ÓBUDAI EGYETEM

Keleti Károly Gazdasági Kar
Vállalkozásfejlesztés és Infokommunikációs Intézet

SZAKDOLGOZAT

ÓE-KGK
2023

Hallgató neve: **Solti Péter**
Hallgató törzskönyvi száma: **T007175/FI12904/G**

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Óbudai Egyetem
Keleti Károly Gazdasági Kar
Vállalkozásfejlesztés és Infokommunikációs Intézet

SZAKDOLGOZAT FELADATLAP

Hallgató neve: Solti Péter
Szakdolgozat száma: [redacted]
Törzskönyvi száma: T007175/FI12904/G **Neptun kódja:** [redacted]

Szak: Gazdaságinformatikus
Specializáció: Vállalatinformatikai specializáció

A dolgozat címe: A mesterséges intelligencia társadalmi kockázatai
A dolgozat címe angolul: Social risks of artificial intelligence
A feladat részletezése:
1. Mutassa be a mesterséges intelligencia kiberbűnözésre releváns alapjait!
2. Mutassa be a kiberbűnözés aktuális trendjeit!
3. Elemezze a MI kiberbűnözésre gyakorolt közvetlen hatását!
4. Készítsen kvantitatív/kvalitatív előrejelzést a folyamatok közeljövőben várható alakulására!

Intézményi konzulens neve: Horváth Ádám Béla

A kiadott téma elévülési határideje:2024. 12. 15.
Beadási határidő: 2023. 12. 15.

A szakdolgozat: Nem titkos.

Kiadva: Budapest, 2023. 11. 29.

Óbudai Egyetem Keleti Károly Gazdasági Kar Vállalkozásfejlesztés és Infokommunikációs Intézet * 1. Budapest

P.H

.....
Intézetigazgató

A dolgozatot beadásra alkalmasnak találom:

.....
belső konzulens

.....
külső konzulens

ÓBUDAI EGYETEM

Keleti Károly Gazdasági Kar

HALLGATÓI NYILATKOZAT

Alulírott Solti Péter (Neptunkód: [redacted]) hallgató kijelentem, hogy a szakdolgozat saját munkám eredménye, a felhasznált szakirodalmat és eszközöket azonosíthatóan közöltem. Az elkészült szakdolgozatban található eredményeket az egyetem és a feladatot kiíró intézmény saját céljára térítés nélkül felhasználhatja, a titkosításra vonatkozó esetleges megkötések mellett.

Budapest, 2023. 12. 13.

Solti Péter

hallgató aláírása

TARTALOMJEGYZÉK

ÁBRAJEGYZÉK

TÁBLÁZATOK JEGYZÉKE

1. BEVEZETÉS

A mostanában hatalmas teret nyerő és egyre inkább az átlag felhasználó köztudatába is bekerülő Mesterséges Intelligenciának (MI) a társadalmi kockázatai kerülnek ebben a dolgozatban bemutatása, különös tekintettel ezek kiberbűnözési aspektusára.

Felmerül a kérdés, hogy kik ellen valósulhatnak meg, valamint milyen módon befolyásolja ez a bűnözést. Erre próbálok meg választ adni a dolgozatban. A téma bemutatása a következő módon fog zajlani, a bevezetést követő fejezetben a Mesterséges Intelligencia kiberbűnözési oldalának egyénekre gyakorolt hatása lesz a középpontban, bemutatásra kerülnek a leggyakrabban alkalmazott bűncselekmények és ezeknek az MI-vel módosított, még hatékonyabbá tett változatai. Ezt követően a vállalatokra gyakorolt negatív hatások kerülnek felsorolásra, egy kisebb betekintéssel a hazai információbiztonsági világba, mert ezzel tisztább képet kapunk az egész helyzetről, majd a szervezetekre jellemző Mesterséges Intelligenciával kisegített esetek lesznek bemutatva. Lezárás képpen pedig a védekezésről lesz szó, mit lehet tenni ellene, mit lehet tenni általánosságban a nagyobb biztonságért és hogy ez az új technológia hogyan tud a védekező oldalon is segíteni.

Elsősorban elengedhetetlen, hogy a témához szorosan kapcsolódó szakirodalmi fogalmak mindenekelőtt tisztázásra kerüljenek. Az IT világában az utóbbi időben egyre gyakrabban használt kifejezés, az Artificial Intelligence már sok ember számára ismert lehet, de mit is értenek ez alatt? Kezdjük a legelején, amin az egész információs társadalom alapszik, az az adat, minden erre az egy dologra épít. Két nagy csoportra osztjuk őket, a strukturált és a strukturálatlan adatra. Az előbbi már szűrt állapotban van, egy adatmodell formai követelményeit követi, adatbázisokban kerül tárolásra, ezzel szemben a strukturálatlan adathalmaz, pedig bármilyen formában lehet, képek, videók, hangok, alkalmazások log archívumai. Ezeket először egységes, leginkább szöveges formára kell átalakítani az egyszerűbb elemzés érdekében. Miután elérhetőek számunkra az adatok, ezekből információt kell kiszűrni, itt lép a képbe a Data Mining és a Data Science.

Data Mining	Data Science
• Bármilyen formátumú adat • Előrejelzés • Rejtett kapcsolatok feltárása • Nagy adatbázisokkal dolgozik • Felhasználási terület: Vásárlói viselkedés elemzés, betegségek ok-okozati összefüggésének kimutatása	• Csak strukturált adat • Biznisz analízis • Statisztikai algoritmusok használata • Csak a kiválogatott hasznos adattal dolgozik • Felhasználási terület: Célzott reklám, logisztikai döntéshozatal

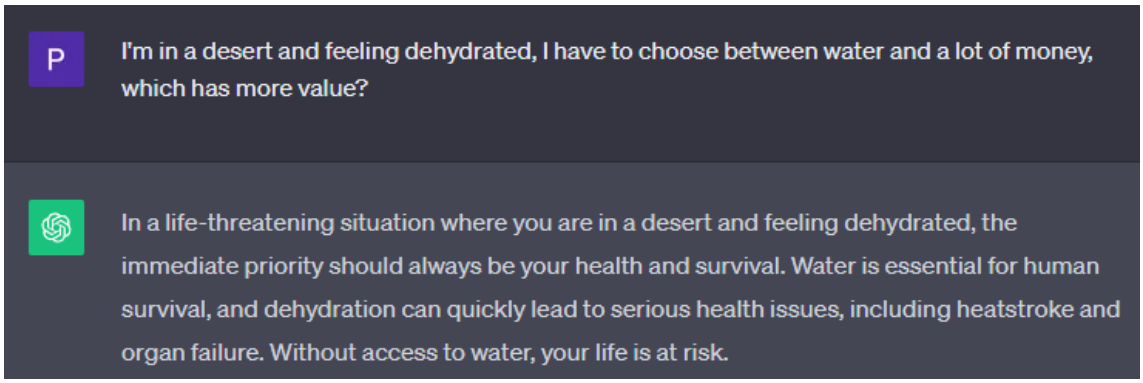
1. táblázat: Data Mining és Data Science összehasonlítása

Forrás: https://shorturl.at/cehwN

Ezeknek az adatoknak a feldolgozása régebben kizárólag ember által történt, de a mai világban már a segítségükre van a Mesterséges Intelligencia. Három nagy rész épül egymásra a gyakorlatban a következő sorrendben:

1. Deep Learning,
2. Machine Learning,
3. Artificial Intelligence.

Legkisebb eleme a Deep Learning, amely elemzi a dolgokat mesterséges neurális hálózat segítségével és ezáltal lesz képes például képet vagy beszédet felismerni. Ezt követi a Machine Learning, (gépi tanulás) ennek feladata tanulni az adatokból, statisztikai algoritmusokat használ, annak érdekében, hogy a gép a következő alkalommal egy hasonló feladatot már rövidebb idő alatt, hatékonyabban tudjon elvégezni. Erre épül rá az Artificial Intelligence, neki köszönhető a számunkra is könnyen értelmezhető kimenet, emberszerűen próbálja meg megoldani a problémákat, nem leegyszerűsített igen vagy nem megoldásokat kínál, hanem kontextusba helyezve tud válaszokat adni. Például, ha a sivatagban lennénk és pénz vagy víz közül kell választani, a vizet fogja ajánlani, holott a pénznek nagyobb értéke van. (ZekiahTech, 2019)



1. ábra: ChatGPT működésének szemléltetése
Forrás: www.chat.openai.com

Habár a kiberbűnözés lesz a fő irány, de emellett, számos más kockázata is lehet ennek az új technológiának, ezek csak az átszellemülés jegyében kerülnek rövid bemutatásra, hogy lássuk milyen sokoldalú dologról van szó.

A későbbiekben akár leválthatja a telefonos tudakozók, chatbotok vagy call-centerekben dolgozó humán munkaerőt. Az egyre fejlődő nyelvi modellek betaníthatóak specifikusan a vállalat igényeire szabva, megismertetik velük a termékeket, a szolgáltatásokat és utána tudnak válaszolni a vásárlók kérdésire. Ettől, ha még távolabb tekintünk, el tudjuk képzelni, hogy egy állásra való interjúztatást egy Mesterséges Intelligencia fog végig vinni. Analizálja a szókincset, szóhasználatot, a technikai kérdésekre adott válaszok pontosságát, az interjúzó delikvens hangjának változását és kamera segítségével tudja figyelni a mimikát. Ezt követően ebből riportot generálhat az adatok elemzése után. Jelenleg azt lehet mondani, hogy ez egy inhumánus megoldás lenne, de ahogy változik a világ új normák alakulnak ki és régi normák lesznek elfogadhatatlanok, honnan tudhatnánk, hogy milyen jövő vár erre az apró részletre. Nagy előnye lenni, hogy nincs véleménye a rendszernek, a tényeket fogja csak alapul venni és mindig rendelkezésre áll, nincs betegég, nincs hirtelen közbe jött vészhelyzet, ami miatt elnapolásra kerülni az esemény. Ezen felül pedig nem kell külön időpontokat szervezni a meghallgatottaknak, azonos időben valamennyi jelentkező lehetőséget tud kapni az interjúra. Hasonló helyzet képzelhető el az onboarding folyamatával kapcsolatban, amikor a már felvett új

munkaerőt kell elnavigálni a helyi céges világban és az ahhoz tartozó struktúrában. (WITSEC Szakmai nap, 2023)

A Mesterséges Intelligencia Kínában már jelenleg is használatban van megfigyelő rendszerek formájában, a világ térfigyelőkameráinak fele itt található, ez megszámlálhatatlan lehetőséget nyújt az államnak a társadalom elemzésére, kisebbségi csoportokat figyelnek meg, folyamatos arcfelismerés megy, adatbázisban tárolják, milyen autója van az illetőnek, kik a barátai, milyen öltözéket visel. (The New York Times, 2022)

A kiberbűnözés az egyik leggyorsabban növekvő bűnelkövetési módszer az utóbbi időben. A THE HILL című online lapra hivatkozva, 2020-ban a pandémiás időszak kezdete után az amerikai Szövetségi Nyomozóiroda (FBI) internetes bűncselekményekért felelős panaszközpontja szerint napi 3000-4000 panaszbejelentés történik. Mindez egy jelentős ugrás a COVID-19 előtti napi 1000 esethez képtest. Tonya Ugoretz, az FBI kibervédelmi részlegének helyettes asszisztens igazgatója szerint a megnövekedett otthoni munkavégzés párhuzamosan növelte a cégek sebezhetőségét is. (Maggie Miller, 2020)

Azonban a lehetséges negatív felhasználás mellett számtalan pozitív oldala is van ennek az újításnak. Segítséget nyújt az orvoslásban, a megfelelő kérdések feltevésével szűkíteni tudja a betegségek körét. Redukálni tudja az emberi hibák számát különböző folyamatokban, a gép nem lesz fáradt vagy figyelmetlen, mindig maximálisan teljesít. A háztartásokban is segítségünkre tud lenni, az okos házak képesek maguktól állítani a hőmérsékletet az ember szokásához igazodva, becsukják az ablakot, ha elkezd esni vagy a hűtő tud rendelni ételt, ha már látja, hogy valami elfogyott.

De minek köszönhető ez a hirtelen robbanásszerű terjedése a Mesterséges Intelligenciának? (CloudFactory, 2017)

- egyik eleme a számítási kapacitás növekedése, a 2010-es évektől kezdődően évről évre jöttek a technológiai újítások, itt számunkra most leginkább a Központi Feldolgozó Egység (CPU) fejlődése a meghatározó. A Google 2016-ban kifejlesztette a Tensor Processing Unitot (TPU), melyet kifejezetten a Machine Learning és neurális hálozatok területén használnak, (Deepgram, 2023)
- az adatok sokszorozódása játszik még kulcs szerepet, 2010 óta az adatok mennyisége is rohamosan növekszik, egyre több kamera van a világban, mobiltelefonokban, térfigyelésnél, autókban, minden szenzorokkal, érzékelőkkel van tele. Ennek megkerülhetetlen következménye az adatok számának növekedése,
- az algoritmusok javulása az adatok növekedésének közvetett kimenete volt. Ezelőtt az algoritmusok csak megmondták a számítógépnek, hogy mit csináljanak, de most már a tömérdek adat elemzésre kerül a Machine Learning segítségével és a számítógépek saját magukat tudják tanítani, melynek köszönhetően folyamatosan fejlődnek. Emlékeznek már régebben felfedezett mintákra és ezeket újra felhasználva hatékonyabban hajtanak végre egy-egy feladatot. Példaként gondoljunk az önvezető autókra, régen csináltak egy prototípust és az egyedül gyűjtött adatot, csak egymaga fényképezte le a táblákat, egy adott környéken, amit utána megnéztek és aszerint pontosították a működését. Manapság már számtalan darab autó kamera képéből nyernek ki vizuális adatot a különböző útjelzésekről és tanítják vele az algoritmust, hogy egy táblát fel kell ismerni a programnak sötétben is, akkor is, ha tükröződik, ha máshogy verődik rá a fény. Ezeket csekély mennyiségű adatszolgáltató eszközzel exponenciálisan több ideig tartana megtanítani a rendszernek.

2. A MESTERSÉGES INTELLIGENCIA KOCKÁZATAI EGYÉNEKRE NÉZVE

2.1.1. Személyazonosság-lopás

Egy régóta fennálló bűncselekmény fajta, másnak adják ki magukat, mint akik igazából. Valamilyen úton szert tesz a bűnöző személyes adatokra, Társadalombiztosítási Adóazonosító Jelre (TAJ szám), személyi igazolvány számra, banki adatokra, jelszavakra. Több fajtáját különböztethetjük meg ezeknek a bűncselekménynek: (EQUIFAX, 2023)

- büntetőjogi személyazonosság-lopás,
- pénzügyi személyazonosság-lopás,
- személyazonosság másolás,
- egészségügyi személyazonosság-lopás,
- gyermek személyazonosság-lopás.

Követhetnek el bűntényt, ami miatt utána minket keres a rendőrség, adóvisszatérítést kérnek a nevünkben, személyazonosság másolásnál megszerzik valakinek a névjegyét és annak a személynek a nevében élnek vissza jogaikkal, például egy internetszolgáltatónak az embereiként mennek be házakba esetlegesen, egészségügyi szolgáltatást vesznek igénybe a TAJ szám eltulajdonításával. A gyermekek személyazonosságának ellopása inkább az Amerikai Egyesült Államokban terjedt el, azért, mert tőlünk eltérően ők akkor kapnak kedvező hitelt, hogyha a hitel kártyájukat időben egyenlítik ki vagy a további hitelüket mindig pontosan törlesztik, ezért egy fiatalkorúnak a hiteltörténete mindig makulátlan lesz. Küldenek egy emailt egy nyereményről, amihez „csak” meg kell adni pár adatot és ha valaki körültekintés nélkül elhiszi már meg is történt a baj. Általánosságban elmondható ezekről a bűncselekményekről, hogy gyakran hosszú ideig ki sem derül a probléma megléte, egyszer csak idézést kapunk a rendőrségre vagy bemegyünk a bankba és nem tudunk hitelt felvenni. (Eszteri & István, 2016)

Ezek a régimódi változatai a személyiség-lopásnak, viszont a Mesterséges Intelligenciának köszönhetően megszületett az úgynevezett Deepfake, ez az új kifejezés egy szóösszetételből született meg, a deep learning és a fake (hamis) szavakból. Célja egy olyan valósághű átverés, ahol audiovizuális eszközök segítségével próbálnak meg elhitetni velünk hamis információkat. Legszélsőségesebb esetben már egy majdnem bármilyen videóra, amin egy ember valami cselekményt végez rá tud kerülni bárkinek az arca.

A „Hiszem, ha látom" és ehhez hasonló mondások, melyek arra utalnak, hogy bizony csak azt hisszük el, amit saját magunk megtapasztalunk, előfordulhat, hogy a jövőben már érvényüket veszítik. Akár teljesen laikusok vagyunk, akár van némi hozzáértésünk és tapasztalatunk e téren, egyre nehezebben tudjuk megítélni a valóság és a mesterségesen létrehozott képek, videók közötti különbséget. Régen egyszerű volt a szemünknek hinni, ezért is terjedtek el és kerültek be a köztudatba ezek a mondások, de mára ez megváltozott.

A Deepfake-ek természetükből adódóan nem váltják ki a már meglévő bűncselekmények összes fajtáját, de néhány területen különösen jól felhasználhatónak bizonyulnak. Elsősorban a személyazonosság másolása az a terület, ahol összpontosul ennek a hátránya. Gyakori szempont ilyen esetben az emberek lejáratása, gyermekek arcának rá helyezése pornográfikus tartalmakra, hírességek lejáratása valótlan szexuális tartalmak készítésével, volt partner megszégyenítése hamis képek terjesztésével. Más esetekben előfordulhat szimpla rémhírkeltés, félrevezetés. A legkiválóbb célpontok a politikusok, mert végtelen nagy mennyiségű videóanyag áll rendelkezésünkre, gyakran ugyan abból a szögből, mindig jó megvilágítással, a pulpitusnál állva, itt a kép elemző szoftvernek nem kell sok különböző szöget, árnyékot elemzeni, majd mesterségesen létrehozni. A dezinformálás ellehetetlenítheti a demokratikus működést, nem lehet kiállni ügyek mellett, mert hitelességét veszíti bárki, ahogy feltűnik róla egy videó. Jelenleg nem ilyen súlyos a helyzet, szakértők megtudják állapítani a videók eredetiségét, de a fejlődési ütemet tekintve elkerülhetetlen lesz ezek megjelenése.

2.1.2. Alkalmazott technológiák

2. ábra: A Video Rewrite működése

Forrás: https://youtu.be/5ymelRjHIfI?si=N6mgLTLS-lkm8XZe

Az első mérföldkő ezeknek a videóknak a készítésében az 1997-ben megjelent Video Rewrite program volt, amit Christoph Bregler, Michele Covell, Malcolm Slaney készített. Ez arra volt képes, hogy egy meglévő videót elemezzen, majd egy másik hangsávot használva módosítsa a videón beszélő ember szájának a mozgását, artikulálását, állkapocspozícióját, annak érdekében, hogy egy valósághű videó jöjjön létre. A program elemzi a videón látottakat, majd eltárolja, hogy egyes szavak, hangok kiadásakor milyen mozgást végez a száj, ezt követően beszédfelismerést futtatnak a hangsávon és automatikusan kiválasztásra, aztán összefűzésre kerülnek a megfelelő szájmozgások. Végezetül ez felkerül az eredeti videóra. (Christoph Bregler, 1997)

A következő mérföldkő jellegű anyag alanya a már leköszönt amerikai elnök Barack Obama volt, a projectet a SIGGRAPH 2017-ben rendezett konferenciáján mutatták be Synthesizing Obama: Learning Lip Sync from Audio címmel. Supasorn Suwajanakorn, Steven M. Seitz és Ira Kemelmacher-Shlizerman munkája már jóval megtévesztőbb

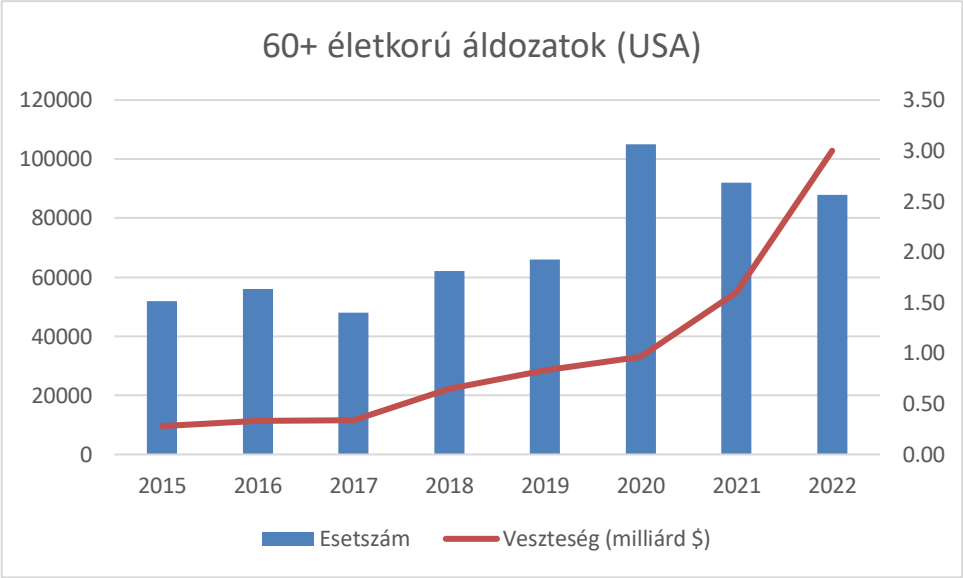
videóanyagot gyártott, a metódus náluk is hasonló volt, a fellelhető dokumentumokban említést is tettek az 1997-es Video Rewrite programról. (Supasorn Suwajanakorn, 2017)

Említésre méltó hasonló technológia ezen a téren az Adobe beszédgeneráló alkalmazása, az Adobe VoCo, melyet 2016 novemberében mutattak be az Adobe Max eseményen, ez egy évente megrendezésre kerülő kreatív konferencia, ahol az ő általuk létrehozott új, innovatív megoldásokat mutatják be a szakmabelieknek, 2017-ben 12000 ember vett rajta részt. A program képes az alany 20 percnyi beszédéből további tetszőleges szavakat valósághű hangszínnel generálni. A vállalat azt állította, csökkenthető majd vele a hanggyártás költsége, de végül csak egy kutatási prototípus maradt.

2.1.3. Felhasználás

Tehát elméletben mindenki rendelkezésére áll ugyan az a technológia, de ki mire fogja használni? A bemutatott lehetőségek közül mindennek meg lehet találni a jó és a rossz oldalát egyaránt, ebben a dolgozatban mi most a rossz oldalt vizsgáljuk leginkább. Akiket a bűnözők először célba fognak venni, mint magánszemélyek, ők a társadalom idősebb résztvevői lesznek. Biztos sokak tudomására jutott, hogy milyen átverésekkel próbálkoznak időnként emberek. Különböző furfangos módokon próbálnak pénzt kicsalni nyugdíjasoktól. Mivel teljesen más technológiai korban szocializálódtak, megszokott módon hisznek szemüknek vagy fülüknek és mint mindenki más, bármit megtennének, hogy szerettüket biztonságban tudják, nem is gondolnak arra, hogy teljesen valótlan helyzettel állhatnak szembe, ezért képzik ők a tökéletes célpontot.

Kapnak egy videót, egy telefonhívást, amiben úgy gondolják, az ő hozzátartozójuk található és segítségre szorul, nem is kell több, ilyen helyzetben a pánik és a veszély, hogy elveszíti a másik embert gyakran irracionális dolgokra késztetheti, emellé még jön a siettetés, nehogy át tudja gondolni a reálisságát az információnak. Elmondják, hogy sürgősen pénzre van szüksége és majd egy ismerős elmegy hozzá a pénzért, csak készítse elő. Bizonyára többen ismerjük a folytatását a történetnek, az összespórolt pénz hirtelen semmissé válik egy kreált, mesterséges szituáció miatt. Egyszer aztán csörög a telefon újra és az a bizonyos ismerős az, aki mit sem tudott a történtekről, most értesül róla, hogy az aggódó hozzátartozója átverés áldozatává vált.



3. ábra: A 60 fölötti áldozatok vizualizációja

Forrás: https://www.ic3.gov/Home/AnnualReports

A fenti ábra a Szövetségi Nyomozóiroda évente kiadott IC3 riportja alapján készült, ami az internetes bűntény panaszbejelentő központ adatait tartalmazza és az amerikában elkövetett kiberbűncselekményekről szól. Az első példa az esetszámok és az okozott kár értékét hivatott jelezni, kék színű oszlop a károsultak száma, narancssárga folyamatos vonal pedig a veszteség mértéke milliárd dollárban kifejezve. Fontos megjegyezni, hogy ez csak a megjelölt korcsoportról beszél, de minden őket érintő internetes bűncselekményt összegezve. A személyiséglopási statisztikákról később esik szó. A diagrammon megfigyelhetjük, hogy 2015-től egészen 2022-ig bezárólag évente hány 60. életévét betöltött ember esik áldozatául az internetes átveréseknek. Ha felidézzük, hogy a 2019-es évben jelent meg a koronavírus, akkor észrevehetjük, hogy az ezt követő években jelentősen megnőtt eme bűncselekmények száma. 2019-et követően a körülbelül 66000 áldozatból egy év leforgása alatt csaknem 105000 áldozat lett, ez majdnem 160%-a az előző évnek. A következő évben ez a szám már csökkent és a 2022-es évre is megtartotta ezt a tendenciát, feltehetően sokan kezdték el hirtelen tanácsokkal ellátni idősebb rokonaikat, ismerőseiket és az oszlopokat nézve ezek értő fülekre találtak, mert javult a helyzet ilyen téren.

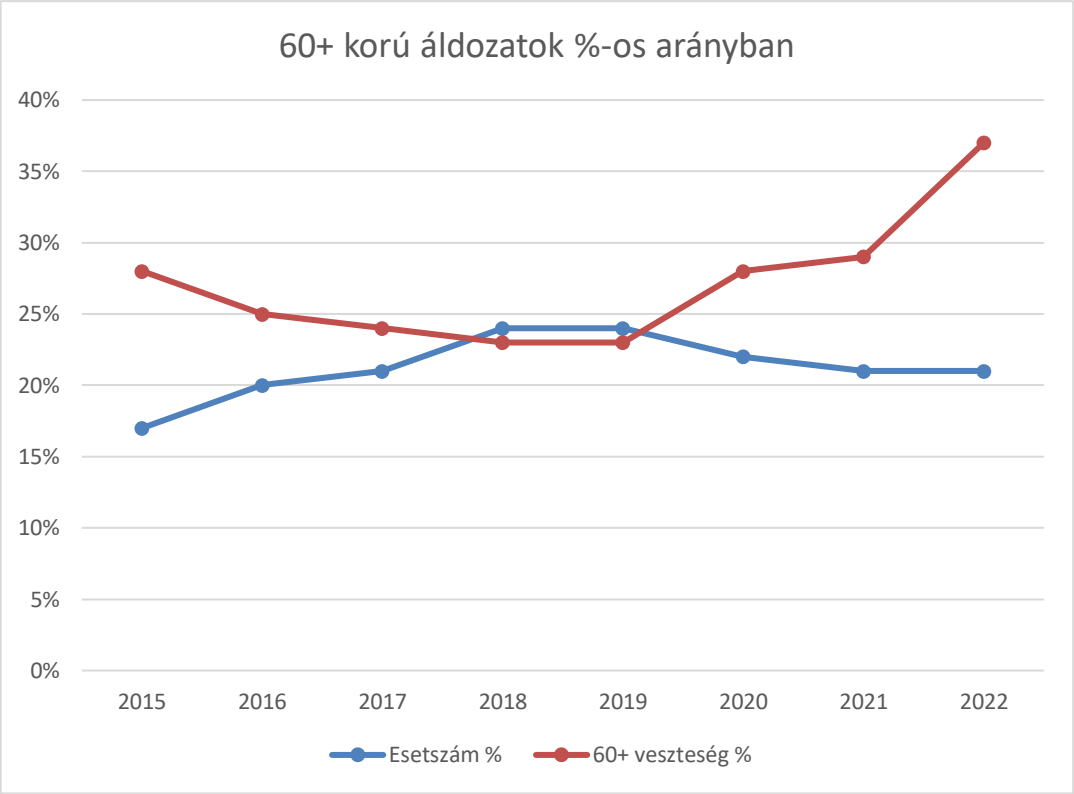
A veszteség értékének skáláját nézve a kiugrás nem a koronavírus kezdetén történt, sokkal inkább ennek a vége felé haladva. A vírus kezdetén lévő esetszám növekedést véleményem szerint a pénzbeli veszteség azért nem követi, mert a bezártságnak köszönhetően olyanok is elkezdtek ezzel próbálkozni, akik azelőtt egyáltalán nem az interneten tényked tek és teljesen kezdőként próbálkoztak. Ennek köszönhetően sok kis értékben elkövetett csalás történt, ami 2019-ről 2020-ra emelte az esetszámokat, de a veszteség összegét kevésé. Azonban a 2020-as évvel kezdődően jelentősen megváltozott a helyzet az esetek és a veszteség kapcsolatának tekintetében (Internet Crime Complaint Center, 2022):

Államokbeli 60+ korcsoport	2020	2021	2022
Áldozatok (darab)	105 301	92 371	88 262
Átlagos veszteség (Dollár)	9 175	18 246	35 101
Több mint 100 000 Dollár veszteséget elszenvedők (darab)	1 921	3133	5456

2. táblázat: Jelentős összeget meghaladó veszteségek száma

Forrás: saját szerkesztés a https://www.ic3.gov/Home/AnnualReports alapján

Itt is megfigyelhetjük, hogy három egymást követő évben végig csökkent az áldozatok száma, ennek ellenére a diagramra vissza emlékezve tudjuk, hogy az elvesztett pénzösszeg jelentősen nőtt évről évre. A 2021-es évre az előző évhez képest a duplájára nőtt az átlagos veszteség, majd a 2022-es évre ugyancsak a duplájára emelkedett az összeg, emellett a 100000 Dollár feletti bűncselekmények száma is fokozatosan emelkedett.

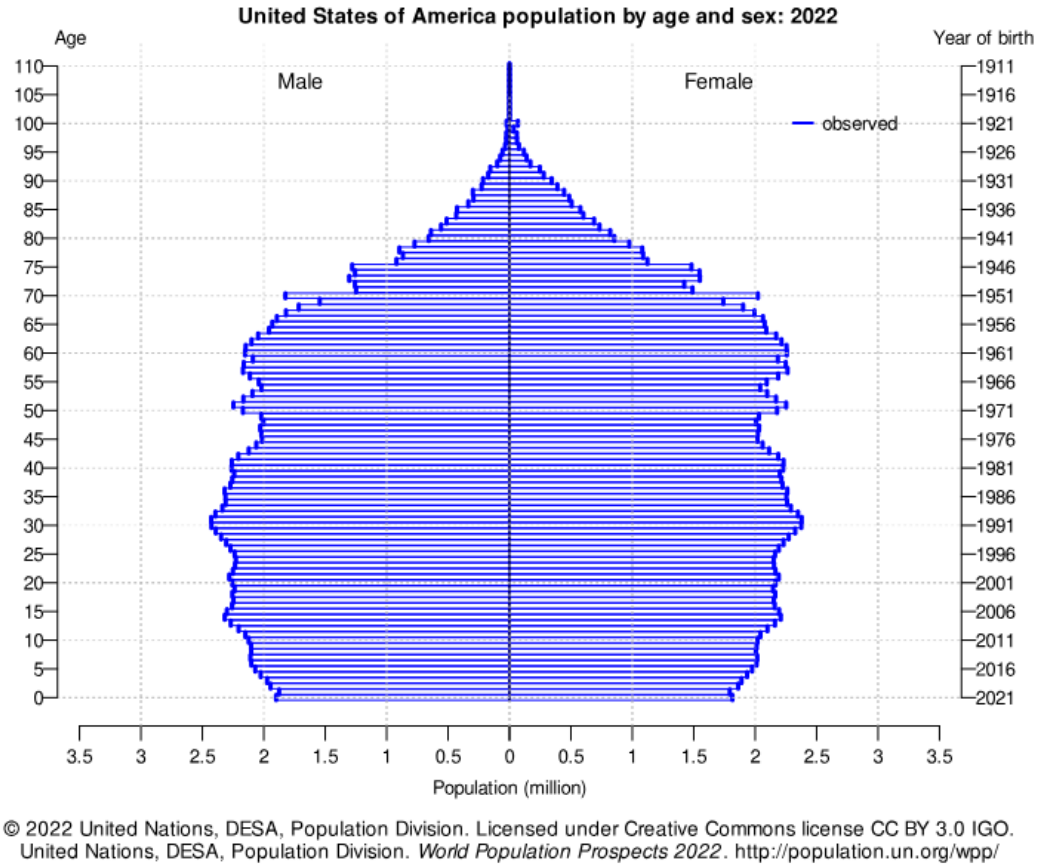


4. ábra: 60+ korú károsultak aránya a teljes sokaságra vetítve

Forrás: saját szerkesztés a https://www.ic3.gov/Home/AnnualReports alapján

Amennyiben korcsoportokat emelünk ki a sokaságból, akkor kötelességünk ezt hasonlítani a teljes sokasághoz, hogy mindenki számára tisztázzuk a teljes képet. Ugyancsak az IC3 jelentésekből derülnek ki a fent szemléltetett adatok, általánosságban elmondható, hogy az elveszített pénz nagyobb részét teszi ki a teljes egésznek, mint a megkárosított emberek száma, magyarul, habár lakosság arányosan kevés 60 fölötti korú embert esik áldozatául az elkövetőknek, ez mégis jelentős pénzveszteséget jelent. A 2022-es évben volt a legdrasztikusabb a különbség, ekkor a korosztály a megkárosítottak 21%-át tette ki, elvesztett érték tekintetében ez mégis 37% volt, ez pénzben kifejezve 3 milliárd Dollárt jelentett.

Annak érdekében, hogy még teljesebb képet kapjunk a korcsoportról meg kell tekintenünk egy demográfiai ábrát, a korfát:

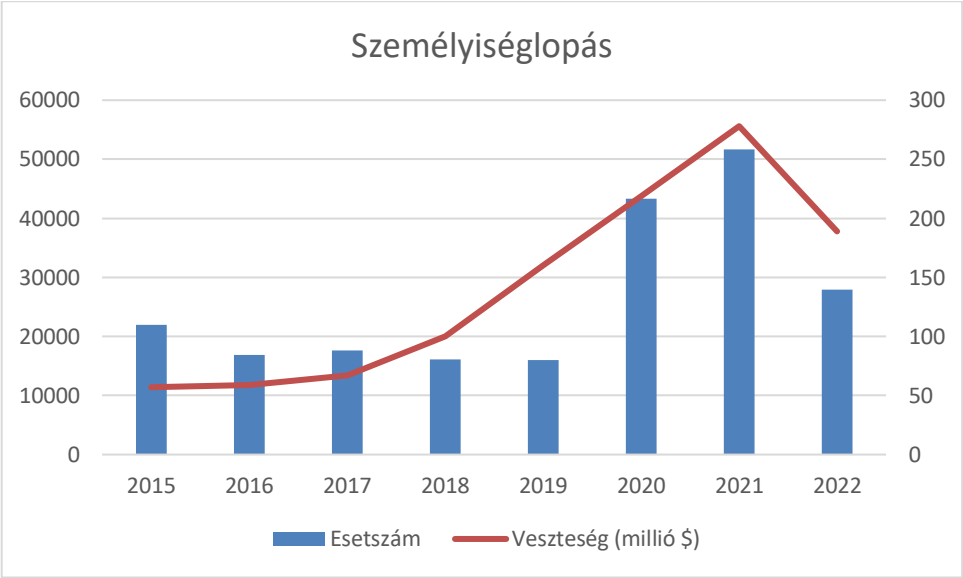


5. ábra: Korfa (2022)

Forrás: https://population.un.org/wpp/Graphs/DemographicProfiles/Pyramid/840

Számolnunk sem kell, szemmel látható, hogy a 60. évet követően drasztikusan csökken a lakosság száma. Ha pontosabb adatokat akarunk, akkor nagy közelítéssel a táblázat területét figyelve az állapítható meg, hogy a 65 fölötti lakosság a 10-100 korcsoportot nézve 21%, a 10-65 közötti pedig 79%. Ezt tudva még szembe ötlőbb az eredmény, hogy a lakosság 21%-ából kerül ki az internetes veszteség 37%-a.

A korosztályi kitekintés után maga a személyiséglopás statisztikái is érdekesek lesznek számunkra:



6. ábra: Személyiséglopási adatok

Forrás: saját szerkesztés a https://www.ic3.gov/Home/AnnualReports alapján

A diagram felépítése a megszokott módon alakul, az esetszám és az elveszített vagyon kapcsolatát mutatja. A vírus miatti bezártság hatása minden egyes ábrán látható lesz, bármi féle internettel kapcsolatos adatot nézünk, a személyiséglopás esetében viszont ez az időszak számottevőbb volt, a betegség elterjedését követő évre duplájára emelkedett az elkövetett személyiséglopások száma.

2.1.4. Adathalászat

Az adathalászat internet korában teret nyerő, leginkább csak a virtuális térben elkövetett bűncselekmény fajta. Célja az érzékeny adatokhoz való hozzájutás, például felhasználó név, jelszó párosok illetéktelen megszerzése. Igazán összeszedett definíciót nehezen találunk, köszönhetően a folyamatos változásnak és fejlődésnek a tevékenység keretein belül. Az elkövetés típusa alapján való csoportosítás a következő: (FORTINET, 2023)

- e-mail, biztosan mindenki kapott már gyanús e-mail címről levelet, az elkövető hozzájut egy adatbázis emailcímeihez és azok mindegyikére elküldi tömegesen az e-mailt. Egyik streaming szolgáltatónknak adja ki magát, annak reményében, hogy beírjuk adatainkat, utána ezt a dark web-en (sötét web, internet azon oldala, amit a szokásos keresőmotorok, mint például Google nem ér el) eladásra kínálják,
- szigonyozás, itt a másik fél személyes adatokat tud meg a felhasználóról és külön neki írja a levelet, személyesen neki szól. Általában könyvvizsgáló vagy auditáló vállalat dolgozóit célozzák, mert ők számos hasznos adathoz hozzáférhetnek,
- klónozás, megszereznek egy korábban elküldött e-mailt a címzettek e-mail-címeivel együtt, majd az ebben található linket vagy fájlt egy rosszindulatú verzióra változtatják és elküldik az összes címre, arra hivatkozva, hogy ez egy frissített verzió az előzőhöz képest,
- hangalapú, felhívják az illetőt, mert a bankszámlájával valami baj történt és fel kell hívjon egy telefonszámot, amit a bűnöző kontrollál és ráveszik, hogy adja meg az adatait a számlája biztonsága érdekében,
- SMS alapú, hasonlít az e-maileshez, fel kell venni a kapcsolatot egy bizonyos emailcímmel, ahol adatot próbálnak meg kicsalni az emberből,
- oldal eltérítés, az elkövető hozzáférést szerez egy oldalhoz, amit módosít és rossz indulatú oldalakra jutunk tovább a linkekkel. Más esetben exploit kitekre irányít át, melyek maguktól települnek a gépünkre.

Az elkövetés típusán kívül még módszerek alapján tudjuk őket kategorizálni: (A Aleroud & L Zhou, 2017):

- link manipulálás, a webhely URL címe hasonlítani próbál egy sokak által jól ismert oldaléra, vegyük példának az *otpbank.hu* című weboldalt, ami az OTP Bank Nyrt. tulajdonában van, lemásolják az oldal működését, hogy hihető legyen, amikor ott vagyunk és az URL címet pedig *otp-bank.hu*-ra változtatják, ez ha nem járunk nap mint nap az oldalon nem fog megmaradni az emlékeinkben, hogy itt nincs kötőjel a címben, a hamis oldalra lépünk és megpróbálunk bejelentkezni, melynek során megadjuk banki adatainkat, egy másik manipulálási módszer, a betűk felcserélése egy hozzájuk közel azonosan kinézővel, nagy i betű (I) kicserélése l betűre vagy fordítva, valamint más nyelvek betűkészletében megtalálható hasonló betűk átemelése,
- szűrők kikerülése, szöveg helyett képek megjelenítése, így a kezdetleges automatikus ellenőrzést képesek kijátszani, fejlettebb szűrők már tudnak képről betűket és szöveget felismerni, így ez nem minden esetben működik sikeresen,
- pszichológiai manipuláció, különböző trükkökkel próbálnak meg az üzenetben rávenni minket arra, hogy beírjuk az adatainkat, ha nem cselekszünk elég gyorsan ez és ez fog történni a bankszámlánkkal, biztos találkoztunk már olyannal, ahol egy akció csak egy bizonyos ideig él, ez is ide a manipulálás címszó alá tartozik, csak ott – általában – nem lopják el az adatainkat.

2.1.5. Alkalmazott technológiák

Általánosságban véve az adathalászat inkább mennyiségi, mintsem minőségi alapokon fekszik. Számtalan próbálkozásból sikerül néhány. A sikerek alacsony száma köszönhető egy részben a szűrőknek, másrészben a célpont figyelmességének, valamint ha Magyarországot vesszük példának, akkor harmadrészben annak, hogy sokszor ezek a támadások ázsiai országokból érkeznek és a magyarra való fordítás a nyelvünk nehézsége miatt problémákat okoz a készítőknek. Emellett a mennyiségi hozzáállás miatt az email személytelen, muszáj úgy fogalmazni, hogy mindenkire igaz legyen, különben még többen fogják figyelmen kívül hagyni.

A Mesterséges Intelligencia megjelenésével a nyelvi hibák száma nagy mértékben redukálható, a méltán népszerű ChatGPT 73 nyelven képes szöveget generálni, amely majdnem minden esetben nyelvtanilag helyesebb, emberibb lesz, mint a Google Fordítótól megszokhatott. Habár ez is egy számottevő javulás az adathalászat terén, ennél nagyobb hatása van a fejlett adatelemzésnek, amely a Mesterséges Intelligenciával karöltve célzott támadásokat tud eredményezni, ez a csoportosításnál említett szigonyozás vagy angolul spear phishing. Rendszerezi az adatokat, statisztikákat állít fel, trendeket jelenít meg, majd ezeket az információkat felhasználva célzott támadást indíthatnak.

2.1.6. Felhasználás

Gondoljunk bele, ránk köszön valaki az utcán és azt állítja, ismer bennünket régről, ha olyan információkat mond rólunk, amik igazak és nem tudhatja mindenki akkor arra következtetünk, hogy valóban ismer minket és mi felejtettük el őt, ilyenkor egyből nyitottabbak vagyunk az illetőre, mert elméletileg ismerjük. Ugyan erre játszik a célzott támadás, látnak egy ismerős dizájnt plusz társul hozzá pár személyes információ, például a korházi kezelésről és le van írva, hogy nem került térítésre a teljes összeg. Ez akár egy valóságos dolog is lehet, emellett még oda van írva, a haladék dátuma, mert utána tovább fog nőni az összeg és idő szűkében, ha nem ellenőrzi le az ember akkor már be is csapták és valakinek kifizetésre került az összeg. Ennél még rosszabb, ha a támadó tudja, még egyáltalán nem rendeztünk egy számlát és ő előbb küldi a fizetési kérelmet, mint akinek ténylegesen fizetnünk kellene, ebben az esetben talán nem is kerül ellenőrzésre az e-mail valóságtartalma, vártuk az e-mailt, tudtuk, hogy jönni fog és már indul is a fizetés.

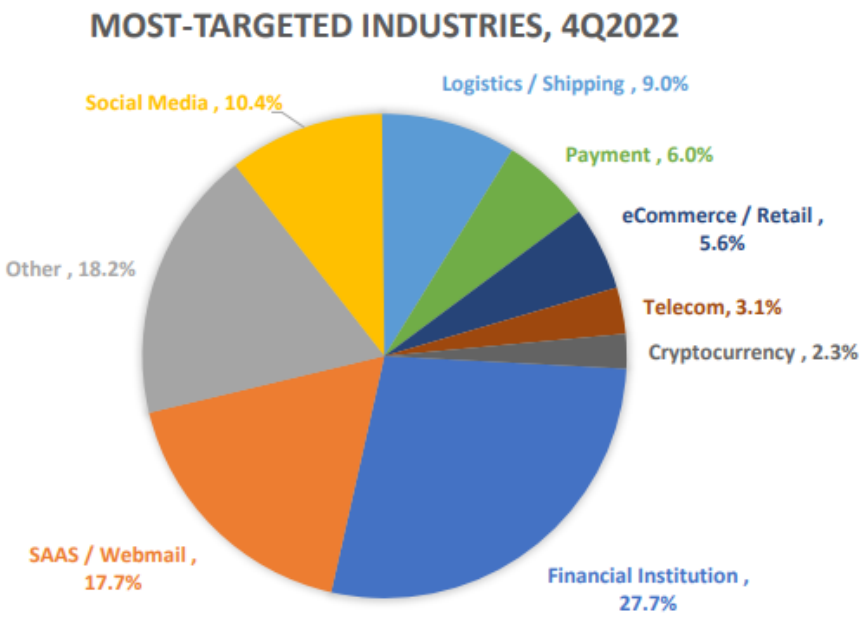
7. ábra: Adathalász bejelentések számának vizualizálása

Forrás: saját szerkesztés a https://apwg.org/trendsreports/ alapján

A táblázat adatai az APWG, magyarul Adathalászat Ellenes Munkacsoport negyedéves jelentéseiből lettek összegyűjtve. A különböző adathalász weboldalak és az egyedi számukra tovább küldött adathalász e-mailek összességéből jöttek létre a számok, globális elemzés, bárhonnan lehet nekik bejelentést tenni, egészen 2004 januárjától kezdődően dolgoznak fel adatokat, amiket meg is lehet tekinteni az oldalukon.

2015-től kezdődően láthatunk a diagramon enyhe fluktuációt, folyton felfele-lefele megy az esetek száma, majd elérkezünk a 2019-es évhez, ami egy mélypont, de ezt követően jelentős és folyamatos emelkedés veszi kezdetét egészen az utolsó elérhető riportig. 2021-ről 2022-re másfélszeresére nőtt a bejelentett esetek száma. Ennek az évnek a második felében jelent meg a ChatGPT első publikus verziója, ami biztosan hozzátett néhány esetet az eredményhez. Ilyenkor még alig volt korlátozva a rossz indulatú tevékenységekről való társalgás vagy nagyon egyszerűen ki lehetett játszani. Egyik leghíresebb interneten keringő példa az volt, amikor illegális kalóz oldalakat kért tőle a felhasználó és válaszként azt kapta, hogy nem reklámozhat illegális tevékenységet. A felhasználó következő kérése az volt, hogy sorolja fel milyen kalóz oldalakat kerüljön el és a gép egyből felsorolta a 7 legnépszerűbb ilyen oldalt.

Érdekesség képpen meg kell említeni, hogy 2023 júniusában ki lett adva egy WormGPT nevű nyelvi modell, melyet márciusban jelentettek be a www.hackforums.net weboldalon. Ez az eszköz teljes mértékben levette a korlátozást az eredeti verzióról és bármire meg lehetett kérni. Ezt egyből ki is használták etikátlan dolgokra és hamar híre ment a médiában is. Havidíjas rendszerben működött, mint bármelyik ma ismert sorozat vagy film szolgáltató. Azonban a készítői nem visszás célokkal indultak neki a fejlesztésnek, ők csak egy mindenre válaszoló nyelvi modellt szerettek volna. Kapott még memóriát is és így emlékezett a beszélgetésekre a felhasználóval, valamint nem alkalmazták a karakter mennyiségi korlátozást. De gyorsan kiderült, hogy ez egy illegális útra terelődő project, mert a legális dolgokat a ChatGPT megválaszolja. A készítők nem akartak ezzel a tudattal továbbmenni és augusztus első harmadában leállították a működését. (Sancho & Ciancaglini, 2023)

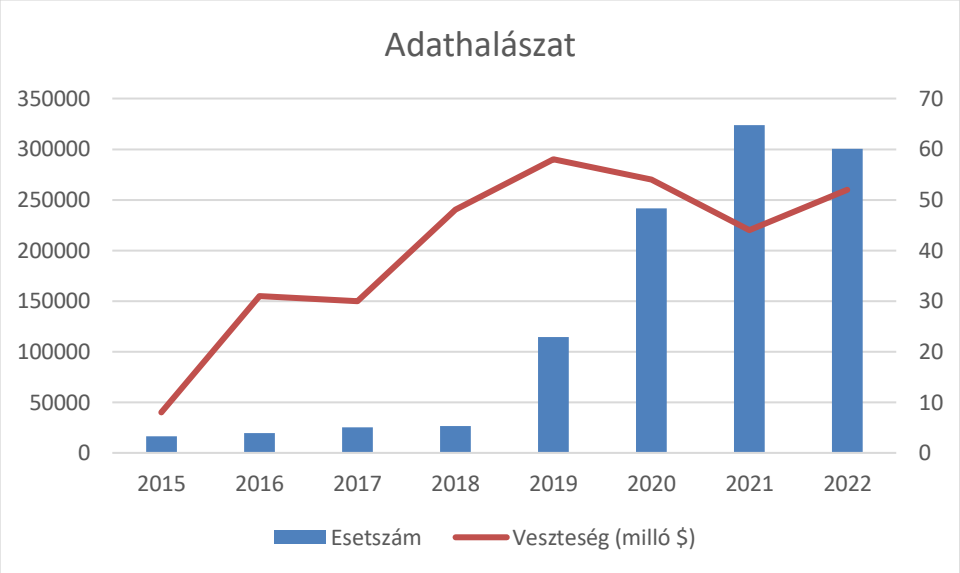


8. ábra: 2022 utolsó negyedév legcélzottabb szektorai

Forrás: https://shorturl.at/HIT02

2022-ben végig növekedett a bejelentések száma, így az utolsó negyedév volt a legnagyobb adathalmazt felmutató, ezért ezt választottam, annak megtekintésére, hogy mik voltak a leggyakrabban támadott iparágak ez idő alatt. Első helyre került, talán nem meglepő módon a pénzügyi szektor, ahová a bankok is tartoznak. Esetleg az játszódhat

szerepet ebben az esetben, hogy ha egyből azt a helyet támadják, ami pénzt kezel, úgy azt remélik, nagyobb eséllyel juthatnak pénzhez.



9. ábra: Adathalászati statisztikák alakulása

Forrás: saját szerkesztés a https://www.ic3.gov/Home/AnnualReports alapján

Az APWG jelentéséhez hasonlóan az IC3 államokbeli belföldi jelentése is összességében egy növekvő trendet mutat. Itt az áldozatok vesztesége is fel van már tüntetve. Fontos észrevennünk, hogy a felsorolt első 5 évben a kevés bűncselekményhez arányaiban mégis nagy érték társul, míg az időben tovább haladva az esetek gyakorisága nő, de a veszteség stagnál.

3. A MESTERSÉGES INTELLIGENCIA KOCKÁZATAI VÁLLALATOKRA NÉZVE

Különböző technológiáknak különböző felhasználási területei vannak, vannak amelyek több területre kiterjednek, vannak amelyek csak egy területet uralnak, a Mesterséges Intelligencia számtalan helyre beférkőzött már, így a mi mindennapi életünkön kívül például a vállalkozások napjait is átszövi. Az egyénekre gyakorolt hatásaihoz hasonlóan ez is lehet pozitív, illetve negatív. A pozitív hatások egy másik dolgozatban kerülnek részletes áttekintésre, itt a negatívakról lesz a későbbiekben szó. Nagyon sok különböző támadást erősített fel a Mesterséges Intelligencia vagy akár ide vehető az ezt megelőző réteg, a gépi tanulás. Nem kell egyből a nyelvi modellt okolnunk a fejlett és egyre sokrétűbb támadások miatt. A kiszivárgott adatban lévő információ kiaknázása legalább annyira kulcs szerepet játszik ezeknek a sikerességében, mint maga a nyelvi modell által nyújtott előny.

„Aki lemarad, az kimarad” szokták mondani, ez hatványozottan igaz a nagyvállalatokra, az Ipar 4.0 megjelenése alapjaiban változtatta meg a gyártási folyamatokat. Nagy mértékű automatizálás, adatelemzés, robotika és mindez a világhálóra kötve. Célja az okos gyárak létrehozása nagy fokú optimalizálás következtében. A végtelen mennyiségű adatból megállapíthatóak a szűk keresztmetszetek a gyártásban, kirajzolódnak a hiányosságok és a szervezési problémák. Azonban, hogyha minden rá van kötve az internetre, akkor szembe kell nézni az ebből következő problémákkal, mint az internetes támadások. A digitális korban a biztonsági őrök és a fizikai védelem messze nem elégséges már, sőt a vállalati titkok, a termék elkészítésének tudása (know-how), a partneri kapcsolatok privát kézben tartása már elsősorban inkább a virtuális adatvédelem kérdése. Természetesen az Ipar 4.0 elemei közül nem mind lesz releváns a pénzügyi vagy más szektorokban, kicsit kevesebb robotizálás képzelhető el itt, de az alapkövei, mint az internetes elérés és az adatok kitüntetett szerepe az összes helyen kulcsfontosságú. (F. A. Alenizi & S. Abbasi et al, 2023)

Critical infrastructure	Percentage of businesses with monetary loss – $100 thou. or more	Percentage of businesses with system downtime of 25 hours or longer
All businesses	13	40
Agriculture	4	46
Chemical and drug manufacturing	18	33
Computer system design	13	41
Finance	29	38
Health care	14	39
Petroleum mining and manufacturing	12	30
Real estate	6	39
Telecommunications	12	47
Transportation/pipelines	11	40
Retail	18	42
Scientific research and development	12	43
Accounting	13	29
Advertising	12	26
Architecture and engineering	11	40
Business and technical schools	5	45
Insurance	20	41
Construction	8	41
Food services	11	33
Forestry, fishing, and hunting	8	50

3. táblázat: Jelentős veszteséget elszenvedő esetek szektorokra bontva

Forrás: doi: 10.1515/itms-2017-0011

A helytakarékosság érdekében félbe van vágva a táblázat, ez egy 2017-ben kiadott riport alapján készült, amit az egyesült államokbeli Igazságügyi Minisztérium statisztikái alapján készítettek. Az egyének táblázataihoz hasonló módon itt is 100 000 Dollár a lélektani határ, amire kiemelt hangsúly van fektetve. Ez az összeg vállalatok életében kevésbé számottevő mennyiség, mint magánszemélyek esetében. Azonban a szervezetek életében a pénzügyi veszteségen kívül egy másik kulcsfontosságú szempontot is figyelembe kell venni, ez pedig a második adatoszlopban feltüntetett leállás ideje. Egy vállalkozás életében az időkiesés kritikus lehet, ha egy gyáregység nem gyártja le és nem tudja leszállítani a beígért, előre lebeszélt mennyiséget, akkor súlyos pénzektől eshetnek el.

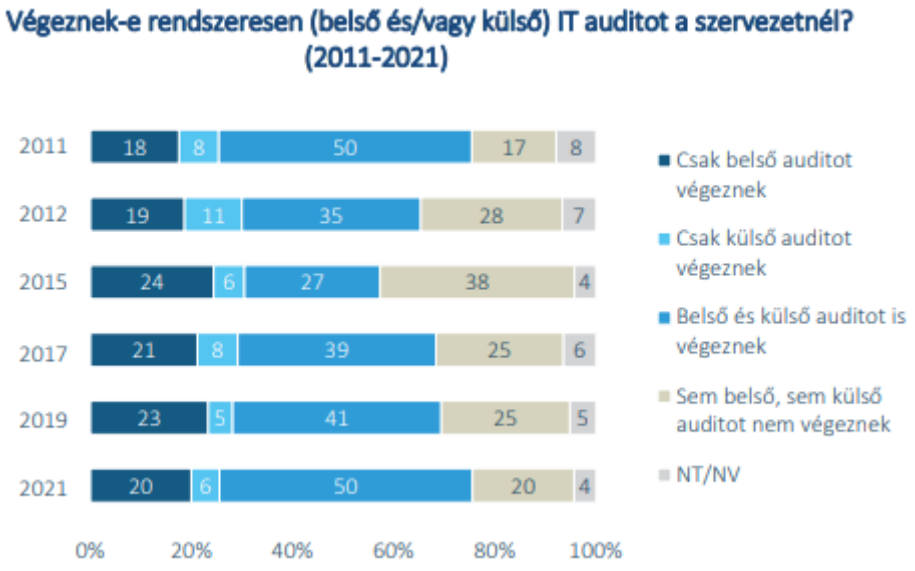
3.1. Információbiztonság helyzete Magyarországon

Először is pár szó magáról az információbiztonságról. Az információbiztonság nem összekeverendő az informatikai biztonsággal, az információbiztonság nem merül ki a hardverekben, tűzfalakban és vírusirtókban, ennél jóval összetettebb probléma. A hitelesség, számon-kérhetőség és letagadhatatlanság jelentős szerepet játszanak az „információbiztonság” szó teljesítésében. Ezek fontos részei a vállalati folyamatoknak, az informatikai rendszerben megtalálható adatok sérthetetlensége elengedhetetlen szempont a mai világban. A siker kulcsa a mérés és az értékelés, mert kell valami

kézzelfogható információ a helyzetről. Az IT audit kézenfekvő megoldás lehet a fennálló státusz megismerésére.

Fontos kihangsúlyozni, hogy az információbiztonság az egy állapot, ezt fent kell tartni hosszútávon is, nincs az életben két egyforma támadó, nincs két egyforma támadás. Hogyha valaki megpróbálta és nem járt sikerrel, ugyan azt a módszert nem fogja újra próbálni. Fokozatosan fejlődnek az elkövetők és a módszereik, ezzel párhuzamosan szerencsére a védekező oldal lehetőségei, technikái is erősödnek. (Michelberger, 2012)

Az ISACA Magyarországi Egyesület megbízásából készülő 2011 óta kétévente megjelenő jelentés a belföldi vállalatok helyzetét hivatott bemutatni. A mintát legalább 250 főt foglalkoztató és/vagy 4 milliárd Forintot meghaladó éves nettó árbevétellel rendelkező vállalkozások és intézmények alkotják. 150 cég töltötte ki a kérdőívet és külön ügyeltek arra, hogy olyan töltse ki, aki kompetens a területen, így remélve a pontos és valósághű végeredményt.



10. ábra: Rendszeres IT audit gyakorisága

Forrás: https://shorturl.at/myI48

Az ábrát elemezve láthatjuk, hogy az itthoni helyzet egyáltalában nem borzalmas, a válaszadó szervezetek több mint háromnegyede (76%) rendszeresen végez auditot. Külön kiemelendő, hogy 50% külső és belső auditot is egyaránt végez. Jó hír, hogy 2015 óta

folyamatosan és jelentősen növekszik azok száma, akik mindkettőt elvégzik rendszeresen.

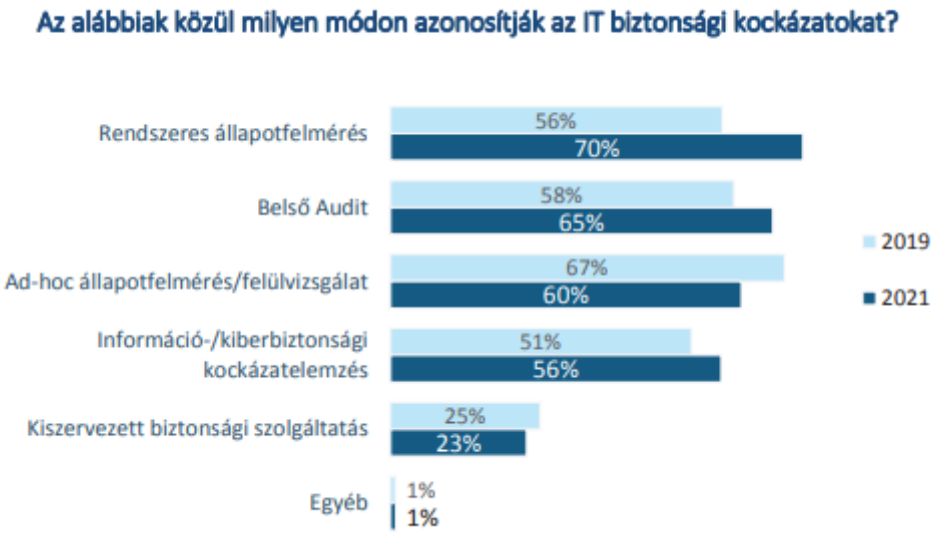
A jelentés szövegéből megtudhatjuk, hogy az IT audit kiszervezésének gyakorisága 2021-re csökkent, annak ellenére, hogy hatékonyabb és gazdaságosabb kiszervezni, ez egy nagyon kényes kérdés a vállalatok számára, mert a belső adatokhoz hozzáférést kell biztosítaniuk külső cégek számára. 2015-ben volt a legrosszabb a helyzet, ekkor a válaszadók kétharmada (66%) nem szervezte ki addig az auditálás folyamatát és nem is tervezte ennek bevezetését egyáltalán. Azonban az idő múlásával ezek az ellenérvek háttérbe szorultak és ha bár fluktuálást követően, de javult a helyzet az utolsó évre. 2021-re 8% ponttal nőtt a kiszervezett IT auditok száma, valamint 56% pontra csökkent azoknak a tábora, akik egyáltalán nem fogják ezeket a feladatokat átadni külsős szakértőknek.

11. ábra: Elmúlt 1 évben bekövetkező negatív események (2021)

Forrás: https://shorturl.at/myI48

Talán nem is gondolnánk milyen gyakorisággal fordulnak elő rosszindulatú esetek az internetes térben, közeli ismerőseimet kérdezve egyáltalán nem mondható el, hogy a negyedük az elmúlt egy éven belül személyesen találkozott vírussal, kémprogrammal vagy valamilyen rosszindulatú szoftverrel. Eközben pedig ahogy látjuk, a vállalkozások

életében ez gyakrabban előforduló esemény. Csak a többször szembejövő eseteket láthatjuk az ábrán, gyakori eset még a személyiséglopással párhuzamosítható második pont, ahol a vállalat nevével és jó hírével próbálnak visszaélni.



12. ábra: IT biztonsági kockázatok azonosítási módjának eloszlása

Forrás: https://shorturl.at/myI48

Ez a diagram a fellelhető fejlődés mértékét hivatott jelezni az IT biztonsági kockázatainak azonosítása terén. Az utolsó előtti állapothoz képest észrevehetjük, hogy jelentősen növekedett az ütemezett állapotfelmérések száma és ezzel ellentétben pedig csökkent a véletlenszerű, ad-hoc módszer. Ez azt sugallhatja, hogy egyre inkább elkezdik megérteni a cégek a fontosságát ezeknek a módszereknek és elfogadják, hogy a fejlődés útja errefelé vezet. A véletlenszerűen elvégzett állapotfelmérések gyakran csak olyan esetben történnek meg, amikor körvonalazódik, hogy valami nem megfelelően működik és ezt akarják hirtelen felülvizsgálni.

3.2. BEC támadások

Egy sok embert foglalkoztató vállalatban az e-mailek átbogarászása senkinek nem tartozik a legkedveltebb feladatai közé, lehet, nem is mi vagyunk a fő célpontja egy e-mailnek, lehet csak egy másolatot kapunk, de mégis elolvassuk, nehogy véletlen ránk is vonatkozzon. Esetleg mi kezdtük a köremailt, de már megkaptuk a válaszunkat és valaki más folytatta, mindenki bőszen kattintja a dedikált „válasz mindenkinek” gombot és bármi, ami fontos volt számunkra már 10 másik válaszlevél alatt van. Előfordulhat, hogy olyan pozícióban dolgozunk, ahol a tevékenységek ellátása egy e-mailel kezdődik, jön a levél és csináljuk, ami benne van. Pontosan ennek a fajtájú tevékenységnek a kijátszására találták ki a következő támadást.

Egyik legfontosabb Mesterséges Intelligenciával karöltött kibertámadás a BEC (Business E-mail Compromise), magyarul arról van szó, hogy a vállalati levelezőrendszert kompromittálják. Vannak források, melyek ezt az adathalászattal veszik egy kalapba, de ez nem csak egyszerű adatgyűjtésről szól, egyből bekövetkező károkozás történik (EUROPOL, 2021).

Működése nagyvonalakban a következő: a vállalati email kinézetével megegyező vagy nagyon hasonló küllemű levelet juttatnak el a megfelelő személynek, melyben egy mindennapi, átlagos feladatot adnak meg egy kicsi változtatással.

13. ábra: BEC lépései

Forrás: Saját szerkesztés a https://doi.org/10.1016/j.matpr.2021.03.647 alapján

Első pont, hogy a támadó megkeresi a célpontot, ahol el akarja végezni a támadást, következő lépés a cég feltérképezése és információ gyűjtés. Meg kell találni a megfelelő embereket a vállalaton belül, akik olyan kapcsolatban állnak egymással, ahol nem kelt különös figyelmet a dolog, lehet ez akár egy külsős cég, aki számlákat küld vagy valaki a pénzügyön. Megnézi a szóban forgó pénzösszegeket, hogy azzal is jobban elvegyüljön az email a többi között. Miután megszerzett minden információt, megírja a levelet a megfelelő küllemi tulajdonságokkal és egy akár 1 betűvel eltérő e-mail-címről elküldi a levelet az illetékesnek. Amikor sorra kerül a levél, számára kedvező esetben megtörténik a pénz utalása, ezt egyből tovább utalja egy külföldi számlára, amihez az adott országnak korlátozott a rálátása. (N. Saud Al-Musib, 2021)

A BEC mellett elengedhetetlen, hogy megemlítsük az egyik ehhez nagyban hasonlító bűncselekménytípust, ez nem más, mint az EAC (E-mail Account Compromise). Ez abban különbözik az előzőtől, hogy a támadó nem el akarja hitetni, hogy ő a bizonyos személy, hanem ebben az esetben konkrétan ő az. Nem egy hasonló e-mail-címről ír, a feltört levelezőfiókot használja. A vállalkozásoknál használt e-mail szolgáltatók nagy részénél már jellemző, hogy a rendszer kiírja nagybetűkkel, hogy külsős embertől jött az üzenet, de ilyenkor ez értelemszerűen nem fog megtörténni. Az áldozatnak nagyon nehéz dolga van, hiszen, ha még meg is nézi a fura levelet, látja, hogy legitim helyről érkezett. (proofpoint, 2020)

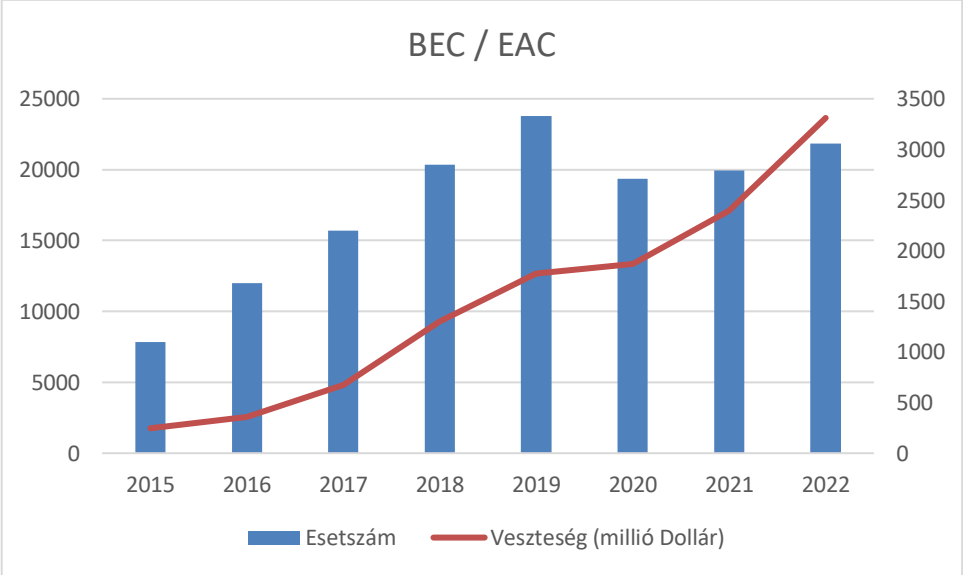
Néhány indikátor, melyek intő jelek lehetnek az e-mail valóságosságát illetően: (N. Saud Al-Musib, 2021):

- megmagyarázhatatlan sürgősség,
- utolsó utáni pillanatban történő változás,
- másik kommunikációs csatornán történő megerősítés kizárása.

Egyelőre nem esett szó eddig arról, hogy hogyan jutnak hozzá a belső rendszerhez a támadók. Ebben az esetben is több opció van, lehet feltörni jelszavakat, általában a nyers erő módszerét alkalmazzák és végül sikerrel járnak, de a sötét webre kiszivárgott jelszó halmazokat is végig próbálhatnak vagy az interneten fellelhető „leggyakoribb jelszavak” táblázatot végig járják. Másik gyakori módszer, amikor valamilyen USB eszközt hagynak hátra, ami később bekerül a gépbe, lehet ez egy töltőnek álcázott pendrive vagy egy

teljesen átlagos pendrive, amit beleraknak egy borítékba és ráírnak valami figyelemfelkeltőt. A „legénybúcsú 2022” címmel ellátott adathordozó biztosan sokaknak elindítja a fantáziáját és a képek helyett egy vírus jut fel a belső számítógépre.

Emellett óriási tévedésben vagyunk, hogyha azt hisszük, meg is kell nyitnunk valamit ahhoz, hogy az bajt okozzon a számítógépen, elég bedugni a csatlakozóba az eszközt és előre megírt kódsor le is fut pár másodperc alatt, ezek mellett key-logger is működhet a háttérben, ami minden billentyűnek a lenyomását elküldi a támadónak, ezzel megszerezve a jelszavakat. A https://shop.hak5.org/ weboldalon számtalan illegális dolgokra használható termék rendelhető, köztük a fentebb említett töltő kábelnek álcázott pendrive, amely távoli hozzáférést tud biztosítani a számítógéphez. Ez úgy lehetséges, hogy a portban egy vezeték nélküli elérési pont van, amihez az elkövető csatlakozik. Az USB ártalmatlan eszközként van érzékelve az operációs rendszer által, például billentyűzetként. Ez is elküldi a WiFi hálózaton keresztül a leütött billentyűket és utána már egyszerűen be tud lépni az illető. Minden céges adatvédelmi oktatáson elmondják, hogy semmi külsős hardvert nem szabad bedugni a számítógépbe, de mindig lesz olyan, aki ennek nem tesz eleget vagy elbagatellizálja az egészet és egyből meg van a probléma.



14. ábra: BEC/EAC támadások gyakorisága

Forrás: saját szerkesztés a https://www.ic3.gov/Home/AnnualReports alapján

A Szövetségi Nyomozóiroda jelentésében külön szerepet kap ez a fajta internetes bűncselekmény is, ha visszatekintünk az egyéneknél bemutatott diagrammokra, amelyek az adathalászatot és a személyiséglopást vizualizálták, láthatjuk, hogy a veszteség ott csak a töredéke az itteni ábrán feltüntetettnek. Ez rámutat arra, hogy a vállalkozások mekkora veszteségeket szenvednek el az ilyen események bekövetkezése során és ebbe nincs belekalkulálva a leállás miatti idő és pénzveszteség. A 2022-es évben 3 milliárd Dollár veszteséget termelt csak az Amerikai Egyesült Államokban. Az esetek száma nem is növekszik gyorsan, mert ezek célzott támadások, de az illetéktelenek kezére került vagyon mégis számottevő. Ez köszönhető annak, hogy az átlagnál könnyebb bedőlni ezeknek a támadásoknak. Fontos észrevennünk, hogy ezeknél a bűncselekményeknél 2 áldozat van 1 elkövetés alatt. Egyik a cég lesz, aki elszenvedi a kárt, a másik pedig a személy, aki közvetetten a kárt okozta, ő ugyan direkt módon nem tehetett róla, de mégis egyfajta szerepet játszott ebben és ez mentálisan leterhelő lehet egyesek számára.

Egyik nagy port kavaró eset 2019-ben került lezárásra, amikoris egy Evaldas Rimasauskas nevű, 50 éves, litván nemzetiségű férfit 5 év börtönre ítéltek, mert több mint 100 millió Dollárt csalt ki 2013 és 2015 között két amerikai nagyvállalattól, a Facebooktól és a Googletől, számos hamisan kiállított számla segítségével. (Tom Huddleston Jr., 2019)

És hogy hogy kapcsolódik ide a Mesterséges Intelligencia? A technológia képes kódot generálni weboldalak képe alapján, ezt utána a hozzáértők tudják módosítani, úgy, hogy a végén a tökéletes mása legyen egy oldalnak. Ezt BEC / EAC támadáson belül el lehet juttatni a megfelelő embernek, aki akár egy fontos banki felületnek hiheti és bejelentkezik rajta. Ugyan ez a dolog megvalósítható e-mail templateken is. Újra alkotják a megjelenését az e-mailnek, hogy ne tűnjön fel, amikor egy kárt okozó dolgot kell végrehajtani a célpontnak. A gépi tanulás tud segíteni a munkahelyi hierarchia feltérképezésében, feltudja ismerni miről szólnak a levelek, az embernek nem kell egyesével mindent átnéznie, ez jelentős idő spórolás a kiválasztott cég méretének függvényében. A szövegezésben nem mindenki tud olyan kreatív és találékony lenni, amivel meggyőzi a másikat, ebben segítenek a nyelvi modellek, meg lehet adni a

hangnemet és az e-mail szövegi része el is készül és ha ez nem lenne elég jó, az ember még mindig tud rajta javítani. (taskade, 2023)

3.3. Ransomware

Ransomware egy olyan fajta internetes vírus, amely megakadályozza a hozzáférést a számítógépen lévő fájlokhoz és csak akkor oldja fel ezt a tiltást, hogyha az áldozat kifizeti a kért összeget a támadónak. Zsaroló vírusnak lehet hívni magyarul és az utóbbi években egyre nagyobb népszerűségnek örvend sajnos. Egy ilyen támadás magánemberek ellen is előfordulhat, de vállalatoknál sokkal jövedelmezőbb, ezért ott terjedt el jobban. Szellemileg egy más fajta megterhelés, mert a megoldás csak egy karnyújtásnyira van az áldozattól, de senki nem szívesen ad ki pénzt idegeneknek, valamit egyáltalán nem biztos, hogy az elkövető fél tartani fogja majd a szavát a megbeszéltekhez. Rombolhatja a hírnevét egy szervezetnek azáltal, hogy nem biztonságosnak tünteti fel, másik esetben eladhatja az információt az interneten riválisa cégeknek vagy más bűnözőknek, akik hasznot tudnak húzni az adatszivárgásokból.

Kettő fő zsaroló vírust különböztetünk meg egymástól:

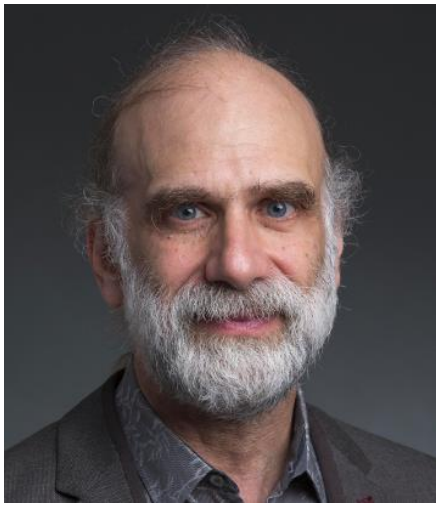
- fájl titkosítás, ami bizonyos adatokhoz való hozzáférést blokkolja,
- képernyőzár, ahol nem tudunk bejelentkezni a számítógépünkre.

A Mesterséges Intelligencia akkor lép be a képbe, amikor a célpontot kell kiválasztani. A feljavított zsaroló vírus abban különbözik a már régóta ismerttől, hogy keres a hálózaton, gondolkodik. Feljavítja a hatékonyságot azáltal, hogy kibogarássza a nagy mennyiségű adatból az információkat és olyanokat zár le, amiket kulcsfontosságúnak ítél meg, mint például könyvelési adatok és számlák. Mindezt töredéknyi idő alatt teszi meg, ahhoz képest, amit egy ember el tud érni. Egy embernek minden egyes mappát és fájlt meg kell néznie, hogy tudja, miért fognak a későbbiekben fizetni. Leveszi a terhet az elkövető válláról, amíg ő más, nem automatizálható tevékenységet végez, például másik áldozatot keres. (FORTINET, 2023)

4. A MESTERSÉGES INTELLIGENCIA ÉS A BŰNÖZÉS JÖVŐBENI ALAKULÁSA

Eddig a múlt és a jelen állapotát vizsgáltuk, de mire számíthatunk a jövőben, hogyha a technológia fejlődése hasonló léptékben halad tovább? Elsősorban remélhetőleg szabályozásokra, ezen belül is egységes szabályozásokra, amik országhatárokon át ívelnek. A friss technológia szabályozása kezdetben mindig nehéz, de a jövőben több év tapasztalatával már egyre kevesebb gondot kellene, hogy okozzon a megfelelő hivatalos szerveknek.

Egyre elterjedtebb lesz a CaaS (Crime as a service), ami annyit jelent, hogy az internet sötét oldalán egy-egy bűncselekményt szolgáltatásként lehet majd vásárolni. Ez azért jelentős probléma, mert ha valamihez könnyebb hozzájutni, akkor többen fogják használni. A program készítője a saját céljain felül további profitra tehet szert, amiből újabb eszközöket vásárolhat és bővítheti technikai hátterét, mindez tovább fogja terhelni a rendőrséget és a károsultak számát ezzel párhuzamosan növeli. A legkülönbözőbb fajta bűntények vásárlására nyújthat ez majd lehetőséget, a ransomware típusúaktól, a DDOS (Dsitributed Denial of Service) támadáson keresztül – ami elárasztja a szervereket kérésekkel és a nulláig lassítja őket – egészen célzott adathalász e-mailekig. (FORTINET, 2023)



15. ábra: Bruce Schneier amerikai kriptográfus
Forrás: https://carrcenter.hks.harvard.edu/people/bruce-schneier

Az internet gyors terjedésével, a térfigyelő kamerák számának növekedésével lehetőség nyílt az emberek tömeges megfigyelésére, a Mesterséges Intelligencia pedig ezt tovább fokozza és lehetőséget teremt tömeges kémkedésre az embereken. A megfigyelés és a kémkedés merőben eltér egymástól, előbbi arról szól, hogy mit csinál az ember, kivel, mikor és hol, míg utóbbi inkább a személyesebb dolgokat érinti, mint hogy mit mondtunk a másiknak, mit nézünk az interneten, miket írunk a többieknek. Az internet előtt mindkettő egy időigényes és költséges folyamat volt, folyton követni kellett a másikat, rejtőzködni kellett, a mai világban a telefonunk lefedi a túlnyomó részét mindezeknek, GPS tudja merre járunk, a kimenő és bejövő üzeneteket pedig lehallgathatják, ismerik a böngészési adatainkat, ezért láthatjuk sokszor néhány internetes keresés után a keresett terméket reklámként megjelenítve a hírfolyamokon.

Az internet és a telefon megoldotta ezt a problémát, de még mindig kell egy humán erőforrás, aki az adatokat elemzi, hallgatja a beszélgetéseket és velünk együtt nézi, amit mi nézünk. A Mesterséges Intelligencia ezt fogja megváltoztatni. Segíteni fog a profilozásban, sokkal gyorsabban elemzi a nagy mennyiségű adatot és nem igényel emberi beavatkozást a folyamat teljes időtartamán át. (Bruce Schneier, 2023)

A következő példák egy olyan tanulmányban találhatóak, amiben a készítők úgy próbálták kiválasztani a technológiákat, hogy mekkora lesz a jövőbeni használatának valószínősége és mekkora lesz a bekövetkező hatások mértéke, mindezeket a predikciókat a következő évtizedre tartják hitelesnek.

IoT (Internet of Things), azaz minden világhálóra kapcsolódó dolgok összessége, ennek a technológiának a terjedés területenként eltérő, a modern gyártási környezetben már elterjedt, de a mindennapi életünkben és otthonunkban tapasztalatom alapján még lemaradás van, kevés az okos hűtő és kevés az okos ház, amiben minden számítógép vezérelt. A jövőben ennek a változásával és az otthonok fokozatos automatizációjával új fajta betörések fognak megvalósulni, mindenkinek a napi rutinja el lesz tárolva az eszközök által és biztonsági réseket mindig talál az, aki eleget keres, ezeket a lehetőségeket kihasználva pedig betöréseket hajthat végre vagy el is adhatja az adatot másoknak, akik érdekeltek a hozzánk való bejutásban. (RAND Europe, 2020)

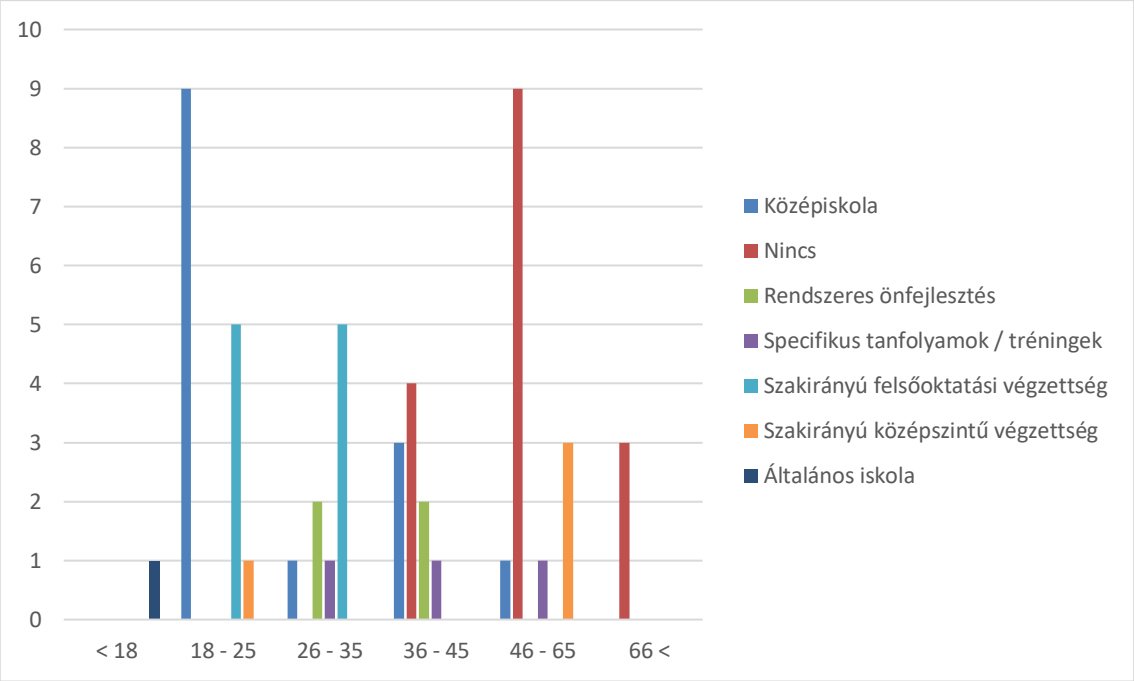
A második a telekommunikációs infrastruktúra, ami magába foglalja a fizikai és digitális hálózatokat is, amelyeknek köszönhetően áramlik az információ napjainkban. A gyártók törekednek a folyton növekvő igényeket kielégíteni, nagyobb sávszélesség, kisebb válaszidő, de észre kell vennünk, hogy a bűnözök is ugyan úgy felhasználók, mint mi és vásárlói igények kielégítése őket is előnyökhöz fogja juttatni. Nagyobb sebességgel tölthetnek le majd adatot, nagyobb felhő alapú számítási kapacitáshoz férhetnek hozzá ezáltal. (RAND Europe, 2020)

Egy az előzővel ellentétes probléma lehet az, hogy elterjed az infrastruktúra decentralizálása, igen, a nagyon-nagy számítási kapacitást igénylő tevékenységek még mindig felhő alapú szolgáltatáson keresztül fognak futni, de a hétköznapi számítógépek fejlődésével sok visszafogottabb program már saját körben is használható lesz, csökkentve a nyomozás hatékonyságát. (Philip Treleaven et al., 2023)

Összefoglalva a jövőjét ennek a lehetőségnek, a baj nem csökkenő tendenciát fog mutatni, az elmúlt években is növekedett az internetes csalások száma és továbbra is nőni fog, emellett óriási aszimmetria van jelen a területen, számtalan biztonsági kockázatra kell gondolni az illetékeseknek, de a másik oldalnak csak egyetlen gyengepontot kell találnia.

5. SAJÁT KÖRBEN VÉGZETT KUTATÁS EREDMÉNYEI

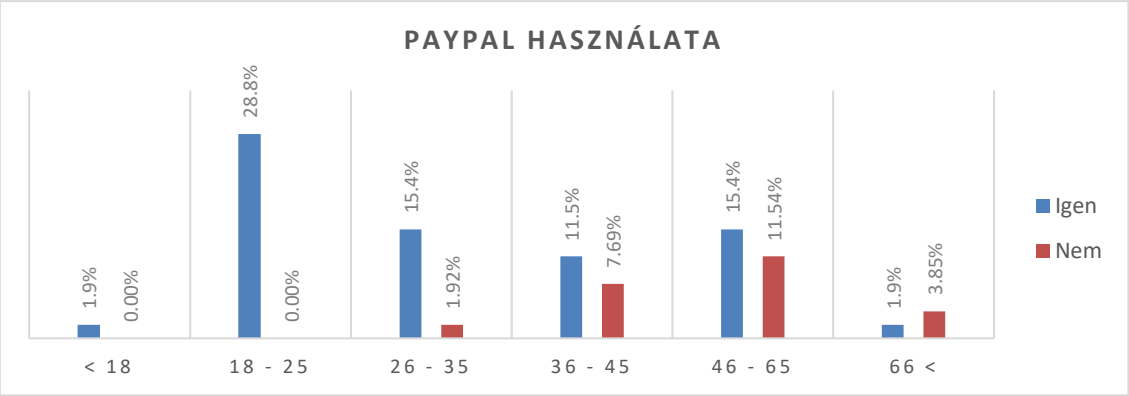
Az interneten fellelhető kutatások mellé én magam is készítettem egyet, ami az általam elért embereknek az informatikában való jártasságát hivatott tükrözni. Az adatok fő ismérve a korcsoport volt, a kérdések kitértek az informatikai tanulmányokra, az elszenvedett kiberbűncselekményekre, a virtuális biztonsági lehetőségek népszerűségére, valamint egyes alkalmazások használati szokásaira.



16. ábra: Végzettség megoszlása korcsoport alapján

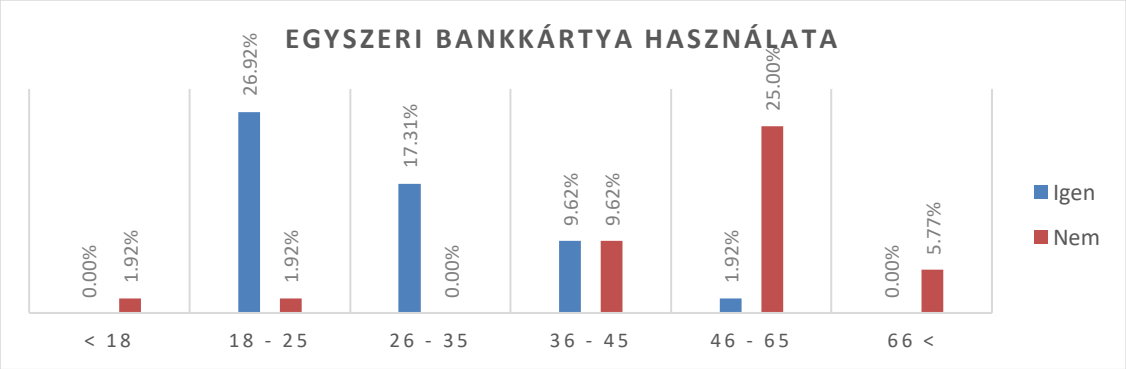
Forrás: saját szerkesztés

Legelső ábrával a kérdezettek informatikával kapcsolatos viszonyát szeretném bemutatni, sajnos nagyon kevés 18 év alatti gyermekhez jutott el a kérdőív, így arról az oldalról különösen kevés információim van. Ami elsőre szembetűnik, hogy az életkor növekedésével egyre nagyobb százalékban jelenik meg a „Nincs” opció, hogy semmilyen informatikai tudásuk nincsen. Ez egy teljesen normálisnak mondható életkori sajátosság, régen az informatikai tudás sokkal kisebb számban játszott szerepet a mindennapi életben, de ez mára már negatívumként fog jelentkezni, mind a való életben, mind a később látott diagrammokon is.



17. ábra: PAYPAL használatának népszerűsége

Forrás: saját szerkesztés

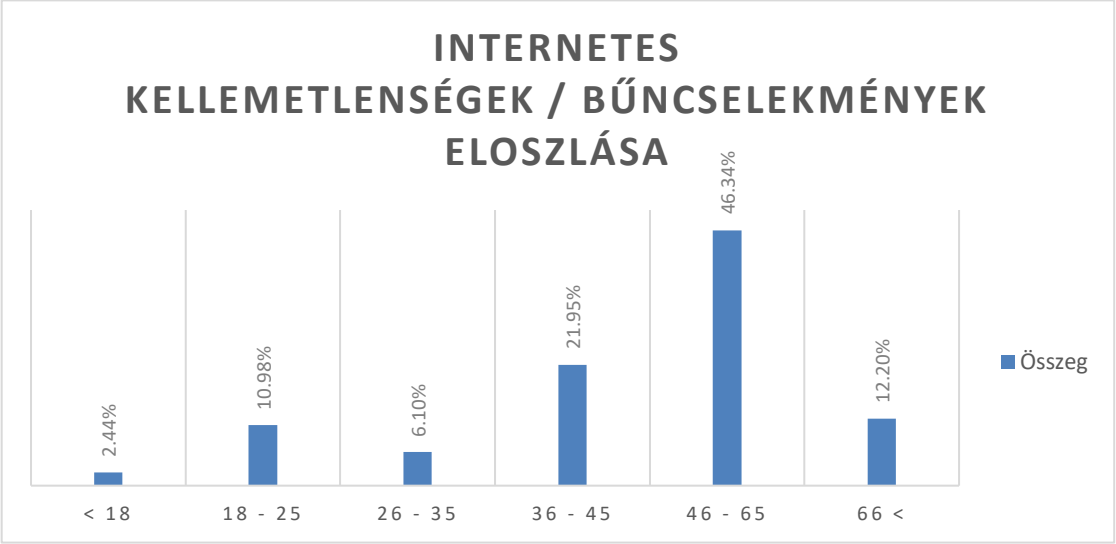


18. ábra: Egyszer használatos bankkártya népszerűsége

Forrás: saját szerkesztés

Talán a legbiztonságosabb internetes fizetés két módszerét sikerült felsorakoztatni itt, a két diagramot egymással kontextusban érdemes nézni. Az interneten való rendeléshez régen óriási népszerűségnek örvendő PayPal és egy viszonylag újnak mondható technológia, az egyszer használatos (angolul single-use) virtuális bankkártya. Mindkettő lényege, hogy a bankkártyánk adatait nem kell megadnunk a vásárlás oldalán. Olyan helyzetekben, amikor nem tudjuk eldönteni egy oldal hitelességét, akkor ez hirtelen egy kulcs szemponttá válik mindenki szemében.

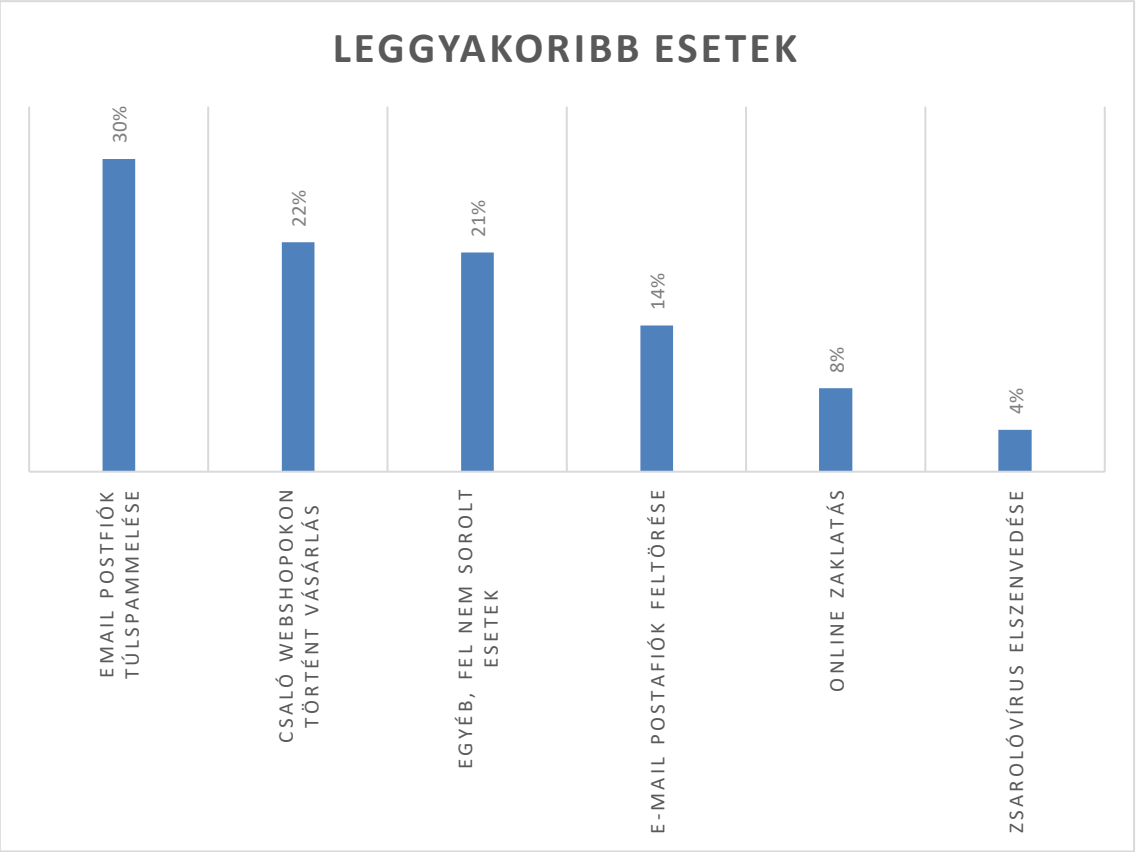
A válaszok nem vagy/vagy formátumban vannak, mindkettőre külön lehetett igennel vagy nemmel válaszolni. Megnézve a két ábrát láthatjuk, hogy a virtuális kártya a fiatalok körében jobban elterjedt, míg az idősebb korosztály a PayPal rendszerét favorizálja és nagy mértékben adtak nemleges választ az egyszeri kártya használatára.



19. ábra: Válaszadókat ért esetek megoszlása korcsoport alapján

Forrás: saját szerkesztés

Ahogyan a dolgozat első felében is szó esett már arról, hogy az interneten elszenvedett bűncselekmények nagyobb hányadát a társadalom idősebb társai élik át, úgy az én általam vizsgált környezetben is ez figyelhető meg. Nekünk hozzátartozóknak fontos feladatunk lenne őket edukálni ezen a területen, mert az ő gondjuk részben a mi gondunk is lehet. A legalapvetőbb dolgok elmagyarázása is nagy segítség lehet számukra, amikor a következő esetben találkoznak valami kétes kérdéssel. A 18 és 25 év közötti korosztálynál látható kisebb kiugrás véleményem szerint az internetes zaklatásnak tudható be leginkább, mert itt ez a fajta jelölés kiemelkedő arányban szerepel.



20. ábra: Válaszadokat elggyakrabban ért esetek rangsorolása

Forrás: saját szerkesztés

Végezetül nézzük meg, melyek azok az események, amik leggyakrabban előfordultak a megkérdezettek között. Majdnem minden harmadik ember találkozott már azzal a jelenséggel, hogy nagyon sok e-mailt kap, ez egy idegesítő dolog, de szerencsére nem jár közvetlen veszteséggel. Második helyen már egy sokkal komolyabb problémát látunk, ami kicsit több mint az ötödét érinti a csoportnak, itt már egyértelműen megkárosítják az embert, ezzel közel egy szinten találjuk az egyéb kategóriát, erről nehéz megállapításokba bocsátkozni. Mindenkinek az e-mail az, amit először regisztrál az interneten, nem gondolja túl a jelszót vagy több másik oldalon is ezt adja meg és ezért gyakorta szembesülnek a kompromittált levelező fiókkal. Ezt követően inkább a fiatalok körében elterjedt internetes zaklatás szerepel és a sort pedig a zsaroló vírus zárja.

6. MIT TEHETÜNK MINDEZEK ELLEN?

A veszteségek és kellemetlenségek elkerülésének leghatékonyabb módja a megelőzés, magánszemélyként és vállalatként is ez a legfontosabb pont. Tekinthetjük ezt egy ökölszabálynak, ami mindenre igaz az életben, kármentés helyett megelőzés lesz a kulcs. Minél jobban elterjed (és ezáltal az illetékesek fülébe jut) egy új bűncselekmény, annál gyorsabban fog rá új szabályozás is születni. Előfordult ez az internet megjelenésénél is és most is végbe megy egy a Mesterséges Intelligencia miatt. Azonban a hatóságok többségében csak a kármentéssel és a büntetés kiszabásával foglalkoznak, nem ők adják a megoldásokat a megelőzésre. A vírusok megjelenése után a vírusirtók is hamar megjelentek, az MI térnyerésével pedig ezt integráló vírusirtók vagy szűrők terjednek el. Ha egy zsarolóvírust kapunk akkor utólag kell fizetnünk az adatainkért cserébe, de ha vírusirtót vásárolunk, akkor előre fizetünk az adataink biztonságáért, összeesküvés elméletekbe nem belemenve, remélhetjük, hogy nem ugyan az csinálja a vírusokat, aki készít ellenük vírusirtó szoftvert.

Általánosságban véve azonban a védelem nem csak a megelőzést foglalja magába, mint ami megakadályozza az adatok kiszivárgását, jogosulatlan felhasználást és társait. Beszélhetünk még elrettentésről, ez egy vállalkozáson belül is elképzelhető etikus keretek között, de túlnyomó részben egy felsőbbrendű szabályozó szerv feladata. A büntetéstől való félelem kettő dologból adódik össze, első az, hogy mekkora bizonyossággal fog a cselekmény büntetéssel végződni és a második pedig, hogy ez a büntetés mennyire lesz szigorú különböző esetekben. A bizonyosságot az határozza meg, hogy a bírósági szerv mennyire látja át a problémát és ezt mennyire tartja azt jogsértőnek. A szigorúságot a kiszabható büntetések spektruma adja. (Diptiben Ghelani, 2022)

Következő elem a megfigyelés, a szervezeteken belül ez manapság egy alapvető dolog, minden naplózva van, bármit vissza lehet keresni, ki lépett be, mikor, mit csinált, minden módosítás, törlés, ez elengedhetetlen a biztonság kiépítésében. Az államnak is vannak eszközei, a titkosszolgálatnál fórumokat ellenőriznek, social-media kommenteket néznek folyamatosan és ezeket pszichológusokkal együtt elemzik, eldöntésre kerül, hogy mennyire gondolhatja komolyan az illető, amiket ír vagy csak frusztrációból mond mindent. Alkalomadtán akár folyamatos megfigyelés alá is vonhatnak kérdéses

embereket. A megfigyelés fontosságára egy magyarországi példát lehet említeni, a 2008-2009-es romagyilkosságok idejéből, itt a három elkövető közül mindhármat megfigyelték visszás tevékenységük miatt, de a támadássorozat megkezdése előtt mindegyiküknek felfüggesztették a megfigyelését és így csak 6 áldozattal és több mint 1 ével később kerültek kézre az elkövetők. Habár ez nem az internet korából van és nem is azzal kapcsolatos, de a megfigyelés jelentőségét vagy a megfigyelés hiányát jól tükrözi az eset. (Szemán László János, 2020)

Utolsó szempont az észrevétel, ez a megfigyeléssel szemben nem egy folytonos és sok irányba kiterjedő tevékenység, maga a probléma létrejötténél van szerepe, hogy milyen gyorsan lehet eliminálni a felmerülő kockázatot és mit lehet tenni a kármentés érdekében. (Diptiben Ghelani, 2022)

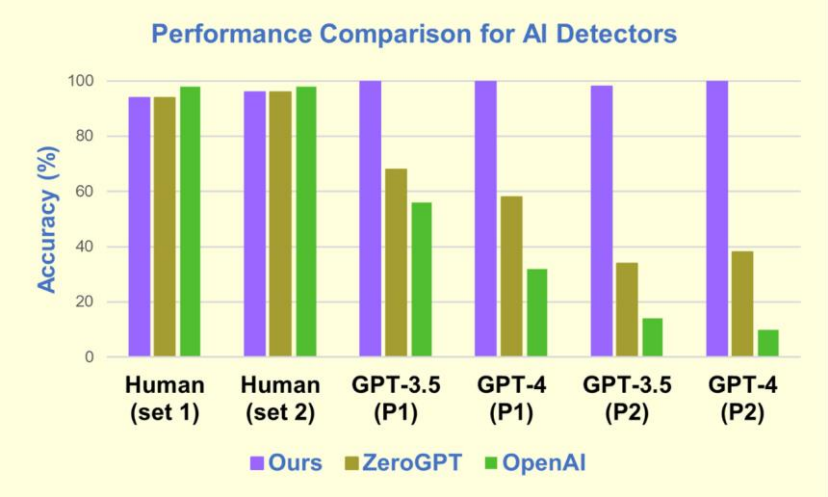
Előbbiekben szó volt a kiberbűnözés elleni védekezésről és megelőzésről, de ezek elméleti síkon vannak bemutatva. Mit tehetünk hétköznapi emberként annak érdekében, hogy ne essünk áldozatául ezeknek a bűncselekményeknek? (Ashley Pugh, 2023)

- megfelelő jelszó használata,
- nézzük meg, hogy egy kattintható link milyen oldalra hivatkozik,
- telepítsük a biztonsági frissítéseket,
- nagy körültekintéssel adjuk meg adatainkat,
- készítsünk biztonsági mentéseket fontos dolgainkról,
- legyünk naprakészek az aktuális internetes bűntények tekintetében.

Ezek már bizonyára lerágott csontnak hangzanak, de ezek azok a lépések, amivel nagyban csökkenthetjük a kockázatot. Ahogy az utcán is körültekintőek vagyunk, úgy a virtuális világban is körültekintőnek kell lennünk, legyenek ezek tiszavirág életű akár lakóhelybeli csalások vagy régóta fennálló módszerek.

Azonban saját magunk biztosítása csak egy dolog, a számítógépet kevésbé járatosan használó ismerőseink vagy családtagjaink még nagyobb veszélyben vannak. Az interneten elérhetőek oktatóanyagok külön nekik, hogy ők is könnyen megtudják érteni, milyen formában találkozhatnak a veszélyekkel. Bármelyik internetes keresőt használva az „Internet Safety for Seniors” kifejezést beírva számtalan hasznos bemutatót lehet találni ezzel kapcsolatban.

A védekezésben is megjelenik Mesterséges Intelligencia, ha támadáshoz tudják használni, akkor védekezéshez is, például már léteznek szoftverek, amik azt próbálják megállapítani, hogy a bevitt szöveg egy ember által lett írva vagy generálva lett MI által. Ez segítséget nyújthat akkor, amikor egy adathalász levél érkezik és a szövegezéséről nem tudja az ember teljes bizonyossággal eldönteni, hogy ki írta, ez szűrőként beépítve, sokat tud segíteni a levelezőrendszer használata közben ilyen helyzetben. Ezek egyelőre nem tökéletesek, bár egy novemberben megjelent tanulmány szerint egy új szoftver képes nagy pontossággal megállapítani tudományos cikkekről, hogy ember vagy gép írta-e. (Desaire et al., 2023)



21. ábra: Különböző MI Detektorok hatékonysága
Forrás: https://doi.org/10.1016/j.xcrp.2023.101672

Az itt látható ábra azt mutatja, hogy mekkora bizonyossággal tudja megmondani a program, hogy gép által generált-e a szöveg, amit elé raktak, az itt feltüntetett esetben kémiai tudományos cikkek elemzését nézték meg. A diagram úgy épül fel, hogy bal

oldalon van a két ember által írt cikk, középen (P1) MI generált szöveg, ami úgy készült, hogy a nyelvi modell beviteli mezőjébe csak egy címet írtak és az létrehozta a tudományos cikket, jobb oldalon pedig (P2), a beviteli mezőbe ember által írt szövegből teljes kivonatokat, bekezdéseket raktak be és a Mesterséges Intelligencia legenerált egy új szöveget belőlük. A színek jelölik, hogy melyik szoftvert használták a megállapításra, az oszlopok alatt megtalálható szöveg pedig azt jelzi, melyik programmal készültek a generált szövegek. Minden teszteset 50 darab dokumentumot tartalmazott, tehát ez a 3 fajta detektor minden esetben 50 szövegről hozott döntést és az eredmény százalékos arányban látható számunkra. (Desaire et al., 2023)

Habár már létezik a szoftver és remélve feltételezzük, hogy ez nem csak tudományos cikkekre működik, hanem köznapi nyelvezetre is, ennek az integrálása különböző környezetekbe nem fog megtörténni a következő napra virradóra, ezáltal nem vagyunk védve a gép által írt szöveges átverések ellen, valamint ezek az átverések ember által írott verziói is léteznek, csak azok kevesebb számban vannak jelen, az automatizáció hiánya miatt, ezért jelenleg a legfontosabb fegyverünk a kellő körültekintés és a lehetőségszerinti önfejlesztés.

A vállalatokon belül ez saját tapasztalatom szerint egy igen elterjedt módszer, évente el kell olvasni oktatóanyagokat és meg kell csinálni a hozzájuk tartozó kérdéseket a végén. Ezek szólhatnak adatvédelemről, belső házirendről, GDPR-ról vagy akár tűz esetén szükséges teendőkről is, minden oktatással eltöltött perc csak hasznunkra vállhat hosszútávon, elsősorban természetesen a cég saját érdeke a megfelelő oktatás az információ biztonság terén, de ez egyúton saját magunk hasznára is válik.

Utolsó dologként a Deepfake típusú képeket és videókat kell megemlíteni, aminek a tisztázása még nagyobb nehézséget okozhat. Az interneten megtalálható néhány oldal, ahol Deepfake videókat és hangsávokat lehet hallgatni és megpróbálni eldönteni, melyik oldalhoz tartoznak (https://detectfakes.media.mit.edu/), ez kiváló lehetőség arra, hogy teszteljük önmagunkat, de ha pontokba szedve szeretnénk tudni a jeleket akkor azok a következők: (Matt Groh, 2023)

- a száj körülötti terület hasonlósága az arc más részeihez,
- a fej forgásánál az árnyékok vetülése,
- szemüveg lencséjének különös tükröződése,
- a mondanivalóhoz illő arc- és kézmozgás,
- ajak mozgásának természetessége.

Csak azt tudjuk megismerni, amit sokszor használunk, ez igaz az internet egészére, hogy felismerjük a sorból kilógó mintákat otthonosan kell éreznünk magunkat a világhálón. Ez sok időt és figyelmes használatot igényel, ami nem mindenki számára az alapvető módja az internetezésnek, ezért körültekintőnek és előrelátónak kell lennünk az ismeretlenben, de voltaképpen ez mindenkire egyformán vonatkozik.

7. ÖSSZEFOGLALÁS

A dolgozat végéhez érve egy tisztább képet kapunk a Mesterséges Intelligenciáról, annak működéséről és veszélyeiről. Bemutatásra kerültek a technológia építőkövei, hogy mi tette lehetővé az utóbbi időben ugrásszerű terjedését, milyen negatív hatásai vannak és hogy hogyan is kell hozzáállnunk ehhez a témához. Tisztázásra kerültek a definíciók, mint például a gépi tanulás, Deep Learning, Deepfake, különbséget tettünk data mining és data science között, valamint pár jövőbeni alkalmazási területet is át tekintettünk.

A Mesterséges Intelligencia lassan, de biztosan átformálja, revolúcionizálja a munkaerőpiacot és hatással van mindennapi életünkre is. Sajnos ezek mellett megjelennek a negatív hatások is, amik nem kerülhetik el sem a vállalatok, sem a hétköznapi emberek figyelmét. Fegyverként használják és még kifinomultabb bűncselekményeket visznek véghez vele még nagyobb volumenben.

Megnéztük az egyénekre gyakorolt hatását, amivel a mindennapjainkban mi is találkozhatunk és szó volt a szervezetekre gyakorolt hatásáról is, milyen veszélyeknek vannak kitéve a szervezetek, milyen nehéz dolguk van az összes munkavállalót megvédeni a külső hatásoktól és milyen könnyen keletkezhet milliós kár egy figyelmetlen kattintás okán. A dolgozat két fő csoportjához tartoztak konkrét példák is, hogy hogyan történnek meg ezek az esetek egy szempillantás alatt a való életben. Láthattunk egy kisebb kitekintést a magyarországi információbiztonsági helyzetre. Statisztikákat sorakoztatott fel, a bűncselekményekkel kapcsolatban, külön kitért a 60 év feletti korosztályra, akik egy fokkal nehezebb helyzetben vannak a mai világban. Saját kérdőívből is lehetett tenni megállapításokat, amik gyakran párhuzamosak voltak az interneten talált, FBI által közölt statisztikákkal. A végén a védekezésről is szó esett, hogyan legyünk óvatosak az interneten, milyen támpontok alapján tudjuk beazonosítani a hamis média tartalmat, legyen az kép vagy esetleg videó. A kiberbiztonság hangsúlyozása egy kulcs mondanivaló az egész dolgozatban, amire nem lehet elégszer felhívni a figyelmet.

A Mesterséges Intelligencia fejlődésével és a nehezen belátható jövőbeni útjával kapcsolatban csak találgatni lehet, de a szabályozások előkészítései már megkezdődtek és ezek országokat átívelő egyezmények alapján kerülnek megvalósításra a jövőben.

Fontos az egységes keretrendszer a még el nem készült technológiák és a már elkészültek egységbe zárása érdekében. Ha a Mesterséges Intelligenciának ennyi mindent megtanítottak már az internetről, akkor az etikus és a fair működés is elérhető kellene, hogy legyen. Jelenlegi helyzetben teljes káosz uralkodik ezen a területen, a pornográf tartalmat megvalósító Deepfake videók készítése semmilyen jogszabályba nem ütközik, pedig nemes egyszerűséggel életeket tehet tönkre.

IRODALOMJEGYZÉK

1. ZekiaTech (2019): An introduction to Deep Learning, Machine Learning, and AI https://www.zekiah.com/insights/data-analytics/an-introduction-to-deep-learning-machine-learning-and-ai (Elérés dátuma: 2023.09.20)
2. WITSEC szakmai nap (2023): Az AI Chatbotok kora https://youtu.be/Yay7t4g-Ja8?si=EwvcLd5gn4sLDyF_ (Elérés dátuma: 2023.11.10)
3. The New York Times (2022): How China's Surveillance Is Growing More Invasive https://youtu.be/Oo_FM3mjBCY?si=Co3ZcVopCLYE1TpV (Elérés dátuma: 2023.11.15)
4. Maggie Miller (2020): FBI sees spike in cyber crime reports during coronavirus pandemic https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic/ (Elérés dátuma: 2023.10.05)
5. Cloudfactory (2017): The 3 Forces that Brought AI to Life (And Why it's Only Now Changing the World): https://blog.cloudfactory.com/3-forces-brought-ai-to-life (Elérés dátuma: 2023.10.15)
6. Deepgram (2023): Tensor Processing Unit (TPU) https://deepgram.com/ai-glossary/tensor-processing-unit-tpu
7. (Elérés dátuma: 2023.10.20)
8. EQUIFAX (2023): 8 Types of Identity Theft You Should Know https://www.equifax.com/personal/education/identity-theft/articles/-/learn/types-of-identity-theft/ (Elérés dátuma: 2023.11.10)

9. Eszteri & István (2016): Identity Theft in the Virtual World: Analysis of a Copyright Crime in Second Life from the Perspective of Criminal Law and IT Forensics
https://doi.org/10.1556/2052.2016.57.4.7
10. Christoph Bregler (1997): Video Rewrite: Driving Visual Speech with Audio
https://chris.bregler.com/videorewrite/
(Elérés dátuma: 2023.10.18)
11. Supasorn Suwajanakorn, Steven M. Seitz, és Ira Kemelmacher-Shlizerman (2017): Synthesizing Obama: Learning Lip Sync from Audio. ACM Trans, Cikk 95, 13. oldal
https://dx.doi.org/10.1145/3072959.3073640
12. Internet Crime Complaint Center (2022):
https://www.ic3.gov/Home/AnnualReports?redirect=true
(Elérés dátuma: 2023.11.12)
13. FORTINET (2023): 19 Types of Phishing Attacks
https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks
(Elérés dátuma: 2023.11.05)
14. Ahmed Aleroud, Lina Zhou (2017): Phishing environments, techniques, and countermeasures: a survey, Computers & Security
http://dx.doi.org/doi:%2010.1016/j.cose.2017.04.006
15. David Sancho és Vincenzo Ciancaglini (2023): Hype vs. Reality AI in the Cybercriminal Underground
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hype-vs-reality-ai-in-the-cybercriminal-underground
(Elérés dátuma: 2023.10.30)
16. Farhan A. Alenizi, Shirin Abbasi, Adil Hussein Mohammed, Amir Masoud Rahmani (2023): The artificial intelligence technologies in Industry 4.0: A taxonomy, approaches, and future directions
https://doi.org/10.1016/j.cie.2023.109662
17. Michelberger Pál, & Lábodi Csaba. (2012): Vállalati információbiztonság szervezése, Vállalkozásfejlesztés a XXI. században, II.(10), 241-302.o

18. EUROPOL (2021): Internet Organised Crime Threat Assessment (IOCTA) https://doi.org/10.2813/113799
19. Norah Saud Al-Musib, Faeiz Mohammad Al-Serhani, Mamoona Humayun, N.Z. Jhanjhi (2021): Business email compromise (BEC) attacks https://doi.org/10.1016/j.matpr.2021.03.647
20. Proofpoint (2020): What Is Email Account Compromise (EAC)? https://www.proofpoint.com/us/threat-reference/email-account-compromise (Elérés dátuma: 2023.11.02)
21. Tom Huddleston Jr. (2019): How this scammer used phishing emails to steal over $100 million from Google and Facebook https://www.cnbc.com/2019/03/27/phishing-email-scam-stole-100-million-from-facebook-and-google.html (Elérés dátuma: 2023.11.03)
22. Taskade (2023): AI HTML Code Generator https://www.taskade.com/generate/programming/html-code (Elérés dátuma: 2023.11.25)
23. FORTINET (2023): Cyber Threat Predictions for 2023 An Annual Perspective by FortiGuard Labs https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-threat-prediction-2023.pdf (Elérés dátuma: 2023.12.03)
24. Bruce Schneier (2023): The Internet Enabled Mass Surveillance. AI Will Enable Mass Spying https://www.schneier.com/essays/archives/2023/12/the-internet-enabled-mass-surveillance-ai-will-enable-mass-spying.html (Elérés dátuma: 2023.11.23)
25. RAND Europe (2020): The Future of Cybercrime in Light of Technology Developments https://doi.org/10.7249/RRA137-1
26. Philip Treleaven et al. (2023): The future of Cybercrime, AI and Emerging Technologies are creating a Cybercrime tsunami http://dx.doi.org/10.2139/ssrn.4507244

27. Szemán László János (2020): Magyar Nemzet: Gyurcsányék szerepét vizsgáltatná a romagyilkos
https://magyarnemzet.hu/belfold/2020/03/gyurcsanyek-szerepet-vizsgaltatna-a-romagyilkos
(Elérés dátuma: 2023.11.20)
28. Diptiben Ghelani (2022): Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review. American Journal of Science, Engineering and Technology. Vol. 3, 12-19 oldal
https://doi.org/10.11648/j.XXXX.2022XXXX.XX
29. Ashley Pugh (2023): 8 ways to fight cybercrime
https://www.e-careers.com/connected/8-ways-to-fight-cybercrime
(Elérés dátuma: 2023.12.01)
30. Heather Desaire, Aleesa E. Chua, Min-Gyu Kim, and David Hua (2023): Accurately detecting AI text when ChatGPT is told to write like a chemist
https://doi.org/10.1016/j.xcrp.2023.101672
31. Matt Groh (2023): Detect DeepFakes: How to counteract misinformation created by AI
https://www.media.mit.edu/projects/detect-fakes/overview/
(Elérés dátuma: 2023.11.28)

TARTALMI KIVONAT

A dolgozat bemutatja a jelenlegi helyzetét a Mesterséges Intelligenciával átszőtt kiberbűnözésnek, hogyan került be mindennapjainkba a technológia és milyen dolgokra képes a mai világban. Négy részre tagolt, foglalkozik az egyénekre gyakorolt hatásával, a vállalatokra és szervezetekre gyakorolt befolyással, ezen kívül jövőbeni predikciókat kíván tenni a majdani alakulásról és tanácsokat ad a védekezéshez, hogy lehet felkészülni ellene, mik az ismertetőjelei. A dolgozat elolvasása azoknak ajánlott, akik szeretnének egy közérthető, de ugyanakkor szerteágazó ismeretanyagot tudásuk részévé tenni. A Mesterséges Intelligencia létrejöttétől egészen a jövőbeni trendekig átfogóan foglalkozik a témával, jelentős hangsúlyt fektetve a társadalmi kockázatokra, ezen belül pedig ennek a kiberbűnözési aspektusára.

SUMMARY

This examination presents the current state of the cyber criminalistic world, that is undergoing a change thanks to the Artificial Intelligence. It tries to find the answer for questions, like how it came to our everyday lives, what made it possible to spread so intensely. Four main topics can be found in the paper: how does it affect individuals, how does it affect organizations and institutions, also tries to make future predictions regarding the relationship of cybercrime and Artificial Intelligence, and in the last topic presents us answers on how to keep an eye on the ever-evolving virtual network, so that we do not fall in the trap of threat actors. This paper should be read by those, who would like to have an articulate read on this new technology and want to have a wider range of knowledge by their side.