Sigurnosti aspekti virtualne mobilnosti

Sučić, Marko-Ferdo

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Marko – Ferdo Sučić

SIGURNOSNI ASPEKTI VIRTUALNE MOBILNOSTI

DIPLOMSKI RAD

Zagreb, srpanj 2020.

SVEUŠILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 8. travnja 2020.

Zavod: **Zavod za inteligentne transportne sustave**
Predmet: **Računalna sigurnost**

DIPLOMSKI ZADATAK br. 5689

Pristupnik: **Marko-Ferdo Sučic (0268014280)**
Studij: Inteligentni transportni sustavi i logistika
Smjer: Logistika

Zadatak: **Sigurnosti aspekti virtualne mobilnosti**

Opis zadatka:

U ovom diplomskom radu potrebno je opisati povijest virtualne mobilnosti, koncept virtualnih privatnih mreža te tržište usluga virtualne sigurnosti. Također u radu je potrebno opisati sigurnosne aspekte virtualne mobilnosti, mobilne uredske jedinice te provesti ogledni primjer analize troškova i koristi rada od kuce.

Mentor:

doc. dr. sc. Pero Škorput

Predsjednik povjerenstva za diplomski ispit:

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

SIGURNOSNI ASPEKTI VIRTUALNE MOBILNOSTI

SECURITY ASPECTS OF VIRTUAL MOBILITY

DIPLOMSKI RAD

Mentor: doc. dr. sc. Pero Škorput

Student: Marko - Ferdo Sučić, 0268014280

Zagreb, srpanj 2020.

Zahvala:

Zahvaljujem na podršci svojoj obitelji i zaručnici Martini koji su mi pomogli da zakružim cijelu svoju edukaciju u diplomiranog inžinjera logistike.

Zahvaljujem mentoru doc. dr. sc. Pero Škorput i dragom prijatelju struč. spec. ing. rač. Antunu Nemaniću na pomoći u izradi ovog diplomskog rada.

Sažetak

Stalni tehnološki napredak tjera gospodarstvo u smjeru inovacije i pružanja više za manje. Takvi koncepti mogući su zbog sve većeg prihvaćanja tehnologija koje reduciraju potrebu za fizičkim prisustvom i kretanjem između dvije točke. Digitalna komunikacija pruža jako veliki prostor za smanjenje operativnih troškova u poslovanju, te sa digitalnom komunikacijom omogućena je i virtualna mobilnost. Virtualna mobilnost podrazumijeva korištenje javne infrastrukture u svrhu komunikacije i podjele podataka ali zbog korištenja javne infrastrukture ugrožena je povjerljivost podataka koji se razmjenjuju u komunikaciji između dvije točke. Zbog rizika izloženosti povjerljivosti podataka potrebno je ulagati u sigurnost virtualne mobilnosti. Kriptografija sa tehnologijom algoritama i mrežnih protokola omogućuje zaštitu podataka tokom korištenja javne ali i privatne mrežne inrastrukture. Najveća izloženost malicioznim napadima u poslovanju vezana je za rad od kuće zbog rizika za štetno djelovanje zaposlenika ili napadača putem presretanja komunikacije.

KLJUČNE RIJEČI: kriptografija, virtualna mobilnost, sigurnost, rad od kuće

Continuous technological advancements are driving economy towards innovation and providing more for less. Such concepts are possible because of the increasing acceptance of technologies that reduces the need for physical presence and movement between two points. Digital communication gives a very large space to reduce operating costs in business, and with digital communication virtual mobility is enabled. Virtual mobiliti involves the use of public infrastructure for the purpose of communication and data sharing, but due to the use of public infrastructure, the confidentiality of data exchange in communication between two points is endangered. Due to the risk of exposure to data confidentiality, it is necessary to invest in virtual mobility security. Cryptography with the technology of algoritms and network protocols enables data protection while using both public and private network infrastructure. The highest exposure to malicious attacks in business is related to working from home due to the risk of harmful actions of employees or attackers by intercepting communication.

KEY WORDS: cryptography, virtual mobility, security, work from home

SADRŽAJ

1. Uvod

Razvojem tehnologije omogućena je globalizacija tržišta sa trenutnom razmjenom podataka i mogućnosti distribucije dobara između svih djelova svijeta. Povećanjem tržišta povećava se i konkurentnost između proizvođača i pružatelja usluga. Sama cijena pojedinog proizvoda diktira poželjnost na tržištu, a tu istu cijenu određuje kretanje cijene rada, energenata te cijene sirovina i repromaterijala. Stoga gospodarstvo definira svoju tržišnu poziciju balansiranjem efektivnosti (kvaliteta proizvoda/usluga kao prioritet) i efikasnosti (reduciranje logističkih i proizvodnih troškova što često rezultira smanjenjem kvalitete proizvoda ili usluge).

Jedan poseban dio svakog opskrbnog lanca je uzvodni i nizvodni tok informacija. Ovaj dio poslovnih procesa je najkompleksniji zbog specifičnih zahtjeva tržišta i poslovnih proces unutar opskrbe i potrošnje. Zbog kompleksnosti tok informacija pruža najviše prostora za stručno proučavanje i ulaganje u razvoj poslovanja. Sami početci u razvoju komunikacijske tehnologije bili su usmjereni na analogni tip komunikacije sa infrastrukturom posvećenom za povezivanje dvije lokacije. Uz rast i razvoj tehnologije uviđena je manjkavost u iskorištenosti potencijalnog kapaciteta infrastrukture te sama potreba za reduciranjem troškova je plasirala ideju o dijeljenju infrastrukture između više korisnika. Dijeljenje je opravdano činjenicom da potrošaći u svojoj komunikaciji ne koriste servis razmjene informacija od 0-24 nego eventualno nešto više od 30% kapaciteta ukoliko se svih 8 sati rada koristi infrastruktura za razmjenu podataka. Postepeno se na tržištu pojavljuju uređaji koji omogućuju dijeljenje infrastrukture poput jedinice za prijenos (*Hub*) i preklopnika (*Switch*). Druga prekretnica u komunikacijskoj tehnologiji je digitalizacija i kompresija podataka. Podatkovne tehnologije kontinuirano odmjeravaju odnos između potrebe za zaštitom povjerljivosti podataka i troška implementacije korištenja ovakvih tehnologija.

Svi prethodno navedeni koraci razvoja komunikacijske tehnologije prikazuju osnovne principe logistike koja traži maksimalizaciju iskorištenosti kapaciteta, obuhvaćanje što većeg tržišta i pružanje dodatne vrijednosti proizvoda i usluga.

Detaljna tematika podatkovne komunikacija i virtualne mobilnosti je razrađena kroz diplomski rad koji je podijeljen u 8 cjelina:

1. Uvod
2. Povijest virtualne mobilnosti
3. Virtualna privatna mreža
4. Tržište virtualne sigurnosti
5. Sigurnosni aspekti virtualne mobilnosti
6. Mobilne uredske jedinice
7. Analiza troškova i koristi rada od kuće
8. Zaključak

U radu druga cjelina prikazuje povjesni razvoj mreža, mrežnih slojeva i postepenu pojavu potrebe za zaštitom komunikacije unutar mrežnih sustava. Treća cjelina opisuje principe rada virtualne privatne mreže (*Virtual Private Network* - VPN). VPN tehnologija omogućuje sigurnost u virtualnoj mobilnosti koristeći kriptografiju i raspoloživu infrastrukturu. Nakon pojašnjavanja funkcioniranja VPN tehnologije u radu se posvećuje pažnja tržištu koje potiče rast i razvoj ove tehnologije. Kod osnovne podjele tržišta VPN-a na osobno i korporativno tržište više pažnje je usmjereno na kompleksnije korporativno tržište. Peta cjelina zaokružuje dosadašnju tematiku vezanu za sigurnost implementacije i potencijalnih ugroza u virtualnoj mobilnosti. Šesta i sedma cjelina razrađuju potencijalna rješenja za rastuće tržište rada od kuće sa popratnom analizom o troškovima i rizicima. Rad završava sa zaključkom o promjenama na tržištu rada i kako na te promjene djelovati s obzirom na obrađeno gradivo u radu.

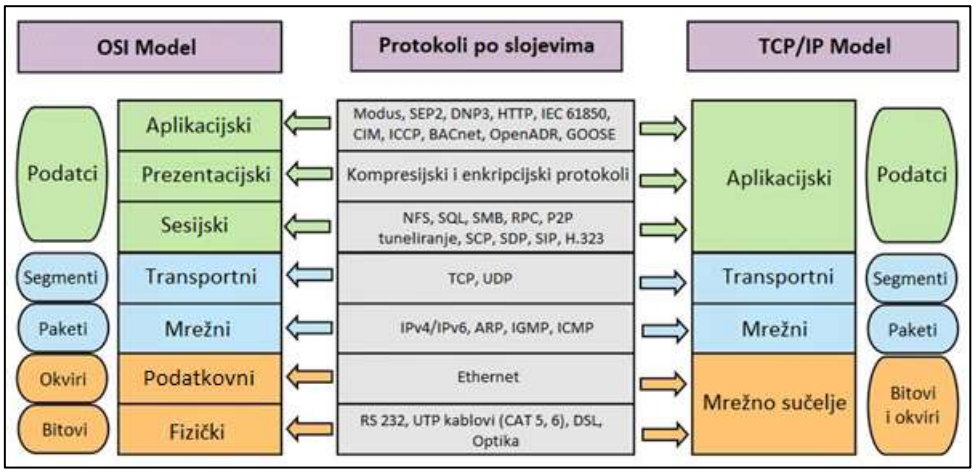
2. Povijest virtualne mobilnosti

Razvoj virtualne mobilnosti možemo pratiti kroz razvoj tehnologije VPN-a. U stručnoj literaturi pojama VPN-a objašnjen je kao skup protokola tokom povezivanja dvije mreže sa svrhom zaštite povjerljivosti podataka koristeći postupke tuneliranja u javnoj mrežnoj infrastrukturi. Jednostavnu i jasnu definiciju pružio je autor Dave Kostur u svoj djelu „Building and Managing Virtual Private Networks“. Kostur pojam VPN-a definira: „Virtualna privatna mreža je mreža virtualnih sklopova za provođenje privatnog prometa“. U nastavku autor dodatno pojašnjava da „Virtualni sklop je veza uspostavljena na mreži između pošiljatelja i primatelja gdje se obje rute za sesiju i propusnost dodjeljuju dinamično. VPN-ovi se mogu uspostaviti između dvije ili više lokalnih mreža ili između udaljenih korisnika i lokalne mreže“. Dakle osnovno definiranje VPN-a nalaže da je to privatna veza između dva korisnik te se izuzima pojam enkripcije i korištenje javne mreže kao uvjeti za mogućnost metodologije rada VPN-a. Unatoč općem poimanju da je VPN isključivo mrežna veza za kriptiranu komunikaciju između dva ili više korisnika putem jave infrastrukture.[1]

Za potpuno razumijevanje ovakvog tipa mreže potrebno je prvo razumjeti razvoj ove tehnogije kroz povijest. Početci potrebe za sigurnom mrežnom vezom između dva korisnika nametnuto je od korporativnog tržišta, državnih sustava i vojske. Zahtjevi na koje sigurnosni informacijski sustav mora odgovoriti su povjerljivost, integritet i raspoloživost podataka. Podatak je povjerljiv kada je nerazumljiv svima osim onima koji su autorizirani za njegovo korištenje, integritet je identičnost podataka stanju koje je ostavljeno od zadnjeg autoriziranog korisnika, raspoloživost je dostupnost podataka autoriziranom kosniku u dogovorenom formatu i razumnom vremenskom roku. Prvi oblici zaštite podataka su se realizirali kroz vlastitu mrežnu infrastrukturu što je značio izrazito visok trošak ali i infrastrukturnu limitiranost u povezivanju udaljenih ili nedostupnih lokacija. Neefikasnost pri korištenju djelomičnog kapaciteta vlastite infrastrukture nameće razvoj tehnologije koja će omogućiti veću iskoristivost infrastrukture, odnosno dijeljenje postojeće javne mrežne infrastrukture.

Kasnih 60-ih Američko ministarstvo obrane projektom ARPANET gradi prvi oblik mreže koji započinje potrebu za standardizacijom formatiranja podataka u svrhu realizacije međusobnog povezivanja različitih lokalnih mreža. Prvi iskorak u povezivanju više mrežnih sustava započinje uvođenjem mrežnih slojeva OSI model (*Open Systems Interconnection*) te nešto kasnije kasnije i TCP/IP 70-ih (*Transsmition Control Protocol/Internet Protocol*) (slika

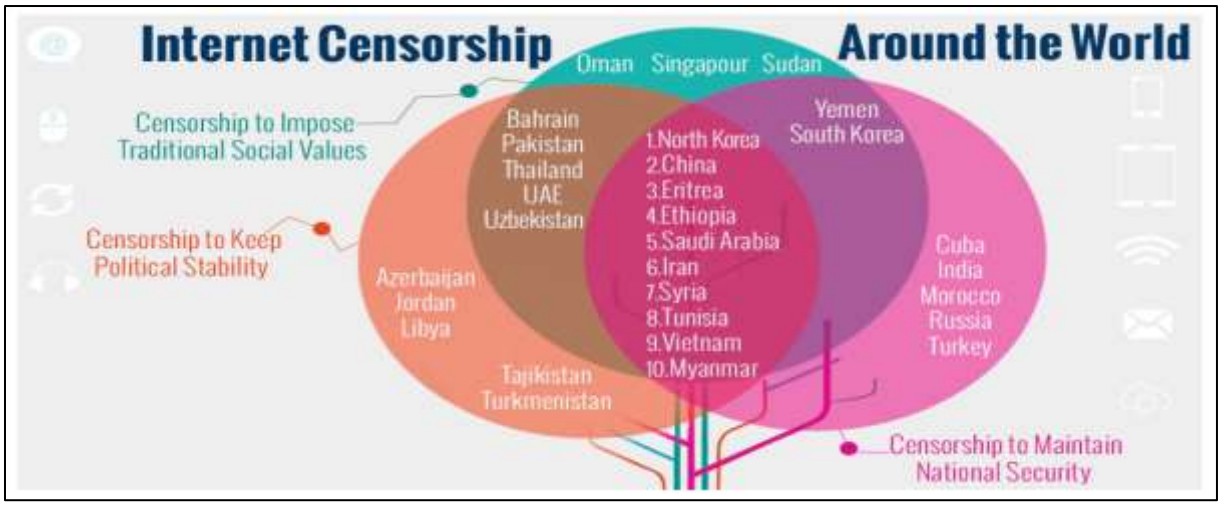
1). Uz ovakav tržišni napredak započinje konkretnija ideja za tehnologije poput VPN-a. 1993. AT&T Bell Labs i Columbia University sa zajedničkim istraživačkim timom razvija SwIPe (*Software IP Encryption Protocol*) što predstavlja prvi oblik privatne mreže sa enkripcijom. SwIPe projekt je prioritizraio sigurnost podataka na višu razinu u odnosnu na druge oblike povezivanja u to vrijeme. 1994. Postavljeni su prvi sigurnosni protokoli za enkripciju i autentifikaciju paketa podataka dijeljenih mrežama u obliku IPsec (*Internet Protocol Security*) sustava.



Slika 1: Usporedba OSI i TCP/IP modela sa protokolima u pojedinom sloju

Izvor: https://www.researchgate.net/figure/The-logical-mapping-between-OSI-basic-reference-model-and-the-TCP-IP-stack_fig2_327483011/ 15.04.2020.

Prvi oblik VPN tehnologije koji je prepoznatljiv danas nastao je na temeljima postavljenim od zaposlenik Microsofta, Guardeep Singh Pall 1996. Pall je svoj doprinos u stvaranju VPN-a pridonio razvojem PPTP (*peer-to-peer tunneling protocol*) protokola.



Slika 2: Internetska cenzura u svijetu

Izvor: https://www.le-vpn.com/history-of-vpn/ 15.04.2020.

Paralelno uz razvoj korporativne VPN tehnologije, tržište fizičkih pojedinaca postepeno razvija svijest o sigurnosti i potrebi za zaštitom osobnih podataka. Svijest kod opće populacije se razvija uz događaje poput wikileaks-a, geopolitičkih restrikcija, cenzura, eksploatacija osobnih podataka poput događaja vezanih za djelovanje Cambridge Analytica, regionalna zaključavanja pojedinih aplikacija (poput nemogućnosti korištenja Whatsapp aplikacije u Ujedinjenim Arapskim Emiratima) i druge slične potrebe nastale zbog pojedinih restrikcija ili zakonskih zabrana koje su aktivne u pojedinim državama (slika 2).

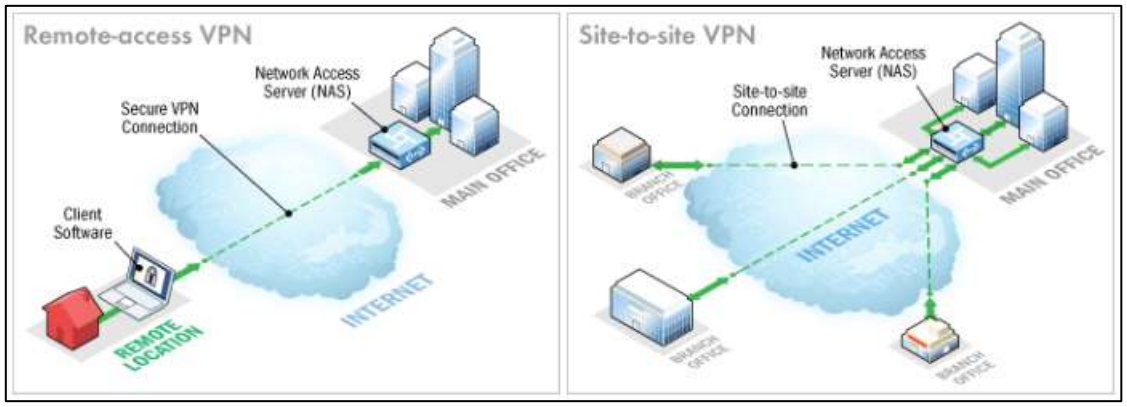
Uz prethodno osnovno definiranje VPN-a ovu tehnologiju dalje dijelimo po obliku tehnologije rada, VPN opremi i infrastrukturi, mrežnim protokolima te enkripcije mrežne povezanosti. Svaka ova podjela je razvijena za određeni dio tržišta koji pokušava uspostaviti ravnotežu između cijene, razine sigurnosti i brzine razmjene podataka uz dodatna ograničenja za konkurentnost na pojedinim tržištima. Kvalitetan rad ovakve tehnologije ovisi o njenoj namjeni. Ukoliko se tehnologija koristi za razmjenu podataka koji trpe povremene prekide povezanosti poput dijeljenja datoteka ili preuzimanja podataka onda programski alati pružatelja VPN usluga zadovoljavaju tu potrebu. Ako ovu tehnologiju želimo koristiti za dijeljenje funkcija računalne periferije poput ekrana i audio komunikacije (VoIP – *Voice over IP*) između udaljenih lokacija i na taj način koristiti računalne programe tada može doći do otežanog rada pri korištenju ove tehnologije jer pojedini računalni sustavi traže da se na akciju korisnika javlja trenutna reakcija sustava. Glavni problem zbog kojeg dolazi do prekida veze VPN-a u slučaju djeljenja ekrana je veliki zahtjevi skidnja i slanja podataka koji se šifriraju i dešifriraju pa se

stvara usko grlo u komunikacijskoj vezi. To usko grlo može biti uvjetovano brzinom kriptivnih programa, opreme ili nedostatna internetske brzine.

Svaki zahtjev za ovom tehnologijom se može individualno promatrati stoga i opširnije treba gledati slijedeće podjele unutar ove tehnologije.

2.1. Tehnologije rada

Tehnologije rada odnose se na oblik konfiguracije mreže. Prepoznajemo tri oblika: intranet, udaljeni pristup i extranet. Sve ove tehnologije koriste mrežni pristupni server (*network access server* - NAS) putem kojeg se potvrđuje identitet korisnika prije ulaza u zaštićenu mrežu kao što je prikazano slikom 3. Intranet i extranet spadaju u zajedničku kategoriju *eng. site-to-site* povezivanja koji svojim principom rada omogućuje korisnicima pristup računalnim resursima jedne lokacije drugoj.



Slika 3: Vrste povezivanja putem mrežnog pristupnog servera

Izvor: https://computer.howstuffworks.com/vpn4.htm/ 21.04.2020.

Intranet VPN je oblik povezivanja više lokacija unutar kompanije u jednu zajedničku privatnu mrežu. Ovaku primjenu načešće koriste firme koje imaju više udaljenih podružnica sa vlastitom lokalnom mrežom. Ova tehnologija omogućuje kreiranje zajedničke mreže širokog područja (*Wide Area Network* - WAM). Intranet najčešće služi za razmjenu email komunikacije u kompaniji ili razne oglasne platforme koje su namjenjene djelatnicima kako bi bili upućeni u ciljeve i obaveze unutar poduzeća. Česti korisnici ovakve tehnologije su trgovački putnici koji trebaju mogućnost povezivanja sa internom mrežom firme u svrhu pristupa i ažuriranja podataka (npr. promjena stanja skladišta u slučaju kupovine na terenu).

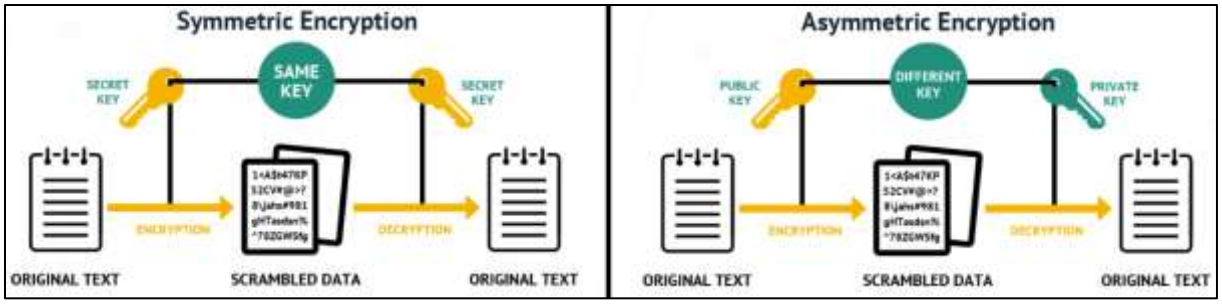
Extranet VPN je sličan princip rada kao i intranet ali on nije namjenjen kako bi povezao podružnice unutar kompanije nego kako bi povezao dvije partnerske kompanije. Zbog partnerskog odnosa kompanije imaju potrebu za komunikaciju u svrhu realizacije usluge ili razmjene informacije relevantne za obostrano poslovanje. Ovaj oblik VPN-a je često prisutan kod održavanja poslovnog odnosa sa dobavljačima i kupcima uz određene restrikcije koje onemogućuju pristup kompletnom intranetu kompanije.

Udaljeni pristup ili VPDN (V*irtual Private Dailup Network*) je princip rada *eng. client-to-server*. VPDN uz NAS zahtjeva instalirani program kod korisnika koji pokušava uspostaviti povezanost sa zaštičenom mrežom. Ova tehnologija je najpogodnija za potrebe rada od kuće gdje je djelatniku omogućen pristup njegovom računalu korištenjem adekvatnog programskog alata. Većina operativnih sustava ima u sebi ugrađen program koji omogućuje ovakvo povezivanje što uvelike olakšava implementaciju i rasprostranjenost ove tehnologije.

2.2. Enkripcija mrežne povezanosti

Sve prethodne tehnologije i tehnička rješenja koriste algoritme za enkripciju podataka i ključeve koji autoriziranom korisniku omogućuju dešifriranje podataka. Svrha svake enkripcije je osigurati integritet, povjerljivost, autentičnost i neporecivost primatelja ili pošiljatelja podataka. Ključeve za dešifriranje podataka dijelimo na simetrične i asimetrične, javne i privatne ključeve (slika 4). Simetrični ključevi su predviđeni za brže procesuiranje pa su samim time na manjoj razini enkripcije iako se smatraju sigurnim oblikom enkripcije. Simetrični ključevi koriste jednostavnije algoritme koji ne zahtjevaju visoku procesnu snagu opreme. Asimetrični ključevi su kompleksiniji i otporniji na sigurnosne ugroze ali cijena više sigurnosti je potreba za kvalitetnijom procesnom snagom računalne opreme. Asimetrični ključevi se lako distribuiraju korisnicima koristeći certifikacijska tijela (*Certification Authority* - CA) za izdavanje certifikata javnog ključa. Primjer CA je povezivanje na internet bankarstvo putem USB-a za digitalni potpis. U modernoj kriptografiji često se koristi kombinacija simetričnog i asimetričnog ključa kako bi se iz obje tehnologije iskoristio maksimalni potencijal. Asimetrični dio moderne kriptografije zadužen je za razmjenu privatnih ključeva te na taj način omogućuje lakšu razmjenu i modifikaciju privatnog ključa za simetričnu enkripciju. Simetrični ključ omogućuje bržu komunikaciju i manju procesnu snagu potrebnu za enkripciju.

Koncept moderne kriptografije stavlja CA u ulogu praćenja cijelog sustava komunikacije i ključeva koji se koriste.



Slika 4: Usporedba procesa enkripcije sa simetričnim i asimetričnim ključem

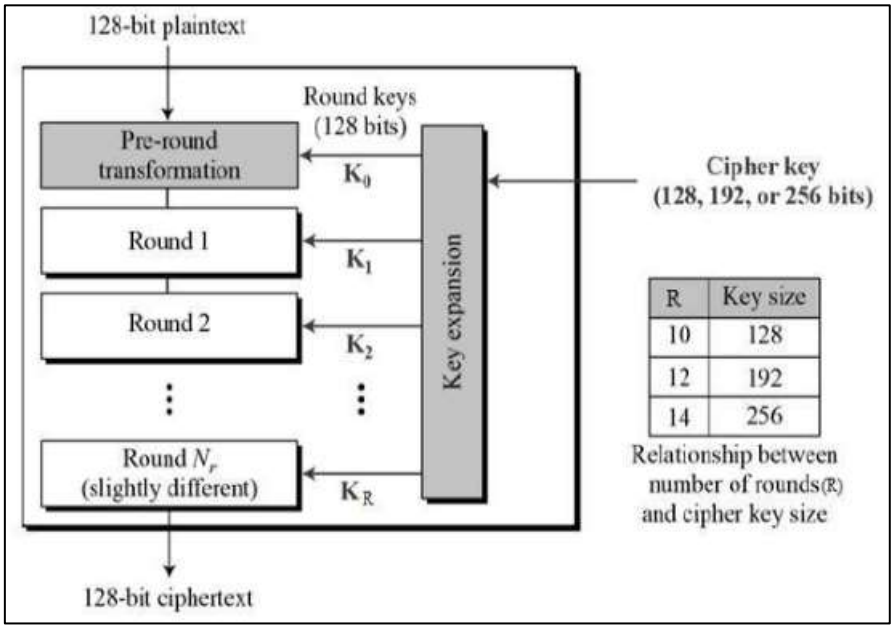
Izvor: https://www.cheapsslshop.com/blog/symmetric-vs-asymmetric-encryption-whats-the-difference/ 21.04.2020.

U samom procesu enkripcije koristimo *eng. hash* funkcije. Hash je jednosmjeran i jednoznačan što znači da je svaki hash jedinstven i može se pratiti njegova postepena promjena kroz komunikaciju. Jednostavniji primjer ove tehnologije je u kriptovaluti kod *eng. Blockchain* tehnologije koja ovisi o mogućnosti povjesnog pregleda transakcija i jedinstvenosti kriptovalute.

Kada govorimo o algoritmima u digitalnoj kriptografiji onda time obuhvaćamo jako široki spektar mogućnosti od jednostavnijih algoritama poput Cezarove šifre do algoritama koji se koriste u VPN tehnologiji poput 3DES, DES, AES sa simtričnim ključevima i Diffie-Hellman, RSA, ECC sa asimetričnim. Unutar svakog algoritma definira se duljina ključa izražena u bitovima te količinu podataka u blokovima. Varijacija između ove dvije vrijednosti definiraju izloženost na *eng. brute force* napada. Ukoliko koristimo više i veće ključeve onda je i sama otpornost na napad veća. Također veći podatkovni blokovi omogućuju višu razinu sigurnosti uz cijenu brzine.

Jedan od sigurnijih i bržih algoritama je AES (*Advanced Encryption Standard*) sa tehnologijom simetričnog ključa. AES je nastao nakon što se 3DES u široj upotrebi prikazao presporim za funkcionalnost VPN-a. AES je također postigao višu razinu sigurnosti sa rasponom ključeva od 128 bita do 256 bita. Za razliku od prethodnika koji su vršili enkripciju na razini bita AES tu funkciju obavlja na razini bajta. Osnovni princip rada ovog algoritma je zamjena i permutacija bajtova tokom generiranja kriptiranih podatkovnih blokova. Blok od 16 bajtova u 4 stupca i 4 red se procesuira kao matrica. Broj transformacija u AES algoritmu ovisi

o konfiguraciji ključa pa za 128-bitni ključ koristi 10 ciklusa, 192-bitni 12 ciklusa, 256-bitni 14 ciklusa. Po završetku svakog ciklusa algoritam kreira novi ključ koji je inicijalno izračunat po uzorku na originalni AES ključ (slika 5).

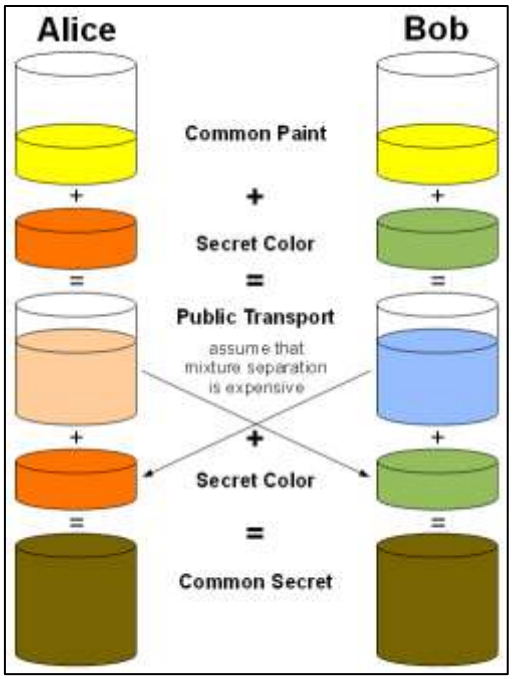


Slika 5: Transformacijski ciklusi u AES algoritmu

Izvor: https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm/ 25.04.2020.

Unutar jednog ciklusa AES obavlja funkcije *SubBytes, ShiftRows, MixColumns i AddRound Key*. Tokom dešifriranja koriste se inverzne funkcije izuzev *AddRound Key* koji je sam sebi inverzan zbog prethodnih koraka i funkcija.

Za razmjenu javnog ključa često se koristi asimetričnih algoritama Diffie-Hellman koji je patentiran 1977. Često se Diffie-Hellman objašnjavanja pomoću usporedbe algoritma sa miješanjem boja (slika 6). Svaki korisnik ima svoju jedinstvenu boju (odnosno šifru) u trenutku pokretanja komunikacije između dva korisnika. Oba korisnika koriste javni prostor koji ima svoju boju (šifru) te svaki korisnik uzima identični definirani uzorak iz javnog prostora. Nakon toga svaki korisnik u svoj privatnom prostoru obavlja miješanje (kriptiranje) svog i javnog dijela. U slijedećim koracima oba korisnika novu pomiješanu boju (šifru) razmjenjuju kroz javni prostor te se ponavlja procedura miješanja sa vlastitim bojama (šiframa) u privatnom prostoru. Rezultat je identična količina i nijansa boje (šifre) koje napadač nije u mogućnosti replicirati promatrajući razmjenu podataka u javnom prostoru.



Slika 6: Diffie-Hellman razmjena ključa

Izvor: https://www.wst.space/ssl-part-2-diffie-hellman-key-exchange/ 27.04.2020.

Za zaštićenu komunikaciju putem enkripcijskih algoritama potrebno je odabrati one koji sadrže optimalnu količinu ključeva, bitova po ključu i veličine podatkovnih blokova. Ukoliko se svi resursi usmjere na sigurnost, a zanemari se komponenta brzine moguće je zasićenje računalnog kapaciteta za procesuiranje koje rezultira gubitkom funkcionalnosti mrežnog sustava.

2.3. Mrežni protokoli

Mrežni protokoli za VPN povezanost ranije je spomenuta kod udaljenog pristupa te je njihova osnovna svrha namijenjena za realizaciju takvog oblika mrežne povezanosti iako se koristi u kombinaciji sa drugim tehnologijama radi više sigurnosnih slojeva zaštite. Ovakvi programi su protokoli koji omogućuju tuneliranje između dva korisnika koristeći kriptografske tehnologije. Tuneliranje je proces povezivanja dvije mreže koristeći resurse treće mreže koju najčešće čini internet. Postoji dosta programskih alata koji se koriste u svrhu ovakve povezivosti sa međusobnim razlikama u enkripcijskim metodama poput:

1. IPsec – koristi protokole *eng. Authentication Header* (AH), *Encapsulated Security Payload* (ESP), *Security Assosiation* (SA). AH je zadužen za integritet i neporecivost IP paketa, ESP je zadužen za enkripciju korisnog dijela IP paketa uz osiguravanje integriteta i autentičnosti podataka. SA protokol je zadužen az generiranje i razmjenu ključa putem IKE (*Internet Key Exchange*) faza. IKEv2 (nova generacija prethodnika IKE) koristi algoritme poput 3DES, AES sa veličinom do 256 bitnih ključeva. IPsec se smatra sigurnim protokolom kada se koristi u obliku tuneliranja. Uz tuneliranje IPsec je moguće konfigurirati na transportni način rada koji izlaže sigurnost veze zbog kriptiranja samo korisnog djela IP paketa što ostavlja adrese primatelja i pošiljatelja javnim, odnosno sigurnosno izloženim.

2. PPTP – *Point-to-Point Protocol* koristi P2P (*Point-to-Point*) protokol za enkripciju sa RSA algoritmom i maksimalnim 128 bitnim ključem. Zbog jednostavnijeg ključa ovaj protokol se smatra brzim ali i izloženijim potencijalnim napadima.

3. TLS – *Transport Layer Security* je protokol koji je zamijenio SSL (*Secure Sockets Layer*) 2015. SSL je i dalje u upotrebi zbog svoje raširenosti tokom prošlosti. Prednost ovog protokola je njegova integriranost u preglednike poput Firefox, Chrome, Safari. Zbog toga je relativno jednostavan za udaljeno povezivanje koristeći preglednike koji ujedino pružaju korisničku potporu. Enkripcija u ovom algoritmu se vrši na transportnom sloju OSI modela. Za razmjenu ključa u TLS protokolu se pokreće takozvano rukovanje između dva korsnika koje inicira razmjenu enkripcijske metode. TLS uz klasično tuneliranje nudi i povezivanja VPN-a putem preglednika.

4. L2TP – *Layer 2 Tunneling Protocol* vrši enkripciju na drugom mrežnom sloju. Često se koristi zajedno sa IPsec ili PPTP za pokretanje VPN veze. L2TP je optimalna kombinacija PPTP i svog prethodnika L2F (*Layer 2 Forwarding*).

Svaka od ovih tehnologija ima svoje specifične namjene i različitosti po obliku enkripcije, razine mrežnog sloja koji je obuhvaćen enkripcijom te mehanizme vezane za podjelu ili generiranje ključa.

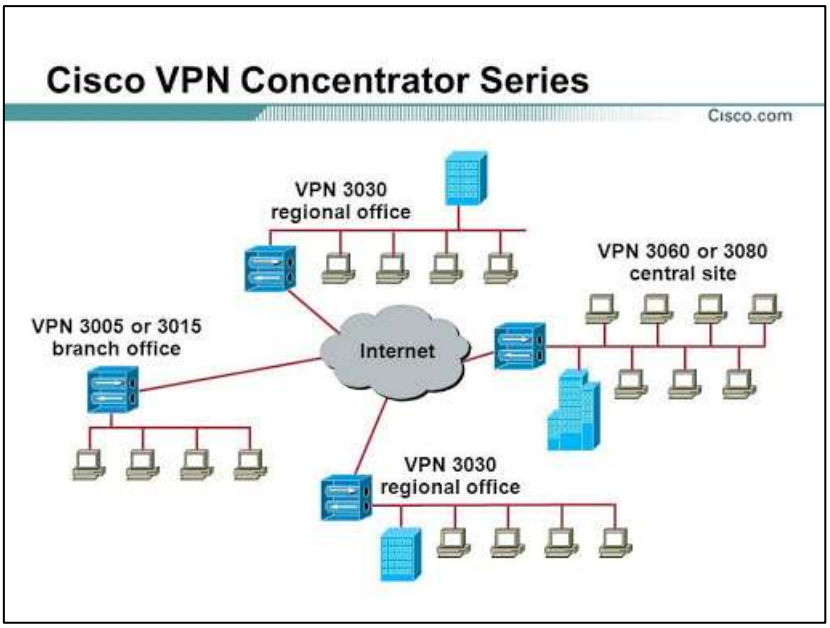
2.4. VPN oprema i infrastruktura

Specijalizirana VPN oprema usmjerena je na održavanje stalnih sigurnih veza između više lokacija, ovakvo tehničko rješenje najčešće je korišteno u intranet i extranet konfiguracijama. VPN oprema može omogućiti dodatnu sigurnost i brzinu u obradi podataka tokom enkripcije što je važno za brze direktne komunikacije između dva poslovna partnera sa velikim mrežnim prometom. Oprema obuhvaća VPN koncentrator za omogućavanje velikog broja mrežne povezanosti, VPN usmjerivač za povezivanje i komunikaciju manji broj uređaja s jednom VPN vezom, VPN vatrozid i VPN klijent program na računalu. Ovakva oprema je izrazito skupa i može vrlo brzo generirati troškove od nekoliko desetaka tisuća eura ali u tu cijenu korisnik dobije najbolju moguću razinu sigurnosti.

VPN usmjerivač obavlja više zadataka ovisno opremi i programima koji se koriste u mrežnoj konfiguraciji. Ovisno o postavkama operativnog sustava usmjerivač može kreirati i određenu količinu VPN tunela. Cisco ruteri podržavjaju IPsec, L2F, L2TP, PPTP, IPinIP i GRE te vrše enkripciju u samom usmjerivaču. Povoljniji usmjerivači na tržištu isto tako obavljaju funkciju procesuiranja enkripcijskih alata ali svaki ima razlike u oblicima protokola koje koristi i kapacitetu ovisno o operativnom sustavu i komponentama opreme poput memorije. Ovakvi ruteri su pogodni za kreiranje nekoliko stotina VPN veza što je uglavnom dovoljno za poslovanje manjeg i srednjeg poduzetništva. Za povećanje kapaciteta kreiranja i održavanja VPN veza koristi se VPN koncentrator.

VPN koncentrator je mrežni uređaj za kreiranje VPN veza i komunikaciju između mrežnih čvorova. Koncentrator možemo promatrati kao usmjerivač specijaliziran za kreaciju i konfiguraciju komunikacijske infrastrukture mreže širokog područja. Ovakav uređaj predviđen je za kreiranje i održavanje velike količine VPN veza. CISCO serija 5000 VPN koncentratora upravlja sa do 50.000 tunela, dok serija 3000 ima mogućnost kreiranja 10.000 tunela (slika 7). Takvi uređaji su zastupljeni kod pružatelja VPN usluga. Uz postizanje veze između dva čvora

ovaj uređaj se koristi i za autetifikaciju korisnika za ulaz u središnji server, definiranje parametra i načina funkcioniranja mrežne veze te upravljanje ključevima.



Slika 7: Cisco VPN koncentratori, serija 3000

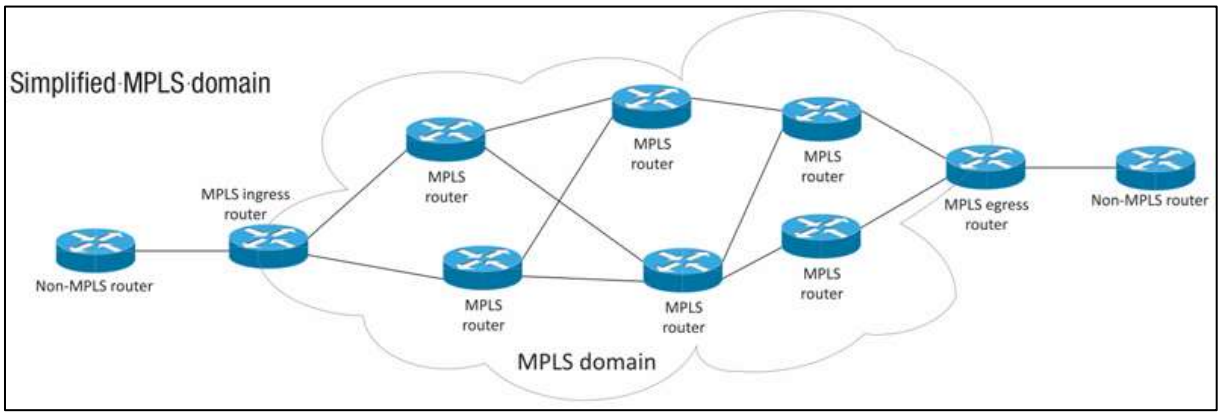
Izvor: http://www.myshared.ru/slide/892021/ 21.04.2020.

VPN vatrozid ili Cisco ASA u slučaju korištenja Cisco tehnologije. Cisco ASA ima nekoliko verzija od nešto slabijih uređaja sa kapacitetom od 300 Mbps (*Megabit per second*) i kvalitetnih modela sa brzinom do 2 Gbps (*Gigabit per second*). ASA vatrozid podržava nekoliko varijacija protokola koji se mogu konfigurirati za zaštičenu komunikaciju poput IPsec udaljenog pristupa sa IKE razmjenom ključeva ili IPsec site-to-site VPN sa IKE ili IKEv2. U sklopu porotkola koriste se enkripcijske metode poput AES, 3DES, RSA, itd.

VPN klijent je program za krajnjeg korisnika koji se koristi na računalu i serveru za kreiranje tunela prema usmjerivaču, koncentratu ili vatrozidu. Cisco Secure VPN klijent nudi opciju SafeNet klijenta za povezivanje računala sa usmjerivačem ili vatrozidom i drugu opciju povezivanja korisnika sa koncentratorom.

Funkcije ovakve infrastrukture moguće je zamjeniti korištenjem usluga djeljenja servera koji onda obavljaju aktivnosti prethodne opreme. Takvo dijeljenje infrastrukture ugrožava sigurnost podataka u VPN-u koje pojedino poduzeće koristi. Pod VPN opremu klasificiramo i mrežnu infrastrukturu koju je moguće zakupiti radi realizacije direktne veze između dvije lokacije koje imaju potrebu za stalnom zaštićenom komunikacijom. Na taj način poduzeće u svojoj mrežnoj infrastrukturi ima veću propusnost podataka i manju izloženost njuškanja

prometa od potencijalnih napadača. Direktna veza omogućuje stabilnost u komunikaciji koja je pogodna za konferencijsku komunikaciju pružajući raspon brzine skidanja i slanja od 5 Mbps do 10 Gbps ovisno o potrebi korisnika. Problem direktne veze je oko 20 puta viša cijena od širokopojasne mreže.



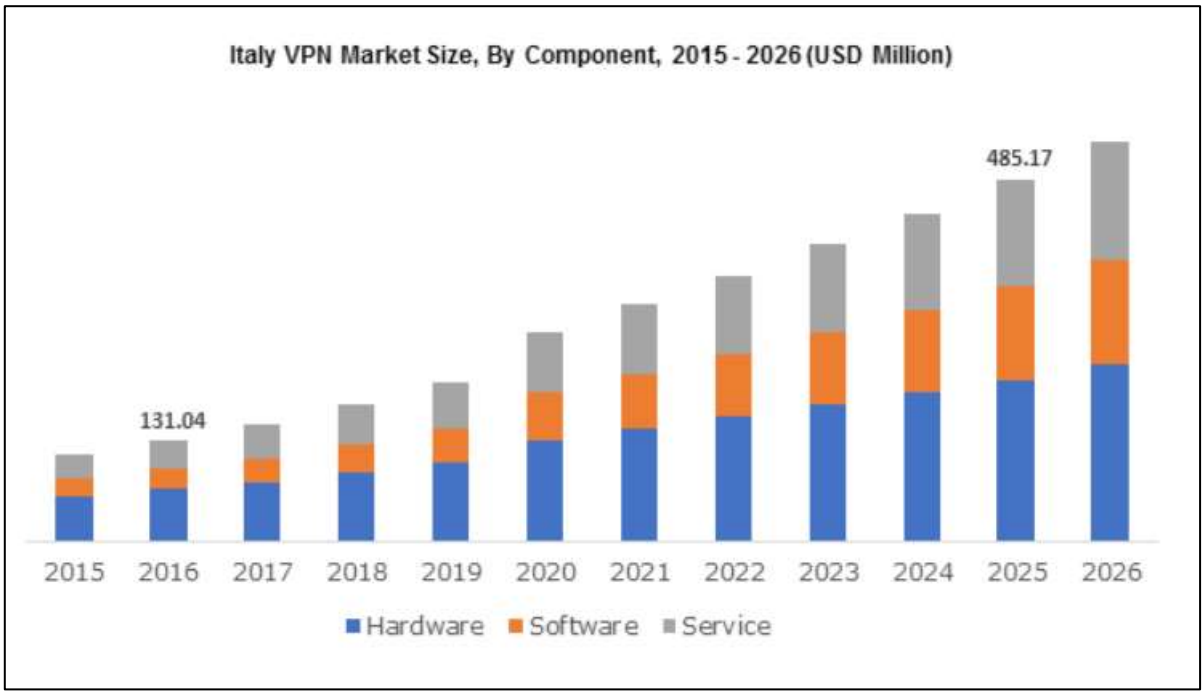
Slika 8: Pojednostavljen prikaz MPLS mreže

Izvor: https://broadbandlibrary.com/mpls-what-is-it-in-plain-english-please/ 25.04.2020.

Na tržištu se nudi i MPLS (*Mulitiprotocol Label Switching*) tehnologija koja umjesto nasumičnog kretanja IP paketa od mjesta slanja do mjesta primanja podataka nudi fiksiranu mrežu kretanja podataka u trenuku pokretanja mrežne komunikacije (slika 8). Uz kreiranje fiksne rute tokom kretanja podataka na IP pakete stavlja *eng. Lable* sa funkciom spriječavanja kontinuiranog pregleda adrese paketa što bi u teoriji trebalo ubrzati komunikaciju između dva čvora. Neki od ponuđača ovakvih usluga tvrda da imaju kompletnu vlastitu infrastrukturu kako bi se povećala brzina i sigurnost mrežne komunikacije.

3. Tržište virtualne sigurnosti

Kada govorimo o ekonomskom potencijalu tržišta sigurnosti virtualne mobilnosti potrebno je podijeliti ga na korporativno i osobno tržište virtualne sigurnosti. Korporativni aspekt je usmjeren u korištenju specijalizirane opreme kako bi se maksimizirala brzina i privatnost podataka koji se razmjenjuju. Osobni aspekt je usmjeren u zaštitu ili prikrivanje identiteta tokom surfanja internetom. Kompletno tržište možemo razdvojiti na tri dijela: VPN računalna oprema, programi i pružatelji VPN usluge. Globalno tržište VPN-a 2019. procjenjuje na 25 bilijuna USD uz predviđeni rast složene godišnje stope rasta (CAGR) od 12% što predstavlja projekciju od 70 bilijuna USD tržišne vrijednosti VPN-a u 2026. Razvoj VPN tržišta potiče izloženost interneta malicioznim napadima, širenje internetskih usluga, razvoj sigurnosnih standarda za digitalnu komunikaciju, povećena implementacija kriptirane komunikacije unutar poslovnih procesa te posebno bitno za 2020. godinu pojava globalne pandemije.



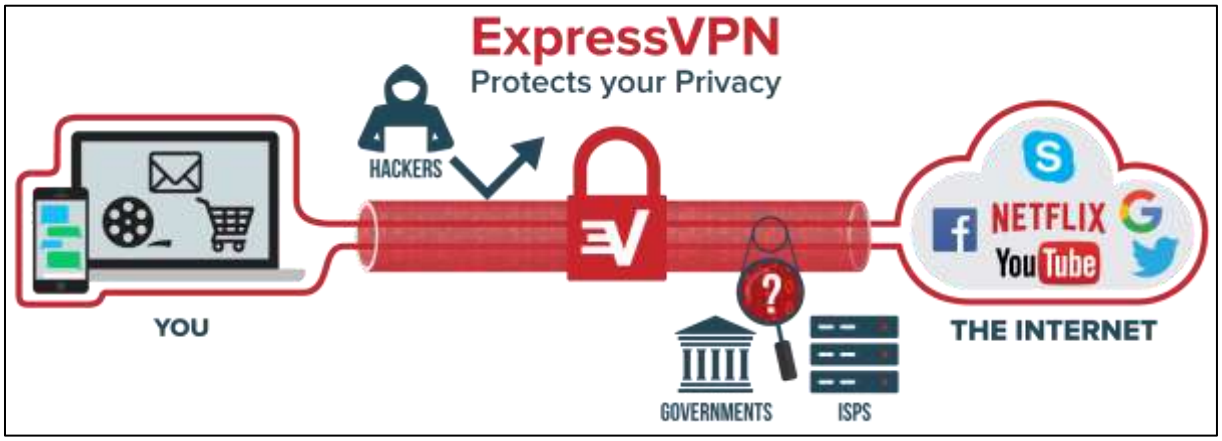
Slika 9: Tržište VPN tehnologije u Italiji

Izvor: https://www.gminsights.com/industry-analysis/virtual-private-network-vpn-market/ 21.04.2020.

Po primjeru Italije sa slike 9 možemo vidjeti da je najveći udio tržišta VPN-a 2019. bio usjeren na računalnu opremu za pružanje VPN-a ali trendovi se sve više usmjeravaju na ekonomičnija i jednostavnija programerska rješenja.

3.1. Osobno tržište virtualne sigurnosti

Kao što je prethodno navedeno ovo tržište ima primarni cilj zaštitu i prikrivanje identiteta korisnika. Ovaj dio tržišta isključivo je usmjeren u korištenju programskih rješenja kako bi se postigla sigurna veza između pružatelja VPN usluge i internetske stranice na koju se korisnik želi spojiti (slika 10). Programska rješenja su poželjna za ovo tržište zbog ekonomičnosti uz prihvatljiv rizik manje sigurnosti i brzine u odnosu na korištenje specijalizirane VPN opreme (sklopova). Ovakav princip VPN-a koristi se za zaobilaženje regionalnog zaključavanja poput geografske restrikcije kompanije Netflixa (EU tržište u odnosu na Američko tržište). Za zaobilaženje tih restrikcija korisnici uz pomoć VPN maskiraju svoju IP adresu u IP regije koja ima propusnost prema traženom servisu. Uz prethodni razlog, VPN se koristi u osobne svrhe kako bi se zaštitili od malicioznih napada (krađa lozinke ili korisničkog imena) te kako bi uspjeli zaobići državne restrikcije koje su aktivne u pojedinim zemljama (Vatrazid u Kini za Youtube, Whatsapp, itd.). Neki od najpoznatijih VPN servisa su NordVPN, ExpressVPN, Surfshark, TunnelBear, itd.



Slika 10: Promotivni materijal pružatelja VPN usluge

Izvor: https://www.expressvpn.com/what-is-vpn/ 15.04.2020.

Također uz upotrebu već postojećih pružatelja VPN usluge moguće je i samostalno „podići“ vlastiti VPN uz *eng. cloud hosting*, postavljanje terminala i programskih skripti dostupnih poput na stranici Pritunl. Podizanje vlastitog VPN-a ima ograničenje u korištenju maskiranja IP adrese. Ukoliko vlastiti VPN želimo koristiti u svrhe maskiranja IP-a onda je

potrebno samostalno fizički postaviti server u željenoj regiji sa svrhom pružanja VPN-a za njegovog korisnika.

3.2. Korporativno tržište virtualne sigurnosti

Korporativno tržište virtualne sigurnosti obuhvaća sve oblike povezivanja između više poslovnih subjekata za realizaciju zaštičene razmjene podaka putem tuneliranja i VPN serverske opreme. Uz prethodnu potrebu ovo tržište zahtjeva povezivanje mobilnih korisnika sa intranetom poduzeća. Povezivanje se ostvaruje u svrhu dostupnosti i razmjene podataka između poduzeća i djelatnika te povezivanje korisnika sa uslugama poslovnog subjekta uz zaštičenu mrežnu komunikaciju.

Korporativno tržište je izuzetno osjetljivo na sadržaj svojih podataka zato puno više ulaže u više slojeva zaštite mrežne infrastrukture. Primjeri višeslojne zaštite je korištenje zakupljene mrežne infrastrukture sa VPN opremom koja ima u sebi integrirane protokole koji omogućuju zaštićenu komunikaciju. Nastavno na tu opremu se dodatno podižu i tuneli poput IPsec protokola što ukupno čini tri sloja zaštite kada to promatramo na način da imaju svoju infrastrukturu za komunikaciju, oprema koja ima integriranu protokolarnu komunikaciju i programsku zaštitu putem tuneliranja. Više razine sigurnosti su potrebne u sustavima poput bankarstva gdje manji sigurnosni propust može rezultirati velikim gubitcima za poslovanje.

Veliki potencijal za koporativno tržište krije se u izvedbi poslovnog procesa u obliku rada od kuće. Kapital u ovakvom poslovanju je vezan za troškove uredskog prostora, putnih troškova i zadovoljstvo djelatnika kao kapital poduzeća u privlačenju tržišta radne snage. Tržište prijevoda i izrade transkripti je iskoristio ovu mogućnost kako bi uspio proširiti svoju ponudu raznovrsnih jezika i pristupačnijih prevoditelja ali i kako bi obuhvatio veću potražnju na globalnom tržištu. Isti mehanizam leži i u implementaciji rada od kuće gdje poduzeće potencijalno obuhvaća veće tržište rada sa puno većim izborom kvalificirane radne snage ali i jednako tako mogućnost širenja svojeg poslovanja na veće tržište. Naravno uvjeti za realizaciju ovakvog modela poslovanja jako ovisi o sigurnosnim uvjetima koji moraju biti zadovoljeni kako bi se zaštitio ugled firme. Tradicionalni način poslovanja omogućuje lakšu kontrolu osjetljivih podataka korištenjem fizičkog nadzora. VPN tehnologija omogućuje da se rad od kuće proširi na ta osjetljivija radna mjesta uz pravilno propisane dodatne mjere sigurnosti.

Dosta novootvorenih kompanija vodi svoje poslovanje bez fizičkih ureda kako bi minimizirali fiksne troškove uredskog interijera i najma prostora. Takav oblik poslovanja se kreira u samom dizajniranju svojih poslovnih procesa. Kompanije sa izuzimanjem fizičkog ureda iz svog poslovanja nazivaju se *eng. remote office* ili udaljeni ured. Ovakvi uredi pružaju fleksibilnost svojim djelatnicima u zamjenu za smanjenje opretivnih troškova što daje rasterećenje početnog ulaganja za pokretanje poslovanja. Početci ovakvog formata poslovanja su prepoznatljivi u *eng. freelance* angažmanima koji su česti kod programera. Tržište programskog razvoja kontinuirano ima veću potražnju od ponude za svojim uslugama pa je bilo bitno žrtvovati direktnu komunikaciju i pojačane kontrole nad poslovnim procesom u zamjenu za angažman djelatnika kojih na tržištu nema dovoljno. U prilog ovakvom obliku poslovanja ide sveprisutna adekvatna informatička oprema, educiranost radne snage za rad na računalu ali i dostupnost internetske odnosno mobilne tehnologije koja prije nekoliko desetljeća nije bila ni približno pristupačna kao danas. Danas je moguće realizirati cjelodnevnu komunikaciju za cijenu internetske veze koja je daleko niža od troška samog održavanja uredskog prostora za pojedinca. Uz tehnologije oblaka poduzeća danas nemaju potrebe čak ni za vlastitim računalima ukoliko svojim djelatnicima tokom sklapanja ugovora o radu uvjetuju korištenje vlastitih računala za rad od kuće. Važno je napomenuti da će uvijek postojati fizički dio prostora koje pojedini poslovni subjekt mora zauzeti zbog zakonskih regulativa i potreba za papiratim zapisima ali i zbog sigurnosti podataka. Sigurnost podataka je veća ukoliko je poslodavac sam vlasnik opreme za pohranjivanje podataka.

Tema u ovom radu fokusirana je na poslovanje koje se uvelike razlikuje od prethodno navedenih poslova sa pružanjem pristupa ograničenom dijelu podataka. Administrativne djelatnosti poput ureda zaštite na radu, tajništva, voditelji poslovanja, administracija nabave i prodaje imaju potencijal za redizajniranje trenutnog oblika poslovanja. Uz VPN tehnologiju i VoIP moguće je kompletnu uredsku infrastrukturu reducirati na nekoliko serverskih računala sa funkcijom vođenja i pohrane podataka u bazi. Infrastrukturni zahtjevi za takvu adaptaciju su upotreba adekvatne opreme i dobre internetske veze koja može opslužiti spajanje više djelatnika na računala poslodavca. Dobra internetska veza moguća je kroz trenutne poslovne internete koji omogućuju jednaku propusnost u oba smjera kretanja podatkovne komunikacije. Iako VPN tehnologija ne zahtjeva veliku internetsku brzinu potrebno je provjeriti kapacitet poduzeća dok za djelatnike osnovni kućni internet je dovoljan (brzine od 5 Mbs mogu biti dovoljne uz manje smetnje kroz rad). Konkretan primjer za potencijalnu adaptaciju postoji u pozivnim centrima koji zapošljavaju veći broj djelatnika za rad u jednom uredskom prostoru. Zaposlenici tokom

rada raspolažu sa osjetljivim podatcim poduzeća (poput izračun cijena usluga, kupci, baza podataka za operativni rad,...) ali i direktno predstavljaju svog poslodavca u komunikaciji sa potencijalnim ili postojećim kupcima. Svi ti ugrozi usporavaju prijelaz poslovanja na rad od kuće ali kontinuirano prilagođavanje tržišta zahtjevima radne snage i manjih troškova usmjeravaju poslovanje prema konceptu rada od kuće. Rad od kuće je u 2020. godini najzastupljeniji oblik poslovanja zbog iznenadne pandemije te se može očekivati da će zbog ovakvog skoka tržište razvijati nove metodologije i alate kako bi takav poslovni proces bio održiv i u budućnosti.

4. Sigurnosni aspekti virtualne mobilnosti

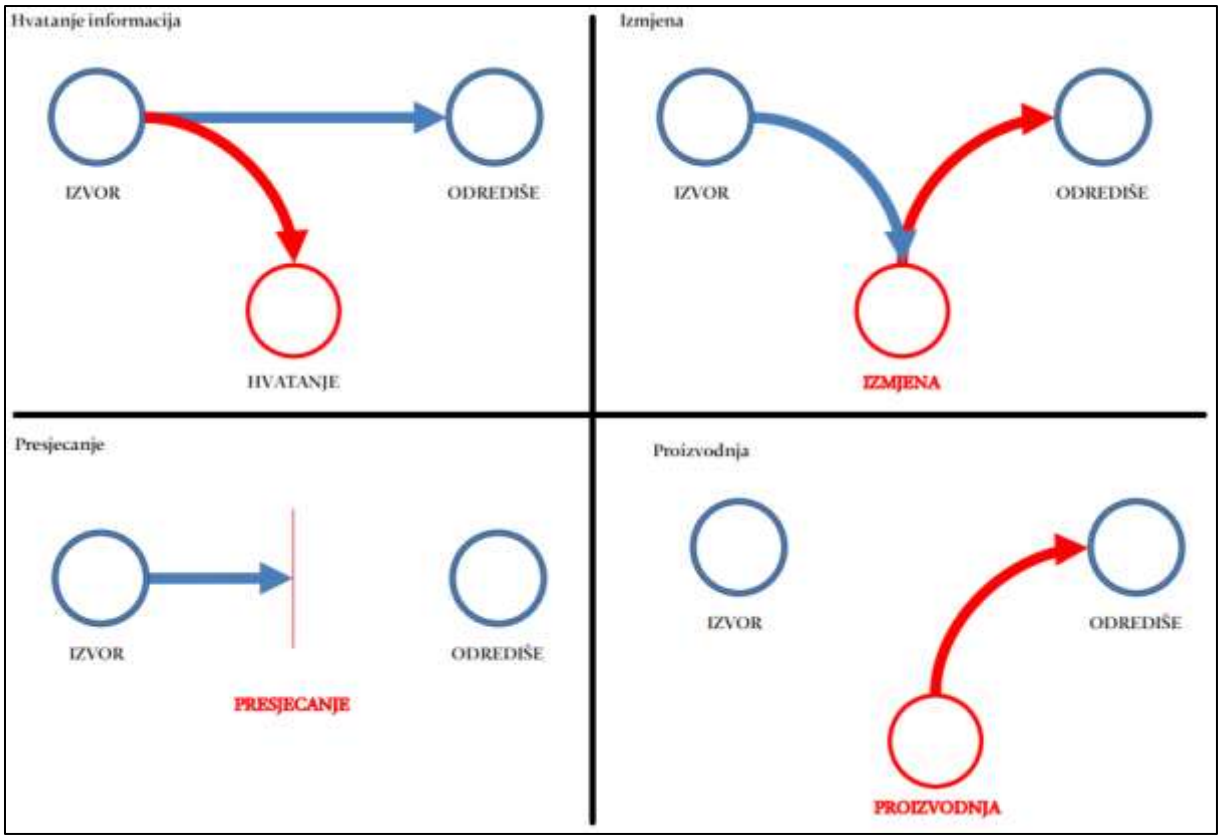
Virtualna mobilnost dolazi uz određenu cijenu, u ovom radu to je cijena zaštičenosti poslovanja od potencijalnih negativnih utjecaja. Računalni sustavi sami po sebi imaju određene ranjivosti koje kategoriziramo na:

1. Fizičke ranjivosti (radni prostor i okruženje)
2. Prirodne ranjivosti (elementarne nepogode)
3. Strojne i programske ranjivosti
4. Ranjivost medija
5. Nesavršenost strojne podrške
6. Komunikacijska ranjivost (mreža)
7. Ranjivost osoblja (djelatnici ili vanjski dobavljači sa mogućnošću pristupa sustavima)

Ranjivost računalnog sustava potrebno je kontinuirano evaluirati kako bi se pokušao reducirati negativan utjecaj na poslovanje. Uz samu kategorizaciju ranjivosti prepoznajemo i prijetnje računalnim sustavima poput prirodne pojave, namjerno djelovanje čovjeka, slučajno djelovanje čovjeka, tehničke prijetnje, organizacijske prijetnje.

Svaki računalni odnosno mrežni sustavi su potencijalno izloženi napadima koji mogu namjerno ili nenamjerno utjecati na funkcionalnost sustava ili povjerljivost podataka. Napadi se često povezuju sa visoko tehnološkim aktivnostima poput virusa ili presretanja i dešifriranja veze između dva računala dok u stvarnosti ti napadi su najčešće povezani sa ljudskim elementom i infrastrukturnim manama.

Napade na mrežu u obliku MITM (*man-in-the-middle*) dijelimo na hvatanje, presijecanje, izmjena i proizvodnja (slika 11). Hvatnje je napad sa ciljem uvida u podatke koji idu iz izvora prema odredištu, presijecanje je prekid toka komunikacije iz izvora prema odredišta. Izmjena je prekid komunikacije između izvora i odredišta tako da se podatci iz izvora promjene i šalju prema odredištu. Proizvodnja je slanje podataka predstavljajući se kao provjereni izvor unutar komunikacijske mreže.

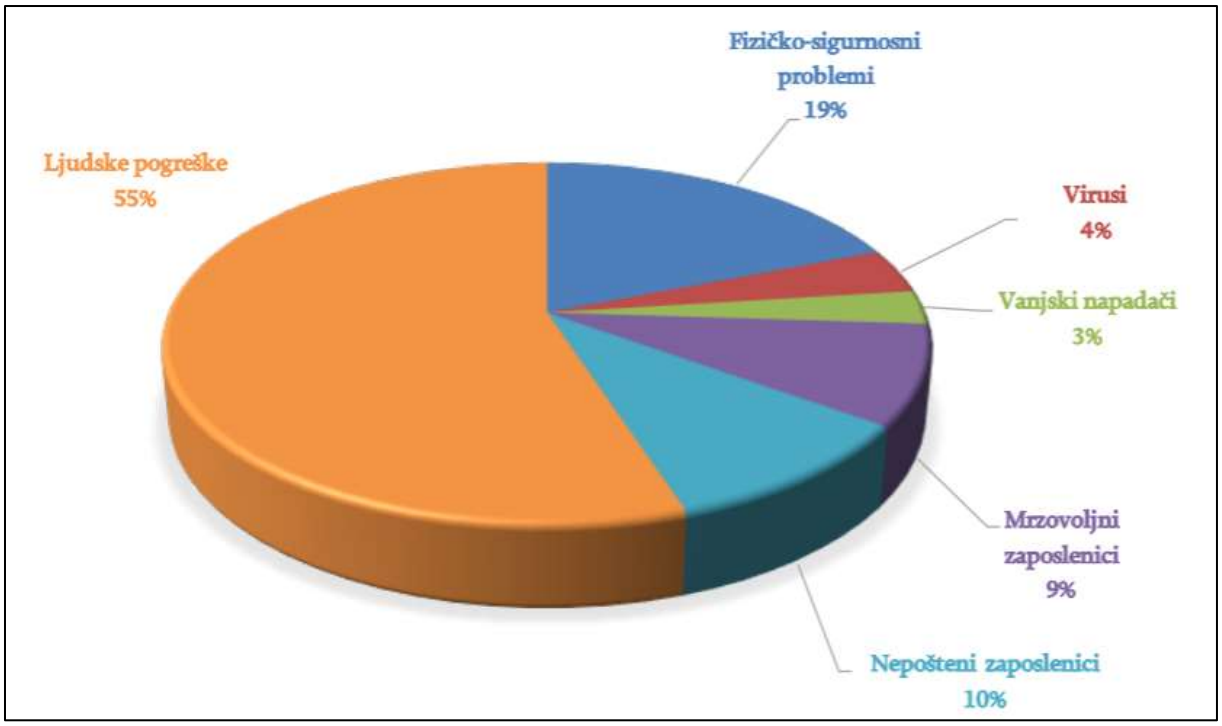


Slika 11: Tipovi MITM napada

Izvor: https://moodle.srce.hr/2019-2020/pluginfile.php/2955085/mod_resource/content/7/RS_003%20Racunalna%20sigurnost%20i%20prijetnje.pdf/ 15.04.2020.

Napad na računalni sustav poput MITM mogu biti generirani prema volji počinitelja (slučajni, namjerni), učinku (aktivni, pasivni), mjestu napada (unutarnji, vanjski), cilju napada, metodi napada.

Ljudski faktor je najutjecajnija komponeta za sigurnost računalnih sustava. U prilog toj tvrdnji idu statistički podatci prikazani na slici 12 koji ukazuju da napadati poput MITM i računalni virusi obuhvaćaju tek 7% ukupnih napada na sustav. Najveći dio počinitelja odnosi se na ljudske greške sa čak 55% i dodatnih 19% na zaposlenike sa namjerom nanošenja štete sustavu. Ostalih 19% su projektirane greške tokom dizajniranja sigurnosnog sustava (previdi u dizajnu, nedovoljno prostora za širenje, nove tehnologije sa novim uvjetima održavanja,...).



Slika 12: Statistika udjela napada na računalni sustav po vrsti

Izvor: https://moodle.srce.hr/2019-2020/pluginfile.php/2955085/mod_resource/content/7/RS_003%20Racunalna%20sigurnost%20i%20prijetnje.pdf/ 15.04.2020.

Primjer pogreške u dizajnu je slučaj Hrvatske kontrole zračne plovidbe (HKZP) čiji su se serveri za radarski sustav nalazili u podrumu. U početnoj prilagodbi prostora serverska prostorija bila je smještena u podrum zbog lakšeg održavanja temperature na konstantnoj razini. 30. srpnja. 2014. pojavila se ogromna količina padalina koja je probila montažnu branu i poplavila zgradu HKZP-a i sve što se nalazilo u nižim djelovima zgrade poput serverske sobe. U roku nekoliko minuta od proboja vode došlo je do ručnog gašenja sustava kako bi se izbjegla ogromna novčana šteta na opremi potrebnoj za radarski sustav oblasne kontrole zračnog prostora. U trenutku gašenja sustava oblasne kontrole HKZP-a imao je 49 aviona pod svojom kontrolom koji više nisu imali kontakt sa kontrolom leta i kretali su se nekontrolirano zračnim prostorom. Djelatnici HKZP-a su brzom reakcijom kontaktirali susjedne kontrole leta kako bi preuzeli kontrolu Hrvatskog zračnog prostora. U ovom slučaju su postojali rezervni sustavi ali zbog needuciranosti operativaca i nedovoljno jasnog pravilnika o postupanju u ovakvim situacijama došlo je do greške koja je rezultirala kompletnim gašenjem sustava. Štete u ovom slučaju prelazi u ogromne cifre zbog ispada sustava i naknadne odštete koju su tražili tadašnji

kontrolori. Najveća šteta bila je učinjena za ugled ovom poduzeću. Djelomičan prikaz štete u zgradi oblasne kontrole zračnog prostora vidljiv je na slici 13. Sve ovo bi bilo izbjegnuto da se u samom dizajniranju predvidio scenarij poplave ili da su se provodile adekvatne edukacije tehničkog osoblja o pravilima postupanja vezanih za ovaj konkretni slučaj.

Slika 13: Poplava u prostorijama HKZP-a

Izvor: https://www.jutarnji.hr/vijesti/hrvatska/foto-jutarnji-u-posjedu-izvjestaja-o-poplavi-zgrade-hrvatske-kontrole-zracne-plovidbe-dan-kad-je-nestala-kontrola-leta-iznad-hrvatske/398893/ 25.04.2020.

Kako bi se spriječio prethodni scenarij potrebno je prvo napraviti kvalitetnu analizu sigurnosnih ugroza. Početak procjene ugroženosti bilo kojeg sustava zapčinje izradom analize osjetljivosti sustava.

Primjenom analize osjetljivosti postavljamo pitanja:

1. Kakve će informacije odnosno podatke obrađivati sustav (odnosno djelatnik)?
2. Kakve mogu biti posljedice uslijed sigurnosnih propusta?
3. Koji zakonski akti definiraju aspekt sigurnosti?
4. Kakve su sigurnosne karakteristike korisnika?
5. Koji su interni sigurnosni akti?

Popunjavanjem analize osjetljivosti imamo grupu predodžbu o izloženosti sustava uvođenjem novog poslovnog procesa ili tehnologije rada. Nakon osnovne analize slijedi procjena rizika sa tri nova pitanja (U ovom slučaju to je rad od kuće u *call centru*):

1. Što želimo zaštititi?
   - Podatke o kupcima i poslovanju

2. Što nam je potrebno da se zaštitimo?
   – Onemogućiti kopiranje ili snimanje podataka

3. Koliko vremena, truda i novaca moramo uložiti kako bismo postigli adekvatnu zaštitu?

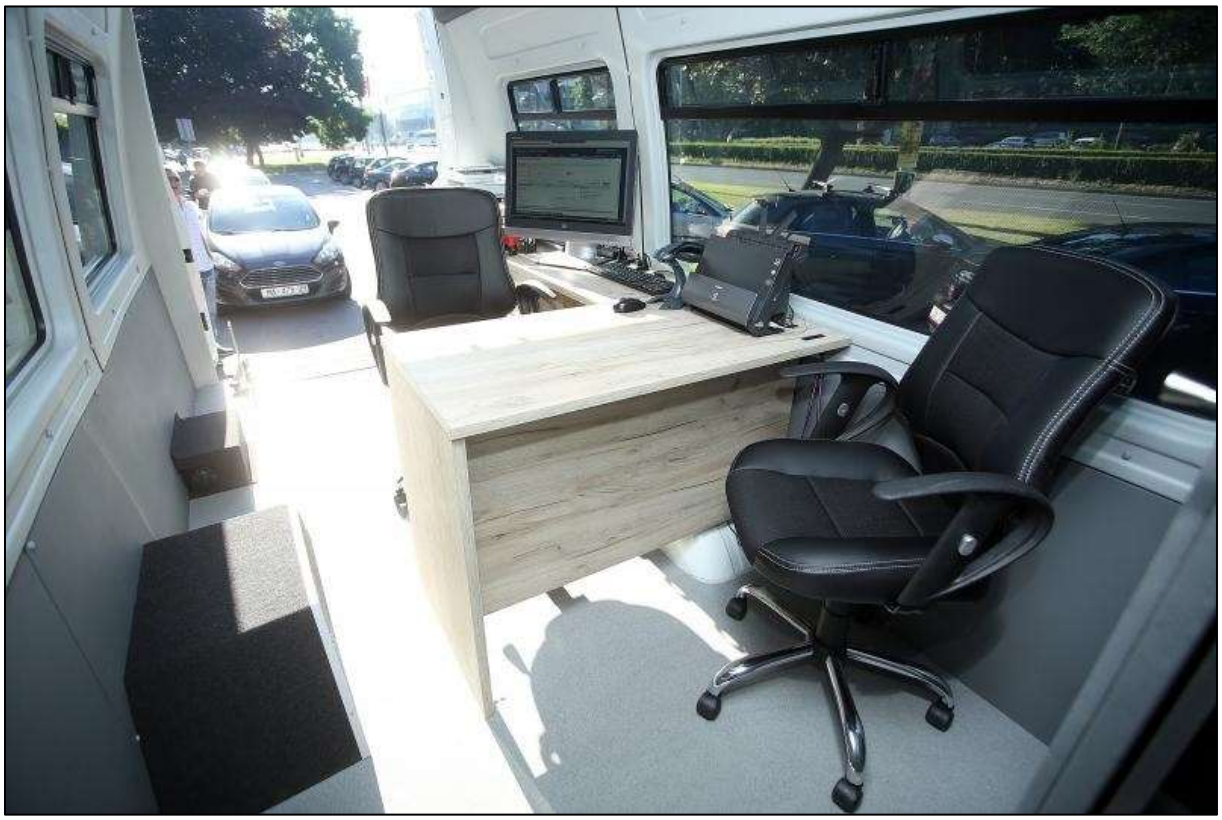
Zadnje pitanje u procjeni rizika traži dodatno dizajniranje potencijalnih rješenja. Kako bi se prva dva uvjeta zadovoljila rješenje rada od kuće mora omogućiti identične uvjete zaštite podataka kao i rad u uredu. Dva rješenja imaju potencijalnu implementaciju prvi je mobilna uredska jedinica u obliku adekvatno opremljenog vozila, a drugi je adaptacija djelatnikovog stambenog prostora pružajući poslodavcu kontrolu nad potencijalnim prijetnjama.

Nakon detaljne analize novih rješenja potrebno je ponoviti proces procjene rizika. Uz inicijalnu procjenu sa donesenom odlukom o smjeru poslovanja potrebno je periodično ponoviti procjenu rizika kako bi ona bila u skladu sa promjenama koje se pojavljuju tokom razvoja tržišta i poslovnih procesa. Kada procjena rizika bude kompletna potrebno je napraviti oblik edukacije djelatnika sa novim poslovnim procedurama. Uz edukaciju je vezana i popratna dokumentacija o pravilniku rada. Ova dva dokumenta su nužna kako bi se definirani utjecaj ugroza sa procjene rizika pokušali minimizirati na prihvatljivi rizik. Uz svaku novu verziju procjene rizika treba napraviti reviziju edukacije i pravilnika rada te donijeti zaključak o eventualnoj potrebi za izradom nove verzije dokumentacije.

Poželjno je pručiti i kakvo je iskustvo tržišta te ukoliko postoji mogućnosti napraviti usporedbu sa vlastitim rješenjima. U ovom slučaju treba promatrati sigurnosne propuste u povjerljivosti podataka tokom VPN povezanosti. Na tržištu VPN servisa ima jako puno primjera o servisima koji su bili napadnuti i njihovi korisnici su bili izloženi napadu. NordVPN je jedna od kompanija koja je zakazala u zaštiti svojih korisnika tako da je *eng. Data Centar* u Finskoj bio mjesec dana pod MITM napadom. Navedene lokacije nisu bile u vlasništvu NordVPN nego se radilo o poddobavljaču sa pružanjem infrastrukture za *eng. Cloud hosting*. VPN servisi su često bili izlagani malicioznim napadima zbog stalne utrke sa pružanjem usluge sa što većom pokrivenosti i što nižom cijenom. Algoritmi koji se koriste u protokolima su isto tako više puta bili probijeni. Jedan od primjera je izrada EFF DES *cracker* (*Electronic Frontier Fundation DES*) računala. EFF DES izgrađen je 1998. u svrhu dokazivanja mogućnosti probijanja DES zaštite što je i uspio unutar jednog dana.

5. Mobilne uredske jedinice

Kao što je u prethodnoj cjelini navedeno potencijalno rješenje ovog problema postoji u upotrebi adekvatnih vozila sa adekvatnom opremljenošću. Vozila ovakve namjene postoje danas na tržištu. Jedan od primjera je i Zagrebački holding sa pokretnim uredom prikazanog na slici 14.



Slika 14: Pokretni ured Zagrebačkog Holdinga

Izvor: https://www.rtl.hr/vijesti-hr/foto/2634829/uskoro-cete-holdingove-racune-moci-placati-ispred-vrata-bandic-predstavio-pokretni-ured/?slika=1318143/ 23.04.2020.

Uz sigurnu virtualnu privatnu mrežu ovakve pokretne jedinice omogućuju nadzor uz dodavanja opcija trenutnog gašenja sustava udaljenog pristupa ukoliko se uoći neadekvatno korištenje sustava. U autoindustriji proizvođač Nissan je 2016. predstavio električni mobilni ured (slika 15) sa ciljem da manji poslovni subjekti mogu priuštiti poslovanje u užem gradskom centru koji ima visoke cijene najma. Udobnost u ovakvim uredima je upitna ali koncept zadovoljava potencijal za pružanje više razine sigurnosti u poslovnim procesima rada od kuće.

Slika 15: Uredski prostor Nissan e-NV200 WORKSPACe

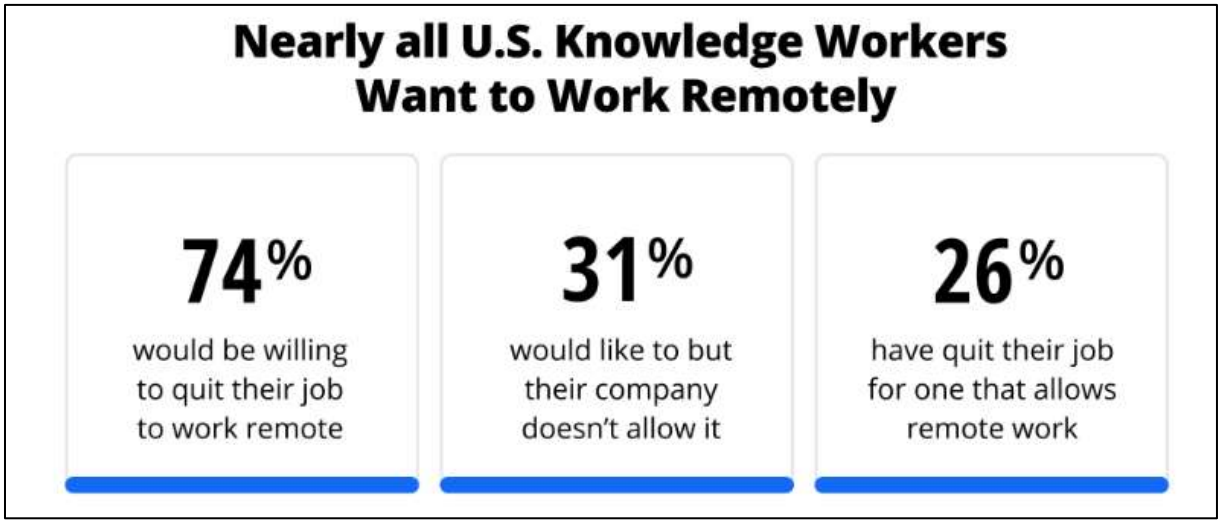
Izvor: https://www.parkers.co.uk/vans-pickups/news/2016/nissan-e-nv200-workspace-concept-driven/ 23.04.2020.

Drugo rješenje je pretvaranje privatnog stambenog prostora djelatnika u privremeni ured. Za realizaciju ovakvog rješenja zaposleniku treba biti omogućena montažna pregrada uz prijenos video zapisa rada u svrhu nadzora potencijalnog kopiranja ili zloupotrebe podataka. Oba principa rada moraju imati posebne pravilnike i procedure rada kako bi zaposlenik bio u potpunosti upoznat sa pravilom ovakvog rada.

Uvjet za ovakve oblike rada je spremnost djelatnika na posebne uvjete rada kao što su kontinuirani nadzor tokom rada i restriktivne mjere tokom rada koje sprječavaju potencijalno ugrožavanje povjerljivosti osjetljivih podataka.

6. Analiza troškova i koristi rada od kuće

Prethodna procjena rizika omogućuje izradu analize troškova i koristi rada od kuće kako bi se stvorila brojčana vrijednost koja može ali i ne mora nužno biti financijski isplativa. Ovake promjene radne okoline mogu pozitivno utjecati na zadovoljstvo djelatnika koji u tradicionalnim okruženjima nemaju priliku rada od kuće. Istraživanje provedeno nad Američkom populacijom na slici 16 prikazuje da se rad od kuće nameće kao poželjna beneficija tokom zapošljavanja.



Slika 16: Važnost rada od kuće za tržište rada u SAD

Izvor: https://zapier.com/blog/remote-work-report-by-zapier/ 23.04.2020.

U brojkama promatramo scenarije mobilne uredske jedinice i scenarija klasičnog koncepta rada od kuće za grad Zagreb. Mobilna uredska jedinica generira trošak vozila koji teško može opravdati ovakvo ulaganje iako nudi dobru razinu sigurnosti s obzirom na mogućnost potpune kontrole pri dizajniranju radnog prostora. Problem mobilnih jedinica se također krije i u manjku iskustva upravljanja sa većim vozilom koji se očekuje od djelatnika u trenutku preuzimanja vozila, postoje troškovi parkiranja, fiksni troškovi registracije, osiguranja, goriva. Svoju primjenu ovakva vozila imaju u gusto naseljenom području gdje su cijene prostora za najam izrazito visoke. Također postoji i primjena kod poslova čiji trošak u slučaju proboja u sigurnosni sustav generira izrazito visoke gubitke koji opravdavaju ovakav oblik ulaganja u slučaju prisilne potrebe za radom kod kuće kao što je to bilo u slučaju sa pandemijom COVID-19.

Praktičniji princip je rada od kuće i adaptacija stambenog prostora zaposlenika za potrebe poslovanja. Pretpostavka je da djelatnik tokom sklapanja ugovora o radu pristaje na ustupanje vlastitog stambenog prostora u svrhu obavljanja rada od kuće. Takve adaptacije moraju biti montažnog oblika kako bi se u što kraćem periodu prostor zaposlenika vratio u stanje izvan radnih sati. Trošak kod ovakvih konfiguracija se reducira na nekolicinu prijenosnih montažnih panela, nadzorni sustav i VPN povezivanje.

U izračunu slijedeće analize su korišteni podatci za najpovoljniji izbor nabave potrebne opreme i najma prostora. VPN vatrozid netgate XG-7100 1U sa cijenom od 999,00 USD (6.943,05 HRK, po srednjem tečaju HNB od 6,95 HRK za 14. svibnja) je najoptimalniji omjer kvalitete i cijene. Iz izračuna je izuzet trošak tehničkog osoblja koji mora izvršiti konfiguraciju VPN-a te trošak djelatnika koji vrše nadzor rada od kuće.

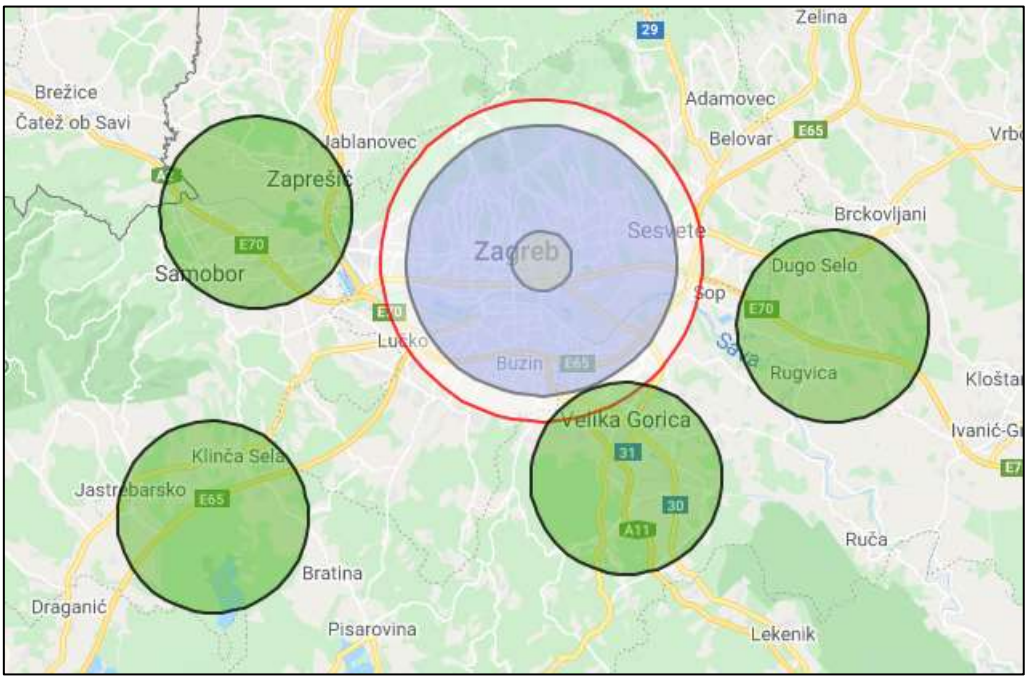
Troškovi za montažni ured od $2m^2$ raspisani po stavkama su: 2x pregrade sa ukupnom cijenom od 3.000,00 kn, nadzorni sustav (kamera sa mikrofonom) 300,00 kn, VPN veza 6.943,05 kn što je ukupni jednokratni trošak od 10.243,05 kn sa amortizacijom troškova u periodu 2 godine koji je garantni rok opreme koja se koristi za ovu analizu. Kada se taj trošak podijeli sa 24 mjeseca dobijemo izračun od 426,80 kn mjesečno. Sustav nadzora je potrebno kontinuirano pratiti što se može dodijeliti jednom od zaposlenika da prati eventualna kršenja pravila poput izrade zapisa, izgovora osjetljivih podataka ili bilo kakav drugi postupak koji može rezultirati prijenosom podataka sa mrežnog sustava poduzeća. Potencijalno rješenje djelatnika za nadzor je zaduženje djelatnika koji se nalaze u uredu poduzeća da uz svoj dnevni rad na dodatnom monitoru imaju pregled rada djelatnika koji radi od kuće. Nadzorni sustav mora biti detaljno preciziran kako bi se onemogućile malverzacije sa sustavom. Prikaz adaptacije stambenog prostora u montažni ured prikazan je na slici 17.

Slika 17: Montažni ured za rad od kuće

Izvor: Izradio autor 25.04.2020.

Usporedno sa prethodnim prikazom troškova implementacije montažnog ureda, troškovi tradicionalnog principa rada su svedeni na putni trošak. Praksa na tržištu rada je da se iznosi potrebne mjesečne karte za javni prijevoz i 1,00 kn/km za dolazak do stanice javnog prijevoza računaju kao putni troškovi na koje djelatnik ima pravo. Putni trošak se često obračunava ukoliko je djelatnikovo mjesto boravišta udaljeno više od 2 kilometara. Poslodavac najčešće isplačuje putne troškove u vrijednosti najekonomičnijeg troška putovanja. Na slici 18 prikazana je grafička analiza putnih troškova vezanih za ured na adresi Heinzelova ulica 60, Zagreb. Prvo je potrebno postaviti koji od dva oblika naknade je prihvatljiv. Za ovaj izračun su korišteni podatci o mjesečnim kartama ZET-a sa troškovnikom: zone 1 – 360,00 kn, zona 2 – 610,00 kn. Računajući mjesečnu naknadu za zonu 1 od 360,00 kn dijeljenjem sa 20 (broj radnih dana u mjesecu) pa ponavljanjem radnje dijeljenja sa 2 (dva smjera kretanja) dobijemo 9,00 kn što prikazuje visinu dnevne naknade za kretanje u jednom smjeru. Najmanja kružnica od 2 kilometra označava područje koje nije pokriveno obaveznom naknadom o putnom trošku. Plava kružnica označava područje gdje je najekonomičnija opcija plaćanja troškova korištenje vlastitog automobila (≤9 km). Zelena kružnice označavaju područja gdje je financijski isplativije implementirati rad od kuće s obzirom na mjesečni trošak od 426,80 kn. Iz kružnice na području Velike Gorica se isključuje prostor označen sa kružnicom crvene granice gdje je osobnim vozilom isplativije u odnosu na trošak montažnog ureda. Kružnica sa crvenim obrubom predstavlja prostor od 10.7 kilometara koji je prikaz *break even* točke između osobnog

vozila i montažnog ureda. Za izračun kružnice sa crvenim obrubom korišten je iznos mjesečnog troška montažnog ureda podijeljen sa 20 radnih dana te podijeljen sa količinom smjera kretanja odnosno 2 (426,80/20/2=10,7). Prostor između zelenih kružnica i plave kružnice označava zone sa isplativijim troškom javnog prometa u obliku mjesečne karte od 360,00 kn.

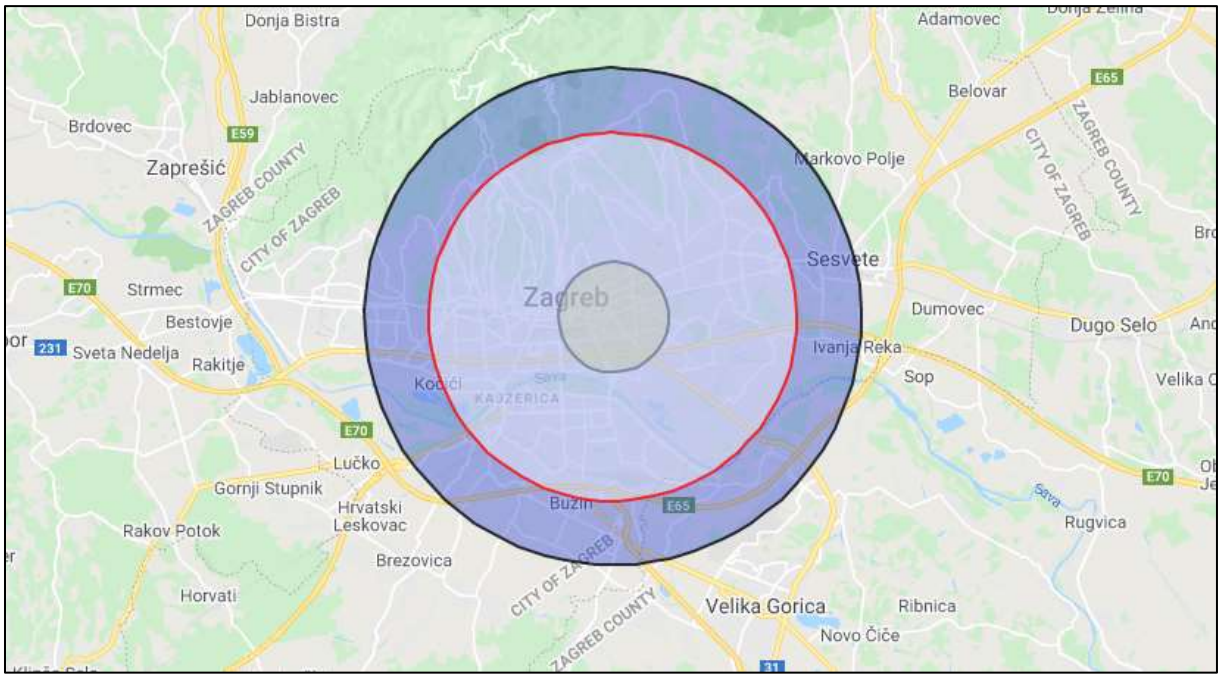


Slika 18: Karta putnih troškova za lokaciju Heinzlova 60

Izvor: Izradio autor 25.04.2020.

Ukoliko kod računanja troška uvedemo koncept rasporeda gdje je montažni ured uvijek iskorišten bar jednim djelatnikom onda troškove putovanja možemo staviti u visini mjesečne naknade za jednog djaltnika od 80,00 kn do 426,80 kn u slučaju vlastitog vozila, 360,00 kn 1. zona, 610,00 kn 2. zona . U takvom konceptu možemo reducirati troškove uredske opreme za jedno radno mjesto: stol 300,00 kn, stolica 150,00 kn, mjesečni najam minimalnih $2m^2$ uredskog prostora 160,00 kn. Dodatni troškovi su vezani za održavanje i čišćenje. Tokom izračuna isplativosti treba računati na prethodno navedene podatke koji ukazuju na poželjnost rada od kuće kao dio radnog mjesta kao dodatni kapital tokom sklapanja ugovora sa zaposlenikom. Potencijalni zaposlenici uz rad od kuće mogu izbaciti vremenski trošak putovanja vezan za odlazak na posao te posvetiti dio radnog vremena za vlastite obaveze u kućanstvu. Nastavno dio troška tradicionalnog ureda vezan je za računalnu opremu koja se također može reducirati uporabom servera za dijeljenje dokumentacije (trošak radnog računala

je 1.500,00 kn). Ukupan zbroj svih prethodnih stavki je 1.950,00 kn početnih troškova i od 240,00 kn do 770,00 kn mjesečnih ovisno o mjestu boravišta djelatnika.



Slika 19: Izračuna putnih troškova za lokaciju Heinzlova 60 sa svim parametrima

Izvor: Izradio autor 30.06.2020.

Zbog mjesečnog najma inicijalna grafička analiza se korigira u korist montažnih ureda te se područje isplativosti može vidjeti na slici 19 prikazano sa smanjenom crvenom kružnicom koja označava *break even* za implementaciju rada od kuće. Nova kružnica je korigirana izračunom inicijalnih mjesečnih troškova opreme za montažni ured umanjen za mjesečni trošak najma uredskog prostora nakon čega je izračunata vrijednost podijeljena sa 20 radnih dana i sa 2 smjera kretanja odnosno (426,80 – 160,00) / 20 / 2 = 6.67 km – polumjer crvene kružnice. U izračunu nove kružnice je izostavljen jednokratni trošak od 1.950,00 kn jer on ovisi o načinu implementacije sustava. Ukoliko se i taj fiksni dio troška oduzme od potrebnog ulaganja u opremu za montažni ured polumjer kruga se smanjuje na vrijednost (345,50 – 160,00) / 20 / 2 = 4,6 km.

8. Zaključak

Sigurnost virtualne mobilnosti se stalno prilagođava uvođenjem novih protkola i algoritama koji omogućuju novoj generaciji tehnologijE zaštičenost od trenutnih opasnosti. Sa razvojem računalne tehnologije i procesne moći omogućuje se proboj u sustave zaštite, ali isti ti tehnički napredci omogućuju uvođenje novih kompleksnijih enkripcija koje zadovoljavaju sigurnosne potrebe do slijedećeg novog tehnološkog razvoja. Cijeli taj tehnološki napredak zahtjeva stalno ulaganje u praćenje tržišta virtualne mobilnosti. Raširenost tehnologije i zadovoljavajuća razina opće educiranosti radne snage omogućuju uvođenje VPN tehnologije u poslovne procese sa svrhom realizacije sigurnog rada od kuće. Rad od kuće prije pojave globalne pandemije nije bio nužan za poslodavce nego je to bila pogodnost koju je tržište rada koncipiralo kao dodatak u okviru svog ugovora o radu. Današnje poslovanje je prisiljeno razmišljati više o radu od kuće zbog razarajućeg utjecaja pandemije 2020. godine na gospodarstvo ali i sve buduće potencijalne pandemije. Poslovni subjekti prisiljeni su više razmišljati o prilagodbi za rad od kuće kako bi drugi put bili spremniji odgovoriti na uvjete rada koji su nametnuti kod ovakvih oblika tržišnih promjena.

Kao što je i prikazano rad od kuće je ekonomičan i bez scenarija pandemije. Ekonomičnost definira oblik modela koji se uvodi u poslovni proces i ciljevi poslodavca koji može prividno gubiti novac sa ovakvim poslovanjem ali može biti poželjniji na tržištu rada koje je prije same pandemije bilo potkapacitirano.

Ukoliko poduzetništvo ignorira tehnološke napretke i ne ulaže u prilagodbu sigurno će se dogoditi trenutak kada će cijenom odstupati od konkurencije. Jako puno primjera postoji vezanih za tromost adaptacije tradicionalnog poslovanja sa tehnološkim rastom. *Eng. Low-cost* aviokompanije su jedan od primjera koji idu u prilog ovoj tvrdnji. Tradicionalne kompanije nisu bile spremne uvoditi u svoje poslovne procese izbacivanje nepotrebnih poslovnih procesa poput fizičkog izdavanja karata i *check in* procedure. Tehnološki napredak omogućuje uklanjanje tih *eng. junk* poslovnih procesa. Prepoznavanjem razvoja tržišta tehnologije omogućuje adaptaciju poslovanja koje mogu rezultirati tržišnim promjenama poput pojave da jedna od najvećih aviokompanija postane Rayan Air. Rayan Air i sve druge *Low-cost* kompanije sa svojim cijenama ruše isplativost tradicionalnog poslovanja aviokompanija. To je samo jedan od primjera u kojem tržište kontinuirano traži komfort i manju cijenu tokom korištenja usluge ili proizvoda. Potrebno je sve više razvijati gospodarstvo u smjeru implentacije rada od kuće

kao sastavni dio poslovanja kako bi to isto gospodarstvo obuhvatio nova tržišta ali i zaštitio postojeće poslovanje.

POPIS LITERATURE

1. Building and Managing Virtual Private Network, Kosuir D., Wiley Computer Publishing, John Wiley & Sons, inc., New York, 1998.
2. Opravdanost primjene IPsec i SSL/TLS tehnologija u kartičnom poslovanju, Nemanić A., Visoko učilište Algebra, Zagreb, 2016.
3. Sigurnost u virtualnim privatnim mrežama, Hofman D., Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb, 2005.
4. Secure PIX ans Secure VPN Study Guide, Edwards, W., Lancaster, T., Quinn, E., Rohm, J., Tow, G., John Wiley & Sons, inc., San Francisco, 2006.
5. Practical Unix & Internet Security, 3rd Edition, Garfinkel, S., Schwartz, A., Spafford, G., O´Reilly & Associates Inc., Sebastopol, 2003.
6. Autorizirana predavanja iz kolegija Računalna sigurnost, Škorput, P., Fakultet prometnih znanosti, Zagreb 2015.
7. Ćulumović, D., Žigman, D., Mamuzić, I.:Spajanje dviju kompanija u VPN, Polytechnic & Design, Tehničko veleučilište u Zagrebu, Vol. 4 (8), Zagreb, 2016.
8. Combaj, G., Pongrac, D., Žigman, D.: GETVPN enkripcija, Polytechnic & Design, Tehničko veleučilište u Zagrebu, Vol. 3 (2), Zagreb, 2015.
9. Specification of Internet Transmission Control Program, Cerf, V., Dalal, Y., Sunshine, C., Network Working Group, 1974.
10. The swIPe IP Security Protocol, Ioannidis, J., Blaze, M., Internet Engineering Taska Force, 1993.
11. GeeksforGeeks (dostupno s URL: www.geeksforgeeks, travanj 2020)
12. Perimeter81 (dostupno s URL: www.perimeter81, travanj 2020)
13. howstuffworks (dostupno s URL: www.computer.howstuffworks, travanj 2020)
14. Le-VPN (dostupno s URL: www.computer.le-vpn, travanj 2020)
15. History-computer (dostupno s URL: www.history-computer, travanj 2020)
16. Pirtunl (dostupno s URL: www.pirtunl, travanj 2020)
17. Global Market Insights (dostupno s URL: www.gminsights, travanj 2020)
18. Cisco (dostupno s URL: www.cisco, travanj 2020)
19. MarketWatch (dostupno s URL: www.marketwatch, travanj 2020)
20. Parkers (dostupno s URL: www.parkers, travanj 2020)

21. Zapier (dostupno s URL: www.zapier, travanj 2020)
22. SSL2BUY (dostupno s URL: www.ssl2buy, travanj 2020)

POPIS SLIKA

POPIS KRATICA

VPN (Virtual Private Network) virtualna privatna mreža

ARPANET (The Advanced Research Projects Agency Network) projektna agencija za napredno istraživanje mreža

TCP/IP (Transsmition Control Protocol / Internet Protocol) prijenosni kontrolni protokol / internetski protokol

OSI model (Open Systems Interconnection model) model otvorenih sustava međupovezanosti

SwIPe (Software IP Encryption Protocol) program protokola IP enkripcijske

IPsec (*Internet Protocol Security*) sigurnosni internetski protokol

PPTP (*peer-to-peer tunneling protocol*) protokol tuneliranja od točke do točke

P2P (*Point-to-Point*) protokol od točke do točke

VoIP – (*Voice over IP*) glas putem IP-a

NAS (*network access server*) mrežni pristupni server

WAM (*Wide Area Networ*) mreže širokog područja

VPDN (V*irtual Private Dailup Network*) virtualna privatna pozivna mreža

CA (*Certification Authority*) certifikacijska tijela

DES (*Data Encryption Standard*) standard enkripcije podataka

3DES (*Triple DES*) trostruki DES

AES (*Advanced Encryption Standard*) napredni enkripcijski standard

RSA (*Rivest-Shamir-Adleman*) Rivest-Shamir-Adleman

ECC (*Elliptic Curve Cryptography*) kriptografija eliptične krivulje

SSL (*Secure Sockets Layer*) protokol osiguranja paketa slojeva

TLS (*Transport Layer Security*) protokol osiguranja transportnog sloja

IKE (*Internet Key Exchange*) Internetska razmjena ključeva

IKEv2 (*IKE version 2*) IKE verzija 2

MPLS (*Mulitiprotocol Label Switching*) više-protokolarna razmjena oznaka

MITM (*man-in-the-middle*) računalni napad čovjek u sredini

Mbps (*Megabit per second*) Megabit po sekundi

Gbps (*Gigabit per second*) Gigabit po sekundi

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj diplomski rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu diplomskog rada pod naslovom **Sigurnosni aspekt virtualne mobilnosti**

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

U Zagrebu, 7.7.2020

Student:

(potpis)