NEMZETBIZTONSÁGI SZEMLE
11. évfolyam (2023) 1. szám 78–107. • DOI: 10.32561/nsz.2023.1.6

Legárd Ildikó[1]

Információbiztonsági incidenstrendek a közigazgatásban[2]

Information Security Incident Trends in Public Administration

A közigazgatás a kibertér felől érkező fenyegetések egyik leggyakoribb célpontja, az állami és önkormányzati szervek elleni kibertámadások egyre célzottabbak, kifinomultabbak és egyre nagyobb kár okozására képesek. Az elektronikus információs rendszerek biztonsága érdekében hatékony fizikai, logikai és adminisztratív intézkedéseket szükséges alkalmazni, amelyek meghatározásához elengedhetetlen az aktuális információbiztonsági incidenstrendek ismerete.

Jelen tanulmány célja a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet által, 2019 és 2021 közötti időszakban detektált információbiztonsági események átfogó elemzése, a közigazgatást érintő hazai incidenstrendek azonosítása érdekében. Az írás kiemelten vizsgálja, hogy a kibertámadók hogyan reagáltak a Covid–19-világjárványra, és ez milyen módon jelenik meg a hazai incidenstrendekben. Az elemzés további célkitűzése annak megállapítása, hogy mely szektort érte a legtöbb incidens a vizsgált időszakban, és mely incidenstípusok jellemzők ebben az ágazatban. További kutatási kérdésként merült fel, hogy a pszichológiai manipuláció milyen százalékos arányban mutatható ki a detektált incidenstrendekben.

Kulcsszavak: *információbiztonság, incidenstrendek, közigazgatás, Nemzeti Kibervédelmi Intézet, kibertámadások, Covid–19*

Public administration is one of the most common targets of cyber threats. Cyberattacks against public and local governments are becoming increasingly targeted, sophisticated, and are capable of causing ever greater damage. Information systems security requires effective physical, logical and administrative measures, which needs knowledge of current trends in information security incidents.

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Doktori Iskola, e-mail: ildiko.legard@gmail.com

[2] A tanulmány a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet támogatásával készült. Külön köszönöm dr. Munkácsi Viktor nb. alezredes úr, a Nemzeti CSIRT vezetőjének szakmai támogatását, tanácsait, amelyet az adatok elemzéséhez és a tanulmány megírásához nyújtott.

The aim of this study is to provide a comprehensive analysis of information security incidents detected by the National Cyber-Security Centre of Hungary between 2019 and 2021 in order to identify national incident trends affecting public administrations. The paper focuses on how cyber attackers have responded to the Covid–19 pandemic and how this is reflected in national incident trends. A further objective of the analysis is to identify which sector was affected the most by incidents during the period under review and which incident types are typical for this sector. A further research question was the percentage of social engineering in the detected incident trends.

Keywords: *information security, incident trends, public administrations, National Cyber-Security Centre of Hungary, cyber-attacks, Covid–19 pandemic*

Bevezetés

A *Nemzeti Digitalizációs Stratégia* (NDS) 2022–2030 kiemeli, hogy a „technológia fejlődésével az informatikai és kiberbiztonsági helyzet is egyre összetettebbé válik. Emiatt szükséges a biztonságtudatosság növelése, a megelőzés, az egyének, szervezetek és vállalkozások mélyrehatóbb biztonsági védelemének kialakítása”,[3] valamint „ágazati és központi szinten kiemelten szükséges az információbiztonsági elemek és a kibervédelmi kapacitások bővítése, összhangban a hazai és az EU-s szintű törekvésekkel”.[4] A stratégia a digitális állam pillér intézkedéscsoportjai keretében a megfogalmazott célok megvalósítása eszközeként a kormányzati elektronikus szolgáltatások információbiztonságának növelését jelöli meg. A kibertérben jelentkező és a kibertérből érkező fenyegetések és az ezzel járó kockázatok kezelése leghatékonyabban a megelőzésre épülő hatékony védelmi intézkedések útján valósítható meg, amihez elengedhetetlen az aktuális incidenstrendek ismerete.

A biztonsági események kezelése[5]

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.) Preambuluma kimondja, hogy: „A nemzet érdekében kiemelten fontos – napjaink információs társadalmát érő fenyegetések miatt – a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága.” Az elektronikus információs rendszer biztonsága érdekében a szervezetnek

[3] Miniszterelnöki Kabinetiroda 2022: 149.

[4] Miniszterelnöki Kabinetiroda 2022: 68.

[5] Az angolszász terminológia elkülöníti a biztonsági esemény és a biztonsági incidens fogalmát: az előbbi alatt minden megfigyelhető előfordulást ért egy hálózatban vagy egy rendszerben, az utóbbi, tehát az incidens fogalmába a számítógépes biztonsági szabályzatok, az elfogadható felhasználási irányelvek megsértésének vagy közvetlen fenyegetésének veszélye tartozik. A magyar jogszabályok azonban nem határolják el e két fogalmat, kizárólag a biztonsági esemény fogalmát alkalmazzák, amely terminológia alatt valójában a biztonsági incidenseket értik. Krasznay et al. 2019: 136.

külön jogszabályban előírt logikai, fizikai és adminisztratív védelmi intézkedéseket kell meghatároznia, amelyek támogatják:

a) a megelőzést és a korai figyelmeztetést,
b) az észlelést,
c) a reagálást,
d) a biztonsági események kezelését.[6]

Az Ibtv. értelmező rendelkezése – 1. § (1) – értelmében:

- biztonsági esemény: nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül;
- súlyos biztonsági esemény: olyan informatikai esemény, amely bekövetkezése esetén az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be, súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek;
- biztonsági esemény kezelése: az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység.

A biztonsági események kezelését – az eltérő ellátotti körre tekintettel – az alábbi szervezetek látják el:

- NBSZ NKI, amely kezeli:
  - az Ibtv. 2. §-ában – az Ibtv. 19. § (2) bekezdése szerinti kivétellel – meghatározott szervek nyílt,
  - a bejelentésköteles szolgáltatók,
  - a honvédelmi létfontosságú rendszerelemek kivételével az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt létfontosságú rendszerelemeket működtetők,
  - a központosított informatikai és elektronikus hírközlési szolgáltató

  elektronikus információs rendszereit érintő biztonsági eseményeket és fenyegetéseket.
- Katonai Nemzetbiztonsági Szolgálat: az Ibtv. 19. § (2) bekezdése alapján a honvédelmi célú elektronikus információs rendszereket érintő biztonsági eseményeket és fenyegetéseket kezeli.

[6] Ibtv. 6. §.

Az NBSZ NKI-n, illetve a KNBSZ-en kívül speciális eseménykezelési feladatokat lát el a Kormányzati Informatikai Fejlesztési Ügynökség (KIFÜ),[7] amely az ügyfélkörébe tartozó közoktatási, felsőoktatási, közgyűjteményi intézmények és kutatóhelyek részére nyújtott informatikai infrastruktúra fejlesztéséhez és üzemeltetéshez kapcsolódóan kezeli az érintett intézmények biztonsági eseményeit is. A HUNCERT a magyar internetszolgáltatókat segíti a számítógépes hálózati incidensek kockázatainak kezelésében, valamint az ilyen incidensek esetén az incidensek felderítésében, kezelésében és elemzésében.[8]

Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet

A Nemzetbiztonsági Szakszolgálat szervezetén belül 2015. október 1-jével hozták létre a Nemzeti Kibervédelmi Intézetet, amelynek tevékenysége három pillérre épül:

- hatósági feladatok ellátása: a Nemzeti Elektronikus Információbiztonsági Hatóság az Ibtv.-ben, valamint a 187/2015 (VII. 13.) Korm. rendeletben meghatározott feladat- és hatáskörben a jogszabályi előírások ellenőrzésével és érvényesítésével foglalkozik;
- incidenskezelési tevékenység: az eseménykezelő központ a kibertérből érkező támadásokkal és fenyegetettségekkel kapcsolatos eseménykezelési feladatokat látja el;
- sérülékenységvizsgálat: az informatikai rendszerek gyenge pontjainak feltárására, a rendszer védelmi képességeinek tesztelésére irányul.

Biztonsági események kezelése során az NBSZ NKI:

- az Ibtv. 2. §-ában meghatározott szervek – a honvédelmi célú elektronikus információs rendszerek kivételével – nyílt,
- az alapvető szolgáltatást nyújtó szolgáltatók és a bejelentésköteles szolgáltatók,
- a honvédelmi létfontosságú rendszerelemek kivételével az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt létfontosságú rendszerelemeket működtetők,
- a központosított informatikai és elektronikus hírközlési szolgáltató, valamint
- a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat

elektronikus információs rendszereit érintő biztonsági eseményeket és fenyegetéseket kezeli.[9]

Az incidensek kezelésének alapszabályait az Ibtv. felhatalmazása alapján az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól szóló 271/2018. (XII. 20.) Korm. rendelet fekteti le, amely rendelkezik az intézmények és az eseménykezelő központ jogairól és kötelességeiről, valamint egyéb lehetőségekről is.

---

7 Lásd: https://kifu.gov.hu/
8 Lásd: www.cert.hu/
9 Ibtv. 19–20. §, 271/2018. (XII. 20.) Korm. rendelet 3. § (1).

Az NKI által kezelt incidensek statisztikai adatai

Az NBSZ NKI által detektált és gyűjtött, incidensekre vonatkozó statisztikai mutatókat az alábbi kategorizálás szerint tagolva bocsátotta kutatási célból a rendelkezésemre 2022. februárban:

- évenkénti bontás (havi bontásban is),
- szektorális bontás,
- incidensek típusai szerinti bontás.

- Évenkénti bontás: 2019, 2020, 2021 évenként, hónaponkénti bontásban.
- Szektorális bontás
  - állami és önkormányzati szervek: Az Ibtv. 2. §-ában meghatározott szervek;
  - nemzeti létfontosságú rendszerelemek: 2012. évi CLXVI. törvény (Lrtv.)[10] alapján kijelölt létfontosságú rendszerelem, amelynek kiesése a létfontosságú társadalmi feladatok folyamatos ellátásának hiánya miatt elsősorban Magyarországon lenne jelentős hatással (energia, közlekedés, agrárgazdaság, egészségügy, TB, pénzügy, infokommunikációs technológia, víz, honvédelem, közbiztonság-védelem);
  - alapvető szolgáltatásokat nyújtó szereplők:[11] Lrtv. alapján alapvető szolgáltatásokat nyújtó szereplőnek azon szervezet vagy gazdasági szereplő intézmény jelölhető ki, amely:
    - alapvető szolgáltatást nyújt (kritikus társadalmi vagy gazdasági tevékenységek fenntartásához szükséges, elektronikus információs rendszertől függő, az alapvető szolgáltatások jegyzékében feltüntetett szolgáltatás),
    - az általa nyújtott alapvető szolgáltatás elektronikus információs rendszerektől függ,
    - az általa nyújtott alapvető szolgáltatást érintő biztonsági esemény – kormányrendeletben meghatározott – jelentős zavart okozna szolgáltatás nyújtásában és
    - az erre irányuló eljárásban alapvető szolgáltatást nyújtó szereplőként került azonosításra.
  - bejelentésköteles szolgáltatók: 2001. évi CVIII. törvény (Ekertv.) alapján bejelentésköteles szolgáltatást nyújtónak minősül a magyarországi székhelyű gazdasági társaság, amely a következő információs társadalommal összefüggő szolgáltatások valamelyikét nyújtja:
    - aki online piacteret működtet, vagy egy elérhető online piactér igénybevételével online adásvételi és szolgáltatási szerződések megkötését teszi lehetővé fogyasztók és kereskedők/ kereskedő és kereskedő között,
    - keresőszolgáltatást,
    - felhőalapú számítástechnikai szolgáltatást nyújt.[12]

[10] 2012. évi CLXVI. törvény (Lrtv.) 1. § *k)*.
[11] 2012. évi CLXVI. törvény (Lrtv.) 1. § *d)*.
[12] 2001. évi CVIII. törvény (Ekertv.) 2. § *j)*.

  - közvetítő szolgáltatók: Az Ekertv. alapján az információs társadalommal összefüggő szolgáltatást nyújtó szolgáltató, amely
    - az igénybe vevő által biztosított információt távközlő hálózaton továbbítja, vagy a távközlő hálózathoz hozzáférést biztosít (egyszerű adatátvitel és hozzáférés-biztosítás);
    - az igénybe vevő által biztosított információt távközlő hálózaton továbbítja, és az alapvetően a más igénybe vevők kezdeményezésére történő információtovábbítás hatékonyabbá tételét szolgálja (gyorsítótárolás);
    - az igénybe vevő által biztosított információt tárolja (tárhelyszolgáltatás);
    - információk megtalálását elősegítő segédeszközöket biztosít az igénybe vevő számára (keresőszolgáltatás);
    - alkalmazásszolgáltató;
    - videómegosztóplatform-szolgáltató.[13]
  - nemzetbiztonsági védelem alá eső szervezetek: A nemzetbiztonsági védelem alá eső szervek és létesítmények köréről szóló 2009/2015. (XII. 29.) Korm. határozat 1. mellékletében felsorolt szervek (például NAIH, AB, ÁSZ, KEH, OBH);
  - oktatási intézmények;
  - egyéb szervezetek:
    - a honvédelmi létfontosságú rendszerelemek kivételével az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt létfontosságú rendszerelemeket működtetők[14],
    - a központosított informatikai és elektronikus hírközlési szolgáltató[15],
    - a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat[16],
    - egyéb bejelentések alapján.
- Incidensek típusai szerinti bontás
  Az NBSZ NKI az incidenstípusok meghatározásánál az Európai Unió Hálózat- és Információbiztonsági Ügynöksége (ENISA) által kidolgozott rendszer módosított változatát használja, ugyanis a magyar gyakorlat nem sorol be minden incidenst biztonsági eseménynek, amelyet az ENISA annak tekint.[17] Az eseménykezelő központ által a 2019–2021. években detektált eseményeket az alábbi incidenstípusok szerint határozták meg:
  - adminisztrátorfiók kompromittálódása *(privileged account compromise);*
  - behatolás *(intrusions):* ez jelentheti egy rendszer vagy alkalmazás (szolgáltatás) sikeres kompromittálását is, amely történhet távolról egy ismert vagy új sebezhetőség révén, de akár jogosulatlan helyi hozzáférés is okozhatja. Ide tartozik a botnet is;[18]
  - behatolási kísérlet *(intrusion attempts):* egy rendszer veszélyeztetésére vagy bármely szolgáltatás megzavarására irányuló kísérlet, például ismert vagy

13 Ekertv. 2. § (l).
14 271/2018. (XII. 20.) Korm. Rendelet 3. § (1).
15 271/2018. (XII. 20.) Korm. Rendelet 3. § (1).
16 Ibtv. 20. § (3).
17 Marsi 2018: 58.
18 ENISA 2018.

ismeretlen sérülékenység kihasználása révén, vagy többszöri bejelentkezési kísérlettel (jelszavak kitalálása/feltörése, *brute force*);[19]
- bejelentkezési kísérlet *(login attempts):* többszöri bejelentkezési kísérlet például jelszavak kitalálása/feltörése, brute force segítségével;[20]
- C&C szerver: a parancs- és vezérlőkiszolgáló (C&C) egy támadó vagy kiberbűnöző által vezérelt számítógép, amelyet arra használnak, hogy parancsokat küldjenek a rosszindulatú programok által feltört rendszereknek, és fogadjanak ellopott adatokat a célhálózatról. Számos kampányban felhőalapú szolgáltatásokat, például webmail- és fájlmegosztó szolgáltatásokat használnak C&C-kiszolgálóként, hogy elvegyüljenek a normál forgalomban és elkerüljék a felderítést;[21]
- DDoS: Distributed Denial of Service – elosztott szolgáltatásmegtagadással járó támadás, olyan logikai támadás, amely az informatikai rendszer egy (vagy több) kiszolgálóját tömeges szolgáltatásigénnyel túlterheli, ami a felhasználók hozzáférését nehezíti, vagy akár a kiszolgáló teljes leállásához is vezethet;[22]
- defacement research: weboldal rongálása;
- DoS: Denial of Service – szolgáltatásmegtagadással járó támadás;[23]
- elemzés;
- elérhetőség *(availability):* az elektronikus információs rendszer vagy annak elemének tulajdonsága, amely arra vonatkozik, hogy az (ideértve az abban vagy az által kezelt adatot is) a szükséges időben és időtartamban használható;[24]
- erőforrások illetéktelen használata *(unauthorized use of resources):* az erőforrások jogosulatlan célokra való felhasználása, beleértve a nyereségszerzést is (például az e-mail használata illegális profitszerző láncelevelekben való részvételre vagy piramisjátékokban);[25]
- féreg *(worm):* olyan program, amely a számítógép-hálózaton keresztül, a hálózati funkciók kihasználásával terjed számítógéptől számítógépig, és károkozó hatását önmaga – a számítógép összeomlásáig tartó – reprodukálásával, továbbításával éri el;[26]
- illicit/sértő tartalom *(abusive content):* például spam, harmful speech, azaz valakinek a lejáratása vagy diszkriminációja (például internetes zaklatás, rasszizmus, fenyegetések egy vagy több személy ellen), illetve ide tartozik a gyermekpornográfia és az erőszak magasztalásával kapcsolatos tartalmak is;[27]

19 ENISA 2018.
20 ENISA 2018.
21 Lásd: www.trendmicro.com/vinfo/us/security/definition/command-and-control-server
22 Muha–Krasznay 2014: 115.
23 Berzsenyi et al. 2018: 392.
24 Ibtv. 1.§ (1) 38. pont
25 ENISA 2018.
26 Muha–Krasznay 2014: 116.
27 ENISA 2018.

- információbiztonság (Information Security): Az adatokkal és rendszerekkel való helyi visszaélés mellett az információbiztonságot veszélyeztetheti egy fiók vagy alkalmazás sikeres kompromittálása, valamint olyan támadások, amelyek révén információkat hallgatnak le és férnek hozzá átvitel közben (lehallgatás, hamisítás vagy eltérítés). Ugyanakkor az emberi/konfigurációs/szoftverhiba is veszélyeztetheti az információbiztonságot;[28]
- információgyűjtés *(information gathering):* például szkennelés *(scanning)* útján, amelynek során mintegy a tesztelési folyamat részeként olyan kéréseket küldenek egy rendszerhez a gyenge pontok felderítése érdekében, amely információt gyűjt a hosztokról, szolgáltatásokról és fiókokról (például DNS-lekérdezés, portellenőrzés). Információ gyűjthető lehallgatás *(sniffing)* útján is, amely a hálózati forgalom megfigyelése és rögzítése. A social engineering technikák is alkalmasak információgyűjtésre;[29]
- információk illetéktelen hozzáférése *(unauthorised access to information);*
- információk illetéktelen módosítása *(unauthorised modification of information);*
- ismeretlen típusú káros kód: ismeretlen rosszindulatú számítógépes program (például vírus, féreg, logikai bomba, kémprogram stb.);
- ismert sérülékenység kihasználása *(exploiting known vulnerabilities):* a sérülékenység az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat;[30]
- IT-biztonsági szaktanácsadás *(IT security consulting)* vagy szaktanácsadás;
- káros tevékenység: káros kód, fertőzött rendszer, C&C server, káros kód konfiguráció.
- letapogatás *(scanning):* szkennelés során mintegy a tesztelési folyamat részeként olyan kéréseket küldenek egy rendszerhez a gyenge pontok felderítése érdekében, amely információt gyűjt a hosztokról, szolgáltatásokról és fiókokról (például DNS-lekérdezés, portellenőrzés);[31]
- logelemzés: például a vállalati informatikai rendszerek, tűzfalak, behatolásgátló és vírusirtó rendszerek naplóbejegyzéseinek, elemzése;
- megszemélyesítés *(masquerade):* a social engineering egy esete, amikor egy entitás (személy, program, folyamat stb.) magát más entitásnak tünteti fel;[32]
- nem adminisztrátor fiók kompromittálódása *(unprivileged account compromise);*
- nyitott port *(open port):* „nyitott kapuk", amelyeken elérhetők a hálózat szolgáltatásai, így például a vírusok ezen a porton keresztül is bejuthatnak a szerveztek informatikai rendszereibe és gépeibe, ezáltal megbénítva a működést;
- pszichológiai manipuláció *(social engineering):* a social engineering az emberi hiszékenységre, együttműködésre építő támadási forma. Bár ezt az élet sok

28 ENISA 2018.
29 ENISA 2018.
30 Muha–Krasznay 2014: 121.
31 ENISA 2018.
32 Muha–Krasznay 2014: 119.

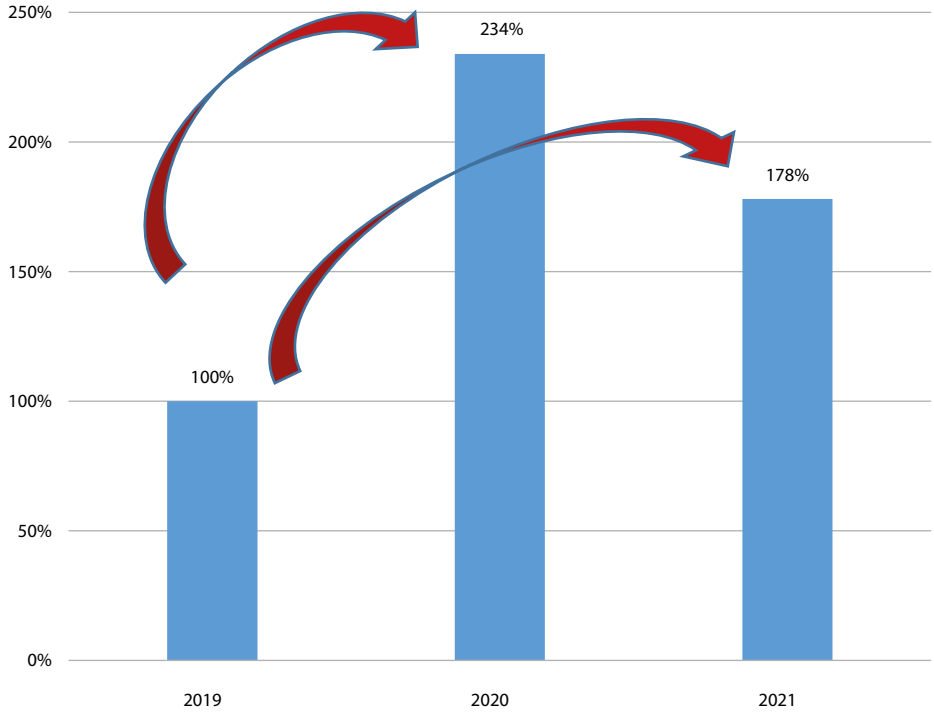
más területén is kihasználják, a social engineering kimondottan az információ megszerzésére irányul, ezen belül is elsősorban az informatikai eszközökön tárolt adatokra fókuszálva;[33]
- *ransomware:* zsarolóvírus;
- *spam:* levélszemét minden olyan kéretlen üzenet, amelyet tömegesen küldenek (kéretlen tömeges e-mail vagy UBE);[34]
- SPAM IP: egy botnetfertőződésből fakadóan, spamelés miatt a használt IP-cím feketelistákra kerülhet, és bizonyos levelezőszerverek nem fogják befogadni az innen érkező, küldött leveleket;[35]
- trójai *(trojan):* olyan kártékony program, amelyet alkalmazás, játék, szolgáltatás vagy más egyéb tevékenység mögé rejtenek, álcáznak. Futtatásakor fejti ki károkozó hatását;[36]
- visszaélés *(fraud):* például erőforrások illetéktelen használata, megszemélyesítés, adathalászat, vagy licenc nélküli kereskedelmi szoftverek vagy egyéb szerzői jogi védelem alatt álló másolatok felajánlása vagy telepítése;[37]
- zaklatás *(harassment):* bántó, valótlan üzenetek küldözgetése online;[38]
- egyéb.

Az NKI által detektált incidensek összehasonlítása évenként és incidenstípusokként

Az NKI az incidensekre vonatkozó átadott adatokat számszerűen – hónaponként, szektoronként és incidenstípusonként – bocsátotta a rendelkezésemre. Tekintettel arra, hogy az Ibtv. 22. § (4) bekezdése szerint az NBSZ NKI eljárásai során keletkezett adatok nem nyilvánosak, továbbá a konkrét számadatok tükrében olyan – a kapacitásaikra és képességeikre vonatkozó – következtetések is levonhatók, amelyek megnehezíthetnék a szolgáltatások ellátását, a konkrét számadatok nem publikálhatók. Az adatok feldolgozása során kizárólag a számadatokból levont következtetéseket, a számadatokban való változás százalékos mértékét vagy egymáshoz viszonyított arányát lehet bemutatni. A tanulmány az adatok elemzése során a fenti követelmények figyelembevételével mutatja be a hazai incidenstrendeket.

Az NKI által kezelt incidensek százalékos eloszlását évenkénti összehasonlításban az 1. ábra mutatja be:

[33] Muha–Krasznay 2014: 53.
[34] Lásd: www.eset.com/hu/levelszemet/
[35] Lásd: https://nki.gov.hu/it-biztonsag/tudastar/keretlen-level-feketelista-spam-blacklist/
[36] Muha–Krasznay 2014: 122.
[37] ENISA 2018.
[38] Monori 2016: 247.



1. ábra: Kezelt incidensek százalékos eloszlása évenkénti összehasonlításban
Forrás: a szerző szerkesztése

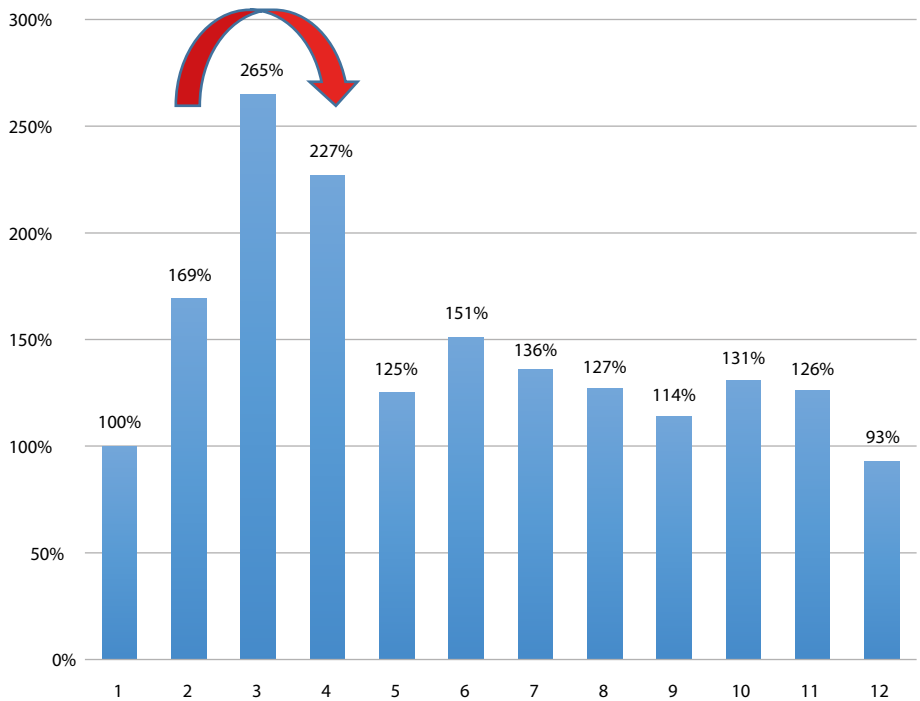
A grafikon segítségével egyértelműen kimutatható, hogy amennyiben a 2019-es évben, az összes kezelt incidens számát tekintjük 100%-nak, akkor a 2020-ban kezelt összes incidensek száma közel két és félszeres emelkedést mutat, és bár arányait tekintve csökkenés tapasztalható a 2021-es évben, ugyanakkor 2019-hez viszonyítva a kezelt incidensek aránya még mindig meredeken emelkedett. A tapasztalható emelkedés lehetséges okai a következők lehetnek:

- Early Warning System (EWS): 2020. május 30-án hatályba lépett az elektronikus információbiztonsági korai figyelmeztető rendszerről szóló 214/2020. (V. 18.) kormányrendelet, amelynek értelmében a korai figyelmeztető szolgáltatás nyújtására a NBSZ NKI-t jelölték ki. Az EWS egy szignatúra alapú illetéktelen hálózati behatolást jelző rendszer (*network based intrusion detection system,* nIDS), amely kifejezetten nyílt internetről elérhető rendszerek (például web-oldalak) elleni támadásokat képes felismerni és jelezni;
- koronavírushoz kapcsolódó világjárvány és az ezzel összefüggésbe hozható megtévesztő levelek, álhírek, közösségimédia-üzenetek, valamint az új koronavírussal kapcsolatos, Covid–19 témájú káros tartalmú mobilalkalmazások és weboldalak;
- távmunka, otthoni munkavégzés kockázatai.

A Deloitte által készített, a Covid–19-járvány hatásait vizsgáló tanulmány szerint a felhasználók 47%-át érte adathalász támadás otthoni munkavégzés során. 2020. február és május között a videókonferencia-szolgáltatásokat igénybe vevő, több mint félmillió felhasználó adatait szerezték meg a támadók, és adták el a dark weben. Azon kibertámadások száma, amelyek korábban még nem ismert rosszindulatú programokat vagy módszereket alkalmaztak a korábbi 20%-ról a pandémia alatt 35%-ra emelkedtek.[39] Az Interpol a Covid–19-hez kapcsolódó kiberfenyegetések kapcsán az adathalászatra, a különböző csalásokra, a rosszindulatú domainnevek, a malware-ek, a ransomware-ek valamint az álhírek gyorsan emelkedő terjedésére figyelmeztetett.[40]

2020. év vizsgálata

Ahhoz, hogy hazai viszonylatban is megvizsgáljam a világjárvány hatásait, elemezni szükséges a 2020. év emelkedő tendenciát mutató hónapjaiban azonosított incidenstípusokat. A 2020-ban kezelt incidensek havi eloszlását a 2. ábra részletezi.

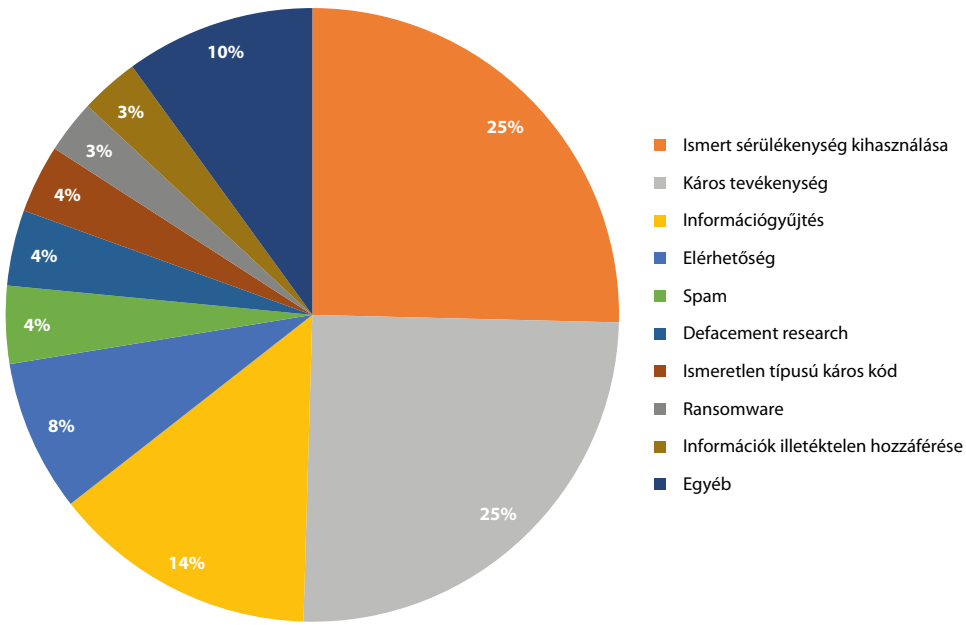


2. ábra: A 2020-ban kezelt incidensek havi eloszlása
Forrás: a szerző szerkesztése

[39] Nabe (é. n.).
[40] Interpol (é. n.).

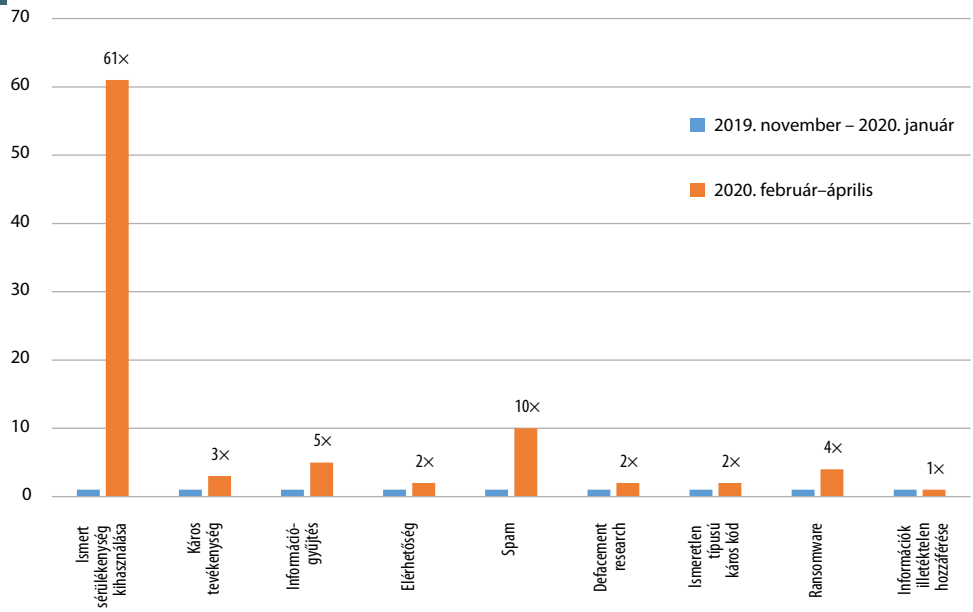
A havi eloszlásokból egyértelműen megállapítható, hogy az incidensek száma a Covid–19 első hullámában indult meredek emelkedésnek. A márciusban kezelt incidensek – a 2020-ban kezelt incidensek összesített számához viszonyított – százalékos aránya több mint két és félszeres emelkedést mutat a januári eredménnyel összehasonlítva.

A 2020. február–április közötti időszakban az NKI által kezelt incidensek típusait a következő, 3. ábra szemlélteti.



3. ábra: az NKI által kezelt incidenstípusok 2020. február–április
Forrás: a szerző szerkesztése

Az incidensek képzeletbeli dobogóján az első három helyen az alábbi incidensek szerepelnek: első helyen megosztottan az ismert sérülékenység kihasználása (25%) és a káros tevékenység (25%), második helyen az információgyűjtés (14%), a harmadik helyen pedig az elérhetőség (8%) szerepel. Amennyiben összehasonlítjuk a 2020. február és április közti, valamint az azt megelőző három hónapot (2019. november és 2020. február között), az egyes incidenstípusok esetén a 4. ábrán leolvasható emelkedést tapasztalhatjuk.



4. ábra: 2020. február–április és 2019. november – 2020. január összehasonlító vizsgálata
Forrás: a szerző szerkesztése

A grafikon alapján megállapítható, hogy az ismert sérülékenység kihasználása mutatja a legnagyobb emelkedést (61-szeres), de a spamek (10x), az információgyűjtés (5x), a ransomware (4x), valamint a káros tevékenység is (3x) többszörös növekedést mutat. Az ismert sérülékenység kihasználása tekintetében, amennyiben megvizsgáljuk a jelzett időszakban az NKI által kiadott riasztásokat, tájékoztatásokat, híreket, megállapíthatjuk, hogy az emelkedés hátterében több olyan konkrét fenyegetés is azonosítható, amelyek egyenként is okozhatták a kiemelkedő statisztikai eredményt. Ilyen fenyegetések többek között: Microsoft Windows 0. napi sérülékenysége,[41] az Exchange mail szerverek ellen detektált támadások,[42] a HP Support Assistant segédprogramjának kritikus sérülékenysége, az Adobe és Oracle szoftverek,[43] valamint a VMware vCenter Server[44] sérülékenységei.

A megnövekedett káros tevékenység és az információgyűjtéshez kapcsolódó incidensek hátterében a koronavírushoz, valamint az otthoni munkavégzéshez kapcsolódó fenyegetések állnak. A NKI 2020. márciusban tájékoztatást[45] adott ki az új koronavírus témájú kiberfenyegetésekről, amelyeket az 5. ábra mutat be.

41 Lásd: https://nki.gov.hu/figyelmeztetesek/riasztas/microsoft-windows-0-napi-serulekenysegek/
42 Lásd: https://nki.gov.hu/it-biztonsag/hirek/exchange-szerverek-veszelyben/
43 Lásd: https://nki.gov.hu/figyelmeztetesek/tajekoztatas/tajekoztatas-adobe-szoftverek-serulekenysegeirol-4/ https://nki.gov.hu/figyelmeztetesek/tajekoztatas/tajekoztato-oracle-szoftverek-serulekenysegeirol/
44 Lásd: https://nki.gov.hu/figyelmeztetesek/tajekoztatas/tajekoztatas-vmware-vcenter-server-serulekenysegerol/
45 Lásd: https://nki.gov.hu/figyelmeztetesek/tajekoztatas/az-nki-tajekoztatoja-az-uj-koronavirus-temaju-kiberfenyegetesekrol/

5. ábra: Koronavírus témájú kiberfenyegetések
Forrás: a szerző szerkesztése

A vizsgált időszak további kiemelt fenyegetései közé tartozik az Emotet vírus, amelyet az Europol a világ legveszélyesebb rosszindulatú programjaként tart számon.[46] A 2014-ben felfedezett Emotet egy fejlett, moduláris banki trójai, amely a kormányzati és magánszektort egyaránt célozza. Alapképességeit tekintve elsősorban banki adatok lopására szakosodott, ugyanakkor az évek során megjelenő újabb változatai szinte bármilyen más káros tevékenységre alkalmasak (például személyes adatok ellopása vagy zsarolóvírus telepítése), nem véletlen tartják az egyik legköltségesebb és legpusztítóbb vírusnak.[47] Jellemző a kártevőre, hogy aktívan kihasználja az aktuális tendenciákat, híreket, így a vizsgált időszakban jellemzően a Covid–19 témájához kapcsolódva terjedt a gyanútlan áldozatok között.

46 Europol 2021.
47 Lásd: https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-egeszsegugyi-intezmenyeket-erinto-emotet-terjesztesi-kampannyal-kapcsolatban/

Elsősorban az otthoni munkavégzéshez kapcsoló fenyegetésként jelentek meg a zsarolólevelek és a zsarolóvírusok. A Phobos ransomware például nyitott vagy nem biztonságos távoli asztali kapcsolaton keresztül, RDP hitelesítő adatok brute force támadásával, kiszivárgott vagy megszerzett RDP hitelesítő adatok segítségével, valamint klasszikus és jól bevált adathalász technika segítségével terjedt.[48]

Az ENISA minden évben kiadja a kiberbiztonsági fenyegetettség helyzetéről szóló éves jelentését. Az ENISA Threat Landscape 2020, a 2019. január és 2020. április közötti időszakra vonatkozóan határozza meg a legfőbb fenyegetéseket[49], amelynek részeként külön foglalkozik a 2020-ban kezdődő pandémiás időszakkal.

Az összesített jelentés a 2018-as fenyegetettségi helyzethez képest a legnagyobb változásként a digitális környezet Covid–19 által vezetett átalakulását említi. A világjárvány során a kiberbűnözők képességeiket továbbfejlesztették, gyorsan alkalmazkodtak és hatékonyabban célozták meg a releváns áldozati csoportokat.

Az ENISA a Covid–19 során detektált fenyegetettségi térképe alapján, a hazai detektált incidensekkel egybehangzó módon megállapítható, hogy az Európai Unióban is megnőtt a távmunkához kapcsolódó infrastruktúrákhoz köthető támadások, a csaló, koronavírussal kapcsolatos domainek, az sms-es és az e-mailes adathalászat, a hamis tesztelési alkalmazások, valamint a támadások száma az egészségügyi szervezetek ellen. A támadások eredményeként szignifikánsan emelkedett a személyes adatok, információk és jelszavak eltulajdonítása, a pénzügyi csalások, a zsarolóvírusokhoz kapcsolódó váltságdíjfizetések és egyéb, a szervezetek működését befolyásoló zavaró tényezők száma.[50]

A 2020. évet tovább vizsgálva a következő kiugrást a júniusi hónapban láthatjuk, amelynek hátterében a Covid–19-hez kapcsolódó, újra erőre kapó, több esetben rosszindulatú csatolmányokat tartalmazó adathalász-kísérletek, koronavírusra hivatkozó csaló honlapok, valamint a mobiltelefonokat veszélyeztető zsarolóvírusok állnak. Ebben az időszakban az NKI riasztást adott ki,[51] az ORFK[52] pedig arra figyelmeztetett, hogy az országos tisztifőorvos, valamint a Nemzeti Népegészségügyi Központ nevében elektronikus leveleket küldtek elsősorban egészségügyi, állami intézményekbe és cégekhez, amelyek csatolmánya feltehetően rosszindulatú programot tartalmaz. A csaló levél példáját a 6. ábra szemlélteti.

48 Lásd: https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-phobos-zsarolovirus-terjedeserol/

49 ENISA Threat Landscape 2020, lásd: www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape/enisa-threat-landscape-2020

50 Lásd: www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/threat-landscape-mapping-infographic-2020

51 Lásd: https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-a-nemzeti-nepegeszsegugyi-kozpont-neveben-kuldott-karos-csatolmanyt-tartalmazo-levellel-kapcsolatban/; https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-nemzeti-nepegeszsegugyi-kozpont-arculati-elemeit-felhasznalo-adathalasz-levelekkel-kapcsolatban/

52 Lásd: https://koronavirus.gov.hu/cikkek/operativ-torzs-visszaeltek-az-orszagos-tisztifoorvos-es-az-nnk-nevevel

P 2020. 06. 12. 9:12

Nemzeti Egészségügyi Központ Magyarország <Muller.Cecilia@nnk.gov.hu>

Message has been disinfected :A Covid-19 védőfelszerelés ingyenes forgalmazása (Nemzeti Egészségügyi Központ Magyarország)

Címzett undisclosed-recipients:

NEMZETI NÉPEGÉSZSÉGÜGYI KÖZPONT

Állami Népegészségügyi és Tisztiorvosi Szolgálat

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

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

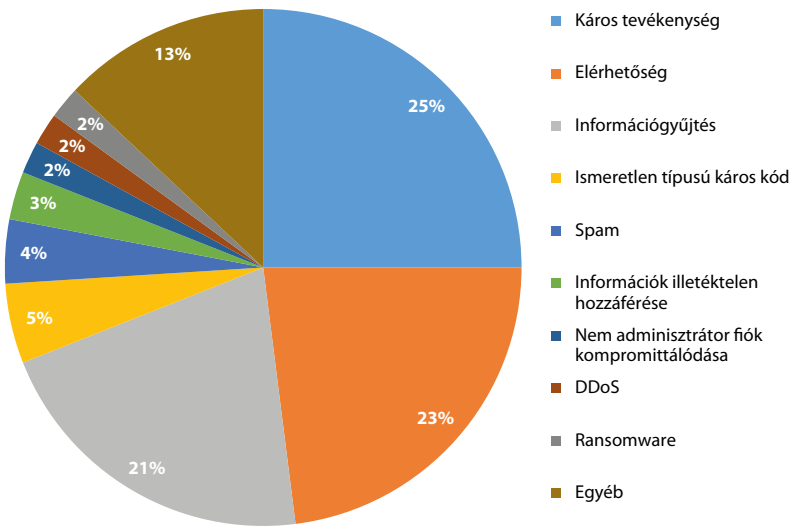
Az összes kitöltött nyomtatványt erre az e-mailre kell küldeni: Müller.Cecília@nnk.gov.hu

Szia

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

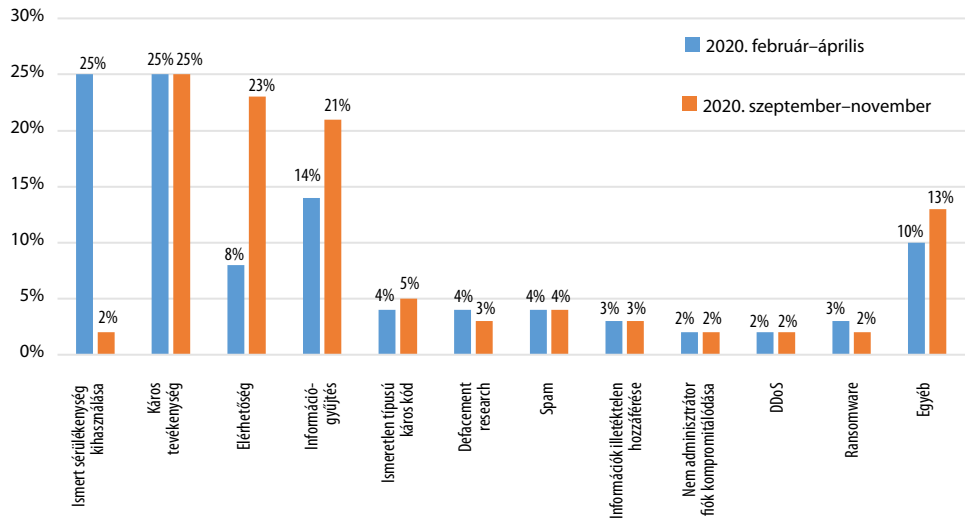
6. ábra: Riasztás a Nemzeti Népegészségügyi Központ nevében küldött, káros csatolmányt tartalmazó levéllel kapcsolatban
Forrás: https://bit.ly/3nAuAFl

A 2020-ban a detektált incidensek száma tekintetében a következő emelkedés az őszi, szeptember és november közötti időszakra, tehát a Covid–19 második hullámára tehető. Ezen időszakban az alábbi, 7. ábra által bemutatott incidenstípusokat azonosították.



7. ábra: Az NKI által detektált incidensek eloszlása 2020. szeptember–november
Forrás: a szerző szerkesztése

A dobogó legfelső fokán elhelyezkedő káros tevékenység hátterében a megnövekedett Emotet-aktivitás áll, amely jellemzően egészségügyi intézmények nevében kiküldött, káros csatolmányt tartalmazó csaló levelekkel,[53] valamint fertőzött e-mail-fiókok kapcsolati listája útján terjed.[54] Emellett a jelzett időszakban közüzemi szolgáltatók nevével visszaélő,[55] valamint Covid–19 témájú adathalász/káros tartalmú levelek okoztak incidenseket, a kormányzati és a pénzügyi szektorokat érintő DDoS-támadások[56] mellett. Ez utóbbinak köszönhető, hogy az őszi időszakban az elérhetőség a dobogó második helyén végzett. A következő, 8. ábrán látható grafikon a Covid–19 első és második hulláma során azonosított incidensek típusait hasonlítja össze.



8. ábra: A Covid 1. és 2. hulláma alatti incidenstípusok összehasonlítása
Forrás: a szerző szerkesztése

Az elemzésből egyértelműen megállapítható, hogy míg az első hullám során az ismert sérülékenység kihasználása, illetve a káros tevékenység voltak a domináló incidenstípusok, addig a második hullámban a káros tevékenység mellett már az elérhetőség és az információgyűjtés voltak a legmeghatározóbbak. Egyéb típusok tekintetében, mint az ismeretlen típusú káros kód, defacement, spam, információk illetéktelen hozzáférése, nem adminisztrátor fiók kompromittálódása, valamint a DDoS és a ransomware, kiegyenlített volt az összes incidenshez viszonyított arányuk mindkét időszakban.

53 Lásd: https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-egeszsegugyi-intezmenyeket-erinto-emotet-terjesztesi-kampannyal-kapcsolatban/
54 Lásd: https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-megnovekedett-emotet-aktivitas-kapcsan/
55 Lásd: https://nki.gov.hu/figyelmeztetesek/tajekoztatas/tajekoztatas-kozuzemi-szolgaltatok-nevevel-visszaelo-adathalasz-uzenetekrol/
56 Lásd: https://nki.gov.hu/figyelmeztetesek/tajekoztatas/tajekoztatas-kormanyzati-es-penzugyi-szektorokat-erinto-ddos-tamadasokkal-kapcsolatban/

Amennyiben a kapott eredményeket összevetjük az ENISA által, a Threat Landscape 2020 keretében bemutatott Covid–19-hez kapcsolódó elemzésével,[57] illetve az Interpol által összeállított jelentéssel, amely a kibertámadások riasztó arányát mutatja a Covid–19 idején,[58] megállapíthatjuk, hogy az elemzés eredményeként a Covid 2020-as időszakában azonosított hazai incidenstrendek megfelelnek az európai trendeknek. Az összehasonlítást az 1. táblázat mutatja be részletesen.

1. táblázat: A Covid–19 idején, az NKI által detektált hazai incidensek összehasonlítása az európai incidenstrendekkel

ENISA Threat Landscape 2020 – Covid–19 Incidenstrendek	NKI, 2020 (1. és 2. hullám) Incidenstrendek	Interpol – Covid–19 Incidenstrendek	NKI, 2020 (1. és 2. hullám) Incidenstrendek
Távmunkához kapcsolódó infrastruktúrákhoz köthető támadások	✓	Adathalászat/Átverés/Csalás	✓
Koronavírussal kapcsolatos domainek	✓	Malware/Ransomware	✓
Sms-es adathalászat	✓	Rosszindulatú domainek	✓
E-mailes adathalászat	✓	Álhírek	✓
Hamis tesztelési alkalmazások			
Támadások egészségügyi szervezetek ellen	✓		

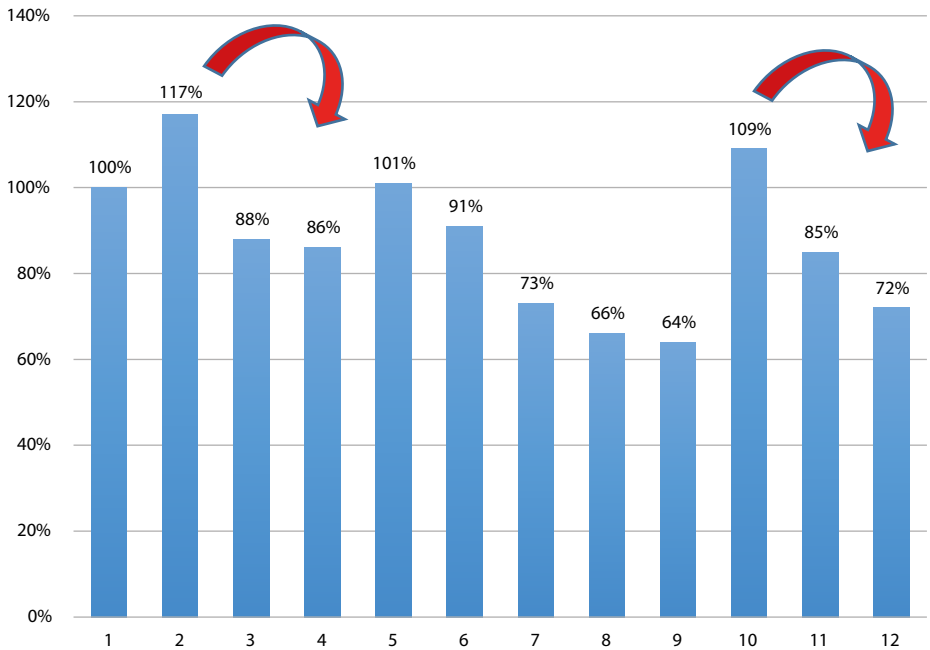
Forrás: a szerző szerkesztése

2021. év vizsgálata

A 2021. évben, az NKI által azonosított incidensek havi eloszlása tekintetében – a 2020. évhez hasonlóan – megállapítható a Covid tavaszi (harmadik) és őszi (negyedik) hulláma során történő százalékos emelkedés. (A 9. ábrán látható elemzés során – az előző két évhez hasonlóan – a januári hónapban azonosított incidenseket tekintem 100%-nak, és az ehhez képest való elmozdulást vizsgálom havonkénti viszonylatban.)

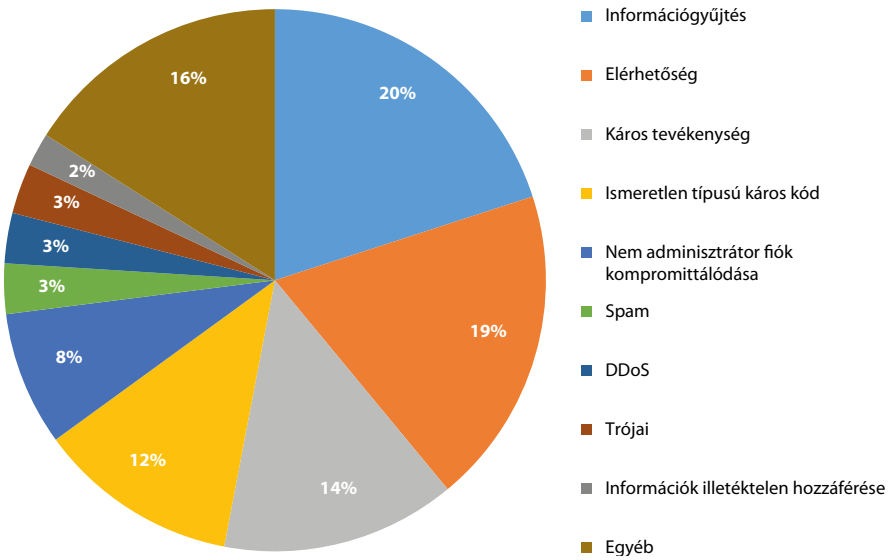
[57] Threat Landscape Mapping Infographic 2020, lásd: www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/threat-landscape-mapping-infographic-2020

[58] Interpol 2020.



9. ábra: 2021. évi vizsgálat – Az incidensek havi eloszlása
Forrás: a szerző szerkesztése

A 2021-ben kezelt incidensek típusai szerinti eloszlást az alábbi, 10. ábra mutatja be:



10. ábra: A 2021. év NKI által kezelt incidensei
Forrás: a szerző szerkesztése

Az incidensek típus szerinti eloszlása tekintetében az előző évhez képest nem történt jelentős változás, az arányok tekintetében csupán néhány százalék eltérés mutatható ki. A három leggyakoribb incidenstípus az információgyűjtés (20%), az elérhetőség (19%), valamint a káros tevékenység (14%), de jelentős százalékban fordul elő az ismeretlen típusú káros kód (12%), valamint a nem adminisztrátor fiókok kompromittálódása (8%) is.

A statisztikai eredmények hátterében a következő tendenciák azonosíthatók:

- a Covid–19-járványhoz kapcsolható kiberfenyegetések és incidensek száma csökkent;
- az Emotet vírus a Covid harmadik hullámának elején (2021. február),[59] valamint az őszi következő hullámban (2021. november)[60] ismét fokozott aktivitást mutatott;
- 2021. márciusban a Microsoft Exchange szerverek esetében négy nulladik napi, tehát a fejlesztők által még fel nem fedezett sérülékenységet (ProxyLogon, illetve a ProxyShell) azonosítottak, amelyek kihasználásával a támadók teljes irányítást szerezhettek a levelezőrendszer felett;[61]
- 2021. márciusban megjelent, majd októberben[62] újra erőre kapott a Flubot malware, amely csomagküldő szolgáltatók nevével visszaélő, káros kód terjesztésével összefüggő sms-üzenetek útján terjedt;[63]
- 2021. októberben a Pécsi Tudományegyetem,[64] valamint a Magyar Posta nevével és arculati elemeivel visszaélő[65] káros csatolmányt tartalmazó levelek terjedtek el a magán- és a közszférában egyaránt;
- 2021. októberben nagy mennyiségű kéretlen, adathalász tartalmú, káros csatolmánnyal rendelkező e-mail-üzenetek terjedése volt megfigyelhető;[66]
- 2021. novemberben a Microsoft Exchange szervereket érintő újabb 0. napi sérülékenységet (ProxyNotShell) azonosítottak. Sikeres kihasználás esetén a megfelelő jogosultsággal rendelkező támadó távoli kódfuttatást hajthatott végre az érintett szerveren;[67]

59 Lásd: https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-emotet-malware-kapcsan/

60 Lásd: https://nki.gov.hu/figyelmeztetesek/tajekoztatas/tajekoztatas-emotet-malware-ismetelt-felbukkanasaval-osszefuggesben/

61 Lásd: https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-microsoft-exchange-szerverek-serulekenysegeivel-kapcsolatban/

62 Lásd: https://nki.gov.hu/figyelmeztetesek/tajekoztatas/rendkivuli-tajekoztato-flubot-malware-rel-kapcsolatban/

63 Lásd: https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-csomagkuldo-szolgaltatok-nevevel-visszaelo-malware-terjesztessel-osszefuggo-sms-uzenetekkel-kapcsolatban/

64 Lásd: https://nki.gov.hu/figyelmeztetesek/tajekoztatas/tajekoztatas-a-pecsi-tudomanyegyetem-nevevel-visszaelo-karos-csatolmanyt-tartalmazo-levelekkel-kapcsolatban/

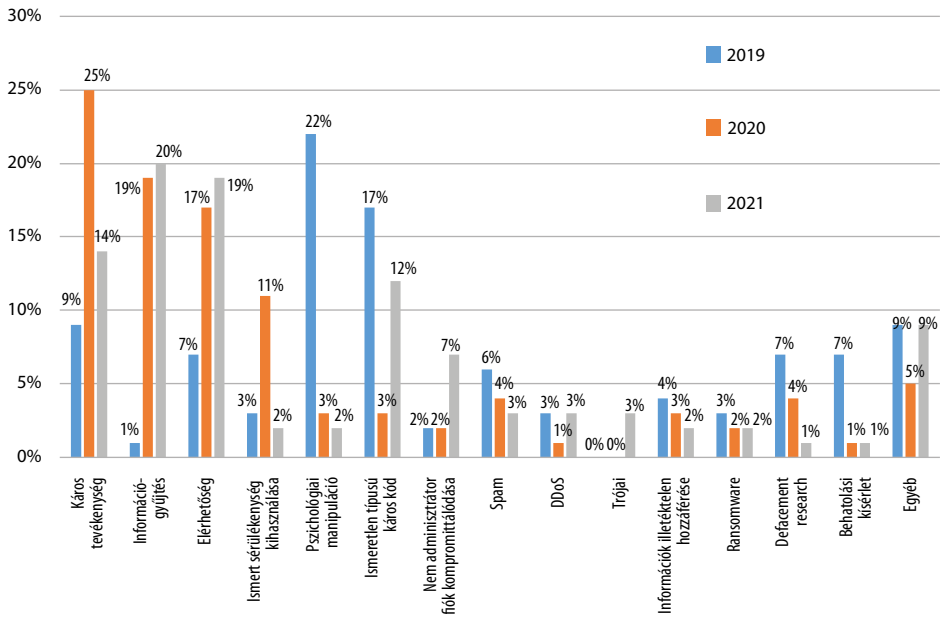
65 Lásd: https://nki.gov.hu/figyelmeztetesek/tajekoztatas/tajekoztatas-a-magyar-posta-nevet-es-arculati-elemeit-felhasznalo-adathalasz-uzenetekkel-kapcsolatban/

66 Lásd: https://nki.gov.hu/figyelmeztetesek/tajekoztatas/rendkivuli-tajekoztato-keretlen-adathalasz-tartalmu-e-mail-uzenetek-kapcsan/

67 Lásd: https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-microsoft-exchange-szervereket-erinto-0-napi-serulekenysegrol/

- 2021. decemberben az azonosított Log4shell sérülékenység kihasználásával kapcsolatban ransomware-/malware-terjesztés volt megfigyelhető. A sérülékenység hitelesítés nélküli, tetszőleges, távoli kódfuttatást tett lehetővé a támadók számára, amelynek sikeres kihasználása estén teljes, rendszerszintű hozzáféréssel rendelkezhettek.[68]

A 11. ábra, a 2019–2021 közötti időszak évenként azonosított, leggyakoribb tíz incidenstípusának összehasonlítását mutatja be (az egyes évek tekintetében, az adott incidenshez kapcsolódó százalékos arány az adott évben detektált valamennyi incidenshez viszonyított aránya).



11. ábra: 2019–2021 TOP 10 incidenstípusai
Forrás: a szerző szerkesztése

A vizsgált három év viszonylatában megállapítható, hogy az egyes incidenstípusok tekintetében – néhány kivételtől eltekintve – a 2019. évhez viszonyítva 2020-ban és 2021-ben százalékos emelkedés figyelhető meg, amely hangsúlyosan a dobogó első három helyét elfoglaló incidenstípusok, a káros tevékenység, az információgyűjtés és az elérhetőség esetén jelenik meg. Hasonló tendencia mutatkozik meg a nem adminisztrátor fiók kompromittálódása, valamint a trójai vírus esetében is. Az ismert sérülékenység kihasználásának 2020-ban tapasztalható kiugróan magas aránya a Microsoft Exchange mailszervereket érintő támadásnak volt köszönhető.

[68] Lásd: https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-apache-log4j-konyvtart-erinto-kritikus-serulekenyseggel-kapcsolatban/

A pszichológiai manipuláció esetében a 2019-es évhez viszonyítva jelentős visszaesés tapasztalható a 2020–2021-es években. Szakmai tapasztalatom és megfigyelésem alapján ez nem jelenti a social engineering típusú támadások tényleges csökkenését, valójában egy kategorizálásból eredő eltérés állhat a hátterében. Ugyanis, ha jobban megvizsgáljuk a grafikont, akkor látható, hogy a pszichológiai manipuláció csökkenésével párhuzamosan emelkedik az információgyűjtés százalékos aránya. Az ENISA referenciaincidens-taxonómiája[69] szerint a pszichológiai manipuláció az információgyűjtés fő kategóriájához tartozik, annak egyik alkategóriája, így feltételezhetően az incidensek osztályozása során a pszichológiai manipulációval megvalósuló információgyűjtés esetén az utóbbi típust, tehát az információgyűjtést jelölte meg a 2020. és 2021. években.

Az ismeretlen típusú káros kód, a spam, az információk illetéktelen hozzáférése, a ransomware, a defacement és a behatolási kísérlet százalékos arányában, az adott évben detektált incidensek összesített számához képest, a 2020. és 2021. évben csökkenés figyelhető meg. Természetesen ez nem jelenti feltétlenül az adott típushoz tartozó incidensek számszerű csökkenését, ez csupán arra a tendenciára utal, amely az adott incidenstípus esetében, az adott évben bekövetkező összes incidenshez viszonyított arányában való változást szemlélteti.

Szektorális összehasonlítás

A tanulmány jelen részében, az NKI által detektált, az írás elején részletesen bemutatott alábbi szektorok tekintetében azonosított incidenseket elemezzük:

- állami és önkormányzati szervek,
- nemzeti létfontosságú rendszerelemek,
- alapvető szolgáltatásokat nyújtó szereplők,
- bejelentésköteles szolgáltatók,
- közvetítő szolgáltatók,
- nemzetbiztonsági védelem alá eső szervezetek,
- oktatási intézmények,
- egyéb szervezetek.

A 2019 és 2021 közötti időszakban az NKI az egyes vizsgált szektorokat érintően az állami és önkormányzati szervek tekintetében detektálta a legtöbb eseményt – a vizsgált három évben az összes incidens 47%-a –, míg a nemzetbiztonsági védelem alá eső szervezetek esetében ez az arány 8%, a közvetítő szolgáltatók és az oktatási intézmények tekintetében pedig 7%.

A 2. táblázat összefoglalja a 2019–2021 közötti időszakban az egyes szektorokat érő incidenseknek az összes detektált incidenshez viszonyított százalékos arányát.

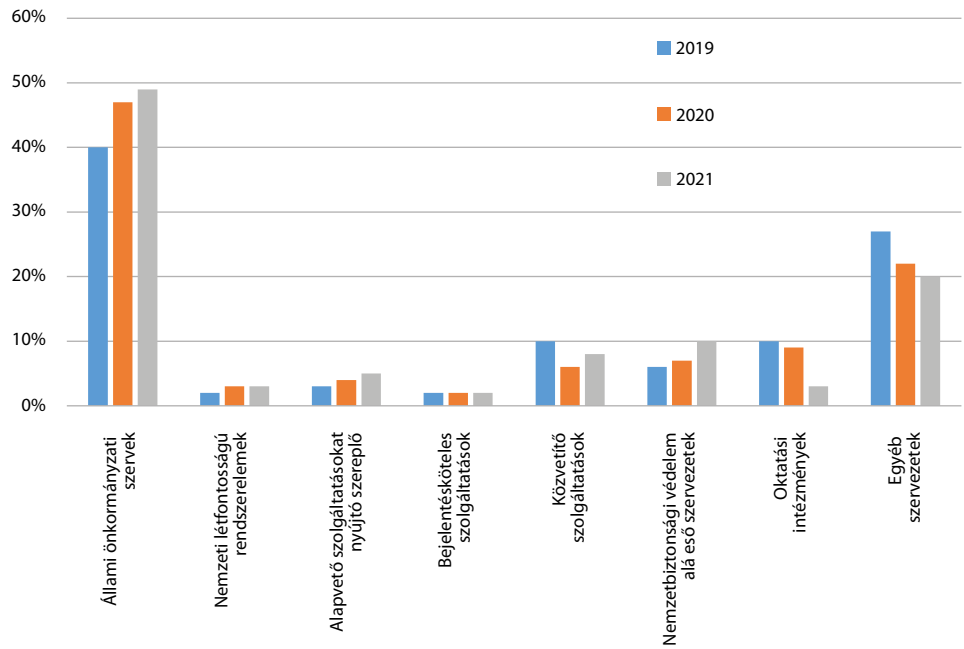
[69] ENISA 2018.

2. táblázat: Az egyes szektorokban kezelt incidensek százalékos eloszlása a 2019–2021. évek összesített eredményeinek tükrében

Az incidensben érintett szektor	Incidensek összesített százalékos aránya 2019–2021
Állami és önkormányzati szervek	47%
Nemzetbiztonsági védelem alá eső szervezetek	8%
Közvetítő szolgáltatók	7%
Oktatási intézmények	7%
Alapvető szolgáltatásokat nyújtó szereplő	4%
Nemzeti létfontosságú rendszerelemek	3%
Bejelentésköteles szolgáltatók	2%
Egyéb szervezetek	22%

Forrás: a szerző szerkesztése

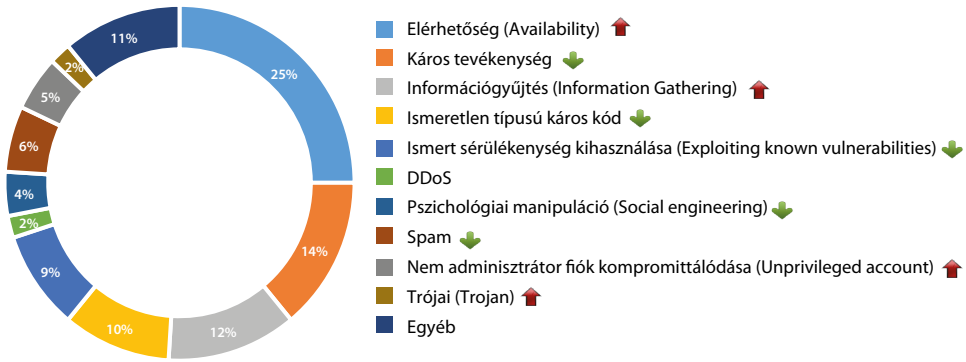
Ahhoz, hogy az egyes szektorokat érintő trendek is kimutathatók legyenek, meg kell vizsgálni, hogy az egyes szektorokat évenkénti bontásban milyen arányban érte incidens, amit a 12. ábra szemléltet.



12. ábra: Szektorális bontás 2019–2021 közötti időszakban, évenkénti bontásban
Forrás: a szerző szerkesztése

A grafikon alapján megállapítható, hogy a leginkább támadott állami és önkormányzati szervek esetében az egyes években, az eseményeknek az összes detektált incidenshez viszonyított aránya nő, így e szektor részéről fokozott védelmi intézkedések szükségesek a további emelkedés megakadályozása érdekében. Hasonló emelkedő tendencia mutatható ki a második legtámadottabb szektor, a nemzetbiztonsági védelem alá eső szervek tekintetében is, valamint az alapvető szolgáltatásokat nyújtó szereplők és a nemzeti létfontosságú rendszerelemek esetében is. A bejelentésköteles szolgáltatók esetében stagnálás, míg a közvetítő szolgáltatók és az oktatási intézmények tekintetében csökkenés figyelhető meg. Az állami és az önkormányzati szervek – mint a legtámadottabb szektor – különálló, incidenstípusok szerinti vizsgálata is indokolt annak érdekében, hogy azonosíthatók legyenek a leginkább fenyegető támadási vektorok.

A 2019 és 2021 közötti időszakban, az állami és önkormányzati szerveket érő incidensek eloszlását a 13. ábra mutatja be.



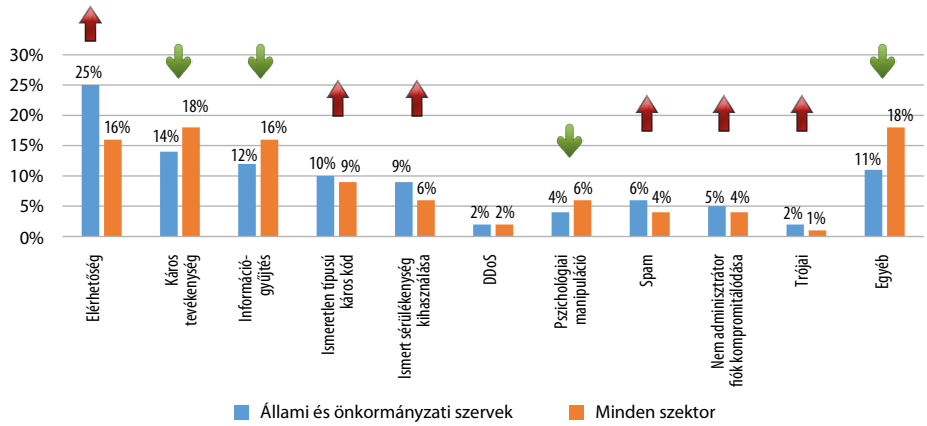
13. ábra: Az állami és önkormányzati szervek incidensei, 2019–2021
Forrás: a szerző szerkesztése

A vizsgált időszakban az elérhetőség volt a legkritikusabb incidenstípus, minden negyedik incidens eredményezte a rendelkezésre állás problémáját az állami és önkormányzati szerveknél (az összes detektált incidenshez viszonyított aránya 25%). Káros tevékenység az incidensek 8%-ában, információgyűjtés 12%-ban, míg ismeretlen típusú káros kód, illetve ismert sérülékenység kihasználása 10, illetve 9%-ban fordultak elő. Az összincidensekhez viszonyítva 10% alatti az aránya a spameknek, a nem adminisztrátor fiók kompromittálódásának, a pszichológiai manipulációnak, valamint a DDoS- és a trójaivírus-támadásoknak.

Amennyiben összehasonlítjuk az állami és önkormányzati szerveket érő leggyakoribb tíz incidenstípus százalékos arányát az egyes incidenstípusoknak az összes szektoron belüli arányával, az alábbi összefüggéseket állapíthatjuk meg a 14. ábra segítségével:

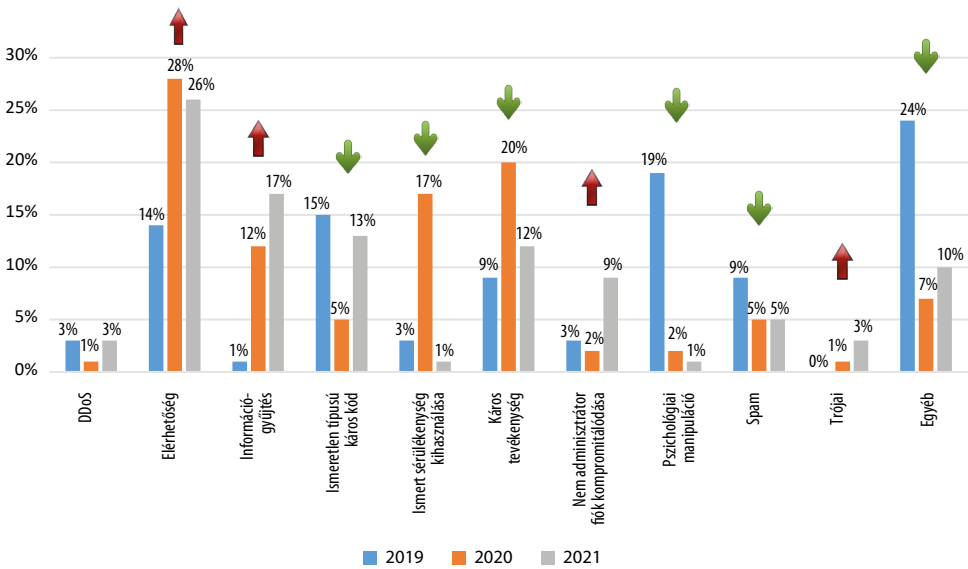
Az elérhetőség, az ismeretlen típusú káros kód, az ismert sérülékenység kihasználása, a spam, a nem adminisztráror fiók kompromittálódása, valamint a trójai vírus incidenstípusok nagyobb arányban fordulnak elő az állami és önkormányzati szervek esetében (az összes szektort érintő átlaghoz viszonyítva), ugyanakkor a káros

tevékenység, az információgyűjtés és a pszichológiai manipuláció kisebb százalékban mutatható ki.



14. ábra: Összehasonlító statisztika az állami és önkormányzati szervek és az összes szektor tekintetében, incidenstípusok alapján
Forrás: a szerző szerkesztése

A 15. ábra segítségével meghatározhatók az állami és önkormányzati szerveket érintő leggyakoribb incidenstípusokhoz kapcsolódó trendek is.



15. ábra: Az állami és önkormányzati szervek incidenstípusai évenkénti összehasonlításban
Forrás: a szerző szerkesztése

A grafikon alapján az elérhetőség, az információgyűjtés, a nem adminisztrátor fiók kompromittálódása, valamint a trójai vírus esetében emelkedő trend azonosítható, míg az ismeretlen típusú káros kód, az ismert sérülékenység kihasználása, a káros tevékenység, a pszichológiai manipuláció, illetve a spamek esetében csökkenő tendencia látható. A DDoS esetében a 2020-ban történő csökkenést követően 2021-ben az arányszám ismét a 2019-es szintre emelkedett.

Pszichológiai manipuláció *(social engineering)*

A pszichológiai manipuláció (social engineering) az emberi hiszékenységre és együttműködésre építő támadási forma. Bár ezt az élet sok más területén is kihasználják, a social engineering kimondottan az információ megszerzésére irányul, ezen belül is elsősorban az informatikai eszközökön tárolt adatokra fókuszálva.[70]

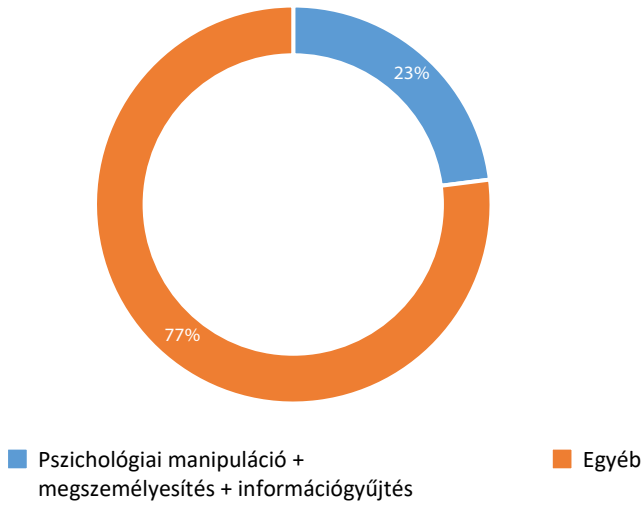
A NKI adatait évenkénti bontásban vizsgálva már megállapítottuk, hogy a pszichológiai manipuláció esetében a 2019-es évhez viszonyítva jelentős visszaesés tapasztalható a 2020–2021-es években, ami azonban nem jelenti a social engineering típusú támadások tényleges csökkenését, valójában egy kategorizálásból eredő eltérés állhat a hátterében. Az elemzett adatok alapján megállapítottuk, hogy a pszichológiai manipuláció csökkenésével párhuzamosan emelkedik az információgyűjtés százalékos aránya, aminek hátterében az ENISA referenciaincidens-taxonómiája állhat, amely szerint a pszichológiai manipuláció az információgyűjtés alkategóriáját képezi. Így feltehetően az incidensek osztályozása során a pszichológiai manipulációval megvalósuló információgyűjtés esetén az utóbbi típust, tehát az információgyűjtést jelölték meg a 2020. és 2021. években.

E jelenségből adódó statisztikai eltérések kiküszöbölése érdekében a pszichológiai manipuláció vizsgálatánál az incidenstípusok alábbi három kategóriájának összesített százalékos eloszlását vizsgáltam a 2019–2021. időszakban:

- pszichológiai manipuláció,
- megszemélyesítés (amely a pszichológiai manipuláció egyik támadási formája) és
- információgyűjtés.

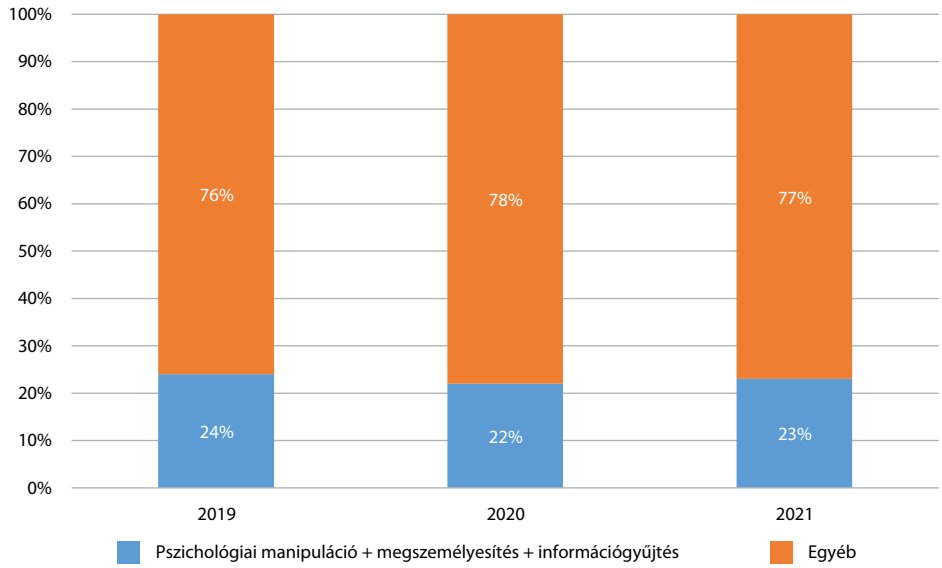
A 16. ábra alapján megállapítható, hogy a három incidenstípus összesített aránya a 2019–2021. években detektált összes incidenshez képest 23%.

[70] Muha–Krasznay 2014: 53.



16. ábra: A pszichológiai manipuláció, a megszemélyesítés és az információgyűjtés összesített aránya, 2019–2021
Forrás: a szerző szerkesztése

A tágabb értelemben vett pszichológiai manipulációt jellemző trend meghatározása érdekében összehasonlítottam az egyes években kimutatható arányukat az összes incidensen belül, amit a 17. ábra szemléltet.



17. ábra: A pszichológiai manipuláció, a megszemélyesítés és az információgyűjtés együttes, egyéb incidenstípusokhoz viszonyított aránya, 2019–2021
Forrás: a szerző szerkesztése

Az elemzés segítségével megállapítható, hogy a pszichológiai manipuláció, a megszemélyesítés és az információgyűjtés együttes aránya kiegyensúlyozott az egyes években, az egyéb incidenstípusokhoz viszonyított arányuk 22% és 24% között mozog. Ugyanakkor meg kell jegyezni, hogy még ha százalékos arányban a detektált incidensek majd egynegyedénél mutatható csupán ki tágabb értelemben vett pszichológiai manipuláció, sikerességük esetén jelentősen nagyobb és komolyabb károk következhetnek be, legyen szó akár információk jogosulatlan megszerzéséről, adatok titkosításáról vagy egyéb káros tevékenységről.

Összegzés és következtetések

A digitalizáció robbanásszerű terjedésének köszönhetően a kibertérben megjelenő, különböző forrásból származó fenyegetések száma és volumene, valamint a támadások következményei is jelentősen megnövekedtek. A kiberbiztonság megfelelő szinten tartása és folyamatos fejlesztése, a kockázatok kezelése, a hatékony védelmi intézkedések alkalmazása az állam elsőrendű feladata. A biztonsági események típusainak és az azonosítható trendeknek az ismerete nagyban elősegíti e kibervédelmi feladatok ellátását és Magyarország szuverenitásának védelmét a magyar kibertérben.

A 2019 és 2021 közötti évek incidenstrendjei azonosítása érdekében e tanulmány keretében elemeztem a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet által detektált incidensekre vonatkozó statisztikai adatokat évenkénti és szektorális bontásban. Az egyes évek vizsgálata során bemutattam a Covid–19-pandémia kiberbiztonságra gyakorolt hatását is. Az ágazati elemzés során kiemelten vizsgáltam a leginkább támadott szektort, az állami és önkormányzati szerveket érő incidenseket, az eredményeket összevetettem az NKI által kezelt egyéb ágazatokban kimutatható események típusaival és az azokhoz köthető trendekkel. Külön fejezetben tértem ki az emberi hiszékenységen és együttműködési készségen alapuló pszichológiai manipuláció, azaz social engineering típusú támadási forma vizsgálatára.

Elemzésem során néhány kiemelkedő tendenciát összevetettem a nemzetközi incidenstrendekkel, aminek segítségével megállapítottam, hogy a hazai incidenstrendek a vizsgált években jelentős eltérést nem mutattak a nemzetközi trendekhez képest. Ennek hátterében elsősorban az áll, hogy a magyar kibertér nem határolható le a klasszikus fizikai országhatárokhoz hasonlóan. A Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat értelmében

> „Magyarország kibertere a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve amelyekben Magyarország érintett".

E megfogalmazásból is jól látható, hogy a magyar kibertérben zajló események egyáltalán nem függetleníthetők a globális kibertértől, ez utóbbinak részei, így a globális

hatások hazánkban is kimutathatók, a világszerte tapasztalható incidensek valamilyen formában itt is megjelennek.

A 2020-ban megjelenő világjárvány tökéletesen megmutatta a határokon, sőt kontinenseken átívelő tendenciákat. A 2020. évre vonatkozó elemzésből kiderül, hogy a koronavírus egyes hullámaihoz kapcsolódóan szignifikánsan megemelkedett az NKI által detektált incidensek száma, a tavaszi (2020. február–április) és az őszi hullám (2020. szeptember–november) incidenseinek összesített aránya eléri az összes éves incidens közel 60%-át. 2021-re is igaz, hogy az incidensek százalékos aránya a tavaszi (2021. február–április) és az őszi (2021. szeptember–november) hullám során jelentősen megemelkedett. Mind a számszerű emelkedés, mind pedig az incidenstípusok tekintetében jelentős átfedés tapasztalható a nemzetközi trendekkel, amelyeket a kibertámadók praktikusan alakítottak át, sok esetben a magyar viszonyoknak megfelelően.

Az azonosított trendek egyértelműen bizonyítják a kibertámadók rendkívül gyors alkalmazkodóképességét a világ megváltozott körülményeihez. A Covid–19-világjárvány egyedülálló lehetőségeket teremtett a fenyegetettségi szereplők számára, hogy hasznot húzzanak a bizonytalanságból, a korlátozásokból és az egyes termékek iránti kereslet fellendüléséből. A pandémia alatt a támadók a kiberbűnözés már létező formáit úgy alakították át, hogy azok megfeleljenek a világjárvány narratívájának, kihasználva a helyzet bizonytalanságát és a lakosság megbízható információ iránti igényét. A csalók előszeretettel alkalmaztak social engineering technikákat az emberi viselkedés manipulálására és a gyenge pontok kihasználására az információk megszerzése érdekében.

Az elemzés egyértelműen rávilág arra a tényre, hogy a kiberbiztonsági fenyegetések, a bekövetkezett biztonsági események típusainak, számszerűségének és következményeinek ismerete, valamint az incidenstrendek vizsgálata és figyelemmel kísérése jelentősen hozzájárul a hatékony védelmi intézkedések meghatározásához, végső soron a magyar kibertér megfelelő védelméhez.

Irodalomjegyzék

Berzsenyi Dániel et al. (2018): *Incidensmenedzsment. Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára.* Budapest: Dialóg Campus.

ENISA (2018): *Reference Incident Classification Taxonomy.* Online: www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

Europol (2021): *World's Most Dangerous Malware EMOTET Disrupted through Global Action.* 2021. január 27. Online: www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

Interpol (é. n.): *COVID-19 Cyberthreats.* Online: www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats

Interpol (2020): *Interpol Report Shows Alarming Rate of Cyberattacks during COVID-19.* 2020. augusztus 4. Online: www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

Krasznay Csaba – Dobos László – Palla Gergely – Pollner Péter (2019): Információbiztonsági incidensek a közigazgatásban. In Auer Ádám – Joó Tamás (szerk.): *Hálózatok a közszolgálatban.* Budapest: Dialóg Campus, 135–154.

Marsi Tamás (2018): A Nemzeti Kibervédelmi Intézet szerepe az eseménykezelésben. In Berzsenyi Dániel et al.: *Incidensmenedzsment.* Budapest: Nemzeti Közszolgálati Egyetem, 49–84. Online: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/6848/Incidensmenedzsment.pdf?sequence=1

Monori Zsuzsanna Éva (2016): Zaklatás-e a cyberbullying? Az internetes zaklató magatartások büntetőjogi szankcionálásának dilemmái. *In Medias Res,* 5(2), 246–261.

Muha Lajos – Krasznay Csaba (2014): *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest: Nemzeti Közszolgálati Egyetem.

Miniszterelnöki Kabinetiroda (2021): *Nemzeti Digitalizációs Stratégia 2022–2030.* Online: https://cdn.kormany.hu/uploads/document/6/60/602/60242669c9f12756a2b104f8295b866a8bb8f684.pdf

Nabe, Cedrik (é. n.): Deloitte, Impact of COVID-19 on Cybersecurity. *Déloitte,* (é. n.) Online: https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html

Jogi források

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

271/2018. (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól