EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA FENYEGETÉSEK 2021-BEN

2020 áprilistól - 2021 július közepéig

2021. OKTÓBER

AZ EINSA-RÓL

Az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) az Unió azon ügynöksége, amelynek célja az Európa-szerte magas szintű általános kiberbiztonság megvalósítása. A 2004-ben létrehozott és az uniós kiberbiztonsági jogszabály által megerősített Európai Uniós Kiberbiztonsági Ügynökség hozzájárul az uniós kiberpolitikához, kiberbiztonsági tanúsítási rendszerek alkalmazásával javítja az IKT-termékek, -szolgáltatások és -folyamatok megbízhatóságát, együttműködik a tagállamokkal és az uniós szervekkel, és segíti Európát abban, hogy felkészüljön a jövő kiberbiztonsági kihívásaira. A tudásmegosztás, a kapacitásépítés és a figyelemfelkeltés révén az Ügynökség a legfontosabb érdekelt felekkel együtt arra törekszik, hogy megerősítse az összekapcsolt gazdaságba vetett bizalmat, fokozza az uniós infrastruktúra ellenálló-képességét és végső soron megőrizze Európa társadalmának és polgárainak digitális biztonságát. Az ENISA-ról és tevékenységéről további információkat találhat itt: www.enisa.europa.eu.

KAPCSOLAT

Ha kapcsolatba szeretne lépni a szerzőkkel, kérjük, írjon a következő email címre: etl@enisa.europa.eu.
A dokumentummal kapcsolatos sajtómegkereséseket, kérjük, az alábbi címre küldjék: press@enisa.europa.eu.

SZERKESZTŐK

Ifigeneia Lella, Marianthi Theocharidou, Eleni Tsekmezoglou, Apostolos Malatras – Európai Uniós Kiberbiztonsági Ügynökség

KÖZREMŰKÖDŐK

Claudio Ardagna, Stephen Corbiaux, Andreas Sfakianakis, Christos Douligeris

KÖSZÖNETNYILVÁNÍTÁS

Szeretnénk köszönetet mondani az ENISA kiberfenyegetettséggel foglalkozó ad hoc munkacsoportja tagjainak és megfigyelőinek a jelentés hitelesítéséhez nyújtott értékes visszajelzéseikért és észrevételeikért. Szeretnénk köszönetet mondani az ENISA tanácsadó csoportjának és a nemzeti összekötő tisztviselők hálózatának is értékes visszajelzéseikért.
Szeretnénk köszönetet mondani az ENISA helyzetfelismerési és eseménybejelentő csoportjainak is a különböző információknak a fenyegetettségek rendszerezésében nyújtott aktív közreműködésükért és támogatásukért.

JOGI NYILATKOZAT

SZERZŐI JOGI NYILATKOZAT

ISBN: 978-92-9204-536-4 – DOI: 10.2824/324797 – ISSN: 2363-3050

TARTALOMJEGYZÉK

VEZETŐI ÖSSZEFOGLALÓ

Ez az ENISA Fenyegetettségi helyzetjelentésének (ETL) kilencedik kiadása, amely a kiberbiztonsági fenyegetettségről szóló éves jelentés, amely azonosítja az elsődleges fenyegetéseket, a fenyegetések, a fenyegető szereplők és a támadási technikák vonatkozásában megfigyelt főbb tendenciákat, valamint ismerteti a vonatkozó enyhítő intézkedéseket. A fenyegetettségi helyzet feltérképezésére szolgáló módszertanunk folyamatos javítása során az idei évi munkát az ENISA újonnan létrehozott, a kiberbiztonsági fenyegetettségi helyzet feltérképezésével foglalkozó ad hoc munkacsoportja (CTL) támogatta.

Az 2021. évi fenyegetettségi helyzetjelentés időintervalluma 2020. áprilisától 2021. júliusáig tart, és a jelentésben végig „jelentési időszakként" hivatkozunk rá. A jelentési időszakban az elsődlegesen azonosított fenyegetések a következők:

- **Zsarolószoftverek**
- **Rosszindulatú szoftverek**
- **Cryptojacking**
- **E-mail üzenetekhez kapcsolódó fenyegetések**
- **Adatok elleni fenyegetések**
- **A rendelkezésre állás és az integritás elleni fenyegetések**
- **Dezinformáció - félretájékoztatás**
- **Nem rosszindulatú fenyegetések**
- **Ellátási láncot érintő támadások**

Ebben a jelentésben az első 8 kiberbiztonsági fenyegetéskategóriát tárgyaljuk. Az ellátási láncot fenyegető veszélyeket, a 9. kategóriát, különös jelentőségük miatt részletesen elemezték az ENISA "ENISA Ellátási láncok elleni támadásokra vonatkozó fenyegetettségi helyzet" című jelentésében." [1].

Minden egyes azonosított fenyegetés vonatkozásában megvitatták a támadási technikákat, a lényeges eseményeket és tendenciákat, valamint a javasolt enyhítő intézkedéseket. A tendenciák vonatkozásában a jelentési időszakban a következőket emeljük ki:

- **A zsarolóvírusokat** a 2020-2021 időszak elsődleges fenyegetéseként értékelték.
- A kormányzati szervezetek mind nemzeti, mind nemzetközi szinten intenzívebb tevékenységet folytattak.
- A **kiberbűnözőket** egyre jobban motiválja tevékenységük pénzre váltása, pl. a zsarolóvírusok. A **kriptovaluta** továbbra is a fenyegető szereplők leggyakoribb kifizetési módszere.
- A **rosszindulatú szoftverek** használatának 2020-ban megfigyelt csökkenése 2021-ben is folytatódik. 2021-ben növekedést tapasztaltunk azon fenyegető szereplők körében, akik kódjuk portolásához viszonylag új vagy szokatlan programozási nyelvekhez folyamodnak.
- A **cryptojacking fertőzések** száma az előző évekhez képest 2021 első negyedévében **csúcsot döntött**. A cryptojacking alkalmazásával járó anyagi haszon a fenyegető szereplőket ilyen támadások végrehajtására ösztönözte.
- A **Covid19 továbbra is domináns vonzerőt jelent** a tömeges e-mailes támadásoknál.
- **Az egészségügyi szektorhoz kapcsolódó adatvédelmi incidensek száma megugrott.**
- A **tradicionális elosztott szolgáltatásmegtagadással járó támadás (Distributed Denial of Service) kampányok** 2021-ben célzottabbakká, tartósabbakká váltak és egyre több szektorra irányulnak. Az **IoT (Internet of Things-a dolgok internete)** a **mobilhálózatokkal** együtt a DDoS-támadások új hullámát eredményezi.

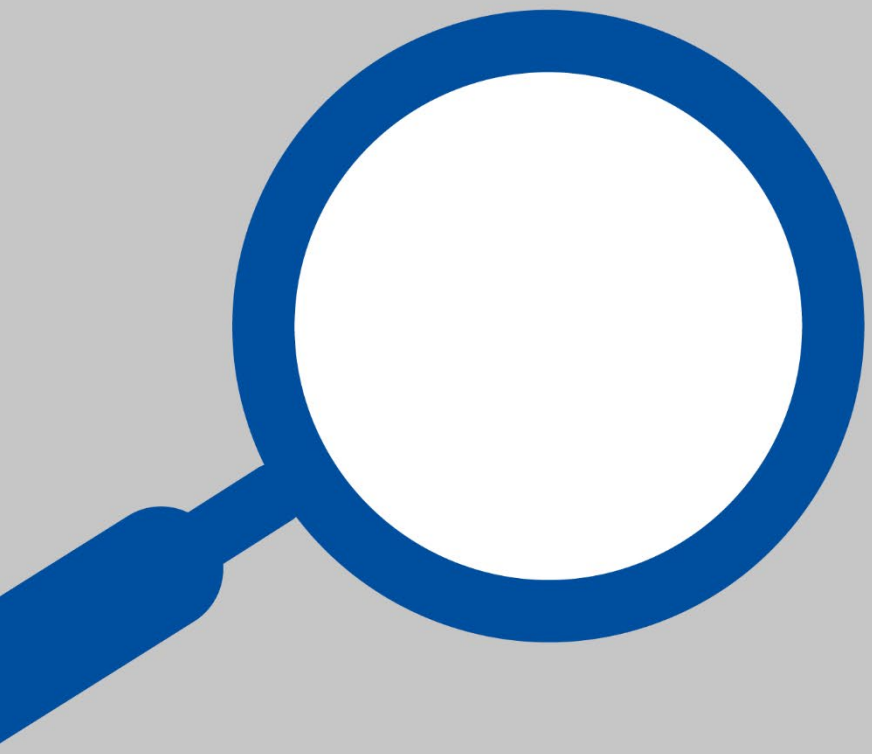
[1] ENISA Ellátási láncok elleni támadásokra vonatkozó fenyegetettségi helyzet 2021 július. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

- A 2020. és a 2021. években a **nem rosszindulatú incidensek számának megugrását** figyelhetjük meg, mivel a Covid19 járvány az emberi hibák és a rendszerhibák multiplikátorává vált, egészen addig a pontig, hogy 2020-ban a legtöbb betörést hibák okozták.

A fenyegető szereplőkkel, motivációikkal és célpontjaikkal kapcsolatos tendenciák megértése nagyban segíti a kiberbiztonsági védekezés és a kárenyhítési stratégiák megtervezését. Ez az átfogó fenyegetettség-értékelésünk szerves részét képezi, mivel lehetővé teszi a biztonsági ellenőrzések rangsorolását és a fenyegetés megvalósulásának potenciális hatása és valószínűsége alapján egy célzott stratégia kidolgozását. Ezt szem előtt tartva a 2021. évi fenyegetettségi helyzetjelentés céljaira a kiberbiztonsági fenyegetések szereplőinek alábbi négy kategóriáját vesszük figyelembe:

- **Államilag támogatott szereplők**
- **Kiberbűnözéssel foglalkozó szereplők**
- **Felbérelt hacker szereplők**
- **Hacktivisták**

A folyamatos elemzés révén az ENISA a 2021. évi fenyegetettségi helyzetjelentésben bemutatott főbb fenyegetések mindegyikére vonatkozóan tendenciákat és fontos elemeket állapított meg. Az értékelésben szereplő legfontosabb megállapítások és értékelések több, nyilvánosan elérhető forráson alapulnak, amelyeket a dokumentum kidolgozásához használt hivatkozások tartalmaznak. A jelentés elsősorban a stratégiai döntéshozóknak és a politikai döntéshozóknak szól, azonban a technikai kiberbiztonsági közösség számára is érdekes lehet.



1. A FENYEGETETTSÉGI HELYZET ÁTTEKINTÉSE

Az ENISA fenyegetettségi helyzetjelentése kilencedik kiadásában általános áttekintést nyújt a kiberbiztonsági fenyegetésekről. A fenyegetettségi helyzetjelentés részben stratégiai, részben technikai jellegű, a szakmához értő és nem értő olvasók számára egyaránt releváns információkat tartalmaz. Az idei évi munkát az ENISA újonnan létrehozott, a kiberbiztonsági fenyegetettségi helyzettel foglalkozó ad hoc munkacsoportja támogatta[2]

A 2020-as és 2021-es években a kiberbiztonsági támadások száma tovább növekedett, nemcsak az irányuk és a számuk, hanem a hatásuk tekintetében is. A Covid19 világjárvány - a várakozásoknak megfelelően - szintén hatással volt a kiberbiztonsági fenyegetettségi helyzetre. A Covid19 világjárvány egyik tartósabb fejleménye a hibrid irodai modell felé való tartós elmozdulás. Ezért a világjárványhoz kapcsolódó kiberbiztonsági fenyegetések és az "új normák" kihasználása egyre általánosabbá válik. Ez a tendencia megnövelte a támadási felületet, és ennek következtében emelkedett a szervezeteket és vállalatokat a home office-okon keresztül célzó kibertámadások száma[3]

Általánosságban, a kiberbiztonsági fenyegetettség növekszik. Az egyre növekvő online jelenlét, a hagyományos infrastruktúrák online és felhőalapú megoldásokra való átállása, a fejlett összekapcsolhatóság és a feltörekvő technológiák - például a mesterséges intelligencia (AI) - új jellemzőinek kihasználása miatt[4][5]a kiberbiztonsági környezet fenyegetettsége az egyre kifinomultabb, összetettebb és hatásosabb támadások révén növekedett. Különösen az ellátási láncok fenyegetettsége és azoknak a potenciálisan katasztrofális kaszkádhatások miatti jelentősége a fő fenyegetések között a legmagasabb pozíciót érte el, olyannyira, hogy az ENISA külön fenyegetettségi helyzetet térképezett fel erre a veszélykategóriára.[6]

Meg kell jegyezni, hogy a fenyegetettségi helyzetjelentés ezen iterációjában különös hangsúlyt kapott a különböző ágazatokban jelentkező kiberfenyegetések hatása, beleértve a hálózat- és információbiztonsági irányelvben (NISD) felsoroltakat is. Érdekes betekintést nyerhetünk az egyes ágazatok sajátosságaiból a fenyegetettségi helyzet, valamint a lehetséges kölcsönös függőségek és a lényeges területek tekintetében. Ennek megfelelően az egyes ágazatok fenyegetettségi helyzete további figyelmet érdemel.

Ebben az évben a kiberközösségben a védekezési oldalról, valamint a politikai döntéshozók részéről is történt néhány figyelemre méltó lépés. A globális közösség kezdte felismerni a kommunikáció és az együttműködés fontosságát a kiberbűnözők vizsgálatában és nyomon követésében, különösen azt tekintve, hogy a globális vezetők stratégiai megbeszéléseinek napirendjén a zsarolóvírus (a fenyegetettségi helyzet 2021. évi jelentési időszakának legjelentősebb fenyegetése) kiemelt témává vált.

A 2021. évi fenyegetettségi helyzetjelentés korábbi kiadásainak elkötelezett olvasói észrevehetik a különbséget a feltérképezett elsődleges fenyegetéseket tekintve. Ebben az évben az ENISA tett egy lépést visszafelé, és összevonta a fenyegetések kategóriáit, amellyel az integráció és a hasonló fenyegetések jobb megjelenítése felé mozdult el Ez a fenyegetések megújított taxonómiájára irányuló folyamatos erőfeszítések részét képezi és segítséget nyújt majd a következő évek során a tendenciák módszertani meghatározásában.

A 2021. évi fenyegetettségi helyzetjelentés számos nyílt forráskódú információn és kiberfenyegetettségi hírszerzési forráson alapul. Azonosítja a főbb fenyegetéseket, tendenciákat és megállapításokat, és releváns, magas szintű

[2] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes
[3] IBM – Jelentés az adatvédelmi incidensek költségeiről 2020 - https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
[4] ENISA AI Fenyegetettségi helyzet: https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges
[5] https://www.stealthlabs.com/blog/top-10-cybersecurity-trends-in-2021-and-beyond/
ENISA Az Ellátási láncot érintő támadásokra vonatkozó Fenyegetettségi helyzet, 2021. július https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks[6]

enyhítési stratégiákat kínál. Az ENISA jelenleg a fenyegetettségi helyzetjelentés módszertanának megszilárdításán dolgozik, hogy elősegítse a munka átláthatóságát és következetességét.

1.1. A LEGFŐBB FENYEGETÉSEK

A 2020. és a 2021. évek folyamán számos kiberfenyegetés jelent meg és valósult meg. Az ebben a jelentésben bemutatott elemzés alapján az ENISA 2021. évi fenyegetettségi helyzetjelentése a következő 8 elsődleges fenyegetettségi csoportot azonosítja, és azokra összpontosít (lásd 1. ábra). Ezt a 8 fenyegetéscsoportot a jelentés tárgyidőszakában kiemelkedő jelentőségük, népszerűségük és az ezen fenyegetések materializálódása nyomán fellépő hatásaik miatt emeltük ki.

- **Zsarolószoftverek**
  A zsarolóprogramok olyan rosszindulatú támadások, amelyek során a támadók titkosítják egy szervezet adatait, és a hozzáférés visszaállításáért fizetést követelnek. A zsarolóvírusok a jelentési időszak alatt a fő fenyegetést jelentették, több nagy nyilvánosságot kapott és nagy visszhangot kapott incidenssel. A zsarolóvírus fenyegetések jelentőségét és hatását az Európai Unióban (EU) és világszerte számos kapcsolódó szakpolitikai kezdeményezés is bizonyítja.

- **Rosszindulatú szoftverek**
  A rosszindulatú szoftver olyan szoftver vagy firmware, amelynek célja olyan jogosulatlan folyamat végrehajtása, amely káros hatással van a rendszer titkosságára, integritására vagy rendelkezésre állására. A rosszindulatú szoftverek által jelentett fenyegetést évek óta következetesen magasra értékelték, bár a 2021. évi fenyegetettségi helyzetjelentés jelentési időszakában a mértéke csökkent. Az új kapcsolt technikák alkalmazása és a bűnüldöző közösség néhány jelentős győzelme hatással volt az érintett fenyegető szereplők működésére.

- **Cryptojacking**
  A cryptojacking vagy rejtett kriptovaluta bányászat a kiberbűnözés egy olyan típusa, amikor a bűnöző az áldozat számítási teljesítményét titokban kriptopénz előállítására használja. A kriptovaluták elterjedésével és a nyilvánosság általi egyre szélesebb körben történő használatával a kapcsolódó kiberbiztonsági incidensek számának növekedése figyelhető meg.

- **E-mail üzenetekhez kapcsolódó fenyegetések**
  Az e-mail üzenetekhez kapcsolódó támadások olyan fenyegetések összessége, amelyek az információs rendszerek technikai sebezhetőségei helyett az emberi psziché és a mindennapi szokások gyengeségeit használják ki. Érdekes módon és az ilyen típusú támadások elleni számos figyelemfelkeltő és oktatási kampány ellenére a fenyegetés továbbra is jelentős mértékben fennáll. Különösen az üzleti e-mailek kompromittálása és a pénzbeli haszon szerzésére irányuló fejlett, kifinomult technikák terjednek.

- **Adatok elleni fenyegetések**
  Ebbe a kategóriába tartoznak az adatvédelmi incidensek/szivárgások. Az adatsértés vagy adatszivárgás érzékeny, bizalmas vagy védett adatok megbízhatatlan környezetbe történő kiadását jelenti. Adatsértés kibertámadás, bennfentes munka, nem szándékos adatvesztés vagy adatfeltárás következtében is bekövetkezhet. A fenyegetés továbbra is nagy, mivel az adatokhoz való hozzáférés számos okból, pl. zsarolás, váltságdíj követelése, rágalmazás, félretájékoztatás stb. miatt a támadók elsődleges célpontját jelenti.

- **A rendelkezésre állás és az integritás elleni fenyegetések**
  A rendelkezésre állás és az integritás számos fenyegetés és támadás célpontja, amelyek közül kiemelkedik a szolgáltatásmegtagadás (DoS) és a webes támadások családja. A szigorúan a webalapú támadásokhoz kapcsolódó szolgáltatásmegtagadást eredményező támadások (DDoS) az informatikai rendszereket érintő egyik legkritikusabb fenyegetés, amely az erőforrások kimerítésével a rendelkezésre állásukat célozza meg, és teljesítménycsökkenést, adatvesztést és szolgáltatáskiesést okoz. Ez a fenyegetés következetesen az ENISA fenyegetettségi lista elején szerepel, mind a tényleges incidensekben való megnyilvánulása, mind a potenciálisan nagy hatása miatt.

- **Dezinformáció - félretájékoztatás**
  A dezinformációs és félretájékoztatási kampányok egyre jobban terjednek, amit a közösségi médiaplatformok és az online média fokozott használata, valamint az emberek Covid19 világjárvány miatt megnövekedett online jelenléte is ösztönöz. A fenyegetések e csoportja most jelenik meg először a fenyegetettségi jelentésben; a kibervilágban azonban nagyjelentőségű. A dezinformációs és félretájékoztatási kampányokat gyakran alkalmazzák hibrid támadásokban, hogy így csökkentsék a bizalom általános megítélését, ami a kiberbiztonság mellett szóló egyik fő elem.

- **Nem rosszindulatú fenyegetések**
  A fenyegetéseket általában olyan szándékos és rosszindulatú tevékenységeknek tekintik, amelyeket olyan ellenfelek hajtanak végre, akiket valamely dolog egy adott célpont megtámadására ösztönöz. Ez a kategória olyan fenyegetéseket fed le, amelyeknél a rosszindulatú szándék nem nyilvánvaló. Ezek többnyire emberi hibákon és hibásan kialakított rendszerkonfigurációkon alapulnak, de vonatkozhatnak az informatikai infrastruktúrákat célzó fizikai katasztrófákra is. Szintén a természetüknél fogva ezek a fenyegetések állandóan jelen vannak az éves fenyegetettségi helyzetjelentésben, és a kockázatértékelések során komoly aggodalomra adnak okot

1. ábra: ENISA Fenyegetettségi helyzetjelentés 2021 - Legfőbb fenyegetések

Meg kell jegyezni, hogy a fent említett fenyegetéseket kategóriák szerint gyűjtötték, amelyeket a fent említett nyolc területre vontak össze. A jelentés a fenyegetéscsoportok mindegyikét külön fejezetben elemzi tovább, amely részletesen kifejti az adott csoport sajátosságait, és konkrétabb információkat, megállapításokat, tendenciákat, támadási technikákat és elhárítási vektorokat tartalmaz.

1.2. LEGFŐBB TRENDENCIÁK

Az alábbi lista a jelentési időszak alatt a kiberfenyegetések terén megfigyelt főbb tendenciákat foglalja össze. Ezeket az ENISA 2021-es fenyegetettségi helyzetjelentésének részét képező különböző fejezetekben részletesen is áttekintjük

- Az ENISA ellátási láncra vonatkozó, külön erre a célra létrehozott fenyegetettségi helyzetjelentésében kiemeltek szerint **egyre nagyobb számban merülnek fel rendkívül kifinomult és hatásos ellátási láncot érintő kompromittálások**. **A kezelt szolgáltatók** a kiberbűnözők értékes célpontjaivá váltak.
- **A Covid19 ösztönözte a kiberkémkedést** és **lehetőséget teremtett a kiberbűnözők számára**.
- A kormányzati szervezetek mind nemzeti, mind nemzetközi szinten intenzívebb tevékenységet folytattak. A kormányok részéről fokozott erőfeszítések figyelhetők meg az államilag támogatott fenyegető szereplők megzavarására és az ellenük való jogi fellépésre.
- A **kiberbűnözőket** egyre jobban motiválja tevékenységük pénzre váltása, pl. a zsarolóvírusok. A **kriptovaluta** továbbra is a fenyegető szereplők leggyakoribb kifizetési módszere.
- A kiberbűnözés **egyre nagyobb mértékben célozza meg és érinti a kritikus infrastruktúrákat**.
- A két leggyakoribb **zsarolóvírus-fertőzési vektort** továbbra is az **adathalász e-mailek és a távoli asztali szolgáltatások (RDP) elleni erőszakos támadások jelentik.**
- A **Ransomware as a Service zsarolószoftver szolgáltatásként - RaaS) típusú üzleti modellek** 2021-ben egyre nagyobb hangsúlyt kaptak, ami megnehezíti az egyes fenyegető szereplők megfelelő azonosítását
- A **háromszorosan kényszerítő zsarolóvírus (triple extortion ransomware)** programok előfordulása 2021. folyamán erőteljes emelkedést mutatott.
- **A rosszindulatú programok** A 2020-ban megfigyelhető csökkenése a 2021. év folyamán is folytatódott. A 2021. évben növekedést tapasztaltunk azon fenyegető szereplők körében, akik kódjuk portolásához viszonylag új vagy szokatlan programozási nyelvekhez folyamodtak.
- A **konténerkörnyezeteket célzó rosszindulatú programok**sokkal elterjedtebbé váltak, olyan újszerű fejlesztésekkel, mint a memóriából futtatott fájl nélküli rosszindulatú programok.
- A rosszindulatú programok fejlesztői folyamatosan módot találnak arra, hogy **megnehezítsék a visszafejtést és a dinamikus elemzést**.
- A **cryptojacking fertőzések** száma az előző évekhez képest 2021. első negyedévében**csúcsot döntött**. A cryptojacking alkalmazásával járó **anyagi haszon** a fenyegető szereplőket az ilyen támadások végrehajtására ösztönözte.
- **A kriptobányászat volumene és a cryptojacking tevékenységek 2021-ben rekordot döntöttek.**
- Látható, hogy a **böngészőalapúról a fájlalapú cryptojacking** tevékenységre való áttérés zajlik.
- A **Covid19 továbbra is domináns vonzerőt jelent** a tömeges e-mailes támadásoknál.
- Az **üzleti e-mailek elleni támadások (Business E-mail Compromise, BEC) egyre gyakoribbakká**, kifinomultabbá és célzottabbá váltak.
- Az **adathalászat mint szolgáltatás (Phishing-as-a-Service - PhaaS)** üzleti modell egyre jobban elterjed.
- A fenyegetések szereplői az adatokra és az információkra irányuló fenyegetésekkel összefüggésben a **vakcinainformációk felé** irányították figyelmüket.
- **Az egészségügyi szektorhoz kapcsolódó adatvédelmi incidensek száma megugrott.**
- A tradicionális megosztott szolgáltatásmegtagadás (DDoS - Distributed Denial of Service) új támadások új célpontjai a **mobilhálózatok és az IoT (Internet of Things)**.
- A **zsarolóvirusos szolgáltatásmegtagadás** a szolgáltatásmegtagadásos támadások új területét jelenti.
- **A virtualizált környezetekben az erőforrások megosztása** a DDoS-támadások erősítőjeként működik.
- A **DDoS kampányok** 2021-ben egyre célzottabbá, sokkal tartósabbá és egyre többtényezőssé váltak.
- A **mesterséges intelligencia (AI) által támogatott dezinformáció** segíti a támadókat a támadások végrehajtásában.
- A **dezinformációs támadások középpontjában az adathalászat áll** és erősen kihasználja az emberek hiedelmeit.
- A **félretájékoztatás és a dezinformáció** a kiberbűnözési tevékenységek középpontjában áll és soha nem látott mértékben növekszik.
- **A dezinformáció mint szolgáltatás (Disinformation-as-a-Service (DaaS) üzleti modell** jelentős mértékben növekedett, amit a Covid19 világjárvány erősödő hatása és a több információ iránti igény ösztönöz.
- A 2020. és a 2021. években a**nem rosszindulatú incidensek számának nagyfokú növekedését** figyelhetjük meg, mivel a Covid19 járvány az **emberi hibák** és a **hibás rendszerbeállítások** multiplikátorává vált, egészen addig a pontig, hogy 2020-ban a legtöbb betörést hibák okozták.

- Nagy **ugrás következett be a nemrosszindulatú felhőalapú biztonsági események számában**.

1.3. AZ ELSŐDLEGES VESZÉLYEK UNIÓS KÖZELSÉGE

Az ENISA által feltérképezett fenyegetettségi helyzettel összefüggésben lényeges szempont, hogy a kiberfenyegetés milyen közel van az Európai Unióhoz (EU). Ez különösen fontos ahhoz, hogy segítse az elemzőket a kiberfenyegetések jelentőségének értékelésében, a potenciális fenyegető szereplőkkel és vektorokkal fennálló összefüggések megtalálásában, sőt a megfelelő célzott enyhítő vektorok kiválasztásában is. Az EU közös biztonsági és védelmi politikájához (KBVP) javasolt osztályozással (CSDP) összhangban[7], a kiberfenyegetéseket négy kategóriába soroltuk, amint azt az 1. táblázat szemlélteti

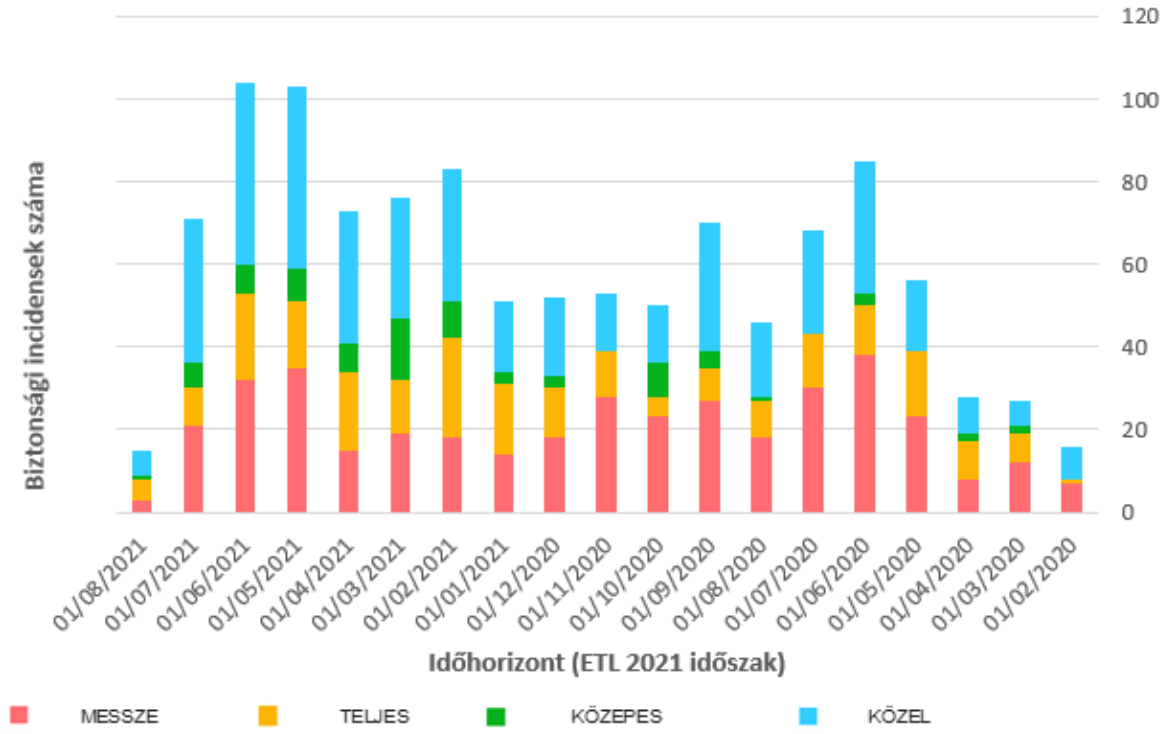
1. táblázat: A kiberfenyegetések közelségének osztályozása

Közelség	Aggodalmak
KÖZEL	Az érintett hálózatokat és rendszereket az EU határain belül ellenőrzik és biztosítják. Az érintett népesség az EU határain belül található.
KÖZEPES	Az EU digitális egységes piacának és a NISD-ágazatoknak a működési célkitűzései szempontjából létfontosságúnak tekintett hálózatok és rendszerek, amelyek ellenőrzése és biztosítása azonban nem uniós intézményi vagy tagállami köz- vagy magánhatóságoktól függ. Az érintett népesség az EU határaihoz közeli területeken található.
TÁVOLI	Az EU digitális egységes piacának és a NISD-ágazatoknak a működési célkitűzései szempontjából létfontosságúnak tekintett hálózatok és rendszerek, amelyek ellenőrzése és biztosítása azonban nem uniós intézményi vagy tagállami köz- vagy magánhatóságoktól függ E hálózatok és rendszerek ellenőrzése és biztosítása túlmutat az uniós intézményi vagy tagállami (tagállami) köz- vagy magánhatóságokon. Az érintett népesség az EU határaitól messze fekvő területeken található.
TELJES	Valamennyi előbb említett terület.

A 2. ábra a 2021. évi fenyegetettségi helyzetjelentésben foglalt elsődleges fenyegetéskategóriákhoz kapcsolódó incidensek idővonalát mutatja be. Meg kell jegyezni, hogy a grafikonon szereplő információk OSINT (nyílt forráskódú hírszerzési adatok) alapján készültek, valamint az ENISA által a helyzetfelismerés területén végzett munkából származnak[8].

[7] https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf
[8] Az EU kiberbiztonsági jogi aktusának 7. cikke (6) bekezdésével összhangban.https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

2. ábra : A fenyegetettségi helyzetjelentés szerinti fenyegetésekhez kapcsolódó főbb megfigyelt események idősíkja (OSINT-alapú helyzetfelismerés) a közelségük szempontjából.



Amint a fenti ábra is mutatja, 2021-ben nagyobb számú incidens történt, mint 2020-ban. Különösen a KÖZELI kategóriában emelkedik folyamatosan az elsődleges fenyegetésekhez kapcsolódó megfigyelt incidensek száma, ami az EU kontextusában betöltött jelentőségükre utal. Nem meglepő módon a havi tendenciák (amelyek a rövidség kedvéért nem szerepelnek az ábrán) meglehetősen hasonlóak a különböző besorolásokat tekintve, mivel a kiberbiztonság nem ismer határokat, és a legtöbb esetben a fenyegetések a proximitás minden szintjén jelentkeznek. Figyelemre méltó, hogy a 2021. évi fenyegetettségi helyzetjelentés által lefedett utolsó hónapokban nagyobb mértékű EU KÖZELI-közelség figyelhető meg, és ezt a tendenciát az ENISA továbbra is figyelemmel fogja kísérni, hogy lássa annak alakulását, és kapcsolódását a fenyegető szereplők tevékenységeihez, valamint a fenyegetések jelenlegi vektoraihoz.

1.4. ÁGAZATONKÉNTI FŐBB FENYEGETÉSEK

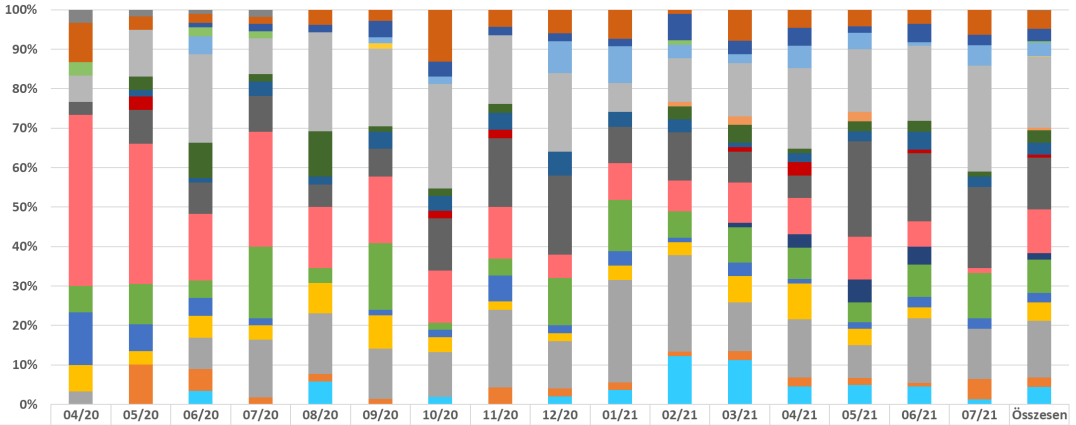
A kiberfenyegetések általában nem egy adott ágazatra korlátozódnak, és a legtöbb esetben több ágazatot is érintenek. Ez valóban így van, mivel a fenyegetések sok esetben a különböző ágazatokban használt IKT-rendszerek sebezhetőségének kihasználása révén jelentkeznek. Ugyanakkor a célzott támadások, valamint az egyes ágazatok kiberbiztonsági fejlettségbeli különbségét kihasználó támadások, illetve egyes ágazatok népszerűsége/dominanciája mind olyan tényezők, amelyeket figyelembe kell venni. E tényezők nyomán a fenyegetések egyes adott ágazatokban incidensek formájában jelentkeznek, és ezért fontos mélyen megvizsgálni a megfigyelt incidensek és fenyegetések ágazati szempontjait. Ezen túlmenően az egyes ágazatokban megfigyelt tendenciák és az ágazatok közötti függőségek olyan megfigyelések, amelyeket egy ilyen elemzésből le lehet vonni.

A 3. és 4. ábra az érintett ágazatokat az OSINT (nyílt forráskódú hírszerzési adatok) alapján megfigyelt incidensek szerint emeli ki az ENISA által a helyzetfelismerés területén végzett munka eredményeként.[9]. Az információk a 2021. évi fenyegetettségi helyzetjelentés elsődleges fenyegetéseivel kapcsolatos incidensekre vonatkoznak. Ez az ENISA első kísérlete arra, hogy feltérképezze a fenyegetések egyes ágazatokra gyakorolt hatását. Az elkövetkező

[9] Az EU kiberbiztonsági jogi aktusának 7. cikke (6) bekezdésével összhangban.https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

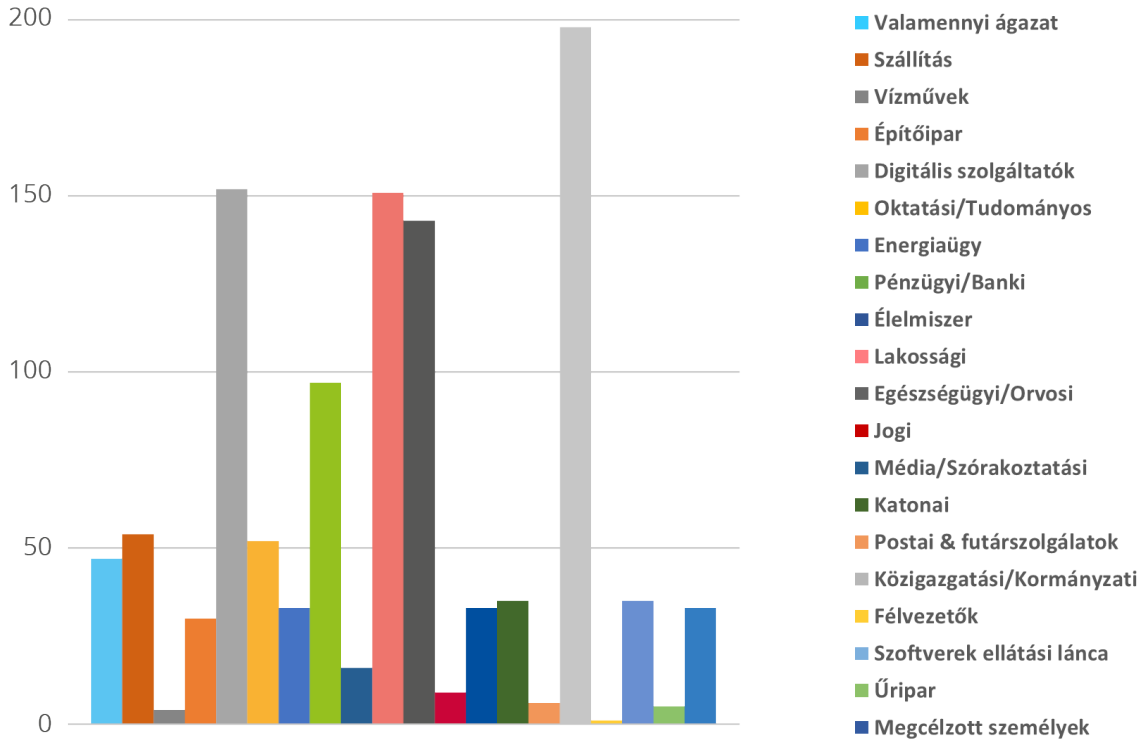
években és a fenyegetettségi térkép jövőbeli iterációiban erőfeszítéseket teszünk arra, hogy az ágazatokat összehangoljuk a hálózat- és információbiztonsági irányelvben (NISD) és az annak felülvizsgálatára irányuló javaslatban (NISD 2.0) felsoroltakkal.

3. ábra: Az fenyegetettségi helyzetjelentés szerinti elsődleges fenyegetésekhez kapcsolódóan megfigyelt incidensek idősíkja az érintett ágazat szempontjából.



	04/20	05/20	06/20	07/20	08/20	09/20	10/20	11/20	12/20	01/21	02/21	03/21	04/21	05/21	06/21	07/21	Összesen
Vízművek	1	1	1	1													2
Szállítás	3	2	2	1	2	2	7	2	3	4	1	7	4	5	4	5	49
Megcélzott személyek			1	1	1	3	2	1	1	1	6	3	4	2	5	2	33
Űripar	1		2	1							1						4
Szoftverek ellátási lánca			4			1	1		4	5	3	2	5	5	1	4	35
Félvezetők						1											1
Közigazgatási/Kormányzati	2	7	20	5	13	14	14	8	10	4	10	12	18	19	21	21	189
Postai & futárszolgálatok											1	2		3			6
Katonai		2	8	1	6	1	1	1			3	4	1	3	3	1	33
Média/Szórakoztatási		1	1	2	1	3	2	2	3	2	3	1	2	3	5	2	32
Jogi		2					1	1				1	3		1		7
Egészségügyi/Orvosi	1	5	7	5	3	5	7	8	10	5	11	7	5	29	19	16	137
Lakossági	13	21	15	16	8	12	7	6	3	5	7	9	8	13	7	1	117
Élelmiszer												1	3	7	5		16
Pénzügyi/Banki	2	6	4	10	2	12	1	2	6	7	6	8	7	6	9	9	89
Energiaügy	4	4	4	1		1	1	3	1	2	1	3	1	2	3	2	25
Oktatási/Tudományos	2	2	5	2	4	6	2	1	1	2	3	6	8	5	3		48
Digitális szolgáltatók	1		7	8	8	9	6	9	6	14	22	11	13	10	18	10	151
Építőipar		6	5	1	1	1		2	1	1	1	2	2	2	1	4	24
Valamennyi ágazat			3		3		1		1	2	11	10	4	6	5	1	47

4. ábra: Az incidensek száma alapján megcélzott ágazatok (2020. április 2021. július között)



Ebben a jelentési időszakban a közigazgatás és a kormányzati és digitális szolgáltatók számos incidens célpontjaként szolgáltak. Ez utóbbi várható volt, tekintettel az ágazat horizontális szolgáltatásnyújtására, és így annak számos más ágazatra gyakorolt hatására. Megfigyeltünk továbbá jelentős számú olyan incidenst is, amelyek a végfelhasználókat, és nem feltétlenül egy adott ágazatot célozták meg. Az egészségügyi ágazatot is jelentős mértékben célba vették, és ez a tevékenység a jelentési időszak utolsó hónapjaiban (2021. május-július) az erősödés jeleit mutatta. Érdekes módon a pénzügyi szektort egész évben hasonló számú incidens érinti. A szoftverek ellátási lánca is megnövekedett számú incidenst mutat 2021. folyamán, ami az ENISA ellátási láncra vonatkozó fenyegetettségi jelentésében is megjelent megfigyelésként.[10].

1.5. MÓDSZERTAN

Az ENISA 2021. évi fenyegetettségi helyzetjelentése a nyílt forrásokból származó, főként stratégiai jellegű információkon és az ENISA saját kiberfenyegetettségi hírszerzési (CTI) képességein alapul, és több ágazatra, technológiára és kontextusra kiterjed. A jelentést törekedtek iparágtól és gyártóktól független módon összeállítani és a szöveg több lábjegyzetben hivatkozik a különböző biztonsági kutatók, biztonsági blogok és a hírmédia cikkeinek munkáira, illetve idézi azokat. Az 2021. évi fenyegetettségi helyzetjelentés időintervalluma 2020. áprilisától 2021. júliusáig tart, és a jelentésben végig „jelentési időszakként" hivatkozunk rá.

Az 2021. évi fenyegetettségi helyzetjelentés összeállításához a következő megközelítést alkalmazták: Az ENISA a vonatkozó időszak alatt a helyzetismeret segítségével összegyűjtötte a nyílt forrásokban megjelenő jelentősebb incidensek listáját. Ez a lista szolgált alapul az elsődleges fenyegetések listájának összeállításához, valamint a jelentésben szereplő számos trend és statisztika forrásanyagául.

Ezt követően az ENISA és külső szakértők mélyreható másodelemzést végeztek a rendelkezésre álló, nyílt forrásokból származó szakirodalomban, például a hírközlő média cikkeiben, szakértői véleményekben, hírszerzési jelentésekben, incidenselemzésekben és biztonsági kutatási jelentésekben. Az ENISA a folyamatos elemzés révén

[10] Az ENISA ellátási láncot érő támadásokra vonatkozó fenyegetettségi helyzetjelentése 2021. július. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

a 2021 évi fenyegetettségi helyzetjelentésben bemutatott főbb fenyegetések mindegyikére vonatkozóan trendeket és lényeges pontokat állapított meg. Az értékelésben szereplő legfontosabb megállapítások és értékelések több, nyilvánosan elérhető forráson alapulnak, amelyeket a dokumentum kidolgozásához használt hivatkozások tartalmaznak.

A jelentésben igyekszünk különbséget tenni a forrásaink által közöltek és a saját értékelésünk között. (Ezt úgy tesszük, hogy kifejezetten a „saját értékelésünk szerint" kifejezést használjuk). Végül, értékeléskor a valószínűséget olyan szavakkal fejezzük ki, amelyek a becsült valószínűséget fejezik ki (pl. valószínű, nagyon valószínű, biztosan)[11].

Ebben a jelentésben a MITRE ATT&CK® keretrendszert[12] használtuk az adott fenyegetés szempontjából releváns támadási taktikák és technikák kiemelésére (lásd az A. mellékletet). Az egyes ATT&CK® taktikák esetében bemutatásra kerülnek a támadó által alkalmazott technikák. Ez elvezethet az alkalmazható ATT&CK enyhítések[13] listájához. A MITRE ATT&CK® egy tudásbázis, az ellenséges taktikáik és technikák közös nyelve, amely valós megfigyeléseken alapul. A MITRE ATT&CK® tudásbázist a magánszektorban, a kormányzati szektorban, valamint a kiberbiztonsági termékek és szolgáltatások közösségében a konkrét fenyegetésmodellek és módszertanok kidolgozásának alapjául használják.

A jelentést az ENISA 2021 áprilisában létrehozott, a kiberfenyegetettségi helyzettel foglalkozó ad hoc munkacsoportja[14] hitelesítette, amely európai és nemzetközi állami- és magánszektorbeli szervezetek szakértőiből áll.

A fenyegetettségi helyzet feltérképezésének jövőbeli fejlesztése érdekében az ENISA jelenleg új módszertan hivatalossá tételén dolgozik, hogy elősegítse az átláthatóságot, és megteremtse a strukturált és jól összehangolt folyamatok alapjait. Ennek során a fenyegetettségek felülvizsgált taxonómiájával együtt a jövőben nyilvánosságra hozzák a fenyegetettségi helyzet feltérképezésének módszertanát.

1.6. A JELENTÉS FELÉPÍTÉSE

Az ENISA 2021. évi fenyegetettségi helyzetjelentése megtartotta a korábbi fenyegetettségi helyzetjelentések szerkezetét, és hasonló struktúrát használ a 2021. évi elsődleges kiberfenyegetések kiemelésére A korábbi iterációk olvasói észrevehetik, hogy a fenyegetettség-kategóriákat a jövőben alkalmazandó új kiberbiztonsági fenyegetés-taxonómia felé való elmozdulással összhangban összevonták.

A jelentés felépítése a következő:

A 2. fejezet a fenyegető szereplőkkel (azaz az államilag támogatott szereplőkkel, a kiberbűnözés szereplőivel, a bérelt hackerekkel és a hacktivistákkal) kapcsolatos tendenciákat vizsgálja).
A **3. fejezet** a zsarolóvírusokkal kapcsolatos főbb megállapításokat, incidenseket és trendeket tárgyalja.
A **4. fejezet** a rosszindulatú szoftverekkel kapcsolatos főbb megállapításokat, incidenseket és trendeket tárgyalja.
Az **5. fejezet** a cryptojacking-gel kapcsolatos főbb megállapításokat, incidenseket és trendeket tárgyalja.
A **6. fejezet** az e-maileket érintő fenyegetésekkel kapcsolatos főbb megállapításokat, incidenseket és trendeket tárgyalja.
A **7.fejezet** az adatokat fenyegető veszélyekkel kapcsolatos főbb megállapításokat, incidenseket és trendeket tárgyalja.
A **8. fejezet** a rendelkezésre állás és az integritás elleni fenyegetésekkel kapcsolatos főbb megállapításokat, incidenseket és trendeket tárgyalja.
A **9. fejezet** kiemeli a hibrid fenyegetések jelentőségét és ismerteti a dezinformációval és félretájékoztatással kapcsolatos főbb megállapításokat, incidenseket és tendenciákat.
A **10. fejezet** a nem rosszindulatú fenyegetésekkel kapcsolatos főbb megállapításokra, incidensekre és trendekre fókuszál.

[11] CIA - A becsült valószínűséget kifejező szavakhttps://www.cia.gov/static/0aae8f84700a256abf63f7aad73b0a7d/Words-of-Estimative-Probability.pdf
[12] MITRE ATT&CK® , https://attack.mitre.org/
[13] https://attack.mitre.org/mitigations/enterprise /
[14] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes

Az **A Melléklet** a MITRE ATT&CK® keretrendszer alapján bemutatja az egyes fenyegetésekhez általánosan használt technikákat.
A **B Melléklet** a jelentési időszak alatt megfigyelt, fenyegetésenként figyelemre méltó incidenseket írja le.