ÓBUDAI EGYETEM

Keleti Károly Gazdasági Kar
Vállalkozásfejlesztés és Infokommunikációs Intézet

SZAKDOLGOZAT

Biztonságos kommunikációs megoldások a (mobil) üzleti világban

ÓE-KGK
2023

Hallgató neve: **Tóth Gábor**
Hallgató törzskönyvi száma: **T008033/FI12904/G**

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Óbudai Egyetem
Keleti Károly Gazdasági Kar
Vállalkozásfejlesztés és Infokommunikációs Intézet

SZAKDOLGOZAT FELADATLAP

Hallgató neve: Tóth Gábor
Szakdolgozat száma: [redacted]
Törzskönyvi száma: T008033/FI12904/G **Neptun kódja:** [redacted]

Szak: Gazdaságinformatikus
Specializáció: Vállalatinformatikai specializáció

A dolgozat címe: Biztonságos kommunikációs megoldások a (mobil) üzleti világban
A dolgozat címe angolul: Secure methods of communication in the business world
A feladat részletezése:
1. Mutassa be a kommunikációt!
2. Mutassa be, miért fontos a kommunikáció biztonsága!
3. Mutassa be a titkosítási módszereket, információbiztonsági alapelveket!
4. Mutassa be a primer kutatást!
5. Mutassa be, hogyan lehetne biztonságosabbá tenni a kommunikációt, valamint milyen kilátások vannak a jövő kommunikációját illetően?

Intézményi konzulens neve: Fehér-Polgár Pál

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

A szakdolgozat: Nem titkos.

Kiadva: Budapest, 2023. 11. 15.

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

P.H.

.....
Intézetigazgató

A dolgozatot beadásra alkalmasnak találom:

.....
belső konzulens

.....
külső konzulens

ÓBUDAI EGYETEM

Keleti Károly Gazdasági Kar

HALLGATÓI NYILATKOZAT

Alulírott Tóth Gábor (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 1.

_____

hallgató aláírása

TARTALOMJEGYZÉK

ÁBRAJEGYZÉK

TÁBLÁZATOK JEGYZÉKE

1. BEVEZETÉS

Jelen témára esett a választásom, ugyanis a kommunikáció minden eddiginél egyszerűbb, ugyanakkor fontosabb tényezővé nőte ki magát. Az internethozzáférés a magyar háztartások többségében az alap „közművek” közé sorolható, 2020-ban a magyar háztartások 87,6%-a, 2021-ben a 90,8%-a, 2022-ben pedig 91,4%-a rendelkezett vele (Központi Statisztikai Hivatal, 2022). Ma már a mindennapok elképzelhetetlenek nélküle, az otthonról történő munkavégzésnek pedig konkrétan alapfeltétele. A helyhez kötött internetszolgáltatás sok helyen réz érpárról „üvegszálasra” (ma már gyakran műanyag) cserélődött, ezzel is lehetővé téve gyors adatátvitelt, kevés késleltetést, és immunitást az elektromágneses zajokra.

A mobilhálózatok fejlettsége az elmúlt 20 évben hatványozódott, mind lefedettség, mind sávszélesség, mind válaszidő terén. Azonban mindössze az elmúlt 10 év hozta el azt a változást, hogy a gyakorlatilag mindenhová is kitelepült tornyokban rejlő lehetőségeket gyakorlatilag bárki ki tudja használni.

Ez alatt leginkább az árra gondolok. Az egyes telefonok között ár-tudás arányban már közel sincsenek akkora különbségek, mint 10 évvel ezelőtt. Egy 100000 forint alatti telefon is bőven képes azokra az alap funkciókra, melyek egy többszörösébe kerülő telefonban találhatók, legfeljebb néhány viszonyszámban térhetnek el. Az 5G technológia szintén elérhető áron van már. Azonban, ami leginkább áttörést hozott, az a mobilhálózat használati díja, amely szintén az elmúlt 10 évben süllyedt megfizethető szintre. Biztosan megvan sok emberben az a pánik, amikor 2010 előtt véletlenül megnyitotta a telefonján a böngészőt. Ma már akár korlátlan adatforgalmi csomagok hozzáférhetők, ezek stabilitása pedig akár távmunkára is elegendő lehet.

Interneten keresztüli kommunikációra rengeteg platform létezik, legyen az cégen belüli vagy személyes. Ezek gyakran a kulisszák mögött ugyanazokat a protokollokat használják más köntösben és hozzáférhetőséggel, azonban sok olyan közös tényező van, (jó példa lehet a mobil infrastruktúra), amitől minden felhasználó függ, legyen az céges vagy magán.

2. A KOMMUNIKÁCIÓ ALAPJAI

A szó latin alakja communicatio, mely röviden közlést, közzétételt jelent. A kommunikáció elengedhetetlen a mai világ minden területén, anélkül gyakorlatilag semmilyen élőlény nem tud működni. Lehetővé teszi gondolatok, ötletek, tervek, érzések és tapasztalatok megosztását, megvitatását emberek között, de rengeteg tevékenységnek, munkának gyakorlatilag az az alapja. Ma már a humán értelmezésen kívül jóval szélesebb körű ez a kifejezés. Mindenféle információtovábbítás kommunikációnak minősül, az átvitt információ jeleitől, kódjaitól függetlenül.

Nemcsak emberek, de állatok és gépek között is létfontosságú a kommunikáció. Amíg az állatok az idő során alakítanak ki valamilyen jelrendszert, addig az ember a gépek (és akár saját maga) számára alakított ki mesterségesen több milliót. Információcsere nélkül a világ összes elektronikai eszköze semmit nem érne, gyártás lehetetlen lenne, tehát egy jól megalkotott szabályrendszerre volt szükség, amely folyamatosan fejlődik, változik a kor igényei, stílusai szerint.

Az emberi kapcsolatok létszükséglet-értékére már az ókorban rájöttek. Egyre több tudományterület kezdte vizsgálni a kommunikációt különféle szempontok alapján, melynek jelentősége rohamosan nőtt a valóság megismerésének előrehaladtával, valamint a tudományos és technikai vívmányok megjelenésével, és az emberi kultúra bővülésével. Az emberre nézve szükségszerű dolog, mert az ember kénytelen kommunikálni embertársaival, ugyanis a szükségleteit (többnyire) csak rajtuk képes kielégíteni. Elkerülni nem lehet, ugyanis akkor is kommunikálunk, amikor nem teszünk semmit (a válasz hiánya is válasz) (Forgó, 2010, old.: 13-14).

A **kölcsönösség** elve létfontosságú, azaz az egyik fél megnyilvánulása szükségszerű feltétele a másik fél megnyilvánulásának. **Tudati** jelenség, azaz az emberi tudat bizonyos jelekhez jelentéstartalmat köt, azaz kódol, és vice versa. Tudatból kiinduló, és tudatban befejeződő folyamat, azonban nem mindig tudatosan történik! **Folyamatjellegű,** tehát valaki valamiről valamit valamiért valahogyan valakinek el akar mondani. Ebből következik, hogy megtalálhatóak közös jegyek minden kommunikáció során, melyek:

- küldő

- tárgy
- üzenet
- közlés eszköze
- címzett
- kommunikáció eredményessége.

Szerepet játszhat még a másik fél **befolyásolása** is, mely lehet rejtett, nyílt, de akár manipulatív is. **Irányultságát** tekintve lehet közvetlen, vagy közvetett, azaz médiumok által közvetített. Közvetlen esetben nincs a két fél között semmiféle közvetítő eszköz, azaz szimbólum-konvertáló átkódoló nélkül történik a folyamat. Közvetettnél a feleket tér és/vagy időbeli távolság választja el, így valamilyen médium közvetíti az információt. Ez esetben szükséges megfelelő hordozók, közvetítők, megjelenítők, hangszórók használata. Térbeli elkülönülés esetén szinte egyidejű az adás-vétel, de tárolók segítségével áthidalható az időbeli távolság is (pl. videók).

Eszköz- és érzékszervi csatornaigényes, és többcsatornás a folyamat. **A társadalmi méretek szerint eltér**, tehát másképp működik egy személyes, csoport, valamint tömegkommunikációs folyamat. Hierarchizáltság szempontjából is eltérő, azaz egyenrangú körülmények a válaszadás, visszajelzés kölcsönössége alapján, és egyenlőtlenek egy egyirányú közlésnél a visszacsatolás lehetősége nélkül, pl. újság, könyv, TV (Forgó, 2010).

Jellemzően szándékos közlések minősítik az emberi kommunikációt, a nem szándékos közlések pedig minősítik, hitelesítik, vagy éppen tagadják a verbális közlés valóságtartalmát. Éppen ezért meg van különböztetve a direkt csatorna, mely a közlés tartalmára vonatkozik, illetve indirekt csatorna, mely nem tudatos vagy szándékos, de a közlés tartalmával szabályszerű összefüggésben áll, többnyire érzelmi alapon. Ez a megnyilvánulás a közlő és befogadó viszonyáról árulkodik. Azonban ezeken felül akad még néhány tényező, amelyek megléte szintén rendkívül fontos:

- kódolás
- csatorna
- dekódolás
- visszajelzés

- jel
- zaj (Bányász, 2010).

Az információ és üzenet fogalma között lényegi különbség van. Ezeket nagyjából így lehetne jellemezni:

Információ → természetes jel, vagyis nem szimbolikus és nem kommunikatív.

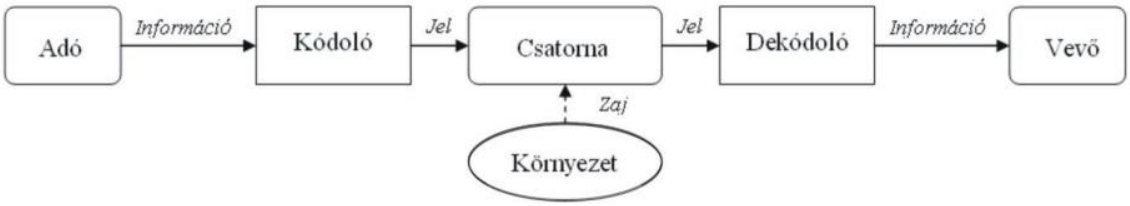
Ember alkotta jel → nem természetes, vagyis szimbolikus kommunikatív.

Színekhez hasonlítva valahogy így nézhet ki: a színinformáció természetes jel, melyet kellő tapasztalat birtokában dekódolni tudunk. Pl. a piros gyümölcs érett, ehető, édes, a vörös égalja pedig időjárás változást jelez.

A kommunikáció szándékolt közlés, melyet szintén értelmezünk, dekódolunk. A színkommunikáció nem természetes, hanem szimbolikus jelekre épül: pl. a piros táblák és lámpák tiltást jeleznek (Földvári, 2017). A jel egy alapfogalom mind az információ, mind a kommunikáció körében, a jelek világára pedig külön tudomány létezik, melyet **szemiotikának** hívnak. Néhány szemiotikai dologra kitérnék. Azt azonban meg kell jegyezni, hogy a szemiotika nem:

- filozófia
- logika
- tudományelmélet
- esztétika
- nyelvészet
- nyelvfilozófia
- információelmélet
- pszichológia
- kommunikációelmélet
- strukturalizmus,

hanem gyakorlatilag társadalomtudomány, amely objektív vizsgálatra és kvantitatív módszerekre törekszik (Horányi & Szépe, 1975).



1. ábra: híradástechnikai modell, (Kucsma Daniella, Miskolci Egyetem GTK, 2018)

A jelek által hordozott információ mindig egy adott funkcióhoz kötődik. Tárgyaktól, jelenségektől függenek, és pont emiatt változhatnak, például új fejfedezések, információk által. A jel tartalma összefügg a társadalmi környezettel és szokásokkal, pl. egy koszorú jelentése más, ha győzelmi jel, és szintén más, ha halotti kultusz része, ezáltal gyakran több jelentésűek.

A jel **szintaktikája** az összetételt, szerveződést, megjelenést, valamint belső struktúrát, és más jelekkel való integrálhatóságot jelenti. Ide tartozik a forma, szín, anyag, mozgás, melyek felépítését és összetételét definiálni kell. A jel **szemantikája** a jelek jelentésével foglalkozik, mire utal a jel. Ennek előfeltétele, hogy legyen egy elfogadott **konvenció** (jel-jelentés kapcsolat). Ismerni kell a kontextusokat, valamint a tartalmakat meg kell tanulni.

A jel **pragmatikája** magát a jelhasználatot vizsgálja, a jel és recipiens viszonyát figyeli. A jelek funkcionálisak, és információt kell továbbítaniuk, valamint hatást kiváltaniuk, pl. cselekvést, viselkedést, mentalitást, érzelmet.

A jelek vizsgálata során egy bizonyos sorrendet kell követni. Először érdemes a szintaktikai elemeket vizsgálni, a jelek egymáshoz való viszonyának áttekintésével, ugyanis ez befolyásolhatja a tartalmat. Ezután következhet a szemantikai analízis, majd utána a pragmatika (Kelenyi, 2006).

2.1. Kódolás, kód

Az állatvilág kutatása során kirajzolódott egy olyan szabályszerűség, hogy minél szociálisabb lény az adott állat, annál komplexebb kommunikációs kódokat használ, és annál jellemzőbb a kódok használata az egyéni kapcsolataik kialakítására, fenntartására. Jelzéseket tekintve az emlősökhöz hasonló módon sokszínűek a társas rovarok, például

méhek és hangyák. Azonban még így is jóval korlátozottabb számú jelzést használ minden állatfaj az emberhez képest.

Az emberi kommunikáció a legösszetettebb, melynek legfőbb része a verbális kommunikáció. Ez az ember egész fejlődéstörténete során alakult ki, a kódrendszer pedig maga a nyelv, ami kulturális terméknek minősül. Ezen felül a nonverbális csatornák is fontos pillérei a közvetlen emberi kommunikációnak. Ezek a jelzések nem konkrét tanulással, hanem örökletesen keletkeznek, és fontos szerepük van a közlendőnk bizonyításában, alátámasztásában. Itt fontos az arcmimika, tekintet, hangsúly, gesztikuláció, testtartás, valamint kulturális szignálok.

A kódok bonyolult hierarchikus szintsorokat alkotnak, ahol az alsóbb szintű rendszer (pl. természetes úton kialakult nyelvek) egy magasabb szintű rendszerbe tartozó jelek (pl. művészet, tudomány jelrendszere) kódolását szolgálja. Ezen hierarchikus sorokba tartozó jelrendszerek közül mindegyik létrehozhatja a szintek rendezett folytonosságát. Leginkább olyan kutatási módszereket dolgoztak ki, melyek a természetes nyelvek szintjei között lévő viszonyokra vonatkoznak, de hasonló feladatok vonatkoznak azon tudományok elméleteiben, melyek saját eredményeik kidolgozásához más tudományok jelrendszereit használják fel. Ilyen mintázatot lehet megfigyelni például a biológia, fizika, és kémia között.

A világ modellezésére használt jelrendszerek mennyisége, bonyolultsága az egyén és a társadalom fejlődési szintjének is értékmérője lehet. A jelrendszerek számának állandó növekedése elengedhetetlenné teszi az egyik jelrendszerről a másikra való fordítás kutatását, ideértve a természetes nyelvről mesterségesre való gépi fordítást is, valamint a különböző jelrendszerek egységesítését, amely a szemiotika legfontosabb kiegészítőjének tűnik fel a tudományos problémák szintézisében. A tömegkommunikáció eszközeinek gyors fejlődése fontos és sürgető követelménnyé tette a társadalomban az információáramlás csatornáinak kutatását, mely szorosan kötődik az utóbbi évtizedben az információelmélet terén végzett kutatásokhoz is.

A társadalmi kapcsolatok csatornáinak elemzése a közösség tanulmányozásának egyik módja, mellyel kapcsolatban nemcsak a jelrendszereknek az egész társadalomban való elterjedései érdekesek, hanem a jelrendszerek kriptográfiai felhasználásának sajátosságai

is. A szemiotikai módszereket bátran hasonlíthatjuk a matematika jelentőségéhez a természettudományokban, de maga a matematika, mint jelrendszer, beletartozik a szemiotikai elemzés tárgyainak szférájába, valamint a szemiotikát is áthatják a matematikai eszmék és módszerek. A szemiotika megteremtője a matematikai logika egyik vezéralakja, Peirce volt, akinek tevékenysége folytatódott Morris és más olyan mai kutatók munkáiban, akik Peirce hagyományait Carnap logikai módszereivel egyesítették.

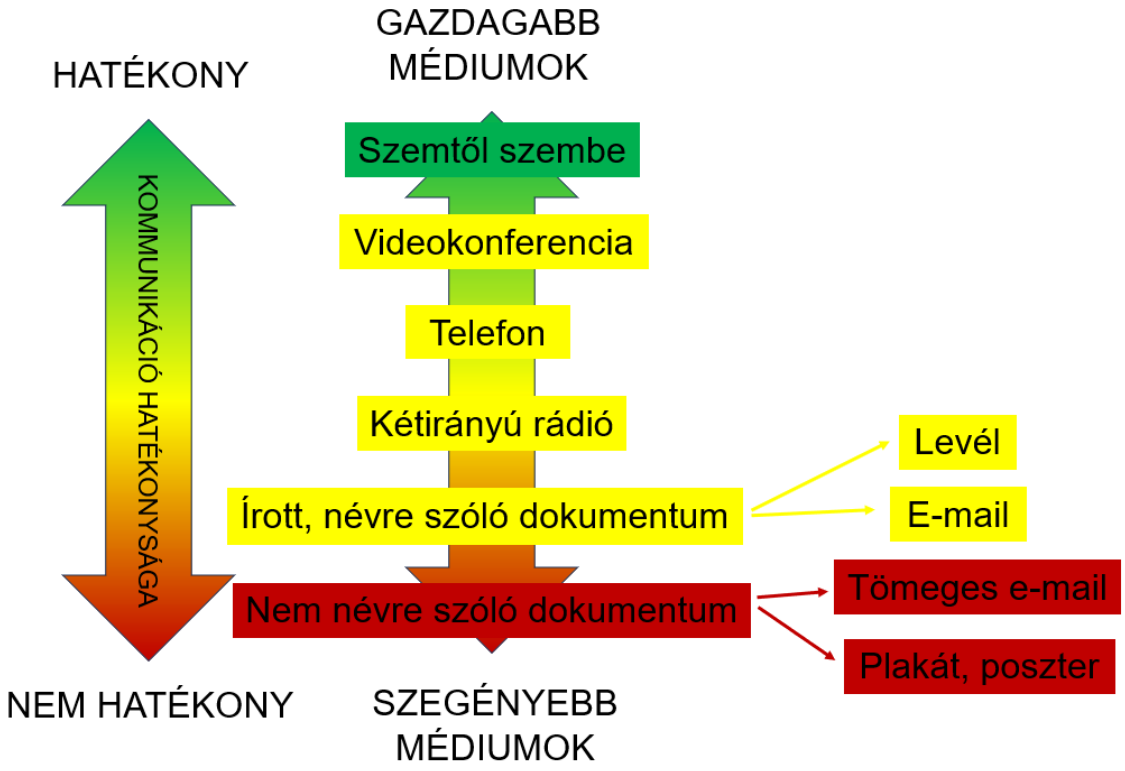
A legegyszerűbb jelrendszerek teszik lehetővé azoknak a módszereknek a kidolgozását, amelyeket a későbbiekben alkalmazni lehet a bonyolultabb rendszereknél, ezért is fontos az elemi rendszerek tanulmányozása (pl. kártyajáték, vasúti jelzések). De még ezeket az egyszerűbb rendszereket is a matematikai pontosságtól távoli humán terminusokkal kell leírni, a kutatás bonyolultabb tárgyainak leírásához szükséges formális nyelvek kidolgozását pedig csak most kezdtél még el (Horányi & Szépe, 1975).

2.2. A kommunikációs csatorna

A csatorna egy közeg, amely információtovábbításra alkalmas. Az információt közvetítheti papír, elektromágneses rezgés, levegő, de akár egy harmadik személy is.

Ezek közül a legfontosabbak:

- Szóbeli,
- írásbeli,
- vizuális,
- digitális,
- nonverbális
- közösségi média,
- tárgyi kommunikáció,
- média.



2. ábra: kommunikációs csatornák és hatékonyságuk (Lumen Learning, d.n.)

A leggyakoribb és legegyszerűbb az emberi beszéd, amely hang útján terjed, valamint az ezzel párhuzamosan történő testbeszéd. Ahogy feljebb (2.1) is elhangzott, az emberi kommunikáció során a testbeszéd is hatalmas szerepet játszik, ugyanis az a fő eszköze a mondanivaló alátámasztásának, valamint verbális kommunikáció nélkül, önmagában is megállja a helyét. A vokális, azaz hanggal történő kommunikáció gyakorlatilag bele van kódolva a verbálisba, és szintén jelentős szerepet játszik. Hanggal ki tudjuk fejezni a lelkiállapotunkat, erősen jelzi a belső feszültség változásait. A vokális kommunikáció elemeit tudatosan alkalmazzuk, és minden embernél egyedi jellemzőkkel bír. A heves érzelmi kitörések magas hanggal, míg kiegyensúlyozott érzelmi állapotban történő közlések alacsonyabb hanggal történnek. Sok múlik az adott ember beállítottságán is; egy gátlásosabb ember halkabban, egy agresszívebb ember többnyire hangosabban beszél.

Nonverbális kommunikáció több részből tevődik össze. Legjelentősebb ezek közül a mimika, melynek többsége nem tudatos szinten jelenik meg. A verbális üzenettartamot befolyásolja, és egybeolvad vele. Szintén fontos még a tekintet, mely visszajelzést ad a megértésről, valamint a másik személyhez való érzelmi viszonyról, és többnyire

akaratunktól függetlenül lép fel. A szemkontaktus a legrégebbi kapcsolat felvételi és fenntartói forma. Ha kedveljük a kommunikációs partnerünket, akkor a szemkontaktust hosszabb ideig fenntartjuk, ha nem, akkor rövid ideig. A tekintet iránya és tartalma szerint különböző jelentésekkel bírhat, ideértve a kontaktus kerülését is, valamint kultúránként is változhat.

A fej, kezek, kar mozgása is feltűnő és fontos jelentéseket hordoz. Vannak olyan gesztusok, amelyek helyettesítő szerepet töltenek be, de olyanokat is ismerünk, amelyek megerősítik, vagy tagolják a beszédet, a mondottak egymáshoz való viszonyát jelzik. A gesztusok sokkal figyelemfelkeltőbbek, mint a mimika és tekintet, mivel jobban figyelünk a mozgásra.

A fej gesztusai világosan értelmezhetőek: oldalirányú mozgás bizonytalanságot jelent, a fej lehajtása pedig bűntudatot, szomorúságot. A kéz gesztusai viszont több jelentéssel bírhatnak: hívhatunk, elutasíthatunk, köszönhetünk, azonban ez is nagyon sokszínű kultúránként (Bányász, 2010).

Alapvetően megkülönböztetünk egyirányú és kétirányú kommunikációt. Kétirányú esetben a hallgatónak van módja visszajelzésre, azaz a beszélő és hallgató állandóan szerepet cserélnek, azonban nem mindig egyenrangú a viszonyuk. Gyakori az olyan helyzet, amikor a partnerek között egyenlőtlen viszony lép fel. Ha a feladó és címzett egyszerre, azaz egy időben és egy helyen vannak jelen a kommunikációban, akkor közvetlen kommunikációról beszélhetünk. Bármilyen térbeli, időbeli eltérés esetén már csak közvetett kommunikációról beszélhetünk, azonban ettől még továbbra is lehet egy vagy kétirányú. Kétirányú, közvetlen kommunikációra tipikus példa, hogy 2 ember beszélgetnek valahol. Egy telefont – akár írásban, akár telefonálva – közbeiktatva, rögtön közvetetté változik a kommunikáció. Egyirányú kommunikáció lehet egy előadó egy tömeg előtt, TV-t közbeiktatva viszont ez is közvetetté válik (Centroszet Szakképzés-szervezési Nkft., d.n.).

2.3. Kommunikációt befolyásoló tényezők

Minden ember egyedi gondolkodásmóddal rendelkezik, eltérő értelmet tulajdonít az egyes üzeneteknek. Sok tényező befolyásolhatja, hogy az adott kommunikáció mit is jelent az egyénnek, többek között az adott információcserében játszott szerepe, és maga az egész helyzet is. Az értékek tükrözik azokat a dolgokat, melyeket az egyén fontosnak tart az életben, és ezek szintén befolyásolják a kifejezésmódot, valamint gondolatok értelmezését. A fejlődési szint, környezet, személyes tér, valamint nem szintén fontos tényezők. Érzelmek is befolyásolhatják azt, ahogyan valaki kommunikál, és viszonyul másokhoz, és ezek az üzenetek téves értelmezését, vagy figyelmen kívül hagyását is okozhatják. A kultúra alakítja ki az emberekben a világképet, előítéleteket, és a nyelv, hangsúly, beállítótás szintén a kultúrából ered.

A tudásszintek közti különbség is bonyolulttá teheti a kommunikációt, tehát meg kell találni egy „közös hangot” ilyen téren is. A szereplők egymás közti viszonya, valamint a konkrét társaság, mint környezet is befolyással lehet a folyamatokra.

A zavar formái lehetnek:

- **Kóros: az adóban keletkezik a zavar**, pl.: betegség, érzékszervi fogyatékosság, tudatzavar
- **nyelvi szocializáció hiánya, pl.:** iskolázottság hiánya, családi szocializáció hiánya,
- **szövegtúltengés, pl:** az adónak nincs mondanivalója, vagy épp túl sok van,
- **zsargon:** szűk csoport által használt kifejezések, belsős poénok, másokat gyakorlatilag kizár a kommunikációból,
- **általánosítás, közhely, pl:** igénytelenség, eredeti ötletek hiánya,
- **kulturális eltérésekből adódó félreértések, pl:** hangszínek közti különbség, emblematikus jelek közti különbség,
- **durvaság, vagy eufemizmus,**
- **hazugság, hallgatás,**
- **szégyenlőség, gátlásosság, pl:** gesztusokban, mimikában, tekintetben, hangszínben.

Az így fellépett zajokat el lehet nyomni többféle módszerrel. Ezek közül a legegyszerűbbek:

- Csendes környezet kiválasztása: lehetőség szerint minimalizálni a konkrét szó szerinti hallható zajt, ez igaz mindenféle csatorna alkalmazása esetén
- Időzítés: érdemes olyan időpontban konzultálni, amikor a legkisebb a társaság, lekisebb a forgalom, sokan vannak otthon stb.
- Artikulálás, érthető beszéd: a fontos információkat hangosan, többször érdemes elmondani
- Rövid, és világos üzeneteket fogalmazzunk meg, érdemes kerülni a bújtatott kifejezéseket.
- Érdemes kérdéseket feltenni és megerősítést kérni, ezzel is kiküszöbölve a félreértéseket (Seres, 2010).

3. ELEKTRONIKUS KOMMUNIKÁCIÓ, VALAMINT ANNAK BIZTONSÁGOSSÁ TÉTELE

3.1. Mi az az elektronikus kommunikáció?

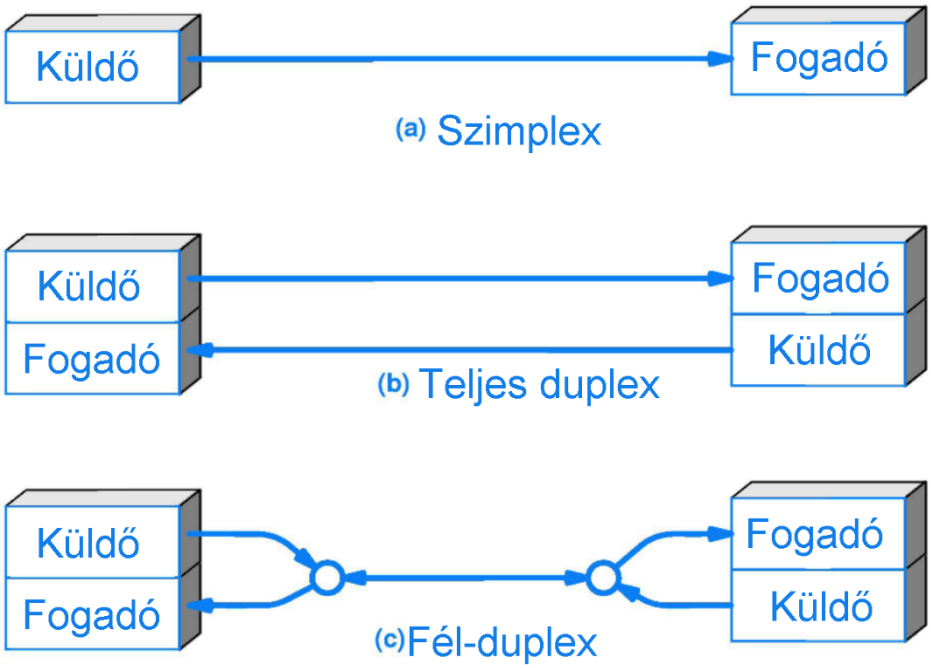
A szemiotika és egyéb társadalomtudományi leírások után érdemes közelebb kerülni a fő témához. Valamilyen elektronikus kódoló-dekódoló berendezést beiktatunk akár az írott, akár a szóbeli közléseinkbe, ezzel teremtve kapcsolatot a felek között.

Elektronikus adattovábbítás során 3 alapvető módszert különböztetünk meg.

Szimplex: Az információ csak egy irányba halad, a feladótól a fogadó felé. A fogadó fél nem képes válaszolni vagy visszajelzést küldeni, nincs lehetőség a kommunikáció folyamatos ellenőrzésére. Olyan helyeken használják, ahol nincs szükség visszajelzésre vagy válaszra, többnyire informatív célok esetén. Ilyen lehet a TV, utaskijelzők, rádió, újság, videók, mérőberendezések.

A félduplex kommunikáció esetén lehetséges az információ áramlása mindkét irányban, de nem egy időben. Adott pillanatban az egyik fél közöl míg a másik fél hallgat, majd megfordulnak a szerepek. Ezt a rendszert többnyire walkie talkie rádiók használják (pl. tűzoltóság, rendőrség, rendezvényszervezés), viszont a WiFi is ide tartozott egészen a WiFi 6-ig.

A teljes duplex kommunikáció olyan adatátviteli mód, ahol az információ kétirányú és egyidejű, azaz mindkét fél egyszerre képes adni és fogadni. Ez lehetővé teszi a szimultán kétirányú kommunikációt, amely legtöbbször az interaktív beszélgetések, telefonhívások és videochat alkalmazások alapja. A legismertebb felhasználása az Ethernet, VoIP, telefonálás, valamint már a WiFi 6 is, de a mobilhálózatok is így működnek.



3. ábra: szimplex, teljes-, és félduplex összeköttetés (BlackBox.co.uk, 2023)

Az internetes VoIP (Voice over Internet Protocol) szolgáltatások, például a Skype és a Zoom, lehetővé teszik a teljes duplex hang- és videokommunikációt az interneten keresztül. A későbbiekben részletesen is kitérek rá.

Kezdve az elejéről, az egyik legprimitívebb példával: **gramofon**. Teljesen analóg, de már (általában) áramot igénylő eszköz, amely a felvett hangot mechanikusan tárolja egy korongon, barázdák segítségével. Az írás-olvasás folyamata gyakorlatilag megegyezik. Ez egy egyirányú kommunikációt lehetővé tevő gép, amely az adott pillanatban hallható hangokat örökíti meg. Szimplex módon „kommunikál” (Wikipédia, 2023).

Szintet lépve a technológiában, képbe jön a **távíróberendezés**. Samuel Finley Breese Morse találta fel, akinél egy családi tragédia vezetett a gép megálmodásához. Morse célja volt az azonnali adatátvitel, ugyanis a kor optikai, szemaforos, vagy elektrokémiai távírógépei lassúak és hosszú üzenetekre alkalmatlanok voltak. 1832-ben mutatták be neki az elektromágnest, ezzel megszületett fejében a forradalmi ötlet. Ez egy félduplex berendezés, tehát mindkét irányban működik.

Több évnyi gondolkodás, fejlesztés, szerelés után 1837. szeptember 4-én Morse bemutatta az elektromágneses távírót, amely akkor 500 méterrel távolabbról gond nélkül

üzent. Az ehhez tartozó kódot maga Morse fejlesztette ki, amelyben minden betűt számokkal kódoltak, viszont ez túl bonyolultnak látszott. Lecserélték olyan kódolásra, amely már betűket is tartalmazott, azonban ez is túl soknak tűnt. Végül Morse asszisztense, Alfred Lewis Vail találta fel a ma is használatos amerikai Morse kódot (Wikipédia, 2023). Ezután 1844-ben már Washington és Baltimore között (légvonalban kb. 38 mérföld) történt üzenettovábbítás. Mindezek után Morse pereskedett, hogy az asszisztense által kitalált kód kizárólagos tulajdonosa lehessen, valamint tagadta, hogy a megvalósításhoz bármiféle elméleti segítséget kapott volna. A Morse-féle távíró több változatban is létezett: egygombos, illetve konkrét billentyűzetes „betűíró" kivitelben (Magyar Tudományos Akadémia - National Geographic, 2016), (Wikipedia, 2023).

A telefont a közhiedelem szerint Alexander Graham Bell találta fel majd mutatta be 1876-ban, azonban rajta kívül még rengetegen közreműködtek a fejlesztés során. A klasszikus módon vett telefon analóg módon, elektromos árammá kódolva továbbítja a hangot vezetékeken, valamint közéjük iktatott jelismétlőkön, kapcsolóközpontokon keresztül.

Minden telefon teljes duplex rendszerű, és kötelezően rendelkezik egy mikrofonnal és hangszóróval, valamint legtöbb esetben szükséges rájuk egy jelző (pl. sípoló, csörgő, esetleg fényjelző) és valami beviteli eszköz, amin a másik fél telefonszámát beírhatjuk (Wikipédia, 2023).

A kezdetleges telefonok idején az emberek 1-1 lakás között húzattak ki kábelt, nem volt igény arra, hogy több emberrel beszéljenek, azonban ez gyorsan megváltozott. Puskás Tivadar szeretett volna egy európai távíróközpontot létesíteni, azonban a tőzsdések ezt leszavazták attól félve, hogy a központban a hírek kiszivároghatnak. Ekkor értesült arról, hogy időközben feltalálták a telefont is. Ennek hatására kiment Amerikába, és látta ahogy pókháló módon néznek ki a telefon és távíróvonalak. Felkereste Bellt, akitől addigra már Edison vette át a telefon ügyeit, és Puskással karöltve elkezdtek fejleszteni.

Az első központot 1878-ban nyitották a Connecticut állambeli New Haven-ben, de 79-ben Puskás már Párizsban építette a következőt. Minden előfizetőt a központhoz kötöttek, ezzel eltüntetve a rendezetlenséget. Budapesten 1881. május 1-jétől működik. A központokban a diszpécser akár 100-200 vonal kapcsoltatását intézte, konkrét kábelek

dugdosásával egy hatalmas táblán lévő aljzatokba. Ezt a rendszert később automatizálták, először elektromechanikus, majd később digitális módon (Wikipédia, 2023).

Térjünk át kicsit a „mobil” részére a dolgoknak. Az 1920-as években hatalmas áttörést jelentett az AM (amplitudómoduláció) rádió feltalálása. Ezek kezdetben tekercset és detektort használtak (detektoros rádió), semmilyen erősítő elemet nem tartalmaztak és áramellátásra sem volt szükségük. A detektoros rádiók nagy méretű antennát és nagy térerőt igényeltek, valamint hangerőben sem voltak túl jók, ezért rövidesen elektroncsöves erősítéssel oldották meg a dolgot. Ez elsősorban szimplex eszköz, tömeges kommunikáció hallgatására használták (Wikipédia, 2023).

Szintén AM-et (de ma már inkább Narrow Band FM, röviden NBFM-et) használó, már félduplex rendszerű a CB rádió, ami már gyors, könnyen használható volt bárki számára, és elég nagy hatótávval is bírt. Az információ azonnal eljutott A-ból B-be, vezetékek nélkül, 27 MHz környéki frekvenciákon. Magyarországon is népszerű rendszer volt és a bejelentése nagy eseménynek számított, ugyanis a rendszerváltás előtt (főleg politikai okokból) meglehetősen nehéz volt az átlagembernek telefonszolgáltatáshoz jutni, és minden távközlő berendezés szigorúan ellenőrzött volt. A CB felforgatta az egész országot elérhetősége és könnyű használata miatt, barátságok, ismeretségek, klubok alakultak ki rajta keresztül. Később leginkább taxisok és kamionosok kezdték használni, ez utóbbi ma is fő célközönsége a rendszernek (Wikipédia, 2020). Ezt ma már sokszor leváltotta a VHF frekvenciatartományban üzemelő, NBFM vagy egyéb digitális modulációt használó rádió (Kövendi, 2017).

A repülésben mai napig használatos és alap a rádiókommunikáció, amelyhez egy külön mesterséges „nyelvet” fejlesztettek ki, ez pedig a **fónia**. Az 1944-ben létrejövő ICAO (Nemzetközi Polgári Repülési Szervezet) vezette be azzal a céllal, hogy az akkoriban elég kaotikus kommunikációt egységesítse, akkor még elég szerény szókinccsel. Később, 2000-es évek elején az ICAO statisztikái alapján kiderült, hogy ez még mindig nem elég, ugyanis a repülési balesetek jelentős részében nyelvi problémák játszottak közre. Ezért kifejlesztettek egy 6 szintű vizsgarendszert (melyből 4-5-6 elfogadható), és minél jobban teljesít valaki, annál ritkábban kell a vizsgát ismételnie. A mai fóniát (elméletben) a világon mindenhol ugyanúgy beszélik, gyakorlatilag az angol nyelv végtelenül

leegyszerűsített, néhány 100 szóból álló változata. Pontosan azért jött létre, hogy a félreértéseket, félrehallásokat megelőzzék, ugyanis a repülés egy nagyon biztonságkritikus terület. Irányváltoztatásra, magasságváltozásra, viharok kikerülésére, valamint fel- és leszállási engedélyre vonatkozó utasításokat lehet rajta megvitatni (HungaroControl, 2021).

Ehhez kapcsolódik a rádióamatőr tevékenység, ami szintén egy vizsgához kötött dolog, és különböző célok által művelhetik művelői:

- Hullámterjedési megfigyelések
- Antenna konstrukciók
- Rádió áramkörök tervezése, építése
- Digitális jelfeldolgozás, moduláció fejlesztés
- Adat és hangtovábbítás TCP/IP-t használva
- Rendszerek összekapcsolása TCP/IP-t használva
- DX-elés, azaz nagy távolságú összeköttetések
- Minél távolabbi, minél különlegesebb rádióállomással összeköttetés (pl. Nemzetközi Űrállomás) (Wikipédia, 2023)

CB-vel ellentétben az amatőr rádió gyakorlatilag bármelyik frekvenciatartományban működhet (ha az épp nem ütközik törvénybe és/vagy fontosabb használatban lévő dologba). Ma már eléggé kihalófélben van a rádióamatőr szokás, leginkább az Internet elterjedése miatt, azonban még mindig vannak Magyarországon is követői, az ilyen úton szerzett megfigyeléseiket pedig büszkén teszik közzé a közösségi oldalakon.

Ezek azonban még eddig kb. végig analóg kommunikációs módszerek. Egy analóg jelátvitelt nem nehéz lehallgatni, CB rádiót bárki vehet aprópénzért, amivel bármely más CB felhasználó beszélgetéseit lehet venni, akár beleszólni is. Ugyanez igaz az amatőr rádiózásra is. Az 90-es években népszerű analóg, de vezeték nélküli telefonokat sokszor szintén egy egyszerű CB vagy VHF rádióval lehetett fülelni, és a primitív vezetékes telefonoknál is egy egyszerű lakatfogó jelenthette a dolgok nyitját. Ezen sokat segített később a digitalizáció, azonban 100%-ig biztonságos rendszer mai napig nem létezik.

3.2. Digitalizáció

1964-ben a Xerox szabadalmaztatta a ma is használatos faxot, azonban az igazi áttörést a két évvel később kiadott faxgépük hozta, ami „csak” 21 kg-os, társaihoz képest könnyen használható volt, és bármely telefonrendszerhez csatlakoztatva működött, valamint 6 perc alatt továbbított egy levélnyi szöveget. Az 1980-as években kifejlesztették a digitális faxot, és ekkortájt virágkorát élte a fax, azonban 2000-re eléggé megritkult a használatuk, manapság többnyire csak Japánban használják, ugyanis mai napig megbízhatónak és biztonságosnak számít (Wikipedia, 2023).

1981-ben az Európai Posta és Távközlési Konferencia létrehozta a Groupe Spécial Mobile bizottságot. 1987-ben 13 európai ország 15 képviselője írt alá egy egyetértési nyilatkozatot Koppenhágában egy közös celluláris telefonrendszer kifejlesztéséről és beüzemeléséről, erre pedig a 900 MHz-es frekvenciasávot ajánlották. Az első GSM hívás 1991. július 1-jén történt, 1992-ben pedig az első SMS-t. 93-ban elindult az első 1800 MHz-es rendszer is, valamint ugyanekkor Ausztráliában üzembe helyezték az első, Európán kívüli GSM hálózatot. 1995-ben már kereskedelmi adat és SMS forgalom működött GSM-en keresztül, 98-ra az előfizetők száma a 100 milliónál járt (Wikipédia, 2023).

Ez egy olyan rendszernek bizonyult, ami a korábbi analóg technológiákhoz képest sokkal biztonságosabb, újításként pedig forradalmi, ugyanis a további mobilkommunikációs rendszerek végig a GSM-en alapultak. Egy GSM kapcsolatot ugyan részben le lehet hallgatni, de teljesen dekódolni, visszafejteni mai napig szinte lehetetlen, erre csak a Nemzetbiztonsági Szakszolgálatnak van esetleg lehetősége.

Áramkör-kapcsolt hálózatról lévén szó, ha telefonálásra kerül sor, egy mátrix alapú kapcsolatot létesít küldő és fogadó között, abba másnak beleszólása nincs. Erre a célra 2 különböző rendszert tartanak fenn a szolgáltatók: egy áramkörkapcsolt a telefonálásra, és csomagkapcsolt az adatátvitelre (GPRS) (Ghodbane, d.n.).

A GSM egy úgynevezett „kérdés-válasz” mechanizmus alapján ellenőrzi a felhasználó kilétét. Kezdetben a hálózat egy 128 bites véletlen számot (RAND) küld az előfizető telefonjának (MS). Ez később egy 32 bites választ generál (SRES), melyhez a RAND

titkosítását alapul véve használja a hitelesítési algoritmust (A3), és az egyedi felhasználói kulcsot (Ki). A felhasználói kulcs soha nem kerül „adásba”, az csak a SIM kártyán, valamint az AUC, HLR, és VLR adatbázisokban szerepel. A mobilhálózat miután megkapta az SRES-t (választ) az előfizetőtől, megismétli ezt a kalkulációt az azonosításhoz. Ha a két helyen számított érték megegyezik, akkor sikeres volt a hitelesítés, ha nem, akkor megszakad a kapcsolat hitelesítési hibával.

Minden számítás a SIM kártyán belül zajlik, ugyanis a SIM tartalmazza a titkosítási kulcs (Kc) generálásához használt algoritmust (A8). Ezt a kulcsot úgy számítja ki, hogy a RAND-ot az A8 algoritmus bemeneti paraméterként használja, az egyedi felhasználói kulccsal (Ki) együtt. A „Ki” értékét sem a SIM, sem a mobilhálózat, sem a telefon nem fogja felfedni soha. Ezen felül, a GSM hálózat köteles a „Kc” értékét változtatni megadott időközönként, amelynek kiszámítását szintén a SIM kártya végzi.

A beszéd és adatforgalom is egy külön titkosítási algoritmussal (A5) zajlik. Ennek kezdetét egy titkosítási mód parancs vétele jelenti hálózati oldalról, és az így titkosított forgalom megindul a hálózaton az A5 és a Kc igénybevételével. Egy további biztonsági réteg a TMSI (Temporary Mobile Subscriber Identity), amely az előbb említett kezdeti hitelesítést követően jut el a mobiltelefonra. A TMSI csak azon a területen érvényes, ahol kiállították, ezen kívüli kommunikációhoz Location Area Identification használata szükséges a TMSI-n kívül. Az így folyó adatok ugyan biztonságosnak mondhatóak, de az itt használatos SMS kommunikáció már kevésbé. Ezt valószínűleg nehéz még így is „menet közben” lefülelni, viszont a szolgáltató tökéletesen lát minden ki- és bemenő üzenetet, ez pedig nem túl jó (Tutorialspoint, d.n.).

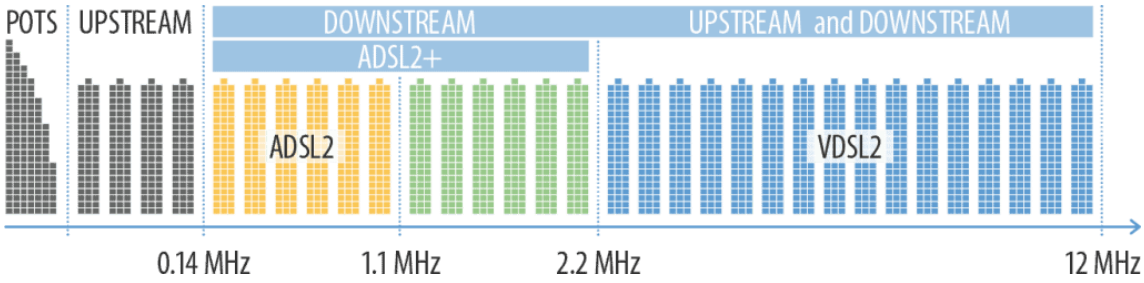
Ebben az időszakban kezdett el terjedni a ma már szintén forradalmi jelentőségű Internet. Ennek története még a GSM előtti időszakra nyúlik vissza, 1960-as évekre. Az USA akkori elnöke, Eisenhower, a Szputnyik-1 fellövésének hírére elrendelte a DARPA (Defense Advanced Research Project Agency) megalapítását. Ez a testület finanszírozta a későbbiekben egy többközpontú, decentralizált, csomagkapcsolt hálózati protokollt, melyet NCP-nek hívtak, és a mai TCP/IP elődjének tekinthető, majd 1969-ben ezt a szabványt használva indult el az ARPANET (Advanced Research Projects Agency

Network). Ez a hálózat elsősorban katonai célokat szolgált, de egyetemi, katonai, valamint kormányzati laboratóriumok közti információcserére is használták.

Nem sokkal később, 1972-ben elkészült az első e-mail, 74-ben a konkrét „internet" kifejezés. 1985-86 között kiépítették az NSF 6 nevű szuperszámítógép központját (NSFNET), majd ezt összekötötték az akkor már 10 éve működő ARPANET-tel. Az NSFNET mai napig jelentős gerinchálózat az USA-ban. Ezt követően több száz különálló hálózaton több tízezer gépet kapcsoltak az azóta is folyamatosan növekvő internethez.

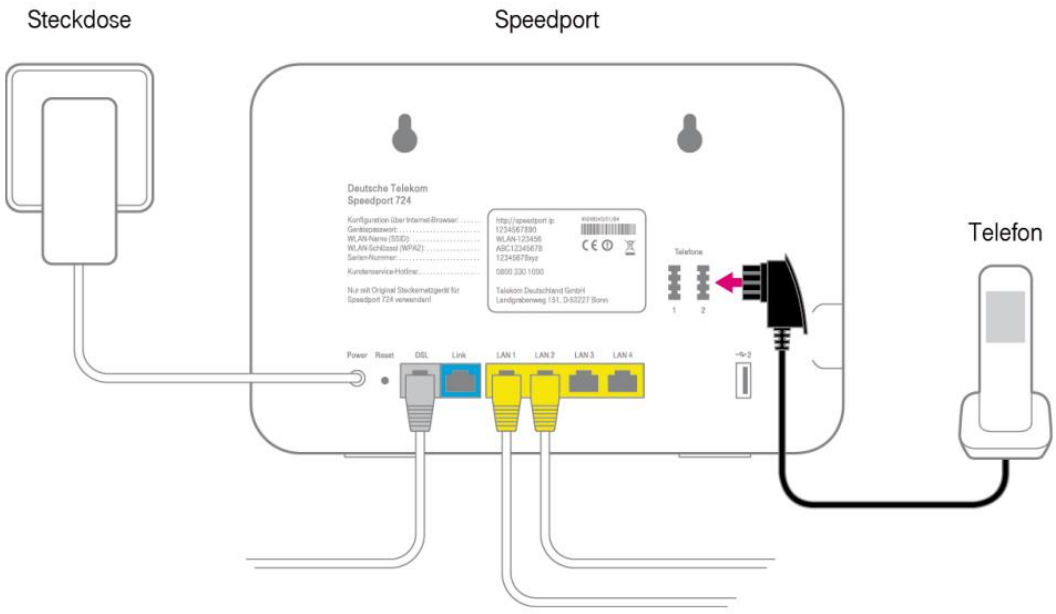
Az internet decentralizált, bármely pontja képes kapcsolatot teremteni bármely pontjával, épp ezért hozzáférhető, és ma már gyakorlatilag létszükséglet a mindennapi életben. Az e-mail után hamar megérkeztek a hírcsoportok, majd információkeresők, és végül 1992-ben a World Wide Web, mely leginkább a CERN-nek köszönhető, innentől pedig már egy laikus is tudta használni. Magyarországon az első domaint 1991-ben jegyezték be, 1995-ben pedig a Matáv lakossági és üzleti ISDN szolgáltatást is biztosított, azonban a lakosság többsége ekkor még néhány kilobit sávszélességre alkalmas telefonos modemmel internetezett. Ez volt az általános egészen addig, 2001-ben pedig DSL technológia került bevezetésre. Mire többmilliós nagyságrendben elterjedhetett volna a betárcsázós kapcsolat, addigra a DSL megfizethetővé és könnyen elérhetővé vált. (Wikipédia, 2023).

A DSL (Digital Subscriber Line) egy hatalmas áttörést jelentett az internetelérésben, mind sávszélesség, mind kényelem terén. Már a kezdeti (ADSL) változatai is a betárcsázós elérés által biztosított sávszélesség többszörösét voltak képesek átvinni, a telefonvonalon folyó analóg kommunikáció befolyásolása nélkül; a telefon „beszédforgalmi" frekvenciatartománya felett működött. Külön érdemes megemlíteni, hogy mindezt a már sok 10 éve kiépített réz érpár telefonkábeleken tette, gyakorlatilag újra hasznosítva azokat.



4. ábra: ADSL2 és VDSL2 frekvenciatartományai az analóg beszédforgalom (POTS) mellett (Tyler Cooper, BroadbandNow, 2023)

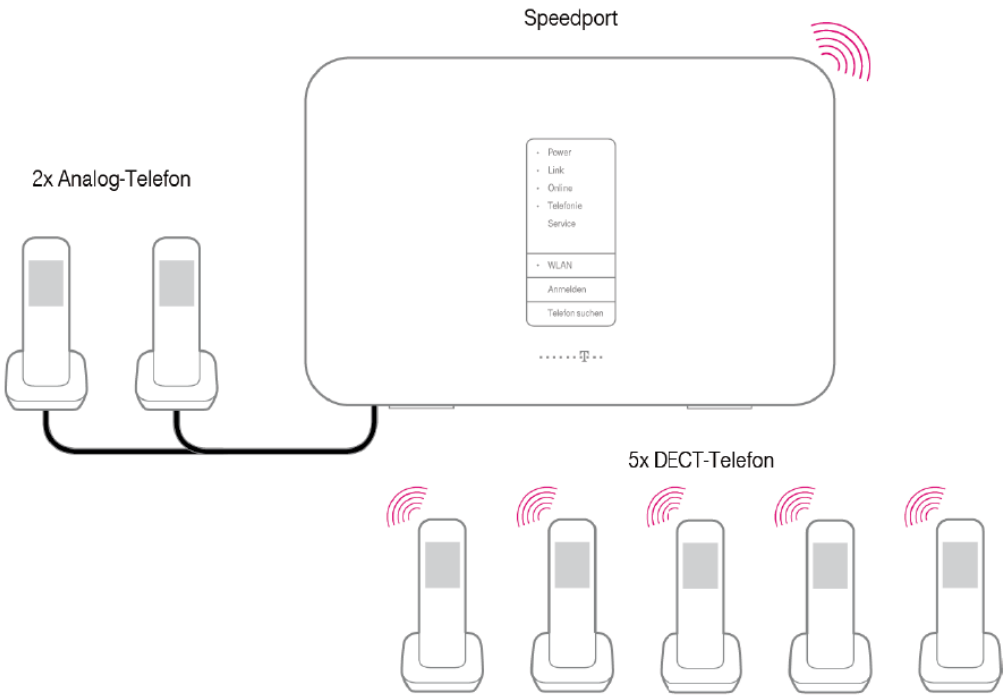
Idővel ez a szabvány is sok fejlődésen ment keresztül, a mai VDSL2 már másodpercenként akár 300 megabit átvitelére is képes, továbbra is ugyanazt az kábelt használva (Cooper, 2023). Ma már az analóg telefonálás nagyon ritkán folyik DSL forgalommal párhuzamosan egy kábelen, a szolgáltatók inkább kizárólag DSL forgalomra nevezik ki azt, ezzel nagyobb stabilitást és sávszélességet eredményezve, a „tradicionális" DSL modemek helyett pedig egyesített modem+router eszközöket biztosítanak az ügyfeleknek. Ez az eszköz a felhasználók többségének igényeit tökéletesen lefedi; megfelelő WiFi lefedettséget biztosít, valamint általában rendelkezik legalább 3-4 Ethernet porttal.



5. ábra: Telekom Speedport W 724V: példa a fent említett modem+routerre (Deutsche Telekom, 2014)

A vezetékes telefon 2010 óta egyre ritkább, azonban hogyan oldják meg ma a szolgáltatók, ha a megmaradt telefonhálózat kábelei is mind DSL vonalként üzemelnek? A már előbb említett kombinált routerek a kulisszák mögött egy mini telefonközpontként üzemelnek, az egész telefonforgalmat pedig VoIP módon bonyolítják le, ebből a felhasználó pedig semmit nem vesz észre, legfeljebb azt, hogy kevésbé zajos a hang. A VoIP nem egy protokoll, mindössze a kétirányú, IP alapon történő hangátvitelnek a gyűjtőfogalma, amely alá rengeteg protokoll, és rengeteg ezen protokollokat használó szoftver és hardver tartozik (Wikipedia, 2023). Már a kezdetleges DSL is képes volt stabil VoIP telefonálásra, ekkortájt kezdett elterjedni a Skype, TeamSpeak és Windows (Live) Messenger, amelyek ingyenesen elérhetőek és itthon nagyon népszerűek voltak.

Ilyenkor még a VoIP szinte teljesen csak a számítógépes szoftverekre, és konkrét, többnyire vállalati célokra szánt IP telefonokra (és telefonrendszerekre) vonatkozott. Ezzel szorosan összefügg az, elsősorban vállalati célra való szabvány, a DECT, amely egy mobilhálózathoz hasonló, azonban annál jóval egyszerűbb és olcsóbb vezeték nélküli digitális telefonszabvány. Itthon ugyan főként cégek használták, de például a Deutsche Telekom már a fent említett lakossági célú Speedport eszközein is biztosította.



6. ábra: DECT-képes Speedport eszköz (Deutsche Telekom, 2014)

Azonban 2011-12 után már a meglévő 3G mobilhálózatot is egyre többen használták ilyen célokra; a már előbb említett szoftverek elérhetővé váltak telefonokra is, ezzel nyújtva egy meghatározó alternatívát a mobilhívásokkal szemben. Ekkortájt még meglehetősen drágának számított a mobilinternet, de 2013-14 után, körülbelül a 4G kereskedelmi bevezetésével egyidejűleg megfizethető árazást sikerült elérniük a szolgáltatóknak. Hamar elterjedt a legtöbb okostelefonon a Facebook Messenger, Viber, WhatsApp, FaceTime, az azóta is toronymagasan jó lefedettségű és sávszélességű 4G hálózatainknak köszönhetően gyakorlatilag bárkit bárhol el lehet érni ezeken a szolgáltatásokon keresztül is, teljesen ingyen.

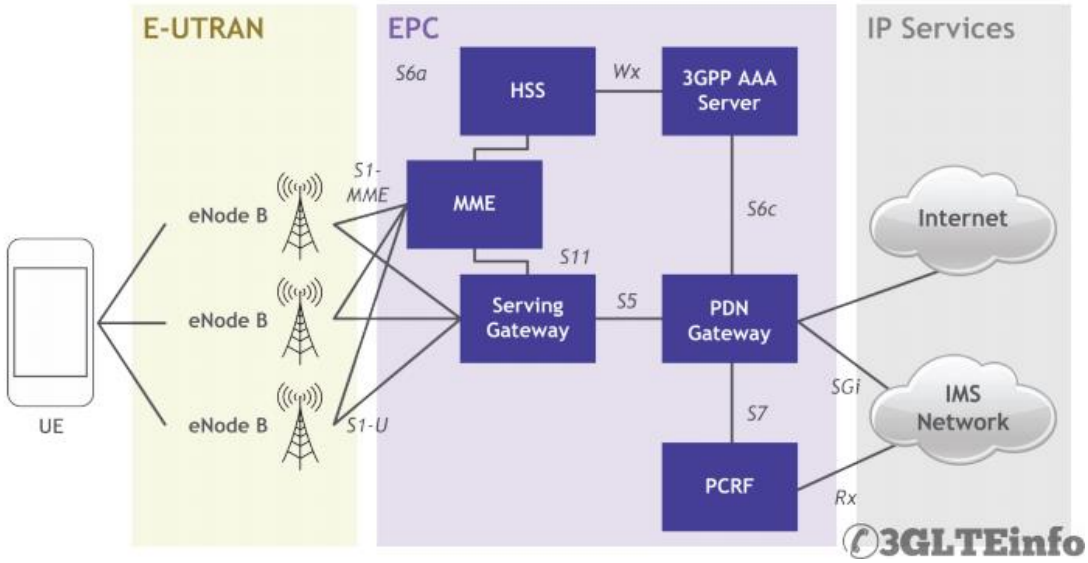
A 2010-es évek végén már tesztfázisba került a már eddig is jó teljesítményt nyújtó 4G után az 5G, ezzel párhuzamosan pedig a szolgáltatók rohamos tempóval építették ki az optikai hálózataikat is, mind lakossági, mind üzleti célú felhasználásra. Az 5G még Magyarországon a meglévő 4G hálózatok „kiegészítőjeként” működik (non-standalone), azonban idővel teljesen új alapokra kerül majd. Azóta bőven telítődött a piac internetszolgáltatók terén, valamint sávszélesség és mobilhálózati lefedettség ügyileg Magyarország világszinten is élen jár.

3.3. Internetelérés infrastruktúrájának biztonsága

Mivel az Internet az ország 99%-ában elérhető és megfizethető, ezért a kommunikációt érdemes és gazdaságos ott bonyolítani, legyen szó akár céges, akár magánjellegű kommunikációról. Mindenekelőtt, az információbiztonság 3 alapelven működik:

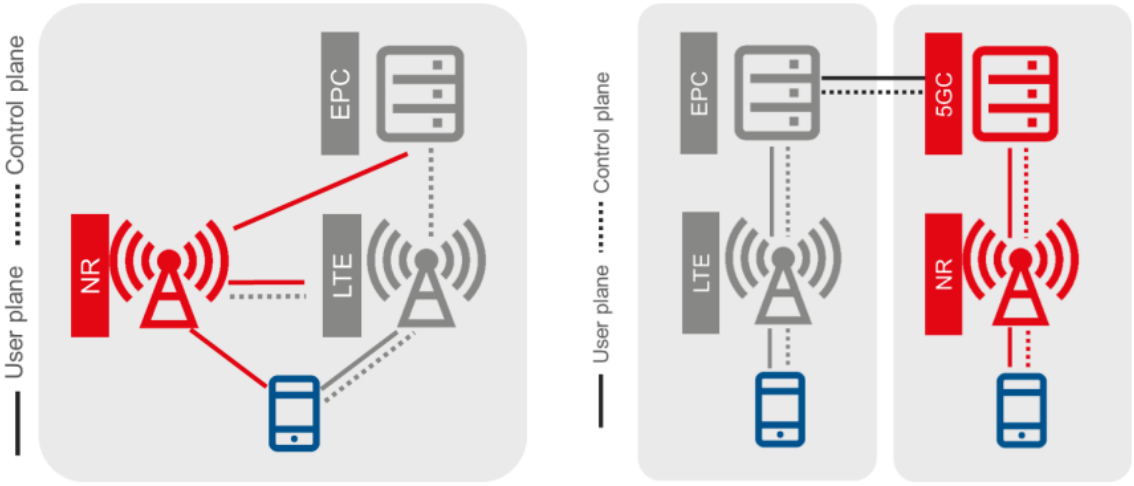
- **Confidentiality (bizalmasság):** Az információ csak az arra felhatalmazottak számára legyen elérhető
- **Integrity (sértetlenség):** Az információk és feldolgozási módszerek teljességének és pontosságának megőrzése
- **Availability (rendelkezésre állás):** Biztosítsuk, hogy a felhatalmazott felhasználók (ld. bizalmasság) mindig hozzáférjenek az információkhoz és kapcsolódó értékekhez, amikor szükséges (Dr. Varga, 2018).

A GSM-re már kitértem korábban, de az azon alapuló LTE rendszer még a korábbiaknál is biztonságosabb. Bevezetésre kerül az E-UTRAN, amely az LTE „rádiós" részét jelenti, és jelenleg világszerte 52 különböző frekvenciasávon működik, ezek „elosztásáról" elsősorban a helyi felügyeleti szervek (nálunk pl. az NMHH), és a szolgáltatók döntenek. A leggyakoribb ezek közül az 1800 MHz, utána követi őket az Európában általános 800 és 2600, de mostanában egyre gyakoribb a 700 MHz, valamint 2100 MHz is (Nagy, 2018), (Wikipedia, 2023).



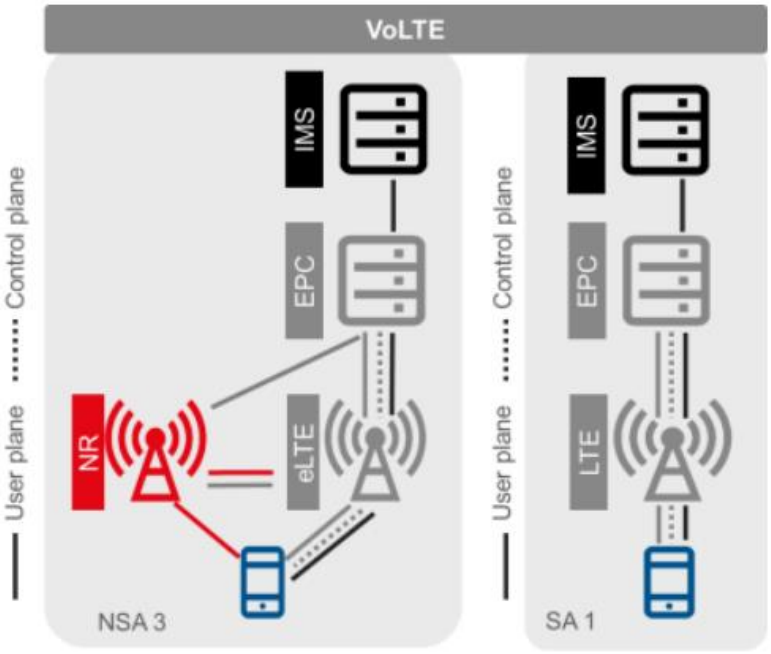
7. ábra: LTE topológia (3GLTEinfo, d.n.)

A telefon nem egy konkrét adótoronyhoz csatlakozik, hanem adótornyok hálózatához, ez maga az E-UTRAN. Ezen hálózat részei az eNode-ok, amelyek feladatai: moduláció, demoduláció. Demodulálja a bejövő rádiófrekvenciás jeleket, és IP csomagokat továbbít a gerinchálózat irányába, majd modulálja az onnan érkező IP csomagokat, és továbbítja őket a telefon irányába, tehát egy teljesen csomagkapcsolt hálózatról beszélünk. Minden, ezen túlmutató hálózati tevékenység „beljebb" zajlik az EPC, illetve IMS által (Tripathi, Kulkami, & Kuma, 2011). Az EPC-vel való összeköttetés ideális esetben (nagyobb városokban főleg) optikai kábelen, kevésbé ideális esetben (kisebb városok) rézkábelen, elszigeteltebb területeken (falvak, úthálózat mentén) rádiós kapcsolattal történik.



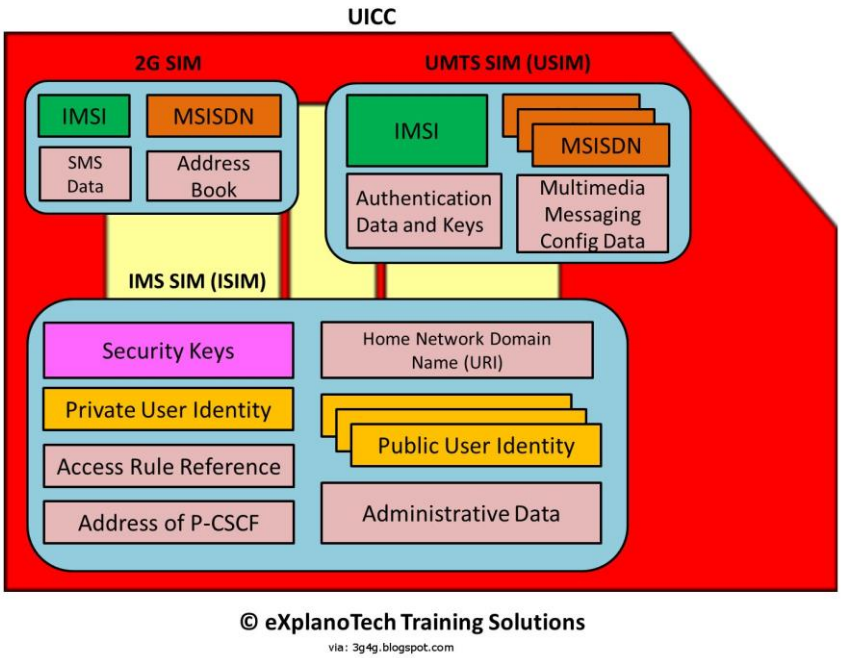
8. ábra: 5G NSA és és SA megvalósítás (GSM Association, 2019)

A Magyarországon jelenleg elérhető 5G rendszer – ahogy korábban is szót ejtettem róla – a 4G „kiegészítése", és 5G NR (New Radio) vagy NSA (non-standalone) néven fut. Itt mindössze az eNode-ok lettek megújítva/kicserélve, és mögöttük ugyanaz az EPC van, mint amit a 4G is használ. Az ilyen hálózatok kiépítése jóval olcsóbb, mint az 5GC-t (gyakorlatilag az 5G-s EPC) használó, különálló 5G SA (standalone) infrastruktúra telepítése. Jelenleg még ilyen rendszert nem támogat egyik hazai szolgáltató sem (GSM Association, 2019).



9. ábra: VoLTE megvalósítás 5G NSA és 4G esetén (GSM Association, 2019)

Idővel rájöttek, hogy ebben a rendszerben van még potenciál, ugyanis a sávszélesség bőven lehetővé teszi az eddigiektől sokkal jobb minőségű hangátvitelt sokkal kevesebb késleltetéssel, így kifejlesztették a VoLTE szabványt, amely a szervezeti inkonzisztenciája miatt nem kevés bosszúságot okozott mind a szolgáltatóknak, mind a gyártóknak. A VoLTE egyik „rokona” a VoWiFi, amely az előbb említett VoLTE minőségét képes biztosítani, csak mindezt WiFi-n keresztül, tehát gyenge vagy semmilyen térerő esetén is használhatóvá teszi a telefonokat. Mind a VoLTE-t, mind a VoWiFi-t a 7. és 9. ábrán is látható IMS (IP Multimedia Subsystem) kezeli, amely 5G NSA esetén gyakorlatilag pont ugyanúgy működik (Wikipédia, 2022), (Bartock, Cichonski, & Franklin, 2015).

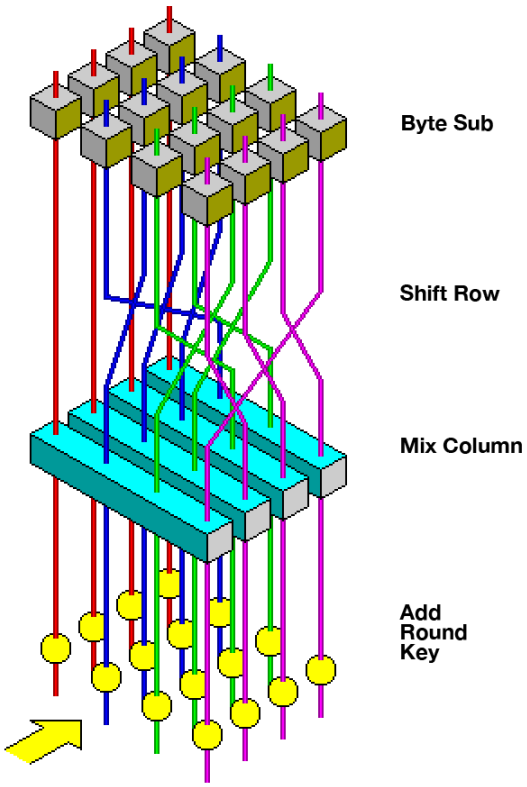


10. ábra: UICC kártya belső felépítése (eXplanoTech, 2012)

Az LTE az előbb megismert GSM hitelesítési módszereken felül alkalmaz még több egyéb technikát is. Legfontosabb ezek közül az UICC, ami egy újfajta SIM kártyának is tekinthető, és igazából észre sem vesszük, hogy mennyit tud. Ezek a kártyák teszik ki a ma használatos „SIM kártyák" többségét, gyakorlatilag az elmúlt 10 év kártyái ilyenek. Az UICC kártya tartalmaz különféle applikációkat, amelyek a különféle hálózatokhoz való hozzáférést biztosítják. A szolgáltató képes ezeket a kártyákat távolról „frissíteni", konfigurálni, manipulálni. Mivel egy kizárólag SIM kártyaként működő kártya fizikailag képtelen ezeket az alkalmazásokat futtatni (mivel primitív), így a 4G vagy akár 3G hálózathoz sem fog tudni hozzáférni, éppen ezért sarkall a szolgáltató mindenkit kártyacserére (Rossebø, 2008), (Ghadialy, 2020).

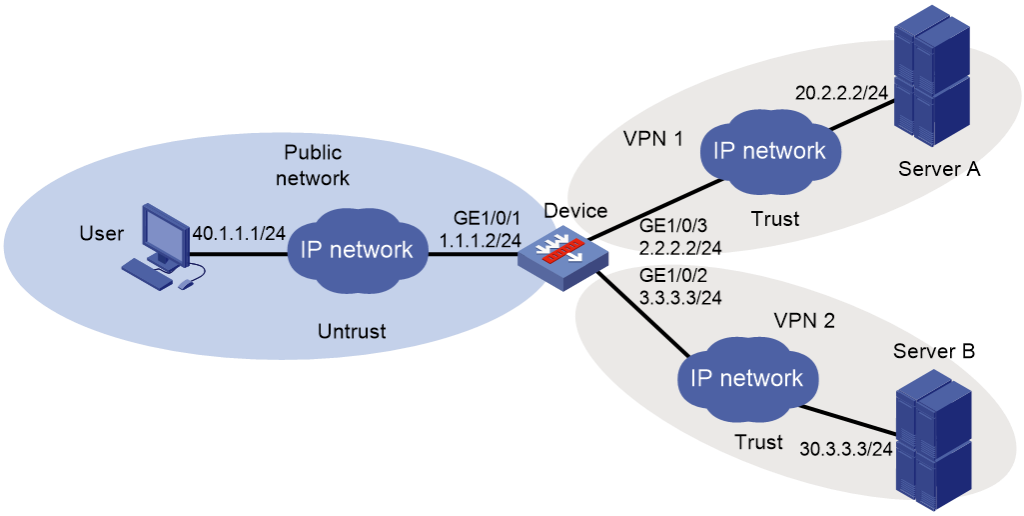
Az internetelérés leggyakoribb módszereként használatos WiFi a kezdetekben egy elég gyenge biztonsági rendszerrel (WEP) működött, azonban erre hamar rájöttek, és elindult a fejlesztés egy megbízhatóbb módszer érdekében. Eleinte a hálózati kártyák esetén elég volt egy szoftverfrissítés is, azonban az elérési pontok (AP) esetén a legtöbbször teljes eszközcsere kellett. A WPA a TKIP biztonsági protokollt alkalmazta, amely minden egyes továbbított csomagnál dinamikusan generál egy 128 bites kulcsot, ez a WEP esetén egyetlen kulcs volt az egész adatátvitelre. Ezt továbbfejlesztendő, megjelent 2004-ben a

WPA2, amely a TKIP mellett az AES titkosítási módszert is alkalmazta (Wikipedia, 2023).



11. ábra: AES logikája, (John Savard, 1999)

Az AES nemcsak a WiFi esetén használatos, ez egy általános algoritmus, amely tömbösítve és több körös adattranszformálással működik, és 128, 192, vagy 256 bites kulcsokat használ. 2018-ban megjelent a WPA3, amely ugyan még nem túl elterjedt, de az eddigieknél jóval biztonságosabb rendszer, amely az előre megadott kulcs módszerét (PSK) SAE-re cseréli, ahol minden egyes hitelesítésnél új hash generálódik. A WiFi eredetileg egy álteljes duplex technológia volt, mindössze időzítésekkel sikerült elérnie az egy időben történő adás és vétel illúzióját, azonban a WiFi 6 technológia óta már ez mindenféle trükk nélkül megoldódott.



12. ábra: egy tipikus céges VPN kapcsolat, (H3C Technologies Co, Ltd., 2020)

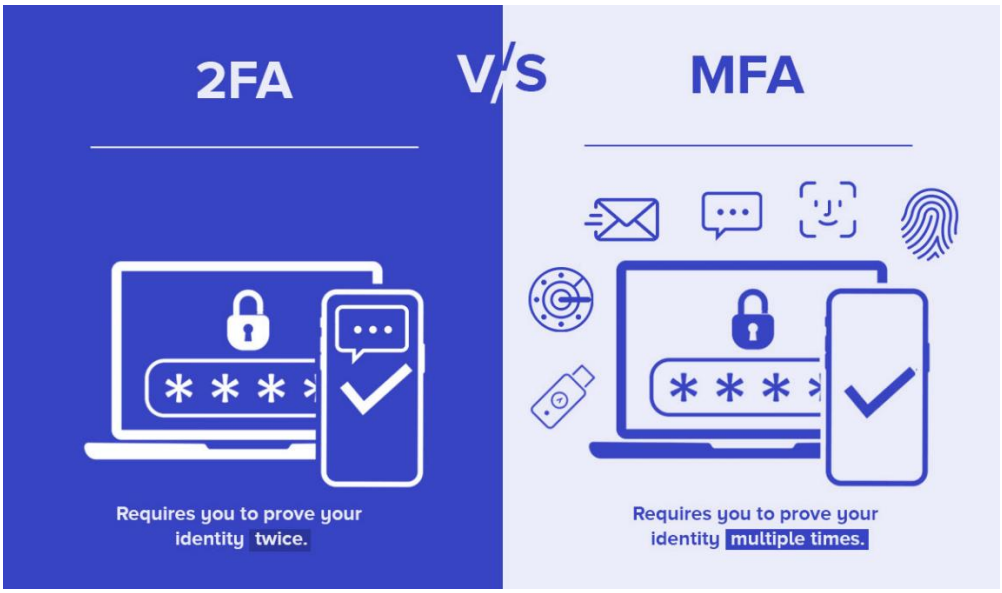
Manapság rengeteg munka végezhető távolról. Azonban meglévő internetelérés esetén is valahogy biztosítani kell a céges erőforrások elérését, ha esetleg távoli munkavégzésre kerül sor. Ilyen esetben VPN használata ajánlott, amely különböző titkosítási módszereket használva egy „alagutat” épít a felhasználó és a céges hálózat között. VPN elérésre rengeteg cég és rengeteg protokoll szakosodott, szintén rengeteg titkosítási módszerrel, ezen felül magát a hozzáférést is lehet (és érdemes) szabályozni egy két-, vagy többfaktoros hitelesítéssel, de azokról majd a továbbiakban több szó esik.

Ehhez kapcsolódhat még az SD-WAN (Software-defined Wide Area Network), amely az egymástól távol eső telephelyek között ad lehetőséget összeköttetésre. Ez egy szoftveres alapokon működő megoldás, mely átviteli technológiától (réz, optika, rádióhullám) független, és akár meglévő WAN infrastruktúrákra is telepíthető. Képes kritikus helyszíneket, alkalmazásokat, feladatokat priorizálni, ezáltal intelligens hálózati összeköttetést teremt, valamint szoftveres úton a terhelést is el tudja osztani az egyes vonalak között, ha azokból több van, és redundanciát is biztosít. A mai SD-WAN rendszerekre külön szolgáltatók specializálódtak (pl. Invitech), és egy ilyen rendszer kiépítése jelentősen csökkentheti a telephelyek közti kommunikációval kapcsolatos költségeket. SD-WAN és VPN kiépítése esetén gyakran Split Tunnel módszert alkalmaznak, azaz a nem belső céges kommunikációt (pl. YouTube, Google, teljes Microsoft felhő) nem vezeti át az SD-WAN-on (vagy VPN-en), ezzel levéve jelentős terhelést (Invitech ICT Services Kft., d.n.).

3.4. Kommunikációs módszerek biztonsága

Az eddigiekben kibeszéltük az infrastruktúrát, van egy működő és többnyire biztonságos rendszer, amit már csak tudni kell használni. Erre szerencsére létezik rengeteg technológia, amelyeket érdemes kiaknázni, legyen szó akár magáncélú, akár üzleti célú felhasználásról.

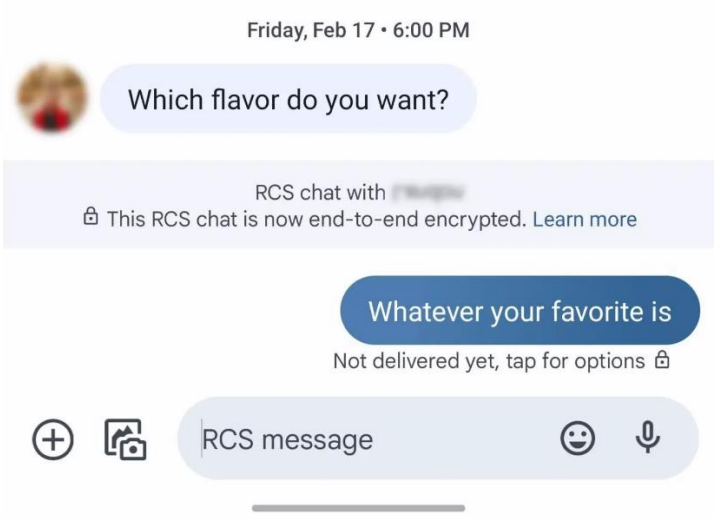
A legismertebb módszer a két-, vagy többfaktoros hitelesítés (2FA, MFA). Egy ilyen belépés során a megadott felhasználónév-jelszó páros megadása után egy második, vagy további hitelesítési módszeren való továbbjutás szükséges. Ez a második módszer lehet többféle, legismertebb közülük az SMS, e-mail vagy push értesítés, külön hitelesítő alkalmazás a telefonon (Microsoft, Google authenticator), vagy bármilyen hardveres kulcs, legyen az egy kártya, vagy pendrive.



Ezt a módszert ma már minden nagyobb, ismertebb „szolgáltató” cég (Facebook, Google, Microsoft, Amazon) alkalmazza, vállalati környezetekben pedig egyre több belső rendszer követeli meg. Működési elve, használata céges és magán környezetekben többnyire megegyezik, cégeknél viszont gyakoribb a kártyás hitelesítés. Ez egy meglepően hatékony és biztonságos dolog, ugyanis lehetőséget biztosít hitelesítési módszer „kiesése” esetén (pl. telefon nem hozzáférhető, nem működik) egy alternatívát biztosítani, másodlagos telefonszám, alkalmazás, vagy e-mail cím hozzáadásával. Itt persze biztonsági rést jelenthet (jelentett is; leginkább az USA-ban, rengeteg ember

nevével visszaélve végeztek szolgáltatóknál SIM cserét arra nem jogosult személyek, ezzel hatalmas anyagi és erkölcsi károkat okozva) a telefonszámhoz vagy e-mailhez való illetéktelen hozzáférés, azonban ez kétélű penge, ugyanis a saját magunk kizárását is könnyen el lehet így érni. Ebből kiindulva a szolgáltatók is elkezdték az ügyintézést komolyabban venni: csak a telefonszám jogos előfizetője intézhet ügyet, vagy vinnie kell közjegyzői meghatalmazást.

Telefonokkal kapcsolatban: az RCS (Rich Communication Services) hivatott lecserélni az SMS-t, egyelőre még csak Android rendszerű telefonokon. A korábbiakban már említettem az SMS hiányosságát, éppen ezért az RCS már teljesen interneten keresztül használható, megfejelve az egészet egy végpontok közötti titkosítással, erről majd később több szó is esik. Szöveges üzeneteken felül nagyméretű kép, videó, és egyéb fájlok átvitelére is képes, valamint kézbesítési állapotot is mutat.



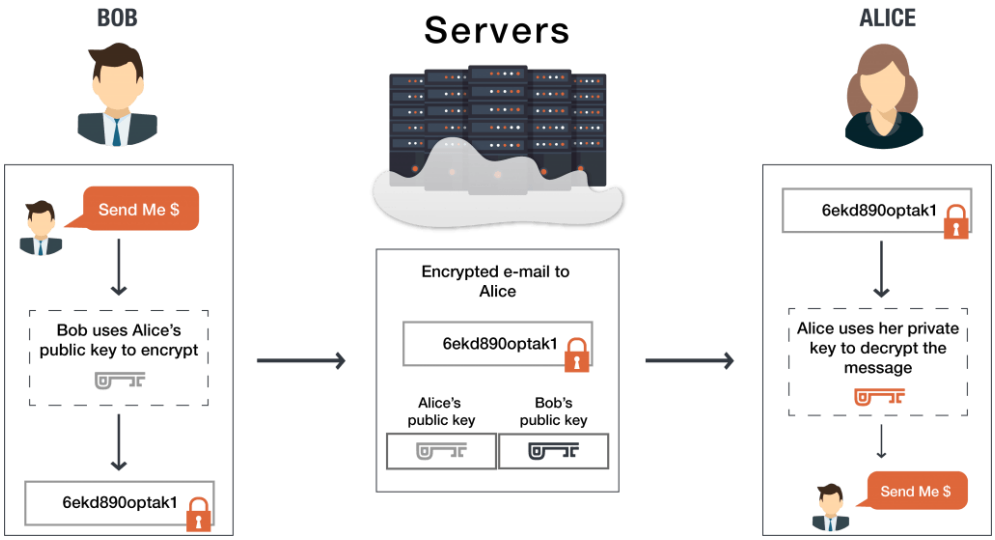
13. ábra: RCS üzenetkezelés Google Messages-ben, végpontok közötti titkosítással (Robby Payne, Chrome Unboxed, 2023)

Ma már szinte minden Androidos telefonon alapból működik, és 2023 novemberében az Apple bejelentette, hogy 2024-től ők is tervezik a szolgáltatást bevezetni eszközeiken, az iMessage-el párhuzamosan üzemelve. Az elsődleges üzenetküldés iOS-en viszont marad az iMessage, azt továbbra is csak iOS eszközök használhatják, mindössze kiegészítő szolgáltatásként implementálják az RCS-t (Miller, 2023).

14. ábra: iMessage és normál SMS üzenet a Messages alkalmazásban (Robert Triggs, AndroidAuthority, 2022)

Az iMessage technológia gyakorlatilag ugyanezeket a funkciókat biztosítja (a végpontok közötti titkosítást is ideértve), viszont kizárólag Apple eszközök között használható, és stabilitásban élen jár az RCS-hez képest (Apple, Inc., 2023).

Szintén népszerű és fontos módszer a végpontok közötti titkosítás. Ezt gyakorlatilag bármilyen kommunikációs formára rá lehet húzni, legyen az szöveges vagy audiovizuális. A már eleve biztonságosabbnak mondható csatornákon felül ez egy kiegészítő technológia, de sok platformon már alapbeállítás. Ilyen esetben aszimmetrikus titkosítás lép érvénybe, azaz különböző kulcsokat használ az adat titkosítására, és „kititkosítására", szemben a szimmetrikussal, ahol mindkét irányba ugyanazzal a kulccsal történik a titkosítás.



15. ábra: Végpontok közötti titkosítás (Orlee Berlove, PreVeil, Inc., 2023)

Mindkét fél kap a „szolgáltatótól” egy publikus-privát kulcs párost. Ezek közül a publikus kulcsok a „szolgáltató” szerverén tárolódnak, a privátok pedig a kommunikációhoz használt eszközökön, „végpontokon”. Ha A szeretne küldeni B-nek bármilyen titkosított üzenetet, akkor B-nek a publikus kulcsát használva elvégzi a titkosítást, majd elindul az így kapott adat átvitele. Ezután B a saját privát kulcsát használva fejti meg az üzenetet. Ha B szeretne A-nak küldeni, akkor ugyanezt kell visszafelé végig csinálni: B az A-nak címzett üzenetét az A-féle publikus kulccsal titkosítja (Berlove, 2023). Ilyen technológiát használ ma már a teljesen ingyenesen elérhető WhatsApp, Facebook Messenger, Viber, iMessage, FaceTime is.

Ehhez kapcsolódhat még a TLS (Transport Layer Security) titkosítás, ami hasonló elven működik, azonban csak végpont és szerver között, tehát a felhasználó adatai ugyan titkosítva haladnak a szerver és a felhasználó között, de magán a szerveren alap esetben titkosítatlanul tárolódnak, amely különösen problémás lehet egy adatszivárgás esetén. A TLS (vagy az ennek alapjául szolgáló SSL) ma már alapkövetelmény a böngészők részéről a weboldalak felé (HTTPS formájában), és ennek hiánya esetén jól látható figyelmeztetésekkel lehet szembesülni. Leggyakrabban tanúsítványok útján működik, amelyekben világosan fel van tüntetve a szerver neve/címe, kiállító hatóság, és a szerver publikus kulcsa. Ezek a tanúsítványok megadott időtartamra érvényesek, lejáratuk esetén még a HTTPS hiányánál is látványosabb figyelmeztetést kapunk. Ezért is fontos, hogy az adott eszközön mindig pontosan legyen beállítva a dátum és idő, ennek jelentős eltérése esetén hitelesítési hiba lép fel (Wikipedia, 2023).

A legjobb példa mindezekre a Microsoft, azon belül elsősorban a Teams, amit az egyetem is használ. Ez a platform része a Microsoft-féle felhőszolgáltatásoknak, mely magában foglalja az e-mailt, Office-t, valamint a külön szakterületként üzemelő Azure (már Entra ID)-t is. Teams-t használ a kommunikációra a cégek többsége, ugyanis Microsoft szolgáltatásokat használ a cégek többsége, és ebbe tökéletesen illeszkedik. Teams-ben lehetőség van közvetlenül felek közötti kommunikációra, csoportokra, valamint „team-ek” szervezésére is. Egyszerűen lehet benne közösen dolgozni Word, Excel, PowerPoint dokumentumokon, szavazásokat kitölteni, valamint online adásokat indítani és nézni is. Nem kötelező teljesen felhőbe migrálni az Exchange e-mail, valamint Active Directory rendszereket, de sok cég tesz így, biztonsági, valamint praktikussági okokból. Ugyan

végpontok közötti titkosítást közvetlenül nem, de TLS titkosítást használ mindenféle adatátvitelhez, legyen az Microsofton belüli, vagy Microsoft és felhasználó közötti. Ez magában foglalja a szöveges üzeneteket, átküldött fájlokat is, hívások esetén pedig az SRTP (Secure Real Time Transport Protocol) használatos. Az SRTP a már meglévő TLS kapcsolaton átvisz egy további hitelesítő kulcsot, amely ezzel egy végpontok közötti titkosítást ér el (Microsoft Corporation, 2023).

Traffic type	Encrypted by
Server-to-server	TLS (with MTLS or Service-to-Service OAuth)
Client-to-server, for example, instant messaging and presence	TLS
Media flows, for example, audio and video sharing of media	TLS
Audio and video sharing of media	SRTP/TLS
Signaling	TLS
Client-to-client enhanced encryption (for example, end-to-end encryption calls)	SRTP/DTLS

1. táblázat: A Microsoft Teams által használt titkosítási eljárások (Microsoft Corporation, 2023)

A Microsoft szerverein tárolt adatok helyben vannak titkosítva a saját fejlesztésű BitLocker segítségével (Microsoft Corporation, 2023). Ez a technológia céges eszközökön is gyakori, és a számítógépben lévő speciális titkosítási kulcsokat tároló chipet (TPM) használja (Microsoft Corporation, 2023). A Microsoft már annyira komolyan veszi a TPM chip meglétét, hogy a Windows 11 telepítését is megtagadja olyan gépeken, amelyek ezt nem tartalmazzák.

Szintén jelentős szolgáltatási területük az e-mail, amely esetén hasonlóan komolyan vették az adatvédelmet. Átvitel közben adott a TLS, de szintén használatos a saját Microsoft Purview titkosítási rendszerük is. Egy ilyen levélben megadhatóak különféle „szabályok”, pl. egy bizonyos címzett felé minden levél titkosítása, vagy a levelek bizonyos részeinek titkosítása, vagy másolás/nyomtatás tiltása. S/MIME (Secure/Multipurpose Internet Mail Extension) protokoll esetén titkosított levelen felül a digitális aláírás is megoldható. Ez szintén aszimmetrikus titkosítást használ, pont, mint a végpontok közötti módszer. Minden levél a küldése esetén a privát kulccsal íródik alá, a címzett pedig a küldő fél publikus kulcsával ellenőrzi, erre leginkább az adathalászat elkerülése miatt van szükség. Az aláírással a tartalom integritása is biztosított, valamint fő célja szavatolni azt, hogy valóban a küldő áll a levél mögött. Digitális aláírás meghamisíthatatlan, azonban nem feltétlenül jelenti azt, hogy az így aláírt levél titkosított is, viszont az S/MIME mindkettőre képes egyszerre (Microsoft Corporation, 2023).

Mindezeken túl, a kommunikációnak mobil oldalon is működőképesnek kell lennie. A Microsoft nem enged csak úgy bárkit hozzáférni az így üzemeltetett erőforrásokhoz telefonról, ehhez az adott telefont „regisztrálni” kell a céges nyilvántartásban, erre jött

létre a Company Portal. Ez egy menedzsment plaform a mobileszközök számára, ahol távolról lehet törölni, letiltani szükség esetén a telefont, és a legtöbb Microsoft-ot használó cég megköveteli ennek használatát. Előkövetelménye egy beállított PIN-kód, valamint eszköztitkosítás megléte. Céges szinten meg lehet szabni, hogy mely alkalmazások telepíthetők az App Store-ból vagy Google Playből, valamint a céges WiFi és VPN hálózathoz való hozzáférést is itt lehet biztosítani. Cégtől függ, hogy mit lehet ezen keresztül látni a telefonon lévő adatokból, de a többségük csak alap adatokkal tud foglalkozni. Ezen felül, a cég biztosíthat csak belső használatra való alkalmazásokat is, amelyeket alapból nem lehetne beszerezni a Company Portal nélkül (Microsoft Corporation, 2020).

Azonban nemcsak a Microsoft létezik. Céges környezetben szintén nagy sikerű a Google Workspace, ami funkcióiban hasonlít a Microsoft szolgáltatásaihoz. Biztosít egyedi e-mail címeket, levelezőlistákat, A Google-féle Gmail a „civil” szférában is a legismertebb, legegyszerűbb e-mail szolgáltató, és ebből kiindulva a céges használatuk is hasonlóan felhasználóbarát. A Google teljesen felhőalapú, helyben futtatható szoftverei nincsenek. A Teams-hoz hasonló üzenetküldő a Google Chat, ami a Google szerint biztonságos, titkosított adatátvitelt és adattárolást biztosít, de végpontok közötti titkosításról említést nem találtam. Ezen felül a Google Meet videó- és hanghívások lebonyolítására használható, amely a Teams-hez hasonló titkosítási eljárásokat alkalmaz. Egyszerű kezelhetősége miatt különösen népszerűek a Google termékek, leginkább azért, mert a céges használatú szoftverek magán változatai ugyanúgy működnek, szinte megegyező felhasználói felülettel és egyszerű kezelhetőséggel, platformtól függetlenül (Wikipedia, 2023).

Gyakran a Google levelezőrendszerével együtt használják a Slack szoftvert. Ez egy integrált kommunikációs rendszer, amely magában foglalja az üzenetküldést és hívásokat is. Lehetőség van a Teams-hez és Google Chat-hez hasonlóan csoportokat, valamint külön részlegeket összeszervezni. Használhatóságát tekintve felhasználóbarát, kicsivel összetettebb, mint a Google, de egyszerűbb, mint a Teams. Van lehetőség „rajztáblák” használatára, valamint akár munkafolyamatok automatizálásra is. A Slack szintén TLS titkosítást használ az adatátvitelnél, valamint FIPS 140-2-t az adattárolásnál. Az összes titkosítási kulcsuk egy szeparált hálózaton lévő szerverükön található, amelyhez ők

maguk is csak korlátozottan férnek hozzá. Elvárás náluk a kétfaktoros hitelesítés, akár az ügyfelekről van szó, akár a saját rendszereikről, valamint jelszókezelők és ezekhez tartozó jelszógenerátorok is használatosak. Szerződésbontás esetén a Slack azonnal törli az összes felhasználói adatot, a biztonsági mentéseiket pedig 14 napon belül megsemmisítik (Slack Technologies, LLC, 2020).

A hálózati infrastruktúráról ismert Cisco is fejleszt ilyen platformot, Webex néven. Lehetőség van videóhívásokra, szöveges üzenetekre, fájlküldésre, biztonságos távoli adattörlésre, kétfaktoros hitelesítésre és végpontok közötti titkosításra. Nem egy népszerű szoftver az előzőkhez képest, ennek ellenére több magyar cég és egyetem is ezt használja a meetingek és/vagy órák miatt (Cisco Systems, Inc., 2021).

Magyar alapítású, de már amerikai székhelyű cég a GoTo, amely nagyjából a Webex-szel van egy szinten népszerűség terén. A Connect nevű szolgáltatásuk egy telefonközpont jellegű rendszer, amelyben normál PSTN hívásokon felül internetes videóhívások lebonyolítására is van lehetőség, valamint ezek összekötésére, továbbítására és automatizálására is, intuitív grafikus felülettel. Gyakori felhasználási területe az ügyfélszolgálatok, és integrálható bele a Slack is. Ezen felül a GoTo Meeting egy meetingek szervezésére és tartására használatos szoftver, amely hamarosan végpontok közötti titkosítást is alkalmazni fog.

A covid járvány elején még csak a GoTo Meeting-hez hasonló szolgáltatást nyújtott, de ma már teljeskörű kommunikációs rendszert szolgáltat a Zoom, amely minden kommunikációt TLS-sel titkosít, lehetőség van végpontok közötti titkosításra is (GoTo Group, Inc., 2020).

Melyik az ideális rendszer? A legtöbb cég mindent Microsoft alapokra helyez, mert ahhoz a legkönnyebb szakértőt találni, és az az általános már 20+ éve. Jól strukturált, többnyire átlátható rendszer, amelyben mindent be lehet igény szerint konfigurálni, legyen szó Windows rendszer-beli engedélyekről, beállításokról, szabályokról, vagy éppen az ezzel szoros kapcsolatban lévő, már felhőbeli e-mail rendszerről. Microsoft-os cégtől Microsoft-os céghez történő váltás esetén gyakorlatilag ugyanazzal a környezettel találhatjuk szemben magunkat.

Startup cégek esetén gyakori a Google vagy Slack, ott ugyanis nem kell egy meglévő Active Directory-t és egyéb infrastruktúrát áthangolni egy alapjaiban teljesen más rendszerre. Valamivel egyszerűbb lehet, hogy nem kell fizikális szervereket helyben üzemeltetni ezekhez a tipikusan Microsoft specifikus szolgáltatásokhoz, hanem minden felhő alapú, főleg, ha a céges számítógépeket az Apple gyártja (itthon nem túl jellemző). Ennek ellenére több nagyobb régi cég is meglépte, hogy átállt alternatív rendszerekre, ezek fogadtatása több-kevesebb siker volt. Nincs tökéletes rendszer, a Microsoft is távol áll tőle. De egy ilyen döntés esetén figyelembe kell venni mind az anyagi oldalát a dolgoknak, mind a felhasználói visszajelzéseket.

4. PRIMER KUTATÁS BEMUTATÁSA

A következőkben bemutatok egy esettanulmányt, amely 3 cég belső (info)kommunikációs módszereit írja le, hasonlítja össze. Ezek valós cégek, és az évek során kapcsolatba kerültem, így volt alkalmam megismerni folyamataik működésének egy részét.

4.1. „A" cég

Az **A** cég egy egészségügyi segédeszközöket gyártó skandináv multinacionális cég, magyar telephellyel, dán székhellyel. Hatalmas alapterületű gyártócsarnokaik vannak, és mivel szendvicspanelből készültek fóliázott üveggel bevonva, így gyakorlatilag Faraday-kalitka módjára szigeteltek a bejövő rádióhullámokkal szemben. A cég bizonyos munkatársai rendelkeznek céges telefonnal, amely minden esetben csak valamely Apple iPhone modell, azonban ez helyi vezetői döntés volt. Ezen céges telefonok mind rendelkeznek a Microsoft Company Portallal, amelynek használatát céges szabályzat írja elő. Külön IT politikát hoztak létre, amely részletesen kidolgozott. A céges IT-val kapcsolatos problémák, kérdések kezelésére jegyrendszer üzemel, amelyet ugyanaz a szoftver kezel, mint ami a leltári rendszert is. Ebbe a jegyrendszerbe e-mail útján kerülhetnek kérések, de az ügyfélszolgálatnak egy külön belső telefonmellék is van fenntartva.

Az **A** cégnél, gyár lévén a mindennapi munkavégzés elengedhetetlen része a **gyors** kommunikáció. Termelési területeket kell bejárni, sokszor oda beöltözni, ott munkát végezni, karbantartani, itt pedig minden perc többmilliós kérdéssé válik, nem beszélve a munkavédelmi aggályokról. Ezért is van biztosítva 2 fajta telefonálási megoldás: értelemszerűen a céges telefonok, és a DECT rendszer.

A korábban már bemutatott DECT rendszer évek óta jól bevált a cégnél. Külső telefonos kommunikáció biztosított, azonban PBX rendszer telepítése szükséges ehhez, amely az **A** cégnél megoldott. AVAYA DECT R4 az itt lévő rendszer hivatalos neve, melynek központjához IP DECT Digital Gateway „elosztók", azokhoz pedig rengeteg IP Base station „adótornyok" csatlakoznak. Vezeték nélküli telefonokon felül használnak még szintén AVAYA márkájú, de helyhez kötött vezetékes IP telefonokat is. A cég lefoglalt

a publikusan elérhető vezetékes telefonszámok közül egy egész számtartományt, amelyek utolsó 4 számjegye a belső IP telefonrendszer belső mellékeinek van megfeleltetve. A használatos protokoll a H.323 a telefonok és a központ között.

A belső IP telefont leginkább csak a gyártásban résztvevők használják, az irodai alkalmazottak többnyire a céges mobiltelefonjaikon kommunikálnak. Ahogy az elején is szóba került, az épület sokat árnyékol, így a „kinti" mobilhálózat tornyai önmagukban nem biztosítanak elég lefedettséget. Ezért szükség volt a céggel szerződésben lévő mobilszolgáltatót megbízni azzal, hogy a belső lefedettséget antennák felszerelésével biztosítsa, így most annak a szolgáltatónak tökéletes a vétele, viszont a másik kettőnek szinte használhatatlan. Ezen felül, a WiFi elérés ugyan biztosított az épületnek szinte minden részén, de az a Cisco ISE hitelesítését használja, amely miatt csak névre szóló hozzáférési tokennel lehet elérni a WiFi hálózatot, és azt is csak iPhone-ról, vagy céges laptopról. Telefonok esetén ennek a hozzáférésnek alapfeltétele a Microsoft Company Portal, és Android esetén ez szándékosan nem is működik. A belső hálózati infrastruktúrát egy külsős társaság tartja karban szoftveresen, a gyárban lévő IT csapat csak a fizikális szerelésért felelős. Egyetlen szolgáltató bejövő optikai bérelt internetvonala lett kiépítve a céghez, a többi telephellyel és anyacéggel való kapcsolat SD-WAN technológiával történik..

A Company Portal biztosítja a hozzáférést az egyéb Microsoft szolgáltatásokhoz is, mint pl. e-mail, Teams, vagy Office alkalmazások. Ez a cég, IT terén a kezdettől fogva Microsoft alapokra épült, és ezen nem is terveznek változtatni, igyekeznek követni a Microsoftnál zajló fejlesztéseket. Kommunikáció terén az e-mail és a Teams egyaránt használatos, a kettő közötti döntés pedig inkább már üzleti kommunikáció témája. A Teams-en belül a szervezet központja az anyacég, és az egész céghálón belül bárki bárkivel kommunikálhat. A legtöbb Microsoft-szolgáltatás, - ideértve az e-mailt és Active Directory-t - már felhő szinten üzemel, így azokra az korábbiakban említett biztonsági előírások érvényesek. Az ezekbe történő bejelentkezéshez már az első belépéskor meg kell adni egy kétlépéses hitelesítési módot, amely lehet hitelesítő app, vagy SMS-hez telefonszám. S/MIME technológiával nem találkoztam, hardveres biztonsági „kulcsot" nem használnak, viszont jelszókezelő „titkos szervert" igen, az Active Directory jelszavaikat évente módosítaniuk kell.

A céges számítógépek amint kikerülnek a cég hálózatából, azonnal automatikusan elkezdenek csatlakozni VPN-re, amelyet szintén a Cisco rendszereivel biztosítanak. A Cisco AnyConnect kliens lehetőséget biztosít különféle hitelesítési eljárásokra, azonban itt nincs szükség semmiféle további azonosításra, jelszóra. Ezeken a gépeken kötelező a BitLocker használata. A telefonok is képesek VPN-re csatlakozni, ezzel elérést nyerve bizonyos hálózati meghajtókhoz.

Előnyök: Elég jól strukturált, átlátható rendszer, ahol mindenki talál „csatornát" a külvilág felé, és gyorsan el lehet érni egymást, valamint külsősöket is. A Teams tökéletesen integrálódik a meglévő Microsoft környezetbe, és aktívan használja is mindenki. Biztonságot tekintve többnyire rendben van, elég komolyan van véve az adatvédelem, a céges IT politika is naprakész. A VPN könnyen használható, stabil. A jegyrendszer fontos egy ekkora cégnél, ebből lehet statisztikákat is készíteni.

Hátrányok: Csak belsősök férhetnek hozzá a WiFi-hez, külsősök (pl. diákok, külsős partnerek) nem, még egy teljesen szeparált és korlátozott VLAN-hoz sem, ami esetleg csak internetelérést biztosítana. A hálózati infrastruktúrához a helyiek szoftveres szinten nem is nyúlhatnak, azt egy másik országban lévő csapat végzi, ezzel nem kevés bosszúságot okozva mindkét félnek. Erre jó példa, hogy a VoWiFi szolgáltatáshoz szükséges beállításokat csak ők tudnák elvégezni, és 2 éve nem jutott rá idejük. Belső jelerősítői csak a céggel szerződésben lévő szolgáltatónak vannak, a többi szinte sehol nem működik, ezzel nehézségeket okozva a külsős munkavállalóknak. A jegyrendszer szoftvere borzasztóan lassú.

A Company Portal nem ad WiFi hozzáférést Androidos telefonon, azonban ez kevésbé releváns amiért (helyi) szabályzat szerint is csak iPhone üzemelhet céges telefonként. A belső AVAYA telefonrendszer ugyan stabilan és egyszerűen működik, de a hangminősége és hangereje sokszor elég nehéz megértést eredményez, főleg egy zajos gyárterületen.

Javaslatok: A VPN biztonságosabb lenne, ha kaphatna egy másodlagos hitelesítést, mint plusz védelmet, ha esetleg valamilyen módon lezáratlanul maradna a gép egy olyan helyen, ahol illetéktelenek is hozzá tudnak férni. Naprakész Androidos telefonok, naprakész szoftverrel tökéletesen használhatóak és biztonságosak lennének céges

használatra. A meglévő jegyrendszert rövidesen jó lenne egy gyorsabbra, nyíltabbra cserélni, pl. Znuny vagy Jira.

4.2. „B” cég

Következő a **B** cég, amely egy magyar tulajdonú és vezetésű KKV, és élelmiszer nagykereskedésként működik. **B** cégnél minden kollégának van céges telefonja, egy 10 éves Nokia formájában. A legtöbben ebből kivették a céges SIM kártyát, és a saját telefonjukba rakták (volna, ha nem lenne az is 10 éves, újabb bürokráciát szülve az ügyfélszolgálaton) a saját kártyájuk mellé. Ezek az előfizetések szerencsére tartalmaznak adatforgalmat, de nagyon keveset, mindössze párszáz MB-ot, viszont cégen belül korlátlan hívást biztosítanak, melyet ki is használnak. Ezen felül kapnak még egy Androidos tabletet, ami szintén 10 év körüli.

Üzenetküldési lehetőségnek létrehoztak egy nagy közös csoportot a Viber üzenetküldőn, amelyet mindenki telepített a (leginkább saját) telefonjára. Ebben a csoportban belső céges számok, adatok, képek fordulnak meg, valamint többnyire a kollégákkal történő beszélgetés is Viber-en történik. A Viber-en és telefonáláson felül konkrét előre megadott vagy javasolt azonnali kommunikációs csatornák nincsenek, esetleg iPhone-ok között gyakori még az iMessage-en vagy FaceTime-on történő beszélgetés.

Napi megrendelési listákat e-mailben küldenek, amelyhez a **B** cég informatikusa minden dolgozónak regisztrált egy külön (civil, nem céges) Gmail profilt, felhőbeli vagy helyben üzemeltetett céges e-mail szolgáltatót nem vesznek igénybe erre a célra, esetleg néhány közös gyűjtő e-mail fordul elő. Ezek a megrendelési listák gyakorlatilag a cég alap működését jelentik, amelyeket teljesen szabadon és bátran küldenek egy bárki által ingyenesen igénybe vehető szolgáltató rendszerén keresztül. A Google privát célú szolgáltatásai is támogatnak kétfaktoros hitelesítést, de ezt az informatikus nem állította be, és nem is közölte senkivel, konkrétan a dolgozóra volt bízva ennek használata. Az így kapott Gmail felhasználóval mindenki a saját telefonjára van belépve.

Előnyök: Kis cég, minden dolgozót érintő információkra megfelelő lehet a Viber. Mindenkinek biztosítottak céges telefon(szolgáltatás)t, mindenki mindenkit el tud érni korlátlanul, bárhol, bármikor. A Gmailt mindenki ismeri és tudja kezelni.

Hátrányok: Régi, elavult tableteket használnak, amelyek szoftveres és hardveres támogatása is régen lejárt. Nincs IT biztonságpolitika, a tableteken nincs elvárt biztonsági beállítás (képernyőzár stb.), és személyes célú Gmail-en folyik a céges levelezés. A csoportos üzenetek Viber-en folynak, és ugyan a Viber támogat végpontok közötti titkosítást, de az csoportos-, és videóhívások esetén nem elérhető (Viber Media S.à r.l., 2023). A cég informatikai ügyeiért felelős egyetlen személyt nehezen lehet elérni.

Javaslatok: Céges előfizetés mellé indokolt lenne adni egy korszerű céges telefont, amely képes lenne futtatni a megrendeléskezelő rendszert. Ezen felül az egész céges kommunikációt „felvinni a felhőbe", pl. Google Workspace használatával. Képzett, tapasztalt rendszermérnökkel ellenőriztetni, átszervezni az egész infrastruktúrát, szoftverekre javaslatot és/vagy ajánlatot kérni.

4.3. „C" cég"

Végül a **C** cégről lesz szó. Jól ismert, nagy német multinacionális cég kisebb magyar leányvállalata. Egy hasonló tevékenységkörű cégekkel körülvett területen helyezkedik el, és kutatás-fejlesztéssel foglalkozik.

Alapvetően minden dolgozó kap egy céges laptopot, amely Windows-t futtat, és az egész cég Microsoft rendszerekkel üzemel, azonban vannak kísérletek Amazon AWS-sel is. Ennek megfelelően a fő kommunikációs rendszer az **A** céghez hasonlóan a Teams és az e-mail, melyeket teljesen felhőbeli módon a Microsoft szolgáltat. Ezeknél a belépéshez alapkövetelmény már az első munkanapon a kétfaktoros hitelesítés beállítása. Használnak jelszókezelőket, az ezekben lévő személyes jelszavak lejárnak, és van az IT csoportnak (meg még bizonyos egyéb dolgozóknak) egy külön AD profiljuk, amelynek a jelszavát egy helyben üzemeltetett jelszókezelő szerver generálja és tárolja. Ez a jelszó 24 karakter hosszú, mindenféle szimbólumot tartalmaz, és minden 12 órában új generálódik belőle, tehát a konkrét dolgozó sem tudja a saját jelszavát. Erre a jelszókezelőre belépni csak Microsoft-féle kétfaktoros azonosítással, vagy a cég saját kétfaktoros azonosításával (mobil app, vagy fizikális kártya) lehet belépni. Ezen felül használnak még offline jelszókezelő adatbázis szoftvert is, melyre a nem változó jelszavakat veszik fel többnyire.

Majdnem minden területhez érkezhetnek kérések (tehát nemcsak az IT-hoz) egy jegykezelő rendszeren keresztül, melyet az IT üzemeltet. Ez a rendszer vagy e-mailben, vagy a saját weboldalán keresztül fogad kéréseket. Az IT-tól külön csapatként üzemelő, azonban velük szorosan együttműködő társaság a Cybersecurity team, akik konkrétan csak az információbiztonsággal foglalkoznak. Kiterjedt IT politikával rendelkezik a **C** cég, amelyet az IT és a Cybersecurity közösen dolgozott ki, az anyacég előírásait figyelembe véve. A céges számítógépekre csak bizonyos, a cég által engedélyezett szoftvereket lehet telepíteni, melyet egy script időszakosan ellenőriz, ezen felül az összes gépen az **A** céghez hasonlóan itt is kötelező egy BitLocker jelszót beállítani. A Zero Trust elvet folyamatosan implementálja a cég.

A másik 2 céggel szemben hatalmas előrelépés, hogy aktívan használják az S/MIME technológiát, annak mindkét részét. Az így küldött leveleknél szavatolja a Microsoft, hogy valóban a küldő küldte azt, és kizárólag a címzett(ek) nyithatja meg, ehhez pedig megköveteli a hardveres kulccsal történő azonosítást, amit jelen esetben a céges kártya jelent. A céges kártya szintén használatos a papíros aláírások elkerülésénél, ugyanis szinte mindent digitálisan írnak alá a kártya használatával, nyomtatásra nagyon ritkán kerül sor.

Belső telefonrendszer nincs, mivel nincs értelme. Az **A** céggel ellentétben nincsenek nehezen megközelíthető területek, körülményes helyek, így szinte mindenki elér mindenkit Teams-en, vagy ha ott nem is, akkor személyesen. Redundáns, két szolgáltatótól is származó optikai bérelt vonal felel az internetkapcsolatért, valamint egy harmadik biztosítja kizárólag a céges erőforrások elérését SD-WAN technológiával. A WiFi rendszer lehetővé teszi „külsős” telefonok csatlakozását is, mely különösen előnyös a külsős dolgozók, főleg diákok részére. A próbaidő letelte után a dolgozók kapnak céges telefont is, amelyre az A céghez hasonló módon szabályzat köti a Company Portal telepítését és használatát. Itt azonban nincs megkötve a telefon típusa; a beszerzés (amelyet szintén a jegyrendszeren keresztül lehet elérni) olyan telefont szerez be a dolgozónak, amilyet szeretne, természetesen ésszerű keretek között. Android és iOS rendszereken egyaránt működik mind a WiFi elérés, mind a Microsoft szolgáltatásai. A cég a piros színű mobilszolgáltatóval van szerződésben, így annak használata az épületen belül tökéletesen biztosított, ezen felül a magenta színű szolgáltatóé is, viszont a zöld színűvel nem sikerült dűlőre jutniuk, így az csak korlátozottan működik. Ezt kompenzálja

a WiFi, amelyen a VoWiFi szolgáltatás is tökéletesen működik. A céges telefonokkal telefonálni jóval ritkábban szoktak, mint az **A** cégnél, ugyanis kevésbé kell hirtelen reagálni történésekre, a kommunikáció többségét Teams-en intézik el.

VPN terén ugyanazt a rendszert használják, mint az **A** cég, viszont csatlakozásnál szükség van egy második hitelesítésre, amit jelen esetben a Microsoft biztosít. Hálózati biztonságot tekintve sokkal előrébb járnak, a hálózati végpontokon keresztül is csak hitelesítés (Cisco ISE, pont, mint az **A**-nál) után lehet hozzáférést szerezni, és itt a hozzáférés mértéke szerepkörtől függ (RBAC, Role Based Access Control), viszont nemcsak WiFi-n, hanem kábelen is. Az IT-val kapcsolatos helyiségekbe csak az IT tagjai léphetnek be, az infrastruktúrát biztosító szerverszoba pedig ezen felül még külön egyedi PIN kódot is igényel. VPN-ről történő munkavégzés esetén „jump server" -ek használata kell a teljes infrastruktúra eléréséhez, ugyanis VPN-en ez csak korlátozottan működik.

Előnyök: teljeskörű adatvédelem, de mégis rugalmas. Az egész hatalmas cégcsoporton belül elér bárki bárkit, mint az A cégnél. Mindig mindenre van valamilyen megoldás, ha kérdés merül fel, mindig van, aki segítsen.

Hátrányok: néhány helyen talán túlságosan komolyan veszik az adatvédelmet (de bizonyos szinten megengedőbben, mint az **A** cégnél), körülményes a céges szervereket elérni a jump servereken keresztül. Eleinte mindenhez kellett a céges kártya a belépésnél, ma már egyre kevésbé. Nagy cég lévén a bürokrácia elkerülhetetlen, a német anyacéggel pedig néha nehézségeket okoznak a kulturális különbségek.

Konklúzió, javaslat: a C cégnél nekem nincs személyes javaslatom, jól kigondolt, jól szervezett rendszer tartozik az információbiztonsághoz. Microsoftot használó nagyvállalat, ilyen téren elég hasonló az **A** céghez.

5. A JÖVŐ BIZTONSÁGOS KOMMUNIKÁCIÓS MEGOLDÁSAI

Már most elég fejlett technológiákat használnak a világban, mind magánszemélyek, mind cégek, ahogyan az előbbi esettanulmányban is elhangzottak, azonban mindig van hová fejlődni. Ma is népszerű téma az informatikában (és minden egyéb területen, amit az IT támogat) a mesterséges intelligencia (AI) és gépi tanulás (ML). Az ilyen algoritmusok képesek nagy mennyiségű adatot átfésülni, és felismerni a bennük rejlő kártékony szabályszerűségeket.

A blokklánc (blockchain) egy decentralizált főkönyv, amelyen keresztül biztonságosan lehet adatot továbbítani, emiatt nehezebben sebezhető. Különösen népszerű a pénzügyi szektorban, egészségügyben, és kormányzatokban.

Szintén nagyon népszerű jelenség az IoT (Internet of Things), amely gyakorlatilag mindenféle elektronikus berendezésnek az online térbe való „bekötését” jelenti. Mind civil használatban, mind ipari automatizálásnál megvan a jelentősége, ugyanis jelentősen meg tudja könnyíteni a mindennapi folyamatainkat, és sokszor kritikus jelentőségű rendszereket, infrastruktúrákat vezérelnek vele. Azonban ezen eszközök jelentős része semmilyen vagy nagyon gyenge biztonsági megoldásokat alkalmaz, emiatt a szervezeteknek külön lépéseket kell tenniük az IoT-t érintő kibertámadások ellen. Ilyenek lehetnek például a rendszeres szoftverfrissítések, kétfaktoros azonosítás vagy hálózati szeparáció.

A szervezetek régebben nem szívesen osztottak meg dolgokat információbiztonságot érintő problémáikról, attól félve, hogy ezzel még jobban veszélybe sodorják magukat. Azonban a mai világban rájöttek a cégek, hogy önmagukban nem mindig képesek kezelni ezeket a helyzeteket, ezért szövetkezni kezdtek, és az ilyen jellegű problémákat közösen megvitatni. Ide tartoznak a bevált módszerek, erőforrások, intelligencia, valamint közös információbiztonsági kutatások, műveletek.

Az egyik legfontosabb módszer a Zero trust (Banafa, 2023). Ez egy biztonsági modell, melyet a NIST tervezett, és 7 alapszabályt mond ki:

1. Minden adatforrás és számítási szolgáltatás erőforrásnak minősül. Ide tartozik a céges laptop, telefon, valamint saját eszközök is, ha a szervezet támogatja a BYOD (saját eszköz használata) elvét
2. A hálózat helyétől függetlenül minden kommunikációnak biztonságosnak kell lennie.
3. A szervezeti erőforrásokhoz való hozzáférést munkamenetenként biztosítják.
4. Az erőforrásokhoz való hozzáférést egy házirend határozza meg, ide tartoznak a tagok, erőforrások, az ezek közti hozzáférési viszonyok, valamint az ezekhez rendelt attribútumok.
5. A szervezet folyamatosan figyeli és biztosítja az integritását és biztonságát minden tulajdonban lévő rendszernek.
6. Minden erőforrás hitelesítés és engedélyezés dinamikus, és megkövetelt a hozzáférés biztosítását megelőzően.
7. A szervezet a lehető legtöbb információt gyűjti az eszközök jelenlegi állapotáról, hálózati infrastruktúráról és kommunikációról, és ezeket felhasználja a biztonsági helyzet javítására (Rose, Borchert, Connelly, & Mitchell, 2020).

Azonban a legújabb, még főleg kísérleti fázisban lévő megoldás a kvantumszámítógépek. Jelenleg a legtöbb titkosítási algoritmus azon alapszik, hogy bizonyos matematikai műveletek nehézséget okoznak a „klasszikus” számítógépeknek, viszont a kvantumszámítógépek ezeket pillanatok alatt képesek megoldani, elavulttá téve a jelenleg titkosítási módszereket. Ez egyrészről azt jelenti, hogy kvantumszámítógépekkel törhetővé válnak a jelenlegi titkosítási módszerek, ezzel egy hatalmas veszélyt okozva az információbiztonságnak. Ugyanakkor úgy is vehetjük, hogy ezáltal újabb, és biztonságosabb módszerek fejlesztése válik lehetővé, amelyekkel eddig elképzelhetetlen szintű biztonságot oldhatunk meg.

Egy lehetséges felhasználási terület lehet az olyan kvantumalgoritmusok fejlesztése, amelyek képesek felismerni a kibertámadásokat, és reagálni is azokra. Ezen algoritmusokkal hatalmas mennyiségű adatot lehet elemezni, és veszélyesnek tűnő jeleket elkapni, ezzel lehetővé téve a szervezetek számára a támadások gyors felismerését és kezelését. Ezzel egy időben, ezek az algoritmusok szintén képesek lehetnek a múltbéli adatok és trendek elemzésével jövőbeli támadások megjóslására, elkerülésére.

6. ÖSSZEFOGLALÁS

A dolgozatban kutatást végeztem az üzleti világban előforduló kommunikáció minden formájáról, kezdve egészen a magával a kommunikációval. Ez egy örök téma marad, amely mindig meghatározó részét képezi az emberi, de jelen esetben egy adott vállalat kultúrájának, és folyamataikat tekintve rengeteg tényező függ tőle.

Megismerhettük, hogy a közvetlen ember és ember közötti kommunikáció is bonyolult jelenség, sok dolog befolyásolhatja és befolyásolja, valamint sok módon történhet sok irányban. Ezen felül egy rövid történelmi áttekintésként szó esett a kezdeti kommunikációs technológiákról, kódokról, fejlesztésekről, egészen az internetig. Az Internet az emberiség egyik legnagyobb találmánya, amely gyökeresen felforgatta az egész világot, kialakítva több, - egyébként nagyon sikeres és jövedelmező - szakmai területet, üzletágat, ezekre pedig még 30 évvel ezelőtt tervként, jövőképként sem gondoltunk. Meglévő üzletágakat is jelentősen befolyásolt, a korral pedig mindenkinek tartania kell a lépést a boldogulás érdekében.

Azonban az információhoz való könnyű és gyors hozzáférés veszélyeket is hordoz magával, ezek pedig mind magánszemélynek, mind cégnek katasztrofális anyagi és/vagy erkölcsi következményekkel járhatnak, így elengedhetetlen meghatározni biztonsági direktívákat, valamint biztonságot jelentő módszerek és technológiák fejlesztését. Ezen felül, az így kapott direktívák betartását is sarkallni, valamint ellenőrizni, ugyanis a biztonságot nem szabad félvállról venni. Emiatt is igyekeznek a kommunikációt szolgáltató cégek saját maguk „házon belül” elintézni az ilyen módszerek alapból történő biztosítását, ezzel jelentős terhet levéve az ügyfélnek minősülő cégek válláról.

7. IRODALOMJEGYZÉK

Apple, Inc. (2023). *Privacy - Features*. Retrieved from Apple: https://www.apple.com/privacy/features/

Banafa, A. (2023, április 3). *The Future of Cybersecurity: Predictions and Trends*. Retrieved from OpenMind: https://www.bbvaopenmind.com/en/technology/digital-world/future-of-cybersecurity-predictions-trends/

Bányász, I. (2010). *A kommunikáció csatornái és jellemzői, a kommunikációs készségek fejlesztése.* Budapest: Nemzeti Szakképzési és Felnőttképzési Intézet. Forrás: https://www.nive.hu/Downloads/Szakkepzesi_dokumentumok/Bemeneti_kompetenciak_meresi_ertekelesi_eszkozrendszerenek_kialakitasa/2_1851_004_101030.pdf

Bartock, M., Cichonski, J., & Franklin, J. (2015). *LTE Security - How good is it?* Gaithersburg, Maryland, US: National Institute of Standards and Technology. Retrieved from https://csrc.nist.gov/CSRC/media/Presentations/LTE-Security-How-Good-is-it/images-media/day2_research_200-250.pdf

Berlove, O. (2023, március 31). *What is end-to-end encryption and how does it work?* Retrieved from PreVeil: https://www.preveil.com/blog/end-to-end-encryption/

Centroszet Szakképzés-szervezési Nkft. (d.n.). *1.2.2. A kommunikáció típusai.* Forrás: Centroszet: https://centroszet.hu/tananyag/kom_alapjai/122_a_kommunikci_tpusai.html

Cisco Systems, Inc. (2021, augusztus 26). *Security Advantage for Webex White Pape.* Retrieved from Cisco: https://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/webex-room-series/white-paper-c11-743769.html

Cooper, T. (2023, október 11). *BroadbandNow.* Retrieved from DSL Internet in the USA: https://broadbandnow.com/DSL

Dr. Varga, P. (2018). *Az Informatikai Biztonság Alapjai*. Budapest: BME Távközlési és Médiainformatikai Tanszék. Forrás: https://www.tmit.bme.hu/sites/default/files/RelNetik_20180918_InfSecurity.pdf

Forgó, S. (2010). *Kommunikációelmélet, üzleti kommunikáció.* Eger: Líceum Kiadó. Forrás: https://publikacio.uni-eszterhazy.hu/5390/1/Kommunik%C3%A1ci%C3%B3elm%C3%A9let%20_%20%C3%BCzleti%20kommunik%C3%A1ci%C3%B3_2010%20online.pdf

Földvári, M. (2017. december 3). *Jel, információ, kommunikáció.* Forrás: Szín + kommunikáció: https://www.szinkommunikacio.hu/21_02.htm

Ghadialy, Z. (2020). *Beginners: UICC & SIM*. 3G4G. Retrieved from https://www.3g4g.co.uk/Training/beginners0041.pdf

Ghodbane, H. (d.n.). *A brief introduction to GSM.* Retrieved from Telecom crash courses: https://telecomcrashcourse.wordpress.com/a-brief-introduction-to-gsm/

GoTo Group, Inc. (2020, április 17). *Web conference security*. Retrieved from GoTo: https://logmeincdn.azureedge.net/gotomeetingmedia/-/media/pdfs/UCC_security_white_paper_snapshot_April2020.pdf

GSM Association. (2019, július 22). *5G Implementation Guidelines.* Retrieved from GSM Association: https://www.gsma.com/futurenetworks/wp-content/uploads/2019/03/5G-Implementation-Guideline-v2.0-July-2019.pdf

Horányi, Ö., & Szépe, G. (1975). *A jel tudománya, szemiotika.* Budapest: General Press Kiadó. Forrás: Communicatio: https://www.communicatio.hu/horanyi/DF-S-0910osz/A%20jel%20tudomanya.pdf

HungaroControl. (2021. március 15). *Fónia – a repülés és a biztonság anyanyelve.* Forrás: HungaroControl: https://blog.hungarocontrol.hu/cikk/fonia-a-repules-es-a-biztonsag-anyanyelve/

Invitech ICT Services Kft. (d.n.). *A régi hálózatokat is okosabbá teszi az SD-WAN*. Forrás: Invitech: https://www.invitech.hu/techpercek/a-regi-halozatokat-is-okosabba-teszi-az-sd-wan

Kelenyi, G. (2006). *Szemiotika*. Forrás: ELTE Művészettörténeti Intézet: https://arthist.elte.hu/BA_courses/Archiv/2006osz/Kelenyi_Gyorgy/Szemiotika.htm

Kövendi, D. (2017. december 18). *Mi is az a VHF rádió.* Forrás: Marina Yacht Sport: https://www.marina.hu/custom/marina/image/data/Szakmai%20cikkek/Mi%20is%20az%20a%20VHF%20r%C3%A1di%C3%B3.pdf

Központi Statisztikai Hivatal. (2022). *12.1.1.14. A háztartások internetkapcsolat típusainak aránya [%]*.* Forrás: Központi Statisztikai Hivatal: https://www.ksh.hu/stadat_files/ikt/hu/ikt0016.html

Magyar Tudományos Akadémia - National Geographic. (2016. április 26). *Az elektromágneses távíró feltalálója.* Forrás: National Geographic: https://ng.24.hu/tudomany/2016/04/26/az-elso-telegraf-kuldoje/

Microsoft Corporation. (2020, január 10). *What happens if you install the Company Portal app and enroll your Windows device in Intune?* Retrieved from IntuneDocs - GitHub: https://github.com/MicrosoftDocs/IntuneDocs/blob/main/intune-user-help/what-happens-if-you-install-the-company-portal-app-and-enroll-your-device-in-intune-windows.md

Microsoft Corporation. (2023, július 11). *BitLocker overview.* Retrieved from Microsoft Learn: https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/

Microsoft Corporation. (2023, november 9). *Encryption in Microsoft 365.* Retrieved from Microsoft Learn: https://learn.microsoft.com/en-us/purview/encryption

Microsoft Corporation. (2023, február 22). *S/MIME for message signing and encryption in Exchange Online.* Retrieved from Microsoft Learn:

https://learn.microsoft.com/en-us/exchange/security-and-compliance/smime-exo/smime-exo

Microsoft Corporation. (2023, október 30). *Security and Microsoft Teams.* Retrieved from Microsoft Learn: https://learn.microsoft.com/en-us/microsoftteams/teams-security-guide

Miller, C. (2023, november 16). *Apple announces that RCS support is coming to iPhone next year*. Retrieved from 9to5Mac: https://9to5mac.com/2023/11/16/apple-rcs-coming-to-iphone/

Nagy, P. (2018. február 17). *E-UTRA működési sávok.* Forrás: HTE site: https://www.fogalomtar.hte.hu/wiki/-/wiki/HTE+Infokommunikacios+Fogalomtar/E-UTRA+m%C5%B1k%C3%B6d%C3%A9si+s%C3%A1vok

Rose, S., Borchert, O., Connelly, S., & Mitchell, S. (2020. augusztus 10). *Zero Trust Architecture.* Gaithersburg, Maryland, US: National Institute of Standards and Technology. Forrás: NIST Technical Series Publications: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Rossebø, J. (2008). *New Trends for SIM cards.* Oslo, NO: Universitetet i Oslo. Retrieved from https://wiki.uio.no/mn/ifi/AFSecurity/images/0/09/AFSec200804-Rossebo-Telenor.pdf

Seres, A. (2010). *Kommunikációs alapismeretek II.* Budapest: Nemzeti Szakképzési és Felnőttképzési Intézet. Forrás: https://www.nive.hu/Downloads/Szakkepzesi_dokumentumok/Bemeneti_kompetenciak_meresi_ertekelesi_eszkozrendszerenek_kialakitasa/1_2321_004_101231.pdf

Slack Technologies, LLC. (2020. december 16). *Security at Slack.* Forrás: Slack: https://a.slack-edge.com/964df/marketing/downloads/security/Security_White_Paper_2020.pdf

Tripathi, S., Kulkami, V., & Kuma, A. (2011). *LTE E-UTRAN and its Access Side Protocols.* Hillsboro, OR, USA: Radisys Corporation. Retrieved from https://go.radisys.com/rs/radisys/images/paper-lte-eutran.pdf

Tutorialspoint. (d.n.). *GSM - Security and Encryption.* Retrieved from Tutorialspoint: https://www.tutorialspoint.com/gsm/gsm_security.htm

Viber Media S.à r.l. (2023). *End-to-end encryption in chats.* Retrieved from Viber: https://help.viber.com/hc/en-us/articles/8909167863453-End-to-end-encryption-in-chats

Wikipédia. (2020. augusztus 7). *CB-rádió.* Forrás: Wikipédia: https://hu.wikipedia.org/wiki/CB-r%C3%A1di%C3%B3

Wikipédia. (2022. december 17). *LTE.* Forrás: Wikipédia: https://hu.wikipedia.org/wiki/LTE

Wikipedia. (2023, november 3). *Electrical telegraph.* Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Electrical_telegraph

Wikipedia. (2023, november 4). *Fax.* Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Fax

Wikipedia. (2023, november 15). *Google Workspace.* Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Google_Workspace

Wikipédia. (2023. július 9). *Gramofon.* Forrás: Wikipédia: https://hu.wikipedia.org/wiki/Gramofon

Wikipédia. (2023. február 15). *GSM.* Forrás: Wikipédia: https://hu.wikipedia.org/wiki/GSM

Wikipédia. (2023. november 5). *Internet.* Forrás: Wikipédia: https://hu.wikipedia.org/wiki/Internet

Wikipedia. (2023, október 2). *LTE frequency bands.* Retrieved from Wikipedia: https://en.wikipedia.org/wiki/LTE_frequency_bands

Wikipédia. (2023. október 31). *Morzekód.* Forrás: Wikipédia: https://hu.wikipedia.org/wiki/Morzek%C3%B3d

Wikipédia. (2023. október 11). *Rádióamatőr.* Forrás: Wikipédia: https://hu.wikipedia.org/wiki/R%C3%A1di%C3%B3amat%C5%91r

Wikipédia. (2023. november 11). *Rádió-vevőkészülék.* Forrás: Wikipédia: https://hu.wikipedia.org/wiki/R%C3%A1di%C3%B3-vev%C5%91k%C3%A9sz%C3%BCl%C3%A9k

Wikipédia. (2023. február 10). *Telefonkészülék.* Forrás: Wikipédia: https://hu.wikipedia.org/wiki/Telefonk%C3%A9sz%C3%BCl%C3%A9k

Wikipédia. (2023. április 26). *Telefonközpont.* Forrás: Wikipédia: https://hu.wikipedia.org/wiki/Telefonk%C3%B6zpont

Wikipedia. (2023, november 8). *Transport Layer Security.* Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Transport_Layer_Security

Wikipedia. (2023, november 16). *Voice over IP.* Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Voice_over_IP

Wikipedia. (2023, november 14). *Wi-Fi Protected Access.* Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

TARTALMI KIVONAT

A dolgozat egy történelmi áttekintés, valamint leírás a használt információátviteli módszerekről, a kezdetleges technológiáktól egészen a ma használtakig.

SUMMARY

In this thesis I've researched different methods of communication, beginning from face-to-face personal communication, and ranging all the way to modern technologies as a historical overview.