VŠPV
VISOKA ŠOLA ZA POSLOVNE VEDE

dr. Julija Lapuh Bele

INFORMACIJSKA VARNOST

Učbenik: Informacijska varnost
Gradivo za predmet: Informacijska varnost

Avtor:
dr. Julija Lapuh Bele
VISOKA ŠOLA ZA POSLOVNE VEDE

Izdajatelj in založnik: Visoka šola za poslovne vede

Ljubljana, 2021

KAZALO VSEBINE

KAZALO SLIK

1 UVOD

Informacijske varnosti je veda, ki se ukvarja z zaščito podatkov. To posledično pomeni zaščito ugleda, preprečitev zastojev pri delu in finančnih izgub organizacije.

V zvezi z izrazom informacijska varnost marsikdo pomisli na kibernetski kriminal, ki je ena najpomembnejših groženj informacijske družbe, a ne edina skrb, s katero se ukvarjajo strokovnjaki za informacijsko varnost.

V gradivu bomo spoznali:

- pomen digitalnih podatkov in njihove zaščite,
- varnostne zahteve za podatke in celoten informacijski sistem,
- kako ščitimo računalniški sistem pred napakami in zlorabami v lokalnem omrežju,
- škodljivo kodo in druge oblike kibernetskega napada,
- kako s tehničnimi sredstvi zaščitimo računalniški sistem pred napadi iz internetnega omrežja,
- da smo osveščeni uporabniki pomemben dejavnik informacijske varnosti in
- kaj vse moramo vedeti in upoštevati za varno elektronsko poslovanje.

Podatke varujemo pred namernim ali nenamernim povzročanjem škode:

- pred napakami uporabnikov ali IKT opreme in
- da preprečimo nepotrebne nevšečnosti in kazniva dejanja.

Napak ne moremo preprečiti. Lahko pa izvajamo ukrepe, ki omogočajo čim hitrejšo vzpostavitev normalnega stanja in čim manj zastojev pri delu. Za razliko od napak, bi goljufije in druge zlorabe v večini primerov lahko preprečili. Izkazuje se, da so za večino uspešno izvedenih dejanj kibernetskega kriminala krive žrtve same – se pravi ljudje (Europol, 2020). Vendar je nevarnosti treba poznati, da bi se pred njimi lahko ubranili. Čeprav jih največ preti preko interneta, se zlorabe dogajajo tudi znotraj lokalnih omrežij. Ranljive so tudi pametne naprave, npr. pametni telefoni.

V tem gradivu bomo spoznali, kaj vse je v računalniškem sistemu potrebno varovati ter kakšno vlogo imajo pri tem računalniški strokovnjaki in uporabniki.

Če se nam pokvari trdi disk in nimamo varnostne kopije podatkov, bodo le-ti morda za vedno izgubljeni. S tem pa naše slike, dokumenti in drugo. Če bomo malomarno ravnali z osebnimi podatki oz. ne bomo poskrbeli za varno uporabo interneta, nam bodo morda zlorabili kreditno kartico, ukradli identiteto, denar z računa, objavili za javnost neprimerne slike ...

Da zaščitimo podatke, moramo varovati celotne računalniške sisteme in osvestiti ljudi za samozaščitno delovanje. Ne smemo dopustiti, da zlonamernež izrabi kakšno ranljivost, zaradi katere smo lahko oškodovani.

Varovanje podatkov zajema različna področja:

- nekatere podatke je potrebno varovati po zakonu (npr. osebne in tajne podatke),

- nekatere podatke je potrebno varovati, ker predstavljajo poslovno skrivnost ali intelektualno lastnino,
- vse podatke je potrebno varovati za primer napak strojne opreme ali uporabnikov,
- vse podatke je potrebno varovati za primer sovražnega delovanja, ki zajema tako namensko neposredno povzročanje škode (s strani konkretnega uporabnika ali kriminalne združbe) ali preko škodljivih programov.

Marsikatero podjetje od svojih partnerjev zahteva podpis pogodbe o varovanju poslovnih podatkov, kjer je navedena odškodninska odgovornost. Zato je smiselno, da lahko posamezni zaposleni dostopa le do podatkov, ki jih pri svojem delu potrebuje in da se zaveda, kako mora s temi podatki ravnati.

Pomembno je predvsem, da preprečimo zastoje v poslovanju, finančno škodo ali zmanjšanje ugleda, ki bi ga lahko povzročile napake ali zlorabe iz lokalnega omrežja ali iz interneta.

Strokovnjak, ki skrbi za informacijsko varnost (ang. ICT Security Specialist), opravlja eno ali več od naslednjih aktivnosti:

- načrtovanje, izvedba, nadgrajevanje in upravljanje varnostnih rešitev,
- krpanje varnostnih lukenj,
- detekcija in odziv na kibernetske napade in druge varnostne grožnje,
- odpravljanje posledic napadov,
- opravljanje varnostnih pregledov in testov,
- osveščanje uporabnikov.

2 ZAŠČITA DIGITALNIH PODATKOV

V lokalnem omrežju se lahko zgodijo zlorabe (npr. kazniva dejanja), še pogosteje pa napake zaposlenih ali strojne opreme. Še več nevarnosti preži od zunaj, preko omrežja internet.

Varovati je potrebno predvsem podatke. Varovanje podatkov se začne (a ne konča!) z varovanjem fizične opreme, kjer so podatki nameščeni ali preko katere se do njih dostopa.

Digitalni podatki so podatki v oblikah, ki omogočajo njihovo hrambo in obdelavo na računalniških sistemih. V današnjem času so praktično vsi podatki shranjeni na računalniških medijih. Vse pomembnejše starejše zapise so shranili na računalnike. Pravimo, da so jih digitalizirali. Stare knjige so npr. skenirane in shranjene v računalniških zapisih.

Kot bomo spoznali v nadaljevanju, podatke zaščitimo z:

- omejevanjem dostopa do podatkov in
- z varnostnim kopiranjem za primer zlorabe, izgube ali poškodbe podatkov.

2.1 VARNOSTNE ZAHTEVE

Podatki v podjetju so dragocen vir, ki ga moramo strogo nadzorovati in upravljati. Nekateri podatki so strateškega pomena za lastnika, zato moramo poskrbeti za njihovo pravilnost in popolnost, razpoložljivost (dostopnost) ter zaupnost.

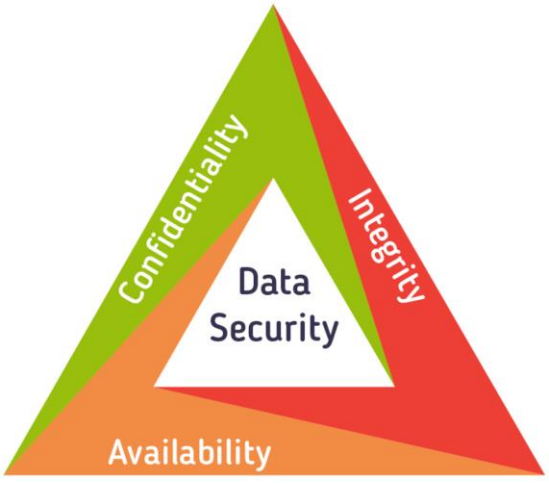
Operacijski sistemi, sistemi za uporabo podatkovnih zbirk in kakovostno napisani informacijski sistemi morajo imeti mehanizme za varovanje podatkov, ki omogočajo, da do njih dostopajo samo pooblaščene osebe. Nepooblaščenim osebam mora biti dostop onemogočen. Pooblaščene osebe morajo za vstop v sistem opraviti overjanje ali avtentikacijo. Postopek bomo pojasnili v nadaljevanju.

Na računalniških diskih imamo številne podatke, ki jih potrebujemo za bolj ali manj pogosto uporabo. Vendar pa se vsak računalniški disk lahko pokvari. V stavbi lahko pride do požara ali do kakšne druge nesreče, ki onesposobi računalniško opremo in s tem podatke.

Podatke zato shranjujemo še na druge spominske medije, npr. na diske, ki so izven lokacije, kjer imamo računalniški sistem in/ali pri ponudnikih hrambe podatkov na internetu.

Informacijska zaščita podatkov obsega izpolnjevanje naslednjih varnostnih zahtev:

- **razpoložljivost** oz. dostopnost (ang. availibity) – podatki in storitve morajo biti na voljo, ko jih potrebujemo,
- **zaupnost** (ang. confidentiality) – omejevanje dostopa do podatkov in storitev samo pooblaščenim osebam,
- **celovitost** (ang. integrity) – skrb za neokrnjenost podatkov in storitev,
- **preprečevanje zanikanja** (ang. nonrepudiation) – onemogočanje naknadnega zanikanja dejanja, npr. podpisa pogodbe, vsebine sporočila, izvršene komunikacije.



Slika 1: CIA trikotnik
(Devopedia, 2020)

Izjemno pomembna je trojka CIA: zaupnost (ang. confidentiality), celovitost (ang. integrity) in razpoložljivost (ang. availibity).

2.1.1 Razpoložljivost

Podatki morajo biti na voljo, ko jih potrebujemo. Tej lastnosti rečemo razpoložljivost ali dostopnost (ang. availability).

Veliki sistemi si ne morejo privoščiti, da bi bili brez dostopa do podatkov. To bi namreč zaustavilo večino njihovih poslovnih procesov.

Če pride do okvare in izgubimo podatke, za marsikatero organizacijo ni dovolj hitro, da jih prikličemo iz arhiva. Postopek lahko traja predolgo. Razen tega se izgubijo podatki, ki so nastali po arhiviranju.

Nenehna razpoložljivost oz. dostopnost podatkov se na splošno doseže z redundanco, ki vključuje aplikacije, shranjevanje in dostopanje do podatkov. Veliki sistemi imajo v pripravljenosti sistem, ki deluje vzporedno in takoj prevzame vlogo, če se »glavni« sistem iz kakršnega koli razloga ustavi.

Vendar pa podatki ne smejo biti razpoložljivi vsakemu.

1.1.1 Zaupnost

V vsakem poslovnem in domačem okolju je potrebno zagotoviti, da podatki ne bodo prišli „v napačne roke“.

Zaupnost (ang. confidentiality) zagotavlja, da podatkov dostopa le pooblaščena oseba. Nepooblaščenim se dostop onemogoča. in se drži stran od tistih, ki jih nimajo pooblastila.

Podjetja so po Zakonu o varstvu osebnih podatkov in na podlagi splošne evropske uredbe o varstvu osebnih podatkov (GDPR) obvezna, da varujejo osebne podatke, ki jih obdelujejo. V primeru zlorab jim preti kazenski pregon in ukrepi, ki se nanašajo na popravek nepravilnosti.

Še prav posebej pa je treba varovati občutljive osebne podatke. Le-ti se nanašajo na vpis ali izbris v kazensko evidenco, spolno življenje, zdravstveno stanje, članstvo v sindikatu, versko ali filozofsko prepričanje, politično prepričanje, rasno in narodno poreklo.

GDPR prinaša številne zahteve, med njimi tudi sledljivost dostopa do osebnih podatkov in evidentiranje sprememb.

Vendar pa niso le osebni podatki potrebni posebne skrbi. V nekaterih okoljih (npr. vojska, policija) imajo tajne podatke. Označeni so z različnimi stopnjami tajnosti.

V podjetjih obdelujemo različne zaupne podatke. Podatki predstavljajo vrednost. Težko jih je zbrati. Pogosto so rezultat dolgoletnega poslovanja in izkušenj. Zato ne želimo, da se do njih dokopljejo nepooblaščene osebe ali druge organizacije in se z njimi okoristijo ali nam škodujejo.

Ukrepe za zagotavljanje zaupnosti bomo spoznali nekoliko kasneje.

2.1.2 Celovitost

Celovitost (ang. integrity) ali integriteta podatkov pomeni, da so podatki točni in nepoškodovani (Whitman in Mattord, 2019).

 Imamo podatkovno zbirko kupcev. Podatki v njej so popolni, če v njej ne manjkajo pomembni podatki (npr. e-naslov, naslov …).

Podatki bi lahko bili netočni tudi zaradi nenamernih ali namernih napačnih vnosov. Zato na različnih nivojih skrbimo, da ni nepooblaščenih dostopov do podatkov. Se pravi, da do podatkov dostopajo le ljudje in aplikacije, ki jih dejansko potrebujejo.

Dostope se omejuje na nivoju:

- operacijskega sistema (vstop z uporabniškim imenom in geslom, kar ima za posledico, da ima posameznik na voljo le, kar potrebuje),
- informacijskega sistema (posameznik lahko uporablja le module, ki jih pri svojem delu potrebuje; vnosi v sistem so podvrženi kontrolam in preprečujejo očitno napačne vnose).

 Delavec v prodaji ne more dostopati do kadrovske evidence in s tem do osebnih podatkov svojih sodelavcev.

 Vnos telefonske številke npr. zahteva vnos največ 13 številk. Če želi uporabnik vnesti več številk ali kak drug znak, program javi napako.

2.2 ARHIVIRANJE DIGITALNIH PODATKOV

V lokalnih omrežjih vsakodnevno uporabljamo podatke, ki nastajajo na podlagi poslovnih transakcij. Najpogosteje so shranjeni v zbirkah podatkov, od njihove pravilnosti in prisotnosti pa je odvisno delovanje poslovnih procesov. Morebitna izguba podatkov bi povzročila resne težave v delovanju poslovnega sistema. Zato je pomembno podatke redno arhivirati in v jih imeti v primeru napak strojne opreme ali človeka na voljo za priklic iz arhiva (ang. restore).

Brez dvoma lahko rečemo, da smo v današnjem času preplavljeni s podatki. Prihajajo z računalnikov, mobilnih naprav, kamer, najrazličnejših senzorjev, pametnih ur in drugih nosljivih (ang. wearable) tehnologij. Podatke ustvarja vsaka interakcija v družabnih omrežjih; vsaka datoteka, ki jo shranimo; vsaka slika, ki jo naredimo; vsako povpraševanje na internetu in še bi lahko naštevali.

Količina digitalnih podatkov je iz leta v leto večja. Živimo v svetu masovnih podatkov (ang. big data).

Količina podatkov, ki jih organizacije arhivirajo, so ogromne. Glede na hitrost nastajanja in hitrost, kakršna je potrebna za vzpostavitev nemotenega delovanja sistema v primeru izgube podatkov, je odvisno, kako pogosto arhiviramo podatke in na kakšen način je realizirana hitra

vzpostavitev prvotnega stanja. Za manjše podjetje je morda primerno arhiviranje v nočnem času. V primeru težav (npr. pokvarjena oprema, kibernetski napad) se bodo morda izgubili podatki za del dneva, kar pri manjši količini podatkov ni velika težava. V velikih sistemih, kakršni so npr. upravne enote, velika podjetja in druge organizacije z mnogo transakcijami, pa arhiviranje enkrat dnevno ni sprejemljivo. Potrebno je pogostejše arhiviranje ali delovanje redundantnega sistema, ki v primeru napake na primarnem sistemu takoj prevzame njegovo delo.

3 KIBERNETSKI NAPADI

V informacijski varnosti poznamo številne izraze, s katerimi opisujemo potencialna in dejanska sovražna dejanja proti informacijskim sistemom.

Izrazi kibernetski napad, kibernetski vdor, kibernetska grožnja in kibernetsko tveganje so med seboj povezani, a imajo različne pomene.

Kibernetski napad (ang. cyber attack) je kaznivo dejanje kot npr. poskus kraje, razkrivanja, spreminjanja, onemogočanja ali uničenja informacij z nepooblaščenim dostopom do računalniških sistemov (Globalknowledge, 2021).

Kibernetska grožnja je možnost, da se zgodi določen kibernetski napad (Globalknowledge, 2021).

Kibernetsko tveganje (ang. cybersecurity risk) se običajno nanaša na kakršno koli tveganje finančne izgube, motenj ali škode za ugled organizacije, ki je posledica okvare njenih sistemov informacijske tehnologije ali kibernetskega napada.

Kibernetsko tveganje, povezano z grožnjo, pa ocenjuje verjetnost morebitnih izgub, ki bi lahko nastale zaradi konkretne grožnje. Ponavadi se naredi oceno tveganja, ki se pogosto začne s popisom vrednosti vseh sredstev (Globalknowledge, 2021). Sredstva za katere se izkaže, da je tveganje veliko in izgube znatne, je treba še posebej varovati.

Kibernetski vdor je nepooblaščeno dejanje, ki se izvede mimo varnostnih mehanizmov omrežja ali informacijskega sistema (NICCS, 2021). Vdor ogrozi računalniški sistem, saj pomeni, da je varnost sistema pomanjkljiva. Dejanje vdora ali pridobivanja nepooblaščenega dostopa do sistema običajno pusti sledi, ki jih lahko odkrijejo sistemi za odkrivanje vdorov. Vendar pa sam vdor še ne pomeni, da se je dejansko (že) izvedlo kaznivo dejanje. Vdor je kot bi npr. nepovabljen poskusil odpreti vrata sosedovega stanovanja. Če odkriješ, da sosed vrat ne zaklepa, imaš informacijo, ki jo lahko posreduješ dalje ali pa jo kdaj kasneje izkoristiš.

Kibernetski napad (ang. cyber attack) ni nujno uspešen. Strokovnjaki za informacijsko varnost dnevno vlagajo veliko napora, da ne bi prišlo do dejanskega vdora v sistem in zlorab.

V tem poglavju se bomo ukvarjali s kibernetskimi napadi.

Kibernetski napad je zlonamerni napad posameznika ali organizacije, da:

- pridobi nepooblaščeni dostop do omrežja drugega posameznika ali organizacije,

- poškoduje, moti ali ukrade informacijsko komunikacijska sredstva, računalniška omrežja, intelektualno lastnino ali podatke (Savanović in Praprotnik, 2012).

Kibernetski napadalci uporabljajo enega ali več računalnikov za napad na enega ali več računalnikov oz. za napad na računalniška omrežja. Posledica tovrstnega napada je lahko onemogočanje delovanja računalnikov, kraja podatkov ali uporaba napadenega računalnika oz. omrežja za druge napade.

Napadalci uporabljajo različne metode za izvedbo kibernetskih napadov, med drugim zlonamerno programsko opremo, zvabljanje podatkov (ang. phishing), izsiljevalsko programsko opremo in onemogočanje[1] storitve (ang. denial of service).

Najpogostejši motiv napadalcev je finančna korist (Europol, 2020; Verizon, 2020). Ostali razlogi so npr. vohunjenje, politični, aktivistični ali osebni (Kaspersky, 2021).

V tem poglavju se bomo posvetili najpogostejšim napadom na računalniške sisteme.

Spoznali bomo:

- različne vrste škodljive kode,
- socialni inženiring,
- prestrezanje in krajo podatkov,
- kako kibernetski napadalci izkoriščajo pomanjkljivo vzdrževanje zapletene tehnološke infrastrukture in
- napredne oblike kibernetskih napadov.

3.1 ŠKODLJIVA KODA

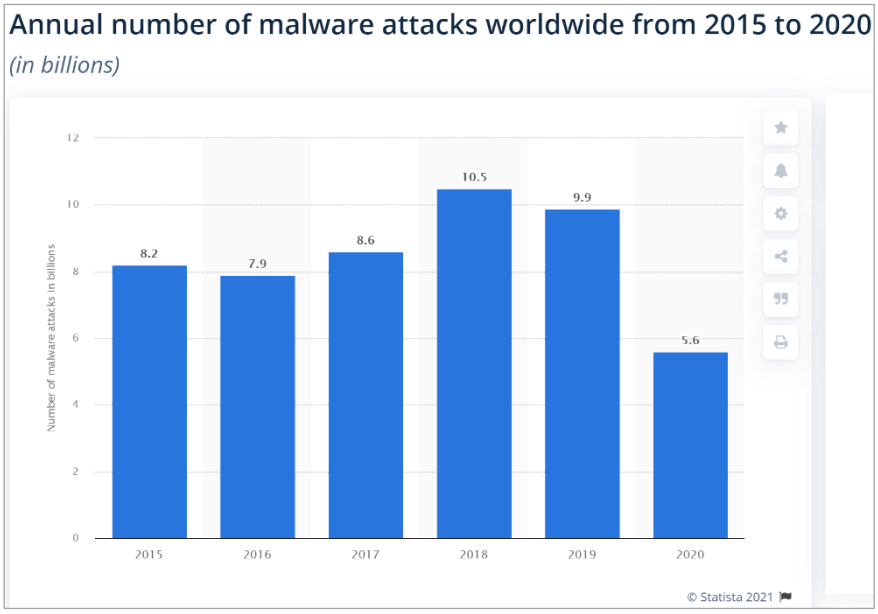
Škodljiva koda (ang. malicious software – malware) imenujemo programsko kodo, ki je namerno zasnovana tako, da povzroči škodo na računalniku, strežniku, odjemalcu ali računalniškem omrežju (Wikipedia, 2021).

V večini primerov gre za programe, ki so zapisani v datotekah. Obstaja pa tudi brezdatotečna škodljiva koda (ang. fileless malware), ki se ob okužbi prenese neposredno v pomnilnik in izvede (McAfee, 2021).

Kot kažejo podatki (Slika 2), je število napadov s škodljivo kodo izjemno veliko.

Dnevno nastajajo novi primerki škodljive kode. Zato je pomembno, da ima računalnik protivirusno programsko opremo, ki se samodejno in neprestano posodablja. Žal pa to ni zadostna varnostna rešitev. Zaradi neprestanega uveljavljanja novih tehnologij na področju računalništva in komunikacij, se tudi na področju zlonamerne kode uporabljajo nove metode in tehnike infiltriranja, maskiranja in skrivanja.

[1] Denial of service prevajamo različno: onemogočanje (SI-CERT), zavrnitev in ohromitev (Islovar) storitve



Slika 2: Število napadov s škodljivo kodo v milijardah
(https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide/)

Najpogostejše vrste zlonamerne kode so:

- računalniški virusi, (ang. virus),
- računalniški črvi (ang. worm) in
- računalniški trojanski konji ali trojanci (ang. trojan horse, trojan).

Različne vrste zlonamerne računalniške kode razvrstimo v nekaj najznačilnejših skupin, ki pa se velikokrat prepletajo med seboj:

- korenski virusi (ang. rootkit),
- stranska vrata (ang. backdoor) – vstopajo skozi stranska vrata v sistem,
- izkoriščevalci (ang. exploit) – izkoriščajo ranljivosti sistema,
- vohunski programi oz. vohunska škodljiva koda (ang. spyware),
- reklamni programi (ang. adware),
- strašilni programi (ang. scareware) ter
- drugi škodljivi in nezaželeni programi.

Zaradi vse številčnejše uporabe antivirusnih programov in učinkovitih izboljšav operacijskih sistemov postaja izdelovanje zlonamerne programske kode vse bolj zahtevno opravilo, programska koda pa kompleksna, saj mora za svoje uspešno širjenje uporabljati kombinacije različnih tehnik.

S stalnim uvajanjem novih informacijskih in komunikacijskih tehnologij ter z razcvetom socialnih omrežij se pojavljajo nove in nove oblike zlonamerne programske kode, nekatere pa zaradi odsluženih tehnologij izginjajo. Virusi, ki so se prenašali preko okuženih disketnih pogonov so izginili. S pojavom USB ključev in njihovo množično uporabo, pa je naraslo število virusov tega tipa (Savanović in Praprotnik, 2012).

 V juliju 2010 se je pojavila škodljiva programska koda poimenovana Stuxnet. Stuxnet je okužil „samo“ nekaj 10.000 računalnikov in ni predstavljal velike nevarnosti navadnim uporabnikom. Kljub temu je povsem presenetil veliko število strokovnjakov in poznavalcev s tega področja in so ga zaradi velike zapletenosti ter vloženega znanja označili kot najkompleksnejša odkrito škodljivo programsko kodo. Virus Stuxnet se močno razlikuje od klasične škodljive kode, saj je prva odkrita škodljiva programska koda, za katero je mogoče skoraj z gotovostjo trditi, da je digitalno orožje, ki povzroča posledice – uničenje centrifug za pridobivanje obogatenega urana. Za črv Stuxnet je značilna kompleksnost izdelane programske kode v katero je bilo vloženo ogromno dela in znanja, saj se ocenjuje, da so stroški razvoja Stuxnet-a stali okoli deset milijonov dolarjev (Langner R. 2010). Znano je, da je virus Stuxnet ustavil iransko jedrsko centralo. Menijo, da sta ga kot kibernetsko orožje skupaj razvila Izrael in ZDA (Wikipedia, 2021).

3.1.1 Računalniški virusi in črvi

Računalniški virus je zlonamerna programska koda, ki potrebuje gostitelja. Virusi so pogosto skriti v izvršljivih datotekah – programih ali v neizvršljivih datotekah kot so npr. Wordovi dokumenti ali slikovne datoteke.

Računalniški črv je zlonamerni program, ki se razširja v računalniških omrežjih in se pri tem samodejno razmnožuje (Islovar, 2021).

Primarna razlika med virusom in črvom je v tem, da mora viruse sprožiti aktivacija njihovega gostitelja (npr. programa, kamor se je vstavil), črvi pa so samostojni zlonamerni programi, ki se samostojno razmnožujejo takoj, ko so uspeli vstopiti v sistem. Črvi ne zahtevajo aktiviranja - ali kakršnega koli človeškega posredovanja - za izvajanje ali širjenje kode.

Računalniški virus je (podobno kot virus gripe) zasnovan tako, da se širi od gostitelja do gostitelja in se razmnožuje. Podobno kot se virusi gripe ne morejo razmnoževati brez gostiteljske celice, se tudi računalniški virusi ne morejo.

Računalniški virus je vrsta zlonamerne kode ali programa, napisana za spreminjanje načina delovanja napadenega računalnika in zasnovana tako, da omogoča širjenje iz enega računalnika v drugega. Deluje tako, da se vstavi ali pritrdi na zakonit program ali dokument, ki podpira makre. Ko se virus uspešno pridruži programu, datoteki ali dokumentu miruje, dokler okoliščine ne povzročijo, da računalnik ali naprava izvede kodo. Virus dejansko okuži računalnik, ko se zažene okuženi program, kar posledično povzroči tudi izvajanje virusne kode. Po okužbi računalnika lahko virus okuži tudi druge računalnike v istem omrežju (Norton, 2020).

Virusni programi izvajajo različne aktivnosti: kraja gesel ali podatkov, beleženje pritiskov tipk, poškodovanje datotek, šifriranje datotek, brisanje datotek, pošiljanje neželene pošte vašim e - poštnim stikom, trajno poškodovanje trdega diska in celo prevzem vašega računalnika so le nekatere uničujoče in nadležne stvari, ki jih virus lahko naredi (Norton, 2020).

Z računalniškim virusom se računalnik okuži na več načinov. Virusi se lahko širijo prek prilog e-pošte, SMS sporočil, prenosov internetnih datotek in s kliki na goljufive povezave v družbenih medijih. Tudi mobilne naprave in pametni telefoni se lahko okužijo s prenosi okuženih aplikacij. Virusi se lahko skrijejo v vsebinah, ki se delijo na socialnih omrežjih, npr. v zabavnih slikah, voščilnicah, zvočnih in video datotekah.

Da bi se izognili stiku z virusom, je pri brskanju po spletu, nalaganju datotek in odpiranju povezav ali prilog pomembno, da ste previdni. Zaradi varnosti nikoli ne prenašajte besedilnih ali e -poštnih prilog, ki jih ne pričakujete, ali datotek s spletnih mest, ki jim ne zaupate.

Znaki okužbe

Da je računalnik okužen, prepoznamo preko enega ali več znakov okužbe:

- Pojavna okna vas lahko spodbudijo k obisku nenavadnih spletnih mest. Lahko pa vas spodbudijo, da prenesete protivirusno ali drugo programsko opremo, ki vsebuje virus.
- Spremembe vaše domače strani. Vaša običajna domača stran se lahko na primer spremeni v drugo spletno mesto.
- Masovna e-poštna sporočila, poslana z vašega e-poštnega računa. Kriminalec lahko prevzame nadzor nad vašim računom ali pošlje e-pošto v vašem imenu z drugega okuženega računalnika.
- Pogoste zrušitve sistema. Virus lahko na trdem disku povzroči veliko škodo. To lahko povzroči zamrznitev ali zrušitev vaše naprave. Prav tako lahko prepreči, da bi se naprava znova vklopila.
- Nenavadno počasno delovanje računalnika. Nenadna sprememba hitrosti obdelave lahko pomeni, da je v računalniku virus.
- Neznani programi, ki se zaženejo, ko vklopite računalnik. To lahko opazite, če preverite seznam aktivnih aplikacij v računalniku.
- Nenavadna sprememba gesla, ki vam prepreči prijavo v računalnik.

Kako se zaščititi pred računalniškimi virusi?

Zaščita pred računalniškimi virusi je nujno potrebna v vsakem računalniškem sistemu.

Uporabljati je treba zaupanja vredno protivirusno programsko opremo in jo redno posodabljati. Žal pa nas to ne varuje pred vsemi virusi. Zato je potrebno še:

- redno izdelovati varnostne kopije podatkov,
- izogibanje klikanju na pojavne oglase,
- preverjanje e-poštnih prilog pred odpiranjem,
- pazljivost pri klikih na povezave v socialnih omrežjih ali na drugih spletnih straneh.

Poštni strežniki običajno preprečujejo sprejem prilog, ki imajo programske končnice. Ne morejo pa npr. preprečiti sprejema dokumenta (npr. v formatu .DOCX), ki ima vgrajen makro s škodljivo kodo.

Kako odstraniti računalniške viruse?

Za odstranitev računalniškega virusa lahko uporabite dva pristopa:

- ročni pristop ali "naredi sam",
- s pomočjo protivirusnega programa.

Vrste računalniških virusov

Norton (2020) opredeljuje devet vrst računalniških virusov, ki se širijo z različnimi tehnikami razmnoževanja. Naslednja klasifikacije se nanaša na mesto okužbe in značilnost delovanja:

- zagonski virus (ang. boot sector virus): računalniški virus, ki se zapiše v zagonski sektor in se aktivira ob zagonu računalnika (Islovar, 2021),
- spletni skriptni virus (ang. web scripting virus): okuži spletno stran; če dostopate do okužene spletne strani, lahko virus okuži vaš računalnik.
- ugrabitelj brskalnika (ang. browser hijacker): izkoristi ranljivost spletnega brskalnika (»ugrabi« njegove funkcije) in uporabnika npr. preusmeri na spletno mesto, ki ga ni želel obiskati,
- rezidenčni virus (ang. resident virus): to je splošni izraz za vsak virus, ki se vstavi v pomnilnik računalniškega sistema in se izvede, ko se naloži operacijski sistem,
- virus neposrednega delovanja (ang. direct action virus): delovati začne, ko izvedete okuženo datoteko (če je ne izvedete, ostane v mirovanju),
- polimorfni virus (ang. polymorphic virus): svojo kodo spremeni vsakič, ko se izvede okužena datoteka (to počne, da se izogne protivirusnim programom),
- okuževalec datotek (ang. file-infecting virus / file injector): virus, ki vstavi zlonamerno kodo v izvedljive datoteke (datoteke, ki se uporabljajo za izvajanje določenih funkcij v operacijskem sistemu ali v programske datoteke),
- večstranski virus: okuži tako programske datoteke kot sistemske sektorje,
- makro virus: širi se, ko odprete okužen dokument (s škodljivim makrom); pogosto se distribuira preko prilog e -pošte.

S stališča uporabnika je ta delitev manj pomembna. Zato bomo v nadaljevanju spoznali vrste škodljive kode glede na učinke, ki jih povzročijo v sistemu.

3.1.2 Trojanski konji

Trojanski konj (ang. trojan horse) ali trojanec (ang. trojan) je vrsta virusa, ki se zažene s pomočjo prevare uporabnika. Uporabnik npr. misli, da je naložil koristen program. Zlonamerna programska koda je lahko:

- skrita v programih, ki jih uporabnik naloži iz interneta,
- skrita na spletnih straneh, ki jih uporabnik obišče,
- pripeta elektronski pošti,

Pogosto izkorišča ranljivosti programske opreme, s katero dostopamo do spleta (brskalnik, razni predvajalniki[2], itd.) (Savanović in Praprotnik, 2012).

3.1.3 Izsiljevalska škodljiva koda

Izsiljevalski programi (ang. ransomware) so ena večjih groženj na področju informacijske varnosti. Podjetjem povzročijo ogromno škode. Najpogosteje jih prenesejo uporabniki sami. Pred njimi se s protivirusno programsko opremo ne moremo ubraniti.

Pogosto rečemo tudi izsiljevalski virusi, čeprav tovrstna škodljiva koda ni nujno virus v ozkem pomenu besede.

Problematika je lepo opisana na spletni strani policije: https://www.policija.si/svetujemo-ozavescamo/varnost-na-internetu/85763-pozor-izsiljevalski-virusi

V zadnjih letih se je povečalo število napadov z izsiljevalskimi virusi.

Koliko so vredni podatki na vašem računalniku? Če boste slučajno staknili računalniški virus, ki vam podatke zaklene in zahteva odkupnino, ta vrednost hitro dobi otipljivo obliko. Ponavadi so tarča napada podjetja, ne glede na velikost (Europol, 2020).

Prvi izsiljevalski virus se je pojavil in povzročal težave že leta 1989. Tovrstni virusi so od tedaj vsako leto bolj nevarni, kriminalne združbe, ki jih razpošiljajo pa bolj predrzne in neizprosne. Opažajo, da pred tem dobro analizirajo žrtev in se na napade pripravljajo dlje časa (Europol, 2020).


AIDS trojanec je ob okužbi skril mape in zašifriral datoteke na disku C. Uporabnika je obvestil, da mora kontaktirati PC Cyborg Corporation in poslati 189 dolarjev na naslov poštnega predala v Panami, da prejme ključ za dešifriranje in odklepanje podatkov. Postopek šifriranja je bil sorazmerno enostaven, kar je omogočilo izdelavo orodja, ki je hitro povrnilo datoteke uporabniku. Po tem prvem primeru smo dolgo časa lahko le bežno tu in tam slišali o kakšnem sorodnem primeru, a le od daleč. Vse do leta 2012, ko se je pojavil Ransomcrypt (https://cert.si/izsiljevalski-virusi/, 18. 9. 2014).

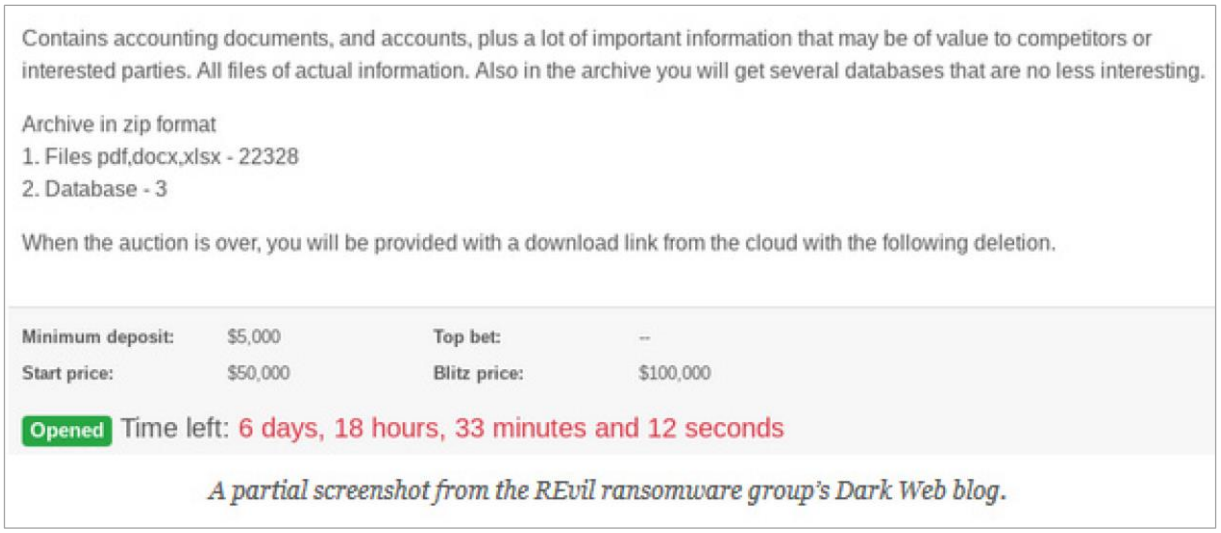
AIDS trojanca se je dalo hitro ustaviti, podatke pa z lahkoto dešifrirati. Današnjih izsiljevalski virusi uporabljajo zelo zapletena šifriranja. Zato imajo žrtve le dve možnosti: plačajo ali pa morajo vse okužene podatke izbrisati in jih nato na novo naložiti iz arhivov.

Lekarna Ljubljana je bila avgusta l. 2019 napadena z izsiljevalskim virusom, ki je za vsaj teden dni ustavil normalno delovanje računalniškega sistema. Lekarne so bile na začetku celo fizično zaprte. Škoda je bila ogromna, čeprav odškodnine niso plačali.

Od prvih izsiljevalskih virusov dalje se je višina odkupnin povečevala. Razen tega so začeli zahtevati plačila v bitcoinih ali drugih kriptovalutah, saj so tovrstne transakcije bistveno težje izsledljive.

[2] Zelo ranljiv je bil Flash, ki se prav zaradi tega danes več ne uporablja.

Ker pa so po toliko letih obstoja izsiljevalskih virusov podjetja nanje pripravljena in imajo kopije podatkov na varnem, so izsiljevalci svojo storitev nadgradili. Če žrtev v roku ne plača, objavijo podatke. Na temnem spletu se začne avkcija za podatke. Primer je na sliki (Slika 3)**Napaka! Vira sklicevanja ni bilo mogoče najti.**. Imena podjetja, katerega podatki so na voljo, Europol ni objavil. Kriminalci so ga, saj je v tem bistvo.



Slika 3: Primer objave avkcije na temnem spletu (Europol, 2020)

Na SI-CERT pravijo, da so običajno žrtve vdorov naključno izbrane kot del širše kampanije širjenja virusov. Europol (2020) pa poroča, da se izvajajo tudi napredni primeri ciljanih napadov na posamezna podjetja in inštitucije.

Izsiljevalski virusi se širijo v glavnem na dva načina:

- v obliki priponk elektronske pošte (kot navidezne PDF-datoteke, kot dokumenti programov Microsoft Office z makri ali kot ZIP-arhivi s kodo javascript), ali
- preko okužb v mimohodu (ang. drive-by download).

Elektronska pošta s prilogami, ki vsebujejo izsiljevalski virus, je najbolj pogost način širjenja okužbe.

Okužba v mimohodu se nanaša na nenamerni prenos zlonamerne kode na računalnik ali mobilno napravo, ki uporabnike izpostavlja različnim vrstam groženj. Kibernetski kriminalci uporabljajo "drive-by" prenose za krajo in zbiranje osebnih podatkov, vbrizgavanje bančnih trojancev ali druge zlonamerne programske opreme. Te okužbe se najpogosteje zgodijo z obiskom okuženih spletnih strani, ki se okužijo zaradi ranljivosti v brskalnikih ali aplikacijah.


Do okužbe v mimohodu pride na razne načine, npr. ob prebiranju spletne strani z novicami. Znan je primer, ko so napadalci na novičarsko spletno stran z oglasom podtaknili škodljivo kodo. Ta preveri, ali je v sistemu neposodobljena programska oprema, ki omogoča nepooblaščen dostop in namestitev dodatnih zlonamernih komponent. Podtaknjena koda lahko iz sistema pridobi tudi zaupne informacije, gesla in certifikate (www.cert.si, 2018).

Obramba pred izsiljevalskimi virusi je enostavna:

- ne klikajte priponk v elektronski pošti, za katere vam ni čisto jasno, zakaj ste jih dobili, ali pa vam obljubljajo kaj lepega,
- imejte računalnik z nameščenimi popravki za operacijski sistem in vse programje na njem.

Izsiljevalski virusi v zadnjih letih predstavljajo vse večjo nevarnost tako za posameznike kot za podjetja. Če vemo, kako delujejo, bomo lažje preprečili zlorabo.

Prva in najučinkovitejša zaščita pred škodo, ki jo lahko povzročijo izsiljevalskimi virusi je pravilno zastavljen režim izdelave varnostnih kopij ter ustrezno omejevanje pravic dostopa do skupnih datotek za zaposlene, s čimer se ob morebitni okužbi zameji škoda. Omrežja morajo biti razdeljena na različna območja, kar oteži prehajanje okužb ali njenih posledic med njimi. Sledita redno posodabljanje nameščene programske opreme ter izobraževanje zaposlenih glede obravnave elektronske pošte in odpiranja priponk. Prav tako je nujno ločiti komercialno-administrativno okolje podjetja od morebitnih industrijskih in poslovnih procesov. Komunikacija po elektronski pošti je nujna za delovanje podjetja, a je treba upoštevati možnost okužbe in računati na začasno izgubo podatkov. Okužba, ki bi vplivala na proizvodni proces, pa bi povzročila izpad poslovanja in s tem še dodatne stroške (www.cert.si, 2018).

Leta 2016 so se Europol cybercrime center (EC3), Nizozemska policija in dve podjetji, ki izdelujeta protivirusno programsko opremo: Kaspersky in McAfee, združili v projektu ***No more ransom***. Spletna stran projekta https://www.nomoreransom.org/sl/partners.html ponuja rešitve za nekatere izsiljevalske viruse. Rešitev pomeni navodila za odstranitev virusa in ključ za dešifriranje.

3.1.4 Korenski komplet

Korenski komplet (ang. rootkit) je vrsta zlonamerne programske opreme, ki hekerjem omogoča dostop do ciljne naprave in nadzor nad njo. Večina rootkitov okuži programsko opremo in operacijski sistem, nekateri okužijo tudi strojno in vdelano programsko opremo računalnika (kasperksy, 2021).

Najpogosteje se vtihotapi v operacijski sistem. Pri tem poskuša zabrisati sledi svoje prisotnosti in hkrati prevzeti nadzor nad želenimi funkcijami sistema tako, da spremeni nekatere osnovne funkcije operacijskega sistema. Prepoznavanje takšnih zlonamernih programskih kod je zelo oteženo, saj lahko postanejo okužene datoteke nevidne za protivirusne in protivohunske programe. V nekaterih primerih poskušajo takšni programi blokirati ali onemogočiti protivirusne programe. Za vdor v računalnik lahko korenski virusi uporabijo podobne tehnike napadov kot ostala zlonamerna programska koda (Savanović in Praprotnik, 2012).

Običajno ni en sam program, zato rečemo rooktkit.

Nekateri škodljivi programi vsebujejo programsko kodo, ki omogoča nepooblaščen dostop skozi stranska vrata (ang. backdoor) do okuženega računalnika. Največkrat so to posebna vrsta korenskih virusov.

3.1.5 Drugi škodljivi in neželeni programi

Vohunska programska koda (ang. spyware) je namenjena prikritemu zbiranju podatkov o uporabniku. Teh metod se ne poslužujejo samo kriminalne združbe, ampak tudi večja podjetja, ki na bolj ali manj legalen način zbirajo različne podatke o uporabnikih. Ko jih odkrijejo pogosto trdijo, da zbirajo podatke zaradi izboljšanja uporabniške izkušnje.

Veliko brezplačnih programov se financira tako, da poleg svoje osnovne naloge reklamirajo določeno podjetje ali izdelek. To so v bistvu **reklamni programi** (ang. adware). Obstajajo pa tudi brezplačni programi, ki poleg osnovne funkcije vsebujejo še zlonamerno kodo. Takšne programe bi lahko uvrstili tudi med posebno vrsto trojanskih konjev, saj se zlonamerna koda naloži v računalnik s prevaro. Ker se avtorji takšnih programov zavedajo, da lahko njihovi programi hitro postanejo tarča protivirusnih programov, je običajno takšna zlonamerna koda relativno neškodljiva (Savanović in Praprotnik, 2012).

Strašilna programska koda (ang. scareware) poskuša pri uporabnikih s pomočjo prevare ustvarjati elemente strahu, zaskrbljenosti ali celo panike in na osnovi negativnih emocij uporabnika od njega pridobiti denarne ali kakšne druge koristi. Na internetu je najbolj razširjena strašilna zlonamerna programska koda v obliki lažnih antivirusnih programov, ki uporabniku poročajo o kopici neobstoječih virusov in mu v zameno za določena denarna sredstva obljubljajo rešitve (Savanović in Praprotnik, 2012).

Kriminalni programi (ang. crimeware) so programi, katerih namen je izvedba kriminalnega dejanja na osnovi informacij, ki jih tak program zbere. Kriminalni programi za vdor v računalnik uporabijo podobne tehnike napadov kot ostala zlonamerna programska koda. Ko se naselijo v računalnik, začnejo zbirati koristne informacije, s katerimi se lahko napadalec okoristi. Tako si lahko zapisujejo tipkanje uporabnika (ang. keyloggers) za ugotavljanje gesel, PIN kod, številk kreditnih kartic, lahko pošiljajo zaslonske slike pri uporabi spletnega bančništva, zbirajo informacije za krajo identitete, itd. Ker je količina in vrsta denarnih tokov na internetu v porastu (elektronsko bančništvo, e-trgovine, itd), se povečuje tudi internetna kriminaliteta (Savanović in Praprotnik, 2012).

Človeška domišljija nima meja, zato nastajajo nove in nove ideje, kako pretentati ljudi ali sisteme. Nastajajo nove in nove vrste različnih tipov zlonamernih programov, ki so lahko plod popolnoma novih idej, ali pa nastajajo na osnovi kombinacije že obstoječih tipov zlonamerne računalniške kode. Računalniški kriminal je vsaj toliko inovativen kot računalniška veda sama. Računalniški virusi in drugi zlonamerni programi so lahko za uporabnike zelo neprijetni, saj velikokrat povzročijo ogromno škodo. Predvsem so na udaru neizkušeni uporabniki, ki se premalo zavedajo vseh nevarnosti, ki jim pretijo pri vsakodnevnem delu z računalniki in zato ne posvečajo dovolj pozornosti za zagotovitev potrebnih zaščitnih mehanizmov.

Škodljivo delovanje virusov, predvsem pa njihovo širjenje, lahko učinkovito omejimo s preventivnim delovanjem. Povprečni uporabnik lahko že s pomočjo kvalitetne protivirusne zaščite in z rednim posodabljanjem svojega operacijskega sistema, brskalnika ter s previdnim odpiranjem elektronske pošte doseže dovolj zanesljivo zaščito, ki ga varuje pred veliko večino zlonamerne programske kode (Savanović in Praprotnik, 2012).

3.2 NAPADI ONEMOGOČANJA

Napade, ki neposredno ali posredno povzročajo onemogočanje storitev, imenujemo napadi DoS (ang. Denial of Service) in DDoS (ang. Distributed Denial of Service).

Napadalec dostopne točke omrežja nenehno obsipava z lažnimi zahtevami in ukazi, ki jih le-te ne zmorejo obdelati v realnem času. S tem onemogoči drugim uporabnikom dostop do omrežja in njegovih storitev, v določenih primerih pa celo njegovo sesutje. Napad se izvaja praviloma iz računalnika ali množice računalnikov, ki niso v napadenem omrežju.

Cilj takih napadov je popolnoma zaustaviti ali zavreti delovanje sistema, zaradi nagajanja ali z namenom zahtevati odkupnino za prenehanje napada.

V Sloveniji se je število napadov z onemogočanjem storitev (DDoS) pojavilo v večjem obsegu leta 2014. Konec leta 2015 je skupina z imenom Armada Collective (AC) tako kot drugod po svetu napadala tudi banke v Sloveniji in zahtevala odkupnino za prenehanje motenja spletnih storitev. Njihovi »vzorniki« so bili DD4BC (Distributed Denial-of-Service for Bitcoin), ki pa so jih v začetku leta 2016 v mednarodni akciji aretirali organi pregona. To je bil verjetno razlog, da je skupina AC takrat poniknila. Jeseni leta 2017 so se prebudili (ali pa so njihove metode prevzeli posnemovalci) in spet napadli. Na SI-CERT so obravnavali napade na sedem slovenskih bank in jim priporočili, kako ukrepati ob napadih. (SI-CERT, 2018).

Napad onemogočanja je lahko osredotočen samo na neko znano pomanjkljivost programske opreme, ki povzroči zaustavitev storitve (pogosto gre za različne spletne storitve) in posledično izpad strežnika (npr. strežnika Microsoft IIS).

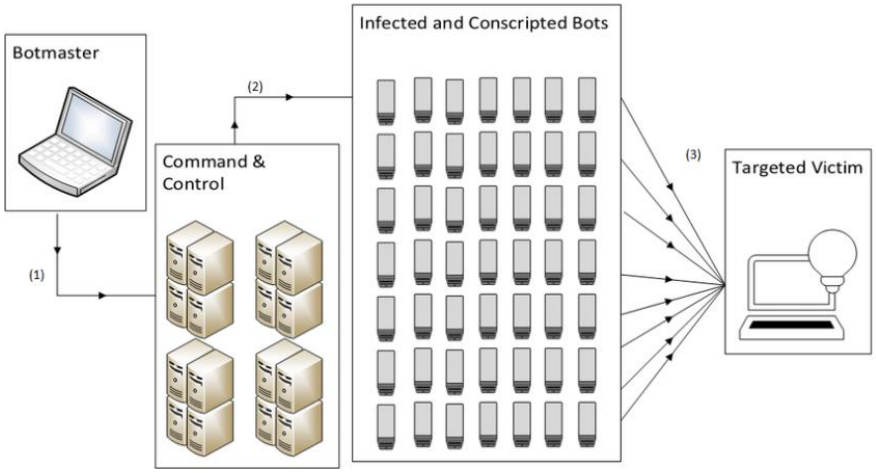
Druga skupina napadov onemogočanja sproži na računalniku dodatna nepotrebna opravila, ki trošijo vire in upočasnijo ali ustavijo delovanje sistema.

Napadi onemogočanja običajno ne omogočijo neavtoriziranega dostopa v sistem. Škoda, ki jo povzročajo, pa je kljub temu velika, saj lahko nedelovanje strežnika onemogoči poslovanje in s tem povzroči izpad prihodka.

DDoS je učinkovitejša različica napada DoS. Napad ne poteka le iz enega vira, temveč je porazdeljen. Napadalec ima nadzor nad večjim številom drugih računalnikov, ki niso v napadenem omrežju in čakajo ukaz za napad. Ko ga dobijo, začnejo vsi, istočasno, pošiljati večje količine podatkov napadeni dostopni točki omrežja in tako onemogočijo njeno normalno delovanje. V DDoS napad je ponavadi vključenih večje število računalnikov, ki so vključeni v t.i. botnet omrežja. Zato je učinek napada viden hitreje kot pri napadu DoS. Napad prikazuje Slika 4.

Vrste DDOS napadov (SI-Cert, 2018):

- Volumetrični napadi (ang. volumetric attack) poplavijo žrtev z veliko količino podatkov. Običajno se uporabijo številni viri, ki pošiljajo podatke. Pri tem si pomagajo z omrežjem okuženih tujih računalnikov, ki so nevede zlorabljeni za sinhrono izvedbo napada.
- Protokolni napadi izkoriščajo lastnosti v zasnovah komunikacijskih protokolov, ki lahko v določenih primerih privedejo do izčrpanja virov (ang. resursov) sistema. Primer takšnega napada je TCP SYN poplava. Storilec pošilja zahteve za povezavo TCP hitreje, kot jih lahko ciljni računalnik obdela, kar povzroči nasičenost omrežja.
- Aplikacijski napadi ciljajo na delovanje aplikacije ali strežnika in s posebej skonstruiranimi zahtevami povzročijo izpad ali upočasnitev delovanja. Najbolj znan napad te vrste je Slowloris, ki povzroči ustavitev spletnega strežnika (ang. web server) žrtve.



Slika 4: DDoS napad
(Hellman, 2017)

Motivi za različne napade onemogočanja storitev segajo od vandalizma, protesta in aktivizma do oviranja konkurence in neposredne finančne koristi, recimo z izsiljevanjem.

Marca 2013 so v Sloveniji zaznali 5.198 odprtih DNS-strežnikov, ki so se uporabljali v porazdeljenih napadih. Večji internetni operaterji so takoj izvedli ukrepe za omejitev dostopa (www.cert.si, 2014).

Kako se učinkovito obvarovati pred napadi onemogočanja? Zelo koristno je, če poznamo arhitekturo in delovanje storitev, da lahko preprečimo in omejimo nepotrebne in nepooblaščene dostope (na primer zapremo dostop na požarnem zidu). Priporočljivo je tudi spremljanje spletnih strani, ki se ukvarjajo z varnostnimi problemi sistemov, ki so del našega omrežja.

3.3 BOTNET OMREŽJA

Botnet je veliko število računalnikov, ki jih brez vedenja skrbnikov napadalec poveže v omrežje z namenom izvajanja zlonamernih dejanj (www.islovar.org, 2011). Besedo računalnik je treba

razumeti v širšem smislu. Botneti lahko povezujejo različne internetne naprave, kamor spadajo tudi mobilni telefoni, pametne tablice in različne IoT[3] naprave (npr. kamere). Na okužene naprave se na enega od različnih načinov naloži zlonamerni program, ki se iz teh naprav poveže v nadzorni strežnik napadalca. Okužba se npr. začne z okužbo spletnih strani oz. spletnih strežnikov in se širi na obiskovalce. Okuženi računalniki - boti (imenujemo jih tudi zombiji) potrdijo lastniku botneta svojo aktivacijo in čakajo nadaljnjih ukazov.

Beseda bot je okrajšava za robot, končnica net v besedi botnet pa prihaja od angleške okrajšave net (ang. network je omrežje).

Bote kontrolira eden (ali več) **nadzornih računalnikov** (ang. bot controller) s katerim upravlja heker – administrator botnet omrežja (ang. botmaster). Boti komunicirajo z nadzornim računalnikom in izvajajo njegove ukaze.

Večino odkritih botnet omrežij nadzorujejo skupine kriminalcev, ki jih uporabljajo za kriminalno dejavnost kot npr. generiranje nezaželene pošte, krajo osebnih podatkov (predvsem številk kreditnih kartic in gesel) ali porazdeljene napade onemogočanja storitev (DDoS).

Teoretično lahko že en sam računalniški strokovnjak izdela škodljivo kodo, ki po vsem svetu spremeni na milijone računalnikov v bot-e, čeprav imajo le-ti naloženo vrhunsko protivirusno zaščito z najnovejšimi popravki. Prav zato so botnet omrežja tako nevarna. V rokah posameznikov ali majhnih skupin postanejo nevarno orožje, ki lahko povzroči ogromno škodo tako posameznikom kot organizacijam ali celo državam. Botnet omrežija ne predstavljajo samo neposrednih groženj (kriminal, DDoS napadi, generiranje nezaželene pošte), ampak lahko kot celota ustvarijo izjemno računalniško moč, ki jo je možno izkoristi v različne namene. Povsem možno bi bilo, da se s pomočjo milijonske množice računalnikov izvede analiza močnih šifrirnih algoritmov, ki predstavljajo trd oreh tudi za najhitrejše superračunalnike. Države, ki si ne morejo nabaviti superračunalnikov (npr. zaradi embarga), lahko s pomočjo botnet omrežij izvedejo potrebne izračune za simulacijo procesov pri izdelavi atomskega orožja (Savanović in Praprotnik, 2012).

Botneti so stalna nevarnost in nikakor ne moremo biti prepričani, da naš računalnik prav v tem trenutku ne opravlja opravil za neko kriminalno omrežje.

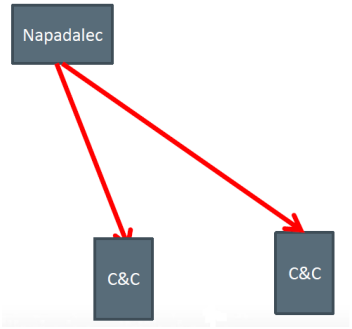
Botneti opravljajo naslednje naloge:

- kraja identifikacijskih podatkov,
- nameščanje orodij za nepooblaščene oddaljene dostope,
- rudarjenje kriptovalut,
- razširjanje trojancev za napade na e-bančništvo,
- izvajanje DDoS napadov,
- pošiljanje neželene oglasne in druge pošte,
- razširjanje izsiljevalskih virusov.

[3] Internet stvari (ang. internet of things – IoT)

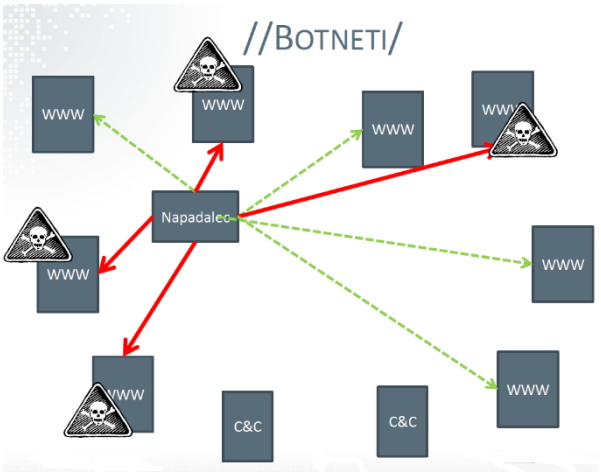
3.3.1 Formiranje botnet omrežja

Napadalec najprej vzpostavi ukazne (ang. command and control - C&C) oz. bot kontroler strežnike, preko katerih upravlja omrežje (Slika 5).



Slika 5: Ustvarjanje botnet omrežja najprej vzpostavi strežnike (Vodopivec, 2010)

Nato se začne infekcija žrtev, ki se okužijo z obiskom okuženega računalnika oz. spletne strani (Slika 6).



Slika 6: Botnet omrežje (Vodopivec, 2010)

Botneti so zaradi velike kompleksnosti njihove dejavnosti precej velika težava.

Botneti pogosto sodelujejo v napadih onemogočanja (Slika 4).

3.3.2 Primeri botnet omrežij

Prvo botnet omrežje je leta 2000 ustvaril takrat 15-letni Kanadčan Michael Calce, z vzdevkom MafiaBoy, ki je svoj botnet zgradil iz omrežja računalnikov, nameščenih v učilnicah njegove srednje šole. Uporabljal pa jih je za DDoS napade. Na kolena je uspel spraviti spletne velikane kot so eBay, Yahoo, Amazon, CNN in nekateri drugi.

Kompleksna botnet omrežja so osnovno sredstvo organiziranih skupin kriminalcev za svoje dejavnosti. Upravljalec ima nadzorni center botneta na svojih strežnikih ter izvaja popoln

nadzor nad okuženimi računalniki. Ponuja kriminalne storitve in jih celo trži drugim kriminalcem preko interneta (Vodopivec, 2010).


Leta 2013 je bilo 30 Joomla[4] strežnikov iz Slovenije povezanih v botnet in sodelovalo v izvajanju napadov onemogočanja, kar so zaznali v US-CERT (SI-CERT, 2014).


Slovenski uvoznik je za specifične potrebe slovenskega trga blagajnam uveljavljenega proizvajalca leta 2016 dodal modul za davčno potrjevanje računov po internetu. Modul je vključeval preprost dostop za daljinsko upravljanje, ki pa ni bil omejen samo na vzdrževalca naprave. Pomanjkljivost so odkrili neznani storilci in module vključili v svoj botnet, prek njega pa razpošiljali neželeno oglasno pošto (SI-CERT, 2017).

Mariposa

Eden izmed najnaprednejših odkritih botnet omrežij je **Mariposa**[5], katerega vodilni avtor je bil Slovenec z vzdevkom Iserdo.

Botnet je bil odkrit maja leta 2008. Uporabljen je bil za pridobivanje osebnih podatkov ter za napade za onemogočanje storitve. Mariposa je eden izmed najobsežnejših botnetov do sedaj. Ustvarjen je bil s pomočjo programa "Butterfly bot". Skupina iz Španije, zadolžena za upravljanje botneta, se je imenovala DDP (špansko "Dias de Pesadilla", slovensko "Dnevi nočnih mor"). Programska oprema je bila prodana tudi tretjim osebam. Mariposo so ustavili 14.3. 2010, v Madridu. Pri preiskavi so sodelovali mednarodni in nacionalni organi pregona spletnega kriminala, Panda Security (španski proizvajalec varnostnih rešitev) ter Defence intelligence, ki pa je kanadsko varnostno podjetje. Do ustavitve botneta, so že okužili skoraj 13 milijonov računalnikov, v kar 190 državah (Wikipedia, 21. 8. 2021).

Zlonamerna programska koda Mariposa se je lahko širila preko P2P omrežij, preko IE6[6] varnostnih lukenj, preko USB ključkov ali preko okuženih spletnih strani. Zato programske kode, ki je ustvarila botnet omrežje Mariposa, ne moremo klasificirati niti kot virus, niti kot trojanski konj, saj je lahko administrator poljubno določil način širjenja škodljive programske kode. S tem se je bistveno povečala možnost širjenja okužb tudi na računalnikih, opremljenih s protivirusno zaščito (Savanović in Praprotnik).

Administratorji botnet omrežja Mariposa so omrežje uporabljali za namestitev dodatne škodljive programske kode na že okužene računalnike kot npr. napredne zapisovalnike vnosov tipkovnice (ang. keyloggers), bančne trojance (npr. Zeus), itd. Tako pridobljene informacije (ukradene številke bančnih in kreditnih kartic ter gesla za njih) so prodajali, hkrati pa so tudi prodajali nadzor nad posameznimi deli botnet omrežja, omogočali namestitev orodnih vrstic

[4] CMS (ang. content management system) sistem za ustvarjanje spletnih strani

[5] Mariposa v španskem jeziku pomeni metulj.

[6] Internet Explorer 6

(ang. toolbars) na okužene računalnike ter se ukvarjali z manipuliranjem iskalnikov (Google) (Savanović in Praprotnik, 2012).

Posamezniki iz DDP skupine so komunicirali z okuženimi računalniki s pomočjo šifriranih ukazov, ki jih je bilo izjemno težko zaznati, še težje pa razvozlati, kar je še dodatno oteževalo njihovo odkrivanje. Poleg tega so se v omrežje povezovali preko anonimnih VPN[7] povezav in šele napaka enega izmed glavnih akterjev je privedla kriminaliste do njegove identitete. Izkazalo se je, da skupina kriminalcev, ki je upravljala z botnet omrežjem Mariposa, ni posedovala veliko računalniškega znanja, ampak je te usluge preprosto kupila „na trgu“ od Iserda. Kljub temu, da so pomladi leta 2010 Iserda aretirali in ugasnili nadzorne računalnike omrežja Mariposa, so leto kasneje strokovnjaki podjetij Unveillance in Panda odkrili še obsežnejše botnet omrežje imenovano **Butterfly** (Raywood, 2011) ali **Metulji** (Clayton, 2011). Botnet Metulji naj bi bilo do sedaj največje odkrito botnet omrežje, saj v njem nezavedno sodelovalo več deset milijonov okuženih računalnikov, ki se nahajajo v najmanj 172 državah. Strokovnjaki podjetja Unveillance in Panda Labs so ocenili, da je velikost botnet omrežja Metulji še enkrat večja od botneta omrežja Mariposa. Botnet omrežje Metulji je zgrajeno s pomočjo izboljšanega orodja za izdelavo zlonamerne programske kode - Butterfly Bot Kit (znano tudi pod imeni Palevo, Pilleuz in Rimecud), ki ga je izdelal in tržil Iserdo. Poleg omrežja Metulji obstaja kar nekaj botnet omrežij, ki so bila zgrajena s pomočjo orodja Butterfly Bot Kit (npr. EvilFistSquad). Pri odkrivanju novih botnet omrežij, ki so bila zgrajena s pomočjo omenjenega orodja, predvsem pa pri iskanju njihovih administratorjev, je oblastem zelo pomagal seznam kupcev, ki ga je Iserdo natančno vodil pri svojem „poslovanju“ (Savanović in Praprotnik, 2012).

Kakovost obstoječe zlonamerne programske kode je že kar na zavidljivi ravni, saj je za njo značilno predvsem evolucijsko napredovanje kakovosti. Razvoj je temeljil na posameznikih, ki so obstoječa znanja in izvorno kodo, pridobljeno na Internetu, počasi dopolnjevali s svojimi novimi idejami, izdelano škodljivo programsko kodo pa so zopet objavili na internetnih straneh. Poleg skoraj neizčrpnih virov znanja pa Internet omogoča tudi enostavno povezovanje, komuniciranje in izmenjavo informacij med hekerji po vsem svetu. Največje mesto povezovanja je temni spet (ang. darknet).

TDL-4

Primer evolucijskega izboljšanja zlonamerne programske kode je botnet omrežje TDL-4.

Kot je razvidno iz imena botnet omrežja, je TDL-4 že četrta generacija škodljive programske kode, ki se je prvič pojavila v letu 2008. Njeni avtorji so programsko kodo postopoma izboljševali do te mere, da je TDL-4 postala ena izmed najbolj izpopolnjenih zlonamernih programskih kod, ki je veliko strokovnjakov s področja IKT varnosti presenetila predvsem s svojo trdoživostjo in odpornostjo na protivirusno zaščito. Za svoje prikrivanje uporablja celo vrsto naprednih metod, ki mu omogočajo učinkovito izogibanje protivirusnim zaščitam.

[7] Navidezno privatno omrežje VPN - Virtual Private Network

Programska koda TDL-4 vsebuje tudi zavidljivo protivirusno programsko zaščito, ki ji omogoča zaznavanje in brisanje velikega števila konkurenčne škodljive programske kode. Poleg onemogočanja konkurence, TDL-4 z brisanjem ostale škodljive programske kode preprečuje upočasnjeno delovanje okuženega računalnika in s tem poskuša odvrniti uporabnikovo pozornost, ki bi se povečala zaradi sumljivega delovanja računalnika. TDL-4 se od starejših verzij loči predvsem po lastnem šifrirnem algoritmu. Zaradi svoje trdoživosti se je botnet omrežju TDL4 oprijelo ime „neuničljivo botnet omrežje“ (Savanović in Praprotnik, 2012).

Različica, ki so jo imenovali TDSS ali Alureon, okuži glavni zagonski zapis (ang. master boot record) tarče, zaradi česar je škodljivo kodo težje zaznati in odstraniti. Razen tega omrežje uporablja šifriranje komunikacij, decentraliziran nadzor, pa tudi brisanje druge zlonamerne programske opreme. Ko je nameščen, lahko blokira dostop do Windows Task Manager, Windows Update in namizja ter je sposoben onemogočiti pravi protivirusni program. Zlonamerna programska oprema je pritegnila veliko pozornost, ko je programska napaka v njeni kodi povzročila zrušitev nekaterih 32-bitnih sistemov Windows ob namestitvi varnostne posodobitve MS10-015. Microsoft je nato naredil popravek, da prepreči namestitev, če je prisotna okužba z Alureonom, Avtorji zlonamerne programske opreme pa so tudi odpravili napako v svoji kodi. (Wikipedia, 2021).

Podobno kot drugi botneti se tudi omrežje TDL uporablja za razširjanje neželene pošte in zlonamerne programske opreme, napade onemogočanja storitve (DDoS), krajo gesel in razne vrste spletnih goljufij.

GhostNet

Botnet GhostNet je bil uporabljen kot orodje za vohunjenje.

Internet je idealno orodje za vodenje vohunske dejavnosti, botnet omrežja pa predstavljajo tudi učinkovito sredstvo za pridobivanje informacij raznim tajnim službam in organizacijam, ki se ukvarjajo s podobnimi dejavnostmi.

Primer napredne zlonamerne programske kode je GhostNet, ki je v letu 2009 okužil računalnike v vsaj 103 državah (Moore, 2009). Programska koda GhostNet je bila izdelana izključno za namene vohunjenja in je bila oblikovana za napade na računalnike, ki so se nahajali v pomembnih ministrstvih in ambasadah. S pomočjo vtihotapljene programske kode so napadalci imeli celo možnost daljinskega vklopa vgrajenih mikrofonov in kamer. Primer omrežja GhostNet je tudi demonstriral, da je skoraj nemogoče izslediti takšne napadalce, še težje pa je napade dokazati. Tudi strokovnjaki, ki so analizirali omrežje GhostNet, so morali na zahtevo Republike Kitajske umakniti obtožbe, da so avtorji botnet omrežja GhostNet iz Kitajske (Savanović in Praprotnik, 2012).

Mirai

Mirai (japonsko: prihodnost) je zlonamerna programska oprema, ki omrežne naprave z operacijskim sistemom Linux spremeni v daljinsko vodene bote za uporabo pri velikih

omrežnih napadih. Namenjen je predvsem spletnim napravam, kot so IP kamere in domači usmerjevalniki (ang. home routers). Izvorna koda za Mirai je bila objavljena na forumih Hack kot odprtokodna in kasneje uporabljena v drugih zlonamernih projektih (Wikipedia, 2021).

Mirai identificira ranljive naprave IoT (ang. internet of things) z uporabo tabele z več kot 60 običajnimi tovarniško privzetimi uporabniškimi imeni in gesli ter se vanje prijavi, da jih okuži z zlonamerno programsko opremo Mirai. Okužene naprave še naprej normalno delujejo, razen občasne počasnosti in povečane uporabe pasovne širine. Naprava ostane okužena, dokler se znova ne zažene, kar lahko povzroči preprost izklop naprave in po kratkem čakanju vklop. Po ponovnem zagonu, razen če se geslo za prijavo takoj spremeni, je naprava v nekaj minutah znova okužena. Po okužbi Mirai odkrije vsako "konkurenčno" zlonamerno programsko opremo, jo odstranil iz pomnilnika in blokira vrata za oddaljeno upravljanje (Wikipedia, 2012).

Najbolj presenetljivo je, da je Mirai kreirala grupa študentov, ki se je na sodišču zagovarjala, da je želela pridobiti prednost v igri Minecraft ter da se niso zavedali, kaj so povzročili. Celo FBI-jevi preiskovalci so se strinjali, da so bili »mulci« zelo pametni, da niso naredili nič na visoki ravni in da so imeli le dobro idejo (Graff, 2017).

V osnovi je bil Mirai ustvarjen za DDoS napad na Minecraft strežnike. Ker pa je bila koda objavljena, je služila nadaljnji uporabi in se razvijala. Odkrite so bile nove različice, ki so se prav tako večinoma uporabljale za DDoS napade (Wikipedia, 2021).

 Leta 2021 so zaznali širjenje okužb s trojanskim konjem QBot. Več je opisano na: https://www.cert.si/si-cert-2021-03-sirjenje-okuzb-s-qbot-trojanskim-konjem/

3.3.3 Obramba in izzivi

Svoj računalnik lahko pred tem, da postane zombi in del botneta, zaščitimo z rednim posodabljanjem operacijskega sistema in druge programske opreme, predvsem spletnih brskalnikov. Pomemben del obrambe je protivirusna programska oprema. Žal pa uporaba protivirusne programske opreme ni nujno rešitev problema. Eden od odkritih botnetov (TDL−4 in njegove različice) namesti škodljivo kodo na zagonski sektor diska, da se zažene še pred operacijskim sistemom in protivirusnim programom. Ima lasten protivirusni program, ki poskrbi, da se računalnik ne okuži z drugim virusom ali črvom, ki bi upočasnil njegovo delovanje in posledično pripeljal do podrobnejšega iskanja nezaželenih programov. TDL-4 vzpostavi tudi posredniško funkcionalnost (t.i. proxy server), da lahko skrbniki ali kupci storitev botneta uporabljajo okužene računalnike za anonimno brskanje po internetu (http://slo-tech.com/novice/t483133, 7. 9. 2011).

Vse več je naprav, ki so povezane v omrežje internet. Govorimo o internetu stvari (ang. Internet of Things oz. IoT). To so naprave, ki so povezane na internet, npr. kamere, telefoni, žarnice, vozila, stroji … Vse te naprave so ranljive.

Okuženi računalniki predstavljajo precej trd oreh za antivirusne programe, saj njihovo učinkovito delovanje sloni na prepoznavanju „prstnih odtisov“ zlonamerne programske kode,

ki jo lahko botnet administratorji na okuženih računalnikih stalno spreminjajo. Zato običajno antivirusni programi postanejo učinkoviti šele, ko se administratorju botnet-a popolnoma onemogoči nadzor nad njegovim botnet omrežjem (Savanović in Praprotnik, 2012).

Pred tem, da bi naši računalniki postali boti, se zaščitimo predvsem s preventivo.

3.4 SOCIALNI INŽENIRING

Socialni inženiring je izraz, ki se uporablja za široko paleto zlonamernih dejavnosti, ki se izvajajo s človeškim sodelovanjem. Osnovni princip takšnih napadov je preslepiti človeka, da stori nekaj, kar mu škodi. V mnogih primerih gre za pridobivanje informacij od ljudi, se pravi od potencialnih žrtev. S temi informacijami nato izvedejo kaznivo dejanje, s katerimi oškodujejo žrtev neposredno ali posredno (npr. delodajalca).

Socialni inženiring izkorišča človeška čustva in lastnosti, npr. zaupanje, pohlep, strah, radovednost, naivnost, osamljenost.

Najbolj pogoste oblike socialnega inženiringa so:

- zvabljanje podatkov (ang. phishing),
- lažno predstavljanje (ang. impersonation),
- goljufije in prevare (ang. scam, fraud).

Preverite svoje znanje in osveščenost na: https://www.varninainternetu.si/nocnamora/.

Socialni inženiring se izvaja na različne načine. Posebna oblika telefonske prevare je klic iz neke čudne države, ki se takoj prekine. Če kličemo nazaj, plačamo drag pogovor, saj gre za plačljive linije.

Če obiščemo okuženo spletno stran, s katere zlikovci kradejo podatke, smo lahko kasneje oškodovani, saj se naši vpisi (npr. geslo, osebni podatki) zabeležijo pri kriminalcih. Skoraj vsakemu od nas so že kdaj ukradli podatke. V najboljšem primeru so nam ukradli e-poštni naslov in geslo za dostop na okuženo spletno stran. Na podlagi tega zlikovci kasneje po e-pošti izsiljujejo žrtve. Podatki uporabnikov so bili ukradeni že na mnogih znanih straneh LinedIn, Yahoo, Sony …

Na spletni strani https://haveibeenpwned.com/ (Have I been pwned?) lahko preverite, če so bili vaši podatki kdaj ukradeni in kje. Seveda pa je treba poudariti, da so podatki le za že odkrite zlorabe spletnih strani. Sklepamo, da je neodkritih zlorabljenih spletnih strani še precej. Zato je pomembno, da za različne spletne strani uporabljamo različna gesla.

3.4.1 Zvabljanje

Zvabljanja ali ribarjenje podatkov (ang. phishing) je način zavajanja uporabnikov, ki na podlagi prevare in zaupanja sami izdajo svoje osebne podatke (npr. številke kreditnih kartic, gesla, podatke o bančnih računih).

Najpogostejše sredstvo komunikacije napadalca in žrtve je elektronska pošta ali njene priloge. Običajno je goljufiva vsebina e-pošte. Žrtev stori napako, če se odzove in storilcu sporoči podatke, s katerimi le-ta nadaljuje kaznivo dejanje.

Napadalci za zvabljanje koristijo tudi SMS sporočila na mobilne telefone, okužene spletne strani in socialna omrežja. Veliko nevarnosti je na socialnih omrežjih in spletnih storitvah.

Znane so tudi telefonske prevare, kjer se kriminalci pretvarjajo, da so npr. računalniški strokovnjaki ali uslužbenci banke in skušajo s pretvezo pridobiti podatke, ki jim kasneje omogočijo krajo podatkov, izsiljevanje ali vdor v sistem.

Nekaj nasvetov za zaščito pred zvabljanjem:

- Nikoli ne vnašajmo številk kreditnih kartic, gesel in ostalih zaupnih osebnih podatkov na spletne strani, na katere smo prišli s klikom na povezavo v elektronski pošti. Verodostojne ustanove tega od svojih strank ne zahtevajo.
- Nikoli ne vnašajmo številk kreditnih kartic, gesel in ostalih zaupnih osebnih podatkov na spletne strani, na katere smo prišli s klikom na povezavo v SMS sporočilu. Tej obliki zvabljanja rečemo smishing. Smishing (kombinacija besed SMS in phishing) je poskus pridobitve osebnih, finančnih ali varnostnih informacij z uporabo SMS sporočila.
- Po telefonu ne izdajajmo podatkov, če nismo 100% prepričani, da govorimo z zaupanja vredno osebo. Ker pa se v zadnjem času izboljšujejo tehnike potvarjanja glasu in video posnetkov, tudi o tem ne moremo biti prepričani.

Prevaranti vas v sporočilih običajno prosijo, da kliknite povezavo ali pokličite telefonsko številko za "preverjanje", "posodabljanje" ali "ponovno aktiviranje" računa. Oboje vodi do zlikovca, ki od vas preko spletne strani ali telefona zvabi podatke (Europol, 2020). Banka, zavarovalnica ali druga zaupanja vredna organizacija na tak način ne komunicira s strankami.

3.4.2 Lažno prestavljanje

Lažno predstavljanje (ang. impersonation) je kibernetska prevara, s katero napadalec doseže zaupanje žrtve, ker ta meni, da je nekdo, ki ga pozna (Islovar, 2021).

Primer lažnega predstavljanja je **ponarejen profil na družbenih medijih**. Zlonamernež npr. ustvari goljufiv račun v socialnem omrežju, ki naj bi bil last uglednega posameznika iz finančne industrije, z namenom prevare potrošnikov.

Zlonamerneži kreirajo **lažne spletne strani**, ki izgledajo kot spletne strani pravih bank ali drugih finančnih institucij. Uporabijo ime domene, ki je podobno kot ime zlorabljene institucije. Nato z napadom zvabljanja (ang. phishing) od prevarane osebe pridobijo podatke. Ta napad se najpogosteje izvede preko elektronske pošte ali druge oblike sporočanja (SMS, telefon). Lažne spletne strani so videti na prvi pogled zelo podobne pravim. Zato vedno preverite URL naslov in bodite pri tem natančni!

Oblika lažnega predstavljanja, ki je mnoga podjetja stala veliko denarja, je **direktorska prevara** (ang. CEO fraud). Goljuf, ki se pretvarja za direktorja, svojemu računovodji odredi

visoko plačilo na različne račune v tujini. Računovodja, ki verjame, da je naročilo poslal direktor, izvede plačilo, podjetje pa izgubi denar. V zadnjem času je bilo na tak način oškodovanih več slovenskih podjetij za desettisoče evrov (SI-CERT, 2020).

Tovrstno goljufijo bi s preverjanjem, ki ne bi bilo preko e-pošte, lahko preprečili.

Covid-19 in delo od doma je kriminalcem olajšal posel, saj je bilo v letu 2020 veliko omejevanje fizičnih stikov, komunikacija med zaposlenimi pa je potekala po e-pošti v večjem obsegu kot prej. Napadi so tehnološko na visokem nivoju. Izkorišča se celo umetna inteligenca za popolno posnemanje nadrejenih (npr. glasu), izboljšuje se njihova uporaba lokalnega jezika in poznavanje lokalnih posebnosti. Napadajo tako velika kot mala podjetja. V zadnjem času so celo bolj na udaru mala podjetja (Europol, 2020).

Čeprav je eden najpogostejših vektorjev napada elektronska pošta, se napadalci usmerjajo tudi na druge medije. Za zvabljanje podatkov z uporabo lažnega predstavljanja uporabljajo SMS sporočila (ang. smishing), glasovno pošto ali telefonske klice (ang. vishing).

Včasih so tarče zvabljanja pomembni posamezniki, npr. poslovneži ali politiki. Takemu zvabljanju rečemo zvabljanje velikih rib (ang. whaling) (Islovar, 2021).

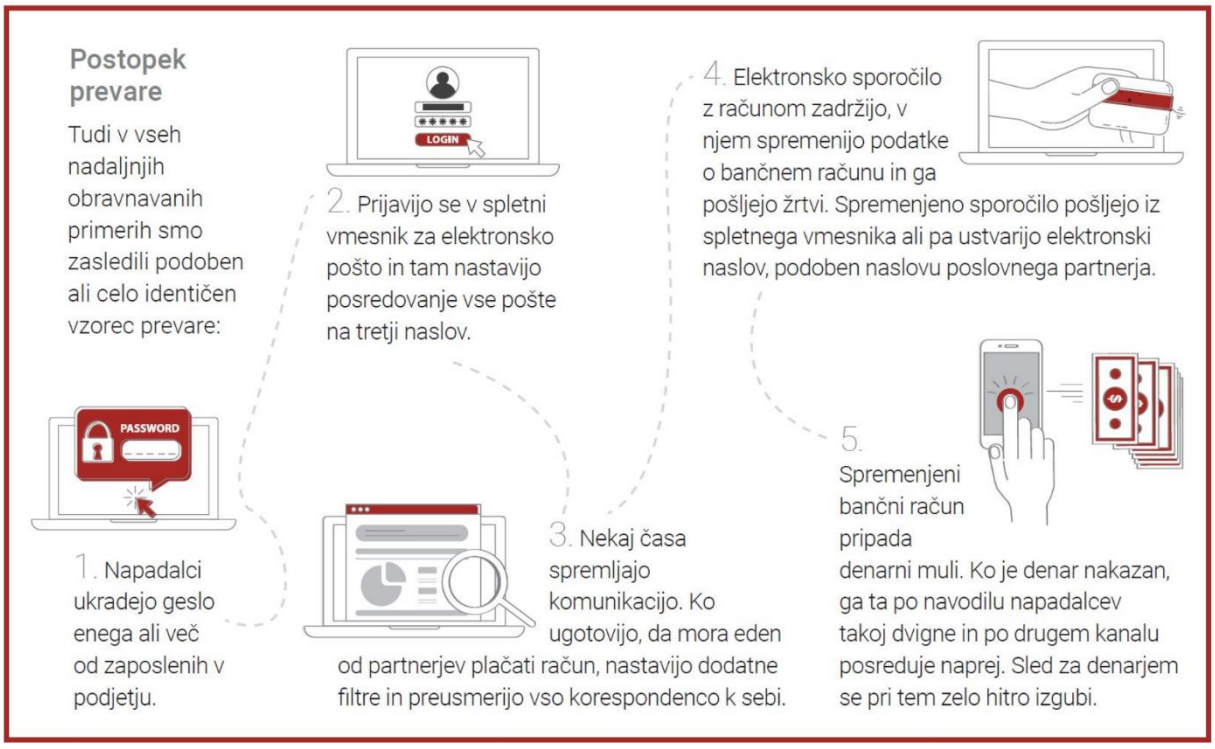
3.4.3 Vrivanje v poslovno komunikacijo

Poglejmo primer vrivanja v poslovno komunikacijo, ki poteka preko e-pošte. Angleško rečemo tej vrsti napada business email compromise.


Napad lahko poteka takole. Napadalec nekomu od zaposlenih ukrade geslo za službeno elektronsko pošto. Običajno se to zgodi preko napada zvabljanja. Nato pa se, ne da bi zaposleni karkoli posumil, prijavi v njegov spletni vmesnik za elektronsko pošto. K sebi preusmeri vso komunikacijo, ki jo prejema žrtev in zbira podatke. Ko prestreže elektronsko sporočilo s fakturo, v njej zamenja številko bančnega računa. Spremenjeno sporočilo ne vsebuje sumljivih znakov, zato žrtev ne zazna prevare in so ti napadi praviloma uspešni (SI-CERT, 2020).

Postopek je prikazan na sliki (Slika 7).

Da je nekaj narobe, se običajno posumi šele takrat, ko plačano blago ni dostavljeno ali pa poslovni partner opozori, da faktura še vedno ni plačana. Sled za denarjem je takrat že povsem izgubljena, podjetje pa čaka dolgotrajna in zapletena analiza vdora ter odprto vprašanje krivde oz. iskanja odgovornosti za nastalo škodo – ali je krivo podjetje, ki so mu vdrli v elektronsko pošto ali tisto, ki pred nakazilom ni dovolj preverilo pravilnosti bančnega računa.



Slika 7: Vrivanje v poslovno komunikacijo (https://www.cert.si/... , november 2020)

Več o teh prevarah lahko preberete na spletni strani Varni na internetu, kjer se najde veliko koristnih nasvetov: https://www.varninainternetu.si/hekerji-vdirajo-v-elektronsko-posto-slovenskih-podjetij/

Opisan postopek kibernetskega napada spada v skupino napadov **mož v sredini** (ang. man in the middle). Razen v elektronski pošti se zlikovec lahko pojavi npr. v brskalniku, kjer prestreza podatke, ki se prenašajo med oddajnikom in sprejemnikom sporočil. To bi bilo lahko npr. med komitentom in banko.

Napad človek v sredini je vrsta napada, pri katerem se napadalci vrinejo in prekinejo obstoječi pogovor ali prenos podatkov zaradi izvedbe nezakonitega pridobivanja podatkov. Take vrste napad je tehnično napreden, a ga brez pomoči človeka (žrtve) ni mogoče izpeljati.

3.4.4 Kraja podatkov za e-bančništvo

Kibernetski kriminalci, ki želijo krasti denar z zlorabo e-bančnih storitev, lahko izbirajo med dvema osnovnima možnostma:

- poskušajo zlorabiti informacijski sistem (IS) banke,
- zlorabiti komitenta (uporabnika) oz. njegov informacijski sistem.

Ker je banka težji oreh, se običajno lotijo komitentov in skušajo s pomočjo zvabljanja od njih pridobiti podatke za dostop do bančnih računov.

Da bi zmanjšali možnosti kraje denarja z računov, so banke uvedle dodatne zaščitne ukrepe. V e-banko se prijavimo z geslom, nato pa vsako transakcijo ponovno potrdimo z geslom, ki ga generiramo na zunanji napravi (npr. telefonu) in mu rok trajanja hitro poteče.

Zavedati se moramo, da 100 % varnosti na internetu, ni. Podobno velja tudi na drugih področjih v življenju. Vendar pa lahko uporabniki s previdnim in preudarnim spletnim obnašanjem največ storimo za lastno varnost. Zavedati se moramo, da ni enega samega magičnega programa, ki bi nas v celoti zaščitil pred nevarnostmi in zagotovil varno elektronsko bančništvo. Upoštevati moramo več korakov oz. postopkov, ki jih lahko najdemo tudi na povezavi projekta Varni na internetu: https://www.varninainternetu.si/nasveti-za-varno-spletno-bancnistvo/.

Banke uporabljajo za zaščito transakcij e-bančništva naslednji pristop: »nekaj, kar veš in nekaj, kar imaš«.

Pri eni obliki je nekaj, kar veš, naše geslo, nekaj, kar imaš pa digitalni certifikat. Za dostop do uporabnikovega e-računa bi goljuf potreboval tako njegovo geslo kot tudi digitalni certifikat. In najpogosteje ju pridobi prek okužbe z zlonamerno kodo. Gre za specializirane programe (trojance), ki beležijo pritiske tipk (t.i. keylogger), nato pa napadalcu pošljejo shranjena in prestrežena gesla z računalnika. Trojanec napadalcu pošlje tudi digitalni certifikat, če je le-ta shranjen na računalniku. Žal ima veliko uporabnikov digitalni certifikat shranjen na disku računalnika. Banke so to slabost skušale zmanjšati s tem, da je po vstopu z digitalnim certifikatom potrebno vnesti še enkratno geslo, ki se generira z dvema podatkoma: enega ima uporabnik, drugega pa banka.

Pametno je, da digitalni certifikat hranimo na pametni kartici ali pametnem USB ključu. To je posebna naprava, ki je namenjena samo shranjevanju digitalnih certifikatov, iz katere certifikata ni mogoče prekopirati. Ko končamo z uporabo elektronskega bančništva, kartico ali USB ključ iztaknemo iz računalnika. Računalnik, na katerem uporabljamo elektronsko banko, ugasnemo, ko ga ne uporabljamo.

Pri drugi obliki elektronskega bančništva je nekaj, kar veš, geslo, nekaj, kar imaš pa generator gesel (posebna naprava ali mobilni telefon), ki ob vstopu v e-banko vedno znova ustvari naključno enkratno geslo. V tem primeru je možnost zlorabe manjša kot ob uporabi digitalnega certifikata.

Uporabniki elektronskega bančništva moramo vedno upoštevati osnovna varnostna priporočila, ne glede na to, katero obliko elektronskega bančništva uporabljamo:

- redno posodabljamo tako operacijski sistem kot vse nameščene programe,
- redno posodabljamo brskalnik in vse njegove vtičnike,
- nameščen imamo antivirusni program in vklopljen požarni zid.

Zavedati se moramo, da antivirusni programi nikoli ne prestrežejo vse škodljive kode, zato je potrebno tudi ustrezno obnašanje, ki zmanjša možnost zlorabe.

Jasno je tudi, da nikoli in nikomur ne zaupamo svojega gesla za dostop do e-banke! Prav tako nikoli ne pošiljamo občutljivih podatkov (številka kartice, digitalno potrdilo ipd.) prek elektronske pošte (Varni na internetu, 2018).

Uporabniki imajo na voljo več načinov obvarovanja pred okužbo. Med temi načini so varnostne posodobitve brskalnikov in operacijskega sistema, protivirusna programska oprema, požarni zid, omrežni usmerjevalnik in skrbno preverjanje, kaj uporabnik namešča na sistem (Vodopivec, 2010).

Okuženega uporabnika pred zlorabo lahko zaščiti banka s potrjevanjem transakcije na podlagi dejanskih podatkov o njej in po kanalu, ki ni pod nadzorom napadalca. Banke tako potrjevanje uvajajo, na primer s:

- kriptografskim podpisovanjem transakcij na napravi, ki je povsem ločena od računalnika (in je napadalec ne more imeti pod kontrolo) – generiranje podpisne kode, ki je odvisna od parametrov transakcije; nato vnos te kode v računalnik,
- pošiljanje SMS sporočila s podrobnostmi transakcije uporabniku, ki nato transakcijo preveri in potrdi (pomanjkljivost te rešitve je, da bi lahko napadalec okužil tudi uporabnikove mobilne naprave),
- telefonska verifikacija transakcije (banka uporabnika pokliče na znano telefonsko številko).

Vse te možnosti za uporabnika predstavljajo dodatne neprijetnosti, a povečujejo verjetnost, da ne pride do zlorabe.

3.4.5 Prevare in goljufije

Ker so tehnična zaščitna sredstva dokaj učinkovita, jih skušajo zlikovci obiti z neposredno komunikacijo s potencialno žrtvijo. Poskusi goljufij so običajni tudi v realnem svetu. V računalniškem okolju je število potencialnih žrtev ogromno, s tem pa je za kriminalce večja možnost, da kdo nasede.

Najpomembnejši cilj posameznih kriminalcev in kriminalnih združb je protipravna pridobitev finančnih sredstev. Zato se poslužujejo različnih prevar, ki jih bomo opisali v nadaljevanju.

Prevaranti so na preži povsod na spletu. Prežijo na iskalce najemniških stanovanj, kupce avtomobilov in plovil, ljubitelje domačih živali. Skoraj ni človekove aktivnosti, kjer ni v bližini kakšnega prevaranta. V goljufivih oglasih pogosto uporabljajo ukradene ali prekopirane fotografije s spleta.

Direktorske prevare

To je prevara, usmerjena na podjetja in organizacije. Storilci kaznivih dejanj uporabljajo tehnike socialnega inženiringa za dostop do podatkov in e-pošte tistih zaposlenih, ki jih za zlorabo potrebujejo.

V bistvu gre za goljufiva elektronska sporočila, ki se jih je prijelo ime “direktorske prevare” (ang. CEO Frauds). Goljuf se pretvarja, da je direktor in svojemu računovodji odredi visoko plačilo na različne račune v tujini. Računovodja, ki verjame, da je navodilo poslal direktor, izvede plačilo, podjetje pa izgubi denar. V zadnjem času je bilo iz celotne Slovenije na tak način oškodovanih že več slovenskih podjetij. Direktorske prevare so posamezna podjetja oškodovala

za nekaj deset tisoč evrov, v dveh primerih pa tudi več kot 100.000 evrov. (www.cert.si, 19. 8. 2019).

To goljufijo bi s preverjanjem, ki ne bi bilo preko e-pošte, lahko preprečili. Nekatere prevare pa so mnogo bolj izpopolnjene.

Investicijske prevare

Investicijske ali naložbene prevare (an. investment fraud) se nanašajo na poskuse goljufij, kjer kriminalci želijo od svoje žrtve zvabiti denar z oglaševanjem privlačnih shem hitrega bogatenja.

Zlikovci obljubljajo žrtvam izredne finančne donose z vlaganjem v sredstva, kot so npr. kriptovalute, diamanti ali zlato. Če žrtev nasede in vplača denar, začno prikazovati lažno stanje portfelja. Žrtev spremlja navidezno rast svoje investicije in se veseli dobre naložbe. Lahko se zgodi, da na zahtevo žrtve manjši znesek celo izplačajo, da se zdijo stvari resne. Če pa žrtev zahteva večje izplačilo iz svoje investicije, se komunikacija prekine. Lažna spletna stran sčasoma izgine. Žrtve pa ostanejo brez investiranih sredstev.

Nekatere žrtve na ta način izgubijo življenjske prihranke.

Oglasi za te »super« naložbe se prikradejo na zaupanja vredne spletne strani in na socialna omrežja. Izrabijo se znane osebnosti, ki v oglasih razlagajo, kako so obogatele. V resnici je vse zmontirano in poneverjeno. Poneverbe postajajo vse bolj avtentične, saj z uporabo sintetičnih vsebin (ang. deepfake) dosežejo izjemni učinek avtentičnosti.

Poseben primer naložbenih prevar so piramidne sheme. Pojavljajo se tako v povezavi s klasičnimi valutami kot kriptovalutami. Eno največjih tovrstnih prevar je izvedel znani in v preteklosti ugleden finančnik Robert Madoff. Njegovo prevarantsko početje je trajalo kar 30 let, saj so mu vlagatelji zaupali in niso potrebovali denarja. Šele finančna kriza l. 2008, ko je veliko investitorjev potrebovalo denar in ga želelo dvigniti je pokazala, da je šlo za obsežno prevaro (Pavlič, 2021). To je primer prevare, ki se ji težko izognemo. Madoff je obljubljal relativno nizke donose in celo nadzorni organ SEC (The U.S. Securities and Exchange Commission - Ameriška Komisija za vrednostne papirje in borzo) njegove dejavnosti ni pravočasno zaznal kot prevaro. Običajno so prevarantske sheme mnogo bolj očitne, saj obljubljajo nerealne donose.

Za finančne prevare so zelo primerne kriptovalute, saj so zakonsko neregulirane, ljudje pa o njih malo vedo. Primer takšne prevare je lažna kriptovaluta Onecoin. Ocenjujejo, da se je v finančno prevaro s to navidezno kriptovaluto ujelo okrog 14 tisoč Slovencev. Kar 3,6 milijonov ljudi po svetu ni prepoznalo znakov prevare. Strokovnjaki pravijo, da so obstajali jasni indici, da gre za prevaro. Finančno bolj izobraženi in osveščeni posamezniki so bili do teh ponudb skeptični. Pristopi goljufov so pogosto inovativni in prepričljivi, zaradi česar je prevaro včasih težko prepoznati. Ljudje so od OneCoina kupovali izobraževalne pakete in glede na vložek dobili ustrezno število fiktivnih žetonov za rudarjenje istoimenske valute, ki sploh ni obstajala. Leta 2016 so jim prevaranti podvojili stanje na navideznih računih. Vlagatelji so imeli lažni vtis, da njihovo imetje raste. Kasneje se je izkazalo, da denarja ni več in da vlagatelji verjetno nikoli ne bodo prejeli niti dela vloženega denarja (Tomšič, 2019).

Kriptovaluto Xaurum so promovirali kot kriptovaluto, ki temelji na zlatih rezervah. Strokovnjaki so opozarjali, da lahko zlato kupi vsak vlagatelj sam in gre verjetno za prevaro, a to ni zaustavilo organizatorjev, ki so svojo prevarantsko shemo reklamirali celo v slovenskih medijih. Vlagatelji v Xaurum danes nimajo niti zlata, niti zagotovila, da bo njihova naložba kdaj povrnjena.

Za investitorje so velika tveganja kripto kovanci, ki jih izdajajo za financiranje projektov.

Prve izdaje kripto kovancev (ICO – Initial Coin Offerings) so zelo pogosta oblika financiranja novonastalih podjetij in njihovih projektov. Kljub izjemno velikim tveganjem, tak način financiranja raste (Shephard, 2019). ICO naložbe potekajo tako, da se v zameno za pravo denarno valuto izdajo digitalni žetoni ali kovanci, ki jih v prihodnosti lahko - ali pa tudi ne - uporabimo za nakup določenega blaga ali storitve. Raziskovalci trdijo, da gre v okrog 80% teh izdaj za prevare (DeLisle, 2018). Veliko tistih, ki imajo poštene namene, v poslovnem svetu ne uspe. Ocenjujejo, da je samo okrog 3 % tovrstnih projektov poštenih in uspešnih. Zato je vlaganje v kovance, ki se reklamirajo kot kriptovalute, izjemno tvegano in skoraj zanesljivo pomeni izgubo denarja.

Prve izdaje kovancev niso registrirane kot vrednostni papirji, zato vlagatelji nimajo nobene pravne zaščite. Večina temelji na poslovnem modelu, katerega cilj je vlagatelje ogoljufati za denar. Tudi v primeru, da so nameni izdajateljev pošteni, gre za financiranje startup podjetij, za katere je velika verjetnost, da poslovno ne preživijo. Po ocenah na osnovi podatkov iz ZDA naj bi le 10% novonastalih podjetij preživelo (Bryant, 2020).

Oglasi za te »super« naložbe se prikradejo na zaupanja vredne spletne strani in na socialna omrežja. Izrabijo se znane osebnosti, ki v oglasih razlagajo, kako so obogatele. V resnici je vse zlagano in narejeno z namenom, da se preslepi potencialnega vlagatelja.

Lažni krediti

Marsikdo se znajde v denarnih težavah, banka pa mu noče odobriti kredita. Takšni ljudje so idealna tarča za spletne goljufe. Ti namreč na spletu ponujajo lažne kredite, ki na prvi pogled izgledajo predobri, da bi bili resnični!

Vedno bodite previdni, ko nekdo na spletu (Facebook, Instagram, email), obljublja denar! Goljufi brez kakršnihkoli dokazil dajejo velike obljube, pošljejo pa nič!

Ves čas dopisovanja od žrtve želijo poplačilo raznih stroškov, po plačilu katerih naj bi prejeli kredit. Posledično žrtev neprestano plačuje, na koncu pa ostane praznih rok, s še več denarnimi težavami.

Kako prepoznamo lažni spletni kredit? Sumljivi znaki so:

- super pogoji,
- nizka obrestna mera,
- dolga odplačilna doba,
- takojšnje izplačilo,
- vnaprejšnje plačilo za razne stroške.

Kadarkoli je treba najprej nakazati denar, da bi kasneje denar dobil, je to znak za goljufijo!

Za še več trikov in nasvetov obiščite www.varninainternetu.si

Denarne mule

Kriminalci, ki preko interneta izvabljajo denar od žrtev, potrebujejo bančne račune za nakazilo protizakonito pridobljenega denarja. Njihov lastni računi niso primerni, saj bi jih preko njih enostavno odkrili. Zaradi tega potrebujejo sodelavce, ki jim za provizijo posodijo svoje bančne račune. Take sodelavce imenujemo denarne mule.

Denarne mule so posredniki, ki jih kriminalne organizacije uporabljajo v transakcijah nezakonito pridobljenih sredstev. Pomagajo jim pri prenosu denarja med bančnimi računi ali državami. Na tak način kriminalne organizacije perejo denar.

Denar oziroma premoženje, ki je pridobljeno s storitvijo kaznivih dejanj je "umazan denar". Denar je "opran", ko je njegov pravi izvor prikrit in pridobi vse lastnosti zakonito pridobljenega premoženja. Končni cilj pranja denarja je postopna vključitev "opranega" denarja v običajne finančne tokove, ki so sestavni del zakonite poslovne dejavnosti ali ponovno investiranje v kriminalno dejavnost (https://www.gov.si, 2019).

Organi pregona najprej izsledijo imetnika bančnega računa, ki se uporablja za pranje denarja. Europol opozarja, da denarne mule zagrešijo kaznivo dejanje, čeprav to storijo iz naivnosti. Utrpijo lahko različne posledice, tudi daljše zaporne kazni. V decembru 2019 je bilo s strani Europola objavljeno, da so odkrili 3833 denarnih mul in 386 tistih, ki so jih novačili. Po navedbah slovenske policije so osumljeni iz Slovenije (med njimi tudi tujci) večinoma prali denar, pridobljen iz kaznivih dejanj računalniške kriminalitete, kot so vdori v informacijske sisteme, zvabljanje podatkov in različne oblike spletnih goljufij (npr. nigerijske prevare, direktorske prevare in druge poslovne goljufije).

Leta 2019 je bilo po navedbah Europola opaziti, da kriminalci vse pogosteje pridobivajo svoje žrtve na spletnih straneh za zmenke in jih čez čas prepričajo, da odprejo bančni račun za prejemanje in nakazovanje denarja. Vse pogosteje uporabljajo tudi družbena omrežja in žrtve privabljajo z oglasi, ki obljubljajo hiter zaslužek. Ta tehnika je še posebej priljubljena za privabljanje mladih in študentov (Europol, 2019).

Da bi ljudi bolje seznanili s tem načinom prevar, so po Evropi decembra 2019 zagnali kampanjo osveščanja o denarnih mulah #dontbeaMule (#nebodimula). Gradivo, ki je na voljo v 25 jezikih, javnost seznanja z delovanjem kriminalcev, ki novačijo denarne mule, kako se lahko potencialna žrtev zaščiti ter kaj lahko stori, če postane žrtev (Europol, 2019).

Tudi slovenska policija opominja: "pomembno je, da se državljani zavedajo dejstva, da posameznik, ki na svoj bančni račun prejme denarna sredstva, za katera ve ali pa bi moral in mogel vedeti, da so bila pridobljena s kaznivimi dejanji, nato pa jih na zahtevo take osebe prenakaže na drug transakcijski račun ali jih dvigne v gotovini, jih uporabi pri gospodarski dejavnosti in s temi dejanji zakrije izvor sredstev, stori kaznivo dejanje pranja denarja."

Ljubezenske prevare

Na spletu so prevaranti, ki izkoriščajo osamljene, romantičnih stikov željne osebe in z njimi navežejo stike. Z njimi komunicirajo dlje časa, vzpostavijo prijateljski odnos, rodijo se čustva, nato pa sledijo finančne zahteve. Praviloma ne gre za izsiljevanje, saj žrtve same želijo pomagati in nakažejo veliko denarja preden se zavejo, da njihov romantični ljubimec ni nič drugega kot lažnivec in prevarant.

Tipične zgodbe so podobne sledečim. Ljubimci so zdravnik v Siriji, marinec na mirovni misiji v Iraku, ovdovel delavec na naftni ploščadi in podobni šarmantni gospodje z zlomljenim srcem, ki na spletu iščejo damo, ki jih bo razumela. To bi lahko bil začetek velike ljubezenske zgodbe, a je vse prej kot to. Osamljene ženske, ki so se na spletu zapletle s šarmantnimi tujci, so po letu dni 'razmerja' na daljavo ostale brez nekaj deset tisoč, nekatere celo brez več kot sto tisoč evrov (Varni na internetu, 2021).

Običajno se stiki začno na družbenih omrežjih, npr. na Facebooku ali Instagramu. Prevaranti pošljejo prošnjo za prijateljstvo. To je posebna oblika zvabljanja, ki ji rečemo catphishing.

Več najdete: https://www.varninainternetu.si/ljubezenska-prevara/

Lažne spletne trgovine in prevare pri spletnem nakupovanju

Kot pri večini prevar, je ponudba izjemno privlačna. Problem nastopi, ko naročenega izdelka ne dobimo. Razen tega goljufom razkrijemo osebne podatke, ki jih lahko uporabijo za prodajo kriminalnih združbam in/ali za pošiljanje novih prevarantskih predlogov.

Nekatere spletne trgovine ponujajo izdelke znanih blagovnih znamk po izjemno ugodnih cenah. V večini primerov gre za trgovine s ponaredki. Naročeno blago pošljejo, a ga na carini zasežejo. Kupec ostane brez denarja ter brez blaga in je lahko vesel, če ne plača še kazni.

Prevare s plačilnimi karticami

Prevare s plačilnimi karticami se izvedejo tam, kjer ob izvedbi transakcije kartica ni nujno fizično prisotna (ang. card-not-present), npr. pri nakupu v spletni trgovini.

Znani sta dve vrsti takih prevar.

Prvi način imenujemo z angleško besedo carding. Nanaša na uporabo ukradenih podatkov plačilne kartice za nakup blaga ali storitev. Kriminalci te podatke pridobivajo na različne načine (npr. z zvabljanjem ali krajo z nezaščitenih ali slabo zaščitenih spletnih mest), jih prodajajo in kupujejo na temnem spletu (ang. darknet).

Drugi način je elektronsko posnemanje (ang. E-skimming).

Skimming oz. posnemanje je neke vrste kopiranje podatkov s kartic. Kriminalec namesti posebno napravo (ang. skimmer) na delujoč bankomat. Ko vanj vstavite bančno kartico, skimmer zapiše podatke, kamera pa posname PIN kodo, ki ste jo vnesli. Ko imajo nepridipravi podatke o kartici in vašo PIN kodo, je zloraba vašega bančnega računa zanje enostavna. Te

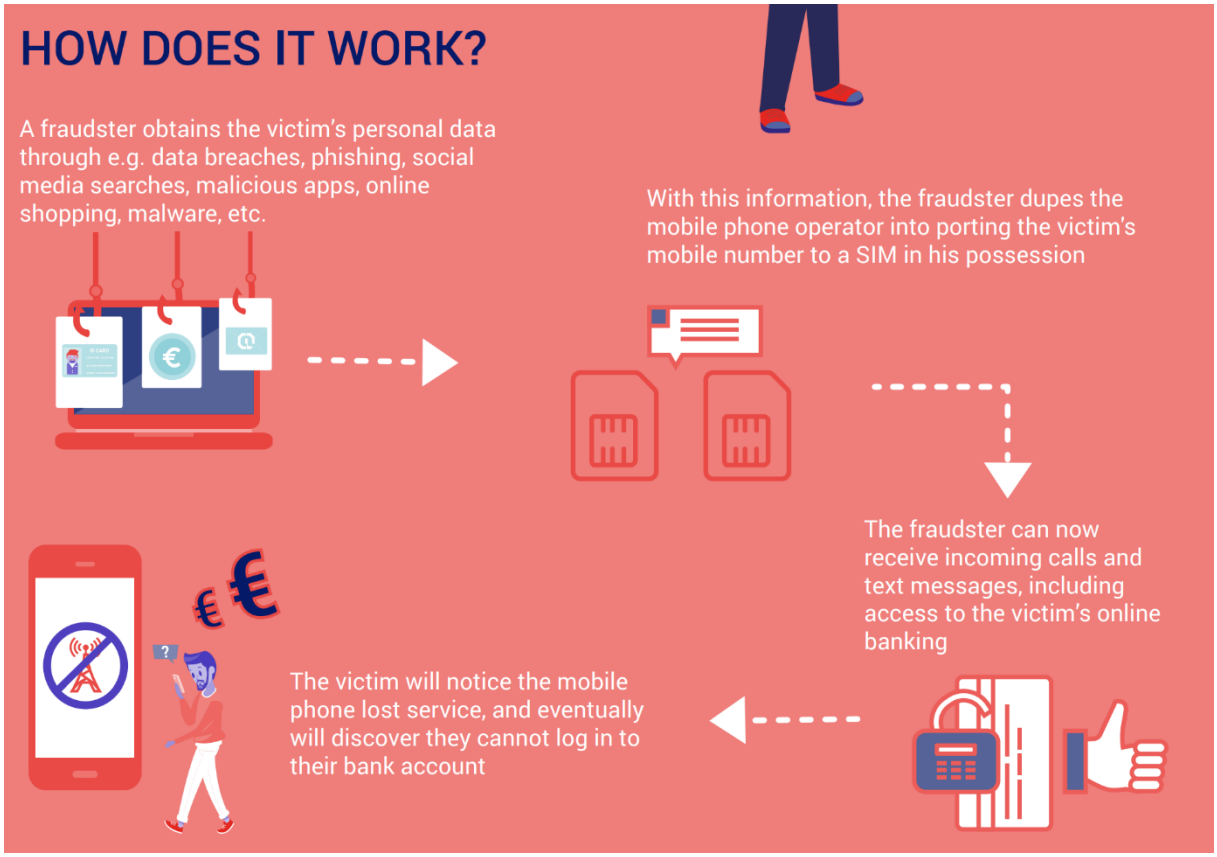
napravice so tako majhne, da jih je težko opaziti. Zato s prosto roko vedno zakrijte tipkovnico, s katero vpisujete PIN kodo.

Elektronsko posnemanje (ang. E-skimming) pa je oblika napada, kjer zlikovec namesti škodljivo kodo v spletno trgovino. Ko kupec vnese podatke, jih zlikovci prekopirajo in kasneje uporabijo za različna kazniva dejanja ali jih prodajo. Kupec prejme naročene izdelke in plačilo se normalno izvede. Zato žrtve (v tem primeru spletna trgovina in kupec) dolgo ne vedo, da so oškodovani. Ko bo kupec kasneje oškodovan, ne bo niti vedel, na kateri slabo zaščiteni spletni strani so bili ukradeni njegovi podatki.

Zamenjava SIM kartice

SIM kartice so za kriminalce zanimive, saj v zadnjem času mnogi uporabljajo mobilni telefon za plačevanje (npr. s storitvami kot so Valu, Flik, ApplePay) ali kot generator enkratnega gesla za potrjevanje transakcij.

Europol je v letu 2020 zaznal znaten porast tovrstnih kriminalnih dejanj.



Slika 8: Zamenjava SIM kartice
(Europol, 2020)

Zamenjava kartice SIM (ang. SIM swapping) je vrsta prevzema računa, ki se nanaša na izogibanje dvofaktorski avtentikaciji (2FA) na osnovi SMS, za dostop do občutljivih uporabniških računov. Kriminalci z goljufijo zamenjajo kartico ali povežejo podatke na kartico zločinca zaradi prestrezanja enkratnega gesla v postopku preverjanja pristnosti. S tem pridobijo

popoln nadzor nad žrtvino banko, e-pošto in stiki, kar jim posledično omogoči številna kazniva dejanja.

Na sliki (Slika 8) je nazoren potek goljufije.

Če ugotovite, da se vaš telefon ne odziva in za to ni očitnega razloga, je morebiten razlog zamenjava SIM kartice. Vaša je bila morda preklicana, delujoči dvojnik pa že ima kriminalec. Pri svojem ponudniku mobilne telefonije preverite, če je bil SIM zamenjan in če je bil, takoj prekličite vse svoje kartice in obvestite policijo.

Sintetične vsebine

Lažne vsebine na socialnih omrežjih in drugih medijih so vedno večji problem. Poslužujejo se jih razni teoretiki zarot, hektivisti (aktivisti, ki za promocijo svojih stališč ali doseganje političnih ciljev uporabljajo hekerska dejanja), finančni in drugi goljufi.

Tehnološko napredni kriminalci ustvarjajo **sintetične vsebine** ali globoke ponaredke (ang. deepfake). To so lažna in goljufiva besedilna, slikovna, zvočna ali video sporočila, ki so ustvarjena z umetno inteligenco ali strojnim učenjem.

Izraz deepfake je nastal iz sestavljanke deep learning (globoko učenje) in fake (ponaredek). Gre za umetno narejeno vsebino.

Ponarejanje vsebine ni nekaj novega. Vendar pa globoki ponaredki uporabljajo napredne tehnike strojnega učenja in umetne inteligence za manipulacijo ali ustvarjanje vizualnih in zvočnih vsebin z velikim potencialom za prevaro. Glavne metode strojnega učenja, ki se uporabljajo za ustvarjanje globokih ponaredkov, temeljijo na globokem učenju in nevronskih mrežah (Wikipedia, 2021).

 Obstaja preprost način, s katerim hitro preverimo pristnost fotografij. S pomočjo funkcije vzvratno iskanje fotografij (ang. reverse image search) lahko preverimo, ali gre za spletno prevaro. V iskalnik Google vpišemo iskanje slik, kliknemo na ikono fotoaparata in z miško prenesemo želeno fotografijo v polje. Iskalnik Google pomaga odkriti, če se sumljive fotografije pojavljajo še v kakšnih sumljivih oglasih, in ali gre verjetno za prevaro (Varni na internetu, 2021).

3.5 PRIPRAVE NA VDOR IN VDOR V SISTEM

Kibernetski vdor (ang. cyber intrusion) je vsako nepooblaščeno dejanje, ki ogrozi varnost sistema in ga postavi v negotovo oz. ranljivo stanje. Dejanje vdora ali pridobivanja nepooblaščenega dostopa do sistema običajno pusti sledi, ki jih lahko odkrijejo sistemi za odkrivanje vdorov (ang. Intrusion Detection Systems - IDS).

IDS je varnostno orodje, ki naj bi:

- zaznalo prisotnost vsiljivcev ali pojav varnostnih kršitev in o tem obvestilo skrbnike,
- omogočilo beleženje varnostnih kršitev,

- sprožilo odziv, na primer prekinitev seje ali blokiranje naslova IP.

IDS velja za bolj pasivno varnostno orodje, saj zazna kršitve, ko se že pojavijo in jih ne preprečuje (Whitman in Mattord, 2019).

Zaščita pred večino napadov na podatke temelji na uporabi šifriranja. Šifrirni algoritmi, ki so v uporabi, so večinoma močni in jih običajno praktično ni mogoče direktno razbiti. Vendar je šifriranje učinkovito le, če ni nepooblaščenega dostopa do šifrirnih ključev. Zaradi tega so nevarni aktivni napadi za pridobitev nepooblaščenega dostopa do virov/informacij v sistemu. Vdori so pomembni za napadalca in kritični za žrtev, ker:

- lahko obidejo zaščito na osnovi šifriranja,
- omogočajo neposredne zlorabe podatkov,
- so odskočna deska za druge vrste napadov/zlorab (Savanović in Praprotnik, 2012).

Vdor pogosto ni primarni cilj napadalca, temveč le prvi korak do dejanskega napada. Pri tem je pomembno poudariti, da napadalci vse bolj pogosto kot odskočno desko za dejanski napad na primarno žrtev uporabljajo vmesne naprave (računalnike), v katere je mogoče vdreti. **Potencialna žrtev računalniških vdorov je lahko vsaka računalniška naprava** (vključno z napravami bralca tega gradiva)**,** pa naj se njenemu lastniku ta naprava zdi še tako nepomembna in nezanimiva za napadalce (Savanović in Praprotnik, 2012).

Vdore lahko razdelimo v štiri večje skupine glede na to, kako napadalci poskušajo vdreti v sistem (Savanović in Praprotnik, 2012):

- preslepijo uporabnika, da prostovoljno preda podatke (npr. uporabniško ime, geslo) − tehnika socialnega inženiringa,
- razbitje šibkega sistema overjanja, npr. gesla − napad z grobo silo (ang. brute force napad),
- izraba znanih ali še neodkritih slabosti v zasnovi ali implementaciji protokolov in sistemov,
- programska oprema (večinoma) ali strojna oprema (redkeje).

Vdori potekajo v več oblikahskeniranje (Savanović in Praprotnik, 2012):

- zbiranje podatkov,
- skeniranje,
- namestitev zlonamernih programov,
- odpravljanje sledi,
- izvedba dejanskega napada.

Vsekakor je potrebno poudariti, da tarče večinoma niso vnaprej izbrane. Tarča je dejansko vsak sistem in vsak posameznik, ki uporablja računalnik in internet.

3.5.1 Zbiranje podatkov

Prva faza v pripravi na izvedbo vdora je osnovno zbiranje podatkov o ciljnem sistemu oz. žrtvi. Pri tem se uporabljajo vsi mogoči viri informacij, tako klasični kot elektronski, npr. spletne strani in družbeni mediji, javne baze s podatki o lastnikih posameznih internetnih domen in javnih IP naslovov. V skrajnem primeru, ko gre za izbrano tarčo, lahko napadalec pridobiva pomembne informacije tudi z brskanjem po odpadkih ali fizičnim vdorom v poslovne ali zasebne prostore žrtve.

Cilj prve faze je pridobiti čim več informacij, npr. IP naslove in imena (kontaktnih) uporabnikov sistema (Savanović in Praprotnik, 2012).

Pogosto napadalci pridobijo podatke na napadenih spletnih straneh.

3.5.2 Skeniranje

Skeniranje ali tipanje (ang. scanning) je zaznavanje lastnosti in stanja računalniškega sistema, da bi se odkrilo njegove ranljivosti. Izvede ga napadalec ali skrbnik sistema. Skeniranje lastnega omrežja je pomembna dejavnost skrbnikov informacijskih sistemov, da sami odkrijejo morebitne ranljivosti v sistemu.

Skeniranje obsega: skeniranje omrežja, vrat (ang. port) in ranljivosti programske opreme (operacijskega sistema, brskalnikov, aplikativne opreme).

Skeniranje omrežja pomaga odkriti delujoče uporabniške računalnike in strežnike, odprta vrata in IP naslove žrtve. Omogoča odkrivanje storitev, ki se izvajajo v sistemu ter arhitekture omrežja.

Skeniranje vrat (ang. port scanning) je metoda, ki se uporablja za iskanje odprtih UDP ali TCP vrat, od koder bi heker lahko dostopal do sistema organizacije. Z natančnim popisovanjem oz. mapiranjem (ang. mapping) omrežja napadalec pridobi informacije o tem, kateri IP naslovi delujejo (delujoči strežniki ali odjemalci), katera vrata (port number) na teh IP naslovih so odprta, itd.

Ko je omrežje popisano, se napadalec loti iskanja ranljivosti na ta način, da od delujočih sistemov poskuša pridobiti informacije o vrstah in verzijah programske opreme (operacijski sistem, posamezne aplikacije, popravki aplikacij) na teh računalnikih (Savanović in Praprotnik, 2012).

Skeniranje obsega tri različne korake, ki niso nujno povsem ločeni in s katerimi napadalec poskuša v žrtvinem sistemu najti vsaj eno od že znanih ranljivosti, tj. takih slabosti oz. varnostnih lukenj, ki jih je mogoče relativno enostavno zlorabiti za vdor v sistem. Za znane ranljivosti namreč že obstajajo dokumentirani postopki in orodja za izvedbo vdora na osnovi take ranljivosti (Savanović in Praprotnik, 2012).

Zloraba omrežja je npr. prisluškovanje (ang. sniffing). To je prestrezanje podatkovnih paketov pri prenosu v omrežju, npr. za pridobivanje gesla.

3.5.3 Namestitev zlonamernih programov

Napadalec na kompromitirani sistem namesti zlonamerne programe, ki mu kasneje omogočajo (Savanović in Praprotnik, 2012):

- enostaven in nepooblaščen vstop v sistem tudi v primeru, če se kasneje spremenijo uporabniška imena in gesla v sistemu,
- (redne) zlorabe kompromitiranega sistema v različne namene, npr. za izvajanje DDoS napadov, pošiljanje nezaželene pošte (spam) ali shranjevanje ilegalnih vsebin

3.5.4 Odpravljanje sledi in slabosti

V tej fazi napadalec poskrbi, da čimbolj temeljito

- zabriše vse sledi pravkar izvedenega vdora in
- namesti vse potrebne varnostne popravke in zaščite, tj. »pokrpa« kompromitirani sistem in s tem odpravi vse ranljivosti, ki bi omogočale kasnejši(e) vdor(e) s strani drugih napadalcev (Savanović in Praprotnik, 2012).

S prvim ukrepom napadalec zaščiti »sadove svojega dela«, saj bi bil ves njegov trud zaman, če bi žrtev odkrila vdor in odpravila njegove posledice ter tako napadalcu preprečila nadaljnjo zlorabo sistema. Drugi ukrep ima enak cilj in tako ni presenetljiv, čeprav je na prvi pogled precej nenavaden in predvsem zelo ironičen. Napadalec v bistvu zelo vestno opravi delo, ki ga že prej očitno ni dovolj vestno opravil njegov »naravni sovražnik« administrator sistema, da bi napadalcu preprečil vdor v sistem. Razlika je le v tem, da se s tem ukrepom napadalec zaščiti pred drugimi napadalci, ki bi lahko s kasnejšim vdorom prevzeli žrtev v svojo korist ali pa bi lahko z malomarnostjo izdali vdor v sistem (Savanović in Praprotnik, 2012).

3.5.5 Izvedba dejanskega napada

Zadnja faza je lahko izvedba dejanskega napada, saj vdor pogosto ni glavni namen pač pa je le odskočna deska za dejanski napad, ki je glavni oz. končni cilj napadalca.

Dejanski napad se lahko izvede bodisi na sam kompromitirani sistem (npr. kraja ali brisanje podatkov), bodisi s kompromitiranega sistema na nek drug sistem (npr. onesposabljanje strežnika z DDoS napadom). Pri tem lahko napadalec izvede tudi verižne vdore, kjer v več etapah (vdor s prvega sistema v drugi, z drugega v tretji, itd.) pridobi nepooblaščen dostop v ciljni sistem. Tak pristop bolj zabriše sledi o izvoru napada in oteži forenziko, tj. iskanje dokazov o okoliščinah in izvoru napada (Savanović in Praprotnik, 2012).

3.6 SLEDENJE IN PROFILI UPORABNIKOV

V nasprotju z doslej opisanimi grožnjami se naslednje dejavnosti pogosto pojmujejo kot koristne in ne kot sporne dejavnosti oz. resna grožnja za uporabnikovo zasebnost:

- sledenje uporabnikovim aktivnostim na internetu,

- zbiranje teh podatkov na različnih mestih ter
- izmenjava in povezovanje zbranih podatkov z različnih mest v enoten in zelo podroben profil uporabnika,

Posameznike bolj skrbi, kaj bi vedela država o njih, kot kaj o njih ve Google in drugi ponudniki, ki zahtevajo ali ponujajo vklop aplikacijskih storitev in vpis drugi osebnih podatkov.

Razlogov za to neprimerno stanje je več, med glavnimi pa bi lahko bili:

- ponudniki internetnih storitev lahko s korektno in transparentno uporabo teh pristopov svojim uporabnikom dejansko ponudijo boljše in prilagojene storitve, podobno kot trgovec v lokalni trgovini, ki svoje redne stranke zelo dobro pozna,
- uporabniki se ne zavedamo ali pa (močno) podcenjujemo pomen svojih osebnih podatkov in še zlasti svoje zasebnosti, temu primerno z osebnimi podatki ravnamo zelo neskrbno,
- za proizvajalce (in trgovce) izdelkov in dobrin so natančni profili posameznih uporabnikov izjemno koristni, saj omogočajo ne le ciljano oglaševanje pač pa celo »personalizirano« oglaševanje, ki je skrajno (ekonomsko) učinkovito pri oglaševanju in trženju izdelkov, saj naslavlja specifične vrednote in interese, ki so najpomembnejše za vsakega uporabnika posebej (Savanović in Praprotnik, 2012).

Glavni koncepti oz. tehnologije, ki omogočajo spremljanje in profiliranje uporabnikov v internetu, so:

- internetni piškotki (ang. Cookies): omogočajo „anonimno“ profiliranje, tj. izdelavo natančnega profila posameznega uporabnika, tudi če ni mogoče ugotoviti njegovega dejanskega imena,
- uporabniški računi (ang. Accounts) v spletnih storitvah: omogočajo poimensko profiliranje uporabnikov, kadar registracija zahteva vnos dejanskega imena in naslova uporabnika, npr. za potrebe dostave kupljenega blaga.

Piškotki sami po sebi niso problematični, temveč celo koristni, saj so bili med prvimi tehnološkimi koraki, ki so omogočili izvedbo kompleksnih spletnih storitev. Vendar pa zakonodaja od ponudnikov spletnih strani zahteva, da obiskovalce opozorijo na piškotke in jim dajo možnost, da se z njimi ne strinjajo. Piškotke lahko iz brskalnika odstranimo, vendar s tem izgubimo tudi nekaj udobja pri brskanju.

Socialna omrežja še posebej ogrožajo zasebnost uporabnika, če uporabniki sami oddajo zasebne vsebine (npr. fotografije, video posnetke).

Sledenje in profiliranje je grožnja za uporabnika, saj:

- ogroža zasebnost in materialne pravice uporabnika,
- vodi v slabo obveščenost in neracionalne odločitve uporabnika,
- uporabniku onemogoča dostop do vseh informacij v internetu,
- v splošnem poslabšuje položaj uporabnika v odnosu do različnih organizacij, ki mu ponujajo storitve (Savanović in Praprotnik, 2012).

Zasebnost uporabnika

V porastu so netransparentne, do uporabnika nepoštene in tudi pravno sporne prakse sledenja in profiliranja, ki na dolgi rok močno ogrožajo moralne (zasebnost) in materialne pravice uporabnika. V nekaterih družabnih medijih gre celo za prevzemanje materialnih avtorskih pravic nad uporabnikovimi podatki in vsebinami, npr. slikami (Savanović in Praprotnik, 2012).

Slaba obveščenost in iracionalne odločitve

Oglaševanje je za uporabnika lahko škodljivo, če je netransparentno in zavajajoče. Ciljano, še zlasti »personalizirano« oglaševanje je pri tem lahko skrajno učinkovito.

Omejen dostop do informacij

Internetni fenomen »filter bubble« pomeni, da programski algoritem v spletni storitvi, npr. v iskalniku, uporabniku ne ponudi vseh informacij, pač pa le omejen nabor informacij, ki jih določi glede na uporabnikov profil. Z drugimi besedami, algoritem brez uporabnikove vednosti in po lastni presoji filtrira/cenzurira informacije in tako uporabniku omeji oz. prepreči dostop do vseh informacij v internetu, zlasti do informacij, ki ne ustrezajo uporabnikovemu profilu oz. so drugačni od njegovih interesov in intelektualnih nazorov. Tako lahko npr. iskalni niz »British Petroleum« vrne le informacije o možnostih investiranja v to podjetje, ne pa tudi informacij o razlitju nafte v Mehiškem zalivu, iskalni niz »Egipt« pa lahko vrne le turistične informacije ne pa tudi informacij o političnih nemirih v tej državi (Savanović in Praprotnik, 2012).

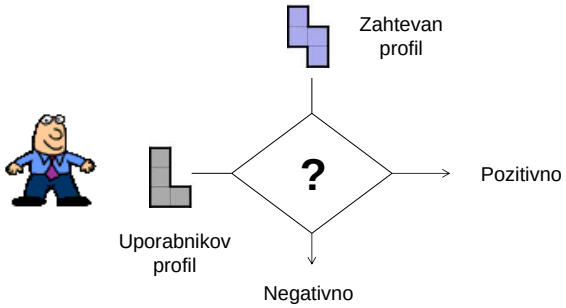
Splošno poslabšan položaj uporabnika

Fenomen »filter bubble« lahko posplošimo, saj smo kot družba na vseh področjih vedno bolj odvisni od avtomatskih programskih algoritmov za odločanje. Slednji lahko na različne načine poslabšajo položaj uporabnika v odnosu do različnih organizacij, ki mu ponujajo različne storitve, npr. (Savanović in Praprotnik, 2012):

- Primerjajo zaseben oz. (preveč) podroben uporabnikov profil z zahtevanim profilom (definiran interno v organizaciji) in uporabniku zavrnejo storitev po kriteriju dobičkonosnosti, zdravstvenega stanja, družinskega statusa (nosečnost), političnih nazorov, verskih nazorov, itd.
- Primerjajo uporabnikov zahtevek (npr. iskalni niz) z njegovim profilom in uporabniku brez njegove vednosti ponudijo prilagojeno informacijo ali storitev, ki pa je omejena, pristranska, filtrirana/cenzurirana, itd. V to skupino sodi fenomen »filter bubble«

Sledenje odstopanj

Algoritmi primerjajo uporabnikovo trenutno obnašanje oz. njegov trenutni profila z njegovim »normalnim« oz. običajnim obnašanjem, ki ga določa njegov zahtevan profil. Vsako pomembnejše odstopanje od normalnega obnašanja lahko vodi v različne posledice. Obveščevalne službe npr. na ta način uporabnika lahko okvalificirajo kot potencialnega terorista, morilca ali storilca kakšnega drugega kaznivega dejanja ter mu nato natančneje sledijo.



Slika 9: Profili in avtomatski algoritmi za odločanje

3.7 VEKTORJI NAPADA

Vektor napada je sredstvo oz. način, s katerim lahko akter kibernetske grožnje (heker) zlorabi slabost ali ranljivost na napadenih sredstvih (vključno z ljudmi), da doseže določen cilj (MJU, 2018).

Vektorje napada bi lahko razvrstili v naslednje skupine glede na primarno tarčo:

- človek – socialni inženiring,
- informacijsko komunikacijska oprema.

Pri socialni inženiringu se napadalci usmerjajo zlasti na zvabljanje podatkov preko e-pošte, socialnih omrežij, direktnih klicev po telefonu ali kakšnem drugem sredstvu komunikacije (npr. Messanger) in spletnih strani. Vektorji napada s škodljivo kodo so npr. zlonamerne priponke e-sporočil, dokumenti s programsko kodo (npr. makro ukazi itd.), okužene spletne strani. Za razne prevare se uporabljajo tako rekoč vsi mediji komunikacije.

Če je primarna tarča napada informacijsko komunikacijska oprema, so vektorji napada npr.:

- nelegalna programska oprema,
- vektorji napada, ki temeljijo na spletu in brskalnikih,
- sredstva, izpostavljena na internetu,
- izkoriščanje ranljivosti in/ali napačnih nastavitev in napak kriptografskih, omrežnih ter varnostnih protokolov,
- napadi v dobavni verigi,
- odtekanje podatkov,
- trgovine za mobilne aplikacije,
- zlonamerni USB ključi,
- posnemanje kartic.

SI-CERT (2021) poroča, da pogosto obravnavajo napade prek nelegalne programske opreme.


Pred kratkim je bila Evropski biomolekularni raziskovalni inštitut tarča napada z izsiljevalskim kripto virusom vrste Ryuk. Posledica napada je bila izguba pomembnih raziskovalnih podatkov za vsaj teden dni. Analiza vdora je pokazala na vstopni vektor

napadalcev preko RDP protokola z avtentikacijskimi podatki enega od študentov. Napadalci so do njegove gesla prišli z virusom, ki ga je vseboval crack za programsko opremo, ki jo je študent potreboval pri svojem delu. Tudi na SI-CERT redno obravnavamo primere okužb skozi nelegalno programsko opremo. Finančne posledice okužb so dostikrat precej višje kot nakup licence (SI-CERT, 2021).

Vektorji napada, ki temeljijo na spletu in brskalnikih, so (MJU, 2018):

- okužbe pri prenosu[8] (ang. drive-by download),
- rudarjenje v mimohodu (ang. cryptojacking),
- zlonamerne skripte,
- kompleti za izkoriščanje,
- napadi na spletne aplikacije − SQL vrivanje (ang. SQL injection),
- zlonamerni dodatki za brskalnike,
- zlorabljene spletne strani,
- lažne spletne strani.

Sredstva, ki so izpostavljena na internetu so npr. IoT naprave in druga slabo zaščitena sredstva, privzete in šibke poverilnice za storitve ter ponovna uporaba gesel oz. uporaba istih gesel na različnih sistemih.

3.8 AKTERJI KIBERNETSKIH GROŽENJ

Razvoj na področju akterjev kibernetskih groženj je napredoval podobno kot je napredoval razvoj kibernetskih groženj. Opazno je povečanje kompleksnosti, izpopolnjenosti in napredka v razvoju zmogljivosti pri večini skupin akterjev. Zaradi uporabe lažnih identitet in prikritega delovanja je vedno težje prepoznati posamezne akterje kibernetskih groženj.

Uporabniki prav tako vedno težje ločijo med dobrimi in slabimi akterji, kar vodi k zmanjševanju zaupanja ne samo do komercialnih ponudnikov storitev, ampak celo do institucionalnih akterjev v kibernetskem prostoru (MJU, 2018).

3.8.1 4.1. Kibernetski kriminalci

V letu 2021 so bili kibernetski kriminalci še vedno najdejavnejša skupina akterjev kibernetskih groženj, saj so bili odgovorni za najmanj 85% evidentiranih incidentov (Hackmageddon, 2021). Usmerili so se v monetizacijo svojih aktivnosti, saj so se osredotočili na napade, po katerih pridobijo denar z izsiljevalskim programjem ali drugimi oblikami izsiljevanja.

Kibernetski kriminal je krovni izraz za številne različne vrste kaznivih dejanj, ki se dogajajo na internetu ali kjer je tehnologija sredstvo in/ali cilj napada. Kibernetski kriminal je ena najhitreje rastočih kriminalnih dejavnosti po vsem svetu in lahko vpliva tako na posameznike kot na podjetja (Europol, 2019).

[8] Okužbe pri prenosu ali okužbe v mimohodu

Kibernetski kriminal delimo na (Europol, 2019):

- kibernetsko odvisna kazniva dejanja (ang. Cyber Dependent Crime),
- kibernetsko omogočena kazniva dejanja (ang. Cyber Enabled Crime).

Pri kibernetsko odvisnem kriminalu je cilj in sredstvo napada računalniški sistem. V to skupino spadajo npr. napadi na računalniške sisteme, ki motijo infrastrukturo IT in kraja podatkov po omrežju z uporabo zlonamerne programske opreme. Namen kraje podatkov je običajno storiti nadaljnje kaznivo dejanje.

Kibernetsko omogočena kazniva dejanja, so „obstoječa“ kazniva dejanja, ki so se z uporabo interneta spremenila v obsegu ali obliki. Rast interneta je omogočila izvajanje teh kaznivih dejanj v velikem obsegu. V to skupino spadajo npr. uporaba interneta za lažje trgovanje z drogami, finančne goljufije in številne druge „tradicionalne“ vrste kriminala.

Kriminalne združbe poslujejo kot dobro organizirana podjetja. Izkoriščajo tehnologije in zmožnosti, s katerimi svojo dejavnost optimizirajo, širijo in razvijajo.

Kriminal ima svoj storitveni model računalništva v oblaku, ki se imenuje kriminal kot storitev (ang. crime as a service – CaaS). Pri tem modelu kriminalne združbe ali posamezniki razvijajo napredna orodja za izvajanje kriminalnih dejavnosti in jih prodajajo ali dajejo v najem drugim, pogosto računalniško manj veščim kriminalcem. Slednji jih nato uporabijo za izvajanje kibernetskih kriminalnih dejavnosti. Kot storitve so na voljo na temnem internetu (ang. darknet) oz. na skritih spletnih straneh (ang. dark web), do katerih je možen dostop le s posebnimi brskalniki. Na voljo je:

- programska opreme za izvajanje kibernetskih napadov,
- okužena omrežja računalnikov (ang. botnet), s pomočjo katerih se izvajajo kibernetski napadi,
- ukradeni podatki in
- storitve kot npr. zagotavljanje denarnih mul (Europol, 2020).

Za denarne mule je značilno, da sodelujejo pri pranju denarja (ang. money laundery). Novačijo jih preko socialnih omrežij in jim obljubljajo velik zaslužek. Če so žrtve naivne in pristanejo na sodelovanje, na svoje transakcijske račune prejemajo nezakonito pridobljena denarna sredstva in nato opravljajo dvige gotovine ali izvršujejo prenakazila na druge transakcijske račune, ki so najpogosteje odprti v tujini. Tovrstna dejanja se v EU obravnava kot kaznivo dejanje pranja denarja. Denarne mule niso le naivne žrtve, temveč sostorilci kaznivih dejanj (Europol, 2019).

Center za boj proti kibernetskemu kriminalu pri Europolu (2020) trdi, da obstoj in delovanje CaaS skupnosti olajšuje kriminalcem izvajanje napadov, organom pregona in varnostnim strokovnjakom pa otežuje boj proti organiziranemu kibernetskemu kriminalu.

Vsi, ki uporabljamo internet, puščamo na njem sledi in podatke. Kriminalci so ves čas na preži za podatki. Z različnimi metodami zvabljanja (ang. phishing) jih skušajo pridobiti in nato uporabiti za izvajanje drugih kriminalnih dejavnosti (npr. izsiljevanje, kraja denarja).

Kibernetski kriminal kot storitev (CaaS) olajša zvabljanje, saj je tehnično manj veščim kriminalcem na voljo vsa potrebna oprema za zvabljanje podatkov.

Kriminal kot storitev deluje na temnem spletu (ang. darkweb). Plačilno sredstvo so kriptovalute (Europol, 2020).

3.8.2 Osebe znotraj organizacije

Grožnje od znotraj in z njimi povezane osebe znotraj organizacije so pomemben dejavnik na področju kibernetskih groženj. Tako kot kibernetski kriminalci tudi osebe znotraj zasledujejo predvsem finančno pridobitne cilje s tem, da neposredno in/ali posredno prodajajo svoje storitve na črnem trgu.

V primeru oseb znotraj, ki so nenamerni akterji, gre običajno za zlorabo njihovih dostopov ali okužbe njihovih računalnikov. Dejansko so pod nadzorom drugih akterjev groženj in se ne zavedajo, da so krivci za zlorabo sistema. Vzrok, da lahko pride do tega, so lahko dolga neprekinjena obdobja, ko so uporabniki prijavljeni v svoje račune, pošiljanje podatkov iz službenih na zasebne račune, shranjevanje podatkov na nosilce izven organizacije in dostopnost (npr. zaradi nepazljivosti) njihovih gesel (MJU, 2018).

3.8.3 Države

Države kibernetske vdore uporabljajo predvsem za vohunjenje in kot orožje.

Kibernetsko vojskovanje (ang. cyber warfare) oz. bojevanje vključuje dejanja neke nacionalne države ali mednarodne organizacije, ki napade informacijska omrežja druge države ali organizacije (npr. teroristične) z računalniškimi virusi, napadi onemogočanja storitve in drugimi oblikami kibernetskih napadov.

Glede na napredne zmogljivosti te skupine, je njihove napade pogosto težko identificirati in se jim zoperstaviti. Zelo verjetno je, da je dejansko število njihovih napadov veliko večje kot kažejo statistike (MJU, 2018).

Glavna cilja državno sponzoriranih kibernetskih aktivnosti so proizvodne zmogljivosti in javne uprave drugih držav, namen vdora pa vohunjenje. Take države veliko vlagajo v razvoj napadalnih kibernetskih orožij, istočasno pa uporabljajo inovativne pristope tako za napade kot tudi obrambo pred njimi. Zaradi uporabe naprednih tehnik napada, uporabe t.i. zero-day ranljivosti in močne tehnične in finančne podpore, so države najbolj strah vzbujajoč akter kibernetskih groženj.

Zero-day ranljivost je ranljivost programske ali strojne opreme, ki še ni bila javno odkrita oziroma objavljena in zato zanjo tudi ne obstaja popravek ali rešitev ali pa je bila pomanjkljivost pred kratkim odkrita in žrtve še niso utegnile poskrbeti za zaščito. Žrtev se je ne zaveda, zato je vse do razkritja na voljo napadalcu (MJU, 2018).

3.8.4 Hektivisti

Hektivisti spadajo med pet najpomembnejših akterjev kibernetskih groženj. Spodbujeni z nekaterimi političnimi dogodki, so odgovorni za razobličenja spletnih strani ter kraje in kršitve podatkov, prvenstveno usmerjenih proti vladam ter organizacijam in podjetjem v javnem sektorju. V to skupino spadajo posamezniki z različnim nivojem sposobnosti za izvajanje kibernetskih napadov. Skupina je predvsem aktivna na področju razobličenja spletnih strani, širjenja propagande in medijsko odmevnih DDoS napadih. Predvideva se, da ti akterji kibernetskih groženj za svoje napade uporabljajo razpoložljive storitve kibernetskega kriminala (ang. Cyber Crime as a Service – CCaaS). Za svoje napade imajo običajno politične motive, ki lahko pritegnejo tudi druge akterje kibernetskih groženj, predvsem države, ki hektiviste pogosto uporabijo kot krinko za svoje kibernetske napade (MJU, 2018).

Hektivisti pa nimajo samo političnih ciljev. Hektivist je vsak aktivist, ki uporablja hekerska dejanja za promocijo stališč ali doseganje političnih ciljev (Islovar, 2021). Stališča so lahko verska, zdravstvena (npr. anticepilci), okoljska …

3.8.5 Kibernetski teroristi

Kibernetski teroristi se podobno kot hektivisti poslužujejo aktivnosti, povezanih z razobličenjem spletnih strani in napadi DDoS, ki pa so lahko usmerjene proti kritični infrastrukturi. Predvideva se, da se zanimajo za razvoj zmogljivosti na področju kriptovalut, predvsem z namenom skrivanja svojih virov pred mednarodnim finančnim nadzorom in za pranje denarja. Prav tako se lahko zanimajo za nakup storitev kibernetskega kriminala, orožja in drog na črnem trgu (MJU, 2018).

Grožnja kibernetskega terorizma lahko izvira tudi od drugih skupin akterjev kibernetskih groženj, npr. tistih, povezanih s političnim ekstremizmom.

3.8.6 Script kiddies

Skupina akterjev kibernetskih groženj, poimenovana »Script kiddies«, obsega akterje z nizko stopnjo zmogljivosti za izvajanje kibernetskih groženj in z nizko motiviranostjo za napade. Tukaj gre predvsem za populacijo najstnikov. Njihove aktivnosti imajo običajno majhen vpliv, vendar lahko v določenih okoliščinah in v povezavi z drugimi skupinami akterjev kibernetskih groženj prerastejo v resne kibernetske napade (MJU, 2018).

 Primer so avtorji škodljive kode Mirai.

3.9 OSVEŠČANJE LJUDI IN PREGON KIBERNETSKEGA KRIMINALA

Za kriminalno dejavnost velja enako kot za vse poštene gospodarske dejavnosti: neprestano se razvija in išče inovativne rešitve.

Obsežno področje informacijske varnosti je boj proti kibernetskemu kriminalu. Žrtve smo lahko vsi – tako fizične kot pravne osebe. Zato je na nivoju držav in sveta poskrbljeno za organizirano delovanje proti kibernetskemu kriminalu. Dejstvo je, da kibernetski kriminal predstavlja iz leta v leto večjo varnostno grožnjo.

V Evropi se s pregonom kibernetskega kriminala ukvarja Europol in njegov European cybercrime center (kratica EC3) in policije posameznih držav.

Informacijska varnost in boj proti kibernetskemu kriminalu je izjemno pomembna dejavnost, ki pa se ne nanaša zgolj na represivne organe. Pomembna je tudi pomoč žrtvam, osveščanje o nevarnostih na splošno, obveščanje o konkretnih varnostnih grožnjah, in kako se pred njimi zaščititi. Države imajo za ta namen agencije, ki se imenujejo CERT. V Sloveniji imamo SI-CERT, v ZDA imajo US-CERT.

Slika 10: Varni na internetu

SI-CERT (Slovenian Computer Emergency Response Team) je nacionalni odzivni center za kibernetsko varnost. Opravlja koordinacijo razreševanja incidentov[9], tehnično svetovanje ob vdorih, računalniških okužbah in drugih zlorabah, ter izdaja opozorila za upravitelje omrežij in širšo javnost o trenutnih grožnjah na elektronskih omrežjih. SI-CERT izvaja nacionalni program ozaveščanja Varni na internetu. Delovanje centra SI-CERT je opredeljeno v 28. členu

[9] Varnostni incident je dogodek, ki vpliva na varnost omrežja, naprave ali podatkov.

Zakona o informacijski varnosti. Storitve odzivnega centra SI-CERT so na voljo širši javnosti (https://www.cert.si/o-nas/, 6. 9. 2021).

Zelo pomembna dejavnost SI-CERTa je osveščanje. Na spletni strani Varni na internetu (https://www.varninainternetu.si/) najdemo primere in nasvete, kako se zaščitimo ped zlorabami (Slika 10).

Pogosto uporabljamo besedo incident. Poenostavljeno rečeno gre za zaznavo nekega varnostnega problema, npr. konkretnega načina zlorabe ali poskusa zlorabe.

Kibernetski kriminal ne pozna državnih meja. Zato je za splošno varnost vseh Zemljanov potrebno sodelovanje in usklajeno delovanje organov pregona različnih držav.

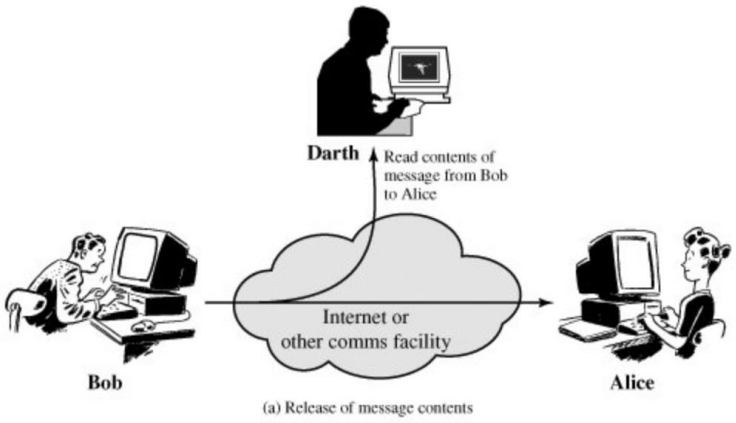
3.10 KLASIFIKACIJA KIBERNETSKIH NAPADOV

Kibernetske napade lahko razvrstimo na več načinov glede na:

- aktivnost napadalca: pasivni in aktivni,
- območje oz. omrežje, od koder se izvaja napad: notranji in zunanji,
- primarno tarčo napada: računalniška oprema ali človek (socialni inženiring).

3.10.1 Pasivni in aktivni napadi

Kibernetski napad je lahko aktiven ali pasiven. V aktivnem napadu poskuša napadalec spremeniti sistemske vire ali vplivati na njihovo delovanje. Pri pasivnem napadu skuša pridobiti ali uporabiti informacije iz sistema, brez vpliva na sistemske vire.



Slika 11: Prisluškovanje
(http://flylib.com/books/en/3.190.1.21/1/)

Pri pasivnih napadih se napadalec omeji na pasivno opazovanje prometa, pri čemer ne posega v direktno komunikacijo med oddajnikom in sprejemnikom. Take napade je običajno težko odkriti, vendar se je pred njimi lažje zaščititi (Savanović in Praprotnik, 2012). Pasivni napad ogroža zaupnost podatkov.

Cilj pasivnega napada je doseči podatke ali ugotoviti ranljivosti omrežja.

Slika 11 in Slika 12 prikazujeta dva najpogostejša tipa pasivnih napadov:

- prisluškovanje (ang. eavesdropping) in
- analizo prometa (ang. traffic analysis).

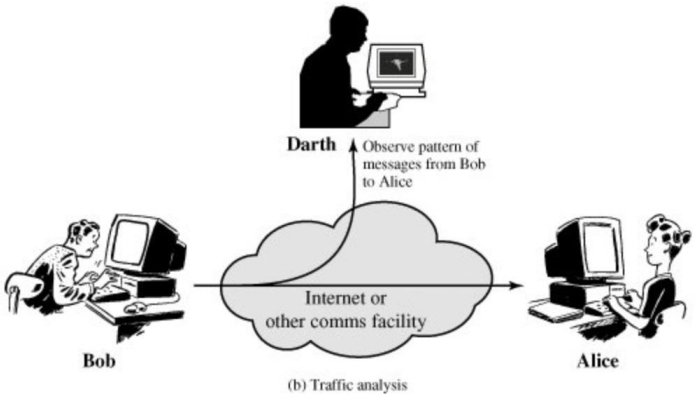
V prvem primeru lahko napadalec prisluškuje celotni vsebini komunikacije, kar je možno, kadar so podatki pri prenosu nezaščiteni (Savanović in Praprotnik, 2012).

Če so podatki zaščiteni pred prisluškovanjem na višjem nivoju, npr. s šifriranjem, lahko napadalec z analizo prometa na nižjem nivoju pridobi pomembne informacije, kot so npr.

- kdo je oddajnik (npr. IP naslov, MAC naslov),
- kdo je sprejemnik,
- kako pogosto poteka komunikacija,
- kdaj poteka komunikacija,
- kakšen je profil komunikacije (trajanje, količina prometa), itd. (Savanović in Praprotnik, 2012).

Za običajno rabo zaščita pred analizo prometa običajno ni potrebna, medtem ko je v posebnih primerih, npr. pri vojaški komunikaciji, potrebna tudi zaščita pred tem. V teh primerih se uporabljajo specifične rešitve, ki omogočajo šifriranje na najnižjih nivojih (npr. Ethernet šifriranje) in generiranje »umetnega« prometa, ki lahko povsem zakrije naravo komunikacije (Savanović in Praprotnik, 2012).

Pri aktivnem napadu napadalec aktivno vpliva na informacije pri prenosu prek omrežja. Take napade je običajno lažje zaznati, a se je pred njimi težje zaščititi (Savanović in Praprotnik, 2012).



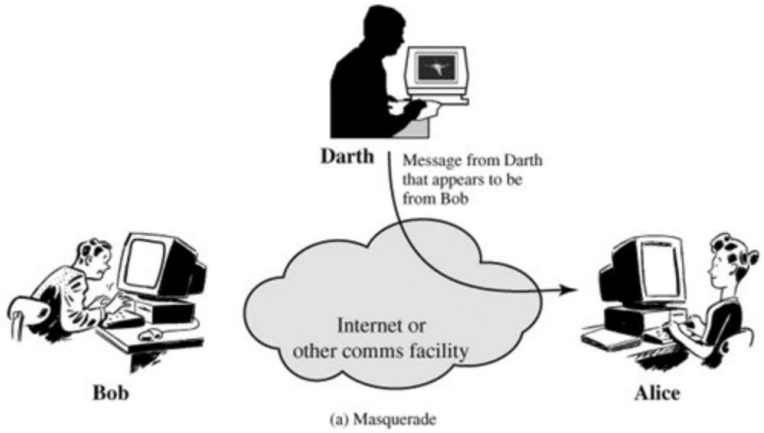
Slika 12: Analiza prometa
(http://flylib.com/books/en/3.190.1.21/1/)

Najbolj značilni aktivni napadi so (Savanović in Praprotnik, 2012):

- pretvarjanje (ang. spoofing, masquerading),

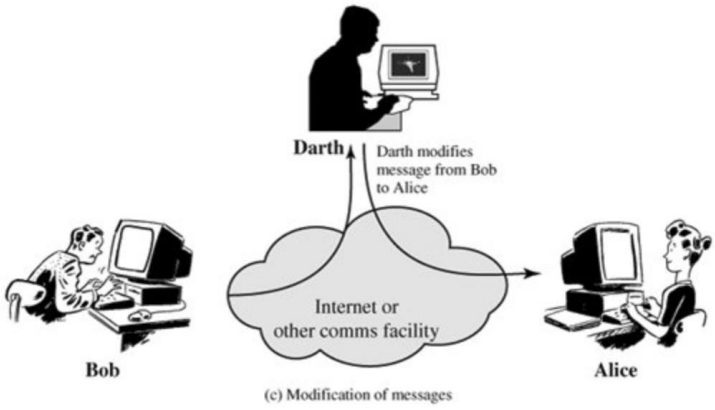
- spreminjanje (ang. modification),
- onemogočanje storitve (ang. DoS – Denial of Service),
- nepooblaščen dostop do virov ali podatkov (ang. unauthorised access).

Pri **pretvarjanju** se napadalec izdaja za nekoga drugega tako, da generira sporočila, v katerih ponaredi podatke o identiteti pošiljatelja, npr. IP naslov ali ime. Sprejemnik v tem primeru zmotno misli, da se pogovarja z nekom drugim. Napadalcu izda zaupne informacije ali pa po njegovih navodilih izvede aktivnosti, ki imajo neželene posledice (Savanović in Praprotnik, 2012). Če napadalec a pomočjo pretvarjanja od žrtve izvabi podatke, takemu napadu rečemo ribarjenje ali zvabljanje podatkov (ang. phishing).



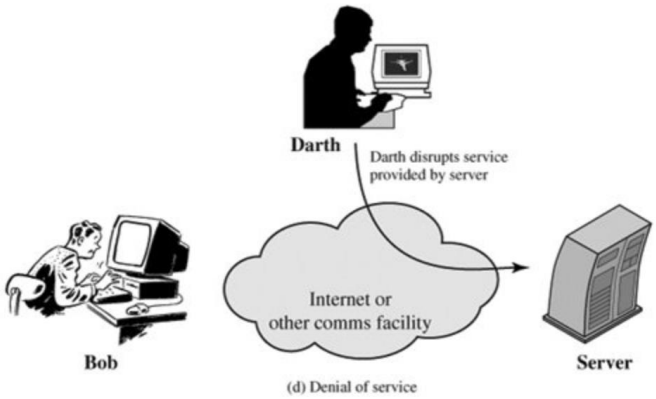
Slika 13: Pretvarjanje
(http://flylib.com/books/en/3.190.1.21/1/)

Pri **spreminjanju** napadalec prepreči neposredno komunikacijo med oddajnikom in sprejemnikom. Obenem prestreže sporočilo, aktivno spremeni (del) njegove vsebine ter spremenjeno sporočilo posreduje sprejemniku. Slednji tako sprejme drugačno sporočilo do originalnega, kar spet lahko vodi v različne incidente (Savanović in Praprotnik, 2012). Primer takega napada je vrivanje v poslovno komunikacijo (ang. business email compromise – BEC), katerega posledica je finančna prevara.



Slika 14: Spreminjanje
(http://flylib.com/books/en/3.190.1.21/1/)

Pri **zavrnitvi oz. ohromitvi storitve** (Slika 15) napadalec izkoristi določeno (znano ali novo odkrito) ranljivost v strežniku ali pa strežnik preprosto zlonamerno poplavi s prometom, tako da postane določena storitev ali pa celoten strežnik nedosegljiv oz. neuporaben za legitimne uporabnike. Tovrstni napadi so za napadalce bolj učinkoviti, če se izvedejo iz omrežja napadalskih računalnikov.



Slika 15: Onemogočanje storitve
(http://flylib.com/books/en/3.190.1.21/1/)

Pri **nepooblaščenem dostopu** (ang. unauthorised access) napadalec izkoristi ranljivosti (ang. vulnerability) v strojni ali programski opremi strežnika in na ta način pridobi nepooblaščen dostop do virov in/ali podatkov v napadenem sistemu. Taki napadi so tipično povezani z vdori v sisteme in običajno predstavljajo odskočno desko za druge vrste zlorab (Savanović in Praprotnik, 2012).

3.10.2 Napadi na opremo in socialni inženiring

Kibernetske napade delimo glede na način izvedbe na:

- napade s tehničnimi sredstvi, kjer je IKT tako sredstvo kot tarča napada in
- socialni (ali družbeni) inženiring, kjer zlikovci obidejo tehnično zaščito in izkoristijo ljudi (Vasiljevič idr., 2006).

Pred napadi s tehničnimi sredstvi nas varuje zaščitna oprema (npr. požarni zid, protivirusna programska oprema) in zaščitni ukrepi. Ob rednem posodabljanju opreme je tehnična zaščita učinkovita in jo zlikovci težje obidejo. Zato poskušajo preslepiti najšibkejši člen v verigi informacijske varnosti – uporabnika.

Zadnja leta napadi s pomočjo socialnega inženiringa povzročijo več škode kot tehnični napadi, kar dokazujejo poročila o internetnem kriminalu (Europol, 2020; FBI, 2019; Verizon, 2020). Osnovni princip takšnih napadov je pridobivanje informacij od potencialne žrtve ali preslepitev žrtve, da izvrši dejanje, ki ji škodi. Najbolj pogosta oblika socialnega inženiringa je zvabljanje (ang. phishing). To je način zavajanja uporabnikov, da sami izdajo svoje osebne podatke (npr. številke kreditnih kartic, gesla, podatke o bančnih računih).

3.10.3 Notranji in zunanji napadi

Napad lahko izvedejo storilci iz organizacije ali od zunaj.

Notranji napad sproži posameznik, ki ima dovoljenje za dostop do sistemskih virov, a jih uporablja na zanj nedovoljen in neodobren način.

Zunanji napad sproži nepooblaščeni ali nelegitimni uporabnik, ki ni iz napadene organizacije. Potencialni zunanji napadalci imajo različne motive: denar, vohunjenje, terorizem, potegavščine, maščevalnost ... Napadalci niso le posamezniki. Veliko kršitev izvedejo organizirane kriminalne organizacije.

Za preprečevanje vdorov od zunaj (npr. z interneta) sta nepogrešljiva pripomočka požarni zid (pregrada) in protivirusna programska oprema. Žal pa t.i. tehnična varnost ne zadošča. Pomembno je, da se uporabniki zaščitno obnašamo in s svojim ravnanjem preprečujemo zlorabe, ki jih s tehnološkimi sredstvi ne moremo preprečiti.

Napadalci v današnjem času ne delujejo zgolj z enega računalnika, temveč z omrežij, ki so si jih pred tem podjarmili. Tem omrežjem rečemo botnet omrežja ali botneti. Ime je nastalo iz kombinacije angleških besed robot in net. Tudi v slovenskem strokovnem izrazoslovju smo besedo poslovenili v botnet (Islovar, 2021). Lastniki računalnikov v takih omrežjih običajno ne vedo, da njihovi računalniki služijo kriminalni dejavnosti in da sodelujejo v orkestriranem napadu na določeno tarčo ali naključne tarče.

4 VARNOSTNE STORITVE IN UKREPI

Zaščito informacijske tehnologije lahko opredelimo kot takšno varovanje informacij, sistemov in opravil, da v primeru neljubih dogodkov kot so kibernetski napadi in napake minimiziramo škodo. Zaščita informacijske tehnologije obsega naslednje elemente varovanja:

- fizično varovanje elektronskih naprav,
- arhiviranja podatkov,
- zaščita pred električnimi udari (strele),
- zaščita podatkov,
- ukrepanje v primeru napak opreme ali uporabnikov,
- zaščita IT sistemov pred zlonamernimi programi in s tem povezanimi nepooblaščenimi vdori v informacijske sisteme (Savanović in Praprotnik, 2012).

Varnostne storitve so namenjene zaščiti omrežij, računalniških naprav, uporabnikov in podatkov pred različnimi grožnjami. Zagotavljajo jih računalniške in omrežne naprave ter programi s pomočjo različnih varnostnih algoritmov, protokolov in tehnologij (Savanovič in Praprotnik, 2012).

Najpomembnejše varnostne storitve so:

- razpoložljivost,
- kontrola dostopa,

- overjanje,
- zaupnost,
- celovitost,
- preprečevanje zanikanja,
- zagotavljanje zasebnosti.

V nadaljevanju so podrobneje predstavljene posamezne varnostne storitve in pristopi, s katerimi lahko te storitve zagotovimo.

4.1 OVERJANJE

Overjanje (ang. (authentication) ali avtentikacija je storitev, ki omogoča preverjanje in dokazovanje identitete. Kdo je uporabnik ali oseba s katero komuniciramo?

Identiteto dokazujejo uporabniki in naprave, kar je pomembno tako v lokalnem omrežju podjetja kot na internetu.

Na internetu pogosto poteka komunikacija s predhodno neznanimi sogovorniki in napravami. Overjanje se izvaja na samem začetku komunikacije, pred dejansko izmenjavo podatkov, tipično v obliki dialoga, kot je npr. naslednji:

- A: Pozdravljen. Kdo si? Prosim za dokazilo.
- B: Jaz sem strežnik www.ime.si. Tule je dokazilo.
- A: Preverjam dokazilo… Da, ti si res www.ime.si (Savanovič in Praprotnik, 2012).

Zelo pogost način overjanja uporabnikov je s pomočjo uporabniškega imena in gesla kot dokazila. Ta pristop je sicer enostaven in pogosto tudi primeren pri kontroli dostopa do sistema, vendar ne omogoča zanesljivega overjanja uporabnika, saj lahko geslo poleg uporabnika pozna tudi sistem[10]. Bolj zanesljivo overjanje uporabnika je možno le s pomočjo takšnega dokazila, ki ga lahko predloži samo uporabnik in nihče drug (Savanovič in Praprotnik, 2012).

4.1.1 Gesla

Uporaba gesel je zelo razširjena, a tudi zelo problematična, saj si večina uporabnikov izbere preveč preprosta gesla. Preprosta gesla je mogoče enostavno in hitro odkriti oz. kot pravimo – razbiti. Metoda, s katero napadalci odkrivajo enostavna gesla, se imenuje napad z grobo silo (ang. brute-force attack). Napadalec sistematično preverja vse možnosti, dokler se ne najde rešitve. V primeru uporabe besed iz slovarja in imen se takšno preverjanje konča izjemno hitro, napadalec pa razpolaga z geslom. Pomislimo, kako hitro iskalnik Google išče zadetke. Enako hitri so napadalci.

Najboljša gesla so unikatni, dolgi nizi naključnih znakov. Problem pa je, ker si jih težko zapomnimo. Zato je pametno, da nas na videz naključni nizi znakov na kaj spomnijo.

Primer: Mi2s5gledava!

[10] Geslo je v sistemu shranjeno v obliki zgostitve (hash) in ne v berljivi obliki.

Primeri slabih gesel, ki močno prevladujejo, so (Savanović in Praprotnik, 2012):

- privzeta gesla[11] (ang. default password) − privzeta gesla je potrebno takoj spremeniti!
- besede iz slovarja,
- besede (iz slovarja) ali imena z dodanim številom, npr. password1, zajec2000, jana1234, itd.
- besede s preprostim zakrivanjem (ang. obfuscation), npr. p@ssw0rd, b@l0n …
- podvojene besede, npr. konjkonj, stopstop …
- enostavne kombinacije s tipkovnice, npr. qwerty, 12345, asdfgh, fred,
- dobro znana števila, npr. 314159 (iz π), 9112001 (ameriški zapis za 11. 9. 2001 – teroristični napad v ZDA), rojstni datumi kot števila …
- registrska številka avtomobila,
- osebne številke, npr. EMŠO, davčna, telefonska, rojstni dan,
- športna ekipa,
- imena hišnih ljubljencev, sorodnikov, prijateljev, znancev …

Pri izbiri gesel je potrebno čimbolj slediti naslednjim priporočilom, ki neposredno izhajajo iz pogostih primerov slabih gesel.

Geslo naj bo:

- dolgo vsaj 12 znakov,
- naključno generirano − uporabimo vse skupine znakov: male in velike črke, števila, simboli.

Izogibamo se:

- geslom, ki smo jih opredelili kot slaba gesla,
- **uporabi istega gesla za več storitev/sistemov.**

Uporabi istega gesla za več sistemov hkrati se je potrebno izogibati zaradi kibernetskih napadov na računalniške sisteme. Če uspejo napadalci z neke spletne strani ukrasti seznam uporabnikov in njihovih gesel, postanete zaradi ukradenega gesla lahka tarča.

Praktično vsakemu od nas so že kje ukradli avtentikacijske podatke, čemur so sledili drugi poskusi zlorabe (npr. izsiljevanje, ribarjenje podatkov). Na spletni strani https://haveibeenpwned.com/ lahko ugotovite, če je bilo vaše uporabniško ime oz. poštni naslov zlorabljen? (ang. Have I been pwned?). Če imate npr. LinkedIn račun od leta 2016, je bilo tedaj vaše geslo verjetno ukradeno. V letu 2021 so mediji poročali, da so Facebooku ukradli številne podatke uporabnikov. Zlorabe so se zgodile na straneh z veliko uporabniki (npr. Yahoo, Sony entertainment network) in se bodo še dogajale, saj so take strani za napadalce izjemno zanimive.

Pri napadu z grobo silo (s preizkušanjem) služijo ukradena gesla enako kot besede v slovarju, kar pomeni, da napadalec hitro odkrije geslo in si s tem omogoči dostop do neke druge spletne strani, storitve ali vaših podatkov.

[11] standardno vnaprej nastavljeno geslo za napravo

Še posebej se je treba izogibati uporabi enakega gesla za sisteme, kjer bi morala biti različna stopnja varovanja podatkov. S krajo na slabo varovani strani, brez posebnih razlogov za varovanje, si napadalci lahko pridobijo podatke za dostope na straneh, kjer imate npr. osebne podatke.

Strategija za izbiro dolgega, a praktično uporabnega gesla je uporaba t.i. polnila (ang. padding). Polnilo je dodatek h korenu gesla, ki bistveno poveča dolžino gesla, obenem pa si ga je enostavno zapomniti. Osnovna strategija uporabe polnil je v tem, da:

- se z izbiro dobrega korena izognemo enostavnemu ugibanju našega gesla in »prisilimo« napadalca v uporabo »brute force« metode.
- Pri zaščiti pred brute force metodo pa je ključna dolžina gesla, kjer nam za podaljšanje koristi polnilo (Savanovič in Praprotnik, 2012).

Primer uporabe polnila: K0nj…….

Pri uporabi polnila je ključna osebna strategija oz. koncept polnila. Vsak uporabnik mora imeti lastno polnilo, kar prepreči t.i. slovarski napad (ang. dictionary attack) na polnila.

Slovarski napad je vrsta napada z grobo silo, kjer se pri iskanju gesla uporabijo besede iz slovarjev.

Mnogi sistemi imajo pravila za kreiranje gesel, kar uporabnikom preprečuje izbiro enostavnih gesel. Pogosto je navzdol omejena dolžina gesla. Takrat si nekateri pomagajo s polnilom.

4.1.2 Dvofaktorska in večfaktorska avtentikacija

Na sistemih, ki zahtevajo višjo stopnjo varnosti, za overjanje ni dovolj prijava z uporabniškim imenom in geslom.

Podatki, ki jih hranimo na internetu so preveč pomembni, da bi jih varovali samo z geslom. Zato uporabljamo kombinacije orodij in pravil, ki omogočajo preverjanje pristnosti, hkrati pa ščitijo pred najpogostejšimi oblikami napadov.

Dvofaktorska avtentikacija (2FA) pomeni dvojno preverjanje pristnosti uporabnika.

Primeri:

- Kupujete v spletni trgovini, v katero ste se prijavili z uporabniškim imenom in geslom. Preden plačate, spletna stran banke pošlje številčno kodo na vaš telefon. To kodo morate vpisati na spletno stran e-trgovine, da lahko zaključite postopek nakupa.
- Uporabniki Microsofta 365 uporabljamo za dvofaktorsko avtentikacijo aplikacijo Authenticator. Le-ta od nas po prijavi v Microsoftov uporabniški račun zahteva, da prijavo potrdimo na svojem mobilnem telefonu.
- Prijava v mobilno ali spletno banko ima prav tako večnivojsko zaščito.

2FA je bistvenega pomena za spletno varnost, saj zmanjša tveganja, ki so povezana z gesli. Napadalcem ne zadošča ukradeno geslo, saj je brez uporabe drugega dejavnika geslo neuporabno.

4.1.3 Močna avtentikacija

S 1. 1. 2021 je na podlagi uredbe EU, pri kartičnih plačilih v okviru e-trgovine zahtevana uporaba močne avtentikacije strank. Za vse ponudnike plačilnih storitev v EU veljajo enotna pravila. Njihov namen je zmanjševanje goljufij pri plačevanju, cilj pa zagotoviti varnost sredstev uporabnikov in dobro uporabniško izkušnjo pri spletnih plačilih (Banka Slovenije, 2021).

Močna avtentikacija je postopek, ki temelji na uporabi dveh ali več elementov iz naslednjih kategorij (Evropska unija, 2017):

- znanje uporabnika (nekaj, kar ve samo uporabnik), npr. geslo, osebna identifikacijska številka;
- lastništvo uporabnika (nekaj, kar je v izključni lasti uporabnika), npr. pametna kartica, mobilni telefon;
- nekaj, kar uporabnika enolično določa uporabnika, npr. biometrična značilnost, kot je fotografija ali prstni odtis.

4.2 KONTROLA DOSTOPA

Kot nakazuje že ime, kontrola dostopa (ang. Access Control) preprečuje nepooblaščenim osebam dostop do informacij in virov v sistemu. Kontrola dostopa pomeni uporabo treh medsebojno povezanih storitev: overjanje, avtorizacija in beleženje (AAA – Authentication, Authorization, Accounting). Overjanje in avtorizacija sta nujna koraka za preprečevanje nepooblaščene uporabe virov in podatkov. Beleženje je pomožna storitev, ki omogoča kasnejšo analizo podatkov o uporabi virov v sistemu.

Beleženje omogoča:

- spremljanje delovanja kontrole dostopa in odkrivanje težav,
- odkrivanje (poskusov) vdorov,
- analizo pooblaščene ali nepooblaščene uporabe virov v sistemu (Savanovič in Praprotnik, 2012).

Za dostop do sistema moramo najprej opraviti overjanje. To pomeni, da se moramo najprej prijaviti vanj (ang. log in) z uporabniškim imenom in geslom ali pa se moramo overiti s pomočjo digitalnega certifikata.

Med uporabo sistema nam kontrola dostopa lahko prepreči uporabo virov in nas opozori, če nimamo ustreznih pooblastil, npr.

- onemogoči dostop do modulov informacijskega sistema, do katerega uporabnik ne sme dostopati (npr. do kadrovske evidence),
- sistem uporabniku prepreči spreminjane sistemskih nastavitev, pri čemer se običajno izpiše opozorilo: “Sistemske nastavitve lahko spreminja le Administrator.”

Kontrola dostopa se v lokalnem omrežju izvaja na nivoju operacijskega sistema. Kontrolo dostopa do omrežja pa med drugim izvajajo namenske varnostne naprave kot so npr. požarni zidovi.

4.2.1 Avtorizacija

Avtorizacija ali pooblastitev je varnostni mehanizem, ki se uporablja za določanje pravic uporabnika ali računalnika, ki ima vlogo klienta. Določi se pravice dostopa do informacijskih virov in sredstev kot so: računalniški programi, datoteke, storitve, podatki in moduli aplikacij (Techopedia, 2021).

Avtorizacija je pomembna, saj je potrebno zagotoviti, da ima uporabnik ali računalnik potrebne pravice za dostop do vira ali storitve in da jih nima, če jih ne potrebuje ali ne sme imeti.

Pooblastila se podelijo pred preverjanjem pristnosti identitete uporabnika. Sistemskim skrbnikom (ang. system administrator − SA) so običajno dodeljene ravni dovoljenj, ki zajemajo vse sistemske in uporabniške vire. Ko se npr. uporabnik zaposli v organizaciji, dobi uporabniški račun, na katerega so vezana pooblastila oz. dovoljenja, ki jih ima v računalniškem sistemu.

Med avtorizacijo sistem preveri pravila dostopa overjenega uporabnika in odobri ali zavrne dostop do virov. Pravice uporabnikov so običajno navedene v seznamu za kontrolo dostopa (ang. access control list - ACL) (Whitman in Mattord, 2019).

Sodobni in več uporabniški operacijski sistemi morajo imeti učinkovito zasnovane postopke avtorizacije, ki olajšajo upravljanje aplikacij. Ključni dejavniki so uporabnik, vrsta uporabnika, poverilnice, ki jih je treba preveriti, ter s tem povezana dejanja in vloge. Na podlagi vlog se določijo uporabniške skupine, ki zahtevajo enake privilegije dostopa do računalniških virov.


Vsi komercialisti imajo npr. enake pravice za dostope, zato je smiselno, da se jih obravnava kot skupino.

Običajno se avtorizacijo izvaja na enega od naslednjih načinov (Whitman in Mattord, 2019):

- avtorizacija vsakega overjenega (ang. authenticated) uporabnika posebej,
- avtorizacija overjenega pripadnika uporabniške skupine − vsi člani skupine imajo enake pravice dostopov,
- avtorizacija za več sistemov, kjer centralni sistem preveri identiteto subjekta, ki mu podeli niz poverilnic.


Mnogi računalniški sistemi v svetu so podprti z okoljem Windows in tehnologijami, ki jih zagotavlja podjetje Microsoft. V Windows okolju se za kontrolo dostopov uporablja aktivni direktorij (ang. active directory − AD). Ta tehnologija omogoča nadzor nad omrežnim okoljem preko centralne baze podatkov, kjer se shranjujejo informacije o uporabnikih, računalnikih in drugih omrežnih napravah. ASP.NET sodeluje z Internet Information Server (IIS) in Microsoft Windows za zagotavljanje storitev preverjanja pristnosti in avtorizacije spletnih aplikacij v

okolju .NET. Windows uporablja datotečni sistem NTFS za vzdrževanje seznamov za nadzor dostopa (ang. Access Control Lists – ACL) za vse vire. Seznam za nadzor oz. kontrolo dostopa (ACL) vsebuje pravila, ki uporabniku dovoli ali zavrne dostop. Obstajata dve vrsti ACL:

- ACL datotečnega sistema nadzoruje dostop do datotek in map. Operacijskemu sistema sporoča, kateri uporabniki lahko dostopajo do sistema in katere pravice imajo uporabniki.
- Omrežni ACL nadzira dostop do omrežja. Usmerjevalnikom in stikalom sporoča, katera vrsta prometa lahko dostopa do omrežja in katere dejavnosti so dovoljene (Techopedia, 2021).

4.2.2 Beleženje

Beleženje (ang. accounting) pomeni spremljanje dostopov do sistema: kdo, kdaj in na kakšen način je uporabljal sistem.

Beleženje se izvaja tako na nivoju omrežja in operacijskega sistema kot na aplikativnem nivoju. Nekateri računalniški programi morajo po zakonu zagotavljati sledljivost, npr. računovodski sistem (ERP). Nekateri beležijo samo spreminjanje, npr. kdo in kdaj je izvedel spremembo zapisa. Včasih se zahteva, da se beležijo tudi vpogledi, npr. vpogledi v bazo davčnih zavezancev, s čimer se preprečuje brskanje po podatkih iz radovednosti, kar v skladu z zakonodajo o zaščiti podatkov ni dovoljeno niti pooblaščenim osebam.

4.3 ZAUPNOST

Zaupnost (ang. confidentiality) razumemo kot zaščito osebnih podatkov drugih oseb in drugih pomembnih podatkov.

Po splošni uredbi o varstvu osebnih podatkov (ang. General Data Protection Regulation – GDPR) je potrebno varovati vse osebne podatke, še posebej občutljive osebne podatke (Ur. list L 119, 4.5.2016).

Nekateri strokovnjaki morajo po zakonu hraniti in ščititi informacije, ki jih deli stranka ali pacient, ne da bi jih razkrili. V nekaterih posebnih okoliščinah jih sicer smejo razkriti, a le, kadar to zahteva ali dovoljuje zakon.

Razen osebnih podatkov ščitimo še tajne [12]podatke, pomembne poslovne podatke in podatke, ki so označeni kot zaupni.

Preprečevati je potrebno prisluškovanje, nepooblaščeno spreminjanje podatkov in varovati podatke pred razkritjem tako v lokalnem omrežju kot pri prenosu prek interneta.

Zagotavljanje zaupnosti omogoča enkripcija (ang. encryption).

[12] Tajni podatek je dejstvo ali sredstvo z delovnega področja organa, ki se nanaša na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države ter ga je treba zavarovati pred nepoklicanimi osebami in je označen kot tajen (https://www.gov.si/teme/tajni-podatki/).

V kriptografiji je enkripcija (ang. encryption) ali šifriranje informacij postopek pretvorbe navadnega besedila, v šifrirano besedilo (tajnopis). V idealnem primeru lahko samo pooblaščene osebe dešifrirajo tajnopis nazaj v navadno besedilo in dostopajo do izvirnih informacij. Šifriranje samo po sebi ne preprečuje prestrezanja, vendar potencialnemu prestrezniku onemogoča razumevanje vsebine.

V računalništvu uporabljamo šifrirne metode, kjer algoritmi generirajo šifrirne ključe. Prejemnik lahko preprosto dešifrira sporočilo s ključem, ki ga je avtor dal pooblaščenim prejemnikom, ne pa tudi nepooblaščenim uporabnikom. Zdi se popolnoma varno, a v praksi le ni tako. Zato so se šifrirne metode razvijale in so danes na voljo take, kjer šifriranega sporočila nepooblaščeni uporabniki ne morejo razumeti.

Šifriranje so v preteklosti pogosto uporabljali v vojaške namene in za prenašanje tajnih informacij. Šifrirne metode poznamo iz zgodovine, od starega Egipta do danes.

Moderna kriptografija uporablja dva osnovna načina šifriranja in kombinacijo obeh:

- simetrično šifriranje,
- asimetrično šifriranje.

Šifrirne metode bomo podrobneje obravnavali v posebnem poglavju.

4.4 CELOVITOST

Celovitost podatkov pomeni, da so podatki točni in popolni.

Zagotavljanje celovitosti ali integritete (ang. integrity) je zmožnost zagotoviti, da sistem in njegovi podatki niso bili podvrženi nepooblaščenim spremembam. Varnostna storitev integritete se ne nanaša le ne zaščito podatkov, ampak tudi na zaščito operacijskih sistemov, aplikacij in strojne opreme pred spreminjanjem s strani nepooblaščenih oseb.

Uporablja se tudi izraz neokrnjenost. Varnostna storitev zagotavljanja celovitosti omogoča tudi odkrivanje nepooblaščenega spreminjanja informacij med prenosom prek omrežja (Savanović in Praprotnik, 2012).

Ukrepi za zagotavljanje celovitosti ščitijo podatke pred nepooblaščenimi spremembami. Zagotavljajo točnost in popolnost podatkov. Potreba po varovanju celovitosti se nanaša na podatke, ki so shranjeni v sistemih in podatke, ki se prenašajo med sistemi, npr. preko e- pošte.

Pri ohranjanju integritete ni potreben le nadzor dostopa na ravni sistema, ampak tudi zagotavljanje, da lahko uporabniki sistema spreminjajo le informacije, za katere so pooblaščeni. Učinkoviti ukrepi za zagotavljanje celovitosti morajo zaščititi tudi pred nenamernimi spremembami, kot so napake uporabnikov ali izguba podatkov zaradi okvare sistema.

Kriptografija ima zelo pomembno vlogo pri zagotavljanju celovitosti podatkov. Pogosto uporabljene metode za zaščito integritete podatkov temeljijo na zgoščevalnih algoritmih.

Za zaščito integritete je mogoče uvesti številne ukrepe.

- Kontrola oz. nadzor dostopa (avtentikacija in avtorizacija) lahko uporabnikom v sistemu prepreči spremembe, za katere niso pooblaščeni.
- Zgoščevalne funkcije (ang. hash) in digitalni podpisi lahko pomagajo zagotoviti, da so transakcije verodostojne in da datoteke niso bile spremenjene ali poškodovane (Whitman in Mattord, 2019).

Enosmerne zgoščevalne funkcije so osnovno orodje, na katerem temelji celovitost. Zgoščevalna funkcija je vsaka funkcija, ki jo lahko uporabimo za preslikavo podatkov poljubne velikosti v vrednosti fiksne velikosti.

Zgoščevalna funkcija (ang. hash function) je algoritem, ki dobi kot vhod poljubno dolgo sporočilo, kot izhod pa vrne fiksno dolgo zgoščeno vrednost (ang. hash value). Uporabljamo jo za preoblikovanje poljubno dolgih vhodnih sporočil v izhodne vrednosti fiksne dolžine (npr. 256 bitov). Značilnost te funkcije je, da je nepovratna ali enosmerna. To pomeni, da je nemogoče najti vhodno sporočilo, če poznamo le izhodno vrednost. Prav tako je nemogoče najdi dve vhodni sporočili, ki bi ob izhodu tvorili enaka rezultata. Novejši zgoščevalni algoritmi so SHA-256, SHA-384, SHA-512. (Whitman in Mattord, 2019).

S pomočjo kalkulatorja na spletni strani https://xorbin.com/tools/sha256-hash-calculator lahko izračunamo 256 bitno zgoščeno vrednost poljubnega sporočila.

Preverjanje celovitosti poteka v naslednjih korakih (Savanović in Praprotnik, 2012):

- Oddajnik izračuna zgoščeno vrednost, ki je nekakšen prstni odtis sporočila in ga pošlje skupaj s sporočilom.
- Sprejemnik na enak način izračuna prstni odtis sporočila in rezultat primerja s prstnim odtisom, ki je prispel skupaj s sporočilom.
- Če se ujemata, je ostalo sporočilo pri prenosu neokrnjeno.

4.5 RAZPOLOŽLJIVOST

Za zagotavljanje informacijskih storitev je pomembno, da so ustrezni strežniki in podatki pooblaščenim uporabnikom vedno na razpolago oz. dosegljivi brez zakasnitev. To lastnost imenujemo razpoložljivost (ang. availability).

Razpoložljivost je izjemno pomembna zahteva za stanje informacijskega sistema, zato je potrebno izvajati ustrezne ukrepe.

Veliko razlogov, da računalniški sistem ni na voljo, ni povezanih z zlonamernimi napadi. Dogajajo se npr. izpadi električnega napajanja, okvare strojne opreme, nenačrtovani izpadi programske opreme in težave z delovanjem interneta.

Zlonamerni napadi vključujejo različne oblike sabotaž, katerih namen je povzročiti škodo organizaciji tako, da uporabnikom onemogoči dostop do informacijskega sistema v celoti ali delno. Pogoste tarče hekerskih napadov so spletne strani. Onesposabljanje storitve (ang. Denial of Service – DoS) je metoda, ki jo hekerji pogosto uporabljajo za motenje spletnih storitev. Strežnik zasujejo z odvečnimi zahtevami in onemogočajo izvajanje storitev za običajne

uporabnike. Ponudniki storitev so v preteklih letih razvili protiukrepe za odkrivanje in zaščito pred napadi DoS, a hekerji svojo dejavnost prav tako razvijajo in takšni napadi ostajajo stalna skrb.

Za doseganje razpoložljivosti sistema je potrebno preprečevati:

- posledice nenamernih napak strojne opreme ali uporabnikov,
- nepredvidenih zunanjih okoliščin (npr. izpad električne energije, internetnega ponudnika),
- zlonamerne napade za onesposabljanje storitve, še zlasti porazdeljene napade te vrste (ang. DDoS – Distributed Denial of Service).

Za zaščito pred nenamernimi napakami in izpadi se uporabljajo redundantna oprema in storitve, zlasti za:

- napajanje,
- komunikacijske povezave,
- komponente omrežnih naprav in strežnikov,
- omrežne naprave,
- strežnike (Savanović in Praprotnik. 2012).

Sistemi, ki imajo visoke zahteve po neprekinjenem delovanju, morajo imeti redundanco s strežniki za varnostno kopiranje in s takojšnjim shranjevanjem vseh podatkov. Veliki poslovni sistemi imajo običajno redundantne sisteme na ločenih fizičnih lokacijah. Vzpostavljena morajo biti programska orodja za spremljanje delovanja sistema in omrežnega prometa. Protiukrepi za zaščito pred napadi DoS oz. DDoS vključujejo požarne zidove in usmerjevalnike.

Zaščita pred DDoS napadi je težka naloga zaradi njihove porazdeljene narave in obsega. Dodatna oteževalna okoliščina je, da zaščita tipično zahteva sodelovanje več različnih organizacij, predvsem internetnih ponudnikov (ang. Internet Service Provider – ISP). V splošnem se za zaščito pred DDoS napadi uporablja kombinacija različne programske in strojne opreme, npr. usmerjevalniki, stikala, požarni zidovi in IDPS sistemi. Zaščita poteka v naslednjih treh korakih:

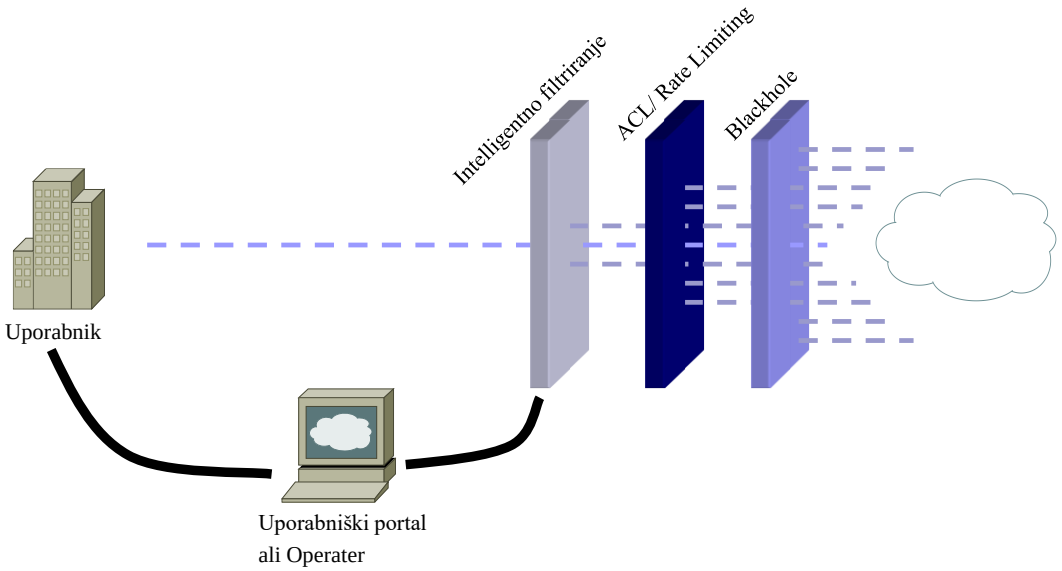
- detekcija napada,
- klasifikacija prometa in identifikacija prometa, ki povzroča napad,
- filtriranje, ki povzroči blokiranje nelegitimnega prometa in prepuščanje legitimnega prometa (Savanović in Praprotnik. 2012).

Filtriranje prometa, ki ublaži (ang. mitigation) oz. odpravi napad DDoS, se v grobem izvaja v treh stopnjah, kar prikazuje Slika 16:

- Prva stopnja je t.i. »Blackholing«, t.j. odmetavanje zlonamernega prometa pri ponudniku storitve (ISP) s pomočjo usmerjevalnega protokola.
- Druga stopnja je filtriranje prometa na osnovi omejitev prometa na podlagi pogostosti zahtev, ki prihajajo iz določenega vira prometa (ang. rate limiting) in seznamov za

nadzor dostopa (ACL – Access Control List) v aktivni omrežni opremi, ki to omogoča (npr. stikala, usmerjevalniki, požarni zidovi).

- Tretja stopnja je inteligentno (natančno) filtriranje z namenskimi sistemi za upravljanje prometa (Savanović in Praprotnik. 2012).



Slika 16: Zaščita pred DDoS napadi
Vir

(Savanović in Praprotnik, 2012)

4.6 PREPREČEVANJE ZANIKANJA

Preprečevanje zanikanja (ang. non-repudiation) je ustvarjanje pogojev, da nekdo ne more zanikati veljavnosti nečesa v elektronski obliki. Preprečevanje zanikanja se nanaša na storitev, ki zagotavlja dokaz o izvoru podatkov in celovitosti podatkov. Za pomembna sporočila in dokumente je pomembno, da ni mogoče uspešno zanikati, kdo je avtor sporočila oz. dokumenta, od kod je prišlo, pa tudi njegove verodostojnosti in celovitosti.

Namen te storitve je uporabnikom preprečiti, da bi tajili komunikacijo, prenos podatkov in elektronske transakcije, kot je npr. podpis elektronskega dokumenta ali pošiljanje in sprejemanje elektronskih sporočil. To je npr. pomembno pri pogodbenih razmerjih in uradnih dokumentih.

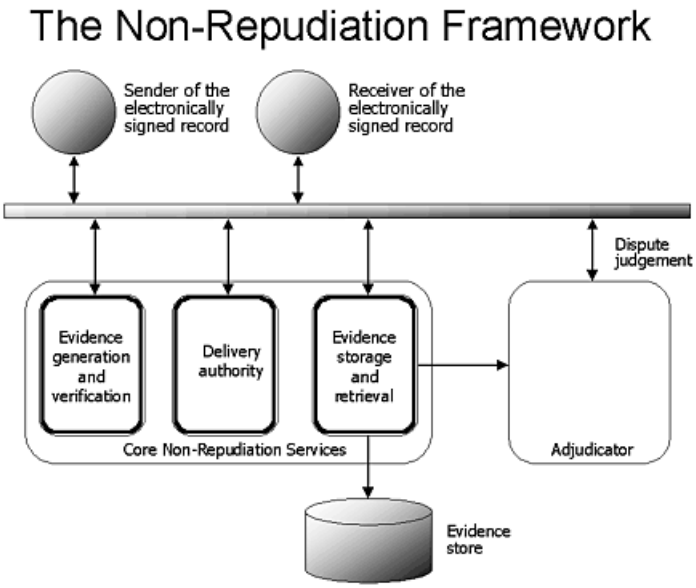
Preprečevanje zanikanja je kompleksna varnostna storitev, ki jo sestavljajo manjše (pod) storitve. Lahko je vezana na določeno vrsto aplikacije. V tem primeru je rešitev za preprečevanje zanikanja specifična za tako aplikacijo. Za preprečevanje zanikanja se uporabljajo naslednje storitve:

- šifriranje,
- digitalni podpisi,

- časovno žigosanje,
- transakcijski protokoli,
- varno shranjevanje dokazov (Savanović in Praprotnik, 2012).

Slika 17 prikazuje splošni okvir za preprečevanje zanikanja po standardu ISO, v katerem so tri ključne storitve, ki jih zagotavljajo zaupanja vredne organizacije (ang. Trusted Third Party – TTP):

- generiranje in preverjanje različnih elektronskih dokazil, kot so npr. digitalni certifikati, časovni žigi, dokazila o oddaji, dokazila o sprejemu, itd.
- zanesljiva dostava elektronskih dokazil, ki je ni mogoče zatajiti,
- shranjevanje in dostava elektronskih dokazil za potrebe kasnejšega razreševanja sporov (National Archive, 2000).



Slika 17: Preprečevanje zanikanja
(https://www.archives.gov/records-mgmt/policy/electronic-signature-technology.html)

4.7 ZASEBNOST IN ANONIMNOST

Storitve za varovanje zasebnosti in anonimnosti (ang. privacy and anonimity) varujejo uporabnika pred sledenjem pri uporabi računalnikov, omrežij in internetnih storitev ter profiliranjem oz. zbiranjem podrobnih osebnih podatkov in preferenc uporabnika.

Zasebnost in anonimnost sta dva različna pojma. Oba sta vedno bolj izpostavljena, saj se nas vse bolj prisluškuje in spremlja in to zakonito ali nezakonito. Pomembno je razumeti, da sta sestavni del naših državljanskih svoboščin, pri čemer daje pravni okvir zakonodaja.

Zasebnost je izraz, ki opisuje dejavnosti, ki jih v celoti zadržimo zase ali za omejeno skupino ljudi. Anonimnost pomeni, da želimo, da ljudje vidijo, kaj počnemo, a da ne vedo, da to počnemo mi.

Za uporabnikovo zasebnost predstavljajo veliko tveganje internetni piškotki. Za zaščito pred zlorabo le-teh je odgovoren uporabnik sam, pri čemer mora uporabljati možnosti ročnih in samodejnih nastavitev in nadzora nad piškotki v svojem spletnem brskalniku:

- potrjevanje namestitve (spletni ponudniki so po zakonu dolžni objaviti, da stran uporablja[13] piškotke),
- avtomatsko brisanje ob zaprtju brskalnika,
- sprotno ročno brisanje.

V nekaterih brskalnikih npr. obstaja možnost (v nastavitvah brskalnika), da se vsi piškotki pobrišejo ob vsakokratnem zapiranju brskalnika. Tak preprost ukrep precej poveča zaščito uporabnikove zasebnosti, po drugi strani pa precej zmanjša udobje uporabnika.

Za zagotavljanje zasebnosti lahko naredimo največ uporabniki sami. Nekaj nasvetov (Rafter, 2021):

- omejite osebne podatke, ki jih delite na družbenih omrežjih,
- brskanje v načinu brez beleženja zgodovine ali zasebnem načinu,
- uporabite spletni brskalnik, ki zagotavlja anonimnost,
- uporabite navidezno zasebno omrežje (ang. Virtual Private Network − VPN),
- pazite, kje klikate,
- zaščitite svoje mobilne podatke,
- uporabite kakovostno protivirusno programsko opremo.

Informacije na Facebooku, Twitterju, Instagramu in drugih socialnih omrežjih lahko kibernetskim kriminalcem olajšajo pridobivanje identifikacijskih podatkov posameznika, kar bi jim v nadaljevanju lahko omogočilo krajo identitete ali dostop do finančnih podatkov.

V primeru brskanja v zasebnem načinu (v Chromu se imenuje način brez beleženja zgodovine) računalnik ne shranjuje zgodovine brskanja, začasnih internetnih datotek ali piškotkov. Poudariti moramo, da tudi zasebni način ni popolnoma zaseben. Ponudnik internetnih storitev (ang. Internet service provider − ISP) še vedno vidi dejavnost brskanja. Če za brskanje uporabljamo računalnik podjetja, lahko te podatke pridobi tudi delodajalec. Razen tega nam spletna mesta, ki jih obiščemo, lahko sledijo. Spletno zasebnost lahko okrepijo anonimni iskalniki in navidezna zasebna omrežja. Anonimni iskalnik, npr. TOR, ne zbira in ne deli zgodovine iskanja ali klikov. Anonimni iskalniki lahko blokirajo tudi sledilce oglasov na spletnih mestih, ki jih obiščemo.

Navidezno zasebno omrežje (VPN) omogoča spletno zasebnost in anonimnost z ustvarjanjem zasebnega omrežja iz javne internetne povezave. VPN prikrije uporabnikov IP naslov, zato njegovim spletnim aktivnostim skoraj ni mogoče slediti. Uporaba VPN-ja je še posebej pomembna, če ste v javnem omrežju Wi-Fi, npr. v knjižnici, kavarni ali na drugi javni lokaciji.

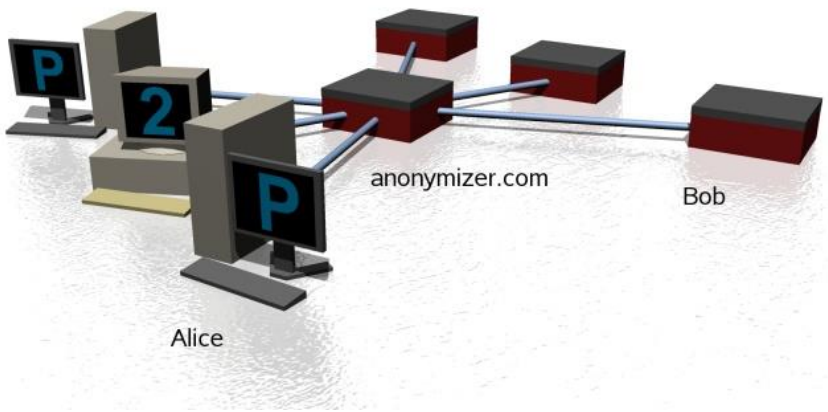
[13] Običajno je dodano: piškotke uporabljamo, da bi vam omogočili nemoteno in prijetno uporabniško izkušnjo. Z nadaljnjo uporabo te spletne strani se strinjate z našo politiko piškotkov. Lahko pa si o uporabi piškotkov preberete več.

VPN kibernetskim kriminalcem oteži kršitev spletne zasebnosti in dostop do uporabnikovih osebnih podatkov. Tehnologije VPN so opisane v posebnem poglavju.

Eden od načinov, s katerim hekerji ogrožajo spletno zasebnost, je lažno predstavljanje (ang. spoofing). Pri lažnem predstavljanju prevaranti poskušajo zvabiti finančne ali osebne podatke (ang. phishing). Pogosto to storijo s pošiljanjem lažnih e -poštnih sporočil, za katera se zdi, da so od bank, ponudnikov kreditnih kartic ali drugih finančnih institucij. V njih je pogosto zapisano, da je potrebno klikniti na povezavo in preveriti finančne podatke. Klik na povezavo uporabnika preusmeri na ponarejeno spletno stran, ki je videti kot prava stran banke ali finančne institucije. V resnici gre za lažno stran, z vnosom podatkov pa le-te prejmejo goljufi. Preden kliknete na sumljivo povezavo, premaknite kazalec miške nad povezavo, da si ogledate ciljni URL. Če ni zaupanja vreden, ne kliknite. Vedite, da vas banke ali druge finančne institucije nikoli ne bodo prosile, da posredujete račun ali finančne podatke po e -pošti.

Mnogi porabimo več časa za brskanje po spletu, odgovarjanje na e -poštna sporočila in gledanje videoposnetkov na pametnih telefonih ali tablicah kot na računalnikih. Zato je pomembno, da poskrbite za zaščito svoje zasebnosti na mobilnih telefonih in tabličnih računalnikih. Nujno uporabite geslo za zaklepanje telefona. Morda se vam zdi, da vnesete kodo vsakič, ko želite dostopati do domačega zaslona telefona, kar je pomembno, če telefon izgubite ali vam ga ukradejo. Pri nalaganju aplikacij bodite previdni. V igre in orodja za produktivnost so lahko vgrajeni nevarni virusi. Igre kupujte samo iz zakonitih in zaupanja vrednih virov. Pri iskanju po spletu ali branju e -poštnih sporočil na mobilnih napravah bodite enako previdni, kot pri uporabi prenosnega ali namiznega računalnika. Prav tako ne pozabite na posodobitev programske opreme. Posodobitve pogosto vključujejo pomembno zaščito pred najnovejšimi virusi.

Za zagotavljanje anonimnosti lahko uporabimo proxy strežnike ali pa t.i. čebulno usmerjanje (ang. Onion Routing). Slika 18 prikazuje anonimizacijski proxy strežnik, ki je posrednik med oddajnikom in sprejemnikom in pred slednjim skrije oddajnikovo identiteto (IP naslov) (Savanović in Praprotnik, 2012).



Slika 18: Proxy strežnik za anonimnost
(http://sarwiki.informatik.hu-berlin.de/Mixmaster_Remailer)

Čebulno usmerjanje bomo spoznali nekoliko kasneje.

4.8 ZAŠČITA PODATKOV PRI PRENOSIH

Eden od najpomembnejših postopkov pri zaščiti informacijske tehnologije je zaščita podatkov pri prenosih. Podatki pri prenosih pogosto fizično zapustijo organizacijo in so izpostavljeni različnim grožnjam. Pri prenosih moramo „odpreti“ komunikacijske poti, kar povzroči potencialno nevarnost nepooblaščenih vdorov v IT infrastrukturo. Za učinkovito zaščito se mora vsak posameznik, predvsem pa vsaka organizacija zavedati pomembnosti zaščite pred vsemi možnimi potencialnimi grožnjami, ki ogrožajo podatke pri komuniciranju preko omrežij. Zato je potrebno vse možne grožnje v naprej predvideti in se nanje skrbno pripraviti. Obstaja veliko potencialnih nevarnosti, od katerih so najosnovnejše:

- prisluškovanje (prestrezanje),
- ponarejanje (spreminjanje, brisanje ali vrivanje),
- pretvarjanje (spreminjanje identitete oddajnika),
- nepooblaščena uporaba virov,
- nepooblaščeno razkritje informacij,
- zanikanje sodelovanja (zakrivanje identitete oddajnika),
- DoS (Denial of Service) oz. DDoS – preprečevanje dostopa do virov ali storitev,
- analiza podatkov (Savanović in Praprotnik, 2012).

Najpogostejši način zaščite podatkov pri prenosih je šifriranje.

5 KRIPTOGRAFIJA

Kriptografija je veda o tajnosti, šifriranju, zakrivanju sporočil in o razkrivanju šifriranih podatkov. Šifriranje je pretvorba vsebine v obliko, ki je nepooblaščeni ne morejo razumeti. Ime je izpeljano iz grščine, kjer kryptós pomeni skrit, gráphein pa pisati. Za šifriranje se uporabljajo različni jezikoslovni in/ali matematični postopki - algoritmi (Wikipedia, 2021).

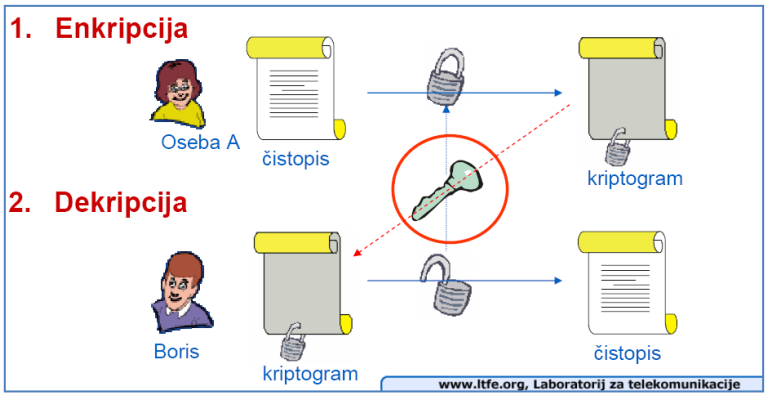
V digitalnem svetu se vsebina, ne glede na to, ali je datoteka, besedilo, fotografija, video posnetek, pogovor ali kaj drugega, z uporabo izbranega matematičnega algoritma in šifre (gesla) pretvori v nerazumljiv skupek ničel in enic (oziroma drugih znakov). Kdorkoli bi sporočilo ali vsebino prestregel, namenoma ali ne, ga ne bo zmogel razvozlati (Varga, 2017).

V e-poslovanju imamo pogosto opravka z denarjem, osebnimi podatki in drugimi pomembnimi podatki, ki jih je potrebno zaščititi pred zlorabo.

S kriptografijo dosegamo informacijske varnostne zahteve kot so zaupnost, celovitost podatkov, overjanje identitete in podatkov. Kriptografija je nastala kot posledica komunikacije v neželeni prisotnosti radovednežev, nasprotnikov ali tekmecev (Wikipedia, 2021).

Osnovno sporočilo ponavadi imenujemo čistopis (ang. cleartext, plaintext), zašifrirano pa šifropis ali tajnopis (ang. cyphertext).

Kriptiranje[14] ali šifriranje ali enkripcija je proces pretvarjanja berljivega teksta ali čistopisa v neberljivi tekst ali kriptogram (ang. cypher text), ki ga ni mogoče razumeti brez uporabe ustreznega ključa. Kriptirane podatke moramo pred uporabo dekriptirati oz. dešifrirati. To pomeni, da jih moramo pretvoriti nazaj v berljivo obliko. Postopek prikazuje Slika 19.



Slika 19: Enkripcija in dekripcija

Kriptiranje si lahko predstavljamo kot sistem za zaklepanje vrat, kjer kriptirni algoritem predstavlja ključavnico, šifrirni ključ pa ključ za njeno odklepanje. Če ključ poznamo oz. ga imamo, postopek dekripcije ni dolg. Če ga ne poznamo, pa nam primeren ključ onemogoči razumevanje podatkov.

Nevarnost prisluškovanja, ponarejanja in pretvarjanja lahko z veliko zanesljivostjo odpravimo z učinkovitim šifriranjem podatkov, kjer s pomočjo raznih šifrirnih metod spremenimo podatke v obliko, ki jo lahko dešifrirajo le pooblaščene osebe. Skrivanje vsebine sporočila pred vdiralci je osnovni namen šifriranja. Potencialni vdiralci so lahko:

- hekerji,
- upravljalci,
- sodelavci,
- državne službe in
- neznani vdiralci (Savanović in Praprotnik, 2012).

Vdiralce delimo na:

- pasivne ali prisluškovalce (posluša oz. bere vsebino),
- aktivne ali ponarejevalce (spreminja ali generira vsebino).

Že pred tisočletji so ljudje na različne načine poskušali zavarovati sporočila pred nepooblaščenimi osebami. Začetki kriptografije segajo 1900 let pred našim štetjem, v stari Egipt. Zelo znan je Cezarjev kriptogram, ki ga je uporabljal rimski cezar Julij. Deluje na principu enostavne zamenjave črk z novo abecedo, ki jo lahko enostavno dobimo tako, da pomaknemo vrstni red abecede za eno črko ali več črk. Namesto črke A lahko npr. uporabimo črko B (če premaknemo za eno mesto), namesto črke B pa črko C, itd. Ker ima takšen način 25

[14] Šifriranje sporočil poznamo še iz časov, ko si računalnikov niti zamišljali niso.

možnosti (število črk v abecedi), lahko sporočilo dešifriramo v največ 25 poskusih (Whittman in Mattord, 2019). To je enostavno celo, če nimamo računalniške pomoči pri dešifriranju.

Danes je kriptografija nepogrešljiva v številnih IT orodjih. Internetni brskalniki vsebujejo vgrajene kriptografske metode, ki omogočajo varno e-poslovanje.

V e-poslovanju potrebujemo kriptografijo za:

- ugotavljanje **verodostojnosti** pošiljatelja oz. izvora sporočila,
- zagotavljanje **zaupnosti** sporočil in podatkov,
- zagotavljanje **celovitosti** podatkov,
- **nezatajljivost** storjenega dejanja.

Zagotavljanje celovitosti podatkov pomeni, da nepooblaščena oseba podatkov ne more spremeniti. Nezatajljivost zagotavlja, da nobena stranka ne more zanikati, da je poslala ali prejela sporočilo ali zanikati pristnosti svojega podpisa na dokumentu.

Kriptografija se v e-poslovanju uporablja povsod. Izbor metode je odvisen od tega, kako pomembno je zaščititi podatke. V e-bančništvu morajo biti zaščite najboljše, saj gre za osebne podatke in denar.

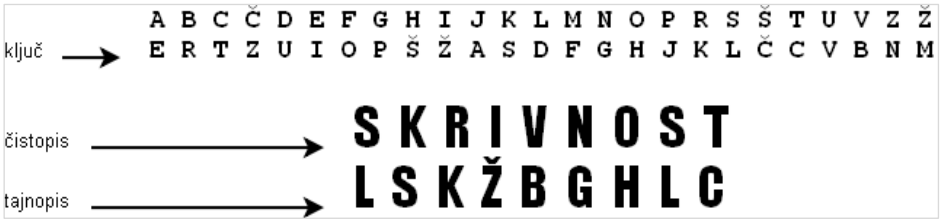
5.1 METODE ŠIFRIRANJA PODATKOV

Glede na način spreminjanje vsebine sporočila (iz čistopisa v tajnopis in nazaj) ločimo dva načina šifriranja podatkov:

- substitucijske metode šifriranja
- transpozicijske metode šifriranja (Savanović in Praprotnik, 2012).

5.1.1 Substitucijske metode šifriranja

Substitucijske metode šifriranja delujejo na naslednjem principu: posamezne črke ali dele besedila zamenjamo z novimi. Če posamezne črke čistopisa nadomeščamo z nadomestnimi črkami iz ene same poljubno razvrščene nadomestne abecede, ki predstavlja naš ključ, imenujemo takšno metodo **monoalfabetska.** Ta metoda šifriranja ima veliko slabost, da tajnopis ohranja vzorec frekvenčne porazdelitve posameznih črk iz čistopisa, zato je pri dovolj velikih besedilih (nad 50 znakov) dešifriranje enostavno s pomočjo frekvenčne analize, kjer štejemo pogostnost nastopa posameznih črk ali njihovih kombinacij (Savanović in Praprotnik, 2012).



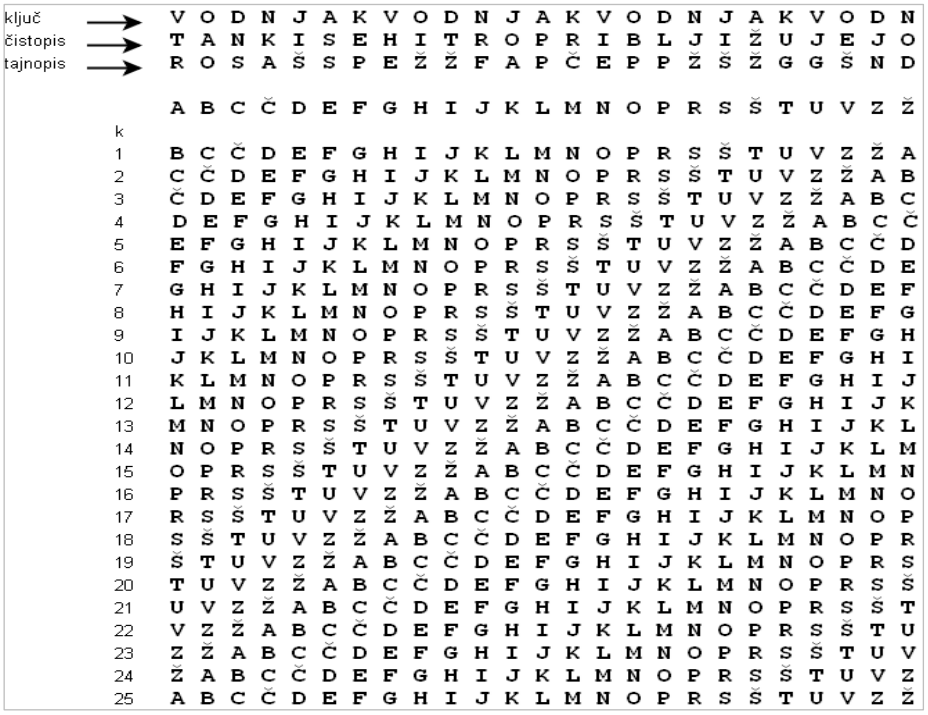
Slika 20: Primer monoalfabetskega šifriranja (Savanović in Praprotnik, 2012

Prvi opisi dešifriranja monoalfabetskih metod šifriranja so obstajali že v arabskem svetu v devetem stoletju. Slika 20 prikazuje preprost primer zamenjave črk s ključem, ki smo ga kreirali tako, da smo vtipkali zaporedje črk na tipkovnici. Šifrirano sporočilo kreiramo tako, da črke čistopisa enostavno zamenjamo s črkami, ki jih preberemo iz izbranega ključa. Tako vse črke A nadomestimo s črkami E, črke B s črkami R in tako nadaljujemo za vse črke abecede.

Boljšo metodo šifriranja je leta 1586 v svojem delu[15] opisal Blaise de Vigenère. Ugotovil je, da za učinkovito šifriranje čistopisa ni dovolj en sam korak, zato je pri šifriranju s substitucijsko metodo uporabil več korakov in s tem v tajnopisu spremenil vzorec frekvenčne porazdelitve črk čistopisa. Takšen način šifriranja imenujemo **polialfabetsko šifriranje** (Savanović in Praprotnik, 2012).

Slika 21 prikazuje primer Vigenère-jevega algoritma, kjer za ključ uporabimo besedo VODNJAK in jo ponavljamo čez celoten čistopis, ki vsebuje stavek TANKI SE HITRO PRIBLJIŽUJEJO. Za šifriranje čistopisa moramo najprej pripraviti tabelo 25 abeced, ki so med seboj zamaknjene za eno črko. Tajnopis dobimo tako, da v tabeli za vsako črko čistopisa poiščemo sečišče stolpca črke in vrstice, ki se začne s pripadajočo črko ključa. Tako za prvo črko čistopisa T poiščemo stolpec, ki se nahaja pod to črko in vrstico, ki se začne s črko V. Presečišče je črka R. V osnovi je delovanje Vigenère-jevega algoritma podobno Cezarjevemu kriptogramu, le da algoritem z vsakim korakom v bistvu uporabi drugo abecedo, rotirano za tolikokrat, kot jih določa črka iz ključa. Zato je takšno šifriranje ostalo nezlomljivo do sredine 19. stoletja, ko je Friderich Wilhelm Kasiski objavil delo, v katerem je opisal postopek za dešifriranje tega algoritma. Ugotovil je, da se pri šifriranju določene kombinacije črk zaradi ponavljajočega ključa lahko večkrat preslikajo na enak način, zato jih lahko na istem mestu opazimo tako v čistopisu kot v tajnopisu. Iz te informacije lahko ugotovimo dolžino ključa in razdelimo tajnopis na toliko monoalfabetskih substitucij, kot je dolžina ključa. Dobljene monoalfabetske tajnopise pa lahko enostavno dešifriramo z analizo pogostnosti nastopanja črk (frekvenčno analizo). Za takšno dešifriranje Vigenère-jevega algoritma je potreben le dovolj dolg tajnopis (vsaj 50 znakov) (Savanović in Praprotnik, 2012).

[15] Blaise de Vigenère „Traicté des Chiffres“, 1586

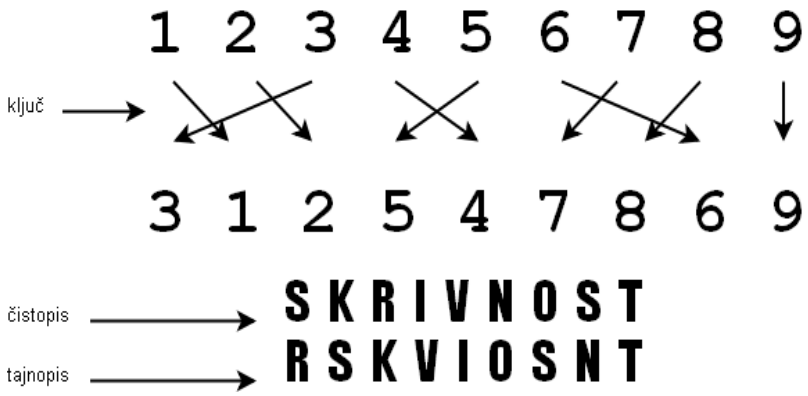


Slika 21: Primer polialfabetskega šifriranja
(Savanović in Praprotnik, 2012

5.1.2 Transpozicijske metode šifriranja

Transpozicijske metode šifriranja temeljijo na principu spreminjanja vrstnega reda znakov, besed ali celo stavkov. Enostavne transpozicijske metode šifriranja ne spreminjajo vzorca frekvenčne porazdelitve posameznih črk, zato se tudi pri tej metodi za dešifriranje (brez poznavanja ključa) uporabi enostavno kriptoanalizo s štetjem pogostosti nastopa posameznih črk ali njihovih kombinacij. Slika 22 prikazuje primer enostavne transpozicijske metode šifriranja, kjer ključ določa zamenjavo vrstnega reda zaporedja črk v čistopisu. Iz navedenega primera tudi opazimo, da sta si čistopis in tajnopis podobna, zato lahko pri tako enostavni transpoziciji relativno hitro uganemo čistopis (**RSKVIOSNT --> SKRIVNOST**). Do takšne situacije pride zato, ker je izbran ključ zelo podoben originalnemu, kar povzroči nezadovoljive transformacije čistopisa (Savanović in Praprotnik, 2012).

Možna je tudi kombinacija obeh načinov šifriranja, saj se s tem lahko izognemo slabostim obeh načinov šifriranja. **Zato je večina modernih šifrirnih metod v bistvu sestavljena iz metod, ki temeljijo na načelih substitucije in transpozicije** (Savanović in Praprotnik, 2012).



Slika 22: Transpozicijska metoda šifriranja (Savanović in Praprotnik, 2012

5.2 ALGORITMI ZA ŠIFRIRANJE

Pri metodah šifriranja s pomočjo ključa ločimo:

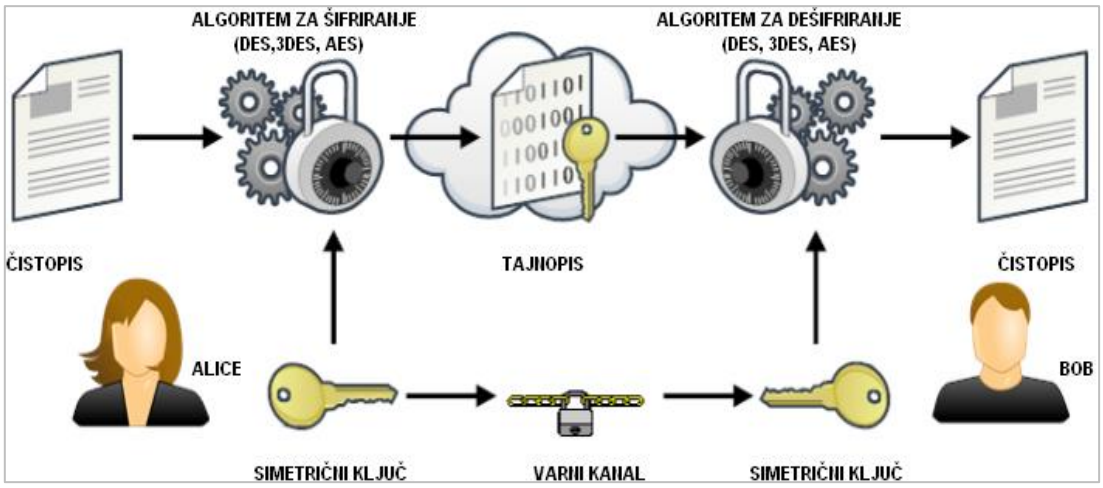
- **simetrične algoritme**, kjer sta enkripcijski ključ (E) in dekripcijski ključ (D) enaka in
- **asimetrične algoritme**, kjer sta ključa različna.

V popularnih kriptirnih sistemih se uporablja kombinacija obeh načinov (Whitman in Mattord, 2019).

5.2.1 Simetrični algoritmi za šifriranje podatkov

Pri simetričnem šifriranju uporabimo **isti** ključ tako za šifriranje (enkripcija) kot za dešifriranje (dekripcija) podatkov. Da je šifriranje dovolj učinkovito, mora ostati ključ tajen za vse, razen za pošiljatelja in prejemnika. To pomeni, da takšno šifriranje sloni na predpostavki, da si pošiljatelj in prejemnik varno izmenjata ključ. Zato je pri simetričnem šifriranju potrebno posvetiti veliko pozornost varni izmenjavi ključev. V primeru, da do ključa pride nepooblaščena oseba, postane šifriranje s tem ključem popolnoma neučinkovito. Pri simetričnem šifriranju je pogosto tudi v navadi, da se ključ periodično menja, saj se s tem povečuje stopnja varnosti (Praprotnik in Savanović, 2012).

Pri simetričnem šifriranju se pojavi tudi problem istovetnosti. Prejemnik ne more tretji osebi neizpodbitno dokazati, kdo je pošiljatelj, saj je lahko sporočilo sam ponaredi. Zato se simetrični ključi ne morejo uporabiti za digitalne podpise.



Slika 23: Simetrično šifriranje
(Savanović in Praprotnik, 2012

Če ključ pridobi tretja oseba, npr. zaradi vdora, pošiljatelj in prejemnik morda ne vesta, da je prišlo do zlorabe ali pa za to izvesta prepozno.

Pomembna aktivnost pri simetričnem šifriranju je prenos ključa. Ta proces mora biti izveden po ločenem kanalu in ne po istem kot se prenese šifrirano sporočilo.

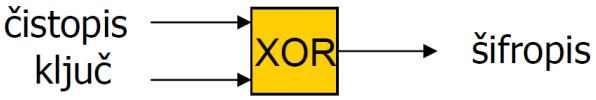
Simetrične algoritme delimo na:

- pretočno šifriranje (ang. stream cipher), kjer sproti šifriramo sporočilo in
- blokovno šifriranje (ang. block cipher), kjer sporočilo razdelimo na posamezne bloke velikost *b* in šifriramo vsak blok zase.

Pretočno šifriranje

Pretočno ali tekoče šifriranje (ang. stream cipher / bit stream chiper) je metoda, kjer se sproti preslika vsak znak. Sporočilo šifriramo bit za bitom. Primer te vrste šifriranja je substitucijsko šifriranje.

Primer zelo hitrega pretočnega šifriranja je uporaba XOR (ekskluzivna disjunkcija).

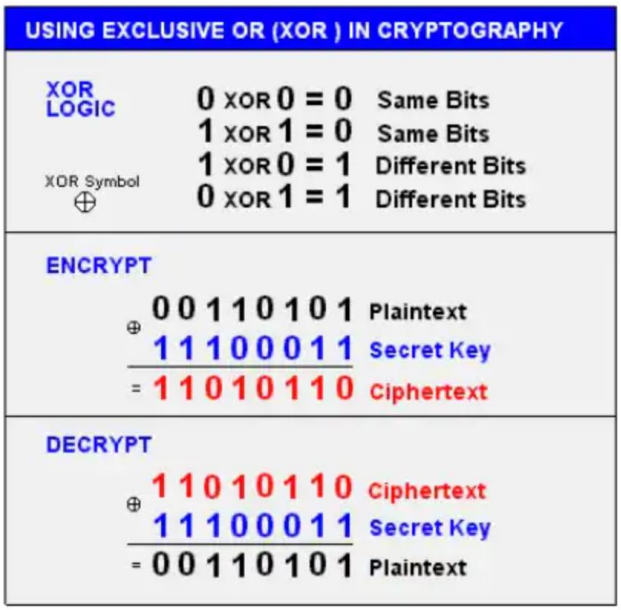


Slika 24: XOR enkripcija

XOR (ang. Exclusive OR) je Boolova logična operacija, ki se v kriptografiji pogosto uporablja. XOR primerja dva vhodna bita in ustvari en izhodni bit. Logika je preprosta. Če sta bita enaka, je rezultat 0.[16] Če sta bita različna, je rezultat 1.

Primer algoritma XOR šifriranja je na sliki (Slika 25).

[16] Seštevanje po modulu 2: 1+1=0 in 0+0=0; 1+0=1 in 0+1=1



Slika 25: Primer XOR šifriranja
(https://www.tech-faq.com/xor-encryption.html, 24. 8. 2021)

Recimo, da je čistopis CAT, ključ pa VVV. Na sliki (**Napaka! Vira sklicevanja ni bilo mogoče n ajti.**) vidimo rezultat šifriranja. Zaradi lažjega prikaza smo uporabili 8 bitno kodiranje.

Besedilo	
CAT v binarni kodi	01000011 01000001 01010100
VVV v binarni kodi	01010110 01010110 01010110
Tajnopis	000101010001011100000010

Slika 26: Primer XOR šifriranja besede CAT s ključem VVV

Blokovno šifriranje

Blokovno šifriranje (ang. block ciphers) je metoda, kjer sporočilo razdelimo na bloke enake velikosti (*b*) in s ključem šifriramo vsak blok zase. Ker zadnji blok največkrat ni popolnoma poln (velikost bloka *b* ni večkratnik velikosti sporočila), ga moramo dopolniti z izbranimi podatki. Pri šifriranju bloka s pomočjo ključa uporabimo razne matematične operacije (npr. permutacije, substitucije) tako, da ima šifrirani blok popolnoma izbrisane vzorce iz vhodnega bloka in se skoraj približa naključnemu vzorcu (Savanović in Praprotnik, 2012).

Posamezen blok ima lahko različno dolžino, npr. 8, 16, 32, 64, 128, 256, 512.

Poznamo številne simetrične kriptirne algoritme, ki temeljijo na blokovnem šifriranju. Zelo znan je **DES** (ang. Data Encryption Standard), ki je bil razvit pri IBM. Uporablja ključe dolžine 128 pred tem pa ključe dolžine 64. Danes velja za nezanesljivega, saj ga je možno zlomiti v realnem času. Nadomestil ga je **3DES** (Triple DES), ki uporablja tri ključe z dolžino 64 bitov (skupaj torej 192 bitov). Nekoč je veljal za industrijski standard, a ga danes pospešeno opuščajo in zamenjujejo z drugimi šifrirnimi algoritmi.

Leta 2001 je Ameriški inštitut za standardizacijo in tehnologijo (NIST) izbral nov algoritem za šifriranje AES, s katerim bi v vseh poslovnih aplikacijah nadomestili zastarel algoritem DES. **AES** (Advanced Encryption Standard) je znan tudi pod imenom Rijndael. Za zaščito podatkov ga uporabljajo številna podjetja in vlade tega sveta. Velja za neprebojnega, uporablja pa lahko ključe treh različnih dolžin – 128, 256 ali 512 bitov. 512-bitno šifriranje podatkov AES omogoča res vrhunsko zaščito (Whitman in Mattord, 2019).

AES je simetrični algoritem, saj za šifriranje in dešifriranje uporablja isti ključ.

AES je najbolj priljubljen šifrirnik datotek na svetu. Ocenjujejo, da se uporablja za šifriranje več kot 50% vseh podatkov po vsem svetu. Pogosto se uporablja v protokolih varnega prenosa datotek, kot so FTPS, HTTPS, SFTP, AS2, WebDAVS in OFTP. Uporablja se tudi v varnih protokolih za brezžična omrežja. Tudi večina storitev VPN uporablja najvišjo raven šifriranja AES (Chernev, 2021).

5.2.2 Asimetrični algoritmi za šifriranje podatkov

Velika slabost simetričnih algoritmov šifriranja je zahteva po tajni distribuciji ključa od oddajnika do sprejemnika, saj se isti ključ uporablja tako za šifriranje sporočila kot za tudi dešifriranje. Rešitev tega problema sta leta 1976 ponudila W. Diffie in E. Hellman. Njuna rešitev je temeljila na preprosti ideji o dveh med seboj povezanih kriptografskih ključih.

- Prvi ključ, s katerim šifriramo neko sporočilo, je **javen** in dostopen vsakomur, vendar neuporaben za dešifriranje.
- Dešifriranje je možno samo z zasebnim ključem, ki ga poseduje pooblaščena oseba.

Javni in zasebni ključ tvorita **par asimetričnih ključev**.

V računalništvu se kot najvišja stopnja zaščite podatkov uporablja asimetrična kriptografija, ki temelji na uporabi para med seboj povezanih ključev: javnega in zasebnega. Javni ključ je, kot ime pove, javen in ga lastnik lahko posreduje komurkoli, ki želi z njim sodelovati v varni komunikaciji. Zasebni ključ ima varno shranjen le lastnik.

Povezava med javnim in zasebnim ključem je naslednja:

- sporočilo, ki je bilo kriptirano z javnim ključem, se lahko dekriptira samo z zasebnim ključem iz istega para.
- Sporočilo, ki ga je pošiljatelj kriptiral s svojim zasebnim ključem, lahko prejemnik dekriptira samo z uporabo javnega ključa iz istega para.

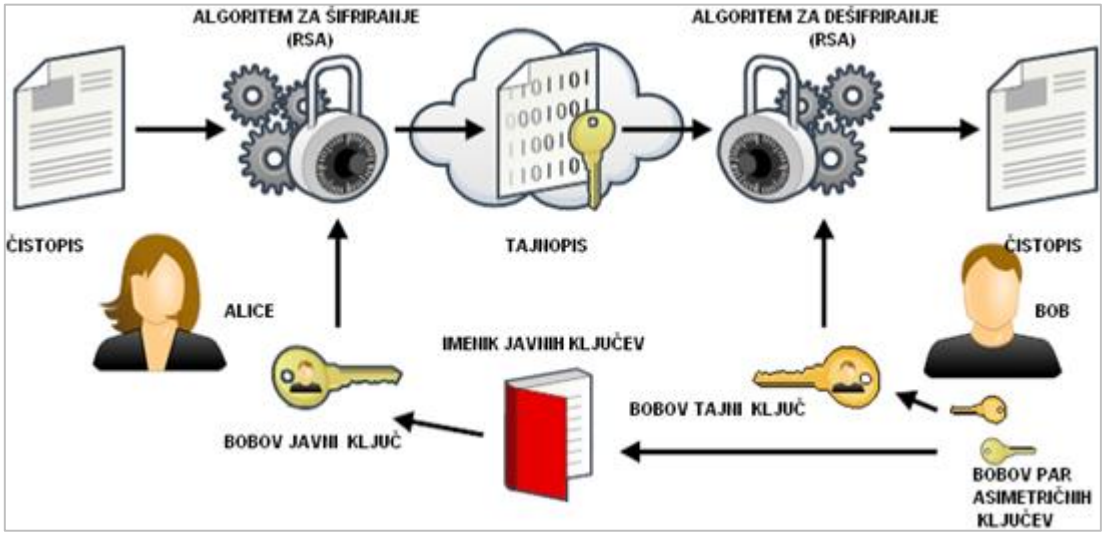
Možna je torej ena ali druga možnost.

Primeri uporabe:

- lastniku zasebnega ključa pošljemo sporočilo, šifrirano z njegovim javnim ključem, in le on ga lahko dešifrira s svojim zasebnim ključem. Na tak način nam npr. banka posreduje podatke o finančnem stanju na našem računu.
- Lastnik zasebnega ključa s kvalificiranim digitalnim potrdilom podpiše dokument. Vsakdo, ki ima njegov javni ključ pa lahko preveri ali je sporočilo podpisal lastnik zasebnega ključa in, ali je vsebina ostala nespremenjena. Na tak način npr. banki pošljemo zahtevek za plačilo položnice, banka ga preveri in izvede.

To je varno, ker sta javni in zasebni ključ matematično povezana, vendar je na podlagi poznavanja javnega ključa nemogoče določiti zasebni ključ.

Svoj javni ključ dobimo s prevzemom digitalnega potrdila, ki ga bomo spoznali v nadaljevanju. Zasebni ključ se ustvari na pametni kartici, USB ključu ali računalniku.



Slika 27: Asimetrično šifriranje
(Savanović in Praprotnik, 2012)

Slika 27 prikazuje tipičen primer uporabe asimetričnih ključev za šifriranje sporočila, ki ga Alice želi poslati Bobu. V prvem koraku mora Bob kreirati par asimetričnih ključev in svoj javni ključ objaviti v imeniku javnih ključev. Alice iz imenika pridobi Bobov javni ključ in z njim s pomočjo asimetričnega algoritma zašifrira svoje sporočilo. Na ta način šifrirano sporočilo Bobu brez skrbi pošlje po nezavarovanih kanalih (Internet), saj objavljen Bobov javni ključ ne omogoča dešifriranja tega sporočila. Za dešifriranje je potreben Bobov zasebni ključ, ki ga ima Bob skrbno spravljenega pri sebi. Zato lahko le on dešifrira poslano sporočilo s pomočjo asimetričnega algoritma za dešifriranje in svojega zasebnega ključa (Savanović in Praprotnik, 2012).

Asimetrična kriptografija je veliko počasnejša od simetrične, saj uporablja matematične operacije, ki zahtevajo več procesorske moči kot simetrična kriptografija, zaradi zahtevane varnosti pa mora uporabljati tudi daljše ključe. **Zato se v praksi največkrat uporablja**

hibridni sistem, kjer se asimetrično šifriranje uporabi samo za varno izmenjavanje simetričnih ključev, simetrično pa za izmenjavo vsebine sporočila (Savanović in Praprotnik, 2012; Whitman in Mattord, 2019).

RSA algoritem

RSA algoritem je nastal leta 1977 na MIT (Massachusetts Institute of Technology). Ime je dobil po začetnih kraticah svojih avtorjev (Ronald Rivest, Adi Shamir in Leonard Adelman), ki so algoritem tudi patentirali (patent je potekel leta 2000) (Savanović in Praprotnik, 2012). RSA je eden najpopularnejših algoritmov za poslovne namene, saj je vgrajen v spletne brskalnike za zagotavljanje varnosti e-poslovanja.

RSA je asimetrični šifrirnimi algoritem, ki ustvarja ključe z najmanjšo dolžino 128 bitov. Ključi RSA omenjene dolžine niso varni, saj jih lahko napadalec z »grobo silo« razbije v vsega nekaj sekundah, zato varnostni strokovnjaki v primeru zaščite z algoritmom RSA priporočajo uporabo večje ključa dolžine ključev. Povprečni ključ RSA je danes (l. 2021) dolg 2048 bitov. Forum CAB[17] je določil, da morajo biti ključi, ki se uporabljajo za podpisovanje programske opreme, dolgi vsaj 3072 bitov, če uporabljamo RSA (Kee, 2021).

Nekateri trdijo, da je RSA ranljiv in da je čas, da se ga opusti. Star je že 45 let, pa še vedno prevladuje, čeprav so objavili številne ranljivosti. Kar 90 % internetnih povezav se začne z uporabo RSA (kot del SSL handshake), zato bi bil napad na tem mestu katastrofalen. Problem je dolžina ključa, saj dosežemo meje, ko dosežemo 4.096 bitov. Problem RSA je v tem, da z daljšanjem ključev povečanje varnosti ni sorazmerno s povečanjem računalniške moči, ki je potrebna za njihovo uporabo. Ranljivosti je še več. Vsekakor pa je zanimivo, da je algoritem precej starejši od svetovnega spleta in da se je tako dolgo obdržal kot vodilni algoritem (Kee, 2021).

Dolžina šifrirnih ključev

Moč šifrirnih sistemov se meri tudi po bitni dolžini ključev. Z večanjem dolžine ključa se poveča število potrebnih poskusov, s tem pa tudi časa, da se zlomi šifra. Časovna kompleksnost je eksponentna (Whitman in Mattord, 2019).

Če bi imeli 3 bitni sistem lahko z njim zapišemo le 8 znakov (000, 001,010, 011, 100, 101, 110 in 111). 8 bitni sistem ima 256 možnih ključev. Z izbiro 24 bitnega ključa (kar je še vedno izjemno šibko) se število možnosti poveča na 16,8 milijonov možnosti.

Kot se lahko prepričamo na sliki (Slika 28) veljajo v današnjem času ključi bitne dolžine od 128 dalje za nezlomljive v realnem času, saj bi bilo potrebno izjemno veliko let za razbitje z »napadom z grobo silo« (Whitman in Mattord, 2019). Ker pa so računalniški sistemi vedno bolj zmogljivi in je možno procesorsko moč združiti, se potrebno število let za razbijanje zmanjšuje.

[17] CA/Browser Forum je skupina certifikatskih agencij (CA).

Key length (bits)	Maximum Number of Operations (guesses)	Maximum Time to Crack	Estimated Average Time to Crack
8	256	0.0000000085 seconds	0.0000000043 seconds
16	65,636	0.0000022 seconds	0.00000109 seconds
24	16,777,216	0.00056 seconds	0.00028 seconds
32	4,294,967,296	0.143 seconds	0.072 seconds
56	72,057,594,037,927,900	27.800 days	13.9 days
64	18,446,744,073,709,600,000	19.498 years	9.7 years
128	3.40282E+38	359,676,102,360,201,000,000 years	179,838,051,180,100,000,000 years
256	1.15792E+77	122,391,435,436,027,000,000,000,000,000,000,000,000,000,000,000,000,000 years	61,195,717,718,013,400,000,000,000,000,000,000,000,000,000,000,000,000 years
512	1.3408E+154	14,171,960,013,891,600,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000 years	7,085,980,006,945,820,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000 years

Table 8-7 Encryption Key Power

18

Slika 28: Moč ključa glede na dolžino
(Whitman in Mattord, 2019)

5.2.3 Zgoščevalne funkcije

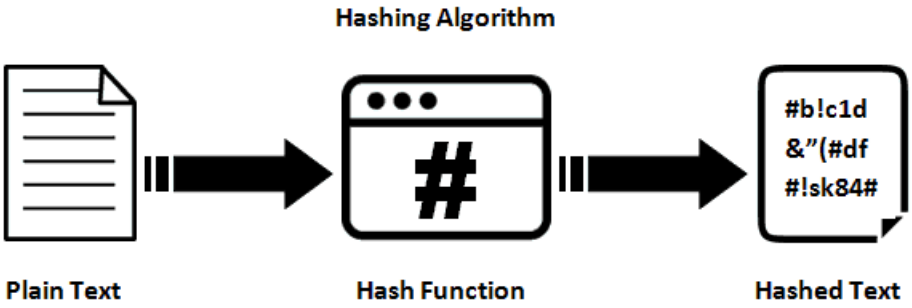
Zgoščevalna funkcija (ang. hash function) je matematični algoritem, ki dobi kot vhod poljubno dolgo sporočilo, kot izhod pa vrne fiksno dolgo binarno vrednost (npr. 128 bitov). To vrednost imenujemo zgoščena vrednost (ang. hash value). Predstavlja povzetek sporočila (ang. message digest). Včasih to vrednost imenujemo tudi prstni odtis (ang. fingerprint) sporočila, saj se algoritem uporablja za potrjevanje celovitosti (integritete) sporočila.

Namen zgoščevanja dokumentov je ustrezno zmanjšanje količine vhodnih podatkov, ki jih nato s pomočjo asimetričnega ključa šifriramo v ustrezen digitalni podpis.

Vsak dokument bi lahko v celoti podpisali z asimetričnim ključem, vendar bi bili takšni postopki dolgotrajni in procesorsko potratni, hkrati pa bi morali poleg dokumenta prenašati še šifriran dokument, ki bi bil iste velikosti kot originalen. Pri dokumentih majhne velikosti to ne bi predstavljalo problema, dokumenti z ogromno količino podatkov pa bi brez dvoma upočasnili delovanje vsakega sistema. Za podpisovanje ne potrebujemo celotnega dokumenta, ampak samo povzetek, ki nedvoumno opredeljuje vsebino dokumenta (Savanović in Praprotnik, 2012).

Zgoščevalna funkcija mora zadostiti naslednjim zahtevam (Savanović in Praprotnik, 2012):

- dva različna dokumenta se praktično ne smeta preslikati v isti povzetek (ne sme priti do kolizije – ang. collision),
- pri vsaki uporabi zgoščevalne funkcije nad istim (nespremenjenim!) dokumentom se morajo podatki preslikati v enak povzetek,
- iz povzetka je nemogoče pridobiti kakršnokoli vsebino dokumenta (enosmernost operacije),
- vsaka manjša sprememba vhodnega dokumenta mora povzročiti večjo spremembo povzetka (ang. avalanche effect).



Slika 29: Postopek zgoščevanja dokumenta
Vir: https://networkencyclopedia.com/hashing-algorithm/

Zgoščena vrednost sporočila, ki se izračuna na avtorjevi (pošiljateljevi) strani, se mora ujemati z zgoščeno vrednostjo sporočila, ki jo izračuna prejemnik. Če se vrednosti ujemata, to pomeni, da se sporočilo pri prenosu ni spremenilo.

Zgoščevalne funkcije morajo biti enosmerne operacije, kar pomeni, da

- isto originalno sporočilo vedno generira isto zgoščeno vrednost,
- zgoščena vrednost pa ne more biti uporabljena za določitev vsebine sporočila.

Zgoščevalni algoritmi ne zahtevajo uporabe ključev, je pa možno dodati MIC (ang. message integrity code), ki dovoljuje dostop do povzetka (ang. message digest) le določenim uporabnikom.

Najbolj znani algoritmi za zgoščevanje so:

- **MD2, MD4, MD5** (**Message Digest**). Serijo algoritmov za zgoščevanje MD je razvil Ronald Rivest (MIT, RSA Inc.), saj je vsak starejši algoritem sčasoma postal nezanesljiv (MD2, MD4). Tudi v algoritmu MD5 so našli ranljivosti. Vsi MD algoritmi so blokovne funkcije, ki vsak čistopis pretvorijo v 128 bitni povzetek in so optimizirani za 32 bitne računalnike. Zaradi odkrite ranljivosti so strokovnjaki za kodiranje začeli priporočati uporabo drugih varnostnih algoritmov.
- **SHA1 (Secure Hash Algoritem)** SHA1 algoritem je razvil Ameriški inštitut za standardizacijo in tehnologijo (NIST) na podlagi idej iz MD4 algoritma. Tudi SHA je blokovni algoritem, ki vhodne bloke velikosti 512 bitov obdeluje v petih 32 bitnih registrih in tako generira končni povzetek velikosti 160 bitov. Načeloma je algoritem

SHA1 varnejši od MD5, vendar so tudi za SHA1 že leta 2005 objavili raziskave o njegovi ranljivostih.

- **SHA-256 in SHA-512** prav tako priporoča NIST. SHA-256 in SHA-512 sta novejša zgoščevalna algoritma. Število bitov, ki se uporablja v posameznem algoritmu je merilo za moč algoritma proti koliziji (ang. collision attack) (Whitman in Mattord, 2019)

Uporaba zgoščevalnih funkcij:

Zgoščevalni algoritmi se uporabljajo v številnih primerih:

- za zaščito gesel: **gesla se hranijo v zgoščeni obliki**

  Zgoščevalni algoritmi se uporabljajo v sistemih, kjer se preverjajo gesla (ang. passwords) za potrjevanje identitete uporabnika. Pri prvi uporabnikovi izbiri novega gesla v določenem sistemu se generira zgoščena vrednost, ki si jo sistem zapomni. Pri vsakem naslednjem vstopu v sistem z geslom, le-ta preveri, če je shranjena zgoščena vrednost enaka sveže izračunani zgoščeni vrednosti.

- kot pseudo naključni generator števil, pri generiranju naključnih imen datotek (npr. http://www.dnevnik.si/uploads/image_cache/305d 4e28924252f4251b2baadb6dbc6a.jpeg)
- za preverjanje integritete pri prenosu datotek (npr. v P2P omrežjih)
- za preverjanje integritete arhivskih in drugih datotek
- pri implementaciji digitalnega podpisa in časovnega žigosanja
- za zagotavljanje integritete podatkov pri digitalni forenziki (Kovačič, 2018)

Zgoščevalni algoritmi so hitri in učinkoviti, vendar zagotavljajo samo integriteto čistopisa. Zato se mora pri prenosu čistopisa in povzetka preko nezanesljivih povezav obvezno opraviti še šifriranje čistopisa in povzetka.

Druga slabost je njihova ranljivost, ki se z dostopom do vse večjih procesorskih moči stalno povečuje. S tem se zastavlja vprašanje popolne integritete starejših čistopisov (npr. starejših digitalno podpisanih pogodb), saj stalno naraščanje procesorske moči in nova odkritja na tem področju kompromitirajo obstoječe in starejše zgoščevalne funkcije.


Zgoščevalno funkcijo uporabljajo tudi operacijski sistemi (OS) za kontroliranje uporabniških gesel. Namesto da OS shrani celotno uporabniško geslo, shrani samo povzetek gesla, ker le-ta zadostuje za kontrolo pravilnosti vnesenega gesla. S tem se prepreči možnost razkritja uporabniškega gesla pri kompromitaciji operacijskega sistema, saj pri močni zgoščevalni funkciji iz razkritega povzetka gesla ne moremo ugotoviti originalnega gesla (Savanović in Praprotnik, 2012).


Windows 10 za zgostitev gesla uporabljajo algoritem MD4 (Microsoft, 2021).

5.2.4 Mešani sistem šifriranja

Mešani - simetrični in asimetrični postopek šifriranja uporabimo na naslednji način:

- Asimetrični postopek uporabimo za izmenjavo začasnega **sejnega** ključa.
- Po simetričnem postopku s sejnim ključem šifriramo in dešifriramo sporočilo.

Pošiljatelj naključno generira sejni ključ, s katerim šifrira sporočilo. Ključ s katerim je sporočilo šifrirano, se šifrira z javnim ključem naslovnika. Pošiljatelj pošlje sporočilo, šifrirano s simetričnim algoritmom in zraven še asimetrično šifriran ključ, s katerim je bilo sporočilo šifrirano.

Prejemnik prejme šifrirano sporočilo in šifriran sejni ključ. S svojim privatnim tajnim ključem dešifrira sejni ključ. Na osnovi sejnega ključa dešifrira sporočilo.

5.3 DIGITALNI PODPIS IN PKI

Tematiko v Sloveniji urejajo naslednji zakoni:

- Zakonu o elektronskem poslovanju in elektronskem podpisu - ZEPEP (Uradni list RS, št. 98/04[18] – uradno prečiščeno besedilo),
- Zakon o spremembah in dopolnitvi Zakona o elektronskem poslovanju in elektronskem podpisu (ZEPEP-B) (Uradni list RS, št. 46/14),
- Zakon o elektronskem poslovanju na trgu - ZEPT (Uradni list RS, št. 61/06) in njegove dopolnitve
- Zakon o elektronski identifikaciji in storitvah zaupanja – ZEISZ (Uradni list RS, št. 121/21)

Ker gre za področje, ki je z rastjo digitalizacije vse pomembnejše, pričakujemo precej razvoja tudi na zakonodajnem področju. Kateri zakoni oz. dopolnitve so v veljavi, se da preveriti na spletni strani http://www.pisrs.si/Pis.web/ - Pravni informacijski sistem. Omogoča iskanje in pregledovanje zakonov, objavljena pa so tudi uradna in neuradna prečiščena besedila.

5.3.1 Elektronski in digitalni podpis

Elektronski podpis je vsak podpis v elektronski obliki, npr. tudi če je izveden z elektronskim pisalom (Islovar, 2021).


Elektronski podpis je tudi podpis, ki ga lastnoročno vnesemo na poštarjevo tablico ali mobilni telefon pri prevzemu poštne pošiljke.

Elektronsko lahko podpišemo ponudbo, pogodbo (npr. z banko o sklenitvi depozita), davčno napoved, bančno nakazilo… Druga pogodbena stranka bi morala imeti nekakšen dokaz, da smo

[18] Uradno prečiščeno besedilo zajema tudi spremembe in dopolnitve ZEPEP-A

dokument res podpisali mi in ne nekdo drug. To še zlasti velja, kadar imamo opravka z denarjem. Tega pa kakršen koli elektronski podpis ne omogoča.

Digitalni podpis (ang. digital signature) je niz šifriranih znakov, dodan ali logično povezan z drugimi podatki, ki omogoča **preverjanje istovetnosti podatkov in podpisnika** (Islovar, 2021).

Digitalni podpis pa nam ne zagotavlja zasebnosti podatkov. Osnovna funkcija digitalnega podpisa je namreč v dokazovanju identitete podpisnika elektronskega dokumenta in zagotavljanju celovitosti podatkov oziroma zaščite pred spreminjanjem vsebine e-dokumentov.

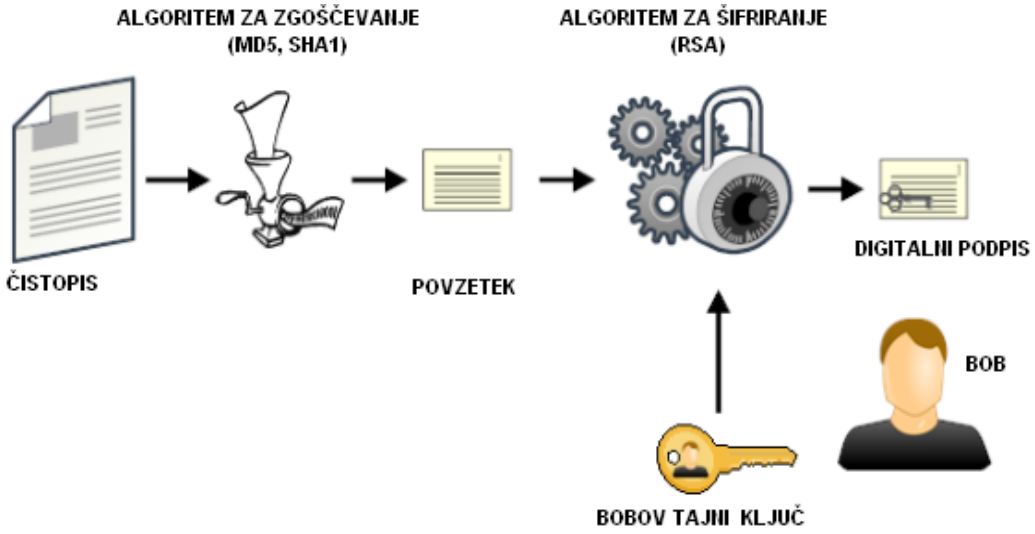
Namen digitalnega podpisa je:

- zagotavljanje celovitosti podatkov (da se na poti niso spremenili),
- nedvoumna potrditev, da je neko sporočilo šifrirala določena oseba.

Z digitalnim podpisom se prepreči zatajevanje podpisanega dokumenta, saj lastnik podpisa ne more zanikati. Digitalni podpis nekega dokumenta v bistvu predstavlja „prstni odtis“ njegove vsebine, ki je unikaten, kar pomeni, da ima lahko vsak dokument samo en prstni odtis (Savanović in Praprotnik, 2012).


Digitalno lahko podpišemo PDF dokument. Dokument ni šifriran in ga lahko prebere vsak, ki ga vidi ali prejme. Digitalni podpis zagotavlja, da je dokument podpisala določena oseba in da se po podpisu vsebina ni spremenila.

Na podlagi dokumenta, ki ga želimo poslati podpisanega, najprej s pomočjo zgoščevalne funkcije (hash) naredimo povzetek oz. zgoščeno vrednost oz. prstni odtis[19]. Dobljeno zgoščeno vrednost šifriramo s pomočjo zasebnega ključa. Rezultat šifriranja je digitalni podpis dokumenta. Prejemniku hkrati pošljemo originalni dokument in njegov digitalni podpis.



Slika 30: Postopek kreiranja digitalnega podpisa (Savanović in Praprotnik, 2012)

[19] Uporabljajo se vsi trije izrazi.

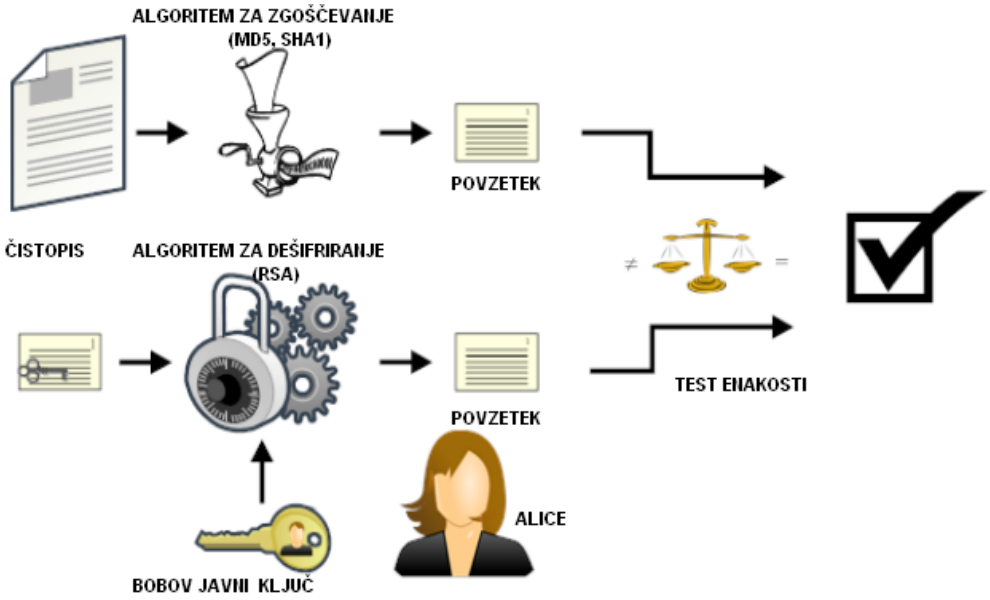
Prejemnik zgoščeno vrednost dešifrira ter jo primerja z zgoščeno vrednostjo dejansko prejetega sporočila.

Slika 30 prikazuje enostaven postopek podpisovanja nekega dokumenta. Bob iz izbranega čistopisa s pomočjo algoritma za zgoščevanje izdela njegov povzetek. Nato podpiše dobljen povzetek s svojim zasebnim (tajnim) ključem s pomočjo asimetričnega algoritma za šifriranje. Digitalno podpisan povzetek predstavlja digitalni podpis čistopisa, s katerim lahko Bob zagotavlja neokrnjenost čistopisa in njegovo overitev, hkrati pa Bob ne more zanikati tega podpisa (preprečevanje tajenja) (Savanović in Praprotnik, 2012).

Če želi Bob poslati Alice digitalno podpisan dokument, ji mora poslati originalen čistopis in digitalni podpis. **Digitalni podpis ne zagotavlja zaupnosti.**

Pri preverjanju istovetnosti prejetega in podpisanega dokumenta moramo le-tega najprej zgostiti in dobljene podatke preveriti s priloženim digitalnim podpisom, ki ga predhodno dešifriramo s pomočjo javnega ključa pošiljatelja. Če sta vsebini identični, je priložen dokument originalen in resnično podpisan s strani dotične osebe (Savanović in Praprotnik, 2012).

Slika 31 prikazuje postopek preverjanja elektronskega podpisa. Alice prejme Bobov čistopis in izvleček z njegovim digitalnim podpisom. Alice iz prejetega čistopisa s pomočjo algoritma za zgoščevanje izdela nov izvleček čistopisa. Hkrati s pomočjo Bobovega javnega ključa dešifrira podpisan izvleček, ki ga je prejela od Boba. Če se izdelan izvleček Bobovega čistopisa in Bobov dešifriran izvleček popolnoma ujemata, je Bobov digitalni podpis pristen in prejeti čistopis neokrnjen (Savanović in Praprotnik, 2012).



Slika 31: Preverjanje istovetnosti poslanega sporočila (Savanović in Praprotnik, 2012)

Če je zaupnost pomembna, mora Bob v primeru, da digitalno podpisan dokument pošilja preko nezaščitenega prenosnega kanala (npr. internet), pred pošiljanjem originalen čistopis in digitalno podpisan povzetek zašifrirati s javnim ključem, ki ga prejme od Alice.

5.3.2 Infrastruktura javnih ključev

Opisani postopek digitalno podpisanega dokumenta ne zagotavlja zaupnosti. Šifrirano bi moralo biti tudi originalno sporočilo oz. čistopis, kar rešujemo z uporabo ustreznih algoritmov.

Pri uporabi dovolj dolgih ključev je postopek z uporabo asimetrične kriptografije zelo zanesljiv, vendar ima eno pomanjkljivost. Oseba (Alice), ki želi uporabiti javni ključ druge osebe (Bob), ne more nedvoumno zaupati temu ključu, saj lahko tretja oseba ta ključ nadomesti s svojim. Nastalo situacijo označimo kot napad s posrednikom (ang. man-in-the-middle). Da bi lahko preprečili takšne situacije, je potrebno vpeljati sistem ustanov, ki jamčijo za pristnost javnih ključev. Zato so zasnovali infrastrukturo javnih ključev (ang. public key infrastructure - PKI), ki sloni na principu uporabe treeeetjih, zaupanja vrednih ustanov (ang. Trusted Third Party - TTP) (Savanović in Praprotnik, 2012).

Digitalno potrdilo je računalniški zapis, ki vsebuje podatke o imetniku (ime, e-naslov, enolična številka,...), njegov javni ključ, podatke o overitelju oz. izdajatelju digitalnega potrdila ter obdobje veljavnosti digitalnega potrdila, ki je digitalno podpisan z zasebnim ključem izdajatelja potrdila (SI-Trust[20], 2021). Digitalno potrdilo (ang. Digital Certificate) je sodobna alternativa klasičnim osebnim identifikatorjem (osebna ali zdravstvena izkaznica, potni list, bančna kartica, ...), s specifičnim namenom - zagotavljanju varnega in legitimnega e-poslovanja.

Digitalna potrdila so sestavni del tehnoloških rešitev, ki nudijo dve osnovni možnosti za zasebnost v elektronskem poslovanju in komuniciranju:

- šifriranje podatkov, ki zagotavlja zaupnost, in
- digitalni podpis, ki predstavlja sodobno alternativo klasičnemu podpisu, zagotavlja pa:
    - identiteto imetnika digitalnega potrdila in nezatajljivost lastništva poslanih e-podatkov, in
    - celovitost (integriteto) sporočila, kar pomeni, da samo dela podatkov ni mogoče spremeniti ali drugače popraviti brez (vednosti) podpisnika (SI-Trust, 2021).

Infrastruktura javnih ključev je sistem, ki skrbi za izdajo, upravljanje in preklic digitalnih potrdil ter časovno žigosanje dokumentov. Zajema organizacijski, tehnični in pravni vidik upravljanja javnih ključev. Osrednja institucija je overitelj digitalnih potrdil.

PKI skrbi za vse postopke, ki so potrebni za učinkovito delovanje sistema zaupanja vrednega digitalnega podpisovanja (Savanović in Praprotnik, 2012):

- generiranje in hranjenje ključev,
- overjanje lastnikov ključev,
- izdajanje digitalnih potrdil javnih ključev,
- objava izdanih digitalnih potrdil (seznam),
- objava preklicanih digitalnih potrdil (seznam),
- časovno žigosanje dokumentov.

[20] Državni center za storitve zaupanja

5.3.3 Digitalna potrdila

Pri uporabi asimetričnih algoritmov za šifriranje naletimo na problem verodostojnosti javnega ključa. Ali je javni ključ, s katerim želimo šifrirati sporočilo, dejansko last prave osebe? Rešitev tega problema je v certifikatnih agencijah (ang. Certificate Authority - CA), ki jamčijo za istovetnost javnih ključev, tako da nedvoumno ugotovijo identiteto lastnika javnega ključa (osebni dokument) in mu izdajo certifikat. S tem se odpravi problem lažne identitete in problem zanikanja identitete. Za lažje razumevanje lahko potegnemo vzporednico z notarji, ki so s strani države pooblaščeni, da na pomembnih dokumentih overijo podpise prisotnih oseb, tako da preverijo njihove osebne dokumente in s tem jamčijo, da so dotične osebe v prisotnosti notarja resnično podpisale nek dokument. Zato digitalno potrdilo predstavlja dokument, ki nedvoumno povezuje lastnika digitalnega potrdila z javnim ključem in je v bistvu njegova osebna izkaznica v elektronskem poslovanju (Savanović in Praprotnik, 2012).

Kvalificirano digitalno potrdilo in zasebni ključ lahko hranimo v obliki datoteke na disku računalnika, USB ključu ali na pametni kartici. Zaradi varnosti je potrebno nepooblaščenim osebam preprečiti možnost dostopa do te datoteke. Praviloma jo dodatno zavarujemo z geslom. Če pametno kartico izgubimo in jo nepošteni najditelj poskuša uporabiti, se kartica običajno zaklene po treh poskusih vpisa napačnega gesla.

Če imamo certifikat shranjen v datoteki na disku in zamenjamo računalnik, ga moramo prenesti s starega računalnika ali medija (npr. zunanji disk, USB ključ), na katerega smo ga predhodno shranili. Tega pa ne moremo storiti, če nismo na prvotni računalnik certifikata shranili tako, da ga bo možno kasneje izvoziti.

Izdajanje digitalnih potrdil

Izdajanje digitalnih potrdil lahko prevzamejo samo inštitucije, v katere mora vsak uporabnik njihovih storitev popolnoma zaupati. Situacija je podobna kot pri notarjih, ki na podlagi predložitve osebne listine podpisnika overjajo podpise na raznih dokumentih in s tem jamčijo njihovo pristnost. Obstaja lahko več overiteljev, ki so lahko med seboj popolnoma neodvisni, lahko pa se med seboj priznavajo. V primeru, da se overitelji med seboj priznavajo, so lahko razmerja med njimi enakopravna, zato se med seboj povezujejo horizontalno in z medsebojno overitvijo omogočajo svojim uporabnikom varnejšo in zanesljivejšo uporabo digitalnih potrdil. V primeru, da posamezni overitelji pooblastijo drugega overitelja, da v njihovem imenu izdaja digitalna potrdila, govorimo o vertikalnem povezovanju, katerega rezultat je lahko hierarhična struktura, ki tvori „verigo zaupanja“ (ang. chain of trust).

Kvalificirana digitalna potrdila v Sloveniji izdajajo štirje ponudniki kvalificiranih storitev zaupanja (https://e-uprava.gov.si/si/podrocja/osebni-dokumenti-potrdila-selitev/osebni-dokumenti/digitalno-potrdilo-za-elektronsko-poslovanje:

- Ministrstvo za javno upravo – SIGOV-CA za javno upravo in SIGEN-CA za druge uporabnike
- Pošta Slovenije d.o.o. - Pošta®CA
- Nova Ljubljanska banka d.d. - AC NLB

- Halcom d.d. - Halcom CA

Overitelj mora objaviti svoj javni ključ in dokumente o overiteljski politiki (ang. Certification policies), kjer so zapisani vsi postopki podeljevanja digitalnih potrdil in način varovanja zasebnega ključa (Savanović in Praprotnik, 2012).

Ker overitelj največkrat ne pozna naročnika, se mora pri izdaji digitalnega potrdila strogo držati postopkov, ki jih predvideva izbrana overiteljska politika. Overiteljska politika pozna več stopenj varnosti in vpliva na potek postopkov izdajanja prvih potrdil (Savanović in Praprotnik, 2012):

- avtentikacija naročnika: način avtentikacije naročnika je odvisen od stopnje varnosti, ki jo zahteva overiteljska politika. Pri najvišji stopnji varnosti poteka avtentikacija naročnika tako, da se mora naročnik osebno zglasiti pri prijavni službi overitelja in svojo identiteto potrditi z veljavnim osebnim dokumentom.
- Avtentikacija overitelja: v primeru, da naročnik overitelju popolnoma zaupa, naročnik preveri overiteljev podpis z javnim ključem overitelja.
- Dostava zasebnega ključa: dostava zasebnega ključa mora biti varna in zanesljiva.

Celoten koncept izdaje in uporabe digitalnih potrdil sloni na stopnji zaupanja uporabnikov do overitelja. Da lahko uporabnik oceni stopnjo zaupanja pri uporabi določenega digitalnega potrdila, mora podrobno poznati delovanje varnostnih mehanizmov overitelja in izpopolnjevanje potrebnih varnostnih zahtev, ki jih mora overitelj doseči. Seznam pravil in postopkov izdajanja, hranjenja ter upravljanja z digitalnimi potrdili imenujemo overiteljska politika (Savanović in Praprotnik, 2012).

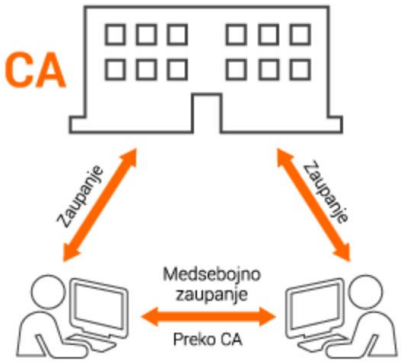
V nadaljevanju bomo spoznali overiteljsko politiko državnih overiteljev SIGEN-CA in SIGOV-CA, ki jo natančneje popisuje Državni center za storitve zaupanja na svoji spletni strani: https://www.si-trust.gov.si/sl/

Ostali slovenski certifikatni agenciji imata podobni overiteljski politiki.

Princip zaupanja med lastniki digitalnih potrdil preko tretje osebe

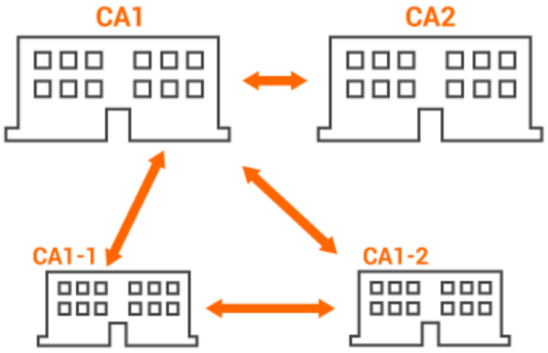
Overitelji (ang. Certification Authorithy – CA) predstavljajo v infrastrukturi javnih ključev osrednje institucije, v katere popolnoma zaupajo vsi uporabniki digitalnih potrdil in digitalnih podpisov. So pravne osebe, ki so pooblaščene za **izdajanje** digitalnih potrdil in opravljanje ostalih storitev v zvezi z overjanjem in digitalnimi podpisi.

Imetniki digitalnih potrdil overitelja pooblaščajo, da upravlja z njihovimi digitalnimi potrdili. Slika 32 prikazuje princip zaupanja med lastniki digitalnih potrdil preko tretje osebe.



Slika 32: Zaupanje v sistemu PKI
(SI-Trust, 2021)

Overitelj je ustanova, ki ji lahko zaupajo tudi ostali overitelji ali posamezniki in posredno s tem zaupajo tudi lastnikom vseh digitalnih potrdil, ki jih je overitelj izdal in potrdil. Tako se lahko različni overitelji povezujejo na različne načine, bodisi horizontalno, kjer se medsebojno overijo in s tem omogočijo varno in zanesljivo komunikacijo med lastniki digitalnih potrdil obeh ustanov (npr. podobno kot pri medsebojnem priznanju potnih listov med državama) ali vertikalno, ko nek overitelj pooblasti neko drugo ustanovo za izdajanje digitalnih potrdil v njegovem imenu, kar je seveda potrebno pri upravljanju z velikim številom digitalnih potrdil, poleg tega pa se z medsebojnim priznavanjem veča nabor e-storitev, ki so možne s posameznimi digitalnimi potrdili (SI-Trust, 2021.



Slika 33: Medsebojno zaupanje overiteljev
(SI-Trust, 2021)

Osnovne lastnosti digitalnih potrdil SIGOV-CA in SIGEN-CA

Digitalna potrdila so namenjena tako za interno e-poslovanje oz. komuniciranje v javni upravi (SIGOV-CA) kot za storitve, ki jih nudi javna uprava državljanom in pravnim osebam na elektronski način (SIGEN-CA). Zato obstajajo med posebnimi in spletnimi digitalnimi potrdili nekatere specifične razlike, pogojene z namenom uporabe. Le-to omogoča posebna tehnologija in specifične lastnosti programske opreme ter infrastrukture.

Spletnim digitalnim potrdilom pripada en par ključev (javni in zasebni).

Posebnim digitalnim potrdilom pripadata dva ločena para ključev:

- za digitalno podpisovanje oz. overjanje ter
- za šifriranje oz. dešifriranje.

Vsak par sestavljata zasebni in javni ključ. Pri tem javnost ključa pomeni, da je le-ta javno dostopen oz. objavljen v t.i. javnem imeniku, zasebnost pa, da ima dostop do tega ključa samo imetnik digitalnega potrdila (SI-Trust, 2021).

Slika 34: Funkcije ključev
(SI-Trust, 2021)

Par ključev za šifriranje/dešifriranje sestavljata:

- zasebni ključ za dešifriranje ter
- javni ključ za šifriranje.

Par ključev za podpisovanje/overjanje sestavljata:

- zasebni ključ za podpisovanje ter
- javni ključ za overjanje podpisa.

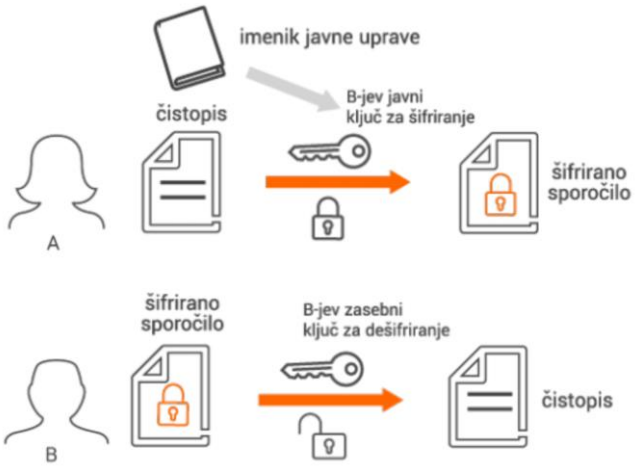
Spletna digitalna potrdila podpira večina brskalnikov in strežnikov in jih je zato enostavno vključiti v spletne aplikacije. Ta potrdila se uporabljajo za e-storitve državne uprave, za oddajo dohodnine, za dostop do geodetskih in katastrskih podatkov, za pošiljanje zašifrirane pošte in podobno. SIGEN-CA ta potrdila izdaja tako fizičnim osebam kot poslovnim subjektom. Za posebno digitalno potrdilo lahko zaprosijo le pravne osebe.

Lastniki digitalnih potrdil lahko vedno zahtevajo preklic ali obnovo svojih potrdil.

Šifriranje z uporabo digitalnega potrdila

Z uporabo digitalnega potrdila poteka postopek šifriranja in dešifriranja na naslednji način, kar prikazuje tudi slika (Slika 35).

Oseba A želi poslati šifrirano sporočilo osebi B. Uporabi javni ključ osebe B za šifriranje, ki se nahaja v **imeniku javne uprave** (javni imenik). Oseba A nato pošlje šifrirano sporočilo osebi B. Ko le-ta prejme šifrirano sporočilo, ga s svojim zasebnim ključem dešifrira. Pod pogojem, da je oseba A izbrala osebo B kot edinega naslovnika njegovega sporočila, ga lahko edino le-ta dešifrira (SI-Trust, 2021).



Slika 35: Postopek šifriranja in dešifriranja (SI-Trust, 2021)

Postopek digitalnega podpisovanja

Oseba A digitalno podpiše svoje sporočilo. Digitalni podpis je narejen tako, da se najprej po posebnem postopku naredi t.i. zgoščena vsebina oz. zgoščena vrednost. To vrednost potem zašifrirano z zasebnim ključem podpisnika (oseba A). Ker svoj zasebni ključ pozna izključno oseba A, je to jamstvo, da je podpis res njegov. Digitalno podpisano sporočilo, ki ga prejme oseba B, sestavljajo čistopis, šifrirana zgoščena vsebina in javni ključ osebe A za overjanje podpisa (SI-Trust, 2021).

Slika 36: Postopek digitalnega podpisovanja (SI-Trust, 2021)

Preverjanje digitalnega podpisa

Oseba B želi preveriti digitalni podpis osebe A. Oseba B najprej z javnim ključem osebe A dešifrira zgoščeno vsebino. Ponovno izračuna povzetek sporočila iz čistopisa z istim zgostitvenim algoritmom, kot ga je uporabila oseba A. Če se zgoščeni vsebini ujemata, pomeni, da je poslano sporočilo res podpisala oseba A.

Slika 37: Preverjanje digitalnega podpisa (SI-Trust, 2021)

Podpisano elektronsko sporočilo lahko bere vsak, vendar pa ne more spreminjati njegove vsebine, ne da bi se spremembe zabeležile. Glede na dejstvo, da pozna svoj zasebni ključ samo in izključno podpisnik (imetnik digitalnega potrdila), pa je zagotovljeno, da je on dejansko tudi podpisal sporočilo.

Dva para ključev pri posebnih digitalnih potrdilih omogočata dostop oz. dešifriranje šifriranih podatkov tudi v primerih, ko digitalno potrdilo, s katerim so podatki zašifrirani, ni več veljavno oz. ni mogoča normalna uporaba tega digitalnega potrdila zaradi različnih vzrokov. To omogoča dostop (berljivost) e-podatkov tudi v nepredvidenih in nezaželenih primerih, kot npr. izguba gesla za dostop do zasebnega ključa za dešifriranje podatkov, poškodovanje pametne kartice, na kateri je shranjen zasebni dešifrirni ključ ... . Pri tem se zasebni ključ za dešifriranje podatkov po posebnem režimu varno hrani znotraj infrastrukture overitelja na MJU in se izdaja izključno na zahtevo imetnika digitalnega potrdila, predstojnika (v primeru službenih digitalnih potrdil ali digitalnih potrdil za pravne osebe) ali na zahtevo pristojnega sodišča, sam postopek izdaje zasebnega ključa za dešifriranje podatkov pa je natančno določen s Politikami delovanja SIGOV-CA in SIGEN-CA. Na osnovi omenjenih značilnosti so posebna digitalna potrdila v prvi vrsti namenjena službeni uporabi (za javno upravo in za pravne osebe), spletna digitalna potrdila pa za državljane.

Druga bistvena razlika med posebnimi in spletnimi digitalnimi potrdili je v veljavnosti in obnavljanju njihovih ključev. Medtem ko je veljavnost ključev pri posebnih digitalnih potrdilih za podpisovanje, šifriranje in dešifriranje največ tri leta ter za overjanje pet let, je veljavnost spletnih digitalnih potrdil pet let. Pri tem se ključi posebnih digitalnih potrdil avtomatično obnavljajo pred pretekom veljavnosti, pri spletnih pa obnavljanje ne poteka avtomatsko, ampak je potrebno vsakič ponoviti postopek pridobitve digitalnega potrdila (SI-Trust, 2021).

Seznam preklicanih digitalnih potrdil

V primeru, da nek zasebni ključ postane kompromitiran (zloraba, okvara, itd.) ali pa naročnik enostavno pozabi geslo za uporabo ključa, je potrebno generirati nov par ključev in na osnovi novega para ključev pridobiti novo digitalno potrdilo, hkrati pa preklicati staro potrdilo. Vsa

preklicana potrdila mora overitelj objaviti na posebnem seznamu CRL (ang. Certificate Revocation List), ki ga tudi digitalno podpišejo. Overitelji objavljajo CRL sezname na svojih spletnih strežnikih, tako da lahko aplikacije, ki uporabljajo njihova digitalna potrdila, do njih neprekinjeno dostopajo (Savanović in Praprotnik, 2012).

5.3.4 Časovno žigosanje dokumentov

Digitalni podpis dokumenta zagotavlja samo avtentičnost dokumenta in dokazuje, kdo ga je podpisal, ne opredeljuje pa časovne dimenzije podpisa. Pravno gledano je takšno podpisovanje nezadovoljivo, saj se iz digitalnega podpisa ne da določiti datuma in časa podpisa. Zato potrebujemo mehanizem, s katerim bi bil digitalni podpis nedvoumno povezan s časom podpisa. Takšen mehanizem predstavlja TSA (ang. Time Stamp Authority), ki ima nalogo izdajanja časovnih žigov za elektronske dokumente. Časovni žig nekega dokumenta dokazuje, da je le-ta dokument obstajal pred časom, ki je naveden v časovnem žigu, z njim pa lahko tudi dokažemo, da se dokument od takrat ni spremenil (Savanović in Praprotnik, 2012).

Kvalificiran elektronski časovni žig je digitalni zapis, ki zagotavlja podpis dokumenta z veljavnim digitalnim potrdilom v določenem časovnem trenutku in sicer na način, da povezuje datum in čas podpisa ter podatke v elektronski obliki na kriptografsko varen način (SI-Trust, 2021).

V praksi je TSA izveden kot ustrezno varovan strežnik, ki je povezan in sinhroniziran s časovnim strežnikom. TSA strežnik mora ustrezati vsem pogojem, da zagotavlja potrebno verodostojnost in da mu vsi uporabniki popolnoma zaupajo (ang. Trusted Third Party - TTP) (Savanović in Praprotnik, 2012).

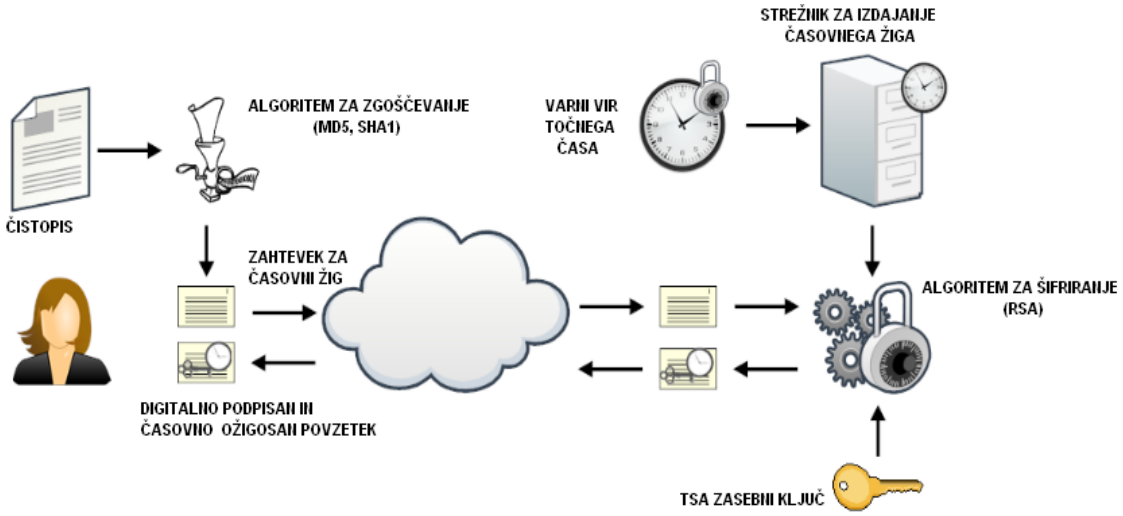
Izdajatelj kvalificiranih elektronskih časovnih žigov SI-TSA (ang. Slovenian Time Stamping Authority) je del infrastrukture javnih ključev (PKI, ang. Public Key Infrastructure) Državnega centra za storitve zaupanja. SI-TSA izdaja kvalificirane elektronske časovne žige, namenjene aplikacijam, s katerimi upravljajo institucije javne uprave, na voljo pa so tudi poslovnim subjektom in drugim končnim uporabnikom, ki s SI-TSA sklenejo dogovor oz. pogodbo (SI-Trust, 2021).

Kvalificirani elektronski časovni žigi se uporabljajo za:

- zagotavljanje, da je bil dokument podpisan z veljavnim digitalnim potrdilom v določenem časovnem trenutku in sicer na način, da povezujejo datum in čas podpisa ter podatke v elektronski obliki na kriptografsko varen način,
- za druge potrebe, kjer je potrebno dokazati časovne lastnosti transakcij in drugih storitev (SI-Trust, 2021).

Postopek časovnega žigosanja je prikazan na sliki (Slika 38). Ko želimo v neki aplikaciji časovno žigosati nek elektronski dokument oziroma podatke, pošljemo strežniku TSA z zgostitveno funkcijo narejen »povzetek« (ang. hash) dokumenta oziroma podatkov. Strežnik temu povzetku dopiše čas in vse skupaj podpiše s svojim zasebnim ključem – to je časovni žig. S tem je dokazano, da je elektronski dokument obstajal pred časom, navedenim v časovnem

žigu, poleg tega pa se da preveriti, da se od časa žigosanja elektronski dokument ni spremenil (ponovni povzetek elektronskega dokumenta se mora ujemati s tistim, ki je del časovnega žiga) (SI-Trust, 2021).



Slika 38: Postopek časovnega žigosanja dokumentov (Savanović in Praprotnik, 2012)

5.3.5 Digitalni podpisi programske kode

Eden od ukrepov, ki nas ščiti pred škodljivo ali zlonamerno kodo na računalnikih, je digitalno podpisovanje. Običajni programi bi morali biti digitalno podpisani, podpis pa overjen s strani priznanega overitelja.

Če operacijski sistem ne najde podpisa avtorja programske kode, overjenega s strani priznanega overitelja, zavrne namestitev programa in uporabnik mora nato izvesti postopek ročne odobritve izjeme. S tem pa hote ali nehote tudi sprejme odgovornost za namestitev neznane programske kode. Avtorji računalniških virusov so se hitro prilagodili in pričeli s pridobivanjem digitalnih potrdil (ang. Code-Signing Certificate), tudi pod krinko slovenskih podjetij (SI-CERT, 2021).

Prvi tak primer so na SI-CERT obravnavali aprila 2020. Analiza enega od vzorcev izsiljevalskega virusa Maze je razkrila, da je bil podpisan z digitalnim potrdilom na ime mikro podjetja iz Slovenije, ki se ukvarja s svetovanjem in je bilo ustanovljeno šele pred kratkim. Na podoben način si je utrl pot v sistem izsiljevalski virus Ryuk.

Lažni certifikat je mogoče pridobiti na enega od naslednjih načinov (SI-CERT, 2021):

- podjetje je utrpelo vdor v svoje sisteme in storilci so ukradli potrdilo,
- podjetje je nekdo uspel prepričati, da naj pridobi potrdilo in ga da v uporabo tretji osebi (piscem virusa),
- mimo vednosti podjetja je nekdo uporabil njihovo identiteto in z njo pridobil potrdilo.

Na Malware Bazaar (https://bazaar.abuse.ch/) spremljajo digitalna potrdila, s katerimi je podpisana zlonamerna koda. Na seznamu je vsaj 22 potrdil, ki so izdana na slovenska mikro podjetja. Seznam pa ima še eno zanimivost: kar 87 % vseh digitalnih potrdil na njem je izdal overitelj Sectigo iz ZDA (SI-CERT, 2021).

Na tem primeru se je pokazala slabost modela overiteljstva na daljavo.

6 VARNOSTNE TEHNOLOGIJE

Izraz varnostne tehnologije se nanaša na standarde, orodja in opremo, ki se uporabljajo za zaščito digitalnih sredstev organizacije.

Pojem vključuje tudi opremo za shranjevanje in premikanje podatkov, česar pa v tem gradivu ne bomo obravnavali.

V nadaljevanju bomo spoznali varnostne protokole, čebulno usmerjanje, požarne zidove, protivirusne programe, sisteme za odkrivanje in preprečevanje vdorov ter navidezna zasebna omrežja, ki so s povečanim obsegom dela na daljavo dobila še dodatno veljavo in pomembnost.

6.1 VARNOSTNI PROTOKOLI

Protokol je skupina pravil, dogovorov ali postopkov, ki se uporabljajo v različnih okoliščinah. V našem primeru se izraz nanaša na komunikacijske protokole v računalniških omrežjih, ki pomagajo pri:

- zaščiti podatkov in
- varnem prenašanju podatkov po omrežju.

6.1.1 Varnostni protokoli za brezžična omrežja

Brezžična omrežja so zasnovana na tehnologiji WiFi (ang. Wireless fidelity - WiFi), ki omogoča brezžično povezovanje po standardu IEEE 802.11.

WiFi je brezžična tehnologija, ki omogoča, da se lahko naprava poveže v računalniško omrežje z 2.4 GHz in 5 GHz radijsko frekvenco. Omrežje WiFi lahko uporablja več različnih naprav kot so pametni telefoni, tablice, kamere in ostale digitalne naprave. Pomanjkljivost WiFi povezave v primerjavi z žično (Ethernet) povezavo je varnost in stabilnost. Skozi leta se je varnost WiFi omrežij občutno izboljšala zaradi boljših zaščitnih protokolov(Wikipedia, 2021).

Tehnologije za varnost brezžičnih omrežij delujejo v povezovalni plasti (ang. data link) OSI oz. TCP/IP modela in zagotavljajo:

- overjanje mobilne naprave,
- kontrolo dostopa do brezžičnega omrežja,
- celovitost podatkov in
- zaupnost podatkov.

Protokoli, ki jih bomo spoznali v nadaljevanju, so implementirani na brezžičnih usmerjevalnikih (ang. router).

WEP

WEP je prvi standard za varnost brezžičnih omrežij, ki pa danes velja za izjemno nezanesljivega in neprimernega. S preprostimi orodji ga je mogoče razbiti v nekaj sekundah.

WPA

Protokol WPA (ang. WiFi Protected Access - WPA) je v primerjavi z WEP mnogo boljši, a žal prav tako neprimeren, saj ga je mogoče s preprostimi orodji razbiti v manj kot minuti.

WPA2

WPA2 (ang. WiFi Protected Access 2) zagotavlja funkcionalnosti po standard IEEE 802.11i (Savanović in Praprotnik, 2012).

Glavna razlika v primerjavi z WPA je, da za šifriranje uporablja boljši algoritem in sicer AES (Savanović in Praprotnik, 2012).

WPA2 je veljal za zanesljivega, vendar so tudi v njem našli ranljivost. Posledica izrabe ranljivosti so odvisne od več dejavnikov, v najhujši obliki pa napadalcu, ki se nahaja v neposredni bližini Wi-Fi omrežja, omogočajo izvedbo napada s posrednikom (t.i. MITM – Man-In-The-Middle), pri čemer lahko napadalec beleži in spreminja omrežni promet. Več o tej ranljivosti je zapisano na: https://www.krackattacks.com/. Do sedaj še nismo bili seznanjeni s primerom, da bi se katera od ranljivosti uporabljala v napadih (SI-CERT, 2021).

WPA3

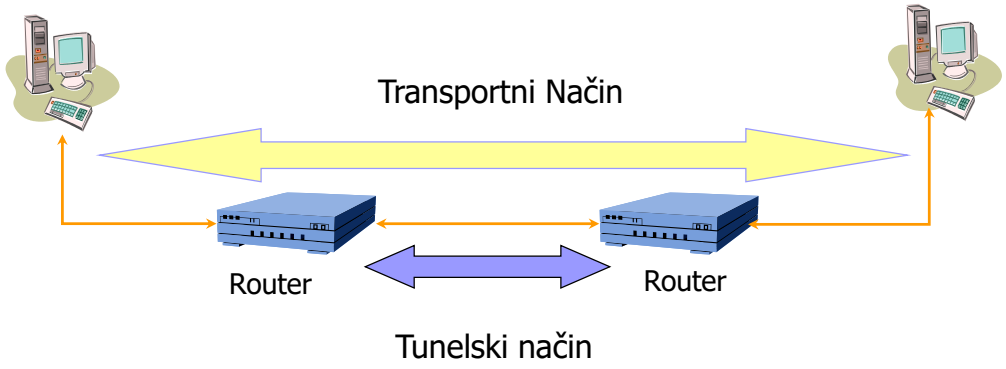
WPA3 je izboljšan varnostni standard za brezžična omrežja. Izšel je leta 2018. Ščiti pred šibkimi gesli, ki jih je mogoče razmeroma enostavno razbiti z ugibanjem (napad z grobo silo). Glede na predhodnika ima nove varnostne funkcije, omogoča bolj robustno preverjanje pristnosti in zagotavlja veliko kriptografsko moč (WiFi alliance, 2021).

6.1.2 IPsec

IPsec (ang. Internet Protocol Security - IPSec) je standardni varnostni protokol na internetu.

Internetni protokol IP je glavni usmerjevalni protokol na internetu. Z uporabo IP naslovov določa, kam bodo podatki šli. IPsec je varen, ker temu procesu doda šifriranje in preverjanje pristnosti.

IPsec deluje v **omrežnem** sloju in zagotavlja overjanje, zaupnost in celovitost komunikacije, poleg tega pa omogoča tudi vzpostavljanje varnih tunelov s pomočjo šifriranja IP paketov. IPsec je obvezni del standardnega protokola IPv6 (Savanović in Praprotnik, 2012).



Slika 39: Transportni in tunelski način IPsec

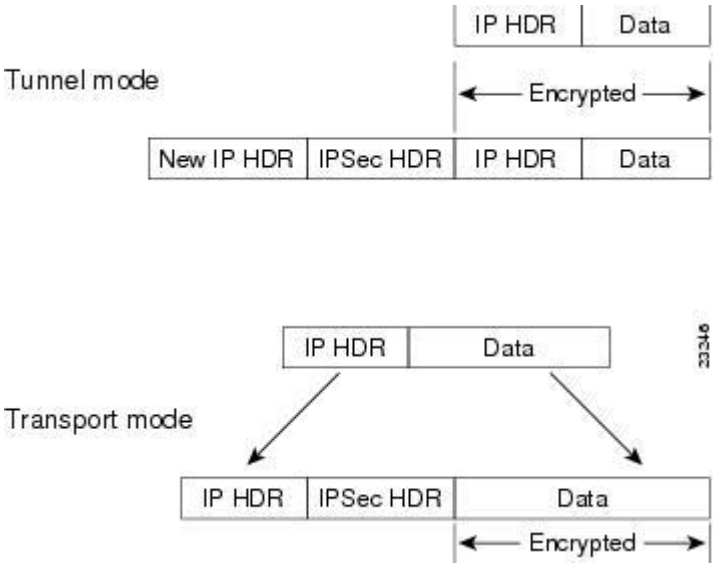
Kot prikazuje Slika 39, IPsec pozna dva načina delovanja, in sicer:

- transportni način, ki se uporablja za zagotavljanje varne komunikacije med koncema (ang. end-to-end),
- tunelski način, ki se uporablja za povezave VPN (ang. Virtual Private Network) in ščiti ves promet med dvema napravama, ki sta povezani s takim tunelom..

V transportnem načinu se glava IP (ang. IP header), ki vsebuje cilj podatkov, ne šifrira. Šifrirajo se samo podatki.

IPsec se v tunelskem načinu uporablja med dvema namenskima usmerjevalnikoma, pri čemer vsak usmerjevalnik deluje kot en konec navideznega "tunela". V tunelskem načinu se poleg paketa podatkov šifrira tudi IP glava, ki vsebuje končni cilj paketa. Da posredniškim usmerjevalnikom pove, kam naj posredujejo pakete, IPsec doda novo glavo IP. Na vsakem koncu predora usmerjevalniki dešifrirajo glave IP, da dostavijo pakete do svojih destinacij. Postopek imenujemo tudi tuneliranje (ang. tunneling).

Slika 40 prikazuje strukturo IP paketa v obeh načinih delovanja.



Slika 40: Struktura paketa IPsec v različnih načinih
(http://www.cisco.com/en/US/docs/security/asa/asa72/configuration/guide/l2tp_ips.html)

Navidezno zasebno omrežje (VPN) je šifrirana povezava med dvema ali več računalniki. Povezave VPN potekajo prek javnih omrežij, vendar so podatki, izmenjani prek VPN-ja, še vedno zasebni, ker so šifrirani. Ko npr. zaposleni delajo na daljavo, namesto v pisarni, pogosto uporabljajo VPN za dostop do poslovnih datotek in aplikacij.

Mnogi VPN-ji uporabljajo paket protokolov IPsec za vzpostavitev in izvajanje šifriranih povezav, a ne vsi. Drugi protokol za VPN je SSL/TLS, ki deluje v drugačnem sloju v modelu OSI kot IPsec.

VPN povezave bomo spoznali nekoliko kasneje.

IPSec deluje na omrežnem nivoju modela OSI, kar pomeni, da imajo uporabniki popoln dostop do svojega poslovnega omrežja ne glede na aplikacijo. Dobra nastavitev VPN bi morala oddaljenim uporabnikom omogočiti, da dosežejo enako raven produktivnosti, kot če bi sedeli za svojimi mizami, povezanimi z LAN[21] -om.

IPSec sestavlja družina protokolov (Savanović in Praprotnik, 2012):

- AH – Authentication Header
- ESP – Encapsulating Security Payload
- IKE – Internet Key Exchange

Protokol AH (ang. Authentication Header) s pomočjo kriptografskih algoritmov zagotavlja varnostne storitve overjanje in celovitosti, vključno s preprečevanjem ponavljanja paketov.

ESP zagotavlja enake storitve kot AH, poleg tega pa še zaupnost s pomočjo simetričnega šifriranja uporabniških podatkov v IP paketu.

IKE (ang. Internet Key Exchange) je ločen protokol, ki se lahko uporablja tudi izven IPsec, njegove funkcije pa so (Savanović in Praprotnik, 2012):

- izmenjava in dogovor o varnostnih politikah: varnostna politika je nabor algoritmov in parametrov za varnostne seje
- vzpostavitev varnostne seje - t.i. varnostne asociacije (ang. Security Association – SA), kar pomeni inicializacijo parametrov za določeno sejo,
- izmenjava ključev.

6.1.3 SSL/TLS

Secure Sockets Layer (kratica SSL) in njegov naslednik Transport Layer Security (TLS) sta kriptografska protokola, ki omogočata varno komunikacijo na internetu, na primer pri brskanju po spletu. Med protokoloma obstajajo majhne razlike, vendar sta v principu enaka (Wikipedia, 2021).

[21] Local area network – lokalno omrežje

Protokol SSL/TLS je zelo razširjen povsod, kjer se pojavlja potreba po prenosu podatkov zaupne narave, npr. pri prenosu osebnih podatkov. SSL/TLS ščiti podatke med pošiljanjem, ne pa tudi po tem, ko prispejo na ciljni računalnik.

Protokol SSL/TLS deluje v transportni plasti in zagotavlja enotne varnostne storitve za vse aplikacije, ki uporabljajo transportni protokol TCP (Savanović in Praprotnik, 2012).

V praksi SSL/TLS največ uporabljajo spletni strežniki in odjemalci v elektronskem poslovanju prek svetovnega spleta oz. interneta. Spletne strani, ki so zaščitene s protokolom SSL/TLS, spoznamo po začetni URL oznaki https:// namesto standardne http://. Ta URL oznaka mora biti nujno prisotna, kadarkoli izvajamo spletno plačevanje blaga in storitev.

SSL/TLS zagotavlja naslednje varnostne storitve:

- overjanje strežnika, opcijsko tudi odjemalca,
- zaupnost,
- celovitost sporočil.

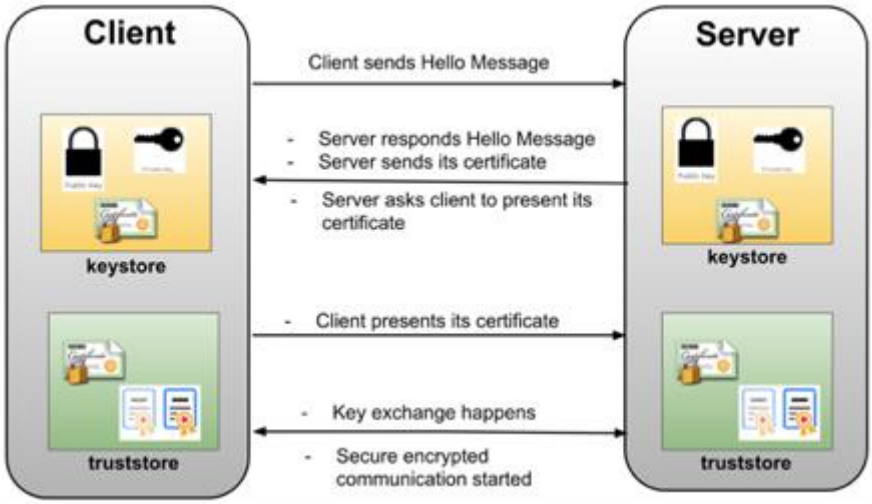
Postopek komunikacije poteka na naslednji način:

- Uporabnikov brskalnik pošlje zahtevo za dostop do spletne strani z varovanim prenosom SSL/TLS.
- Strežnik se predstavi z javnim ključem in digitalnim potrdilom.
- Ko se strežnik predstavi, brskalnik preveri, če je strežnik zaupanja vreden: preveri, da je digitalno potrdilo veljavno (ni pretečeno, ni preklicano in da ga je izdala zaupanja vredna certifikatna agencija).
- Uporabnikov brskalnik z uporabo strežnikovega javnega ključa ustvari simetrični ključ za enkripcijo in ga pošlje strežniku.
- Strežnik prejme ključ in ga dekodira s svojim privatnim ključem. Od tu naprej poteka povezava s pomočjo simetričnega algoritma za šifriranje podatkov, ki je bistveno hitrejša za kodiranje in dekodiranje podatkov ter omogoča hitro preverjanje in odkrivanje, če so bili podatki med prenosom spremenjeni.

Strežnik včasih zahteva tudi uporabnikovo predstavitev. Ta se (podobno kot strežnik) predstavi z digitalnim potrdilom / certifikatom (Wikipedia, 2021).

Na sliki (Slika 41) vidimo, kako poteka komunikacija, če strežnik zahteva uporabnikov certifikat oz. da se predstavi tudi uporabnik.

V povezavi s SSL/TLS srečamo tudi izraza SSL seja in SSL povezava. SSL seja (ang. SSL Session) je varnostna asociacija med odjemalcem in strežnikom, ki določa nabor varnostnih parametrov med določenima odjemalcem in strežnikom. SSL sejo vzpostavi protokol SSL Handshake, posamezno sejo pa lahko kasneje uporablja več SSL povezav. SSL povezava (ang. SSL Connection) je začasna, varna povezava med dvema aplikacija, ki se navezuje na eno SSL sejo, tj. na nabor določenih varnostnih parametrov (Savanović in Praprotnik, 2012).



Slika 41: SSL komunikacija, kjer se predstavita strežnik in uporabnik
(Vir: https://medium.com/@niral22/2-way-ssl-with-spring-boot-microservices-2c97c974e83)

6.2 PROTIVIRUSNI PROGRAMI

Protivirusni programska oprema je skupek programov, ki so namenjeni za preprečevanje, iskanje, odkrivanje in odstranjevanje škodljive kode (ang. malware). Ta orodja so bistvenega pomena za uporabnike, saj se lahko računalnik brez protivirusnega programa okuži takoj, ko se poveže na internet.

Na trgu obstajajo plačljivi in brezplačni protivirusni programi za osebne računalnike in za mobilne naprave (npr. Android in iOS).

V današnjem času imajo uporabniki pestro izbiro protivirusnih programov, pogosto pa se nagibajo k njihovi brezplačni uporabi. Med izbiranjem brezplačnih programov lahko pride do težav, npr. da uporabnik izbere navidezni program, ki se izdaja za protivirusni program, v resnici pa gre za zlonamerni program, ki prinaša viruse (Wikipedia, 2021).

Zaradi velikega števila in hitrosti širjenja škodljive programske opreme potrebuje vsak računalnik protivirusni program, ki se redno posodablja in stalno deluje. Ko uporabljamo računalnik, preži antivirusni program na datoteke, ki jih dobivamo s prenosnih medijev, iz omrežja ali interneta, odkriva viruse in jih odstranjuje.


V operacijskem sistemu Windows je na voljo protivirusna zaščita Windows defender, ki je del aplikacije Varnost sistema Windows.

Novi virusi in drugi škodljivi programi nastajajo dnevno. Proizvajalci protivirusne opreme zato svoje programe dnevno nadgrajujejo, uporabniški računalniki po celem svetu pa se preko interneta dnevno posodabljajo. Če se naš protivirusni program ne posodablja (npr. ker je enoletna licenca potekla), nismo odporni proti novonastalim škodljivim programom. Obstaja pa tudi možnost, da je napadalski virus tako nov, da ga proizvajalci protivirusne programske opreme še niso odkrili in še niso razvili zaščite pred njim.

Največjemu tveganju se lahko izpostavi uporabnik sam, če si kljub vsem varnostnim možnostim ne odloči za nobeno ali pa ne skrbi za posodabljanje varnostne zaščite.

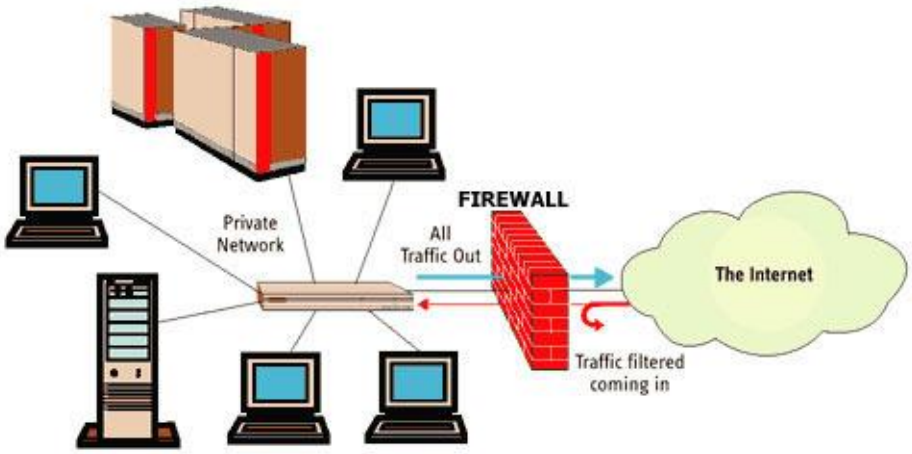
Zapomnimo si, da nas protivirusna programska oprema ne varuje pred okvarami ali pred goljufijami, ki skušajo obiti tehnično zaščito sistemov z izkoriščanjem pohlepnosti, naivnosti in neznanja uporabnikov (socialni inženiring) ali pred ranljivostmi, ki so posledica neustreznega posodabljanja aplikativne programske opreme, brskalnikov ali operacijskega sistema.

6.3 POŽARNI ZID

Požarni zid (ang. firewall) je strojna ali programska oprema, ki preprečuje neavtorizirane komunikacije preko omrežnih povezav. Svojo nalogo opravlja tako, da na podlagi danih pravil dovoljujejo ali preprečujejo omrežni promet.

Požarni zid je ena prvih obrambnih linij organizacije pred zunanjimi grožnjami. Hkrati je orodje, ki omogoča vpogled v naš omrežni promet in nam omogoča večji nadzor nad njim.

Namen požarnega zidu v stavbi je preprečevanje širjenja ognja v stavbi. V računalniškem smislu požarni zid najpogosteje varuje lokalno omrežje pred vdori z interneta tako, da v skladu z določenimi pravili, dovoli ali zavrne pretok podatkov preko njega. Slika 42 prikazuje omejevanje prometa, ki vstopa iz interneta. V marsikaterem okolju pa je prisotno tudi omejevanje izhodnega prometa.



Slika 42: Požarni zid med internetom in lokalnim omrežjem

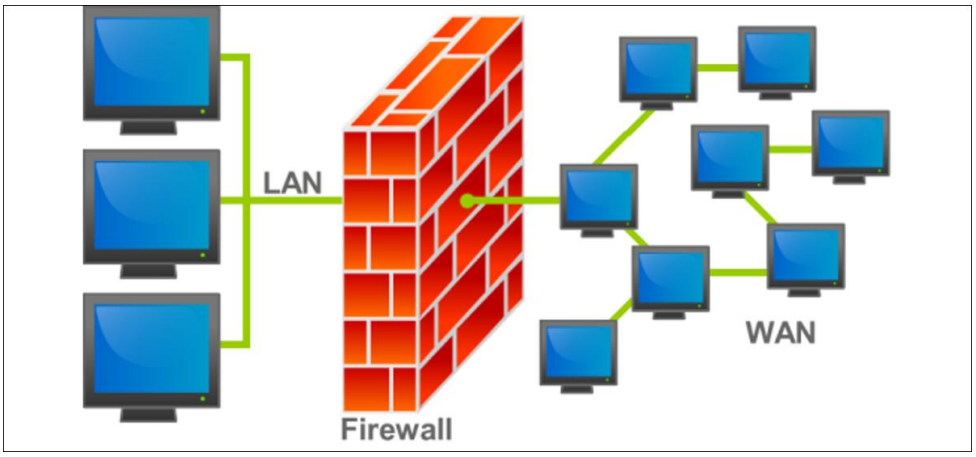
Ni pa internet edino omrežje, zaradi katerega potrebujemo požarni zid. Na splošno so požarni zidovi namenjeni ločevanju dveh odsekov omrežij, kjer enemu odseku zaupamo, drugemu pa ne.

Definicija požarnega zidu se lahko od enega do drugega vira nekoliko razlikuje. V najosnovnejšem smislu je požarni zid orodje, ki spremlja, filtrira in nadzoruje promet, ki vstopa ali izstopa iz našega omrežja. V tem primeru požarni zid filtrira vhodni in izhodni promet. Njegova naloga je omogočiti pretok zaupanja vrednega prometa in preprečiti slabemu dostop

do našega notranjega omrežja ali izstop iz njega. Z ustreznimi nastavitvami namreč lahko dosežemo, da podatki iz našega omrežja ne odtekajo.

S požarnim zidom je mogoče zaščititi vse od domačega računalnika do omrežij večjih državnih uprav in podjetij. Požarni zidovi so na voljo v programski ali strojni obliki. Lahko jih namestimo tudi v računalnike, različne dele omrežja ali v okolje v oblaku. Nekatera podjetja celo ponujajo požarni zid kot storitev (ang. Firewall as a service - FaaS).

Požarni zid deluje kot sistem za filtriranje podatkov, ki poskušajo vstopiti v naš računalnik ali omrežje. Skenira podatkovne pakete in išče take, ki so že identificirani kot uveljavljene grožnje. Če je ugotovljeno, da podatkovni paket predstavlja varnostno tveganje, mu požarni zid prepreči vstop v omrežje ali dostop do računalnika.



Slika 43: Požarni zid med prostranim omrežjem (WAN[22]) in lokalnim omrežjem (LAN)

Med funkcije požarnega zidu spadajo (Savanović in Praprotnik, 2012):

- preverjanje ali uveljavljanje varnostnih pravil,
- spremljanje in beleženje omrežnega prometa, ki poteka skozi,
- zmanjševanje izpostavljenosti notranjega omrežja pred vdori od zunaj,
- preslikava (zasebnih) omrežnih naslovov (ang. oznaka NAT), ki omogoča skupno rabo internetne povezave,
- demilitarizirana cona (ang. oznaka DMZ), ki omogoča ločen priklop bolj izpostavljenih naprav,
- kontekstno odvisni nadzor dostopa, ki na podlagi protokolov dinamično dovoli dostop do storitev,
- nudenje kriptiranih tunelskih povezav in s tem omogočanje navideznih zasebnih omrežij (VPN).

6.3.1 Strojni in programski požarni zidovi

Poznamo strojne in programske požarne zidove.

[22] WAN je omrežje, ki na večjem geografskem območju omogoča regijske in čezmejne povezave.

Požarni zidovi (v takšni ali drugačni obliki) so povsod. Verjetno ga trenutno uporabljate! Številni protivirusni programi imajo požarne zidove. Operacijski sistemi imajo običajno vgrajene požarne zidove kot del ukrepov za kibernetsko varnost.

Windows 10 ima vgrajen Windows Defender požarni zid. Filtrira internetni promet, ki prihaja in odhaja iz računalnika, da zmanjša varnostna tveganja. Preprečuje, da se morebitne nevarne aplikacije brez soglasja uporabnika povežejo z internetom, pa tudi nezaželene zunanje poskuse vzpostavitve povezave z omrežjem. S tem zlonamerna programska oprema ali hekerji težje pridejo do uporabnikovega računalnika. Windows Defender požarni zid je namenjen zaščiti uporabniških računalnikov oz. končnih vozlišč omrežja (ang. endpoint).

Spletne aplikacije imajo za večjo zaščito programske požarne zidove.

Požarni zidovi so:

- nameščeni na usmerjevalnikih (ang. router),
- na strežnikih, ali
- so popolnoma ločen računalniški sistem.

Izbor je odvisen od potreb in finančnih zmožnosti uporabnikov.

Požarni zid kot samostojna strojna oprema je ločena naprava, ki spremlja, filtrira in nadzoruje promet skozi omrežje, se pravi promet, ki vstopa ali izstopa iz omrežja. Ta vrsta strojne opreme je pogosto povezana z usmerjevalnikom, ki je na vhodu v oz. na izhodu iz omrežja.

Slika 44: Požarni zid kot samostojna naprava

Programski požarni zidu namestimo na obstoječe naprave na končnih točkah, se pravi na strežnike, usmerjevalnike itd., da regulirajo omrežni promet za to napravo.

Uporaba obeh vrst požarnih zidov je najboljša izbira!

Prednost programskih požarnih zidov je v enostavnejši uporabi in v ceni. Namenjeni so predvsem osebni oz. domači uporabi. Na voljo so tudi brezplačni programski požarni zidovi.

Strojni požarni zidovi so običajno precej dražji, njihova prednost je v hitrosti in nekaterih funkcijah. Namenjeni so predvsem podjetjem in drugim organizacijam s kompleksnejšo omrežno infrastrukturo.

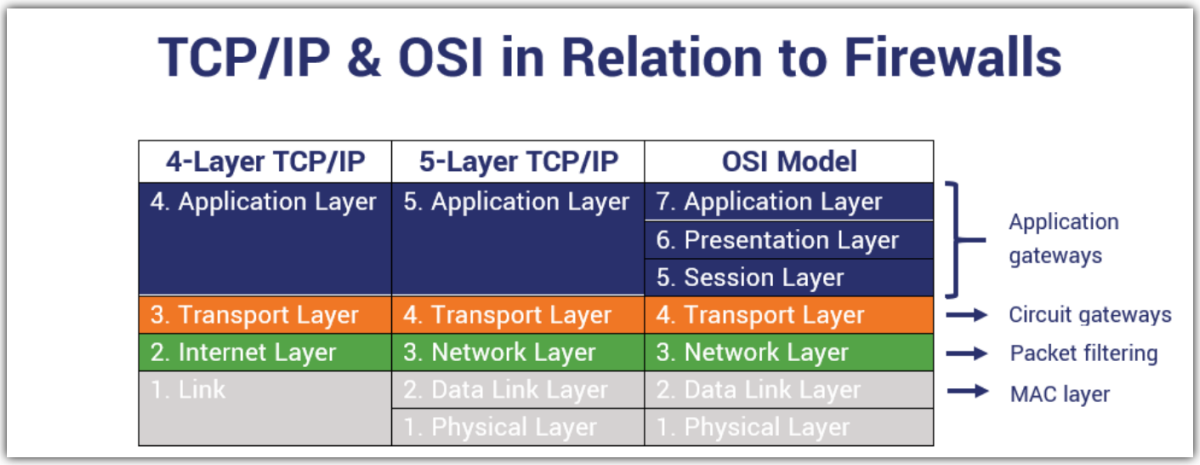
Požarni zid je nujna, nikakor pa ni zadostna rešitev za zaščito omrežja.

6.3.2 Vrste požarnih zidov glede na omrežni sloj

Razvrščamo jih lahko po različnih kriterijih. Delitev na strojne in programske smo že spoznali.

Požarne zidove lahko razvrščamo glede na to, na katerem sloju ali plasti (ang. layer) po OSI ali TCP/IP modelu delujejo.

Požarni zid zaščiti različne plasti protokola TCP/IP. Osnovni požarni zidovi običajno pregledujejo promet in delujejo na nižjih slojih. TCP/IP, naprednejši pa običajno delujejo v vseh slojih. Sodobne požarne zidove pogosto povezujemo s sedmimi sloji OSI modela in ne s štirimi sloji tradicionalnega modela TCP/IP oz. petimi sloji novega modela TCP/IP (Crane, 2020).



Slika 45: Različne vrste požarnih zidov glede na sloje modela OSI

Požarne zidove razvrščamo v različne kategorije glede na njihovo način delovanja. Glede na OSI model poznamo požarne zidove, ki delujejo (Whitman in Mattord, 2019; Crane, 2020) na:

- omrežnem sloju (ang. network layer) - filtrirajo podatkovne pakete,
- aplikacijskem sloju (ang. aplpication layer) - proxy ali aplikacijski prehod (ang. proxy or application gateway),
- sloju podatkovne povezave (ang. data link layer) – MAC[23] sloj,
- transportnem sloju (ang. transport layer) - circuit gateway,
- hibridni.

Požarne zidove kategorizirajo še na druge načine.

Delovanje požarnih zidov na omrežnem sloju

Najenostavnejši požarni zidovi omogočajo paketno filtriranje oz. filtriranje podatkovnih paketov. Filtriranje poteka na omrežnem sloju.

Paketno filtriranje je postopek nadzora prometa paketov na podlagi atributov kot so izvorni naslov, ciljni naslov, vrsta, dolžina in številka vrat (ang. port) (Network encyclopedia, 2021).

[23] Medium access control

Pri **paketnem filtriranju** požarni zid pregleduje podatkovne pakete, ki vstopajo ali izstopajo iz omrežja. Glede na pravila odloča, ali zavrne paket, ali ga posreduje dalje.

Poznamo statično in dinamično paketno filtriranje (Whitman in Mattord, 2019; Cisco, 2021).

Statično paketno filtriranje temelji le na informacijah vsebovanih v glavi IP paketa. Najpogosteje je to kombinacija izvornega in ciljnega IP naslova, protokola TCP ali UDP ter številke vrat. Ta vrsta filtriranja ne beleži aktivnih povezav in jih ne spremlja. Gleda le promet, ko pride v omrežje ali ga zapusti ter ga primerja z nizom **vgrajenih** varnostnih pravil, ki jih določi uporabnik oz. administrator omrežja. Takšno filtriranje je običajno implementirano v omrežnih usmerjevalnikih in prehodih (ang. gateway) (Whitman in Mattord, 2019).

Rule	Source IP Address	Source Port	Protocol	Destination IP	Destination Port	Action
#1	192.0.2.255	80	TCP	203.0.113.255	80	Allow
#2	255.255.255.255	443	TCP	254.254.254.254	Any above 1023	Allow

Slika 46: Primer seznama pravil za požarni zid za filtriranje paketov (Crane, 2020)

S statičnim paketnim filtriranjem bi npr. lahko dovolili le dostop znanim IP naslovom ali pa npr. preprečili dostop določenim IP naslovom, kar bi bilo zabeleženo v seznamu za kontrolo dostopa (ang. access control list – ACL). Onemogočili bi lahko dostop do določenih vrat, npr. do 80, kar bi povzročilo onemogočanje dostopa do strežnika HTTP.

Dinamično paketno filtriranje (ang. dynamic packet-filtering) ali **pregled stanja** (ang. stateful packet inspection – SPI) je tehnologija požarnih zidov, ki izvaja filtriranje paketov dinamično in lahko obravnava bolj zapletena pravila. Pravila se lahko dinamično spreminjajo glede na dogodke ali pogoje. Vrata (porti) se lahko odprejo le, kadar je to potrebno, in se nato zaprejo. Požarni zid, ki uporablja tovrstno filtriranje, odloča, ali sprejme posamezen podatkovni paket na osnovi IP glave in **tovora** (ang. payload), se pravi koristnih podatkov, ki jih prenaša paket (Network encyclopedia, 2021).

Požarni zid s stanjem (ang. stateful firewall), kakor se tudi imenuje, spremlja stanje aktivnih povezav in te informacije uporabi za odločanje, katere omrežne pakete spustiti skozi in katere ne. Beleži informacije o izvornem in ciljnem IP naslovu, vratih, aplikacijah in druge informacije o povezavi. Za razliko od statičnega filtriranja, ki pregleduje pakete le na podlagi informacij v IP glavi, pregled stanja spremlja vsako povezavo, ki prečka požarni zid in vzdržuje tabelo stanja (ang. state table). Požarni zid ne odloča le na podlagi pravil, ki jih je določil uporabnik, ampak tudi na podlagi konteksta, ki se je določil na podlagi uspešnega prehoda prejšnjih paketov.

Tabela stanja je del notranje strukture požarnega zidu. Vsakič, ko se vzpostavi povezava TCP ali UDP za vhodne ali odhodne povezave, požarni zid zabeleži podatke v tabelo stanj. Spremlja vse seje ter pregleda vse pakete, ki gredo skozi požarni zid. Če imajo paketi pričakovane

lastnosti, ki jih predvideva tabela stanj, jim požarni zid dovoli prehod. Tabela stanja se dinamično spreminja glede na pretok prometa (Cisco, 2021).

Delovanje požarnih zidov na nivoju aplikacij

V tem poglavju bomo spoznali, kako poteka nadzor in omejevanje prometa na nivoju aplikacij.

Posredniški požarni zid (ang. application layer proxy firewall) ali aplikacijski požarni zid (ang. application firewall) deluje na slojih 5, 6 in 7 OSI modela oz. na aplikacijskem sloju TCP/IP modela. Ponavadi je nameščen na posebnem računalniku in povezan z usmerjevalnikom, ki filtrira podatkovne pakete. Znan je tudi po imenu posredniški strežnik (ang. proxy server), saj običajno opravlja vlogo posrednika, ko zazna zahtevo neke storitve (ang. service request).

Kot že ime pove, proxy požarni zid služi kot posrednik, ki omogoča dvema sistemoma posredno komunikacijo prek odjemalca.

Posredniški požarni zid (proxy) izvaja zaščito omrežnih virov tako, da filtrira sporočila na ravni aplikacije. Dostope omejuje na ravni aplikacij, kar povečuje raven varnosti, vendar lahko vpliva na funkcionalnost in hitrost.

Tradicionalni požarni zidovi niso namenjeni pregledu prometa na nivoju aplikacij. Proxy strežnik odpravlja to vrzel. Določa, kateri promet je treba dovoliti ali zavrniti, ter analizira dohodni promet, da zazna znake potencialnega kibernetskega napada ali zlonamerne programske opreme.

Včasih požarni zidovi aplikacijskega sloja podpirajo le omejeno število aplikacij ali celo samo eno aplikacijo (Whitman in Mattord, 2019). Nekatere pogostejše aplikacije, ki jih lahko podpira požarni zid aplikacijske plasti, so npr. e-pošta (SMTP), spletne storitve (HTTP), DNS, Telnet, FTP ali SNMP (Cisco, 2021).

Prednosti požarnih zidov aplikacijske plasti (Cisco, 2021):

- Preverjajo pristnost posameznikov (namesto avtentifikacije naprave overi uporabnika, ki zahteva povezavo).
- Hekerji težje ponarejajo (ang. spoofing) in izvajajo napade DoS.
- Spremljajo in filtrirajo lahko podatke aplikacij: spremljati je mogoče vse podatke v povezavi, tako se zazna napade kot so napačni URL-ji, poskusi prelivanja oz. prekoračitve medpomnilnika (ang. buffer overflow attempts), nepooblaščen dostop in drugo.
- Na podlagi podatkov za preverjanje pristnosti in avtorizacije lahko nadziramo, katere ukaze ali funkcije dovolimo posamezniku.

Globoko preverjanje paketov (ang. deep packet inspection - DPI) je tehnika, ki omogoča omrežnim varnostnim napravam, kot so požarni zidovi, da "globlje" pogledajo v paket podatkov. Ne zanašajo se le na informacije glave IP (v bistvu plasti 2 in 3), temveč pogledajo podrobneje po OSI plasteh 4 do 7.

Globok pregled paketov se pogosto uporablja za analizo uporabe omrežja, odpravljanje težav z zmogljivostjo omrežja, zagotavljanje pravilne oblike podatkov, preverjanje zlonamerne kode, prisluškovanje in internetno cenzuro (Wikipedia, 2021). Za prisluškovanje in prestrezanje podatkovnih paketov imamo še poseben izraz vohljanje (ang. packet sniffing).

Če so podatki šifrirani, paketi niso primerni za pregled. Običajno naprave za zaščito omrežja nimajo dostopa do ključev za dešifriranje, ki so potrebni za dekodiranje šifriranih paketov in razumevanje sporočila oz. podatkov. To je primer, ko lahko ena varnostna politika izredno oteži uveljavljanje druge (Cisco, 2021).

Požarni zidovi sloja MAC

Požarni zid plasti MAC (ang. media access control layer firewall) deluje v plasti podatkovne povezave (ang. datalync layer) modela OSI.

Ta vrsta požarnega zidu filtrira pakete glede na njihov MAC naslov. Če je naslov v seznamu MAC ACL, dovoli dostop (Crane, 2020).

Požarni zid na nivoju voda

Požarni zid na nivoju voda (ang. circuit-level firewall) deluje tako, da preverja veljavnost povezave preko niza nastavljivih pravil. V primeru, da povezava izpolnjuje postavljene kriterije, se vzpostavi seja in prenos brez nadaljnjega preverjanja podatkov, saj se smatra, da je bila povezava vzpostavljena s preverjenim virom. Požarni zid lahko v tem primeru samo še kontrolira čas povezave. Slabost takšnih požarnih zidov je, da delujejo na transportnem sloju, zato zahteva preprogramiranje transportne funkcije, kar negativno vpliva na delovanje in zmogljivost omrežja. Druga slabost je zahtevnejša namestitev in njihovo vzdrževanje (Savanović in Praprotnik, 2012).

Požarni zid naslednje generacije

Takšni nazivi niso najboljši, saj se tehnologija izjemno hitro razvija in kar je danes visoka tehnologija (ang. high tech) bo kmalu stara šara. Ker pa se ime požarni zid naslednje generacije (ang. next-generation firewalls - NGFW) uporablja, si poglejmo, kaj pomeni.

Dejansko ne gre za kaj novega, saj se ime pojavlja že izjemno dolgo. Običajno zagotavlja nadzor stanja dohodnega in odhodnega omrežnega prometa in druge funkcije kot npr. nadzor aplikacij, integrirano preprečevanje vdorov in obveščanje o grožnjah v oblaku.

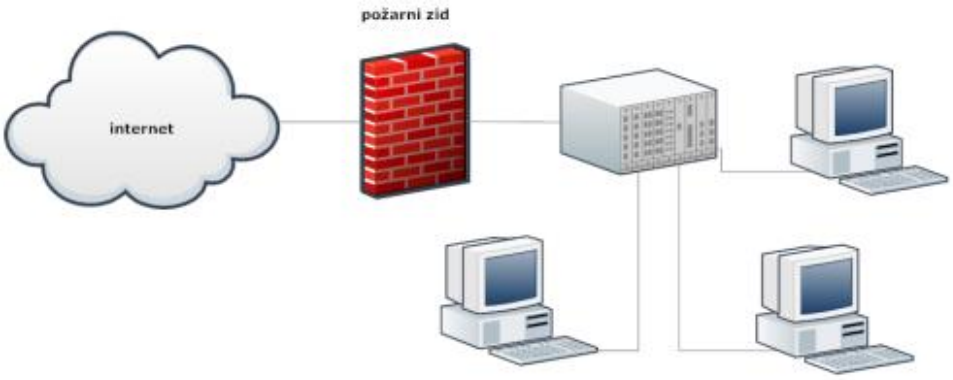
6.3.3 Konfiguracija požarnih zidov

V omrežje lahko postavimo en požarni zid ali več.

Zaščita omrežja z enim požarnim zidom

V primeru uporabe samo enega požarnega zidu, se celotno omrežje (strežniki in uporabniki) skrije za požarnim zidom. Strežniki so v tem primeru zaščiteni navzven, vendar niso zaščiteni

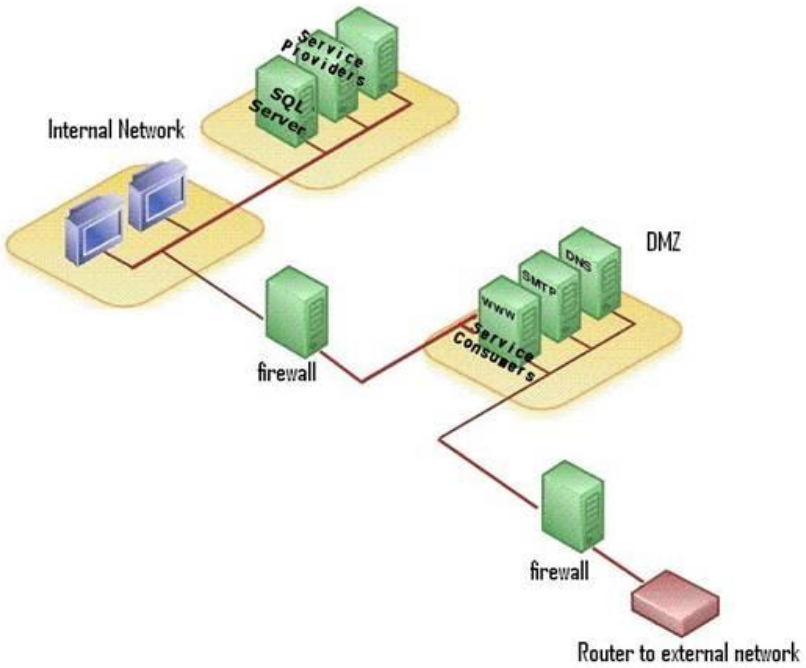
pred uporabniki istega omrežja. Ker lahko pridejo napadi tudi s strani uporabnikov (zavestno ali zaradi okuženih računalnikov uporabnikov), takšna rešitev ni najboljša. V takšnih konfiguracijah se največkrat uporabi požarni zid za paketno filtriranje, ki deluje na omrežnem sloju (Savanović in Praprotnik, 2012).



Slika 47: Zaščita omrežja z enim požarnim zidom (Savanović in Praprotnik, 2012).

Primer prikazuje Slika 47.

Zaščita omrežja z več požarnimi zidovi



Slika 48: Dva požarna zida tvorita DMZ
(http://www.cnux.ca/sqlserver_ws_providers_productpage.html)

Za boljšo varnost se uporablja večje število požarnih zidov. Pogosto se uporablja konfiguracija z dvema požarnima zidovoma, ki skupaj tvorita demilitirazirano cono (ang. Demilitarized

Zone - DMZ). S takšno konfiguracijo se lahko strežniki (spletni, poštni, FTP, VoIP) zaščitijo od zunanjih vdorov, kot od vdorov lastnih uporabnikov. S tem dosežemo večjo varnost, hkrati pa tudi kompleksnost omrežja. Za večjo varnost se za DMZ uporabljata požarna zidova različnih proizvajalcev, saj se s tem zmanjša možnost, da bi se ista ranljivost pojavila na obeh požarnih zidovih (Savanović in Praprotnik, 2012).

Primer prikazuje Slika 48.

6.4 ČEBULNO USMERJANJE

Čebulno usmerjanje (ang. the onion router – TOR) je v praksi razširjena izvedba sistema za zagotavljanje zasebnosti in anonimnosti. Koncept čebulnega usmerjanja (ang. onion routing) je način anonimne komunikacije v računalniškem omrežju, ki zaradi plasti šifriranega prenosa podatkov spominja na čebulo.

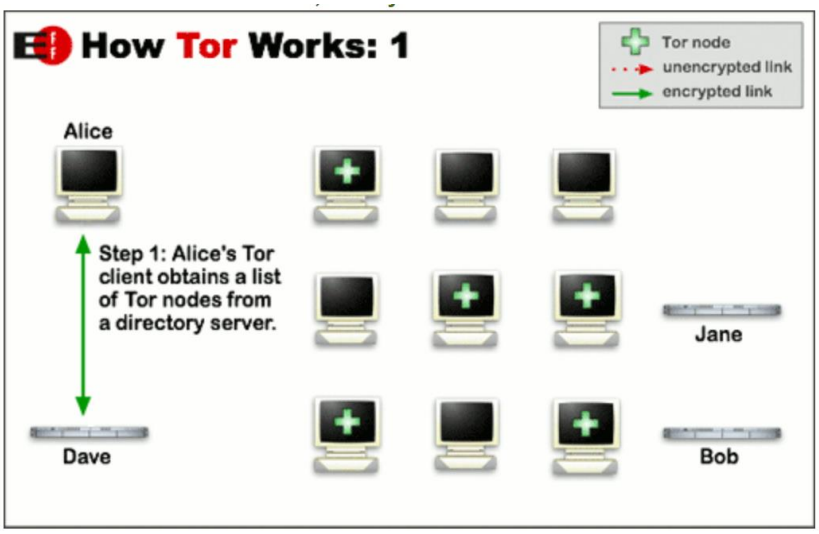
Ime Tor izhaja iz ang. izraza »the onion router«. Vendar je Tor več kot le usmerjevalnik.

Tor je brezplačni odprtokodni program in omrežje, ki omogoča anonimnost in zasebnost na spletu. Lahko se uporablja za poslovne in osebne namene, žal pa se mnogokrat koristi zlonamerno – v kriminalne namene, kar povzroča precej težav organom pregona (Europol, 2020).

V Tor se povežemo s posebno programsko opremo oz. brskalnikom, ki ves lokalni internetni promet preusmerja preko več anonimnih vozlišč v omrežju Tor, preden prispe na cilj. Omogoča, da niti ponudnik interneta, niti katero od vmesnih vozlišč, niti obiskana spletna stran ne morejo vedeti, kdo jih je obiskal. Člani omrežja med seboj komunicirajo prek šifriranih povezav in nastopajo v treh različnih vlogah: vhodni člen, vmesni člen in izstopni člen. Omrežje deluje na podlagi velikega in spreminjajočega se števila vmesnih členov. Vmesni členi so čebulni usmerjevalniki. Vhodni člen je vhodna točka v omrežje, vmesni člen deluje kot posrednik sporočil v omrežju in izhodni člen deluje kot izhod iz omrežja, ki se poveže na ciljni (normalni) strežnik. Stopnja anonimnosti je odvisna od števila vmesnih členov oziroma čebulnih usmerjevalnikov (Torproject, 2021).

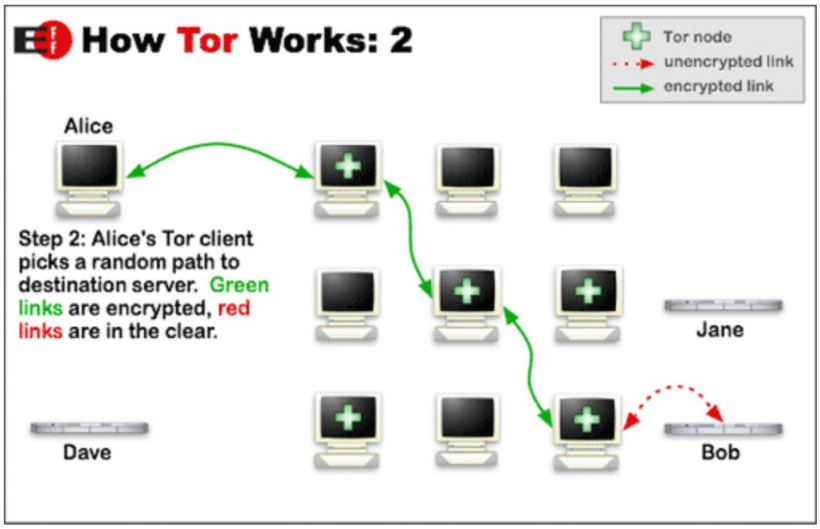
Ozko gledano je čebulni usmerjevalnik, ki je dal omrežju ime, vozlišče čebulnega omrežja, ki prenese šifrirane podatke do naslednjega vozlišča. Šifrirani podatki se torej prenašajo skozi plasti omrežnih vozlišč, imenovanih čebulni usmerjevalniki, od katerih vsako "odlepi" en sloj in odkrije naslednji cilj podatkov.

Oglejmo si postopek na slikah. Alice, ki želi biti na spletu anonimna, mora imeti nameščeno programsko opremo Tor. Kot prikazuje Slika 49 vhodni člen oz. oddajnik (Alice) najprej pridobi seznam čebulnih usmerjevalnikov. To stori na varen način, se pravi z overjanjem.



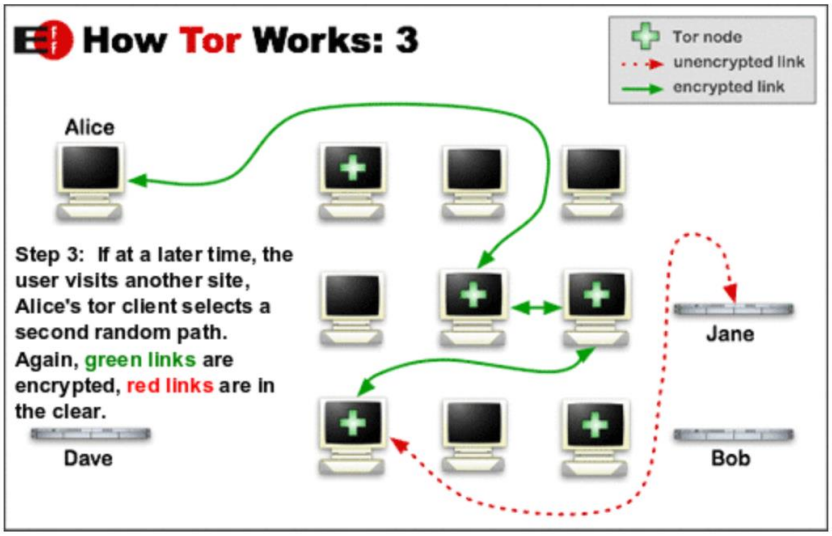
Slika 49: Delovanje omrežja TOR: 1. korak (Torproject, 2021)

Oddajnikov Tor odjemalec izbere naključno pot, tj. zaporedje Tor vozlišč, do sprejemnika oz. končnega cilja. Podatke zaščiti po principu čebulnega usmerjanja, tj. s šifriranjem po odsekih, kar prikazuje Slika 50.



Slika 50: Delovanje omrežja TOR: 2. korak (Torproject, 2021)

Podatki se tako prenašajo v šifrirani obliki med posameznimi Tor vozlišči na izbrani poti in v nešifrirani obliki med zadnjim Tor vozliščem in sprejemnikom (Slika 51).



Slika 51: Delovanje omrežja TOR: 3. korak (Torproject, 2021)

Tehnično gledano gre za decentraliziran sistem za usmerjanje podatkov v aplikacijskem sloju, ki pa deluje po principu odjemalec/strežnik in ne po principi P2P (ang. Peer-to-Peer) (Savanović in Praprotnik, 2012).

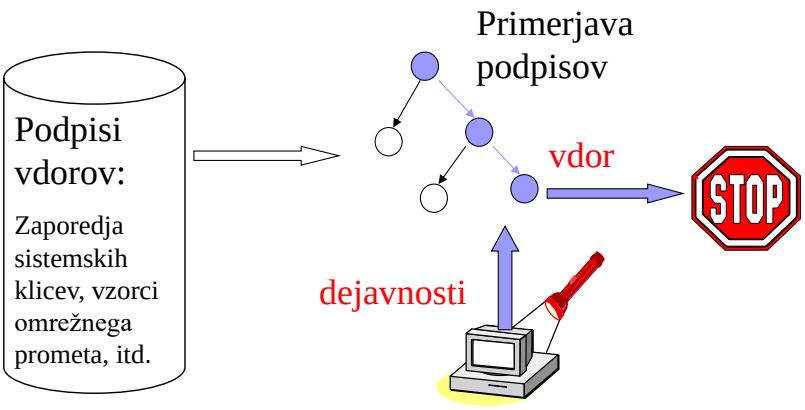
6.5 SISTEMI ZA ODKRIVANJE IN PREPREČEVANJE NAPADOV

Sistemi za odkrivanje in preprečevanje napadov (ang. intrusion detection and prevention system – IDPS) so namenske omrežne varnostne naprave, ki omogočajo podrobno opazovanje in analizo omrežnega prometa z namenom detekcije in zaščite pred napadi.

IDPS sistemi se od antivirusnih programov ločijo po tem, da zagotavljajo zaščito pred zlonamernim prometom na omrežnem nivoju in ne na nivoju računalnika, sicer pa delujejo zelo podobno kot antvirusni programi. Med drugim za detekcijo napadov uporabljajo detekcijo zlorab in detekcijo anomalij. Ti dve metodi pa sta analogni skeniranju podpisov in skeniranju delovanja pri antivirusni zaščiti (Savanović in Praprotnik, 2012).

Slika 52 prikazuje detekcijo zlorab (ang. Misuse detection oz. signature-based), za katero je značilno naslednje (Savanović in Praprotnik, 2012):

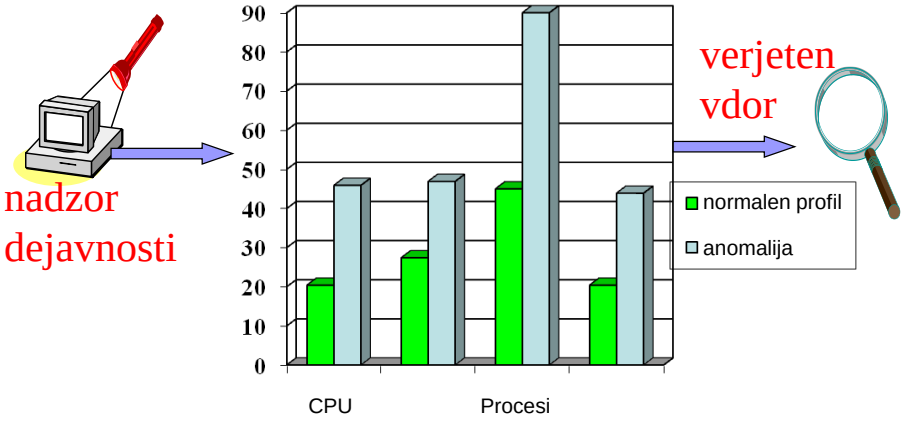
- primerja promet z bazo podpisov znanih napadov,
- javlja manj lažnih alarmov, saj zahteva natančno ujemanje napada s podpisom v bazi,
- ne zazna novih napadov, ki jih še ni v bazi znanih napadov.



Slika 52: IDPS detekcija zlorab
(Savanović in Praprotnik, 2012)

Slika 53 prikazuje detekcijo anomalij (ang. profile/anomaly detection oz. statistical-based), za katero je značilno (Savanović in Praprotnik, 2012):

- primerja promet z »normalnim« prometom (profil),
- relativno veliko je lažnih alarmov (ang. False positive), saj se »normalni« promet lahko povsem legalno spreminja in zato ta detekcija ni povsem zanesljiva,
- lahko zazna nove napade, saj ni odvisna od predhodnega odkritja in analize napada.

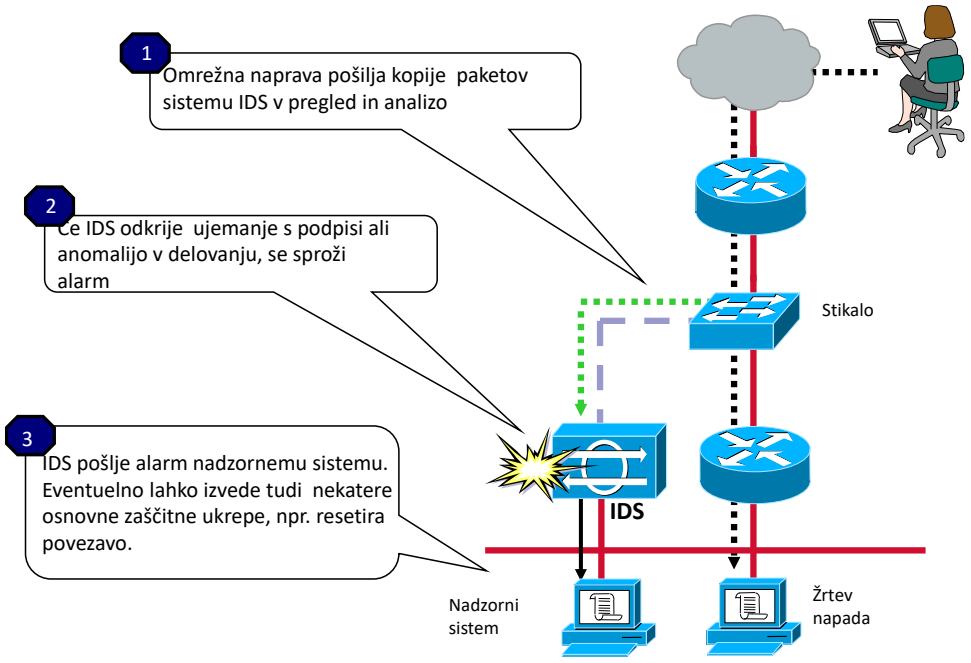


Slika 53: IDPS detekcija anomalij
(Savanović in Praprotnik, 2012)

IDPS sistem je lahko v obliki:

- programske opreme (ang. Host-based IDPS) - v tem primeru spremlja procese, ki se izvajajo na računalniku ali
- namenske omrežne naprave (ang. Network-based IDPS), ki nadzira promet v omrežju (Savanović in Praprotnik, 2012).

Slika 53 prikazuje detekcijo anomalij, ki jo izvede IDS.

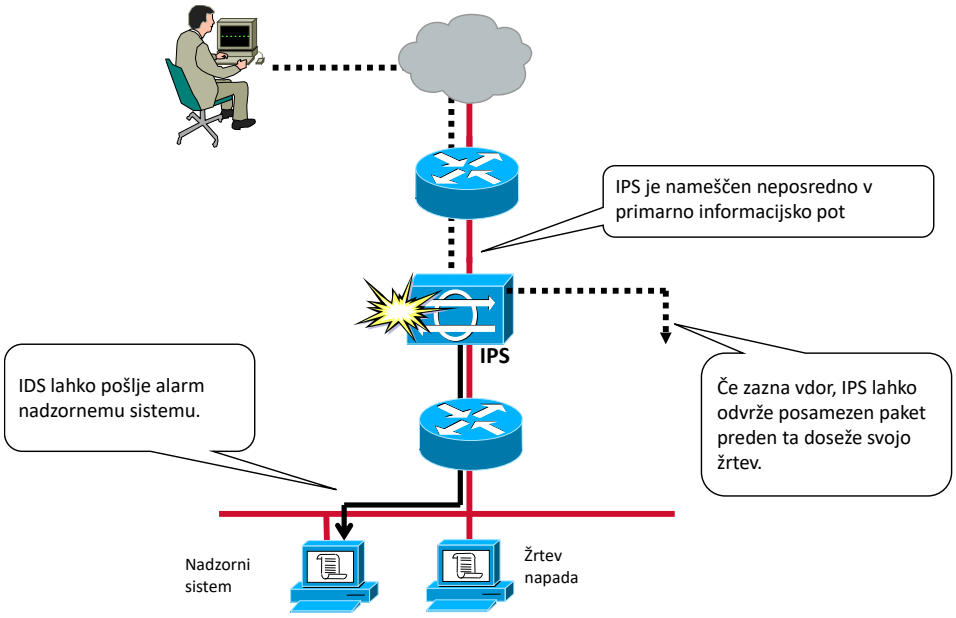


Slika 54: IDS – Intrusion Detection System (Savanović in Praprotnik, 2012)

Zgodovinsko poznamo:

- sisteme, ki se osredotočajo na zaznavanje in javljanje napadov (ang. Intrusion Detection Systems – IDS) in so nameščeni vzporedno s primarno komunikacijsko potjo, ter
- sistemi, ki zaznavajo in ščitijo pred napadi, ki so znani kot IPS.

Slika 55 prikazuje primerjavo med IDS in IPS (Savanović in Praprotnik, 2012).



Slika 55: IPS – Intrusion Prevention System

6.6 NAVIDEZNO ZASEBNO OMREŽJE

Navidezno zasebno omrežje (ang. Virtual Private Network - VPN) lahko definiramo kot storitve različnih tehnologij, ki omogočajo medsebojno povezovanje omrežnih naprav preko omrežij, ki niso zavarovana ali zaupanja vredna. Takšna omrežja so običajno javne telekomunikacijske infrastrukture kot npr. internet. VPN omrežja omogočajo varen dostop dislociranih uporabnikov ali poslovnih enot preko javne infrastrukture do želenih informacijskih virov (Savanović in Praprotnik, 2012).

Prednosti VPN omrežij (Savanović in Praprotnik, 2012):

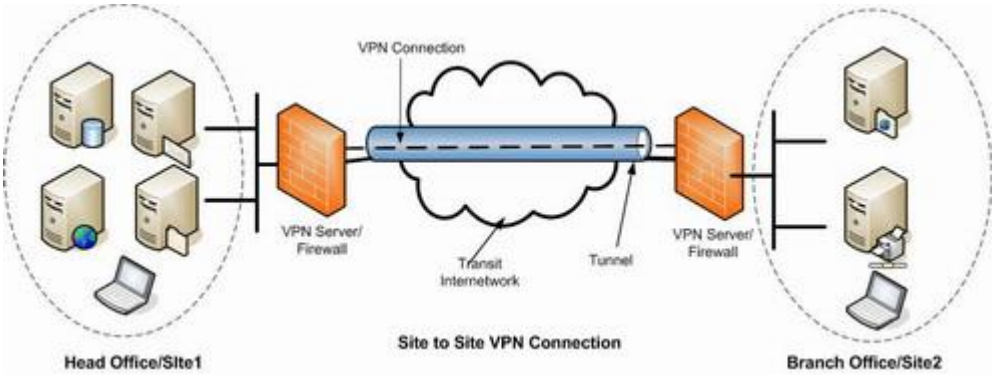
- **manjši stroški** – v primerjavi z najetimi vodi so lahko prihranki ogromni,
- **lažje upravljanje**, ker VPN omrežje temelji na javnem omrežju, ki ga upravlja in vzdržuje operater; vzdrževati je potrebno le VPN tehnologijo, kar je občutno enostavnejše in cenejše,
- poenostavi topologijo omrežja,
- **omogoča razširljivost** s pomočjo tunelov, če se število lokacij poveča (pri rešitvi z najetimi vodi vsaka nova lokacija potrebuje novo najeto linijo),
- **varnost –** ustrezne VPN rešitve zagotavljajo prenašanje kriptiranih podatkov. Kibernetski kriminalci se stalno trudijo prebiti varnostne ukrepe VPN, zlasti kadar se uporablja z nezavarovanimi javnimi omrežji Wi-Fi, vendar so na voljo zaupanja vredne storitev VPN, ki za preprečevanje kraje ali prestrezanja podatkov uporabljajo učinkovito šifriranje (npr. algoritem AES-256).

Slabosti VPN omrežij (Savanović in Praprotnik, 2012):

- **varnost** – ker se zasebni podatki prenašajo preko javnih povezav, je zelo pomembno, da se pri pripravi VPN omrežij skrbno načrtuje varnost delovanja celotnega sistema; glede na občutljivost podatkov je potrebno izbrati ustrezne tehnologije zaščite (npr. šifriranje),
- **kakovost povezav** - ker je kakovost odvisna od javne infrastrukture, kjer se kapaciteta povezav deli med uporabniki, je kakovost praviloma manjša od kakovosti najetih vodov, predvsem pa se spreminja kapaciteta VPN povezav, saj uporabniki ne morejo vplivati na priključitev ostalih uporabnikov in njihovo uporabo kapacitet, kar povzroča različno obremenjenost javne infrastrukture. Zato nekateri operaterji ponujajo zagotovljeno kapaciteto VPN povezave, ki pa so praviloma dražje.
- upočasni delovanje interneta,
- **težavno zagotavljanje konstantne kakovosti prenosa** (zlasti uporabnikom na brezžičnih povezavah),
- **zanesljivost** – zanesljivo delovanje VPN omrežij je popolnoma odvisno od zanesljivosti delovanja infrastrukture, ki jo potrebuje za svoje delovanje.

6.6.1 Tuneliranje

Pri tuneliranju VPN kreira navidezni tunel preko javnega omrežja in tako poveže dve točki med seboj. Tuneliranje je torej proces, ki na oddajni strani skrije oz. ovije (enkapsulira) izvirne IP pakete v nove pakete in jih pošlje preko javnega omrežja do sprejemnika, kjer se izvirni paketi izločijo. Proces tuneliranja se sestoji iz procesa **enkapsulacije**, **usmerjanja** in **dekapsulacije**. V primeru, da se tuneliranje kombinira z zaupnostjo podatkov, se izvirni IP paketi pred enkapsulacijo šifrirajo in po dekapsulaciji dešifrirajo. S tem se prepreči možnost prisluškovanja vsebini VPN prometa v javnem omrežju (Savanović in Praprotnik, 2012).



Slika 56: VPN povezava med dvema omrežjema
(vir http://nirlog.com/2006/01/23/secure-remote-access-ssl-vpn/)

6.6.2 IPSec VPN

Tehnologija IPSec VPN temelji na principu ovijanja (encapsulation) in šifriranja podatkov, ki jih prenašamo preko IP omrežij. Deluje v omrežnem sloju OSI modela in samo v omrežjih, ki temeljijo na IP tehnologiji.

IPSec ima dva načina delovanja (Savanović in Praprotnik, 2012):

- **transportni način** je osnovni način delovanja, kjer se šifrira samo koristna vsebina (tovor) IP paketa, ne pa tudi njegova glava. Transportni način se uporablja pri medsebojni komunikaciji dveh gostiteljskih sistemov (ang. host to host transport mode).
- **tunelski način** se uporablja za kreiranje VPN povezav v komunikaciji omrežje z omrežjem (ang. network-to-network communications), v komunikaciji gostitelj z omrežjem (ang. host-to-network) in komunikaciji gostitelj z gostiteljem (ang. host-to-host). V tem načinu se celotni IP paketi šifrirajo, overijo (ang. authentication) in nato enkapsulirajo v nov IP paket z novo IP glavo.

IPSec VPN uporablja veliko proizvajalcev, ki ponujajo strojne rešitve VPN povezav.

6.6.3 SSL VPN

SSL VPN (ang. Secure Sockets Layer Virtual Private Network) je navidezno zasebno omrežje, ki uporablja protokol SSL za vzpostavitev varne, šifrirane povezave preko interneta. Običajno

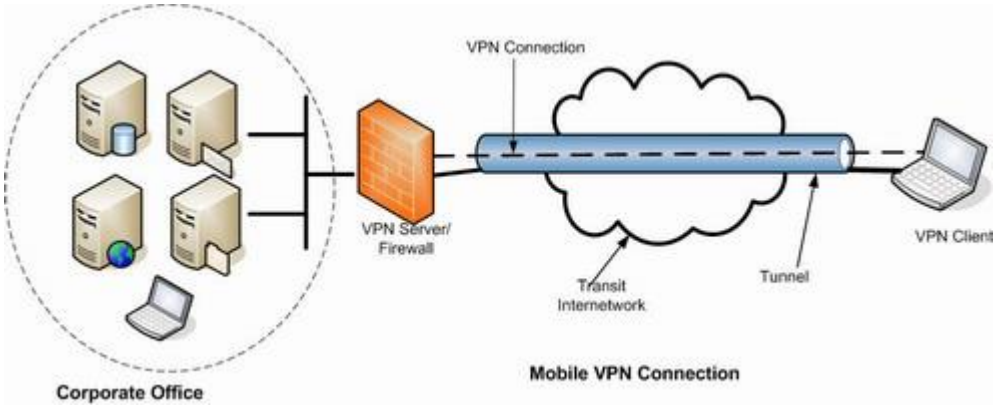
se izvaja prek spletnega brskalnika. Na odjemalski računalnik ni treba namestiti aplikacije, zato je upravljanje veliko lažje. Licenčnih pristojbin ni, programska oprema pa se samodejno nadgradi na strežniku, ne da bi za to potrebovali interakcijo uporabnika. Zaradi tega je ta vrsta VPN veliko manjše finančno breme in olajša obremenitev osebja IT (Palic, 2020).

SSL VPN-ji so v nekaterih primerih varnejši od običajnih, ker lahko preklapljajo le v spletne aplikacije namesto v celotno omrežje. Uporabnikove pravice je mogoče natančneje upravljati, saj lahko dostopajo samo do aplikacij, do katerih imajo pravico dostopati. To pa je hkrati tudi njihova slabost. Glavna pomanjkljivost VPN-ja SSL je, da ga je mogoče uporabiti samo za dostop do spletnih aplikacij. Odjemalec tudi ne more dostopati do fizičnih omrežnih virov, kot so tiskalniki. To nalaga uporabnikom omejitve, kar je v določenih situacijah lahko dobro (Palic, 2020).

SSL VPN postajajo vse bolj priljubljeni, ker se celotna omrežja selijo v oblak. V omrežjih v oblaku je vsa programska oprema omogočena prek spleta, zato SSL VPN deluje tako kot IPsec VPN za fizična omrežja. Dokumente je mogoče natisniti v PDF, prenesti in nato natisniti lokalno, če tako želi uporabnik (Palic, 2020).

Tehnologija SSL VPN temelji na protokolu SSL, ki je že vgrajen v vsakem brskalniku, zato VPN klienti ne potrebujejo posebnih namestitev (ang. clientless solution). Ker deluje v transportnem sloju, se izvaja tuneliranje do aplikacij, zato imajo uporabniki preko SSL VPN dostop samo do izbranih aplikacij na strani VPN strežnika in ne do njegovega celotnega omrežja. S tem se izboljša varnost omrežja na starani strežnika, poleg tega administratorji VPN omrežja lažje nastavijo uporabnikom pravice dostopa do različnih aplikacij.

Slabost SSL VPN omrežja je, da lahko uporabniki uporabljajo samo omrežne aplikacije. Sicer je možno preko SSL VPN omrežja uporabljati tudi druge aplikacije, vendar takšno omrežje zaradi dodatne programske opreme izgubi glavno prednost – enostavnost (Savanović in Praprotnik, 2012).



Slika 57: Gostitelj na omrežje VPN (host-to-network)
(http://nirlog.com/2006/01/23/secure-remote-access-ssl-vpn/)

7 SISTEMATIČNO IZVAJANJE VARNOSTNIH UKREPOV

Ugotovili smo, da je informacijski sistem ranljiv v vseh pogledih in da je skrb za informacijsko varnost ena izmed osnovnih nalog ekipe IT strokovnjakov podjetja. Žal pa njihovi napori in povsem pravilno delovanje ne omogočajo 100 % varnosti. Pomemben deležnik je uporabnik – človek. Informacijska varnost se tiče vseh zaposlenih v podjetju. Zato potrebuje podjetje varnostno politiko, ki jo morajo poznati vsi zaposleni in jo tudi spoštovati.

7.1 VARNOSTNA POLITIKA

Varnostna politika (ang. security policy) neke organizacije je množica postopkov in pravil, ki določajo odnos organizacije do varnosti. S pomočjo varnostne politike se postavijo meje sprejemljivega obnašanja in reakcije na kršenje le-teh. Pomemben del splošne varnostne politike posamezne organizacije je **informacijska varnostna politika**, katere glavni cilj je določitev pravil, vlog in odgovornosti na področju informacijske varnosti (Savanović in Praprotnik, 2012).

Namen informacijske varnostne politike je zaščita informacijskih sredstev in virov organizacije pred različnimi nevarnostmi, ki ogrožajo podatke in informacijsko opremo:

- notranjimi ali zunanjimi,
- namernimi ali nenamernimi.

Organizacije svojo varnostno politiko pogosto definirajo skladno s priporočili standarda ISO 27001. ISO 27001 je mednarodni standard, ki vsebuje zahteve za sistem upravljanja varnosti informacij, da bi omogočil organizacijam sistematično, ponovljivo in primerljivo oceno svojih tveganj in izvajanje ustreznih kontrol za ohranitev zaupnosti, celovitosti in razpoložljivosti informacij. Temeljni cilj je zaščita informacij pred tem, da pristanejo v napačnih rokah in/ali so izgubljene za vedno (Bureau Veritas, 2021).

Informacijska varnostna politika zajema naslednja področja:

- zagotavljanje zaupnosti, celovitosti in razpoložljivosti podatkov,
- varovanje podatkov pred nepooblaščenim dostopom, razkritjem, spremembo ali uničenjem,
- zagotavljanje izobraževanja iz informacijske varnosti za vse zaposlene,
- seznanjanje s pravili varne uporabe informacijske infrastrukture za vse uporabnike,
- obvladovanje varnostnih incidentov ter ustrezno ukrepanje ob zaznanih grožnjah,
- ravnanje v skladu z zakoni in predpisi, ki se nanašajo na varovanje podatkov.

Varnostni incidenti povzročajo škodo. Zagotavljanje informacijske varnosti stane. Zato poskuša varnostna politika določene organizacije določiti optimalno razmerje med ceno informacijske varnosti in ceno možne povzročene ekonomske škode.

Standard ISO 27001 določa smernice. Pravilnik, ki določa varnostno politiko organizacije je za vsako organizacijo unikaten zaradi njene specifike.

7.2 SISTEMATIČNO IZVAJANJE ZAŠČITE

Zaščito računalniškega sistema izvajamo fizično in s pomočjo IKT. Fizična zaščita pomeni, da je ključna računalniška oprema (npr. strežniki) shranjena v posebnih prostorih, kamor nepooblaščeni uporabniki nimajo vstopa. Razen tega se zaščita izvaja na ravni sistemske programske opreme in na nivoju aplikativnih programov.

Zaščita na ravni sistemske programske opreme zajema:

- dodeljevanje pravic uporabe sistema posameznim uporabnikov in skupinam uporabnikov, glede na potrebe, ki sledijo iz narave njihovega dela,
- zaščito diskov, map in dokumentov pred nepooblaščeno uporabo,
- varno komunikacijo preko interneta,
- preprečevanje vdorov v sistem,
- preventivno nadzorovanje sistema, odkrivanje in zapolnjevanje varnostnih vrzeli,
- izdelavo varnostnih kopij pomembnih podatkov in hranjenje varnostnih kopij izven lokalnega omrežja.

Operacijskemu sistemu znani uporabniki se v sistem prijavljajo z geslom, ki jim omogoča dostop do predvidenih virov. To pa hkrati onemogoča dostop nepooblaščenim uporabnikom do virov, ki jih ne potrebujejo (da ne bi npr. povzročili nepotrebnih napak) ali ne smejo uporabljati (npr. podatki, ki se jih ne tičejo in jih je potrebno varovati).

O varovanju računalniškega sistema je treba misliti, preden se zgodi napad na sistem ali okvara, ki bi lahko povzročila izgubo podatkov. Vsaka organizacija mora premisliti, kako bo varovala svoj računalniški sistem in podatke, to zapisati in izvajati. Varnostna politika oz. Pravilnik o varovanju podatkov je formalni zapis varnostnih mehanizmov in drugih pravil, ki jih morajo upoštevati vsi posamezniki z dostopom do opreme, prostorov in informacij. Če je varnostna politika in njena implementacija dobra, je verjetnost uspešnega napada na sistem majhna.

V RS imamo poseben zakon, ki se nanaša na informacijsko varnost: Zakon o informacijski varnosti (ZInfV) (Uradni list RS, št. 30/18 in 95/21).

7.2.1 Zaščita omrežja in pametnih naprav

V omrežje in posledično v internet povezujemo širok nabor različnih naprav: vse od merilnih sistemov, medicinskih aparatov pa tja do nadzornih sistemov naših elektrarn. Navdušenje nad možnostmi, ki jih prinaša internet pogosto preglasi varnostne pomisleke. Danes je sprejeto dejstvo, da moramo na računalnike redno nameščati popravke, ki odpravljajo varnostne pomanjkljivosti, če se želimo izogniti zlorabam. S pametnimi napravami ni nič drugače, saj na njih teče sorodna programska oprema. Vendar programe (aplikacije) običajno namestimo in nato nanje "pozabimo", kar jih pušča na voljo vdiralcem. Srečali smo se že s tiskalniki in TV–snemalniki, ki so izvajali napade onemogočanja, in z ogrevalnimi sistemi, ki so bili prosto dostopni vsakomur na omrežju. V prihodnosti lahko pričakujemo podobne zlorabe na "stvareh", povezanih v internet so pri SI-CERT napovedali l. 2014 (www.cert.si, 2014). Vsekakor so se te napovedi že leta 2016 uresničile z botnetom Mirai.

Applov operacijski sistem za mobilne naprave iOS je zaradi svoje zaprtosti veljal za enega bolj varnih. Vendar pa je celo Apple iOS 6.0 operacijski sistem za iPhone in iPad naprave vseboval več varnostnih ranljivosti. Uporabnike so po odkritju pozvali, da iOS nadgradijo (https://cert.si/si-cert-2013-02-varnostne-ranljivosti-apple-ios-6-0-operacijskega-sistema/, 18. 9. 2014).

Noben operacijski sistem ni brez varnostnih pomanjkljivosti. Kdor jih odkrije ter ima znanje in željo, jih lahko izkoristi. Ko so enkrat odkrite, pa jih lahko izkoristijo tudi tisti, ki prej zanje niso vedeli. Zato je treba operacijske sisteme redno posodabljati. Nasvet velja za vse vrste operacijskih sistemov.

Aplikacije, ki so na voljo za mobilne naprave, nameščamo preko AppStore (za Apple naprave) in Google Play Store (za Android naprave). Čeprav so aplikacije deležne testiranja in preverjanja, preden jih vključijo v trgovino, se je že zgodilo, da je imela aplikacija vgrajeno škodljivo kodo. Google je odkril vsaj 58 zlonamernih aplikacij, šele potem, ko so jih uporabniki že prenesli na svoje mobilne telefone (SI-CERT, 2018).

1.1.2 Zagotavljanje varnosti v omrežju

Znotraj omrežja podjetja so strukturirani podatki shranjeni v zbirkah podatkov, razen tega pa imamo še množico datotek, v katerih so razni izračuni, poslovna dokumentacija …

Podatke, ki so shranjeni v zbirkah podatkov, obdelujemo z različnimi računalniškimi aplikacijami. Zbirke podatkov varujemo pred nepooblaščenimi osebami na več načinov hkrati.

- Dostop do aplikacij in podatkov omejimo le na osebe, ki te dostope potrebujejo. To storimo tako, da dovolimo dostop do aplikacije ali posameznega njenega modula le pooblaščenih uporabnikom, ki se izkažejo z uporabniškim imenom in geslom. Včasih te vrste zaščite ne opazimo, ker dobimo uporabniki z vstopom v operacijski sistem (na podlagi uporabniškega imena in gesla) hkrati pravico dostopati do določenih aplikacij in podatkov.
- Uporabljamo tudi različne metode, ki zagotavljajo informacijsko varnost na ravni operacijskega sistema in omrežja. Omejimo dostope do map, v katerih so podatki in poskrbimo za druge varnostne mehanizme. Nujen je tudi požarni zid in protivirusna programska oprema.

Varnostni sistemski inženirji redno spremljajo napade na sistem (ti se dejansko stalno dogajajo) in po potrebi ukrepajo, skrbijo za izvajanje varnostne politike in redno posodabljanje varnostnih mehanizmov.

7.2.2 Zagotavljanje varnosti e-poslovanja

V e-poslovanju, kjer upravljamo tudi z denarjem in stalno komuniciramo prek interneta, ni dovolj, da ščitimo le podatke znotraj lastnega omrežja. Varnostni problem lahko nastopi, ko se podatki prenesejo preko interneta v neko drugo omrežje. Na vse, kar je izven našega omrežja pa nimamo vpliva. Zloraba se lahko zgodi, posledice pa čutimo mi sami.

Za zavarovanje pomembnih podatkov in sporočil uporabljamo metode šifriranja ali kriptografije. Ob vsej tej tehnično zagotovljeni varnosti pa še vedno nismo zares varni. Najsodobnejša protivlomna vrata ne preprečijo kraje, če jih pozabimo zakleniti. Enako velja za informacijsko varnost. Nezaželeni osebi moramo onemogočiti dostop do naše pametne kartice, osebnega gesla, kvalificiranega digitalnega potrdila ter zasebnega ključa. Vse te pojme bomo spoznali v nadaljevanju.

Svojih osebnih podatkov ne vnašamo v spletne aplikacije, če nismo prepričani, da so verodostojne (res tiste, za katere se izdajajo) in skrbijo za varen prenos ter obdelavo podatkov.

Za zagotavljanje informacijske varnosti smo zadolženi vsi:

- računalniški strokovnjaki, ki vzpostavimo tehnične mehanizme informacijske varnosti in
- uporabniki, ki z ustreznim ravnanjem skrbimo, da varnostni mehanizmi delujejo in ne dopuščamo nepridipravom, da nas z zvijačami pretentajo in nam škodujejo.

7.2.3 Zaščita podatkov med prenosom po internetu

Če dve stranki elektronsko poslujeta je pomembno, da podatke zaščitimo tudi med prenosom med njima.

Podatke je torej potrebno zavarovati na poti med pošiljateljem in prejemnikom. Sam prenos podatkov lahko poteka v lokalnem omrežju ali po internetu, tako na žičnem kot na brezžičnem omrežju. Na tej ravni uporabljamo različne varnostne protokole, kot so SSL (an. Secure Sockets Layer), TLS (an. Transport Layer Security) in IPSEC (an. Secure Internet Protocol).

TLS in njegovi predhodniki SSL so šifrirni protokoli, ki zagotavljajo zaupnost in integriteto podatkov za komunikacijo prek TCP/IP omrežij, kot je internet. **TSL in SSL protokoli omogočajo šifrirano povezavo med strežnikom in odjemalcem.**

Številne različice teh protokolov so razširjene v aplikacijah, kot so spletni brskalniki, elektronska pošta, pošiljanje sporočil in VoIP (voice-over-IP).

S TSL in SSL najpogosteje zaščitimo povezavo med uporabnikovim brskalnikom in spletnim strežnikom tako, da se ji ne da prisluškovati. Poleg tega omogočimo uporabnikom, da preverijo, ali so se priključili na pravi strežnik, saj iz strežnikovega digitalnega potrdila izvedo potrebne podatke. Zato ga uporabljajo praktično vsi zaupanja vredni spletni trgovci, ki na ta način zaščitijo prenos številk kreditnih kartic in drugih osebnih podatkov uporabnikov. Omogočena pa je tudi kontrola v drugi smeri. SSL omogoča tudi overjanje uporabnikov prek digitalnih potrdil, ki jih vključimo v brskalnike. Ob priključitvi na nek strežnik le-ta zahteva, da se brskalnik predstavi s svojim potrdilom. Odvisno od vsebine potrdila strežnik dovoli priključitev ali pa prekine povezavo (sigov-ca.gov.si, 2008).

Pri prenosu podatkov in informacij prek protokola SSL oz. TSL je treba nameniti pozornost tudi ugotavljanju verzije omenjenega protokola. Priporočljiva je uporaba najnovejše različice protokola.

Spletne strani, ki uporabljajo varne protokole, spoznamo po naslovu, ki se začne s https:\\. Preklop v varni režim se praviloma izvrši takoj, ko začnemo s postopkom plačevanja.

7.3 PENETRACIJSKO TESTIRANJE

Zagotavljanje kibernetske varnosti je kompleksen proces, saj se nenehno razvija tako informacijski sistem podjetja oz. organizacije kot kibernetske grožnje.

Na začetku poglavja smo navedli, da organizacija potrebuje celovito varnostno politiko oz. pravilnik, ki določa pravila, vloge in odgovornosti na področju informacijske varnosti. V praksi pri tem naletimo na nekaj težav. Varnostna politika je nepopolna, se ne posodablja redno, zaposleni z njo niso dovolj dobro seznanjeni ali pa se je striktno ne držijo, kar velja zlasti v zvezi z izpostavljenostjo na področju socialnega inženiringa.

Bolj kot je nek poslovni sistem velik in pomemben, bolj je izpostavljen napadom in večjo škodo lahko zaradi napadov utrpi. Zato je pomembna aktivnost zagotavljanja kibernetske varnosti preizkušanje, ali ukrepi resnično delujejo. Pomembno je, da obrambne sisteme preizkusijo izkušeni in dobro usposobljeni strokovnjaki za informacijsko varnost, saj je le tako mogoče najti in odpraviti različne ranljivosti in slabosti sistema. Pregledu, ki ga opravijo strokovnjaki z namenom preverjanja stanja kibernetske varnosti, rečemo penetracijsko testiranje. Smiselno je, da celovit varnostni pregled opravijo najprej strokovnjaki iz podjetja, nato pa še zunanji.

Penetracijski test je postopek, s katerim tretja oseba oziroma organizacija preveri zmožnost varnostnih zaščit podjetja. Svetujejo, da se ne preizkuša celotnega sistema varnosti hkrati in da se določi cilje varnostnega pregleda. Podjetje mora vedeti, kaj želi z varnostnim pregledom doseči (Seliškar, 2019).

Nekatere organizacije morajo penetracijski test opraviti zato, da zadostijo zahtevam regulatorjev in/ali zakonodaje. Nekatere organizacije skušajo ugotoviti, kaj je šlo narobe ob zadnjem vdoru. Obstajajo pa seveda tudi taki, ki se zavedajo, da jim penetracijsko testiranje lahko prepreči mnogo težav v prihodnosti.

Informatiki in varnostni inženirji, ki branijo omrežje in sisteme podjetja, pogosto o njem niso obveščeni, vodstvo podjetja pa bi moralo imeti zelo jasno in natančno predstavo o tem, kaj se bo zgodilo (Seliškar, 2019).

Po penetracijskem testu se običajno pridobi naslednja poročila:

- poročilo za vodstvo,
- analiza tveganj,
- tehnična dokumentacija za poustvarjanje ugotovitev,
- taktična in strateška priporočila.

Omenili smo, da je penetracijski test lahko celovit, ali pa zajema le določene dele sistema.

Primeri ciljno usmerjenega testiranja:

- simulacija kibernetskega napada,

- poskus zlorabe ranljivosti na zunanji infrastrukturi (strežniki, aplikacije, zaposleni),
- preverjanje učinkovitosti notranjih varnostnih kontrol proti napadalcu ali nezadovoljnemu zaposlenemu z dostopom do virov notranjega omrežja,
- odkrivanje ranljivosti v spletni aplikaciji, ki omogočajo nepooblaščen dostop in spreminjanje podatkov,
- odkrivanje ranljivosti v mobilni aplikaciji, ki omogoča nepooblaščen dostop in spreminjanje podatkov,
- test dovzetnosti zaposlenih za napad s tehnikami socialnega inženiringa ter s tem povezano odkrivanje pomanjkljivosti v procesih, postopkih in tehnologiji,
- preverjanje ranljivosti brezžičnega omrežja: ali lahko dobi napadalec nepooblaščen dostop do spletnega omrežja,
- test odpornosti proti DDoS napadom,
- test kibernetske odpornosti blockchain[24] rešitev,
- funkcionalno testiranje programske opreme: ali izvaja samo dokumentirane funkcionalnosti,
- iskanje zlonamerne programske opreme,
- test odpornosti IoT naprav proti kibernetskim napadom.

Seznam je sam po sebi dokaz, da vseh teh preverjanj ne more izvesti ista oseba. Potrebna so specifična in poglobljena znanja na posameznem področju. Celovit pregled je drag.

Zato se podjetja odločajo za preverjanje tistih delov informacijskega sistema, kjer zaznajo največje potrebe ali pa jih zakonodaja sili, da izvajajo neodvisna varnostna testiranja.

[24] Veriženje blokov

8 LITERATURA IN VIRI

Chernev, B. (2021). *What Is AES and Why You Already Love It.* Pridobljeno 9. 9. 2021 s: https://techjury.net/blog/what-is-aes/#gref

Banka Slovenije (2021). *Močna avtentikacija strank pri kartičnih plačilih*. Pridobljeno 8. 7. 2021 s: https://www.bsi.si/placila-in-infrastruktura/nacionalni-svet-za-placila/e-novice/e-novice-nacionalnega-sveta-za-placila-marec-2021/mocna-avtentikacija-strank-pri-karticnih-placilih

Bernik, I. in Meško, G. (2011). *Internetna študija poznavanja kibernetskih groženj in strahu pred kriminaliteto*. Revija za kriminalistiko in kriminologijo, 62(3), 242–252

Bryant, S. (25. 6. 2019). How Many Startups Fail And Why? Investopedia. Pridobljeno 19. 12. 2019, s: https://www.investopedia.com/articles/personal-finance/040915/how-many-startups-fail-and-why.asp

Bureau Veritas (2021). ISO 27001. Pridobljeno 8. 7. 2021 s: https://www.bureauveritas.si/certificiranje/iso-27001?gclid=Cj0KCQjwxJqHBhC4ARIsAChq4atNJIHhvsPVwn2_PgT61KLRppqF97Y0edhEOE6vLuSGquG2HdpaemsaAjyyEALw_wcB

Crane, C. 2020). *What Is a Firewall? Definition, Types & Business Uses.* Pridobljeno 30. 8. 2021 s: https://www.thesslstore.com/blog/what-is-a-firewall-definition-types-uses/

Cisco (2021). Cysco Certified expert: Dynamic or Stateful Packet Filtering Firewalls, Pridobljeno 30. 8. 2021 s: https://www.ccexpert.us/scnd-2/dynamic-or-stateful-packet-filtering-firewalls.html

Cisco (2021). *Cysco Certified expert: Application Layer Proxy Firewall.* Pridobljeno 30. 8. 2021 s: https://www.ccexpert.us/scnd-2/application-layer-proxy-firewall.html

Cisco (2021), *Cysco Certified expert: Deep Packet Inspection.* Pridobljeno 30. 8. 2021 s: https://www.ccexpert.us/data-centers/deep-packet-inspection.html

Clayton, M. (2021). *How the FBI and Interpol trapped the world's biggest Butterfly botnet*. Pridobljeno 4. 8. 2021 s: https://www.csmonitor.com/USA/2011/0630/How-the-FBI-and-Interpol-trapped-the-world-s-biggest-Butterfly-botnet

DeLisle, B. (17. 7. 2018). SATIS Group Report: '78% of ICOs are Scams'. Pridobljeno 19. 12. 2019, s: https://cryptoslate.com/satis-group-report-78-of-icos-are-scams/

Devopedia (2020). *Information Security Principles.* Pridobljeno 8. 7. 2021 s: https://devopedia.org/information-security-principles

Evropska unija (2017). *Delegirana uredba komisije (EU) 2018/389.* Pridobljeno 8. 7. 2021 s: https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:32018R0389&from=EN

European Cybercrime Center (2018). *Internet organised crime threat assessment (IOCTA) 2018.* Pridobljeno 16.11.2020, s: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018

European Cybercrime Center (2019). *Internet organised crime threat assessment (IOCTA) 2019.* Pridobljeno 16.11.2020, s: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019

European Cybercrime Center (2020). *Internet organised crime threat assessment (IOCTA) 2020.* Pridobljeno 16.11.2020, s: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

Fazlić, D. (2021). *Na spletu podatki 533 milijonov Facebook uporabnikov, tudi 230.000 Slovencev*. Pridobljeno 4. 4. 2021 s: https://www.24ur.com/novice/znanost-in-tehnologija/na-spletu-podatki-533-milijonov-facebook.html

FBI (11. 6. 2021). *Investment Fraud.* Pridobljeno 1. 4. 2021 s: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/investment-fraud

Globalknowledge (2021). *Cybersecurity Glossary of Terms.* Pridobljeno 31. 8. 2021 s: https://www.globalknowledge.com/us-en/topics/cybersecurity/glossary-of-terms/

Graff, G. M. (2017). *How a Dorm Room Minecraft Scam Brought Down the Internet.* Pridobljeno 23. 8. 2021 s: https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/

Hackmageddon (2021). *Q2 2021 Cyber Attack Statistics.* Pridobljeno 23. 8. 2021 s: https://www.hackmageddon.com/2021/07/22/q2-2021-cyber-attack-statistics/

Informacijski pooblaščenec. (2009). *Socialni inženiring in kako se pred njim ubraniti?* Ljubljana: Informacijski pooblaščenec. Pridobljeno 6. 10. 2020 s: http://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/socialni-inzeniring-in-kako-se-pred-njim-ubraniti.pdf

Informacijski pooblaščenec, SI_CERT. *ABC varnosti in zasebnosti na mobilnih napravah.* Pridobljeno 6. 10. 2020 s: https://www.ip-rs.si/fileadmin/user_upload/Pdf/novice/ABC_varnosti_in_zasebnosti_na_mobilnih_napravah.pdf

Islovar (2021). Slovar Islovar. Pridobljeno 2. 6. 2021 s: http://www.islovar.org/islovar

Kee, L. (2021). *RSA Is Dead — We Just Haven't Accepted It Yet*. Pridobljeno 9. 9. 2021 s: https://www.forbes.com/sites/forbestechcouncil/2021/05/06/rsa-is-dead---we-just-haventaccepted-ityet/?sh=43ca04ba5d22

Kovačič, M. (2018). *Zgostitveni algoritmi in zagotavljanje integritete digitalnih dokazov.* Pridobljeno 26. 8. 2021 s: https://infosec-seminar.si/arhiv/02_Kovacic_Zagotavljanje_integritete_podatkov_v_digitalni_forenziki.pdf

Lagner (2010). *Stuxnet analysis by Langner*. Pridobljeno 18. 8. 2021 s: https://www.langner.com/Stuxnet/

McAfee (2021). *What Is Fileless Malware?* Pridobljeno 2. 8. 2021 s: https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-fileless-malware.html

Microsoft (2021). *Passwords technical overview.* Pridobljeno 2. 8. 2021 s: https://docs.microsoft.com/en-us/windows-server/security/kerberos/passwords-technical-overview

Mizrahi, A. (2018). *Europol: Hardcore Criminals Are Shifting From Bitcoin to Monero, Zcash and Dash.* Pridobljeno27. 5. 2021 s: https://news.bitcoin.com/europol-hardcore-criminals-shifting-bitcoin-monero-zcash-dash/

MJU (2018). Ocena kibernetskih tveganj, Pridobljeno 15. 12. 2020 s: https://www.gov.si/assets/ministrstva/MJU/DI/Ocena_kibernetskih_tveganj_v1_0_Fina_P.pdf

National Archives and Records Administration (2020). *Records Management Guidance for Agencies Implementing Electronic Signature Technologies*. Pridobljeno 4. 8. 2021 s: https://www.archives.gov/files/records-mgmt/faqs/pdf/electronic-signiture-technology.pdf

Network Encyclopedia (2021). *Network Encyclopedia*. Pridobljeno 1. 10. 2021 s: https://networkencyclopedia.com/

NICCS - National initiative for cybersecurity careers and studies (2021). *Cybersecurity Glossary*. Pridobljeno 4. 8. 2021 s: https://niccs.cisa.gov/about-niccs/cybersecurity-glossary#

Norton (2020). What is computer virus? Pridobljeno 18. 8. 2021 s: https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html

Oracle (2017). *Glossary of Networking Terms.* Pridobljeno 30. 8. 2021 s: https://docs.oracle.com/cd/E53394_01/pdf/E54755.pdf

Palic, J. (2020). *Comparing IPsec vs. SSL VPN*. Pridobljeno 29. 8. 2021 s: https://www.onlc.com/blog/comparing-ipsec-vs-ssl-vpns/

Pavlič, D. (2021). *Razsežnost in kompleksnost Madoffove sheme presenečata še danes.* Časnik Finance. Pridobljeno 10. 5. 2021 s: https://www.finance.si/8974102/Razseznost-in-kompleksnost-Madoffove-sheme-presenecata-se-danes

Policija (28. 5. 2021). *Pozor, izsiljevalski virusi!* Pridobljeno 28. 5. 2021 s: https://www.policija.si/svetujemo-ozavescamo/varnost-na-internetu/85763-pozor-izsiljevalski-virusi

Policija (9. 4. 2021). *Policija obravnava vse več goljufij z lažnimi investicijskimi vlaganji, ki obljubljajo tudi več kot stoodstotno tedensko donosnost.* Pridobljeno 11. 6. 2021 s: https://www.policija.si/medijsko-sredisce/sporocila-za-javnost/sporocila-za-javnost-gpue/108450-policija-obravnava-vse-vec-goljufij-z-laznimi-investicijskimi-vlaganji-ki-obljubljajo-tudi-vec-sto-odstotno-tedensko-donosnost

Rafter, D. (2021). *How to protect your privacy online.* Pridobljeno 4. 8. 2021 s: https://us.norton.com/internetsecurity-privacy-protecting-your-privacy-online.html

Raywood, D. (2011). *Butterfly botnet morph is bigger, badder than Mariposa*. Pridobljeno 4. 8. 2021 s: https://www.itnews.com.au/news/butterfly-botnet-morph-is-bigger-badder-than-mariposa-262306

Roubini, Nouriel. (10. 5. 2018). *Initial Coin Scams.* Project Syndicate, Pridobljeno 15. 11. 2019, s:https://www.project-syndicate.org/commentary/ico-cryptocurrency-scams-by-nouriel-roubini-2018-05?barrier=accesspaylog

Roubini, Nouriel. (16. 7. 2019). *The Great Crypto Heist.* Project Syndicate. Pridobljeno 15. 11. 2019, s: https://www.project-syndicate.org/commentary/cryptocurrency-exchanges-are-financial-scams-by-nouriel-roubini-2019-07?barrier=accesspaylog.

Savanovič, A., Praprotnik, G. (2012). Informacijska varnost. VŠPV.

Seliškar, V. (2019). *Kaj morate vedeti o penetracijskih testih?* Pridobljeno 31. 8. 2021 s: https://www.monitor.si/clanek/kaj-morate-vedeti-o-penetracijskih-testih/191526/

Shepherd, M. (2020). ICO Statistics (2020): Funding, Investment, and Best ICOs. Pridobljeno 15. 1. 2020, s: https://www.fundera.com/resources/ico-statistics

SI-CERT (2018). *Poročilo o omrežni varnosti za leti 2016 in 2017.* SI-CERT. Pridobljeno 8. 9. 2018 s: https://www.cert.si/wp-content/uploads/2018/04/SI-CERT_LP_2016_2017.pdf

SI-CERT (2018). *SI-CERT TZ001 / Ukrepi ob napadih onemogočanja*. SI-CERT. Pridobljeno 5. 9. 2021 s: https://www.cert.si/ukrepi-ob-napadih-onemogocanja/

SI-CERT (2019). *Poročilo o omrežni varnosti za leto 2018*. Pridobljeno 19. 9. 2019 s: https://www.cert.si/wp-content/uploads/2019/09/Poro%C4%8Dilo-o-kibernetski-varnosti_2018_splet.pdf

SI-CERT (2020). *Poročilo o omrežni varnosti za leto 2019*. Pridobljeno 24. 5. 2020 s: https://www.cert.si/wp-content/uploads/2020/07/Poro%C4%8Dilo-o-kibernetski-varnosti_2019_.pdf

SI-CERT (2021). SI-CERT TZ008 / *Vektor okužbe: nelegalna programska oprema*. Pridobljeno 6. 9. 2021 s: https://www.cert.si/tz008/

SI-CERT (2021). *Virusi s podpisi slovenskih podjetij*. Pridobljeno 6. 9. 2021 s: https://www.cert.si/letna_porocila/porocilo-o-kibernetski-varnosti-za-leto-2020/

SI-CERT (2021). *Poročilo o omrežni varnosti za leto 2020*. Pridobljeno 6. 9. 2021 s: https://www.cert.si/virusi-s-podpisi-slovenskih-podjetij/

SI-TRUST (2021). *O kriptografiji.* Pridobljeno 28. 8. 2021 s: https://www.si-trust.gov.si/sl/podpora-uporabnikom/o-kriptografiji/

Techopedia (2021). *Authorization.* Pridobljeno 13. 7. 2021 s: https://www.techopedia.com/definition/10237/authorization

The Spamhouse project (2020). *Spamhaus Botnet Threat Report 2019.* pridobljeno 15. 12. 2020 s: https://www.deteque.com/app/uploads/2019/02/Spamhaus-Botnet-Threat-Report-2019.pdf

Torproject (2021). *Tor: Overview*. Pridobljeno 29. 8. 2021 s: https://2019.www.torproject.org/about/overview

Varni na internetu. *ABC varnosti za lastnike spletnih strani.* SI-CERT. Pridobljeno 26. 9. 2018 s: https://www.varninainternetu.si/wp-content/uploads/2013/09/Varnost_spletnih_mest_web.pdf

Varga, M. (2017). *Zašifrirajmo vse!* Pridobljeno 23. 8. 2021 s: https://www.monitor.si/clanek/zasifrirajmo-vse/181609/

Varni na internetu (2021). *Kako preveriš fotografijo in razkrinkaš prevaro?* Prisobljeno 31. 5. 2021 s: https://www.varninainternetu.si/kako-preveris-fotografijo/

Vasilijevič, B., Jarc, B., Škrobar, D., in drugi (2006). *Informacijska varnost na delovnem mestu: e-gradivo*. Ljubljana: B2 d.o.o., Pridobljeno 16. 12. 2020, s: www.spletno-ucenje.com.

Verizon (2020). *Data Breach Investigations Report, 2020.* Pridobljeno 16.12.2020 s: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Vodopivec, T. (2010). *Ekonomija kibernetskega kriminala na primeru e-bančnih zlorab.* V: Uravnotežite naložbe, tveganja in razvoj za uspeh : zbornik prispevkov. Ljubljana: SDI, 2010.

Vodopivec, T. (2011), *Informacijsko podprto zaznavanje in preprečevanje prevar – čas za dejanja.* V: Nove razmere in priložnosti v informatiki kot posledica družbenih sprememb : zbornik prispevkov. Ljubljana: SDI, 2011.

WiFi alliance, (2021). *Security.* Pridobljeno 27. 8. 2021 s: https://www.wi-fi.org/discover-wi-fi/security

Wikipedia (2021). Stuxnet. Pridobljeno 21.5.2021 s: https://en.wikipedia.org/wiki/Stuxnet

Wikipedia (2021). *Madoff investment scandal.* Pridobljeno 24. 5. 2021 s: https://en.wikipedia.org/wiki/Madoff_investment_scandal

Wilson, T. (2019). *Explainer: 'Privacy coin' Monero offers near total anonymity*.Reuters. Pridobljeno 28. 5. 2021 s: https://jp.reuters.com/article/idUSKCN1SL0F0?mod=related&channelName=businessNews

Whitman, M. E., Mattord, H. J. (2019), Principles of Information Security (6th Edition). Cengage Learning.