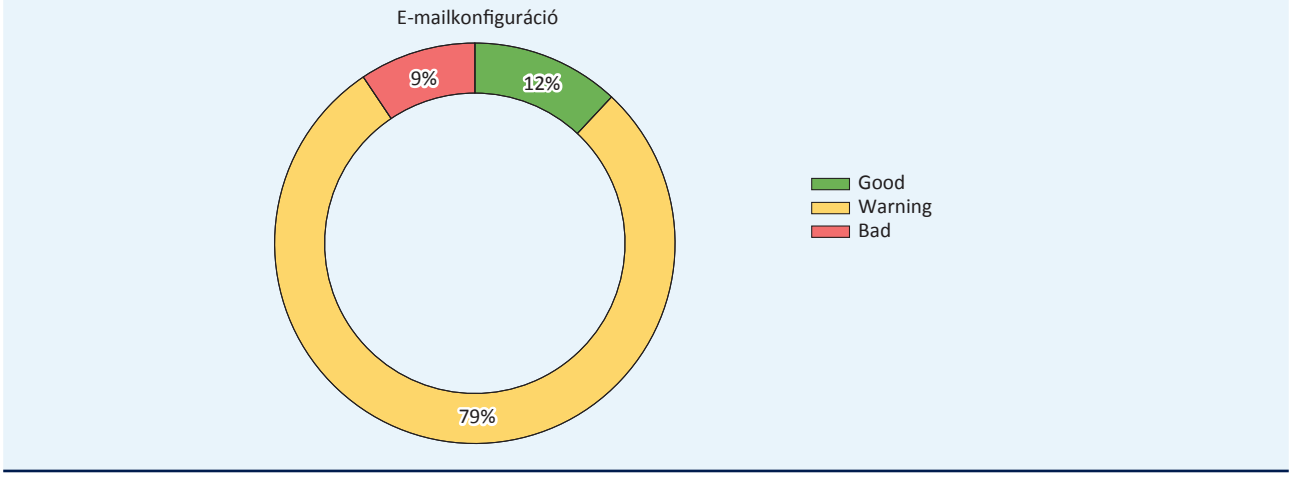
HSTS nélkül az aktív hálózati támadások könnyebben végrehajthatók: egy támadó kényszerítheti, hogy a kliens HTTP-n keresztül (titkosítás nélkül) küldjön kérést a szerver felé, azonban így kompromittálódik a kliens által küldött információ. A HSTS funkciójából adódóan csak azon hosztok esetében vizsgálható, ahol HTTPS protokollon elérhető szolgáltatás. A HSTS Preloaded szintén kliensoldali védelmi megoldás, ám itt a böngésző statikus tartalom alapján kényszeríti ki a HTTPS használatát. A megoldás lényege, hogy a böngészőbe bedrótozott lista alapján, HSTS fejlécek nélkül is, a böngésző csak HTTPS-sel hajlandó próbálkozni a lista elemeihez való csatlakozás során. Ez azt jelenti, hogy már az első látogatáskor is betartható a szigorú biztonság. A megközelítés biztosítja a ma elérhető legjobb biztonságot a webes kommunikációban. Mind a HSTS, mind a HSTS Preloaded beállítások csak azon hosztok esetében vizsgálható, ahol HTTPS protokollon elérhető szolgáltatás, ezért az ábrák az arányok bemutatásakor nem veszik figyelembe a domainek 37 százalékát, más szóval a HSTS és HSTS Preloaded ábrák egy kisebb adathalmaz arányait mutatják be.

Az ábrán látható, hogy az intézmény domainek 77 százalékánál beállították a HSTS-t, a domainek maradék 23 százalékában pedig elvileg lehetséges lenne a HTTPS-ről HTTP-re terelés. Azért csak elvileg, mert a kijátszhatóság nagyban függ a webalkalmazástól: azt, hogy valóban lehetséges-e HTTP-re terelni a forgalmat, csak egy konkrét kísérlet keretében lehetne felderíteni. A HSTS preloaded megfelelőségi aránya 34 százalék, ami azt jelenti, hogy a HTTPS-sel rendelkező domainek csupán 34 százalékát regisztrálták a HTTPS-t kötelezővé tevő listában (a https://hstspreload.org/-on).

A teljesen megfelelően beállított domainek közé sorolhatók az intézmények root domainjei, amivel az ügyfelek is kommunikálnak. Ahol nem állították be a HSTS-t, illetve HSTS preloadot, olyan domainek lehetnek, amik kevésbé kritikus információ megjelenítésére, megosztására, vagy kicserélésére szolgálnak, vagy nem kommunikálnak éles adatokkal.

E-mailkonfiguráció

34. ábra
Összetett e-mailkonfiguráció teljes Pilot projekt domainadatokra nézve

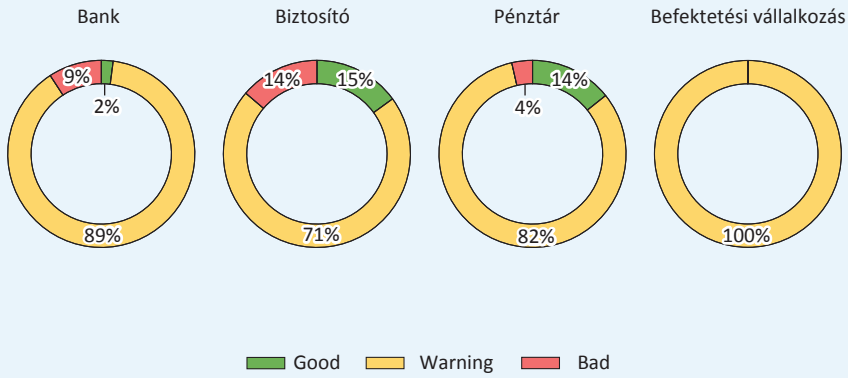


Az e-mailkonfiguráció vizsgálata a domainek elektronikus levelezés vonatkozású biztonsági beállításait hivatott bemutatni.

Az értékelés az e-mail konfiguráció esetében három fő tulajdonságon alapul: az SMTPTLS, SPF, valamint a DMARC paraméterekből, ezen technikai fogalmak tisztázására a későbbiekben térünk ki. „Good” értékelést kapott az a domain, amelyikben az összes paraméter be volt állítva. „Warning” értékelést, azaz figyelmeztető értékelést kaptak azok a domainek,

amelyekben az e-mailkonfigurációs paraméterek közül az SPF vagy a DMARC került beállításra. „Bad” értékelést azok a domainek kaptak, amikben az e-mailkonfigurációk közül az SMTPTLS nem került beállításra. Így az ábrán látható, hogy az intézmények 12 százalékának a beállításai jók voltak, a 79 százalékuk kapott figyelmeztető értékelést, valamint az intézmények kilenc százaléknak a beállításai nem megfelelőek. Valószínű, hogy a domainek közül nem mindegyiket használják levelezésre. Ma már SPF és DMARC nélkül elektronikus levelet küldeni kihívást jelenthet. A nagy levelező szolgáltatók, mint pl. a Gmail, Outlook, AOL, Yahoo, stb., nem veszik át azon domainek leveleit, amelyekre nincs SPF beállítva. Vélhetően kockázatarányosság alapján azon root domainek megfelelően vannak beállítva, amiket az ügyfelekkel való elsődleges kapcsolattartáshoz használnak az intézmények.

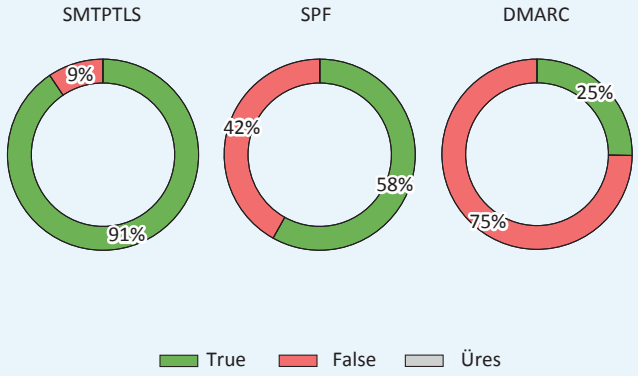
35. ábra
A legtöbb domainnel rendelkező négy intézménytípus e-mailkonfigurációs beállításai



A fenti 35. ábra a négy legnagyobb intézménytípus e-mailkonfigurációs beállításainak megfelelőségét szemlélteti. Az e-mailkonfiguráció értékelése az SMTPTLS, SPF és DMARC beállítások alapján épül fel. Az SMTPTLS, SPF és DMARC technikai fogalmak tisztázására a későbbiekben térünk ki.

Az e-mailkonfigurációk az intézménytípusok tekintetében közel azonosak. A nem megfelelően beállított rendszerek aránya szemmel láthatóan kisebb, mint a webkonfiguráció esetében volt: a bankok SMTP szervereinek kilenc százaléka nem megfelelő módon konfigurált, az SMTPTLS nincs beállítva, így védtelenek a beékelődéses támadások ellen. A biztosítóknál ugyanez 14 százalékról, a pénztáraknál négy százalékról mondható el, a befektetési vállalkozásoknál nem volt rosszul konfigurált SMTP szerver. Mivel a biztosítók és a bankok a teljes domainlistának több mint 60 százalékát alkotják, esetükben könnyebben megjelenhet egy-egy rosszul (vagy félig) bekonfigurált levelezőszerver. A megfelelő érték („Good”) magába foglalja az intézmények alapértelmezett domainjeihez kapcsolódó levelezőszervereket, amelyeknél az ügyfelekkel folytatott kapcsolattartás miatt elkerülhetetlen a szigorú beállítás. Érdekes, hogy a befektetési vállalkozások esetében nem volt „Good” minősítés, ami arra utal, hogy a DMARC funkciót a befektetési vállalkozások nem használják, így az üzenetek hitelesítése és a visszaélésekkel kapcsolatos visszajelzési lehetőség nem minden esetben áll rendelkezésre.

36. ábra
E-mailkonfiguráció paraméterei a teljes Pilot projekt domainadataira nézve



SMTPTLS

Minden e-mailt fogadó gazdagépnek titkosításra van szüksége az e-mailüzenetek bizalmasságának és sértetlenségének biztosítása érdekében. Az egyik legegyszerűbb megoldás az SMTP folyamok TLS felé helyezése (SMTP over TLS). Egy másik lehetőség a már felépített SMTP kapcsolat utáni TLS kiépítés (STARTTLS). A TLS működéséhez érvényes tanúsítvány szükséges, hasonlóan a HTTPS protokoll esetében leírtakhoz. Működő TLS (és SMTPTLS) szolgáltatáshoz szükséges egy aszimmetrikus kulcspár, a publikus kulcsból készített tanúsítvány. A tanúsítvány hitelesítése nem minden esetben történik meg egy minősített hitelesítési szolgáltatóig visszavezethető módon, annak ellenére, hogy ez a teljeskörűséghez elvárható lenne. Az e-mailszervereknek mind küldő, mind fogadó oldalon támogatniuk kell a SMTPTLS-t, valamint megfelelő TLS-konfigurációt és megfelelő tanúsítványokat kell használniuk. Az SMTPTLS megléte csak az SMTP szolgáltatással (MX rekorddal) rendelkező domainek esetében ellenőrizhető. A 35. ábrán látható, hogy az intézmények domainjeinek 91 százalékban be van állítva a SMPTTLS, kilenc százaléknak nincsen az augusztusi scan eredmények alapján.

SPF

A Sender Policy Framework (SPF) lehetővé teszi az intézmények számára, hogy kijelöljenek olyan szervereket, illetve egyéb végpontokat, amelyek jogosultak e-mail üzenetek küldésére a nevükben.

Az SPF beállítások a DNS rekordok szöveges (text) mezőjében kerülnek meghatározásra. Ha az SPF megfelelően van beállítva, a spamforrások (jogosulatlan küldők) könnyebben kiszűrhetőek. Az ábrán látható, hogy az intézmények domainjeinek 58 százalékban be van állítva az SPF, 42 százaléknak nincs az augusztusi scan eredmények alapján. Érdekesség, hogy az Európai Központi Bank a jegybankoktól már több mint tíz éve elvárja az SPF használatát.

DKIM

A DomainKeys Identified Mail (DKIM) egy olyan módszer, amely során az SMTP szerver a kiküldött üzeneteit saját privát kulcsával aláírja.

A validáláshoz használt publikus kulcs az intézmény DNS szöveges rekordjában található, hasonlóan az SPF-hez szükséges információhoz. Amíg azonban az SPF csak IP-címeket és FQDN állomásneveket sorol fel és ezáltal csak a küldő állomások halmazát korlátozza IP-cím, vagy FQDN alapján, a DKIM által szolgáltatott publikus kulcs lehetőséget biztosít az üzenetek egyenkénti validálására is.

A Hardenize külön nem vizsgálja a DKIM működését, csak a DMARC megfelelőségéről mutat visszajelzést.

DMARC

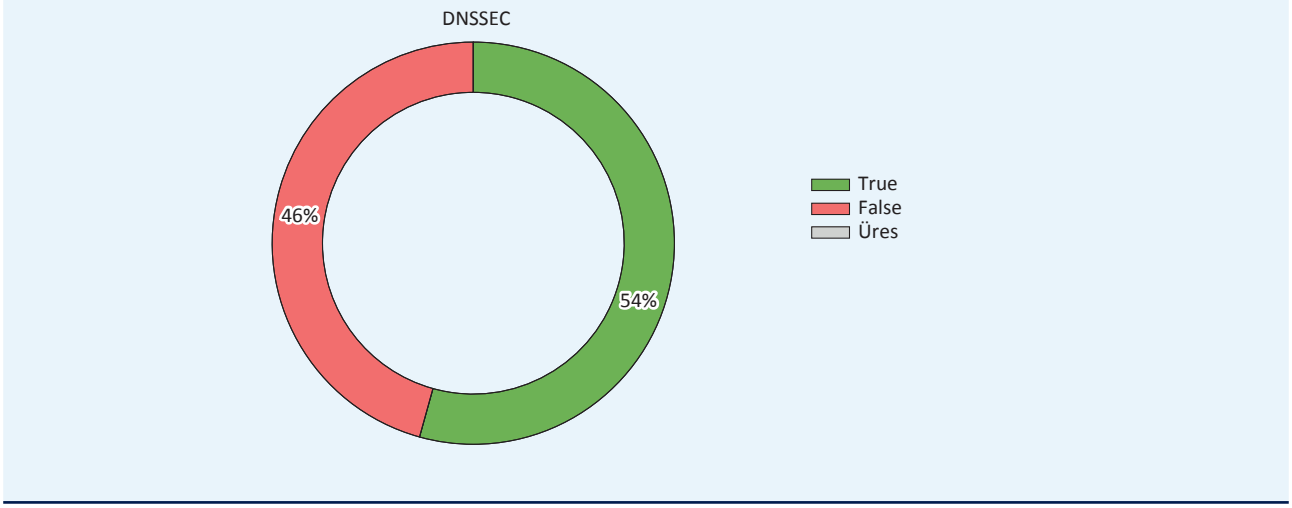
A tartományalapú üzenethitelesítés, jelentéskészítés és megfelelőség (Domain-based Message Authentication, Reporting & Conformance – DMARC) további lehetőségeket biztosít az intézmények számára, hogy az e-mailkommunikációban policy alapú szabályokat határozzanak meg, például hogyan kezeljék a nem hitelesített (SPF és DKIM segítségével nem azonosított) e-maileket, visszajelzést adva a küldő oldalnak. A DMARC bevezetése az SPF és DKIM bevezetése után rendelkezik hozzáadott értékkel, így csak a működő SPF-fel és DKIM-mel rendelkező domainekre vizsgálható.

Az ábrán látható, hogy az intézményi domainek 25 százalékában be van állítva a DMARC, 75 százaléknak nincsen az augusztusi scan eredmények alapján.

3. DNS-KONFIGURÁCIÓ

DNSSEC

37. ábra
DNSSEC-konfiguráció a teljes Pilot projekt domain adatokra nézve



A DNSSEC (Domain Name System SECurity extensions) a DNS-protokoll kiterjesztése, amely kriptográfiai biztosítékot nyújt a DNS-válaszüzenetek hitelességére és integritására. A DNSSEC védelmet nyújt a hálózati támadók ellen, akik képesek manipulálni rekurzív (vagy caching) DNS szervereket, ezzel megóvja az áldozatokat a hamis helyekre történő átirányítástól. A DNSSEC megoldás a DNS válaszok publikus kulcsú kriptográfián alapuló hitelesítésével működik. Az autoritatív DNS-szerverek az átadott tartalmakat a szöveges (text) rekordokban elektronikusan aláírják, a caching DNS-szerverek, vagy az állomások pedig ellenőrizhetik a domain szöveges (text) rekordjában tárolt publikus kulcs alapján a kapott információ hitelességét. Az intézmények domainjeinek 54 százalékban beállításra került a DNSSEC, 46 százaléknál nem. A nem megfelelően konfigurált domainek esetében is lehet olyan indok (speciális célokra vagy belsőleg használhatják az intézmények), ami miatt lehet nem indokolt a beállítás.

4. A HARDENIZE ADATOK TANULSÁGAINAK ÖSSZEFOGLALÁSA

Az NBSZ-NKI által kidolgozott technikai adatbegyűjtést és elemzést a projekt beépítette az elemzési folyamatba, hogy összevethesse a Pilot projekt során tapasztalt incidenselemzéseket és azonosított fenyegetettségi trendeket az NBSZ-NKI által gyűjtött technikai adatokkal. Az egyéni, intézményi konfigurációs adatok alapján elvégzett elemzések azt mutatják, hogy nem állapítható meg egyértelmű összefüggés az egyes intézmények domainkonfigurációinak biztonsági szintje, illetve az intézményeknél bekövetkezett incidensek adatai között. A Pilot projekt során az incidensek zöme nem támadás miatt következett be, hanem működési problémákra volt visszavezethető.

Az NBSZ-NKI az intézmények által szolgáltatott domainadatok alapján a Pilot projekt minden hónapjának elején futtatott egy Hardenize vizsgálatot. Bár a különböző domainkonfigurációs állapotokról hat hónapnyi adatunk van, a technikai adatok ismertetésénél csak az augusztus eleji adatokat használtuk fel. Ennek magyarázata egyrészről, hogy a 2022 augusztusi adatok mutatják be a legfrissebb technikai helyzetképet, másrészről érdemi konfigurációs változásokat nem láthattunk a különböző hónapok között. A vizsgált konfigurációs állapotok között csak pár esetben következett be változás a Pilot projekt hat hónapos időtartama alatt, így megállapítható, hogy a pénzügyi intézményeknél általánosságban nagyobb időtávban változnak a domainekhez köthető konfigurációs paraméterek.

Végezetül levonható az a következtetés, hogy bár az V. fejezetben bemutatott beállítások nem képeznek újdonságot és régóta számítanak bevett gyakorlatnak, a vizsgált intézményi körnél láthatóan nem minden esetben élveznek prioritást.

VI. Módszertan áttekintése

Összefoglalásként a Pilot projekt célja az volt, hogy a projekt során begyűjtött adatok segítségével elkészítsük Magyarország első a pénzügyi szektorra vonatkozó fenyegetettségi térképét, támogatást nyújtva ezzel elsősorban a szektor döntéshozói és szakértői számára, másrészt naprakész fenyegetettségi információt nyújtva minden más szakmai érdeklődő részére. A jelentés elkészítése a jövőbeli lehetőségek függvényében évente megismétlődhet – immár a pénzügyi szektor egészére vonatkozóan – azonosítva az aktuális kiemelt fenyegetettségi trendeket, elemezve a trendek változását. Ahhoz, hogy a riport évről-évre konzisztens módon megismételhető legyen, pontosan meghatározott módszertani javaslatot dolgoztunk ki a fenyegetettségi térkép projekt keretében, mely egyértelműen definiálja az előkészületi tevékenységeket, az adatgyűjtési folyamat lebonyolítását, illetve a kiértékelés szempontrendszerét.

A fenyegetettségi térkép módszertan mellett meghatároztuk azt is, hogy az intézményeknek a különböző incidensekről milyen tájékoztatást, adatokat kell küldeniük az MNB-nek annak érdekében, hogy a kapott adatok alkalmasak legyenek a későbbi fenyegetettségi és incidenstrendek elemzésére és kimutatására. Az egységes riportálás és az adatok későbbi feldolgozhatósága érdekében a bejelentéseket előre meghatározott struktúrában kell az intézményeknek rögzítenük, mely folyamat támogatására elektronikus incidensbejelentési űrlap került kialakításra a projekt keretében. Az űrlap a Pilot projekt során biztosította az incidensek többszintű kategorizálását.

Természetesen a projekt keretében kialakított incidens-adatgyűjtési módszertant az EU-s szabályozásból (DORA rendelet) adódó riportálási kötelezettségek és szabályok felülírhatják, lecserélhetik.

Az incidensbejelentési módszertant és a fenyegetettségi térkép riport kidolgozásához készült módszertant a 2022. február és júliusa közötti hat hónapos pilot időszak keretében ellenőriztük le és próbáltuk ki.

Az első kérdés, amivel szembesültünk a módszertan kidolgozása során, magának az incidens fogalmának definiálása volt. A jelenlegi szabályozási környezet, illetve a különböző informatikai módszertanok és szabványok eltérő definíciókat alkalmaznak az incidens fogalmára, ezért a projekt során a lehető legtágabb értelmezést használtuk. Ennek megfelelően a működési incidensekről, üzemzavarokról is gyűjtöttünk adatokat, nem csak a kibertámadásokról. Várhatóan a DORA rendelet megjelenésével a definíciók pontosításra kerülnek majd, ugyanis a rendelet egyik nyíltan megfogalmazott célja az incidensbejelentési folyamatok egységesítése, ehhez pedig a jelenleg a PSD2 hatálya alá tartozó incidensbejelentéseket is módosítani szükséges. A projekt során az incidensbejelentéshez készített útmutató a következő definíciókat tartalmazta:

Informatikai biztonsági incidens: egy előre nem látható, de már azonosított esemény, amely a hálózatban, vagy az információs rendszerben következett be, függetlenül attól, hogy az rosszindulatú tevékenység eredménye vagy sem. Az incidens jellemzője, hogy kompromittálja a hálózat vagy az információs rendszer biztonságát, vagy az abban feldolgozott, tárolt vagy továbbított adatok biztonságára, vagy az érintett szereplő által nyújtott pénzügyi szolgáltatások rendelkezésre állására, bizalmasságára, folytonosságára, hitelességére kedvezőtlen hatással van.

Kritikus informatikai biztonsági incidens (továbbiakban „kritikus incidens”): olyan incidens, amely az intézmény kritikus funkcióit támogató hálózatát és információs rendszereit kedvezőtlenül és potenciálisan magas hatással érinti.

Az alábbi esetekben biztosan kritikusnak tekinthető az incidens:

- a sajtó érdeklődésének homlokterébe kerülő események esetén;
- több ügyfelet érintő banktitoknak, fizetési titoknak, biztosítási titoknak, értékpapírtitoknak, pénztártitoknak minősülő személyes adat illetéktelen személyhez kerülésekor;
- az informatikai rendszerben több ügyfelet érintő adatmódosítást eredményező jogosulatlan tevékenység esetén;
- az intézmény üzleti hatáselemzése (BIA) alapján kritikusnak tekintett szolgáltatásokra az előreláthatólag 1 órát meghaladó kiesésről vagy a normál szolgáltatási szinttől elmaradó szolgáltatások esetén, külön kiemelve az alábbi területeket:
  - elektronikus csatornák (online értékesítési csatornák, bankkártya, internetbank és elektronikus fizetések)
  - hitelintézetek, befektetési vállalkozások és alapok esetén számlavezetés

A fenti definíciónak megfelelően a sikertelen – tehát elhárított, rutinszerűen kezelt – támadásokról nem gyűjtöttünk adatokat a Pilotban résztvevő intézményektől. Megvizsgáltuk, de elvetettük annak lehetőségét, hogy fenyegetettségi (threat intelligence) adatokkal egészítsük ki az incidensadatokat, mivel a projekt során így is megfelelő mennyiségű adat állt rendelkezésünkre.

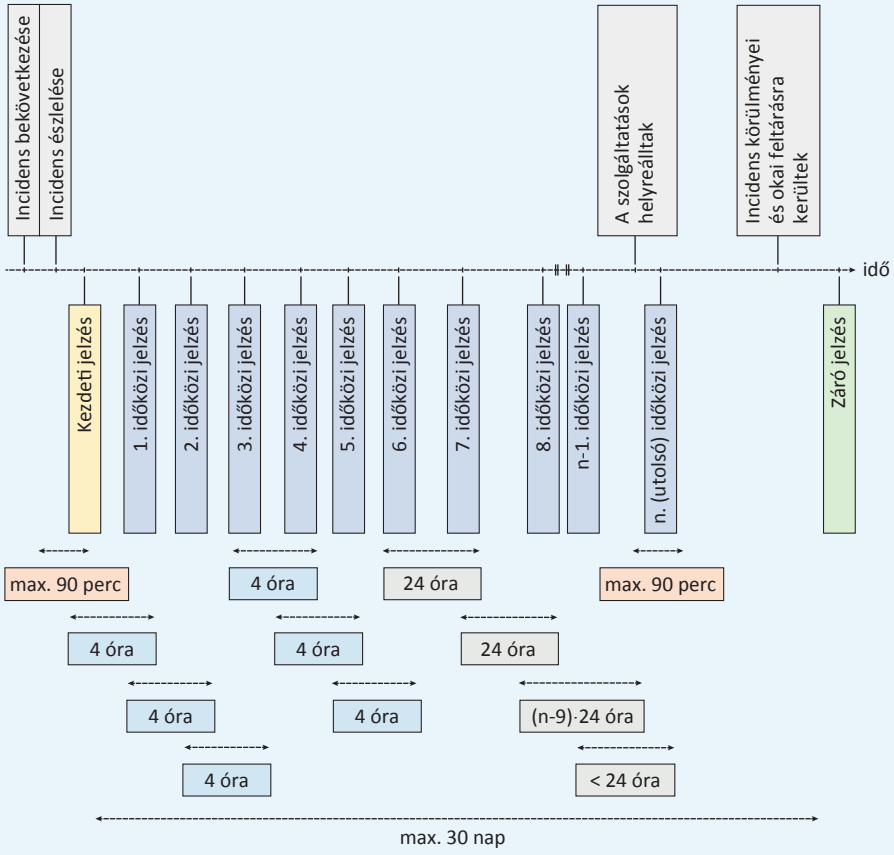
A Pilot projekt során a csatlakozó intézmények az adatgyűjtési periódus alatt kétféle incidens jelentési feladatot vállaltak magukra: havonta küldtek havi jelentéseket, amelyek minden, az adott hónaphoz tartozó incidens összefoglalására szolgáltak, másrészt a havi jelentéseken túl, a kritikus incidensek kapcsán azonnali jelzéseket is küldtek.

A havi jelentéseket a következő hónap 10-éig kellett beküldenie az intézményeknek abban az esetben is, ha az adott hónapban nem történt incidens. A kritikus incidensek esetén egy részletesebb, az alábbiakban ismertetett bejelentési és incidenselhárítást követő folyamatot kellett a bejelentést tevőknek végrehajtani. Néhány intézmény részéről felmerült a havi jelentések automatizálásának igénye és a Pilot projekt előrehaladtával láttunk is arra utaló jeleket, hogy a beérkező havi riportok egy részét automatikus eszközökkel állítják elő. Az incidensek bejelentésére meghatározott időkeretek a havi összefoglalók esetében minden intézmény számára megfelelőnek bizonyultak, az intézmények jelentős része napokkal a határidő előtt tudott érdemi (nem üres) havi összefoglalót küldeni.

A részletesebb jelentéseket jelzéseknek nevezte a Pilot projekt módszertana, mivel a projektben kapott adatokat elkülönítetten kezeltük a többi MNB-hez beérkező adatszolgáltatástól és ezt szerettük volna a használt kifejezések szintjén is hangsúlyozni. A kritikus incidensekhez háromszintű jelzési kötelezettség tartozott: a kezdeti jelzés, az időközi jelzés(ek) és a záró jelzés. A kezdeti és záró jelzésekből egy és csak egy darab készült minden incidens vonatkozásában. Az időközi jelzésekből nulla és 35 darab közötti mennyiségű készülhetett, attól függően, hogy az incidens kezelésének időtartama miként alakult.

A háromszintű jelzési kötelezettségek időbeli ütemezését mutatja a következő ábra:

38. ábra
A háromszintű jelzési kötelezettségek időbeli ütemezése



A kritikus incidenssel kapcsolatos jelzéseket az alábbi ütemezéssel kellett küldeni:

1. A kezdeti jelzést az incidens észlelési időpontjától számított 90 percen belül kellett elküldeni a Felügyeletnek. Kezdeti jelzésből minden kritikus incidens kapcsán csak egyetlen darab volt szükséges.

2. Időközi jelzést (vagy jelzéseket) akkor kellett küldenie az intézménynek, ha 4 órán belül nem tudott zárójelzést küldeni. Az időközi jelzés(eke)t (ha szükség van rá) addig kellett beküldenie az intézménynek, amíg az érintett szolgáltatások helyre nem álltak. Az alábbi ütemezéssel kellett időközi jelzéseket küldeni:

   a. Az első 24 órában 4 óránként,

   b. Az első 24 óra eltelte után naponta (24 óránként) kell küldeni,

   c. A kieső szolgáltatások helyreállása után legkésőbb 90 percen belül kell az utolsó időközi jelzést küldeni.

   d. Amennyiben nincs már kieső szolgáltatás és az utolsó időközi jelzés már beküldésre került, több időközi jelzést nem kell küldenie a felügyelt intézménynek.

3. A záró jelzést a kezdeti jelzéshez képest 30 napon belül kellett szolgáltatni a Felügyelet részére. Akkor készíthetett a felügyelt intézmény záró jelzést, amikor

   a. az érintett szolgáltatások maradéktalanul helyreálltak, azok teljeskörűen használhatók

   b. hiteles források (az incidenshez kapcsolódó naplók/feljegyzések) kiértékelésével felderítették az incidens körülményeit, az incidens megértéséhez szükséges információval már rendelkeztek,

   c. az incidens gyökérokát/gyökérokait már azonosították.

Záró jelzésből is csak egyet kellett küldeni minden kritikus incidenshez kapcsolódóan.

Nem volt feltétele a záró jelzésnek:

1. Az incidens miatt életbe léptetett üzletmenet-folytonossági (BCP) és/vagy katasztrófaelhárítási (DRP) folyamatok lezárása. Amennyiben még futottak aktív BCP és/vagy DRP folyamatok, arról a záró jelzésben tudott az intézmény nyilatkozni.

2. Az incidens elhárítás teljeskörűsége. Amennyiben még további intézkedések szükségesek a felügyelt intézmény oldalán, azokat a záró riportban tudták jelezni.

Az incidensek bejelentésére meghatározott időkeretek felülvizsgálatára szükség lehet a jövőben. A bankok esetében a 90 percen belüli kezdeti jelzés megvalósítható elvárás, mivel a pénzforgalomhoz köthető feladatok ellátása miatt 0-24-es üzemben dolgoznak. Azoknál az intézményeknél viszont, ahol éjjel és hétvégén nincs üzemidő, az ilyen időszakokban bekövetkező incidensek bejelentése még akkor is problémát okozhat, ha egyébként maga az incidens reagálás/elhárítás megoldott.

Időközi jelzéseket feltűnően kevés intézmény küldött, jellemzően a meghatározott időintervallumoknál ritkábban. Ugyanakkor a Pilot projekt során az MNB nem élt felügyeleti eszközökkel a késedelmes bejelentésekkel kapcsolatban, tehát várhatóan a határidők betartása nagyobb figyelmet kapna intézményi oldalon is, amennyiben a Pilothoz hasonló kötelező incidensbejelentési szabályozás valósul meg.

A pilot projektet követően, az adatgyűjtési szakasz utolsó fázisa az adattisztítás volt, amelyben az összes rendelkezésre álló incidensjelentés összegyűjtésre és egységes kritériumok alapján egységesítésre került, továbbá átvizsgálásra került az esetleges eltérések azonosítása érdekében. A kiberfenyegetettségi térkép projekt első iterációjában nagy hangsúlyt kellett például fektetni az egyes adatmezők válaszainak az ellenőrzésére a következők alapján:

- Megadott és elvárt válaszformátum összeegyeztetése (p. szám az elvárt, de szabadszöveges a válasz).

- A logikai összeférhetetlenségek azonosítása (pl. egy incidensnek az észlelés időpontja előtt vagy azzal egyidőben kellett bekövetkeznie) a kimutatások pontosságának elősegítése érdekében.

- Az azonos információs tartalommal rendelkező adatpontok egységesítése (pl. rövid és teljes cégnevek különbsége).

A Pilot hat hónapja alatt nem volt olyan hónap mikor az összes jelentés automatikus betöltése manuális adattisztítás nélkül lehetséges lett volna.

Az adatgyűjtési és adattisztítási fázist követően az elemzési tevékenység került elvégzésre. Az elemzés során a kritikus incidensek és havi összefoglalók adataiból előálltak az előzetesen meghatározott kritériumok mentén kialakított ábrák, összevetések. Az elemzési folyamat során egyrészt kvantitatív elemzések (mivel nagy számban álltak rendelkezésre incidensadatok), másrészt kvalitatívan elemzések (melyek mélyebben vizsgáltak egy-egy kiemeltnek ítélt témakört) készültek. A különböző adatpontokat típus és forrás szerint külön kellett kezelni és elemezni, illetve egymástól függetlenül kellett az összefüggéseket felépíteni.

1. A PILOT PROJEKT TANULSÁGAINAK ÖSSZEFOGLALÁSA

A Pilot projektben az adatszolgáltatások időbeli ütemezése és tartalma kapcsán felfedezhető volt egyfajta fejlődés. Az első hónapban (február) a jelzések rendszeréhez még nem minden esetben tartoztak kiforrott folyamatok az intézmények oldalán, ezért a jelzések nem minden esetben követték a felügyelet ütemezési elvárásait. A jelentések, jelzések tartalma kapcsán is több esetben szükség volt pontosításokra, a megküldött jelzések kiegészítésére. Ezzel együtt a bejelentett incidensadatok elemzése alapján az látszik, hogy a bejelentések többségét adó bankok esetében az említett fejlődési folyamat gyorsan lezáródott, a bejelentések során a banki szereplők lényegében fennakadások nélkül teljesíteni tudták a meghatározott incidensjelentési folyamatot.

Intézménytípustól függően ahogy a módszertan egyre jobban rutinná vált, a jelzések rendszere is egyre inkább igazodott az elvárásokhoz. A Pilot projekt résztvevők oldalán intézményi szinten tisztázódott, hogy milyen szereplők biztosítják a jelzések rendelkezésre állását, milyen tartalmat vár el az MNB és milyen határidőket szükséges szem előtt tartani. A Pilot projekt formanyomtatványai lehetőséget biztosítottak bizonyos felügyeleti kötelezettségek teljesítésének megkönnyítésére is, pl. a 398-5/2015 MNB iktatószámú körlevélben meghatározott adatszolgáltatási kötelezettségnek (a továbbiakban: IFF alert) is eleget tehettek az érintett intézmények. Az IFF alertekhez kapcsolódó e-mailek automatikus generálását is biztosította a formanyomtatvány, ugyanakkor ezzel a lehetőséggel egyetlen intézmény sem élt a Pilot során. Pozitív visszajelzést kaptunk azonban a résztvevő intézményektől és az informatikai felügyelőktől azzal kapcsolatban, hogy a formanyomtatvány megkönnyítette az incidensek megfelelő részletezettségű bejelentését és kevesebb visszakérdezést eredményezett a felügyelők részéről. A kötelező incidensjelentések kapcsán így tapasztalatot szerezhettek azok az intézmények is, melyek eddig nem vettek részt a riportálási folyamatokban.

Mivel a bankok jelentették be az incidensek jelentős részét, és a bejelentett incidensszámban a kezdeti időszakban nem volt elmaradás, így megállapítható, hogy a folyamatot a bankok szoros határidővel, jelentősebb fennakadás nélkül képesek voltak implementálni, vagyis egy hasonló jövőbeli folyamat feltehetőn szintén nem jelentene kiemelkedő nehézséget ebben a szegmensben. Ezzel együtt nem kimutatható pontosan, hogy a legkevesebb incidenst jelentő szereplők, a biztosítási alkuszok és pénzügyi vállalkozások esetében valóban nem volt incidens, nem került azonosításra az incidens, vagy a bejelentési folyamat nem volt kellően kidolgozva. Ennek a kérdésnek a megválaszolására a jövőbeli, nagyobb mintán elvégzett elemzések, célzott adatgyűjtések adhatnak majd választ.

A projekt előkészítési szakaszában létrehozott incidensbejelentő formanyomtatvány megfelelőnek bizonyult, az intézmények rövidebb-hosszabb idő után egyértelműen képesek voltak a kötött szabályok szerinti kitöltésére és megküldésére. A visszajelzések alapján több intézmény szívesen venné a jövőben, ha a kitöltést, vagy annak minél nagyobb részét házon belül automatizálni lehetne.

A bejelentő formanyomtatvány háttéradatbázisát jelentő kategóriák alábontása kritikus volt, mivel az incidensbejelentési folyamatban elvárt a gyors, hatékony működés, a bejelentési folyamatban fontos, hogy adott szakértők minél könnyebben be tudják kategorizálni az incidenseket. Az adatok elemzése alapján az „egyéb" kategóriába sorolt incidensek száma elenyésző, így a kategóriák kialakítása magas szinten megfelelőnek bizonyult, azonban az intézményi visszajelzések alapján finomhangolásra még szükség lehet.

A bejelentő formanyomtatvány Excel formában került kialakításra a mind zökkenőmentesebb használhatóság érdekében makrók használata nélkül, mely állomány elektronikus levél csatolmányaként keresztül került az MNB részére megküldésre. A projekt során megfontoltuk és elvetettük az MNB adatszolgáltatások lebonyolítására szolgáló ERA rendszer használatát, mivel sem a rendszer rendelkezésre állási és átfutási ideje, sem az intézményi oldalon hozzáférők köre (a jelzések tipikusan az IT biztonsági szakterületektől érkeztek, míg az ERA rendszerhez általában a jelentésszolgálat fér hozzá) nem kedvezett ennek a megközelítésnek.

A bejelentő formanyomtatvány alkalmazhatóságával kapcsolatban a Pilot tapasztalatai alapján, az adatbeviteli mezők kitöltése során alkalmazott ellenőrzésének továbbfejlesztése (intézmény azonosító, dátumválasztó stb.), illetve a javítóintézkedések és a kritikus jelzés mellékletei kitöltésének további támogatása, ösztönzése lehet szükséges a jövőben.

A módszertan alkalmazhatóságával kapcsolatban gyűjtött tapasztalatok megerősítik, hogy a kialakított incidensbejelentési folyamat módszertanilag alátámasztott, a gyakorlatban megfelelően alkalmazható, a kialakított formanyomtatvány segítette az intézményeket, hogy minden szükséges információt megadjanak, így redukálható volt a későbbi pontosító kérdések száma. Az „egyéb" kategóriában négy százalék alatti incidens került bejelentésre, ami arra enged következtetni, hogy az incidensek bejelentéséhez összeállított űrlapot az intézmények megfelelően tudták értelmezni és a gyakorlatban felhasználni, ezzel együtt pont ennek a nem besorolt incidenstípusnak a további elemzése, tipizálása adhat majd további lehetőséget a későbbiekben a kategóriák és alkategóriák finomhangolására. További finomhangolási lehetőségként a fraud jellegű incidensbejelentések átstrukturálása, az ügyfelek számosságára vonatkozó adatrögzítések pontosítása, illetve a kisebb intézmények esetén a bejelentési időkeret felülvizsgálata került azonosításra.

Érdekességként megemlíthető, hogy az NBSZ-NKI által gyűjtött Hardenize adatok, amik az adott intézmény külső domainjeinek a helyes konfigurációjáról szolgáltatnak adatokat, illetve az incidensbejelentés során beküldött adatok között korreláció nem volt kimutatható, vagyis nem volt azonosítható összefüggés aközött, hogy a intézmény külső, látható felületeinek konfigurációi milyen magas biztonsági szintet érnek el azzal összevetve, hogy adott intézmény mennyi és milyen jellegű incidenst jelentett be.

Tekintettel a DORA rendelet jövőbeli, incidensbejelentésekre vonatkozó elvárásaira, a visszajelzések alapján a Pilot projekt hasznos, gyakorlati tapasztalatokkal segítette hozzá a részt vevő intézményeket a jövőbeli elvárásokra való felkészülés terén, mind szervezeti, mind döntéshozói, mind szakértői szinten.

Teller Ede

(1908. január 15. – 2003. szeptember 9.)

Magyar-amerikai atomfizikus, nevéhez számos felfedezés és úttörő eljárás kidolgozása fűződik. Részt vett az első atombomba létrehozásában (1945), majd a hidrogénbomba fejlesztőcsapatának vezetője volt, ezért „a hidrogénbomba atyja”-ként vonult be a köztudatba.

A MAGYAR PÉNZÜGYI SZEKTOR KIBERFENYEGETETTSÉGI TÉRKÉPE 2022

2022. december

Nyomda: Prospektus Kft.

8200 Veszprém, Tartu u. 6.

mnb.hu

1013 BUDAPEST, KRISZTINA KÖRÚT 55.