ÓBUDAI EGYETEM

Keleti Károly Gazdasági Kar
Vállalkozásfejlesztés és Infokommunikációs Intézet

SZAKDOLGOZAT

ÓE-KGK
2023

Hallgató neve: **Csárdás Ferenc László**
Hallgató törzskönyvi száma: **T123456/FI12904/G**

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Óbudai Egyetem
Keleti Károly Gazdasági Kar
Vállalkozásfejlesztés és Infokommunikációs Intézet

SZAKDOLGOZAT FELADATLAP

Hallgató neve: Csárdás Ferenc László
Szakdolgozat száma: [redacted]
Törzskönyvi száma: T007104/FI12904/G **Neptun kódja:** [redacted]

Szak: Gazdaságinformatikus
Specializáció: Vállalatinformatikai specializáció

A dolgozat címe: Titkosítás aktuális fejlődésének trendje és problematikája
A dolgozat címe angolul: Trends and problems of the current development of encryption
A feladat részletezése:
1. Hasonlítsa össze a szimmetrikus és aszimmetrikus titkosítás elméleti alapjait!
2. Tárja fel napjainkban a titkosítások felhasználási területeit!
3. Tervezzen meg a forrásfeldolgozás alapján egy laikusok körében lekérdezésre kerülő kérdőívet!
4. A forrásfeldolgozás tükrében elemezze a kérdőív kitöltéséből származó válaszokat!

Intézményi konzulens neve: Horváth Ádám Béla

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

A szakdolgozat: Nem titkos.

Óbudai Egyetem Keleti Károly Gazdasági Kar Vállalkozásfejlesztés és Infokommunikációs Intézet Budapest

Kiadva: Budapest, 2023. 11. 29. P.H.

.....
Intézetigazgató

A dolgozatot beadásra alkalmasnak találom:

.....
belső konzulens

.....
külső konzulens

ÓBUDAI EGYETEM

Keleti Károly Gazdasági Kar

HALLGATÓI NYILATKOZAT

Alulírott Csárdás Ferenc László (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. december 11.

hallgató aláírása

TARTALOMJEGYZÉK

1. BEVEZETÉS 1

2. TITKOSÍTÁS AKTUÁLIS FEJLŐDÉSE 4

2.1. Titkosítás 4

2.2. Titkosítás az IoT és a 5G hálózatokban 5

2.3. HTTPS titkosítás 8

2.3.1. Mi a különbség a HTTPS és a HTTP között? 9

2.3.2. HTTPS Titkosítás 10

2.3.3. HTTPS aszimmetrikus és szimmetrikus titkosítás 12

2.3.4. Digitális tanúsítványok 13

2.3.5. Integritás 14

2.3.6. SSL/TLS összefoglalás 14

2.4. SSL/TLS a levelezésben 15

2.4.1. Email biztonsági kockázatok 16

2.5. Kétlépcsős hitelesítés 17

2.5.1. 2FA Kockázatai 19

2.5.2. Kétlépcsős hitelesítés beállítása Google fiókban 20

2.5.3. Basel III kötelezővététele a Banki rendszerekben 21

2.6. Otthoni és kisvállalati hálózatok biztonsága 22

2.6.1. Otthoni Hálózatok felépítése és működése 22

2.6.2. Kisvállalati hálózatok felépítése és működése 23
2.6.3. Összehasonlítás az otthoni hálózatot a kisvállalati hálózattal 25
2.6.4. Kisvállalti hálózat építése 25
2.7. Hálózati kapcsolatok: vezetékes, vezetéknélküli 27
2.7.1. Vezetékes hálózatok működése 27
2.7.2. Vezetéknélküli hálózatok 31
2.7.3. WPA3 és a WPA2 különbségei 32
3. TITKOSÍTÁS PROBLEMATIKÁJA ÉS KIHÍVÁSAI - KÉRDŐÍV 33
3.1. Kutatás bemutatása 33
3.2. Eredmények áttekintése 42
3.2.1. „Hogyan érint téged a titkosítás a mindennapi életben?” 42
3.2.2. Milyen mértékben érzik magukat a felhasználók biztonságban 45
3.2.3. „Mennyire érdekel téged a kvantumtitkosítás és annak fejlesztése?” 47
3.2.4. Következtetés 49
4. ÖSSZEFOGLALÁS 50
IRODALOMJEGYZÉK I
TARTALMI KIVONAT IV
SUMMARY IV

ÁBRAJEGYZÉK

1. ábra A Mirai által fertőzött IoT-eszközökkel elkövetett támadás vázlata 5

2. ábra A mobilcellás rendszerek evolúciója 6

3. ábra Autentikáció az 5G hitelesítési eljárásban 8

4. ábra Nem biztonságos weboldal előtti figyelmeztetés 9

5. ábra SSL/TLS kézfogás kliens és szerver oldali kommunikáció folyamata 11

6. ábra mail-tester.com eredmény, hiányos DMARC rekorddal 16

7. ábra aktív kétlépcsős hitelesítés google fiókban 21

8. ábra NordLayer működésének rajza 24

9. ábra Ethernet kábel kategóriák 27

10. ábra Kábel árnyékolási típusok 28

11. ábra RJ45 és GG45 csatlakozó 30

12. ábra A kitöltők neme (n=134) 33

13. ábra A kitöltők életkora (n=134) 34

14. ábra A kitöltők lakhelye (n=134) 35

15. ábra A kitöltők iskolai végzettsége (n=134) 36

16. ábra A kitöltők érintettsége a titkosítással a hétköznapi életben (n=134) 36

17. ábra A kitöltők biztonsági érzete az online tevékenységeik során (n=134) 37

18. ábra A válaszadóknak volt-e aggodalma az online személyes adatainak biztonsága miatt (n=134) 37

19. ábra A válaszadók érdeklődése a kvantumtitkosítás iránt (n=134) 38

20. ábra Kvantumszámítógép gyorsasága (n=134) 39

21. ábra Válaszadók viszonyulása a titkosítási módszerekhez (n=134) 39

22. ábra Mennyire tudatos felhasználó a kitöltő? (n=134) 41

23. ábra A kitöltő szerint miért fontos az adatok titkosítása az online térben? (n=134) 41

TÁBLÁZATOK JEGYZÉKE

1. táblázat Internethasználók aránya [a 16–74 éves népesség százalékában] 3

2. táblázat Mennyire tudatos felhasználó a kitöltő? 40

*3. táblázat Hogyan érint téged a titkosítás a mindennapi életben? * Nem* 43

*4. táblázat Hogyan érint téged a titkosítás a mindennapi életben? * Lakhelye* 44

*5. táblázat Milyen mértékben érzed biztonságban magad az online tevékenységeid során? * Életkor* 46

1. BEVEZETÉS

Napjainkban az információbiztonság beli kérdésekre nem fektetnek a fontosságára akkora hangsúlyt az emberek. A home office kitüntetett szerepet játszik a mai kor munkahelyi struktúrájában. Ezért elengedhetetlen foglalkozni a biztonságos adatforgalom kérdés körével, mivel rengeteg cég, amelyek magán és cég adatok felhasználásával foglalkoznak és különböző pénzforgalmakat bonyolítanak le. A személyiségi jogok tiszteletben tartásától kezdve a hekkerek rosszindulatáig minden területre kiterjedő biztonsági intézkedések szükségesek, mind a magán emberek körében, mind cégek, hivatalokat körében. A felhasználók leginkább a sok jelszó miatt félnek, hogy elfelejtik. Ezenfelül nem tudják, hogy hogyan védekezhetnének, a mindennapokban fellelhető kis biztonsági rések ellen.

Jó magam is tapasztaltam a nem megfelelő biztonsági intézkedések figyelmen kívül hagyásából adódó visszaéléseket, ami rengeteg kellemetlenséggel járt, nem beszélve a helyrehozatalához felhasznált rengeteg időről és munkáról.

Próbálták már feltörni a Google fiokomat, de szerencsére be volt kapcsolva a kétlépcsős hitelesítés. Viszont ki volt kapcsolva a fiókomon egy védelmi funkció, így hozzáfértek a levelezésemhez. Így máris hozzáférhettek az adataimhoz. Ezokból sokkal tudatosabban használom az internet különböző szolgáltatásait, hogy hogyan a legbiztonságosabb az interneten aktívan jelen lenni. Az informatikai eszközök és szolgáltatások tudatos és körültekintő használatához hozzátartozik a rendkívüli esetekre való felkészülés is. Személyes, „üzletfolytonosság” és katasztrofa elhárítás.

Az adatlopás és zsarolóvírusok ismét reneszánszát éli napjainkban. Leggyakoribbak a telefonhívások, amiben valaki kiadja magát, hogy ő egy hozzátartozó és balesetet szenvedett. Vagy valami olyan történetet találnak ki, ami bárkivel megtörténhet és így pénzt zsarolnak ki, hogy utaljanak nekik azonnal amennyit csak lehet. Ezenkívül a csomagja érkezett üzenetekkel is rengeteg adatot próbáltak megszerezni és kisebb mikrotranzakciókkal pénzt kicsalni.

Az OTP külön tartalmakat is létrehozott számunkra, hogy feltudjuk ismerni a csalókat. Az adathalász csalások és visszaélések formáit részletezi az oldal, hogy hogyan tudjuk felismerni a csalások formáit, hogyan védekezhetünk a csalások ellen, és mit tehetünk, ha a csalás áldozataivá váltunk. (OTP Bank, 2023)

Ezen technikákat fel kell ismernünk és ha nem figyelünk oda az ilyen apróságokra könnyen áldozatai lehetünk. Egy lehetséges megoldás például, hogy visszaellenőrizzük a rendeléseinket és már is átláthatunk az átverésen. Ha nem vagyunk leleményesek csőbe húzhatnak minket, mint például a telefonhívásokkal. Ezekben nekem is volt részem és könnyen felismerhetőek, mert elszólják magukat. Lehetséges megoldás, hogy letesszük és visszahívjuk a valós embert, aki elvileg bajban van és így azonnal visszatudjuk ellenőrizni a helyzet valóságát.

Ezek a csalások adatlopások, biztonsági problémák jellemzőek voltak már 2005-től, az emberiség 2005-2012 között kezdte el használni rohamosan az internetet/hálózatot. Ezek a felhasználói szám adatok azokból fontosak, mivel összeköthetjük, a sok felhasználó megjelenésével az adatlopások gyakoriságát. Az 1. táblázaton is látható, hogy 7 év alatt duplázódott Magyarországon az internetezők aránya. Továbbá a táblázaton látható még az Európai Uniós országok internetező felhasználók arányának a statisztikája.

A technológia olyan szinten függővé tett minket, hogy ma már nem tudnánk elképzelni a hétköznapjaink, vagy napjaink mobilok, tabletek, gépek nélkül. Van úgy, hogy egy nap akár 60x is felnyitjuk a készülékünket, esetenként előfordul, hogy napi 8 óra képernyőidőt is elérjük, ami rengeteg. Ez idő alatt sok biztonsági kockázattal találkozhatunk. A Covid19 teljes mértékben felforgatta a szokásainkat és rákényszerített bennünket az ekereskedelemre. Ezokból is pár hónap leforgása alatt több mint 50 ezer új magyar vásárló jelent meg az Elektronikus kereskedelemben. Az ekereskedelem első negyedévében 35%-kal nőt a 2019-es azonos időszakhoz viszonyítva. Későbbiekben ez csökkent, mivel rengeteg munkahely leépítés és bevételkiesés történt. (FinTechShow cikke, 2020)

Ország, országcsoport	2005	2006	2007	2008	2009	2010	2011	2012	2022
Magyarország	**37**	**44**	**51**	**58**	**59**	**61**	**67**	**70**	**89**
Ausztria	55	61	67	71	72	74	79	80	94
Belgium	58	62	67	69	75	78	82	81	94
Bulgária	..	24	31	35	42	43	48	52	79
Ciprus	31	34	38	39	48	52	57	61	90
Csehország	32	44	49	58	60	66	70	74	91
Dánia	77	83	81	84	86	88	90	92	98
Észtország	58	61	63	66	71	74	76	78	92
Finnország	73	77	79	83	82	86	89	90	97
Franciaország	..	47	62	68	71	75	78	81	91
Görögország	22	29	33	38	42	44	52	55	83
Hollandia	79	81	84	87	89	90	91	93	95
Horvátország	..	..	38	43	47	54	58	62	82
Írország	37	51	58	63	65	67	75	77	95
Lengyelország	35	40	44	49	56	59	62	62	87
Lettország	42	50	55	61	64	66	70	73	91
Litvánia	34	42	49	53	58	60	63	66	88
Luxemburg	69	71	78	81	86	90	90	92	98
Málta	38	38	45	49	58	62	68	69	92
Németország	65	69	72	75	77	80	81	82	92
Olaszország	34	36	38	42	46	51	54	56	58
Portugália	32	36	40	42	46	51	55	60	62
Románia	..	21	24	29	33	36	40	46	50
Spanyolország	44	47	51	56	59	64	66	69	72
Svédország	81	86	80	88	90	91	93	93	95
Szlovákia	50	50	56	66	70	76	74	77	78
Szlovénia	47	51	53	56	62	68	67	68	73

1. táblázat Internethasználók aránya [a 16–74 éves népesség százalékában]

Forrás: A KSH adatai alapján saját szerkesztés

Kutatásom célja a hétköznapi biztonsági rések összegyűjtése és lehetséges védekezési módszerek bemutatása, illetve a jövőbeni lehetséges titkosítási problémák figyelemfelhívása.

2. TITKOSÍTÁS AKTUÁLIS FEJLŐDÉSE

2.1. Titkosítás

Olyan számítógép-művelet (algoritmus) alkalmazása, mely lehetővé teszi, hogy csak bizonyos felhasználók használhassanak meghatározott adatokat, illetve a titkosítással egy üzenetet is megváltoztathatunk úgy, hogy abból az eredeti üzenet csak valamilyen, kizárólag a küldő és a címzett által ismert eljárás segítségével fejthető vissza. (PALICZ, Tamás, 2020)

A titkosítás és biztonsági lehetőségekről, mint felhasználó és mint szolgáltató, is részletezni fogom, hogy mit tehetünk adataink védelméért. Továbbá, hogyan tudjuk megóvni illetéktelenektől az adatainkat. Felhasználói részről, ami nem csak jelszó alapú, hanem kétlépcsős hitelesítés (2FA - Two Factor Authentication), vagyis jelszóra és/vagy emailben kapott kódra van szükségünk a belépéshez.

Szerveroldalról ennél picit komplexebb a titkosítás, mivel itt fizikailag is és szoftveresen is kell tenni a biztonságért. Kulcs nélkül az adatok értelmezhetetlenek, értéktelenek, feltörésre rengeteg módszer létezik, de időigényesek, vagy eredménytelenek.

A titkosítást sok helyen alkalmazhatjuk, például az internetes kommunikációban, adatbázisokban, banki tranzakciók során, vagy éppen saját informatikai eszközeinken, ami telefontól kezdve akár egy saját kis belső hálózat is lehet. A modern informatikai rendszerek már megkövetelik a titkosítást annak érdekében, hogy védelmet nyújtsanak az adatlopás, kémkedés és egyéb fenyegetések ellen.

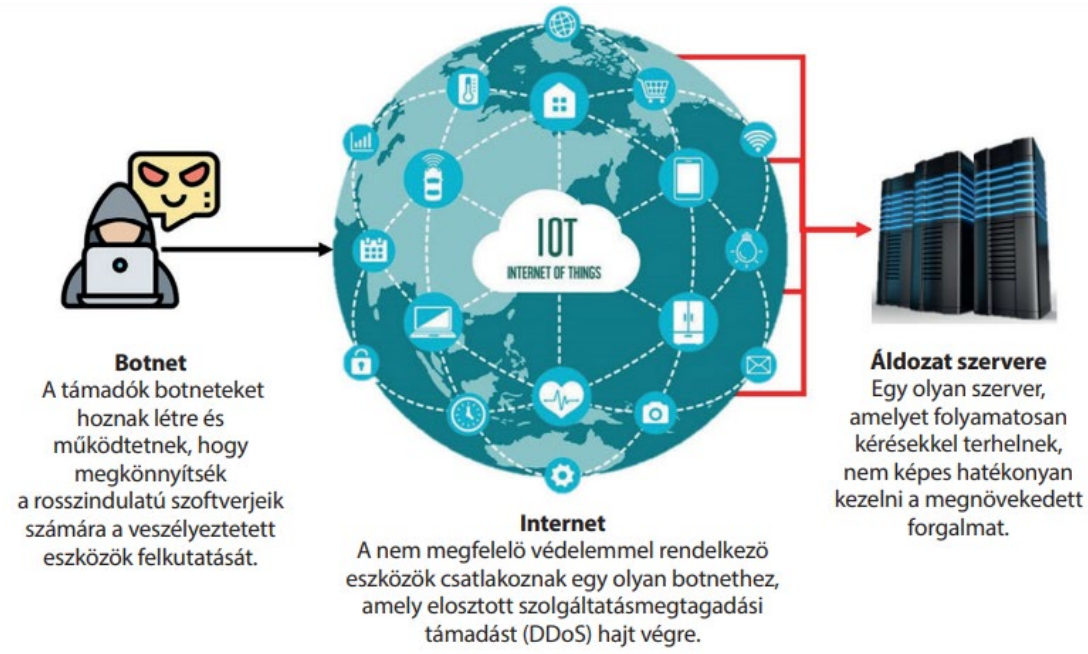
„Titkosítás: Célja a lehallgatás megakadályozása, pontosabban annak biztosítása, hogy egy lehallgatást végző támadó ne értse meg a lehallgatott üzenetek tartalmát.” (Vajda István, 2005)

A titkosítás két fő elemből áll: az adatok átalakításából és a kulcs használatából. Az átalakítás során az eredeti adatokat manipuláljuk, hogy azok mások számára/illetékteleneknek ne legyenek értelmezhetőek. A kulcs egy olyan speciális információ, amivel lehetséges az eredeti adatok visszafejtése. A kulcs nélkül a titkosított adatok értelmetlenek és értelmezhetetlenek.

2.2. Titkosítás az IoT és a 5G hálózatokban

Az IoT(Internet of Things) definíciója szerint ezek az eszközök a tárgyak azon csoportjába tartoznak, amelyek összekapcsolódva infrastruktúrát vagy infrastruktúra-csoportot alkotnak, amely lehetővé teszi az összes eszköz számára, hogy összekapcsolódjanak, kezeljék és hozzáférjenek az összes általuk generált vagy gyűjtött adathoz. Az IoT minden összekapcsolt technológiai eszköz, gép és kapcsolat fogalma. (Tóth András, 2018)

Az IoT-eszközök nagy részénél a legfőbb szempont, hogy a költségeket a lehető legalacsonyabban tartsák. Ez sok terméknél/eszköznél gyenge, rossz konfigurációjú és nyitott kialakítású. Vagyis minimális, vagy éppenséggel semmilyen védelmi funkcióval nem rendelkezik. Ezáltal következtethetünk arra, hogy nyitottak az internet felé. Ezen információ tudatában a hackerek figyelmét is felkeltette ez a könnyen támadható biztonsági rés, amellyel jelentős anyagi károkat is tudnak okozni.



1. ábra A Mirai által fertőzött IoT-eszközökkel elkövetett támadás vázlata

Forrás: The Cost of Compromise, 2017

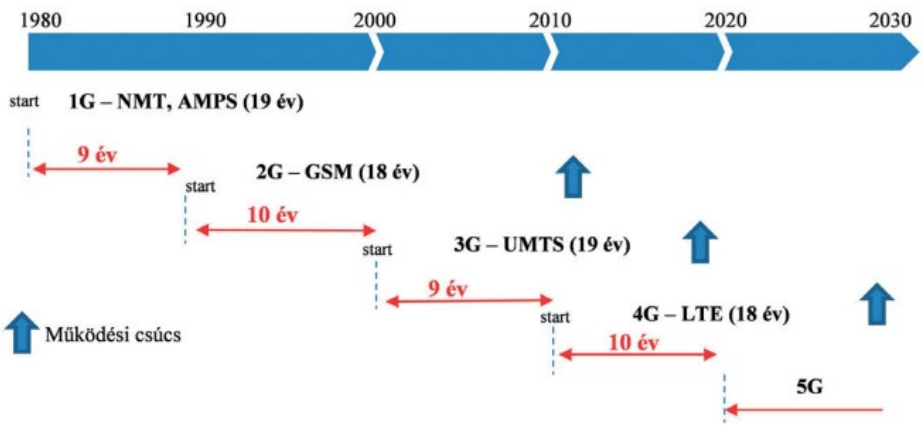
Erre 2016-ban meg is történt a Mirai Botnet támadás, amelynek majdnem félmillió IoT-eszköz felett vették át az irányítást, ezzel kialakítottak egy eddig még nem látott

botnethálózatot. A Mirai és egyéb változatai okozzák a legnagyobb DDoS(Distributed Denial of Service) túlterheléses támadásokat. Mirai Botnet támadásának az egyszerűsített váza látható az 1. ábrán.

A sérülékenységre az internet biztonságát tekintve kijelenthetjük, hogy a hálózatok komplexitása miatt, nem lehetséges garantálni a biztonságot. A biztonsági előírásokat együttesen használva lehetséges a hatékony védekezés. A napjaink legbiztonságosabb megoldása a VPN-kiszolgálók (Virtual Private Network), virtuális titkosított csatornát hoznak létre a felhasználók és az IoT-eszköz között.

A hálózatot viszont nem lehetséges csak hardverrel védeni, szükség van olyan rendszerre, amely átvizsgálja a szoftvert, és kisegíti az IoT-eszközök védelmirendszerét. Mindezek mellett olyan eszközt válasszunk, amelynek van gyártói támogatása. Folyamatos firmware- és szoftver-frissítés is beleértetendő a támogatásba.

A mobilhálózat szabványokat 10 évente vezetik be. Az 5G szabvány 2020-ban került bevezetésre, és folyamatosan építik és bővítik a rendszert. A 2. ábrán látható az eddigi hálózati szabványok evolúciója. (Nagy Lajos, 2021)



2. ábra A mobilcellás rendszerek evolúciója

Forrás: LAJOS, Nagy; 5G MOBILE SYSTEM. Magyar Tudomány

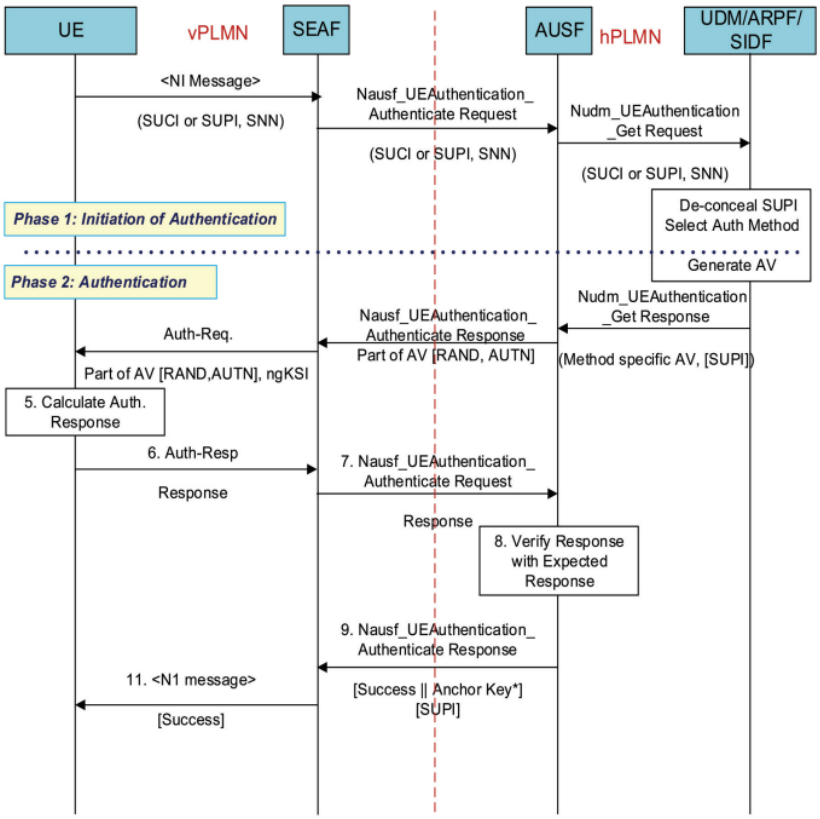
A fő oka a folyamatos fejlesztésnek a megnövekedett sávszélesség igénye. Az 5G hálózatok adaptív spektrumallokációs technikákkal és több antennás (MU-MIMO - Multi-User, Multiple Input, Multiple Output) megoldásokkal kiegészített

mobilcellás rádióhálózat. A rádiófrekvenciás spektrum hullámhossztartományával való kiterjesztése miatt, lehetséges a nagyobb sávszélesség.

„A "Multi-User, Multiple Input, Multiple Output" rövidítése. A MU-MIMO egy olyan technológia a vezeték nélküli kommunikációban, amely lehetővé teszi, hogy egy Wi-Fi router egyszerre több eszközzel kommunikáljon, ahelyett, hogy az eszközök között váltana. Ez javítja a teljesítményt, valamint növeli a kapacitást és a hatékonyságot sűrű vezeték nélküli környezetekben.” (Alza, 2023)

Az 5G biztonsági szabvány számos újszerű biztonsági lépést tartalmaz. A honos hálózat az eszközt tudja hitelesíteni a roamingolás során. Az Egységes Hitelesítési keretrendszer lehetővé teszi, hogy függetlenül a hozzáférés módjától képes legyen hitelesíteni az eszközt. Az EAP (Extensible Authentication Protocol) beépített támogatásával új hitelesítési módok alkalmazhatóak. A SEAF (Security Anchor Function) úgy teszi lehetővé az eszköz újra hitelesítését, hogy az eszköz a hálózatok között mozog, közben nem ismétli meg a teljes folyamatot. (Anand R. Prasad, 2018)

Az 5G hálózat biztonsági rendszere egy rendkívül összetett rendszer, lásd 3. ábrán, a hitelesítési folyamata, amely tartalmazza, az újra hitelesítést is (6. pont).

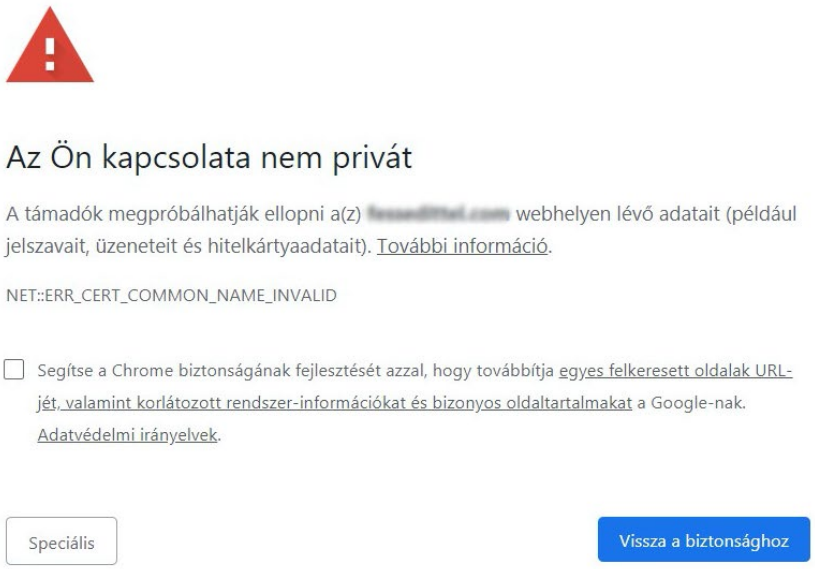


3. ábra Autentikáció az 5G hitelesítési eljárásban

Forrás: PRASAD, Anand R., et al. 3GPP 5G security. Journal of ICT Standardization, 2018

2.3. HTTPS titkosítás

A HTTPS (HyperText Transfer Protocol Secure) a HTTP biztonságos változata, amely titkosításhoz és hitelesítéshez az SSL/TLS protokoll-t használja. Az HTTP alapértelmezetten a 80-as portot használja. Ellentétben a HTTPS-el, ami már a 443-as portot használja. A biztonsági protokoll lehetővé teszi, hogy érzékeny adatokat biztonságosan tudjon továbbítani az interneten. A különböző tranzakciók során (online vásárlás) különösen fontos, az adataink biztonsága. Napjainkban már szinte minden weboldal HTTPS protokollt használ. Ahol esetleg nincs ilyen protokoll ott figyelmeztet minket a webböngésző, hogy veszélynek vagyunk kitéve és térjünk vissza a biztonságos oldalra. A 4. ábrán látható milyen egy lehetséges kimenetele a hibás tanúsítványnak.



4. ábra Nem biztonságos weboldal előtti figyelmeztetés

Forrás: Saját forrás (2023)

De ha gyakorlott felhasználók vagyunk lehetőségünk van „speciális” gomb után tovább jutni a nem biztonságos weboldalra. Ilyen helyeken nem ajánlott a kártyás fizetés, sem semmilyen személyes adat megadása. Továbbá figyelmeztetés akkor is előfordulhat, ha esetleg lejár az SSL tanúsítvány, ezáltal érvénytelen és veszélyes is lehet.

2.3.1. Mi a különbség a HTTPS és a HTTP között?

A HTTP titkosítás nélkül továbbítja az adatokat. Nyíltan és olvasható formában cserélődnek az adatok a számítógép és a weboldal szervere között. A titkosítás hiánya okán, bárki hozzáférhet a kommunikációs csatornához. Könnyen ellophatják, lehallgathatják és akár meg is változtathatják az adatokat. A HTTPS esetén, már titkosítva vannak az adatok a továbbítás során, ezokból a harmadik felek nem tudják könnyen megérteni, módosítani, ellopni az adatokat. A HTTPS alkalmazása növeli az adatintegritást, az azonosítást.

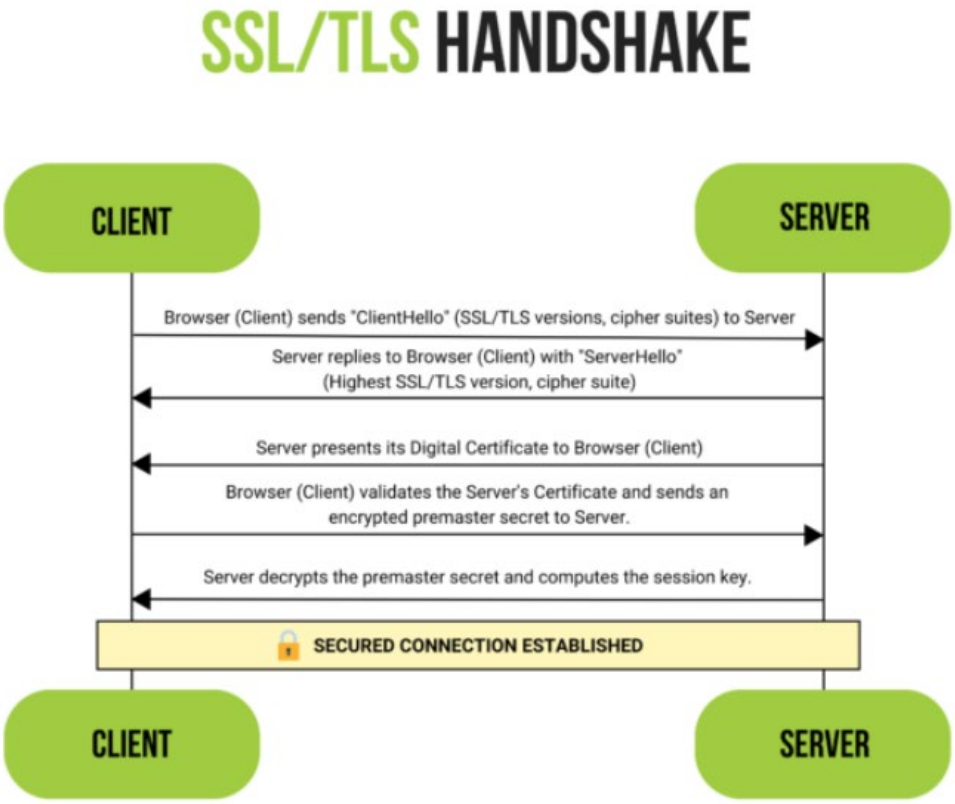
A HTTP/2 (eredeti nevén HTTP/2.0) a World Wide Web által használt HTTP hálózati protokoll főbb változata. A HTTP/2-t az Internet Engineering Task Force (IETF) HTTP-munkacsoportja (más néven httpbis, ahol a " bis " jelentése "kétszer") fejlesztette ki. A HTTP/2 a HTTP első új verziója a HTTP/1.1 óta, amelyet 1997-ben szabványosítottak az RFC 2068- ban. (HTTP/2, 2015)

2.3.2. HTTPS Titkosítás

A HTTP eredetileg szöveges protokollként tervezték, ezért nagyon érzékeny a lehallgatásra. Az SSL/TLS titkosítás a HTTPS által az interneten átmenő adat titkosítva halad át. Értelmezhetetlen egy harmadik félnek, beleértve a fogadását vagy az olvasását.

A TLS (Transport Layer Security) egy kriptográfiai protokoll, ami a kommunikáció biztonságát szolgálja az interneten. Az SSL (Secure Sockets Layer) protokoll továbbfejlesztett verziójaként tervezték, majd a két protokoll szinte egymásra volt építve. A TLS-t általában webböngészők és szerverek közötti biztonságos adatátvitelhez alkalmazzák. A TLS a TCP (Transmission Control Protocol) réteg felett helyezkedik el a hálózati kommunikációban. (George Danezis, 2009)

A TLS a modern, biztonságosabb változata az SSL-nek, és mindkét protokoll olyan titkosítási és hitelesítési módszereket biztosít, amely a biztonságos kommunikációt lehetővé teszi. A webszerver és a böngésző között egy megosztott titkos kulccsal kommunikálnak a nyilvános kulcsú kriptográfia és az SSL/TLS kézfogásával.



5. ábra SSL/TLS kézfogás kliens és szerver oldali kommunikáció folyamata

Forrás: SSL Kézfogás (2020)

A SSL/TLS kézfogás (SSL/TLS handshake) egy protokoll folyamat, amely a biztonságos kapcsolatért felelős. Az 5. ábrán láthatjuk, hogy milyen hívások lehetségesek a kliens és a szerver kommunikáció során.

A kézfogás folyamata az alábbi lépésekből áll:

1. Üdvözlő üzenet
2. Kliens azonosítás és tanúsítvány küldése
3. Szerver azonosító és tanúsítvány küldése
4. Kliens megerősítése és kulcsszerződés
5. Kapcsolat létrejött

Az SSL/TLS kézfogást tekinthetjük akár egy tárgyalásnak két fél között, amely során megállapítják a részleteket. Leggyakoribb eset egy webszerver és egy böngésző között

zajlik. Meghatározza, hogy az adott munkamenetben, lesz-e használva titkosítás, SSL/TLS, és ha lesz a verzióját is megállapítja. A Kommunikáció során többször ellenőrzi a szerver és a kliens is. Ezek a folyamatok a háttérben zajlanak, hogy a felhasználót véletlenül se zavarja össze. (Claude Castelluccia, 2006)

2.3.3. HTTPS aszimmetrikus és szimmetrikus titkosítás

Az aszimmetrikus titkosítás folyamata egy pár kulcsot alkalmaz, egy nyilvános és egy privát kulcsot, a titkosításhoz. A nyilvános kulccsal kódolt adatokat csak a privát kulccsal lehet visszafejteni. Ennek eredményeként biztonságosan továbbíthatók az adatok. A kézfogás folyamata során az aszimmetrikus titkosítás használatba kerül. Az aszimmetrikus titkosítási rendszereknek magas költségei miatt, nem alkalmasak teljes idejű és valós idejű biztonság létrehozására. A kézfogás alatt tehát a nyilvános kulcsot használják a titkosításhoz, a privát kulcsot pedig a visszafejtéshez, amely lehetővé teszi ezzel a két fél számára, hogy bizalmasan létrehozzák és kicseréljék az újonnan létrehozott "megosztott kulcsot". (K GUPTA, Kamlesh, 2011)

A szimmetrikus kulcs pedig egyetlen közös kulcsot alkalmaz az adatok titkosításához és visszafejtéséhez. A szimmetrikus titkosítás az aszimmetrikus titkosításnál gyorsabb. A SSL/TLS kézfogás során az aszimmetrikus titkosítást alkalmazzuk a szimmetrikus munkamenetkulcs biztonságos megosztására a résztvevő felek között. A munkamenet során ez az egyetlen megosztott kulcs szolgál a teljesítéshez, mely szimmetrikus titkosítást alkalmaz, és ennek köszönhetően biztosítja a biztonságos kapcsolatot a két fél között, amely jelentősen költséghatékonyabb. (Hazim Haddad, 2011)

Ezen titkosítást még lehet tovább fokozni a kölcsönösen hitelesített kézfogással, amely egy eléggé komplex téma, de egyszerűsítve fogom taglalni. Az alapmodell lehetővé teszi az ügyfelek számára, hogy biztonságosan kommunikáljanak. Azonban bizonyos titkosító csomagok további extra biztonságot követelnek meg. A kétirányú hitelesítéshez az ügyfélnek, illetve a szervernek is tanúsítványt és nyilvános kulcsot kell küldenie.

A kölcsönösen hitelesített kézfogás sokkal bonyolultabbá teszi a kézfogást, de van néhány eset, például két bank közötti biztonságos átutalások során, a titkosító csomagok ezt elvárják, és úgy ítélik meg, hogy extra biztonságra van szükség az adott körülmények

között. Ezáltal a kölcsönösen hitelesített kézfogás lehetővé teszi, hogy mind a két fél megerősítse egymás azonosságát, ami kritikus lehet az olyan érzékeny tranzakciók esetében, mint a pénzügyi átutalások a bankok között.

2.3.4. Digitális tanúsítványok

A digitális tanúsítványok hatalmas szerepet játszanak az online biztonságban, mivel ezek az eszközök lehetővé teszik az internetes kommunikáció és az adatátvitel biztonságosabbá tételét. A digitális tanúsítványok olyan elektronikus dokumentumok, amelyek digitális aláírást tartalmaznak, és azonosítják az adott entitást az online térben.

Ezek a tanúsítványok segítenek abban, hogy az online kommunikáció biztonságos legyen, és az embereket is be tudjuk azonosítani az úgynevezett közzétett nyilvános kulcs infrastruktúrában (PKI). A digitális tanúsítványok olyan elektronikus dokumentumok, amelyeket egy megbízható kiadó hoz létre, és egy biztonságos harmadik fél ellenőriz. Ezek a dokumentumok segítik azonosítani az adott személyt vagy szervezetet, és segít ellenőrizni, hogy a nyilvános kulcs valódi és megbízható.

Egy digitális tanúsítvány tartalmazza az entitás nyilvános kulcsát, adatait, és egy digitális aláírást a kiadó által. Amikor valaki egy másik féllel, vagy szerverrel biztonságosan szeretne kommunikálni, használhatja ezt a tanúsítványt azonosításra és az adatok titkosítására.

A digitális tanúsítványok alkalmazásai szerteágazóak. Az internetes böngészés során például egy weboldal tanúsítványát ellenőrizzük, hogy megbizonyosodjunk a weboldal hitelességéről és hogy adatainkat biztonságosan továbbíthatjuk. Ezenkívül az e-mail kommunikációban (pl. SSL/TLS port IMAP:995/POP:993 a 110 helyett) és az üzleti alkalmazásokban is gyakran alkalmazzák a digitális tanúsítványokat a biztonságos és hitelesített kapcsolatokhoz.

Továbbá azt is fontos megérteni, hogy a digitális tanúsítványok hozzájárulnak az internetes biztonság növeléséhez, nem csak számunkra biztosítva, hogy a kommunikáció szereplői valóban azok, akinek kiadják magukat és garantálva, hogy az információk csak

a kijelölt félhez jutnak el. Ezen keresztül a digitális tanúsítványok fokozzák az online bizalom és a személyes adatok védelmét a digitális térben.

2.3.5. Integritás

A HTTPS protokoll fontosnak tartja az adatok integritásának biztosítását, és ehhez különböző eszközöket alkalmaz. Minden egyes dokumentum, amelyet a HTTPS webszerver küld a böngészőnek, tartalmaz egy digitális aláírást. A digitális aláírás a dokumentum tartalmának ellenőrzését teszi lehetővé a böngésző számára, azért, hogy megállapíthassa, hogy a dokumentumon nem történt semmiféle változás esetleges harmadik fél által.

A kiszolgáló, amely a weboldalt szállítja, kiszámít egy kriptográfiai kivonatot és a digitális tanúsítványhoz mellékeli a dokumentum tartalmából egy részletet, vagy valami szabály szerint kiemel belőle értékeket. Ezt a kivonatot, nevezzük "hash"-nak, ami egy egyedi digitális ujjlenyomatot képez a dokumentumról. Ezt a hash-t a böngésző összehasonlítja a kiszolgálótól érkező értékkel és a böngésző által újra kiszámolt hash-t. Ha a két érték egyezik, akkor a dokumentum integritása sértetlen, nem történt módosítás a szállítás során. Amikor a böngésző megkapja a dokumentumot, ugyanezt a kivonatot számolja ki a kapott tartalomból.

Ez a digitális aláírás és integritásellenőrzés mechanizmus együttesen biztosítja, a felhasználók számára, hogy bizalommal tekinthessék meg a weboldalakon megjelenő tartalmakat. Az adatok integritásának ellenőrzése elengedhetetlen az online biztonság szempontjából, különösen olyan területeken, mint ahogy már említettem pénzügyi tranzakciók vagy személyes adatok kezelése során.

2.3.6. SSL/TLS összefoglalás

Az SSL/TLS kézfogás folyamata bonyolult, de lényege, hogy biztosítsa az online tevékenységeink biztonságát. Minden olyan szituációban, amikor online vásárlást végzünk, bejelentkezünk az e-mail fiókunkba vagy privát beszélgetéseket folytatunk, akkor jelen van a kapcsolat során a titkosítás.

Az SSL/TLS alkalmazkodik az egyes munkamenetek biztonsági követelményeihez, finomra hangolva a biztonsági paramétereket a konkrét helyzeteknek megfelelően. Ugyanakkor kiemelten fontos, hogy folyamatosan figyelemmel kísérjük a legfrissebb verziókat, és ha szükséges, válasszunk erős titkosítási csomagokat a biztonságos online tevékenységekhez. Naprakésznek kell lennünk a legújabb fejlesztésekkel és ajánlásokkal kapcsolatban, hogy ne érjen minket váratlan helyzet az online térben.

2.4. SSL/TLS a levelezésben

Az emailküldésre és fogadásra használt protokollok, mint az SMTP, POP3 eredetileg nem a biztonság szem előtt tartásával lettek tervezve. Az SSL/TLS és a STARTTLS protokollok, valamint a DMARC (Domain-based Message Authentication, Reporting, and Conformance) szabványok később kerültek bevezetésre a biztonság növelése érdekében.

A STARTTLS egy továbbfejlesztett verziója az SMTP, IMAP és POP3 protokolloknak. A STARTTLS egy kísérletet tesz arra, hogy egy biztonságos SSL/TLS-csatornát hozzon létre az adatok továbbításához. Ilyenkor a csatorna létrehozásakor eldől, hogy a másik végpont támogatja a TLS-t vagy sem. Ha nem támogatja a TLS-t akkor át vált a nem biztonságos csatornára. Illetve, az SSL esetén a STARTTLS után hozza létre a biztonságos csatornát.

A DMARC egy továbbfejlesztett szabvány, ami az SPF (Sender Policy Framework) és DKIM (DomainKeys Identified Mail) szabványokkal együttműködve előzi meg az email hamisításokat. Ezen kulcsok beállítását a hírlevélküldő rendszerek jelzik a felhasználónak, hogyha nincsenek helyesen beállítva, és bizonyos spam szűrő oldalakon ezeket meg is lehet nézni, hogy hitelesek-e, vagy sem. A DMARC részletes irányelveket tartalmaz arra vonatkozóan, hogyan kell SPF és DKIM beállításokat alkalmazni, a hamisításokat jelenteni és feldolgozni.

A 6. ábrán látható egy elterjedt hírlevél küldő tesztelő oldal, ahol átvizsgálja, az emailt a rendszer, hogy 10 pontból mennyit kapna egy spam szűrőtől. Ilyenkor leellenőrzi a tartalmat, a fejlécet, van-e benne leiratkozás gomb, vagy további linkek és azok https-el kezdődnek-e. A képen kifejezetten az SPF és a DKIM azonosítást emeltem ki, hogy

bármikor bárhol le tudjuk kérdezni egy email küldéssel, hogy nekünk megfelelően van-e beállítva.

6. ábra mail-tester.com eredmény, hiányos DMARC rekorddal

Forrás: Saját forrás (2023)

2.4.1. Email biztonsági kockázatok

A TLS/SLL, STARTTLS és a DMARC egy bizonyos szintig növeli a biztonságot, de további fejlesztésre van szükség. A TLS és az SSL biztonságos csatornákat biztosítanak az adatok továbbításához, de ettől függetlenül továbbra is vannak biztonsági kockázatai ennek a kiforrott technológiának. Mivel a STARTTLS érzékeny a középső ember (MitM) támadásokra és a tanúsítványok is lehetnek sérülékenyek.

A DMARC szabvány nagyon jó eszköz a hamisítások ellen, viszont email küldés és fogadás esetén felmerülhetnek bizonyos biztonsági korlátok és kockázati tényezők.

Az EEKS Architektúra (Enhanced Encryption Key System) a biztonságos csatorna kialakítása során egy aszimmetrikus kriptográfiát használ, vagyis beépíti a machanizmusát közvetlenül az SMTP-be, ezáltal megszünteti a GPG/PGP használatát.

A PGP (Pretty Good Privacy) e-mail üzenetek és fájlok titkosítására, digitális aláírások készítésére és azonosításra használják. Az alapelvek közé tartozik a kulcskezelés, a titkosítás és a digitális aláírások létrehozása. A PGP biztosítja az adatintegritást és

bizalmas kommunikációt. A GPG (GNU Privacy Guard) a PGP nyílt forráskódú implementációja. A GPG-t fejlesztették tovább és terjesztik a GNU General Public License (GPL) alatt. (Gabriel Chen, 2022)

2.5. Kétlépcsős hitelesítés

A kétlépcsős hitelesítéssel vagy azonosítással (2FA - Two-Factor Authentication) már szinte mindenki találkozott, akinek közösségi média fiókja, vagy hasonló online fiókja van. A klasszikus jelszavak korszaka lejárt. Alternatívák kezdik leváltani ezeket különböző authentikációs alkalmazásokkal. A kétlépcsős hitelesítési rendszerek a jelszó alapú azonosítás biztonságát erősítik egy második lépcsőfokos azonosítási token bevezetésével. A kétlépcsős hitelesítés magasabb védelmi szintet ígér, kiegészítve a felhasználó azonosító tényezőjét, vagyis amit a felhasználó tud, más azonosítási tényezőkkel, például hardware token, okostelefon, vagy biometrikus azonosítás. Ha esetlegesen feltörték egyik eszközünk annak csekély az esélye, hogy a másik készülékünkön is rajta legyen a kártevő, vagy irányíthassa a készüléket, ezzel a kockázatoknál fogunk foglalkozni a későbbiekben.

Ha a telefonos kétlépcsős hitelesítési rendszereket tekintjük nincs további eszközre szükségünk, esetleges okoskártyára, hardware kulcsra, ahol a biztonsági token-t nem kell külön letárolni, ezáltal egyfajta kompromisszumnak tekinthetjük a költségek lefaragását. Széles körben alkalmazzák a kétlépcsős azonosítást az online bankokban és szinte minden közösségi média felületen, egyéb szolgáltatásoknál is bevezették őket. A nagyobb cégek például Google, Dropbox, Facebook ~ Meta, Twitter ~ X, Apple már régebb óta alkalmazzák ezt a technológiát.

A Biometrikus azonosítás viszonylag költséges, és adatvédelmi problémákat vethet fel. Az egyszer használatos jelszavak (OTP – One-Time Password) nagyon jó alternatívának ígérkezik a kétlépcsős hitelesítési rendszerekhez. Példaképpen a hardver alapú tokeneknek, kedvezőbb költségei vannak az egyszer használatos jelszavak generálásánál, de plusz költségeket tudnak generálni a felhasználóknak, különösképpen akkor, ha a felhasználó különböző szervezeteknél különböző hardver tokeneket kell tárolnia/szállítania (pl. bankok). Viszont a mobilkészülékünk használatával az egyszer

használatos jelszavak kezelésére szolgáló kétlépcsős hitelesítési rendszerek rendkívül népszerűvé váltak, és rengeteg szolgáltató alkalmazza a hétköznapokban.

A mobilos kétlépcsős hitelesítési rendszerekkel viszont kompromisszumokat kellett kötniük a biztonság csökkentésével. A használhatóság és a költségeket tekintve ez elfogadható volt. A mobilokon egyik kiemelkedő kétlépcsős hitelesítő az SMS alapú TAN (Transaction Authentication Number) rendszerek. Pl. mTAN, smsTAN, mobileTAN. Ezen funkció célja, hogy csökkentsék a fiókokkal való visszaéléseket még akkor is, ha a banki hitelesítő adatokat jogtalanul eltulajdonították, például trójai vírussal.

A szolgáltató generál egy TAN számot, amelyet SMS-ben elküld az ügyfél részére a telefonjára. Az ügyfélnek ezt a számot kell beírnia a másik készülékről, amin igényelte ezt a TAN számot. A bankoknak szokásuk tranzakciók előtt is végig menni ezen procedúrán.

Alternatív megoldások is léteznek például a SimplePay mobil alkalmazásban lehet találkozni, a QR-kódos fizetéssel. Ilyenkor általában a webes felület generál nekünk egy QR kódot, amit a mobilkészülékünkkel kell az alkalmazáson belül beolvasni. Ilyenkor az alkalmazás visszafejti a lefényképezett QR kódot és így már automatizáltan végrehajtja a tranzakciót, ha a többi feltétel is adott (kártya, fedezet, jóváhagyás).

A mobil kétlépcsős hitelesítést egyre többen alkalmazzák globális szolgáltatók is, mint ahogy említettem a Facebook, vagy nevezhetjük Meta verzumnak is, mivel az Instagram és további alkalmazásaiban is ajánlják ezt a védelmi funkciót. Ezzel a fő céljuk, hogy csökkentsék a visszaéléseknek a számát, és a véletlenszerű kizárásokat. Bárkivel előfordulhat, hogy elfelejti a jelszavát és utána soha többet nem tud belépni a fiókjába. A felhasználónak szüksége van a bejelentkezési hitelesítő adataira és egy egyszer használatos jelszóra a bejelentkezés befejezéséhez.

A keresztplatformos fertőzési támadások elleni védekezés hatékonyan lehet kezelni, a MitM (Man in the middle) támadásokkal szemben. Lehetőségünk van HTTPS-re kényszeríteni a kommunkációs csatornát. Ha nem megoldható http kapcsolatot úgy le lehet bonyolítani a kommunikációs csatornát, hogy VPN-en keresztül történjen.

Dedikált hardvertokenek helyett a mobilokon létezik biztonságos hardver használat az egyszer használatos jelszó biztonsághoz. Az ARM processzorokba be van építve a TrustZone technológia, a Texas Instruments processzorokba pedig az M-Shield. Továbbá van még lehetőség sim és microSD foglalattal rendelkező biztonsági kulcsra (SEs – Secure Elements). (Prohardver, 2015)

2.5.1. 2FA Kockázatai

Léteznek olyan kémprogramok, malware-k, amik képesek arra, hogy elkapják az SMS üzeneteket és a tartalmát kinyerve továbbítják az egyszer használatos jelszót. Erre volt egy javaslat, hogy dedikált egyszer használatos jelszó csatornák használatával védekezzenek, amelyeket más alkalmazások nem tudnának figyelni, elkapni. Viszont, ha a támadónak van root jogosultsága, akkor megtudja kerülni a rendszert a malware. A Root jogosultsággal, gyakorlatilag bármit megtehet a program az adott eszközön, linuxos rendszeren, az Android is egy Linux alapú operációs rendszer.

A keresztplatformos fertőzés (crossplatform) fenyegetése az SMS alapú hitelesítés. Ez akkor áll fenn, ha a telefonról gépre, vagy fordítva tud terjedni. Ezen támadások egyre gyakoribbak, mivel egyre kifinomultabb és ügyesebb vírusokat, malware-ket gyártanak.

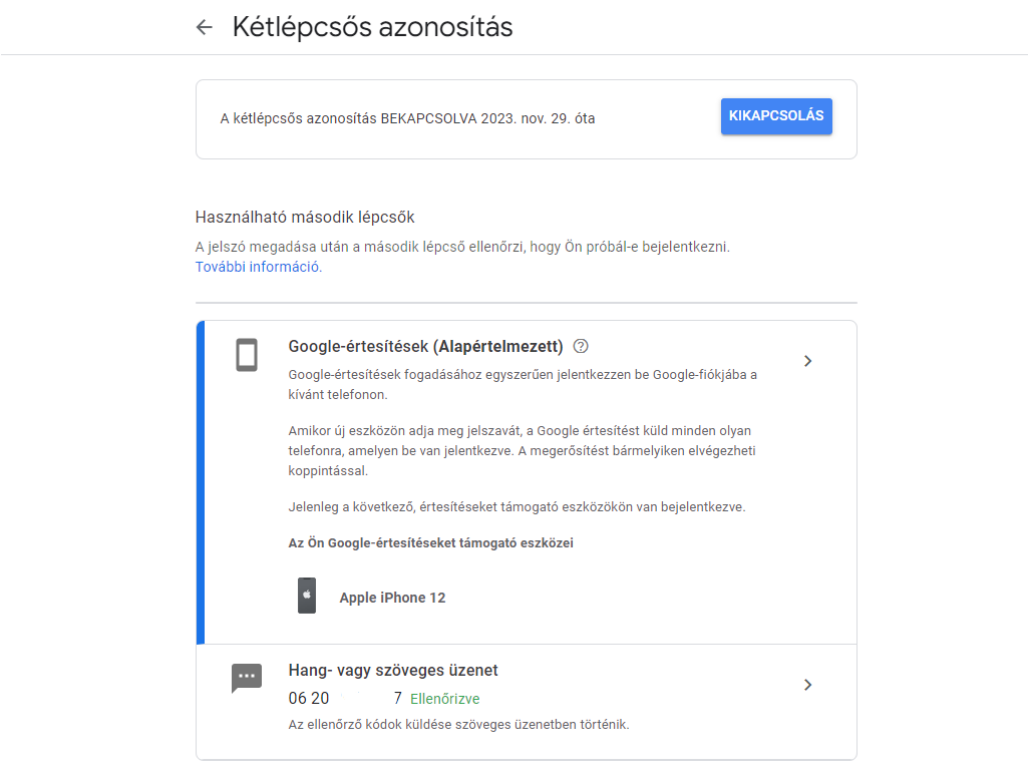
Egy másik támadási lehetőség, ha a felhasználó csak egy eszközt használ. A támadás ilyenkor egyszerűbb, mivel nincs szükség keresztplatformos fertőzésre, és elég csak egy fiókhoz hozzáférni. Ezt már több bank is elismerte, ezokból tiltják is a TAN alapú hitelesítést az ilyen kategóriába tartozó ügyfeleknek.

2.5.2. Kétlépcsős hitelesítés beállítása Google fiókban

A Google fiókon elfogjuk végezni pár lépésben, a kétlépcsős hitelesítés bekapcsolását. Ehhez kezdetképpen szükségünk van egy Google fiókra, vagy regisztráljunk be a google.com oldalon. Ezután lépjünk be a fiókunkba, majd az alábbi utasításokkal állítsuk be a kétlépcsős hitelesítést:

1. menjünk a „mail.google.com” oldalra
2. jobb felül kattintsunk a kisképre és vállaszuk ki a „Google Fiók kezelése” gombot
3. Kattintsunk a „Biztonság” szekcióra
4. görgessünk le a „Kétlépcsős azonosítás” -hoz és kattintsunk rá
5. Ezután kattintsunk az „Első lépések” gombra
6. A következő ablakon látható azok az eszközök, amiken be vagyunk jelentkezve és jóvá tudjuk hagyni a kétlépcsős hitelesítést. Majd kattintsunk a „tovább” -ra
7. Utolsó előtti lépésképpen megkell erősítenünk egy telefonszám megadásával az eszközt, és az OTP (One Time Password) megadásával menjünk a „tovább” gombra.
8. Végezetül kattintsunk a „Bekapcsolás” gombra.

A 7. ábrán láthatunk egy sikeres kétlépcsős hitelesítés beállítását. Ezzel a procedúrával sikeresen beállítottuk a kétlépcsős azonosítást egy mobilkészüléken. Biztonságból a telefonszámot is beállítottuk. Továbbiakban, ha nincs rá szükségünk bármikor kikapcsolhatjuk ezt a funkciót. (MAIL, 2017)



7. ábra aktív kétlépcsős hitelesítés google fiókban

Forrás: Saját forrás (2023)

2.5.3. Basel III kötelezővététele a Banki rendszerekben

A Basel III egy átfogó reformcsomag a banki szabályozásban. A Baseli Bankfelületi Bizottság által kidolgozott intézkedéseket foglalja magában a reformcsomag. A Basel III fő célja, hogy a bankrendszereknek növelje az ellenálló képességét. Valamint a stresszforrásokból származó sokkhatásokkal szembeni felkészültségét segítse. Továbbá a kockázatkezelés és a bankok átláthatóságának és a közzétételének a javítása a célja.

A Basel III megállapodást 2010 novemberében a G2O hagyta jóvá és többlépcsős frissítésből áll. Az EU elkötelezett a Basel III keretrendszer mellett, és ennek a megvalósítása 2013 júliusában kezdődött el, az új CRD IV hatálybalépésével. A Basel III standardok és az EU jogszabályai közötti összefüggéseket térképezi fel. Kötelező technikai szabályokat, iránymutatásokat ír elő. Az EBA félévente önkéntes monitorozást végez az EU bankjainak a mintájával, hogy nyomon kövesse a Basel III hatásait. (European Banking Authority, 2021)

2.6. Otthoni és kisvállalati hálózatok biztonsága

Manapság szinte minden háztartásban, de kisvállalatnál biztosan van helyi hálózat, LAN (Local Area Network). A legegyszerűbb kis modemtől kezdve, lehetőségünk van az okos otthoni eszközökkel (IoT) megtölteni a kis hálózatunkat, vagy éppen különleges igényeket kielégíteni VPN-nel, és/vagy helyi adattárolással (NAS - Network-attached storage).

Napjainkban kulcsfontosságú szerepet játszanak ezek az eszközök. Ha egy picit összetettebb hálózatot szeretnénk kialakítani szükséges a hálózat megtervezése és ezek olyan kihívások elé állíthatnak, amelyekre szakszerű megoldások és technológiáknak az alkalmazása szükséges. A továbbiakban részletezni fogom az aktuális trendeket, a hálózatok teljesítményét és a lehetséges sebesség növelési technikáit. Illetve a hálózati szabványok korlátait hasonlítom össze. Néhány pontban pedig a kisvállalatok és az otthoni eszközök különbségeit hasonlítjuk össze.

2.6.1. Otthoni Hálózatok felépítése és működése

Az otthoni hálózatok fő célja a kommunikációs és szórakoztató lehetőségek szolgáltatása. Az otthoni felhasználóknak igénye, hogy kényelmes és egyszerű legyen a kezelhetősége. Általában a felhasználók nem rendelkeznek különféle hálózatépítő szakmával és informatikai szaktudással.

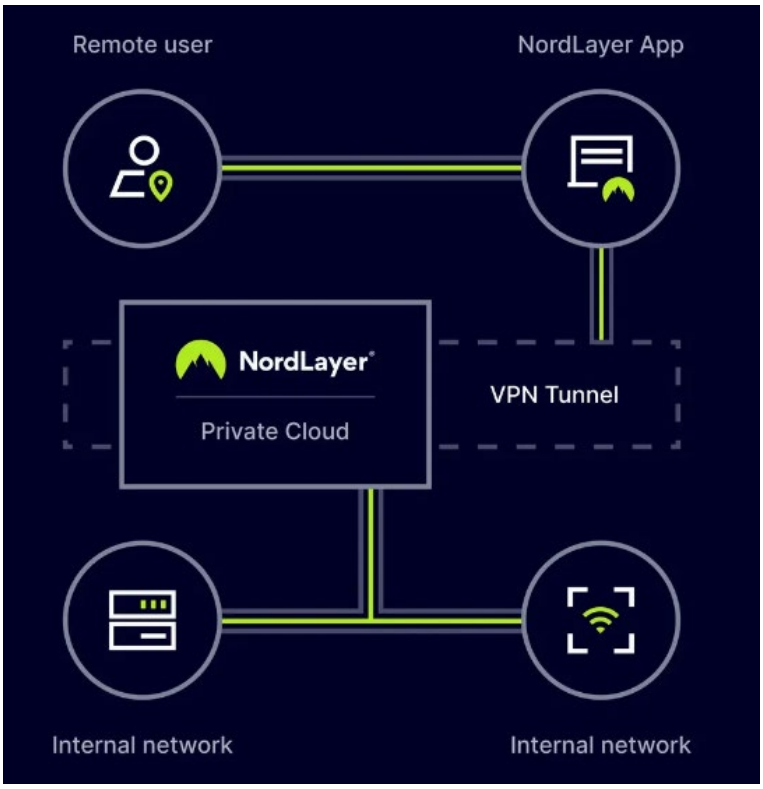
Az otthonunkban különféle eszközök lehetnek, eleinte csak egy-egy számítógép, vagy mobil készülék volt, de manapság már a lámpa izzótól kezdve, a mosogatógépen át, mindenféle okos eszköz található a háztartásban. Ezek az eszközök fő célja, hogy kényelmünket biztosítsák. Például ne kelljen a klíma kapcsolóhoz elsétálni (ha fel van fúrva a falra a távirányító) és bekapcsolni, hanem felnyitjuk a telefonunkat, és az „otthon” alkalmazásban bekapcsoljuk. De lehetőség van már előre beprogramozni, hogy érzékelje mikor szoktunk haza menni és addigra fűtsön be, vagy hűtsön le. Az IoT eszközök általában wifi-vel szoktak kapcsolódni a LAN-ra, de lehetőség van vezetékes csatlakozásra, általában Ethernet RJ45-ös dugaljjal.

Az IoT eszközöket lehetőségünk van integrálni, például IOS Otthon alkalmazásból elérni akár munkahelyünkről, amiből különböző automatizálásokat tudunk végrehajtani. Viszont, ha nem megfelelő szoftvert alkalmazunk könnyen áldozattá válhatunk a hálózaton, mint azt taglaltam az IoT eszközöknél.

2.6.2. Kisvállalati hálózatok felépítése és működése

A kisvállalati hálózatok közel állnak az érdeklődési körömhöz és többször terveztem és kiviteleztem kisebb hálózatokat, mindemellett kiviteleztem egy komplexebb hálózatot. Egy valós cég hálózatának a vázát is befogom mutatni a későbbiekben. A kisvállalti hálózatoknál viszont más jellegzetességek vannak. Itt már nem a kényelem és az egyszerűség a fő cél, hanem hogy az adott eszközök kiszolgálják a kisvállalat összes üzletiigényét hibátlanul. Egy kisvállalatnál elengedhetetlen, hogy megfelelő hálózati kapcsolat és megfelelő sebesség legyen. Míg, ha otthonunkban megszakad egy pillanatra a hálózat, maximum megáll egy pillanatra a Netflix, vagy éppen észre sem vesszük. Viszont, ha egy vállalatnál megáll a hálózat, akár bevétel kiesést is okozhat. Vagy akár adtavesztést is okozhat, bár ez nem gyakori.

Kisvállalati eszközök köre bővül esetenként VPN-nel, vagy egy helyi kis szerverrel, ami akár egy kis helyi NAS is lehet. A VPN-t megvalósítani több lehetőségünk is van. Legelterjedtebb megoldás az, ha egy szolgáltatónál igénybe vesszük a VPN szolgáltatását (pl. NordLayer) és egyben ez a legegyszerűbb megoldás is. A 8. ábrán látható, hogy hogyan működik a NordLayer.



8. ábra NordLayer működésének rajza

Forrás nordlayer

Továbbá lehetőségünk van Szerveren (pl. Windows Server 2019) VPN-t hostolni, több autentikációs metódus létezik, de a legelterjedtebb és biztonságosságban kimagasló az a L2TP (Layer 2 Tunneling Protocol) ami csak egy alagutat biztosít és a nyilvános hálózaton szállítja a csomagokat. A VPN-hez IPsec-et alkalmaz, amely titkosítást biztosít. Van egy régebbi protokoll a PPTP, ami csak annyit csinál, hogy az alagút szerepét betölti és a hálózaton keresztül továbbítja az adatokat. Ha elkell képzelnünk egy levélbe csomagolt levélként lehetne szemléltetni. (VPN infok cikke, 2021)

Vannak olyan routerek, amelyek képesek VPN-t hostolni és akár összekötni őket egy másik VPN-nel. Ilyenkor akár egy egész otthoni hálózatot összeköthetünk egy másik otthoni hálózattal. Ha fizikálisan nem is lehet őket egy hálózatra kötni, a VPN miatt olyan, mintha össze lennének kötve, ami a virtuális térben igaz állítás.

A VPN protokollnak vannak további változatai pl. IKEv2, OpenVPN, Wireguard, Shadowsocks, de ennél mélyebben nem érinti a témánkat.

2.6.3. Összehasonlítás az otthoni hálózatot a kisvállalati hálózattal

Az otthoni hálózatoknál a fő szempont a kényelem és az egyszerűség, a kisvállalatoknál pedig a funkcionalitás. Az otthoni környezetben szinte minden lehet vezetéknélküli kapcsolattal, míg a vállalatoknál bizonyos eszközöknél elengedhetetlen a megfelelő sebesség miatt a kábeles összeköttetés. A kisvállalatoknál továbbá a fókuszban a biztonság és az üzleti igények a meghatározó tényezői a tervezésnek. Ezáltal kijelenthetjük, hogy a kisvállalati hálózatok jelentősen költségesebbek és bonyolultabbak, mint az otthoni hálózatok.

2.6.4. Kisvállalti hálózat építése

Adott egy budapesti vállalat, amely elkezdett terjeszkedni és egy pécsi gyártelephellyel bővül. A budapesti telephelynek ki van már építve a hálózata, amely tökéletesen üzemel. Van egy Windows szerver, amit adattárolásra használnak és oda mentik fel az adatokat az alkalmazottak. Egyes alkalmazottaknak van VPN kapcsolatuk, hogy tudjanak otthonról is dolgozni. Viszont az új telephelyen nem tudják megoldani, hogy egyszerre két alkalmazott is dolgozzon a VPN-en keresztül a helyi hálózaton. Ezért emailen keresztül osszák meg egymás között az adatokat, ami nem a legbiztonságosabb és leggyorsabb módja az adatforgalomnak.

A vállalkozásnak gondot okoz és nem vélik biztonságosnak, hogy mindig levelezésen keresztül történik az adat csere, a gyártandó eszköz tervrajzaival. Amiben igazuk is van, mivel jelentősen biztonságosabb, ha nem küldözgetik a fileokat levélben. Nem tudják, hogyan oldják meg ezt a problémát. Pendriveon hurcolni nem kivitelezhető és verziókezelés is nehézkes. Mi van, ha esetleg megsemmisül útközben a pendrive? Így ez az opció sem életképes. A hálózati eszközöknél viszont van egy olyan megoldási lehetőség, nagyobb beruházás nélkül, hogy a fő telephelyet összekötjük a másik telephellyel a két router által. Vannak olyan fejlett routerek (Mikrotik, UniFi) amelyekben lehetőség van Side To Side VPN-re, vagyis a két főegységet összekötjük így olyan, mintha egy azon hálózaton lennének. Ezt a beállítást a router menürendszerében lehet beállítani, Mikrotik esetében parancssorból. Ezáltal az irodában nem kell gépenként rá csatlakozni a VPN-re és bárki eléri a szervert a pécsi telephelyről. Továbbá az otthoni VPN funkció sem szűnik meg. A titkosítási protokoll, ha megkívánja további védelmi

protokollal növelhetjük a biztonságot, külön tűzfalakkal telephelyenként is. A tűzfalakterén a cisco a legelterjedtebb eszköz. A vállalkozásnál további gondot okozott, hogy nem volt mindenhol megfelelő kábelezés, sem megfelelő wifi hálózat, amelyek megfelelően lefedték volna a területet. A Mesh rendszernek a lényege, hogy különálló hozzáférési pontok (AP - Access Point) egymással összekapcsolódnak és egy összehangolt hálózatot alkotnak.

„A vezeték nélküli IEEE 802.11 szabvány egy Mesh szerkezettel lett kiegészítve. A 802.11s szabvány célja egy olyan protokoll létrehozása mely önállóan tudja konfigurálni az útvonalakat az elérési pontok között egy „mindenki mindenkivel felépítésben”. … A Mesh hálózat felépítése egy decentralizált hálózaton alapul, relative olcsó és a legfontosabb előnye a megbízhatóság.” (Miholics László, 2011)

A mesh rendszer automatikusan optimalizálja a hálózati útvonalakat és a lefedettséget is erősíti. Ezáltal lehetővé teszi, hogy egy azon SSiD alatt több AP akadálymentesen üzemeljen. Mindemellett nem kell folyamatosan wifit váltani. Továbbá javítja a teljesítményt és csökkenti a hálózat terhelését. Ezen információk tudatában kicserélésre kerültek a hozzáférési pontok Wifi 6 és Mesh Technológiás eszközökre. Ahol ki volt építve a kábelezés, ott korszerűsítve lettek a régebbi cat5 kábelek Cat5E-re a megfelelő belsőhálózati sebesség miatt. A szolgáltató a le és feltöltési sebességre, csak 100/100 Mb/s-et garantált, ezért külső hálózati sebességre nem volt szükséges a gigabites sávszélesség, de a belső felhasználásnál a kamerarendszer és a nagy fileok miatt indokolt volt. Az Ethernet kábel kategóriák későbbiekben részletezem.

2.7. Hálózati kapcsolatok: vezetékes, vezetéknélküli

Két fő kategóriát különböztetünk meg, vezetékes és vezeték nélküli hálózati kapcsolat. Mindezek mellett előre leszögezhetjük, hogy a vezetékes hálózat jelentősen gyorsabb, mint a vezeték nélküli hálózat. A vezetéknélküli hálózatoknál a rádiófrekvenciás hullámokat használják ki és az jelentősen lassabb, mint az áram terjedési sebessége.

2.7.1. Vezetékes hálózatok működése

A vezetékes hálózat olyan hálózati kapcsolatot jelent, amin az adat továbbítás fizikailag vezetéken keresztül történik. Ezen kapcsolatok számos előnnyel rendelkeznek, mint például a sebesség, stabilitás, alacsony késleltetés.

Ethernet hálózat a legelterjedtebb vezetékes technológia jelenleg. Különböző kategóriákba sorolják a kábeleket, kezdve a Cat1 és jelenleg a legfejlettebb a Cat8.2. A legelterjedtebb kábel kategória a Cat5 és a Cat5E. A fő különbség, hogy a Cat5 100mb/s-ra képes 100 méteren belül, a Cat5E pedig 1000mb/s maximummal rendelkezik.

Category	Max. Data Rate	Bandwidth	Max. Distance	Usage
Category 1	1 Mbps	0.4 MHz		Telephone and modem lines
Category 2	4 Mbps	4 MHz		LocalTalk & Telephone
Category 3	10 Mbps	16 MHz	100 m (328 ft.)	10BaseT Ethernet
Category 4	16 Mbps	20 MHz	100 m (328 ft.)	Token Ring
Category 5	100 Mbps	100 MHz	100 m (328 ft.)	100BaseT Ethernet
Category 5e	1 Gbps	100 MHz	100 m (328 ft.)	100BaseT Ethernet, residential homes
Category 6	1 Gbps	250 MHz	100 m (328 ft.) 10Gb at 37 m (121 ft.)	Gigabit Ethernet, commercial buildings
Category 6a	10 Gbps	500 MHz	100 m (328 ft.)	Gigabit Ethernet in data centers and commercial buildings
Category 7	10 Gbps	600 MHz	100 m (328 ft.)	10 Gbps Core Infrastructure
Category 7a	10 Gbps	1000 MHz	100 m (328 ft.) 40Gb at 50 m (164 ft.)	10 Gbps Core Infrastructure
Category 8	25 Gbps (Cat8.1) 40 Gbps (Cat8.2)	2000 MHz	30 m (98 ft.)	25 Gbps/40 Gbps Core Infrastructure

9. ábra Ethernet kábel kategóriák

Forrás: Eaton (2023)

A hálózati kábeleket sávszélesség, maximális adatsebesség (megabit per másodperc) és az árnyékolás alapján osztják szét kategóriákba. Mint ahogy a 9. ábrán is látható 8 kategóriára van szétbontva, ezen belül kiadtak kisebb javításokat is.

10. ábra Kábel árnyékolási típusok

Forrás: Eaton (2023)

Az ethernet kábelek vezetékes adatkommunikációjának a lehallgatása lehetséges. Az ethernet hálózatokra úgy tekintünk, mint amely alapból védett, titkosított. Azonban le lehet hallgatni az adatokat. A csavart érpár (UTP 10. ábra első kép) esetén egy vezetéknélküli lehallgatást próbáltak és sikerrel is jártak. Az Ethernet kábel elektromágneses sugárzást bocsátott ki, amely segítségével a támadó a kábel közvetlen közelében tartózkodva képes volt lehallgatni az adatokat. Mindent úgy, hogy nem tett kárt a kábelben. A csavart érpáros kábelek is kibácstanak elegendő elektromágneses hullámot, ahhoz, hogy néhány bit hibahányaddal rekonstruálni lehessen az adatokat. Ezáltal a

támadó észrevétlenül tud adatokat lopni, viszont lehet ez ellen tenni, további árnyékolásokkal és a linkréteg titkosításával. (Matthias Schulz, 2016)

A titkosítás különböző kábelek esetében más és más frekvenciák és jel erősség kibocsátást produkálnak. A továbbiakban részletezem, hogy milyen Ethernet kategóriák vannak.

Kezdetben a Cat1 volt az otthoni és az irodai vezetékes telefon rendszerek kábelezési rendszere. Egy csavart árnyékolatlan érpár alkotja a Cat1 szabvány (Lásd 10. ábra árnyékolási típusok) UTP kábelét.

A 2-es kategória (Cat2) hang- és adatkommunikációra is képes, elsősorban az IBM Token Ring hálózatokhoz használták az 1980-as években.

A Cat3-as kábeleket az 1990-es évek elején vezették be. A kábelezése négy csavart érpárból állt, ami támogatta a 10BaseT Ethernet hálózatokat. Fontos megemlíteni, hogy digitális hangkommunikációt elsőként támogatta. Ezen kábelek még a mai napig is megtalálhatóak régebbi épületekben, de 10 Mb/s-os maximális adatsebességre képesek, ami már szinte semmire sem elegendő.

A Cat4 ugyan azon kábelezést alkalmazza, viszont a sávszélessége a 16 Mhz-ről 20 Mhz-re emelkedik. Így másfélszeres sebesség növekedés érhető el, ami 16 Mb/s-ra nő. Elsősorban IBM Token Ring hálózatokban használták.

A Cat5 típus, amely napjainkban is elterjedt, de elavult akár 100 mb/s-ra is képes. Ezt a típust 1995-ben mutatták be, szabványos 10BaseT és 100BaseT (Fast Ethernet) hálózatokon használják. Akár 100 méteres távolságra is képes, jeleket továbbítani. A Cat5e egy nem hivatalos új kategória, hanem csak egy tovább fejlesztés. Ezen szabvány (Cat5e) akár 1 Gb/s-ra is képes 100 méteren belül. Nagyobb adatsebességet a csavarások számának a növelésével tudták elérni.

Cat6 kategória nagyobb sávszélességet és adatátviteli sebességet biztosít, 100 méteren keresztül akár 1 Gb/s-ig, mint a Cat5e. De rövidebb távon akár 10 Gb/s sebességre is képes, 37 méteres távolságon. Az árnyékolás miatt sikerült növelni a teljesítményt, mivel egy fólia árnyékolással van körbe tekerve a vezeték, az elektromágneses interferencia csökkentése érdekében. Továbbá egy fizikai elválasztót tartalmaz a kábelek között, amit

„spline” -nek neveznek a négy érpár között. A Cat6 kábel visszaféle kompatibilis a Cat5 és a Cat5e szabvánnyal. 2009-ben megjelent a Cat6a szintén egy javított/kibővített kiadás, ami akár 500 MHz-es sávszélességre is képes a Cat6 kábel 250 MHz-évl szemben.

Cat7 viszont már egy vállalat által kifejlesztett és szabadalmaztatott szabvány, amelyet az IEEE nem támogat. A szabadalmaztatott GG45 csatlakozókkal rendelkezik. A 11. ábrán látható az RJ45 (Cat6a) és a GG45 (Cat7) közötti különbség. A Cat7a szintén egy kiterjesztett/javított kiadása a Cat7-nek, amely 50 méter felett 40 Gb/s-ra képes, illetve 15 méterig 100 Gb/s sebességet képes produkálni. Az IEEE és az EIA támogatásának hiánya okán a Cat7/Cat7a nem egy elterjedt szabvány.

11. ábra RJ45 és GG45 csatlakozó

Forrás: Daniel Dunar (2020)

A Cat8 ideális kábel a switch-to-switch kommunikációhoz, amely akár 2000 MHz-re is képes 30 méteres távon és akár 40 Gb/s sebessége is lehet. Jelen esetben már kábel erenként van az árnyékolás, az áthallás kiküszöbölése érdekében. Egyetlen hátránya,

hogy merev vastag kábelt eredményez a sok árnyékolás, így nehézkes a telepítése. RJ45-s szabvány csatlakozóval szerelt, így visszafelé kompatibilis a korábbi verziókkal. A Cat8.1 25 Gb/s-ra képes maximum 2000 MHz-n 30 méteren belül, a Cat8.2 már 40 Gb/s adatátviteli sebességet tud produkálni.

További opció, ami még LAN rendszereknél nem annyira használt technológia az optikai kábel. Működését tekintve egy komplikált rendszer, de egyszerűsítve a lézerfény jelekkel kommunikál.

„Optikai vagy fénykábel igen tiszta, néhány tíz (korábban száz) mikrométer átmérőjű üvegmag szál és az ezt körülvevő, kisebb optikai törésmutatójú héjból áll.” (Gerencsér András, 2006)

2.7.2. Vezetéknélküli hálózatok

A vezetéknélküli hálózatok fő előnye, hogy nincs szükségünk kábelre, mivel az adatátvitel rádiófrekvenciák segítségével történik. Az előnye a vezetékes kábellel szemben, hogy jelentősen költséghatékonyabb a telepítésük. Hátrányuk viszont, hogy lassabb az adatátvitelisebesség és gyakran jelvesztés is lehetséges.

Mobiltelefonunkon találkozhatunk többféle vezetéknélküli kapcsolódási lehetőséggel. Kezdve a mobil hálózattal (3G/LTE/4G/5G), a Bluetooth kapcsolaton át egészen a Wi-Fi-ig. Ez a hármas régebben még ki volt egészítve az Infra kapcsolattal.

A Wi-Fi technológia a vezeték nélküli hálózatok vezető szabványa. A Wi-Fiknek vannak különböző verziói, amelyek a kommunikáció sebességét és lefedettségét határozzák meg. Például 802.11n, 802.11ac és 802.11ax. A 802.11ax szabvány a Wi-Fi 6 technológiát foglalja magában.

Az IEEE 802.11ax a hatodik generációs Wi-Fi, innen ered a Wi-Fi 6 elnevezés. A 802.11ax szabvány lehetővé teszi, hogy a hozzáférési pontok egyszerre több felhasználót kezeljen leterhelt környezetben. Kiszámíthatóbb a teljesítmény és a nagyfelbontású videó lejátszását is könnyedén teszik elérhetővé. Az IoT eszközök is dinamikusabban működnek ezen protokollt alkalmazva.

„A 6. szám azt mutatja, hogy ez a Wi-Fi hatodik generációja, és a korábbi verziókhoz képest nagyobb sebességet és 40%-kal gyorsabb kapcsolatot kínál a felhasználóknak, mint a Wi-Fi 5 szabvány. A Wi-Fi 6 gyorsabb, nagyobb kapacitással és jobb energiahatékonysággal.” (Bytech, 2022)

2.7.3. WPA3 és a WPA2 különbségei

A Wi-Fi hálózatunk védelméért felel a WPA2 (Wi-Fi Protected Access 2) és a WPA3 (Wi-Fi Protected Access 3) ami a WPA2 továbbfejlesztett változata. A WPA3 az AX szabvány bevezetésével került bele a Wi-Fi 6-os eszközökbe. A WPA3 nem kompatibilis visszafelé az eszközökön, de WPA3 és WPA2 támogatással gyártják a készülékeket.

A titkosítás a WPA2-nél AES-CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) titkosítást használ, míg a WPA3 AES-GCM titkosítást, amely jelentősen biztonságosabb a WPA2-esnél. A WPA3 személyre szabott egyéni titkosítást tesz lehetővé, míg a WPA2-ben egy azon előre megosztott kulccsal titkosít, vagyis a WPA3-nál mindegyik eszköz külön titkosított kulccsal kommunikál.

A WPA3 a nyilvános hálózatokon is biztonságosabb, mivel bevezeti az Enhanced Open security mode-ot, amely az OWE (Opportunistic Wireless Encryption)-t használja. Ez azt teszi lehetővé, hogy a nyilvános Wi-Fi is titkosítást biztosít a WPA2-vel szemben, ami ilyenkor titkosítás nélkül kommunikál.

A WPA3 támogatja az IoT-eszközöket. Ezen eszközöket lehetőségünk van QR-kóddal, vagy NFC (Near Field Communication)-vel csatlakoztatni a hálózathoz, ha rendelkeznek Easy Connect tanúsítvánnyal. A WPA2 nem volt felkészítve az IoT eszközökre. A WPA3 megkönnyíti a felhasználók számára, az IoT eszközök üzembehelyezésének a lépéseit és használatát.

A WPA3 gyengeségei jelenleg nem ismertek, mivel a WPA2 gyengeségeit küszöbölik ki. Felhozhatjuk gyengeségnek, hogy nem egy elterjedt szabvány még, ezáltal korlátozott eszköz támogatással rendelkezik. Továbbá nem kompatibilis visszafelé a WPA2-es eszközökkel. Ha nagyobb figyelmet kap és szélesebb körben elterjed, a potenciális támadók körében új sebezhetőségek jelennek meg. (Portnox, 2023)

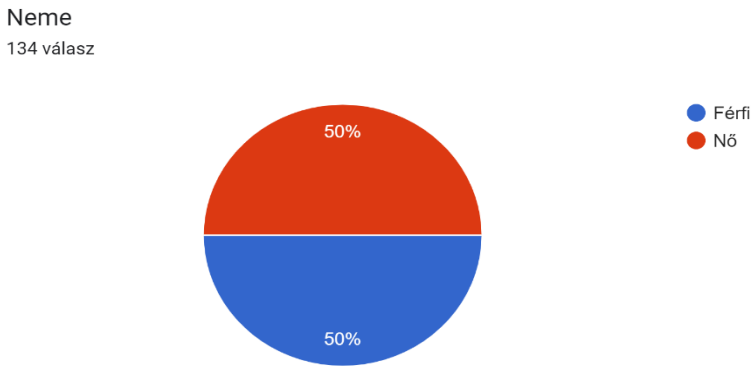
3. TITKOSÍTÁS PROBLEMATIKÁJA ÉS KIHÍVÁSAI - KÉRDŐÍV

A kutatásomat az emberek általános titkosítási és biztonsági szokásainak feltérképezésére éleztem ki. A kutatásom célját a saját megtörtént eseteim által határoztam meg, hogy viszonyulnak a titkosításhoz a felhasználók. A kvantumszámítógépekkel kapcsolatban is elő került pár kérdés, mivel ez a jövőben gondot okozhat majd a titkosítással kapcsolatban. A kvantumszámítógép működését tekintve, majdnem olyan, mint a hétköznapi számítógép, csak alapjaiban teljesen más. Míg egy hagyományos számítógépnél egy bit vagy 0, vagy 1 addig a kvantumszámítógépnél ez a bit lehet egyszerre 0 és 1. Tulajdonképpen egy olyan állapot, amikor kéthelyzetben is létezik, kvantum-szuperpozícióban van. Ezokból feltételezhetjük, hogy egy jelszó feltörése nem évek vagy hónapok. Kutatásom célja, hogy az alábbi kérdésekre választ kapjak:

- Mennyire ismerik és alkalmazzák a felhasználók a kétlépcsős hitelesítést?
- A felhasználók tudatos internetezők?
- Alapos a titkosítási ismeretei a hétköznapi felhasználóknak?

3.1. Kutatás bemutatása

A kérdőívem 3 hétig volt elérhető a kitöltők számára. Különböző médiafelületeken azon belül, közösségi platformokon hirdettem meg, illetve barátaim, munkatársaim és az ő ismerőseiket is megkérdeztem.



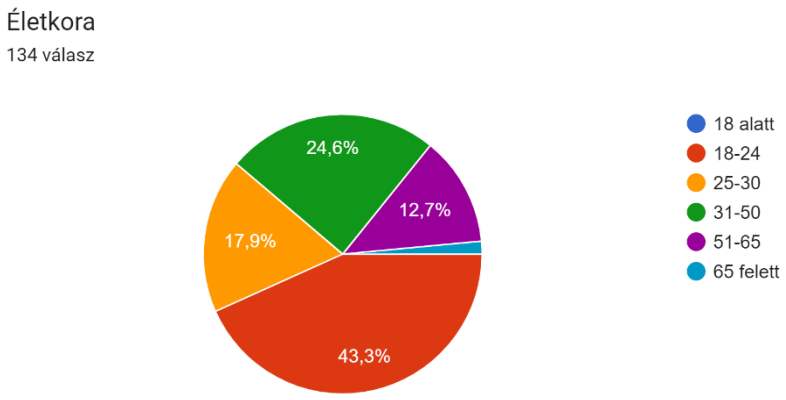
12. ábra A kitöltők neme (n=134)

Forrás: Saját forrás (2023)

A kérdőívemet 3 részre osztottam szét. Az első részben a kitöltő nemét, életkorát és iskolai végzettséget kérdeztem meg. Fontos, hogy tudjuk a kitöltőket valamilyen jellemző alapján csoportosítani és valamilyen következtetést tudjunk levonni. Ezokból lakhelyet és iskolai végzettséget is kértem a kitöltőktől. A kérdőívet, közel 3 hét alatt 134 ember töltötte ki. A továbbiakban ezeket a válaszokat fogom kiértékelni.

A kördiagrammon látható, hogy a kitöltők életkora fele, nő és fele férfi. Százalékban kifejezve 50-50%. Következtethetünk arra, hogy hasonló érdeklődést váltott ki a nőkből, mint a férfiakból is. Ha tovább gondoljuk, levonhatjuk, hogy ugyan úgy érintettek a témában a nők és a férfiak is.

A kérdőívemben a megkérdezettek életkorával csoportosítani tudjuk. A különböző korcsoportokat összetudjuk hasonlítani, hogy mik a válaszadók szokásai, jellemzői egy adott csoportnak.

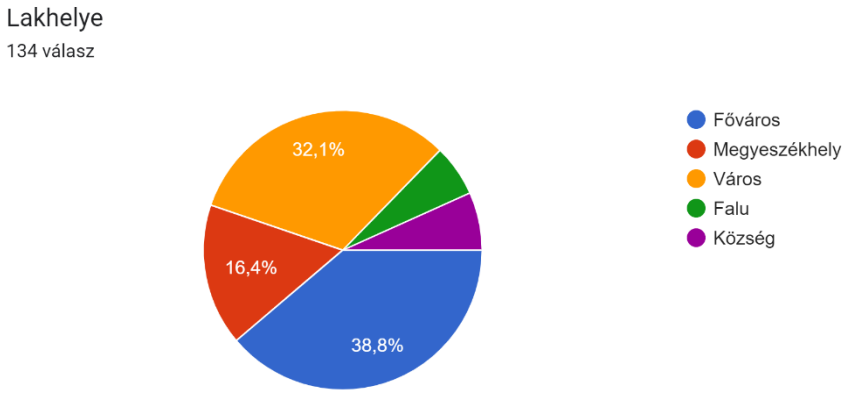


13. ábra A kitöltők életkora (n=134)

Forrás: Saját forrás (2023)

Következtethetünk arra is, hogy mennyire könnyen használható a kétlépcsős hitelesítés az adott korosztálynak. Az ábrán látható, hogy inkább a fiatalok töltötték ki. A 18-24 év közöttiek töltötték ki a legtöbben, azaz 43.3%-a. Ebbe a korosztályba tartozók az Egyetemi hallgatók és a fiatal pályakezdők. A Következő korosztály a 31-50 év közöttiek, akik még nem a tableten és a telefonon szocializálódtak. Ezokból is figyelmesebbek és óvatosabban neteznek, mint a fiatalabbak. A 3. kategória a 25-30 év közöttiek, ezt követi

az 51-65 év közöttiek, majd a 65 felettiek és nem volt 18 év alatti, aki részt vett a kutatásban. Értelemszerűen az idősebb korosztály (51-65) kevésbé van jelen az interneten, mint a fiatalabbak. Ezáltal is kevesebb a kitöltésük.

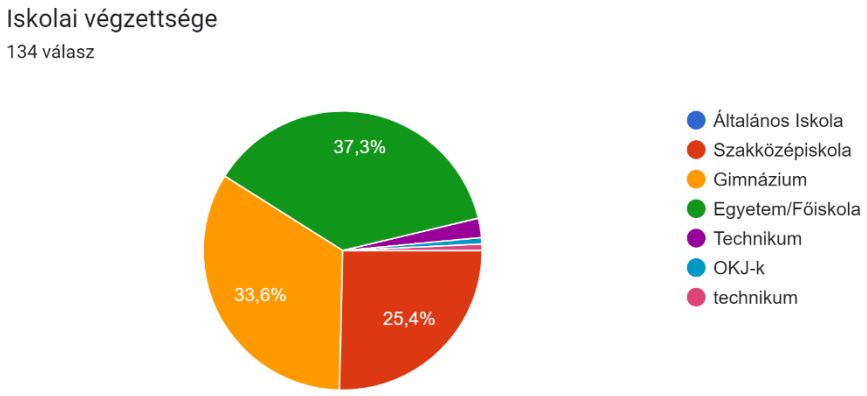


14. ábra A kitöltők lakhelye (n=134)

Forrás: Saját forrás (2023)

A kitöltők lakhelyének eloszlása a 14. ábrán látható. A legnagyobb arányban a fővárosban laknak, illetve a 32,1%-a városban lakik. Megyeszékhelyeken már jelentősen kevesebb százalék él, 16,4%-a. Falun 8 kitöltő (6%) és községben pedig 9 (6,7%) lakik. Ezokból következtethetünk, hogy városokban és megyeszékhelyeken az internet elérhetősége jobban kivan építve.

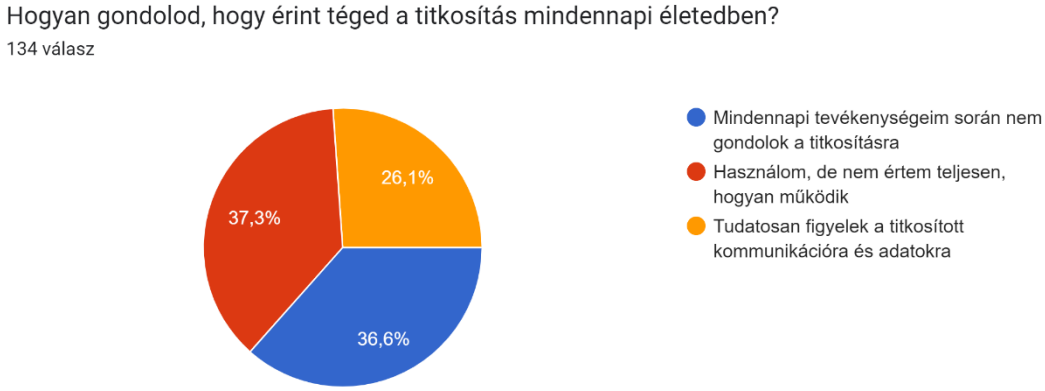
A 15. ábrán látható a kitöltők legnagyobb iskolai végzettsége. Az ábra jól szemlélteti, hogy a kitöltők 37,3%-a egyetemi/főiskolai végzettséggel rendelkeznek. Ezután a Gimnáziumi végzettség következik 33,6%-kal. A szakközépiskola pedig 25,4%-a. További 4 kitöltő (2,9%), pedig technikumi végzettséggel rendelkezik. Illetve van egy okj végzettség is.



15. ábra A kitöltők iskolai végzettsége (n=134)

Forrás: Saját forrás (2023)

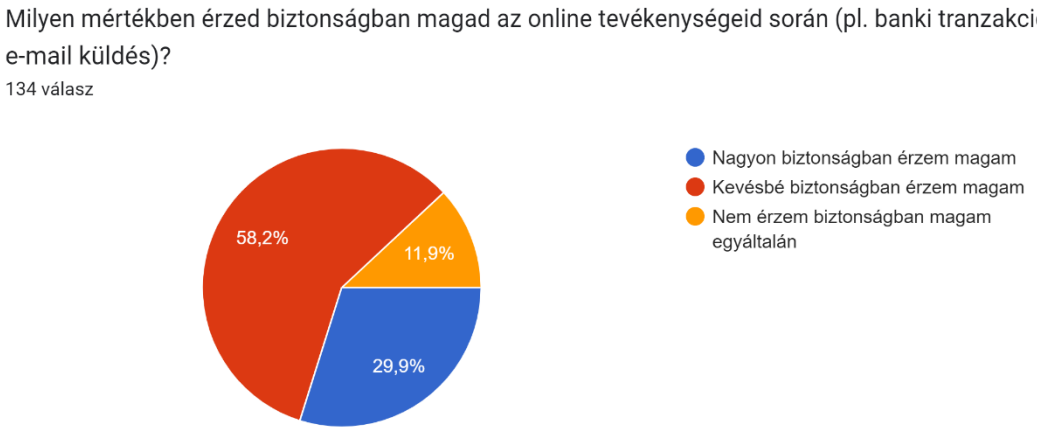
Az iskolai végzettség, azért fontos információ, mert tudunk megfigyeléseket tenni, hogy van-e összefüggés a titkosítási szokás között és a végezettség között.



16. ábra A kitöltők érintettsége a titkosítással a hétköznapi életben (n=134)

Forrás: Saját forrás (2023)

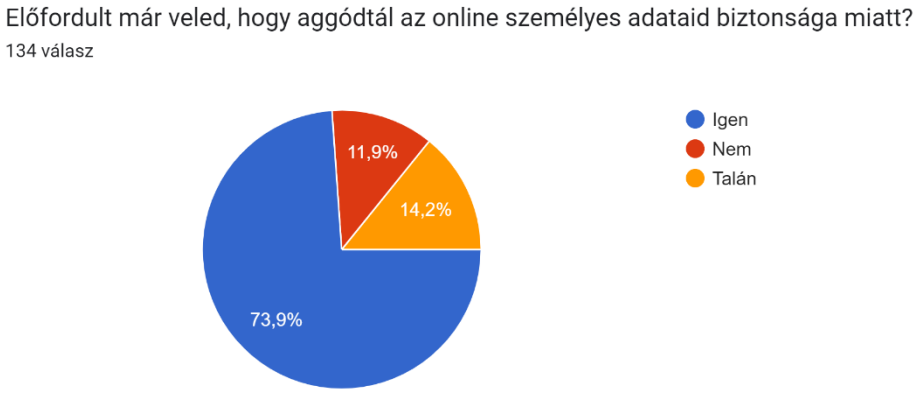
A megkérdezettek 36,6%-a nem gondol a mindennapjai során a titkosításra, de ettől függetlenül kapcsolatba kerülhet ilyen felülettel. A kitöltők 26,1%-a, pedig tudatosan figyeli a titkosításokat, vagyis ők a tudatos felhasználókhoz sorolhatóak. Végezetül, 37,3% pedig használja a titkosítást, de nem tudja, hogy hogy működik, ők is a tudatos felhasználókhoz sorolhatóak. Ezen eloszlás látható a 16. ábrán.



17. ábra A kitöltők biztonsági érzete az online tevékenységeik során (n=134)

Forrás: Saját forrás (2023)

A kitöltők több mint a fele 58,2% kevésbé érzi magát biztonságban az online felületeken, ezzel szemben 29,9% érzi magát biztonságban. Illetve akik nem érzik magukat biztonságban ők 11,9%.

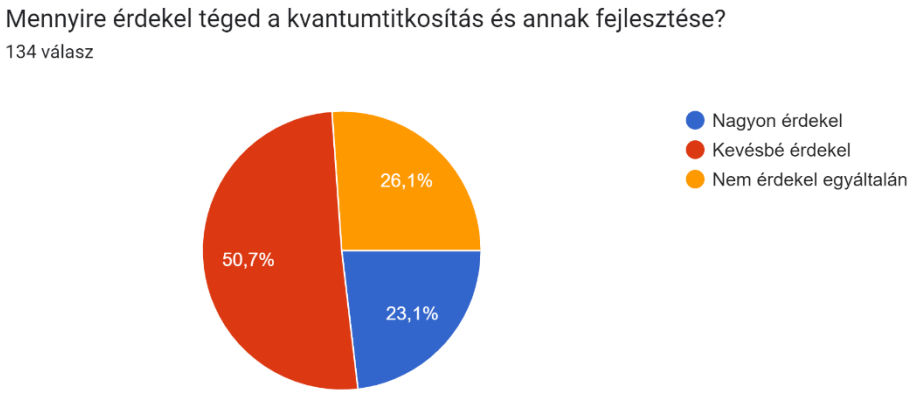


18. ábra A válaszadóknak volt-e aggodalma az online személyes adatainak biztonsága miatt (n=134)

Forrás: Saját forrás (2023)

Érdekes az online személyes adatokkal kapcsolatban, hogy napjainkban szinte mindent online intézünk például vásárlás, banki tranzakciók. Mégis 73,9% Igennel válaszolt, hogy aggódott az adatai miatt. 11,9% nem aggódót és 14,2% nem tudja pontosan. Az

érdekesség pedig az, hogy féltik a kitöltők az adatikat, de mégis online végzik a vásárlást és a banki ügyeket. A 18. ábrán látható az érdekes eredmény.

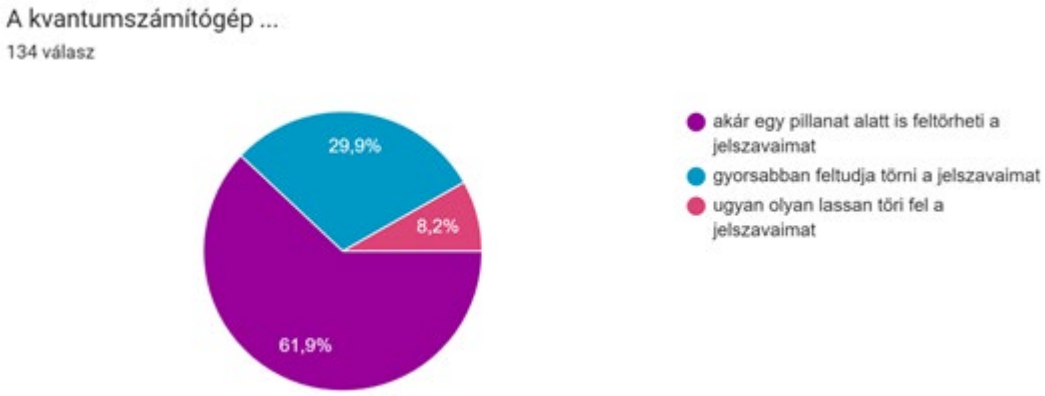


19. ábra A válaszadók érdeklődése a kvantumtitkosítás iránt (n=134)

Forrás: Saját forrás (2023)

A kvantumtitkosítás 19. ábrán látható, első ránézésre az embereket kevésbé érdekli a titkosítás, ami érthető is, de nincsenek tisztában a kockázatokkal. A kérdőív kitöltőinek az 50,7%-át kevésbé érdekli, 26,1%-át teljesmértékben nem érdekli. Csekély 23,1%-át érdekli a kvantumtitkosítás.

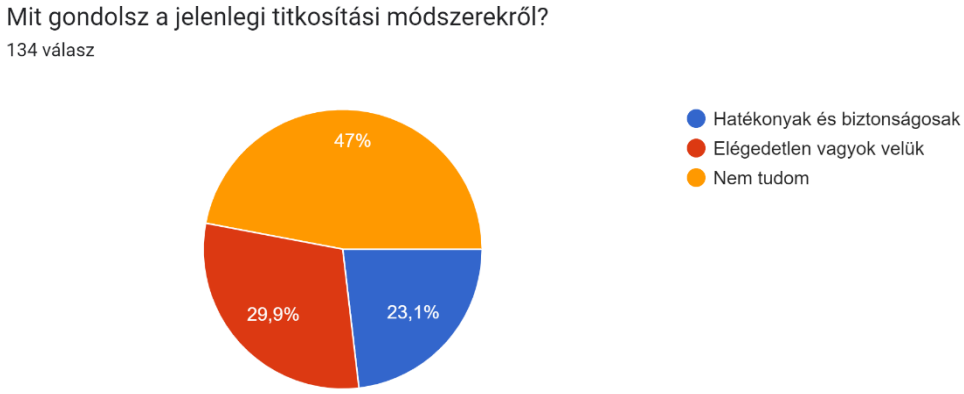
A Kvantumszámítógép működésével nagyjából tisztában vannak a kitöltők, de mély tudásuk nincs róla, 61,9% szerint egy pillanat alatt is feltörheti a jelszavainkat. 29,9% szerint gyorsabban fel tudja törni a jelszavakat. 8.2% szerint ugyan olyan, mint a hagyományos számítógép feltörési ideje. A valóság még, hogy egy pillanat alatt nem tudja feltörni a jelszavakat, de gyorsabb, mint egy szuperszámítógép. (Edward Parker, 2023)



20. ábra Kvantumszámítógép gyorsasága (n=134)

Forrás: Saját forrás (2023)

A kitöltőket az előző kérdésekben próbáltuk behelyezni, mint tudatos felhasználó és láthatjuk az összefüggést, hogy szinte a fele, nem tudja vagy nem alkot véleményt a jelenlegi titkosítási módszerekről. Vagyis 47% nem ismeri a titkosítási módszereket. 29,9% elégedetlen a jelenlegi titkosítási módszerekkel. 23,1% teljes mértékben elégedett az aktuális titkosítással. A 21. ábrán láthatjuk a kördiagramon a titkosítási módszerekről a véleményeket.



21. ábra Válaszadók viszonyulása a titkosítási módszerekhez (n=134)

Forrás: Saját forrás (2023)

Az oszlopdiagramon látható, a válaszadók mennyire tudatos felhasználók. Az 1-Egyáltalán nem igaz rá, 2-Semleges, 3-Teljesmértékben igaz rá. Az első oszlop a „Használok titkosított alkalmazásokat vagy eszközöket" kérdés és 62-en teljesmértékben, 43-an semleges 29-en nem. Második kérdés „Követem a titkosítási trendeket", az ábrán is látható, hogy a „nem" dominál 73 jelöléssel, 43-an „semleges" nem nyilatkozik és végül 18 kitöltő követi a trendeket. A további válaszokat a 2. táblázatban látható és további két kérdést fogok részletezni. A többi kérdés elemzés szempontjából fontos.

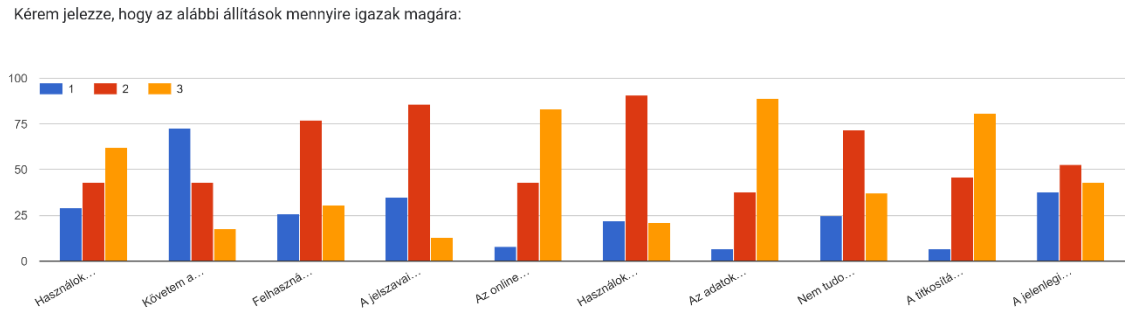
Kérdés	Egyáltalán nem	Semleges	Teljesmértékben
Használok titkosított alkalmazásokat vagy eszközöket	29	43	62
Követem a titkosítási trendeket	73	43	18
Felhasználó barátnak tartom a jelenlegi biztonsági szokásokat (2FA)	26	77	31
A jelszavaimat papíron tárolom	35	86	13
Az online személyes adataim biztonságát valóban komolyan veszem.	8	43	83
Használok jelszókezelő alkalmazást (pl. Google Jelszókezelő)	21	91	22
Az adatok titkosítása fontos a személyes magánéletem védelmében.	7	38	89
Nem tudom kezelni a mostani banki rendszereket, mert bonyolult számomra	25	72	37
A titkosítás és a felhasználóbarát megoldások egyensúlyát fontosnak tartom	7	46	81
A jelenlegi jelszó és fiókvédelmeket (2FA, One Time Password - SMS) tudom és szeretem használni	38	53	43

2. táblázat Mennyire tudatos felhasználó a kitöltő?

Forrás: Saját forrás (2023)

Látható a 2. táblázaton, hogy az eredmények nagytöbbséggel a „Teljesmértékben" és a „Semleges" oszlopban van a legtöbb jelölés. Kivétel „A jelszavaimat a papíron tárolom" kérdés és a „Követem a titkosítási trendeket". Ezek az embereknek egy nagyon rossz tulajdonságából fakad. Lusták vagyunk. Sokkal kényelmesebb leírni egy papírra a jelszót és cipelni, mint hogy megjegyezzük. Kitalálták erre a jelszókezelő alkalmazásokat, hogy

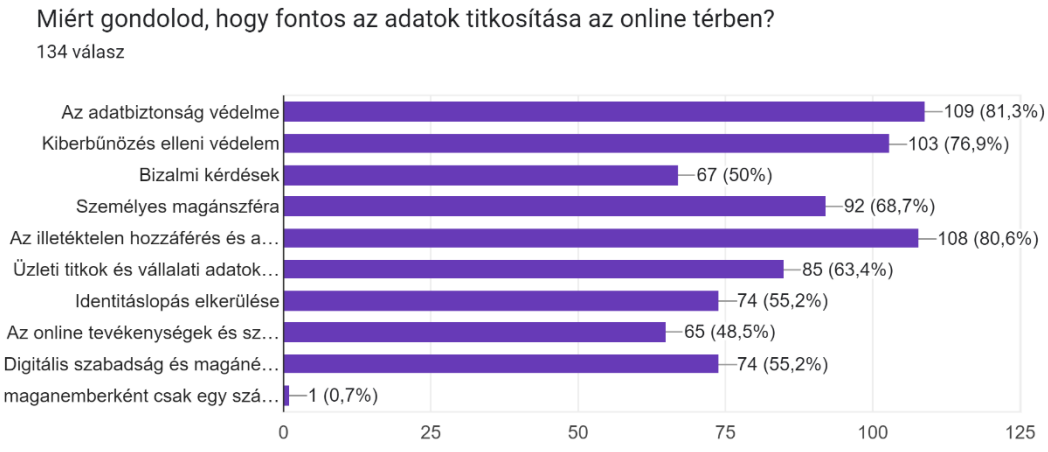
csak egyet keljen megjegyezni, de még így is a papír alapú jelszavaknál maradtunk. A titkosítási trendek követése is a lustasághoz köthető, mivel az emberek nem fogadják be az újdonságokat. Ha megfigyeljük magunkat, vannak szokásaink belekerülünk egy örvénybe és ahhoz, hogy változzunk rengeteg energiát kell belefektetni.



22. ábra Mennyire tudatos felhasználó a kitöltő? (n=134)

Forrás: Saját forrás (2023)

Vagyis, az új trendeket átvenni, például lecserélni a Google Jelszókezelőt az Apple kulcskarikára, szinte biztos, hogy nem cserélnénk le, használnánk ezt is és azt is. Nem érdekli az embert, hogy picit kényelmetlen. Mindenki ismeri a mondást, „Már megszoktam”.



23. ábra A kitöltő szerint miért fontos az adatok titkosítása az online térben? (n=134)

Forrás: Saját forrás (2023)

Az utolsó előtti kérdésnél a felhasználói vélemények nagyon fontosak a technológia további fejlesztésében, mivel sok esetben ezek alapján történik a továbbfejlesztés egy adott szegmensen. A 23. ábrán a felhasználói véleményeket vizsgáljuk, hogy mit tartanak fontosnak a titkosítással kapcsolatban. Az első 3-4 válasz jól elkülönül a többitől ezeket fogom részletezni. Az adatbiztonság védelme szinte majdnem mindenki bejelölte 109-en azaz 81,3%. Érthető okokból jelölték ennyien, mivel a titkosítás célja az adatok biztonságának a védelme. A második 108 jelöléssel 80,6%-kal az illetéktelen hozzáférés és adatlopás megelőzése, ami a titkosítás fogalmába is bele tartozik. A harmadik 76,9%-kal a kiberbűnözés elleni védelem. Az internet elterjedésével a kiberfenyegetések is fokozódtak. A különböző adatlopások és kémkedések miatt, illetve nemzetbiztonsági szempontok miatt hoztak létre külön intézményeket, mint például a Nemzeti Kibervédelmi Intézet.

3.2. Eredmények áttekintése

A minta jellemzők ismertetése után a következőkben bemutatom az elemzésemet. Ehhez az adatokat tisztítottam és az egyes demográfiai változóknál (életkor, lakhely, iskolai végzettség) a kis elemszám miatt és a későbbi könnyebb elemezhetőség miatt egy szomszédos kategóriákat össztevontam. A 65+ kategória 2 válaszadója az 51-65 katógiával került összevonásra. Hasonlóan a kevés válasz miatt a falu és a község kategóriákat is összevontam. Illetve a Szakközépiskola és a Technikum is „Középfokú képesítéssel" kategóriába került, míg a Gimnázium és a Egyetem/Főiskola kategóriákat meghagytam külön, csak átneveztem azokat.

3.2.1. „Hogyan érint téged a titkosítás a mindennapi életben?"

Először a „Hogyan érint téged a titkosítás a mindennapi életben?" kérdés válaszait elemzem. A válaszadók 3db lehetőség közül választhattak, amely a teljesen kívülálló, a laikus felhasználó és a jártas válaszadók csoportját különítette el. A függő változót a nem, életkor, lakhely és iskolai végzettség magyarázó változókkal vetettem össze keresztáblák segítségével, valamit Lamba, Tau és Chi^2-tesztek alkalmazásával. A következőkben az érdekesebb eredményeket ismertetem.

			Neme		
			Nő	Férfi	Total
Hogyan érint téged a titkosítás a mindennapi életben?	Mindennapi tevékenységeim során nem gondolok a titkosításra	Count	26	23	49
		Expected Count	24,5	24,5	49,0
	Használom, de nem értem teljesen, hogyan működik	Count	29	21	50
		Expected Count	25,0	25,0	50,0
	Tudatosan figyelek a titkosított kommunikációra és adatokra	Count	12	23	35
		Expected Count	17,5	17,5	35,0
Total		Count	67	67	134
		Expected Count	67,0	67,0	134,0

*3. táblázat Hogyan érint téged a titkosítás a mindennapi életben? * Nem*

Forrás: Saját forrás (2023)

Ahogy a 3. táblázatból is látszik, a mintában szereplő nők kevésbé érdeklődnek a titkosítás iránt a mindennapi életben, mivel a férfiak körében többen jelezték, hogy ők tudatos felhasználók. A női válaszadók inkább nem gondolnak rá vagy használják, de nem teljesen értik, hogy működik. A lambda, a kapcsolat általános mérőszáma esetében a szimmetrikus érték 0,086, 0,140-es szignifikancia mellett, ami gyenge összefüggésre utal, de a p-érték nem szignifikáns a hagyományos 0,05-ös szinten. Illetve a Pearson Chi^2 értéke 4,921, p: 085. Ez a p-érték nagyobb, mint az általánosan használt 0,05-ös szignifikancia szint. Ezért jellemzően nem sikerül elutasítani a nullhipotézist. Ez arra utal, hogy az adatok alapján nincs szignifikáns kapcsolat a két kategorikus változó között. Ami azt jelenti, hogy első ránézésre van némi különbség, de ez inkább a mintaadottság.

Ezután megvizsgálatam az életkor összefüggést is, Lambda, Goodman and Kruskal tau segítségével, az eredmények gyenge összefüggésre utalnak, de a p-értékekegyike sem éri el a 0,05-ös küszöbértéket. Ahogy, a A Chi-négyzet teszt (5,570, p: 0,473) sem mutat statisztikailag szignifikáns összefüggést ($p > 0,05$). Ez arra utal, hogy nincs erős bizonyíték a két kategorikus változó közötti függetlenség nullhipotézisének elutasítására. Összegezve, a kapott eredmények alapján nincs erős bizonyíték arra, hogy az életkor és a titkosítás mindennapi életre gyakorolt hatásának megítélése között szignifikáns összefüggés lenne. A szignifikancia hiánya azt jelenti, hogy a változók nem állnak szoros kapcsolatban a megfigyelt adatokban.

			Lakhelye				Total
			Község és falu	Város	Megye-székhely	Főváros	
Hogyan érint téged a titkosítás a mindennapi életben?	Mindennapi tevékenységeim során nem gondolok a titkosításra	Count	10	21	4	14	49
		Expected Count	6,2	15,7	8,0	19,0	49,0
	Használom, de nem értem teljesen, hogyan működik	Count	2	14	14	20	50
		Expected Count	6,3	16,0	8,2	19,4	50,0
	Tudatosan figyelek a titkosított kommunikációra és adatokra	Count	5	8	4	18	35
		Expected Count	4,4	11,2	5,7	13,6	35,0
Total		Count	17	43	22	52	134
		Expected Count	17,0	43,0	22,0	52,0	134,0

*4. táblázat Hogyan érint téged a titkosítás a mindennapi életben? * Lakhelye*

Forrás: Saját forrás (2023)

Érdekesség, hogy lakhely szerint mutatkozott összefüggés. Ami annak köszönhető, hogy a kisebb településeken élők kevésbé érezték magukat érintve a témában, míg a fővárosiak tudatosabbak a titkosítás terén. A 4. táblázaton láthatóak az összefüggések.

A Chi^2 teszt a válaszok megfigyelt eloszlását hasonlítják össze a két kategorikus változó közötti függetlenség feltételezése szerinti várható eloszlással. Mivel jelenesetben a „Pearson Chi-Square" értéke 17,736, ahol a 0,007, ami jóval alatta van a 0,05-ös szignifikancia szintnek. Ez arra utal, hogy a válaszok eloszlásában a különböző lakóhelyek között megfigyelt különbségek valószínűleg nem véletlenszerűek, amelyet tovább erősít a magas és szignifikáns Lambda és G&K Tau eredmény.

Fontos megjegyezni, hogy a statisztikai szignifikancia nem jelent ok-okozati összefüggést; csak azt jelzi, hogy a változók között kapcsolat áll fenn. További kutatásokra, többek között kvalitatív elemzésre vagy további statisztikai módszerekre lehet szükség ahhoz, hogy megértsük az összefüggés jellegét és az ahhoz hozzájáruló tényezőket.

Hasonló eredményt találtam, a különböző iskolai végzettségű egyének körében a "Hogyan érint téged a titkosítás a mindennapi életben?" kérdésre adott válaszok eloszlásában. A "Középfokú végzettséggel képesítéssel" rendelkezők nagyobb valószínűséggel válaszoltak "Használom, de nem értem teljesen, hogyan működik", így a minta összességében eltávolodott a tudatos kategóriától. Ugyanakkor általánosságban megállapítható, hogy a magassabb iskolai végzettséggel rendelkezők tudatosabbak.

A Chi-négyzet teszt statisztikailag szignifikáns összefüggést mutatott az iskolai végzettség és a titkosítással kapcsolatos attitűdök között. A Likelihood Ratio teszt erősebb összefüggést jelez, a Pearson Chi-négyzet érték 10,318 ($p = 0,035$) és a Likelihood Ratio érték 11,184 ($p = 0,025$). Ez azt jelzi, hogy az egyének iskolai végzettsége összefügg a titkosítással kapcsolatos megítélésükkel. A Lambda (0,089) és a Goodman és Kruskal tau (0,035) mérsékelt összefüggést jelez, irányított hatással. Konkrétan az iskolai végzettség összefügg a titkosítással kapcsolatos attitűdökkel, ami alátámasztja azt a következtetést, hogy e változók között nem véletlenszerű kapcsolat áll fenn.

3.2.2. Milyen mértékben érzik magukat a felhasználók biztonságban

Az előző kérdéshez hasonlóan a „Milyen mértékben érzed biztonságban magad az online tevékenységeid során?” kérdést is megvizsgáltam kereszttáblák segítségével. Az előzőekkel szemben, ennél a kérdésnél más összefüggéseket találtam.

A válaszadók körében a kereszttábla nemek szerinti különbségeket mutat az online biztonság megítélésében. Nevezetesen, a nők nagyobb százaléka érzi magát kevésbé biztonságban az interneten, mint a férfiak. A válaszadók közül a nők 13,4%-a és a férfiak 10,4%-a egyáltalán nem érzi magát biztonságban az interneten, míg a nők 20,9%-a és a férfiak 38,8%-a nagyon biztonságban érzi magát. A Chi-négyzet teszt statisztikailag szignifikáns összefüggést mutat a nem és az online biztonságérzet között (Pearson Chi-négyzet = 5,132, $p = 0,077$). Ez arra utal, hogy a nemek összefüggnek azzal, hogy az egyének hogyan érzékelik biztonságukat az online tevékenységek során. Az irányított mérések gyenge összefüggésre utalnak (Lambda = 0,098, Goodman és Kruskal tau = 0,025). Bár statisztikailag szignifikáns, az összefüggés gyakorlati jelentősége korlátozott lehet.

			Életkor				
			18-24	25-30	31-50	51-65	Total
Milyen mértékben érzed biztonságban magad az online tevékenységeid során?	Nem érzem biztonságban magam egyáltalán	Count	4	1	7	4	16
		Expected Count	6,9	2,9	3,9	2,3	16,0
		% within Életkor	6,9%	4,2%	21,2%	21,1%	11,9%
	Kevésbé biztonságban érzem magam	Count	31	17	20	10	78
		Expected Count	33,8	14,0	19,2	11,1	78,0
		% within Életkor	53,4%	70,8%	60,6%	52,6%	58,2%
	Nagyon biztonságban érzem magam	Count	23	6	6	5	40
		Expected Count	17,3	7,2	9,9	5,7	40,0
		% within Életkor	39,7%	25,0%	18,2%	26,3%	29,9%
Total		Count	58	24	33	19	134
		Expected Count	58,0	24,0	33,0	19,0	134,0
		% within Életkor	100,0%	100,0%	100,0%	100,0%	100,0%

*5. táblázat Milyen mértékben érzed biztonságban magad az online tevékenységeid során? * Életkor*

Forrás: Saját forrás (2023)

A korcsoportok szerinti kereszttáblákat elemezve látható, hogy az egyének eltérően ítélik meg az online biztonságot. A 31-50 évesek nagyobb százaléka érzi magát kevésbé biztonságban online, mint a többi korcsoport. A korcsoportokon belül a 31-50 évesek 21,2%-a egyáltalán nem érzi magát biztonságban az interneten, míg a 25-30 évesek 70,8%-a kevésbé érzi magát biztonságban.

A korcsoportokra vonatkozó Chi-négyzet tesztek statisztikailag szignifikáns összefüggést mutatnak az online biztonság érzékelésével. Mind a Pearson-féle Chi-négyzet, mind a Likelihood Ratio tesztek p-értékei 0,05 alatt vannak, ami azt jelzi, hogy az életkor és az online biztonság érzékelése összefügg. A Chi-négyzet teszt statisztikailag szignifikáns összefüggést mutat (Pearson Chi-négyzet = 10,806, p = 0,095), de az irányított mérések gyenge összefüggésre utalnak (Lambda = 0,023, Goodman és Kruskal tau = 0,032). Vagyis az idősebb korcsoportok kevésbé számoltakbe, hogy biztonságban érzik magukat, míg a legfiatalabb korosztály a vártnál sokkal inkább így vélekedett. Ennek kiértékelése, nem könnyű mivel az egyiknél a felelőtlenség miatt alulsúlyozás lehet a háttérben, az időseknél viszont az ismeretlentől való túlzott félelem miatti önmaguk alulértékelése húzódik meg.

A lakóhely szerinti kereszttáblázatot elemezve kiderül, hogy a különböző helyeken élő egyének eltérően ítélik meg az online biztonságot. A városokban élő személyek kevésbé érzik magukat biztonságban az interneten (62,8%), mint a falvakban és városokban élők. A fővárosban élők inkább nyilatkoztak úgy, hogy biztonságban érzik magukat. A Chi-négyzet tesztek azonban nem mutatnak szignifikáns összefüggést (Pearson Chi-négyzet = 1,595, p = 0,810), amit az irányított mérések (Lambda = 0,014, Goodman és Kruskal tau = 0,014) is megerősítenek. A trend látszódik, de további vizsgálatok szükségesek.

Hasnolóan Az iskolai végzettségi szintekre vonatkozó kereszttáblázatot elemezve látható, hogy a különböző iskolai végzettségű egyének eltérően ítélik meg az online biztonságot. A "Középfokú képesítés nélkül" végzettségűek, akik korábban a gimnáziumot jelölték, közül 13,3% egyáltalán nem érzi magát biztonságban online, míg 35,6% nagyon biztonságban érzi magát. Korábban azt feltételeztem, hogy az iskolai végzettség egyensen arányos a biztonságérzettel, azonban Chi-négyzet tesztek nem mutatnak szignifikáns összefüggést (Pearson Chi-négyzet = 1,595, p = 0,810), amit az irányított mérések (Lambda = 0,014, Goodman és Kruskal tau = 0,006) is alátámasztanak. Vagyis a mintában nincs ilyen összefüggés.

Összességében, míg a hogyan érinti a válaszadókat kérdésnél a nem és az életkor nem, a lakhely és az iskolai végzettség mutatott összefüggést, addig a biztonságérzet kérdésnél éppen fordított a helyzet. A nők és az idősebbek kevésbé érzik maguk biztonságban, míg a lakhely és az iskolai végzettségre nem tudtam ilyen megállapítást találni.

3.2.3. „Mennyire érdekel téged a kvantumtitkosítás és annak fejlesztése?”

Az online kérdőívben külön kérdesekben foglalkoztam a kvantumszámítógépek adta lehetőségekkel. Ezen kérdéseket a fentiekhez hasonlóan elemeztem. A „Mennyire érdekel téged a kvantumtitkosítás és annak fejlesztése?” kérdésre háromfokú skálán tudták érdeklődési szintijüket kifejezni a válaszadók. A második kérdésnél pedig szintén háromfokú skálán a kvantumszámítógéppel kapcsolatos ismeretük mértékét tudták megválaszolni.

Az érdeklődési kérdésnél se a nem, se az életkor, se a lakhely, se iskolai végzettség szerint nem találtam szignifikáns összefüggést. Vagyis elmondható, hogy a mintát tekintve

valamilyen egyébb magyarázót kell találni egy összefüggés indoklásához. Annyi elmondható, hogy a mintában szereplő férfiak enyhén jobban érdeklődtek, a lakhelynél a kitöltő falusiak a vártnál jobban érdeklődtek, illetve az életkornál a fiatalabb korcsoportokat nem érdekelte „eléggé", hogy szingnifikáns legyen az összefüggés.

Az előző kérdésnek némiképp ellentmond, hogy a kvantumszámítógéppel kapcsolatos ismeretek esetében a nem, az életkor és az iskolai végzettség szignifikáns összefüggést mutat. Mivel a férfi kitöltők inkább nyilatkoztak, úgy hogy nagyon tisztában vannak vele (27 fő, a 20 expected counttal szemben). Pearson Chi-Square értéke 7,027, p: 0,03 mellett, így a kapcsolat szignifikánsnak tekinthető. A Lambda és a Tau értéke azonban viszonylag gyenge, ami arra utal, hogy a változók nem függenek erősen egymástól. Hasonlóan összefüggés mutatkozott a mintában az életkor tekintetében a fiatalabb válaszadók inkább válaszoltak a tudásukról, mint az idősek (Pearson Chi-Square :15,791 6; p:0,015), de Lamba éréke szerint a kvantumszámítógépekkel kapcsolatos vélekedések és az életkor között nagyon gyenge kapcsolat áll fenn. Bár statisztikailag szignifikáns, a hatás mértéke minimális, ami azt jelzi, hogy az életkornak korlátozott hatása lehet a kvantumszámítógépekkel kapcsolatos attitűdökre. Az iskolai végzettség szerint a magassabb iskolai végzettséggel rendelkezők inkább vannak tisztában a kvantumszámítógéppel, de a kis elemszám miatt nehéz pontos megállapítást tenni. 10% szignifikacia mellett elmondható, hogy Chi^2 teszt mutat némi összefüggést, de az erősségi tesztek szerint ez igen csekély. Ugyanakkor az lakhely szerint nem találtam semmilyen összefüggést a mintában.

3.2.4. Következtetés

Összességében tekintve a kérdőív kitöltői tudatos felhasználóknak tekinthetőek, akik figyelnek a jelszavaik védelmére és az interneten hagyott „digitális lábnyomuk” -ra. Kijelenthetjük, hogy az iskolai végzettséggel összefügg a titkosítás kapcsolata, vagyis minél magasabb a végzettsége annál figyelmesebb a titkosítás terén a felhasználó. Illetve, kevesen, de figyelmet fordítanak a jövőbeni titkosítási problémákra és a kvantumszámítógép adta lehetőségekre. Továbbá az elemzések során azt a következtetést vonhattuk le, hogy a nők és az idősebbek kevésbé érzik magukat biztonságban, míg a lakhely és a végzettségre nem lehetett megállapítani. Ezen állításokat kiegészítve levonhatjuk, hogy a felhasználók általánosságban lusták a technológia és trendek cseréje terén, jobban szeretik a megszokott dolgokat. A kutatásom magyar kitöltőkkel és magyar szokásokkal vizsgáltam. A kutatásom reprezentatív és nem teljeskörű, mivel csak 134 kitöltő volt.

4. ÖSSZEFOGLALÁS

A dolgozatomnak a célja az volt, hogy a titkosítási trendekbe betekintést adjak, hogy milyen folyamatai vannak, milyen típusai és a hétköznapokban hogyan érint minket. A titkosítást áttekintettük általánosságban, majd részletekbe menően áttaglaltuk az IoT és az 5G hálózatokat. A böngészés követte a HTTPS összehasonlítása a HTTP-vel, majd az aszimmetrikus és a szimmetrikus titkosítást taglaltam. Az internetes témakörnél maradva az SSL/TLS kézfogást mutattam be, amely szorosan kapcsolódik a HTTPS és a levelezés területénél. Érintettem a VPN funkcióját és működését, majd a kétlépcsős hitelesítésre tértem át. A kétlépcsős hitelesítés önmagában egy részletes és sokoldalú témakör, de összesűrítettem amennyire csak lehetett az OTP jelszavakat és a TAN rendszereket. Ezután Basel III csomagot tekintettük át, amely megváltoztatta a banki szektort. Mélyebben elemeztem az otthoni és a kisvállalati hálózatokat, felépítés ügyileg és kiszolgálás terén is. Mivel az otthoni hálózatoknál a kényelem dominál, addig a vállalati hálózatoknál pedig a funkcionalitás a mérvadó. Ugyanakkor a vállalatnál stabilabb, mint gyorsabb a hálózati kapcsolat. A hálózatokból következtetve a vezetékes és vezetéknélküli hálózatokra tértünk át. A vezetékes hálózatot is érinti a titkosítási probléma, mivel a kábel elektromágneses sugárzást bocsát ki, erre kifejlesztettek egy lehallgatás mentes kábelt. A vezetéknélküli hálózatnál pedig a Wi-Fi hálózatok WPA2 és WPA3 rendszerét részleteztem. Végezetül készítettem egy forms-ot, amiben az internetes felhasználóknak feltettem pár kérdést a szokásaik és a véleményeikről, illetve a jövőtechnológiájáról. A kérdések bemutatása után elemeztem a válaszukat és következtettem, hogy ki mennyire tudatos internetes felhasználó.

A titkosítás sok ágát – úgy vélem – sikeresen bemutattam és a jövőbeni alakulást is érintve a jövőbeni esetleges veszélyre felhívtam a figyelmet. Mégpedig a kvantumszámítógép jelszavak feltörésére. A kvantumszámítógép titkosításával kapcsolatban kevés forrást találtam, mivel egy új technológiáról van szó, így alapos kutatásra volt szükség.

IRODALOMJEGYZÉK

1. CASTELLUCCIA, Claude; MYKLETUN, Einar; TSUDIK, Gene. Improving secure server performance by re-balancing SSL/TLS handshakes. In: Proceedings of the 2006 ACM Symposium on Information, computer and communications security. 2006. p. 26-34.
2. CHEN, Gabriel; WANNER, Rick. Secure Email Transmission Protocols--A New Architecture Design. arXiv preprint arXiv:2208.00388, 2022.
3. DANEZIS, George. Traffic Analysis of the HTTP Protocol over TLS. 2009.
4. GUPTA, Kamlesh; SILAKARI, Sanjay. Ecc over rsa for asymmetric encryption: A review. International Journal of Computer Science Issues (IJCSI), 2011, 8.3: 370.
5. HADDAD, Hazim, et al. Development of anonymous networks based on symmetric key encryptions. Journal of Networks, 2011, 6.11: 1533.
6. LAJOS, Nagy; ATTILA, Szalay Zoltán. 5G-MOBILRENDSZER 5G MOBILE SYSTEM. Magyar Tudomány, 2021, 182.6: 732-744.
7. LEVENTE, Buttyán; LÁSZLÓ, Györfi; ISTVÁN, Vajda. ADATBIZTONSÁG: TITKOSÍTÁS, HITELESÍTÉS, DIGITÁLIS ALÁÍRÁS. Magyar Tudomány, 2005, 5
8. MAIL, A. O. L.; BOX, Drop. Two factor authentication. 2017.
9. MIHOLICS, László. Vezeték nélküli hálózatok biztonsági kérdései. 2011
10. PALICZ, Tamás, et al. „Pénzt vagy életet!”–Zsarolóvírusok az egészségügyi informatikai rendszerekben. Orvosi Hetilap, 2020, 161.36: 1498-1505.
11. PRASAD, Anand R., et al. 3GPP 5G security. Journal of ICT Standardization, 2018, 6.1-2: 137-158.
12. SCHULZ, Matthias, et al. Trust the wire, they always told me! on practical non-destructive wire-tap attacks against ethernet. In: Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks. 2016. p. 43-48.
13. TÓTH, András. Az Internet of Things rendszerek biztonsági kihívásai. 2023.
14. Gerencsér András, Elektronikus kommunikáció. 2006

Elektronikus hivatkozások

1. Alza, Mu-Mimo (2023)
   Forrás: https://www.alza.hu/fogalomtar/mu-mimo
   (Letöltés dátuma: 2023.11.06.)

2. Daniel Dunar (2020)
   Forrás: https://www.linkedin.com/pulse/cat-6a-vs-7-daniel-dunar/
   (Letöltés dátuma: 2023.10.17.)

3. Eaton, Ethernet Cables Explained (2023)
   Forrás: https://tripplite.eaton.com/products/ethernet-cable-types
   (Letöltés dátuma: 2023.11.20.)

4. Edward Parker, When a Quantum Computer Is Able to Break Our Encryption, It Won't Be a Secret (2023)
   Forrás: https://www.rand.org/pubs/commentary/2023/09/when-a-quantum-computer-is-able-to-break-our-encryption.html
   (Letöltés dátuma: 2023.11.14.)

5. European Banking Authority, (2021)
   Forrás: https://www.eba.europa.eu/regulation-and-policy/implementing-basel-iii-europe
   (Letöltés dátuma: 2023.12.03.)

6. FinTechShow cikke (2020)
   Forrás: https://fintechzone.hu/igy-alakitotta-at-a-koronavirus-jarvany-a-hazai-e-kereskedelmet/
   (Letöltés dátuma: 2023.11.01.)

7. HTTP2, Wikipédia (2015)
   Forrás: https://en.wikipedia.org/wiki/HTTP/2
   (Letöltés dátuma: 2023.10.28.)

8. Norbert, Bytech cikke (2022)
Forrás: https://bytech.hu/wifi-6/
(Letöltés dátuma: 2023.12.05.)

9. Otp Bank (2023)
Forrás: https://www.otpbank.hu/portal/hu/Adathalaszat
(Letöltés dátuma: 2023.10.12.)

10. Portnox, What is WPA3 vs. WPA2? (2023)
Forrás: https://www.portnox.com/cybersecurity-101/wpa3/
(Letöltés dátuma: 2023.10.27.)

11. Prohardver, (2015)
Forrás: https://prohardver.hu/hir/arm_mikrovezerlokbe_elhozza_trustzone.html
(Letöltés dátuma: 2023.10.22.)

12. SSL Kézfogás (2020)
https://www.ssl.com/hu/cikk/ssl-tls-k%C3%A9zfog%C3%A1s-biztos%C3%ADtja-a-biztons%C3%A1gos-online-interakci%C3%B3t/
(Letöltés dátuma: 2023.11.01.)

13. VPN infok cikke (2021)
Forrás: https://vpninfok.hu/mi-az-az-l2tp-es-hogyan-mukodik/
(Letöltés dátuma: 2023.11.07.)

TARTALMI KIVONAT

A szakdolgozat az informatika egy mindenki által használt területét vizsgálja, mind a biztonsági kérdéseket, mind a titkosítási folyamatokat. A titkosítás jelenlegi állapotát, múltját jeleníti meg és a jövőbeni biztonsági problémákat is a figyelem központjába emeli. A titkosítás több ágát mutatja be, mely területeken használják a felhasználók, hogyan épül be a hétköznapjaikba. Firtatja továbbá azon területeket, mi az optimális hitelesítési folyamat, egy átlagos felhasználó részére. Hogyan kerülhetik ki a hétköznapi felhasználók az akár telefonos, akár internetes csalásokat. Illetve a kisvállalati hálózatok és az otthoni hálózatok közötti különbségek, felépítésük, továbbá a milyen céloknak kell megfelelnie az adott körülmények között. A felhasználói szokásokat elemezve következtet, hogy ki a tudatos felhasználó, ki az elővigyázatos. A dolgozatban kvantumszámítógép adta lehetőségek miatt kialakulható biztonsági problémákat is megemlíti.

SUMMARY

The thesis examines the field of computer science, which is widely used by everyone, addressing both security issues and encryption processes. It portrays the current state and history of encryption, highlighting future security challenges. The thesis presents various branches of encryption, showcasing the areas in which users employ it and how it integrates into their daily lives. It also explores optimal authentication processes for the average user and investigates how everyday users can avoid phone or internet scams. Additionally, it delves into the differences, structures, and purposes of small business networks compared to home networks. By analysing user habits, it draws conclusions about who is a conscious user and who is cautious. The thesis also mentions potential security issues arising from the capabilities of quantum computers.