Mjerenje aktivnosti korisnika na krajnjem uređaju

Edjut, Katarina

Master's thesis / Diplomski rad

2020

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Organization and Informatics / Sveučilište u Zagrebu, Fakultet organizacije i informatike**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:211:082096

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Katarina Edjut

MJERENJE AKTIVNOSTI KORISNIKA NA KRAJNJEM UREĐAJU

DIPLOMSKI RAD

Varaždin, 2020.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Katarina Edjut

JMBAG: 0016108278

Studij: Organizacija poslovnih sustava

MJERENJE AKTIVNOSTI KORISNIKA NA KRAJNJEM UREĐAJU

DIPLOMSKI RAD

Mentor:

Dr. sc. Mario Žgela

Varaždin, rujan 2020.

Katarina Edjut

Izjava o izvornosti

Izjavljujem da je moj diplomski rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

Autor potvrdio prihvaćanjem odredbi u sustavu FOI-radovi

Sažetak

Glavna tema ovog rada je pojam krajnjeg uređaja i mjerenje aktivnosti korisnika na krajnjem uređaju. Prilikom definiranja i objašnjavanja pojma krajnjeg uređaja dolazi se do poveznice takvih uređaja i računalnih mreža, a ta poveznica dovodi do teme osiguravanja sigurnosti prilikom korištenja krajnjih uređaja i računalnih mreža u kojima se oni nalaze. Jedan od načina osiguranja sigurnosti je kontrola aktivnosti korisnika na uređajima unutar mreže kako bi se osiguralo da ne dođe do nenamjerno ili namjerno lošeg djelovanja prilikom korištenja. Kontrola aktivnosti korisnika uključuje i proces mjerenja samih aktivnosti što se može postići pomoću različitih metoda mjerenja. Za mjerenje aktivnosti korisnika je unutar rada odabrana metoda gdje se bilježe performanse odabranih dijelova sustava.

Ključne riječi: krajnji uređaj, računalna mreža, sigurnost sustava, aktivnosti korisnika, korištenje diskovnog sustava, korištenje memorije, performanse procesora, mrežni resursi

Sadržaj

1. Uvod

Razvoj komunikacijskih i računalnih tehnologija značajno je utjecao na daljnji smjer povijesti čovječanstva i način života kojeg su ljudi poznavali do tada. Ove tehnologije otvorile su mogućnosti o kojima se ranije nije sanjalo i time omogućile velike promjene u područjima kao što su međuljudska komunikacija, putovanje, očuvanje prirode, kvaliteta života, znanstvena istraživanja i druga. Poboljšanjem kvalitete i dužine života povećao se i broj ljudi, a konstantnim napretkom komunikacijskih i računalnih tehnologija one su postale dio svakodnevnog života običnog čovjeka i bitan dio poslovnog svijeta.

Povećanjem broja računala i komunikacijskih uređaja koji se koriste u privatne svrhe i onih koji se koriste u poslovne svrhe, došlo je do pitanja sigurnosti, tj. kakav rizik za pojedinca ili poduzeće predstavlja korištenje ovakvih uređaja i kakva je povezanost između korištenja uređaja od strane pojedinaca i sigurnosnih rizika koje određeni način korištenja uređaja povlače za sobom.

Ovim radom bit će objašnjeni pojmovi krajnjeg uređaja i računalne mreže i kako su oni međusobno povezani. Boljim poznavanjem ovih pojmova dovodi se u pitanje sigurnost takvih uređaja i sigurnost računalnih mreža u koju su oni povezani, a sukladno s time i sigurnost organizacija koje koriste i posjeduju računalne mreže, i zbog toga će biti detaljnije objašnjeno područje sigurnosti računalnih mreža. Nakon ovoga slijedit će praktični prikaz spremanja velikog broja podataka o aktivnostima na krajnjem uređaju (računalu) i potom analiza dobivenih podataka putem programa za vizualizaciju podataka.

2. Krajnji uređaji

Početak korištenja pojma krajnji uređaj vezan je uz područje računalnih mreža. Svrha računalnih mreža je razmjena podataka između različitih čvorova unutar mreže koji su međusobno povezani. Burnham [1] izjavila je da se svi čvorovi unutar mreže mogu nazvati krajnjim uređajima, a prema ovome vidljiva je važnost mrežnih čvorova za očuvanje i djelovanje mreže.

Napretkom tehnologije i znanja o njoj, pojam krajnjeg uređaja dobivao je sve šire značenje i počeo je uključivati veliki raspon uređaja, različitih funkcionalnosti i uloga, operacijske sustave i drugo. Ovakav razvoj ukazao je potrebu za novim definiranjem pojma krajnjeg uređaja, a jedan način su odredili Rai i Chukwuma [2], koji su u svojem opisu krajnjeg uređaja naveli da on može biti bilo koji softver ili hardver koji posjeduje IP adresu, ima mogućnost prijenosa podataka na drugi uređaj, može prikazivati ili obrađivati podatke ili može pristupiti računalnoj ili mrežnoj infrastrukturi.

Mrežne i računalne infrastrukture imaju značajnu ulogu u današnjem poslovanju poduzeća, a povezano time, potrebno je kontrolirati uređaje koji imaju mogućnost spajanja na mrežu organizacije. Krajnji uređaji unutar organizacije predstavljaju značajni sigurnosni rizik za cijeli sustav organizacije, ne samo zbog mogućih vanjskih prijetnji, već i zbog mogućnosti unutarnjih prijetnji nastalih prilikom, namjerno ili slučajno, lošeg korištenja uređaja od strane zaposlenika.

Prema podjeli M. Kandrich-a [3] u nastavku ovog poglavlja biti će navedene grupe krajnjih uređaja i odrednice koje pomažu pri raspodjeli uređaja u grupe. Prikaz raznih grupa krajnjih uređaja bitan je kako bi se lakše razumjela veličina i raznovrsnost njihovih uloga unutar organizacija i važnost, ali i kompleksnost, kontrole ovakvih uređaja za osiguranje sigurnosti poslovanja poduzeća.

2.1. Windows krajnji uređaji

Prvu grupu krajnjih uređaja određuje činjenica da oni izvršavaju neku od verzija Microsoft Windows operacijskih sustava, a M. Kandrich [3] navodi da se ovakve uređaje može zvati Windows krajnjim uređajima. Međutim ovakvo određivanje članova grupe Windows krajnjih uređaja nije dovoljno detaljno opisano, stoga je potrebno reći da, kako bi uređaj koji izvršava Microsoft Windows operacijski sustav bio klasificiran kao Windows krajnji uređaj, minimalan uvjet je da on sadrži integrirani Microsoft Diskovni Operacijski Sustav (MS-DOS) sa Windows upraviteljem (eng. *Windows Manager*).

Microsoft Windows 95 je bio prvi microsoft-ov operacijski sustav koji je razvijen na ovaj način i time je on začetnik Windows krajnjih uređaja. Nakon grupe operacijskih sustava koji su sadržavali MS-DOS, temeljen na komandnim linijama, razvijena su računala s grafičkim korisničkim sučeljem koje je bilo jednostavno za koristiti i koje je podržavalo veliki broj aplikacija. Ulaganje u razvoj grafičkih sučelja omogućilo je da Microsoft Windows sustavi postanu najpopularniji operacijski sustavi za osobna računala. Ovakav razvoj operacijskih sustava privukao je veliki broj privatnih i poslovnih korisnika, a time i veću zainteresiranost u zlonamjerno korištenje i djelovanje nad sustavom, koje je potaknulo istraživanje o prijetnjama prema sustavu kao i razvoj metoda za osiguranje sigurnosti sustava.

2.2. Ne windows krajnji uređaji

Samo ime ovakvih krajnjih uređaja nije dovoljna odrednica kako bi se oni mogli uvrstiti u ovu grupu, i stoga je potrebno detaljnije opisati ovu skupinu. M. Kandrich [3] napominje da se široki obujam ovog skupa treba ograničiti samo na računala, tj. prijenosna računala, stolna računala i servere, koji ne izvršavaju neki od Microsoft Windows operacijskih sustava. Ovakvom specifikacijom se određuje da u skupinu ne windows krajnjih uređaja pripadaju sva računala koja sadrže i izvršavaju neki od UNIX operacijskih sustava.

Popularnost UNIX operacijskih sustava je dobivena jednostavnim korisničkim sučeljem, hijerarhijskom raspodjelom datoteka, što osigurava efikasnu implementaciju i jednostavno održavanje, datotekama s konzistentnim formatom, što omogućava jednostavnije kreiranje novih računalnih programa, višekorisničkim i višeprocesnim sustavom i drugim osobinama, koje navodi M. J. Bach [4]. Popularnost UNIX operacijskih sustava uzrokovala je i pojavu velikog broja različitih operacijskih sustava, a neki od njih su nadalje navedeni.

Linux je operacijski sustav otvorenog koda i jedan od najpouzdanijih, najsigurnijih i najpoznatijih operacijskih sustava otvorenog koda. Moguće ga je koristiti na mnogo različitih uređaja i prilagoditi svakom korisniku, pa je zbog toga nastalo mnogo njegovih inačica, a neke od njih su Manjaro, Debian, Ubuntu, Linux Mint i Solus. BSD operacijski sustav (eng. *Berkeley Software Distribution*) razvijen je od strane istraživača okupljenih oko sveučilišta “University of California ar Barkeley”. AIX operacijski sustav (eng. *Advanced Interactive eXecutive*) je razvio IBM i trenutno je podržan na IBM Power Systems. Apple Inc je u suradnji sa zajednicom otvorenog koda razvio operacijski sustav Darwin koji je otvorenog koda, a potom samostalno operacijski sustav macOS koji je zatvorenog tipa. Operacijski sustav HP-UX ili Hewlett Packard Unix, je razvio Hewlett Packard i namijenjen je PA-RISC i Intel Itanium 2 arhitekturama. IRIX operacijski sustav je osmislilo poduzeće Silicon Graphics i

on je služio za obavljanje zahtjevnih zadataka vezanih uz grafiku, ali je kasnije ukinut. Microsoft je također razvio operacijski sustav baziran na UNIX-u i nazvao ga Xenix, ali on je kasnije ukinut, kao i operacijski sustav Solario, baziran na UNIX-u i napravljen od strane Oracle-a.

2.3. Ugrađeni krajnji uređaji

Postoji mnogo definicija i opisa ugrađenih krajnjih uređaja, ali dva opisa koji su navedeni nadalje predočavaju kompleksnost i raznolikost uređaja ovakve vrste. M. Maxfield [5] je iznio misao o ugrađenim krajnjim uređajima gdje je opisao da se za krajnji uređaj može reći da je on ugrađen krajnji uređaj ukoliko korisnik nije svjestan njegove prisutnosti sve dok uređaj ne prestane raditi ili prestane raditi kako bi trebao. Ovakav opis uređaja dovodi u pitanje koju razinu sigurnosti oni posjeduju i kakav rizik oni predstavljaju za korisnika. Također, ovakav opis uređaja ih ne specificira dovoljno pa se dovodi u pitanje raznolikost funkcionalnosti i uloga koje ovakvi krajnji uređaji posjeduju. O raznolikosti ugrađenih krajnjih uređaja govori i M. Kandrich [3], koji u svojem definiranju ove grupe uređaja objašnjava kako u nju spadaju svi svrhom građeni računalni sustavi. Iz navedenim opisa ugrađenih krajnjih uređaja vidljivo je da oni imaju svrhu u puno aspekata svakodnevnog života od kojih su neki bitni za pravilno funkcioniranje društva, kao što su npr. medicina, zrakoplovstvo, bankarstvo, kućni uređaji i brojni drugi.

Mogućnost krajnjih uređaja da se spoje na internet je dodatno povećala broj mogućih članova grupe ugrađenih krajnjih uređaja, pa se tako u nju svrstavaju i uređaji iz područja koje se naziva Internet stvari (eng. *Internet of Things*) ili skraćeno IoT. IoT predstavlja mrežu međusobno povezanih uređaja koje je moguće identificirati uz pomoć jedinstvenih odrednica, a svrha ovakve mreže je da omogući samostalnu razmjenu korisnih informacija koje se zapažaju i bilježe pomoću senzora i zatim koriste za donošenje odluka na temelju kojih je kasnije moguće izvršavati automatizirane akcije. Prema M. U. Farooq, M. Waseem, S. Mazhar, A. Khairi, T. Kamal [6] uz ranije objašnjenje IoT-a, može se reći i da on omogućava komunikaciju između uređaja, dok su prije njega postojale samo komunikacije između ljudi ili komunikacija čovjek - uređaj.

Nabrajanje postojećih ugrađenih krajnjih uređaja zbog njihove raznolikosti nije praktično, ali zbog predočavanja važnosti njihove uloge nadalje će biti navedeno nekoliko primjera. M. Kandrich [3] naveo je kako je prvi ugrađeni krajnji uređaj bio računalo „Apollo Guidance Computer“ ili skraćeno AGC, koji je 60-ih godina dvadesetog stoljeća imao ulogu u prijevozu ljudi na Mjesec i njihovom sigurnom povratku na Zemlju. Ovakva uloga bila je od povijesne važnosti za čovječanstvo, ali ne treba zanemariti da se oni imaju i manje, ali

jednako bitne uloge, za nesmetano funkcioniranje društva. Tako su neki od poznatijih ugrađenih krajnjih uređaja bankomati, pisači i hladnjaci s pristupom internetu, računala koja upravljaju robotima, uređaji koji osiguravaju bežični pristup internetu (eng. *access points*) i brojni drugi. U današnje vrijeme puno medicinskih kriza, potrebno je napomenuti da u skupinu ugrađenih krajnjih uređaja pripadaju i računalni sustavi koji svakodnevno pomažu u spašavanju nebrojeno mnogo života, a nalaze se unutar medicinskih respiratora.

2.4. Mobilni krajnji uređaji

Mobilni uređaji su računala male veličine koja su prijenosna i je moguće upravljati u rukama, a prema N. L. Beddall-Hill, A. Jabbar, S. Al Shehri [8], oni trebaju imati mogućnosti uspostave komunikacije između osoba, kreiranja, prijenosa i pohrane podataka i medija (npr. fotografije) i povezivanja na internet. Grupa mobilnih krajnjih uređaja obuhvaća pametne telefone, tablete, neke igraće konzole, pametne satove, kalkulatore, digitalne kamere i druge. Mobilni uređaji oduzimaju značajan postotak vremena u danu prosječne osobe, a svrha njihovog korištenja nije samo komunikacija s drugim ljudima ili razonoda, već i pomoć pri poslovnim, edukacijskim i drugim potrebama. Danas su pametni mobilni telefoni član grupe mobilnih krajnjih uređaja za koju se velikim brzinama kreiraju nove aplikacije, poboljšavaju operacijski sustavi i unaprjeđuju tehničke osobine velikim brzinama.

Brzim tehnološkim napretkom mobilnih uređaja nastalo je i mnogo različitih operacijskih sustava koji se koriste na njima. Mobilni operacijski sustavi mogu biti djelomično otvorenog koda, otvorenog koda i zatvorenog koda, a postoji i nekolicina operacijskih sustava koji su ukinuti, a jedno vrijeme su bili popularni na tržištu mobilnih uređaja (npr. BlackBerry OS, Symbian, Windows Mobile…). Najpoznatiji mobilni operacijski sustav današnjice je Android. Prema M. Karch [7], Android je operacijski sustav otvorenog koda, namijenjen za mobilne uređaje (mobitele, tablete, pametne satove, itd.), sagrađen na temelju jezgre Linux operacijskog sustava. Google koji je kreirao Android dopušta mnogobrojnim proizvođačima mobitela da besplatno koriste dijelove android operacijskog sustava na svojim uređajima, koji proizvođačima omogućavaju da kreiraju inačice operacijskih sustava namijenjenih samo za svoje mobilne telefone. Ovim načinom nastali su mnogobrojni operacijski sustavi temeljeni na android operacijskom sustavu, a neki od njih su: EMUI napravljen od strane Huawei-a, HTC Sense, MIUI kojeg je izgradio Xiaomi, One UI od Samsunga i brojni drugi. Drugi najpoznatiji operacijski sustav za mobilne uređaje je iOS razvijen od strane Apple Inc.-a namijenjen za njihove mobilne uređaje kao što su iPhone i iPod. Temeljem iOS operacijskog sustava Apple je razvio inačice koje se koriste za iPad, Apple TV i Apple Watch.

3. Krajnji uređaji u računalnim mrežama

Raznolikost krajnjih uređaja i njihova velika prisutnost ukazuju na to da oni imaju ulogu unutar računalnih mreža. Prema J. Šehanović, Ž. Hutinski, M. Žugaj [9], računala koja su međusobno povezana na određenoj lokaciji nekim oblikom medija koji omogućava razmjenu informacija se nazivaju računalnom mrežom. Usporedbom ovakvog definiranja računalne mreže, i definiranja pojma krajnji uređaj iz prvog poglavlja, gdje je navedeno da su svi čvorovi računalne mreže krajnji uređaji, može se zaključiti da su ova dva pojma međusobno povezana. Uz postojanje fizičkih čvorova koje predstavljaju krajnji uređaji, važan dio računalnih mreža je postojanje komunikacije između čvorova koja omogućava pristup i razmjenu podataka unutar računalne mreže. Prema J. M. Kizza [10], računalne mreže su kombinacija hardverskih i softverskih dijelova, gdje se u hardverske dijelove uvrštavaju krajnji uređaji, dok u softverski dio spadaju svi programi i pravila za komunikaciju, tj. protokoli, koje svi povezani uređaji unutar mreže moraju poštivati. Nastavak ovog poglavlja bit će usmjeren na hardverske osobine računalnih mreža i u njemu će biti prikazane osobine koje su bitne za razumijevanje uloga krajnjih uređaja unutar računalnih mreža i zašto je bitno kontrolirati aktivnosti korisnika na krajnjim uređajima.

3.1. Klasifikacija računalnih mreža

Računalne mreže su kompleksni sustavi i zbog toga ima nekoliko njihovih klasifikacija, ovisno o tome koja od njihovih osobina se promatra. Prvi način klasifikacije računalnih mreža je određen geografskim područjem kojeg mreža pokriva, drugi način klasifikacije se odnosi na strukturu računalne mreže, a treći način se fokusira na način prijenosa podataka kroz mrežu.

3.1.1. Geografska klasifikacija

Raznolikost veličina geografskih lokacija koje računalne mreže pokrivaju postaje upečatljiva kada se uzme u obzir da se računalne mreže mogu nalaziti na području jedne sobe i sadržavati svega nekoliko uređaja, ili uključuju milijune međusobno povezanih uređaja koji se mogu nalaziti bilo gdje sve dok su povezani na Internet. Prema S. Bourgeois [11], s obzirom na geografske odrednice, računalne mreže je moguće svrstati u jedanaest kategorija, i to su redom: PAN (eng. Personal Area Network), LAN (eng. Local Area Network), WLAN (eng. Wireless Local Area Network), CAN (eng. Campus Area Network), MAN (eng. Metropolitan Area Network), WAN (eng. Wide Area Network), SAN (kratica koja se koristi za pojmove eng. Storage-Area Network i eng. System-Area Network), POLAN

(eng. PAssive Optical Local Area Network), EPN (eng. Enterprise Private Network) i VLAN (eng. Virtual Private Network).

Osobna računalna mreža ili PAN je mreža koja pokriva najmanje područje, najčešće se nalazi unutar jedne građevine, i uključuje mali broj uređaja koje posjeduje i/ili koristi samo jedna osoba. Krajnji uređaji koji se nalaze unutar ovakve mreže su bežični modem, jedan ili dva računala i nekolicina manjih uređaja kao što su pisač, pametni telefon, tablet i slični uređaji koje jedna osoba može koristiti u slobodno vrijeme ili za obavljanje posla.

Lokalna računalna mreža ili LAN uključuje više grupa računala i drugih krajnjih uređaja koji se nalaze međusobno nalaze na maloj udaljenosti, npr. unutar iste zgrade. LAN je najpoznatija vrsta računalnih mreža i najčešće se koristi u poslovne svrhe, tj. unutar poduzeća za pristup poslovnom sustavu i potrebnim podacima. WLAN, CAN i MAN moguće je promatrati kao podvrste LAN-a zbog zajedničkih osobina koje dijele s LAN-om, međutim svaka od ovih mreža ima osobine koje ju razlikuju od njega.

Bežična lokalna računalna mreža ili WLAN je istih osobina kao i LAN, osim što se za povezivanje i komunikaciju među krajnjim uređajima koriste bežične tehnologije kao što je Wi-Fi.

Računalna mreža kompleksa sveučilištaili CAN, je računalna mreža koja može pokriti veće područje od LAN-a, ali manje od MAN-a. CAN najčešće uključuje kompleks od više zgrada koje su međusobno u neposrednoj blizini i osobe koje se nalaze unutar njih imaju potrebu za razmjenom zajedničkih podataka. U ovu skupinu spadaju poduzeća koja posluju unutar više zgrada koje se nalaze blizu jedna drugoj, sveučilišta koja se nalaze na više lokacija koje su na maloj udaljenosti i slični kompleksi.

Gradska računalna mreža ili MAN, površinom kojom obuhvaća je veća od LAN-a, ali manja od WAN-a. Površina MAN-a najčešće sadrži neku lokalnu jedinicu kao što je grad, selo ili županija.

Široko područna računalna mreža ili WAN povezuje grupe računala koje se nalaze na velikim udaljenostima kao što države, međunarodna područja, kontinente, a u nekim slučajevima i globalno. Postoji puno primjera WAN-a, internet je WAN-a na globalnoj razini, a neki od primjera na nacionalnoj razini su CARNet (akademska računalna mreža u Hrvatskoj), DATAPAC (državna računalna mreža Kanade), Telenet (javna državna računalna mreža Sjedinjenih Američkih Država). Internet je primjer međunarodne, globalne računalne mreže.

Skladišna računalna mreža ili SAN povezuje grupe uređaja za pohranu podataka i poslužitelje. Prema S. Bourgeois [11], ovakva računalna mreža omogućava odvajanje resursa za pohranu podataka od računalnih mreža kao što je LAN i stvaranje računalne mreže velikih brzina koja je pogodna za pohranu podataka.

Računalna mreža sustava, koja također ima kraticu SAN, je prema S. Bourgeois [11], vrsta lokalne računalne mreže koja omogućava veze velikih brzina kod aplikacija korištenih između poslužitelja, unutar skladišne računalne mreže i aplikacija među procesorima, a računala koja su povezana unutar ovakve mreže mogu izvoditi zadatke jako velikim brzinama i međusobno se ponašaju kao jedan ujedinjeni sustav.

POLAN ili pasivna optička lokalna računalna mreža, je mreža koja, prema S. Bourgeois [11], koristi optičke razdjelnike kako bi iz jednog optičkog signala nastalo više optičkih signala koje mogu koristiti krajnji uređaji i njihovi korisnici.

EPN ili privatna računalna mreža poduzeća, nastaju od strane poduzeća koja žele omogućiti sigurnu razmjenu podataka između računala koja se nalaze na različitim lokacijama koje poduzeće posjeduje, npr. između poslovnica različitih gradova.

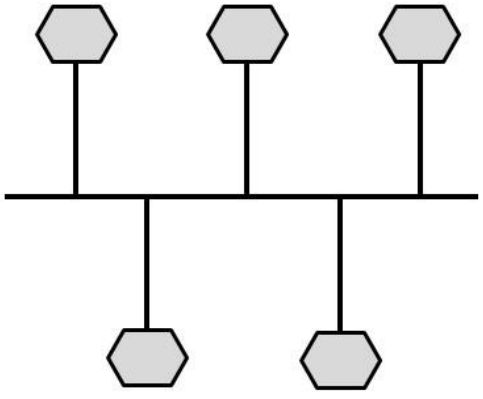
VPN ili virtualna privatna računalna mreža, omogućava krajnjim uređajima pristup na privatnu računalnu mrežu iako oni nisu povezani na nju. Ovakav pristup privatnoj računalnoj mreži na daljinu, omogućen je zbog spajanja mreže na Internet i stvaranja virtualne veze između dva krajnja uređaja.

3.1.2. Topološka klasifikacija

Topološka klasifikacija računalne mreže uzima u obzir fizički sastav same mreže, tj način na koji će krajnji uređaji (čvorovi) unutar mreže biti međusobno raspoređeni i kako će biti izvedeno njihovo spajanje.

P2P (eng. point to point) ili struktura od točke do točke je najjednostavnija struktura računalnih mreža u kojoj postoje direktne veze između dva krajnja uređaja unutar mreže.

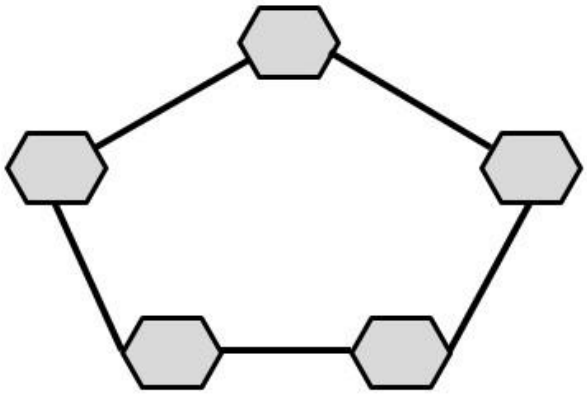
Sabirnička struktura računalne mreže dobila je naziv po sabirnici koja predstavlja kanal za prijenos podataka. Svi uređaji spojeni na ovakvu strukturu računalne mreže imaju pristup svim porukama koje se šalju kroz sabirnicu.



Slika 1: Sabirnička struktura računalne mreže (Prema: K. Pandya, 2013)

Sabirnička struktura je dobra za računalne mreže koje nemaju puno čvorova, tj. krajnjih uređaja, koji su na slici 1 predstavljeni šesterokutima, jer problemom kod jednog čvora može doći do upitne funkcionalnosti cijele mreže zato što svi čvorovi dijele jedan kanal za prijenos podataka. Lokalne računalne mreže s manjim brojem čvorova pogodne su za sabirničku strukturu, koja će omogućit jednostavnije i jeftinije povezivanje postojećih i dodavanje novih uređaja. Unatoč tome potrebno je razmisliti o budućoj isplativosti ovakve strukture mreže, jer s povećanjem broja uređaja u mreži ova postaje sve sporija.

Prstenasta struktura računalne mreže dobila je naziv po rasporedu uređaja unutar mreže. Oni su povezani u oblik kružnice i ne postoji središnji uređaj.

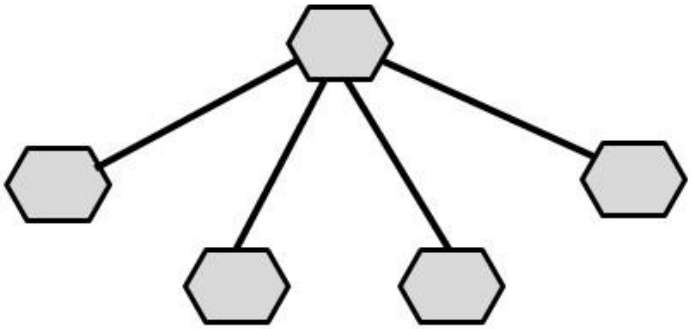


Slika 2: Prstenasta struktura računalne mreže (Prema: K. Pandya, 2013)

Prstenasta struktura računalne mreže, kao što je vidljivo na slici 2, sadrži vezu od točke do točke (P2P) između svaka dva susjedna čvora mreže. Ove veze, prema K. Pandya [12], omogućavaju slanje poruka u samo jednom smjeru zbog čega poslane poruke putuju od jednog čvora do drugog u krug sve dok poruka ne dođe do čvora koji je namijenjen za njeno primanje i njegova adresa se nalazi kao prefiks unutar poslanog paketa. Prstenasta struktura je kao i sabirnička, namijenjena za računalne mreže s manje uređaja kao što je LAN, ali za razliku od sabirničke, prstenasta struktura omogućava izbacivanje čvora sa kvarom iz mreže što dozvoljava nesmetanu komunikaciju između ostatka čvorova. Prstenasta struktura također nudi veće brzine prijenosa od sabirničke jer se paketi regeneriraju kod svakog čvora kroz kojeg prolaze. Negativna strana ovakve strukture je teži pronalazak greški unutar prstena zbog kružnog prolaska paketa i teže postavljanje ovakve mreže za razliku od sabirničke.

Zvjezdasta struktura računalne mreže, za razliku od ranije navedenih struktura, sadrži centralni čvor na kojeg su spojeni svi ostali čvorovi unutar mreže. Čvorovi prilikom

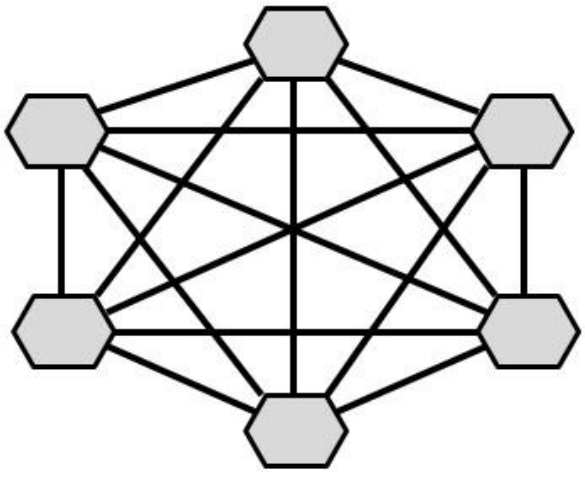
međusobne komunikacije prvo šalju paket centralnom čvoru koji paket zatim preusmjerava odgovarajućem čvoru za prihvat podataka.



Slika 3: Zvjezdasta struktura računalne mreže (Prema: K. Pandya, 2013)

Prema slici 3 na kojoj je vidljiv izgled zvjezdaste strukture, moguće je uočiti da ovakva struktura zahtjeva puno veću količinu fizičkih resursa za spajanje uređaja u mrežu, jer npr. iako su čvorovi susjedni i blizu jedni drugom, nije ih moguće direktno spojiti već je potreban spoj preko središnjeg uređaja/čvora. Pozitivna strana ovakve strukture je da zbog postojanja središnjeg čvora, ukoliko dođe do greške kod nekog od drugih čvorova ona ne utječe na djelovanje ostalih čvorova, a s druge, negativne strane, ukoliko dođe do greške kod središnjeg čvora tada je onemogućeno funkcioniranje cijele računalne mreže.

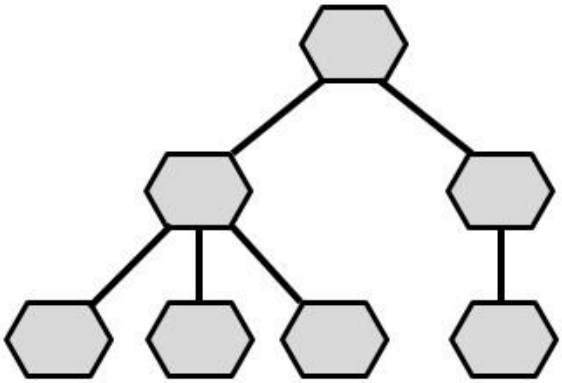
Mrežna struktura računalne mreže specifična je po tome što, ukoliko je povezanost između čvorova dobra, tada postoji direktna veza između svaka dva čvora mreže.



Slika 4: Mrežna struktura računalne mreže (Prema: K. Pandya, 2013)

Primjer mrežne strukture računalnih mreža sa slike 4 prikazuje da u slučaju ovakve strukture postoje redundantne veze između čvorova koje osiguravaju da se sva komunikacija unutar mreže odvija nesmetano. Problem ove strukture je jako velika količina fizičkih poveznica koje su potrebne između čvorova da bi se ostvarila komunikacija što stvara visoke troškove prilikom izrade mreže. Zbog ovakvih osobina mrežna struktura koristi se u slučajevima gdje je bitno konstantno funkcioniranje mreže, kao što je telefonska mreža.

Struktura stabla za računalne mreže je najčešća struktura koja se koristi za lokalne računalne mreže. Struktura stabla sadrži centralni čvor kao i zvjezdasta struktura, ali za razliku od nje sadrži i dodatne čvorove koji su koncentratori (eng. hub) i prosljeđuju poruke od centralnog čvora prema krajnjim čvorovima i obratno.



Slika 5: Struktura stabla za računalne mreže (Prema: K. Pandya, 2013)

Prema slici 5 vidljivo je da je centralni čvor korijen stabla, nakon njega slijedi drugi sloj koji predstavlja koncentratore na koje se kasnije u trećem sloju spajaju ostali krajnji uređaji. Ovakav raspored veza između čvorova unutar mreže osigurava da postoji jedinstveni put za razmjenu podataka između svaka dva čvora.

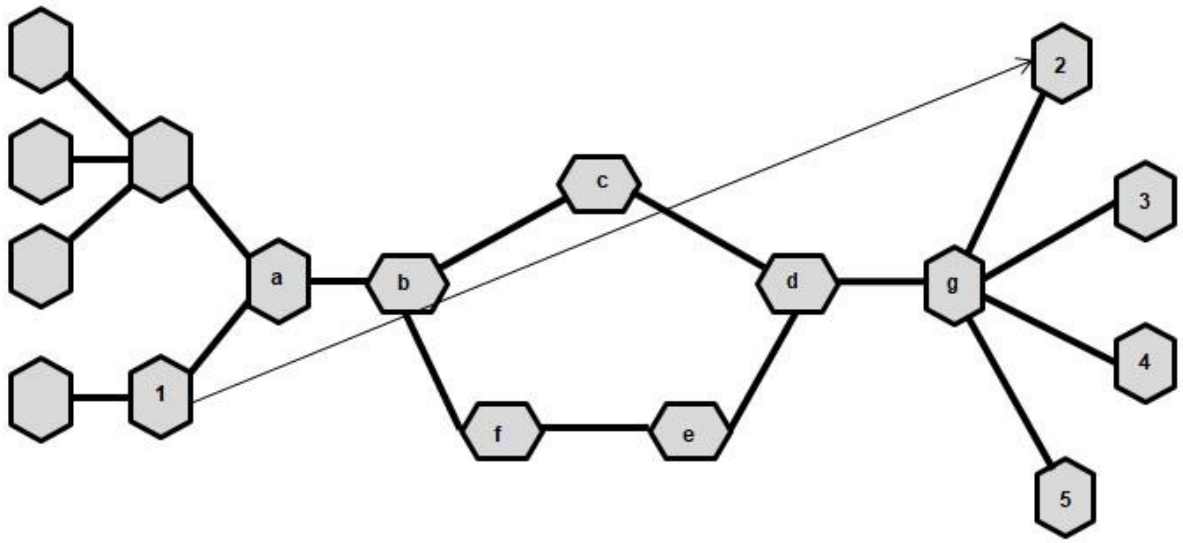
Od svih ranije navedenih struktura računalnih mreža moguće je napraviti hibridnu mrežu koja se sastoji od nekoliko različitih struktura koje su povezane. Ovakva struktura sadrži obilježja od svih struktura od kojih se sastoji, i zato je njezino kreiranje skupo i teže za izvesti za razliku od ostalih struktura. Kompleksnost i prilagodljivost hibridne strukture računalnih mreža odgovara zahtjevima velikih mreža koje se sastoje od velikog broja uređaja i pokrivaju geografski veliku površinu.

3.1.3. Klasifikacija prema načinu razmjene podataka

Klasifikacija prema načinu razmjene podataka, kao što i sam naziv govori, se bavi podjelom računalnih mreža prema načinu na koji uređaji unutar mreže šalju podatke jedni drugima. Prema O. Bonaventure [13], računalne mreže se prema načinu razmjene podataka mogu podijeliti u četiri grupe, a to su: emitiranje (eng. broadcasting), unicast, multicast i anycast.

Emitiranje (eng. broadcasting) je oblik razmjene podataka gdje uređaj pošiljatelj šalje podatke svim drugim uređajima koji se nalaze u geografskom području određenom od strane pošiljatelja. Ovakav oblik razmjene koristi se većinom u televizijskom i radijskom programu za slanje video ili audio poruka velikom broju primatelja, no postoji mogućnost za njegovo korištenje kod lokalnih računalnih mreža.

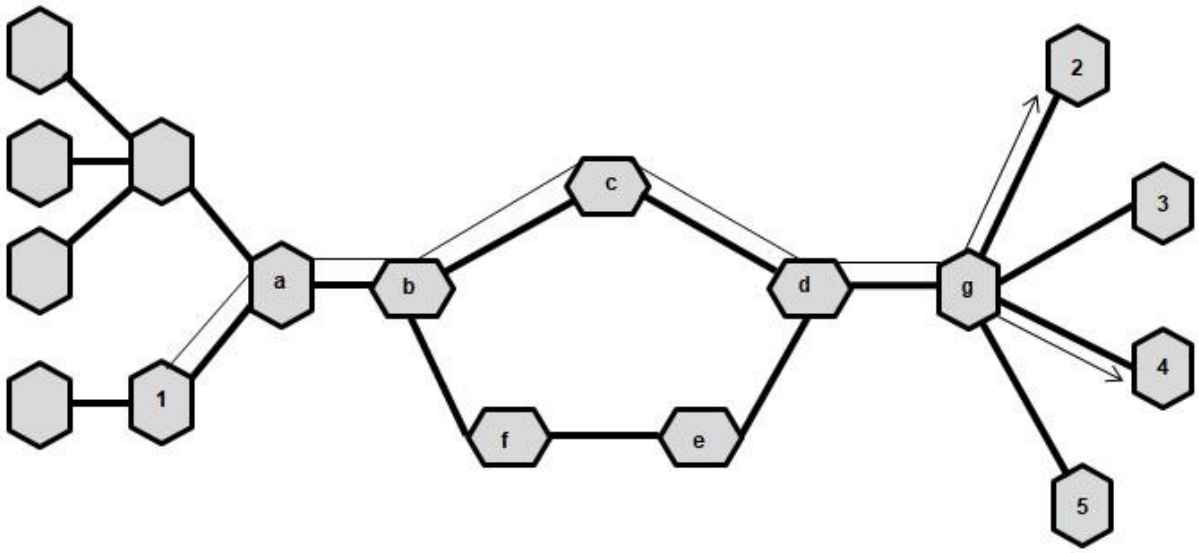
Unicast je oblik razmjene podataka gdje uređaj pošiljatelj šalje podatke jednom uređaju primatelju. Ovakav oblik razmjene podataka najčešće se koristi kod lokalnih računalnih mreža i kod nekih široko područnih računalnih mreža kao što je Internet.



Slika 6: Unicast oblik razmjene podataka (Prema: O. Bonaventure, 2011)

Kada uređaj 1 šalje podatke uređaju 2 unicast načinom razmjene podataka, ti podaci trebaju proći kroz nekolicinu uređaja koncentratora unutar mreže, što je vidljivo na slici 6. U ovom slučaju koncentratori, kroz koje podaci trebaju prvo proći i koji će ih usmjeriti pravom uređaju primatelju (uređaj 2) pomoću adrese uređaje zapisane unutar paketa s podacima, su uređaji a, b, c, d, i g. Nije bilo moguće usmjeriti poruku na način da redom prolazi kroz koncentratore a, b, f, e, d, g zbog toga što su veze unutar prstenastog dijela ove računalne mreže orijentirane u smjeru kazaljke na satu i samo u tom smjeru je moguće slati podatke.

Multicast oblik razmjene podataka se koristi u slučaju kada je potrebno poslati određeni set podataka od uređaja pošiljatelja do više uređaja primatelja, tako da je multicast još moguće opisati i kao oblik razmjene podataka jedan na više.

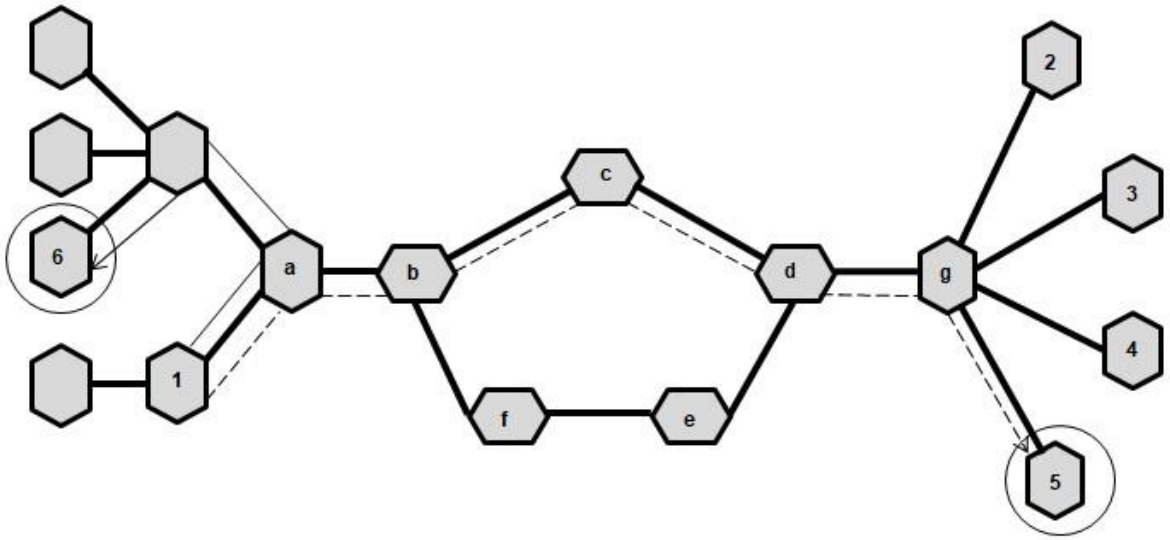


Slika 7: Multicast oblik razmjene podataka (Prema: O. Bonaventure, 2011)

Kada bi se u slučaju na slici 7 radilo o unicast obliku razmjene podataka, tada bi poruka sa podacima trebala dva puta proći kroz čvorove a, b, c, d, e zato što bi uređaj 1 trebao slati poruku dva puta, jednom za uređaj 2, i drugi put za uređaj 3, bez obzira na to što poruke sadrže iste podatke. Time se nepotrebno zauzimaju resursi unutar mreže koji bi se mogli efikasnije iskoristiti.

U slučaju slike 7 ipak se radi o multicast razmjeni podataka, gdje strelica na slici označava put kojem se šalje poruka unutar mreže, a slanje podataka se odvija na drugačiji način u usporedbi sa unicast oblikom i resursi u mreži se bolje iskorištavaju. Multicast oblik razmjene podataka omogućava da uređaj 1 pošalje jednu kopiju poruke s podacima koja se potom šalje prema koncentratoru a, koji prosljeđuje poruku sljedećem koncentratoru u nizu, a to je koncentrator b. Koncentrator b nastavlja sa slanjem poruke koncentratoru c, nakon kojeg poruka odlazi do koncentratora d i zatim do posljednjeg koncentratora g. Koncentrator g izrađuje dvije kopije poruke s podacima i potom prvu kopiju šalje uređaju 2, a drugu kopiju uređaju 4. Ovakav oblik razmjene podataka omogućava optimalnije slanje poruka kroz mrežu kada jedan pošiljatelj šalje jednu poruku prema više određenih primatelja, zato što se ista poruka šalje kroz određenu vezu između čvorova mreže samo jednom.

Posljednji oblik razmjene podataka je anycast. Razmjena podataka kod anycast oblika zahtjeva početno određivanje skupa uređaja koji su pogodni za primanje podataka koji se šalju, a potom računalna mreža određuje kojem uređaju iz zadanog seta će se podaci poslati.



Slika 8: Anycast oblik razmjene podataka (Prema: O. Bonaventure, 2011)

Set mogućih primatelja podataka unutar mreže, koje je odredio uređaj pošiljatelj nazvan 1, je na primjeru sa slike 8 označen sa kružnicama i sadrži uređaje 5 i 6. Nakon što je pošiljatelj odabrao set uređaja za slanje podataka, ovisno o topološkom uređenju računalne mreže, uređaj primatelj će najčešće biti izabran tako da se gleda najkraći put od pošiljatelja do mogućih primatelja. U slučaju računalne mreže sa slike 8, za primanje podataka odabran je uređaj 6, koji je bio najbliže pošiljatelju i na vezi između njega i pošiljatelja, koja je označena strelicom sa punom crtom, je bilo manje čvorova nego na vezi između pošiljatelja (uređaj 1) i potencijalnog primatelja (uređaj 5), koja je označena strelicom sa isprekidanom crtom. Prema O. Bonaventure [13], ukoliko uređaj 1 odluči ponovno slati iste podatke istom setu uređaja primatelja, taka će za primanje biti odabran uređaj koji do tada nije dobio podatke koji se šalju. Ovakav način razmjene podataka omogućava da će podaci doći do barem jednog od željenih primatelja, što stvara redundanciju u mreži, isto kao i kod mrežne strukture računalnih mreža. Redundancija u mreži osigurava željeni protok podataka. ali kreiranje i održavanje ovakvih mreža zahtjeva više resursa nego kod drugih oblika razmjene podataka ili fizičke topologije.

4. Sigurnost računalnih mreža

Sigurnost računalnih mreža odnosi se na korake koji se poduzimaju kako bi se podaci koji se nalaze unutar mreže kao i uređaji i veze od kojih se ona sastoji osigurali od vanjskih ili unutarnjih prijetnji koje bi omele nesmetano funkcioniranje cijele računalne mreže. Prema EC-Council [14], CIA trijada pomaže prilikom kreiranja sigurnosnih modela unutar poduzeća tako što ukazuje na 3 najbitnije stavke sigurnosti unutar računalne mreže, a skraćenica CIA odnosi na povjerljivost (eng. confidentiality), integritet (eng. integrity) i dostupnost (eng. availability). Povjerljivost unutar računalne mreže znači da se u njoj kontrolira tko ima pristup određenim podacima. Integritet unutar mreže je bitan jer osigurava podatke od brisanja ili promjene od strane osoba koje nemaju pristup istim podacima, a dostupnost omogućava pristup traženim podacima kada je to potrebno ukoliko postoji odobrenje za pristup istima. Povjerljivost, integritet i dostupnost su glavna načela koja je potrebno osigurati unutar računalne mreže, a neki od osnovnih postupaka za njihovo osiguranje su prema EC-Council [14], ostvarivanje fizičke sigurnosti računalne mreže, izrada kontrole pristupa, ovjera identiteta za one koji pristupaju mreži ili podacima unutar nje i odgovornost članova za postupke unutar mreže. Osiguranje sigurnosti računalne mreže zahtjeva dobro poznavanje njenih dobrih strana i ranjivosti, kako bi se na vrijeme otkrili potencijali izvori prijetnja i preventivno ugradili mehanizmi koji bi spriječili negativno djelovanje tih prijetnji na računalnu mrežu.

4.1. Sigurnosne ranjivosti računalnih mreža

Sigurnosne ranjivosti računalne mreže, prema J. M. Kizza [15], se mogu pronaći na hardverskim i softverskim dijelovima računalne mreže, unutar pravila, procedura i politika koje se koriste u mreži i također unutar sigurnosnih mjera zaštite te mreže. Ovakav široki pogled na sigurnosne ranjivosti ukazuje na to da je potrebno sagledati računalnu mrežu iz svih mogućih kutova kako bi se zaštitilo njeno pravilno funkcioniranje, jer svaka ranjivost mreže predstavlja mogućnost za loše djelovanje nad istom. Veliki spektar mogućih ranjivosti mreže, koji se svaki dan povećava s razvojem novih tehnologija koje je moguće uključiti u mrežu, potaknuo je autora J.M. Kizza [15] da u svojoj knjizi navede neke od najpoznatijih ranjivosti koje utječu na sigurnost računalnih mreža i to su po njemu mane unutar dizajna mreže, loše upravljanje sigurnošću, loša implementacija, ranjivosti tehnologija povezanih s internetom, razlike u ponašanju uljeza, poteškoće u popravljanju ranjivih mreža, ograničena djelotvornost reaktivnih rješenja i socijalni inženjering.

4.1.1. Mane dizajna

Mane dizajna računalnih mreža mogu se pronaći unutar hardverskih i softverskih područja. Unatoč konstantnom tehnološkom napretku hardverskih dijelova mreže gdje nastaju brojne promjene na uređajima i vezama između uređaja, mane u hardveru je lakše pronaći i otkloniti zbog boljeg znanja o hardverskom sustavu i njegovog lakšeg testiranja. Softverski dio računalne mreže je onaj koji predstavlja problem za uočavanje ranjivosti i njihovo otkrivanje. Promjene u softverskom dijelu koje nastaju na dnevnoj bazi i od strane velikog broja ljudi, zajedno sa promjenama koje bi trebalo implementirati zbog napretka u softverskim tehnologijama, dovodi do toga da su ranjivosti sustava jako dobro sakrivene i da je potrebno dobro poznavanje sustava kako bi se one uočile i otklonile. J.M. Kizza [15] navodi kako je softverske ranjivosti moguće grupirati i to tako da je prva grupa uzrokovana ljudskim djelovanjem, druga grupa je uzrokovana kompleksnošću softvera, treća je određena odabirom pouzdanih izvora za softver, a četvrta se odnosi na implementiranje zastarjelog dizajna, korištenje starih softverskih rješenja i reinženjering postojećih rješenja.

Pogreške u sustavu nastale od strane čovjeka uzrokuju veliki broj ranjivosti. Čovjek može namjernim ili nenamjernim djelovanjem djelovati na računalnu mrežu i stvoriti pogreške zbog kojih ona postaje ranjiva na napade. Nenamjerna djelovanja od strane čovjeka mogu biti brojna, a često u ne idealnim radnim uvjetima može doći do velikog broja njih, od kojih su neki: nezapamćeni zadaci koje treba napraviti da bi se osigurala sigurnost (npr. zaboravljeno testiranje određenog dijela softvera), korištenje neprovjerenih ili neodgovarajućih softverskih rješenja od strane osoba koje misle da računalnu mrežu poznaju bolje nego što je to stvarno istina, brzanje u izradi softverskih rješenja i kreiranje pogrešaka koje bi inače bile uočene i slične situacije. Ovakve greške se događaju kada na mreži rade osobe koje ju ne poznaju dovoljno dobro ili makar posjeduju dobro znanje nisu dovoljno koncentrirane na rad koji izvode što dovodi do kreiranja ranjivosti u mreži koje se ne bi dogodile u idealnim uvjetima. Zlonamjerno djelovanje od strane čovjeka najčešće se događa s predumišljajem i od strane osoba koje dobro poznaju računalnu mrežu te zbog toga imaju više prilika za napraviti štetu u sustavu. Motivaciju za zlonamjerno djelovanje nije teško pronaći i ona je najčešće financijske prirode (npr. želja za zaradom), želja za osvetom, ostvarivanje nekog drugog oblika dobiti (npr. temelj za ucjenu) i slična djelovanja. Općenito ranjivosti koje nastaju od strane čovjekovog djelovanja je teško u potpunosti izbrisati iz računalne mreže, jer nijedna osoba nije idealna, a pogotovo teško je spriječiti ranjivosti koje nastaju ako osoba želi namjerno oštetiti mrežu. Nenamjerno kreiranje ranjivosti moguće je kontrolirati educiranjem zaposlenika i korisnika o mreži ili osiguravanjem dobre okoline za rad kako bi se poboljšala koncentracija educiranih radnika i smanjila kašnjenja koja dovode do brzanja u nadogradnji, izradi i održavanju računalnih mreža.

Kompleksnost softvera otvara mogućnost za postojanje brojnih ranjivosti unutar računalne mreže. Kompleksna softverska struktura programa ili sustava otežava njegovo ispravno kreiranje, održavanje i nadogradnju. Testiranje kompleksnih sustava zahtjeva veliko znanje o sustavu, ali unatoč tome kompleksnost onemogućava testiranje svih mogućih scenarija koji se mogu dogoditi uz sve moguće ulazne parametre koji prate određene scenarije. Ovakvo nepotpuno testiranje uvijek može dovesti do stvaranja ranjivosti sustava koje je teško uočiti na vrijeme prije nego netko iskoristi tu ranjivost za zlonamjerno djelovanje. Jednostavnost kreiranja novih kodova, od strane osoba koje nemaju znanje o softveru ili jednostavno nemaju znanje za kreiranje dobrog koda, omogućava stvaranje pogrešaka koje softver čine ranjivim, a kada je softver kompleksan tada je lakše napraviti nenamjernu pogrešku, pogotovo kad ne postoji dovoljno znanje o njemu.

Pouzdanost softverskih izvora i proizvoda igra veliku ulogu u postojanju mana u dizajnu i povezano s time postojanju ranjivosti u računalnoj mreži. Unutar računalne mreže postoje brojni softverski sustavi prilikom čije izrade ili održavanja se često koriste softverski proizvodi iz vanjskih izvora čija kvaliteta, sigurnost i izvorište su ponekad upitni. Usred nedoumice, neznanja, skupoće izgradnje i sličnih problema, se koriste gotova programska rješenja, koja mogu biti npr. otvorenog koda, i za koja se često ne može sa sigurnošću reći jesu li pravilno testirana i predstavljaju li rizik za mrežu, a koja sve dok obavljaju zadatak kojeg bi trebala, se ne preispituje puno. Povećanjem korištenja ovakvih programskih proizvoda od vanjskog izvora povećava i rizik kojem se računalna mreža izlaže.

Implementiranje zastarjelog dizajna, korištenje starih softverskih rješenja i reinženjering postojećih rješenja događa se zbog sve bržeg napretka u području softvera. Korištenje već postojećih softverskih proizvoda u neku novu svrhu i reinženjering implementiranih softvera se provode zbog toga što zahtijevaju manje vremena provedenog u usporedbi sa kreiranjem novih proizvoda, a ujedno smanjuju vrijeme i troškove koji su povezani sa testiranjem ovakvih prerađenih softverskih rješenja. Unatoč početnom smanjenju troškova i uštedi na vremenu, ukoliko se otkrije da softverski proizvod koji se upotrebljavao za više projekata ima manu koja nije na vrijeme otkrivena ili ne odgovara u potpunosti novoj ulozi u koju je implementiran, tada početni troškovi i vrijeme provedeno za implementaciju počinju rasti i postavlja se pitanje isplativosti korištenja već postojećih ili zastarjelih rješenja.

4.1.2. Loše upravljanje sigurnošću

Upravljanje sigurnošću je prema J.M. Kizza [15], mješavina tehničkih i administrativnih akcija koje uključuju kontrolu sigurnosti i sigurnosne politike koje su implementirane u poslovanje poduzeća. Za upravljanje sigurnošću je bitno stalno kontrolirati

sigurnost sustava i procjenjivati koliko postavljena sigurnosna politika pozitivno djeluje na održavanje sigurnosti sustava. Kada postoji neadekvatna kontrola sigurnosnih politika poduzeća, tj. njihove implementacije, provođenja i praćenja rezultata, može se reći da poduzeće ima loše upravljanje sigurnošću. Dobro upravljanje sigurnošću zahtjeva da poduzeće ima kvalitetan tim zadužen za sigurnost koji će dobro provoditi sigurnosne politike i nadgledati implementacije sigurnosnih stavki, te provoditi upravljanje rizikom, stvarati politike za zaštitu informacija i procedure i standarde za osiguranje sigurnosti, kontrolirati sigurnost i educirati ostale zaposlenike organizacije o održavanju sigurnosti. Efikasan tim za provođenje sigurnosti sustava predstavlja temelje za dobro upravljanje sigurnošću.

Nakon uspostavljanja dobrog tima zaduženog za sigurnost, potrebno je provoditi analizu rizika koja će otkriti koji dijelovi organizacije predstavljaju ranjivost za nju, i ukoliko se takve ranjivosti ne uklone kakve posljedice će nastati za organizaciju. Otkrivanje rizika pomaže u kreiranju novih sigurnosnih politika koje služe za uklanjanje postojećeg rizika i smanjenje mogućnosti da u budućnosti nastane rizik istog tipa kao ranije otklonjeni. Također je potrebno kontrolirati sigurnost sustava kako bi se onemogućilo i otkrilo moguće zlonamjerno djelovanje, otklonilo sigurnosne prijetnje u što kraćem vremenu nakon njihovog nastanka i slične akcije. Bitna stavka održavanja sigurnosti sustava je i edukacija svih osoba koje se nalaze unutar njega. Edukacija daje osobama znanje koje će im pomoći da održe i svojim djelovanjem ne ugroze sigurnost organizacije.

4.1.3. Nepravilna implementacija

Nepravilna implementacija prema J.M. Kizza [15], najčešće nastaje spajanjem nekompatibilnih sučelja. Spajanjem ovakvih nekompatibilnih sučelja dovodi do mijenjanja sučelja na način da poveznice prema jednom ili drugom sučelju više neće djelovati na pravilan način ili će prestati raditi. Kompleksni sustavi sa mnogo raznih sučelja mogu predstavljati problem jer kod spajanja takvih sučelja može doći do nepravilne implementacije. Potrebno je provoditi kontrolu kompatibilnosti sučelja prije njihovog spajanja kako bi se izbjeglo stvaranje pogrešaka i ujedno i ranjivosti sustava. Kompleksnost sustava može direktno dovesti do nekompatibilnosti sučelja zbog postojanja previše podataka i detalja koje treba sagledati i poznavati, prilikom izrade i održavanja softvera za organizaciju zbog loše komunikacije između osoba koja rade na softveru, odabira softverskih proizvoda koji ne odgovaraju postojećim implementiranim softverima i slični problemi. Ukoliko hardverski i softverski proizvodi nisu korektno implementirani, tada se dovodi u opasnost funkcioniranje cijele računalne mreže, a s time i poslovanje organizacije koja sadrži takvu računalnu mrežu

4.1.4. Ranjivosti tehnologija povezanih s internetom

Korištenje interneta, koji je vrsta široko područne računalne mreže, u sklopu različitih društvenih okruženja, kao što su privatni život, poslovanje organizacija, akademsko okruženje, političko djelovanje i brojna druga, sve više i više raste što potiče konstantni napredak hardverske i softverske tehnologije. Ovakav brzi napredak ne prati u svim slučajevima i napredak znanja korisnika o tehnologijama što omogućava otvaranje novih oblika ranjivosti u ovom području. Mnogi korisnici nisu svjesni pogrešaka koje čine prilikom korištenja internetskih tehnologija, kao npr. pogreško implementiranje hardverskih uređaja i korištenje softvera na način da stvaraju ranjivosti koje omogućavaju osobama da zlonamjerno djeluju na računalnu mrežu koja je izložena. Ranjivosti koje potječu od hardvera je puno lakše otkloniti od onih nastalih kod softverskih tehnologija, a prema J.M. Kizza [15], najčešće ranjivosti koje nastaju kod softvera su ranjivosti koje utječu na funkcioniranje operacijskih sustava, ranjivosti koje su povezane s priključcima unutar računalne mreže (eng. port), ranjivosti koje nastaju kao rezultat postojanja pogrešaka unutar aplikacija i programa i ranjivosti unutar programa zaduženih za održavanje protokola sustava.

4.1.5. Razlike u ponašanju uljeza

Brzi razvoj softverskih i hardverskih tehnologija omogućava jednako brzi razvoj tehnologija za zlonamjerno djelovanje nad sustavima. Ovakve zlonamjerne tehnologije postaju sve jednostavnije za korištenje od stane osoba koje ne moraju posjedovati jako dobro znanje o sustavu kojeg žele oštetiti, a niti o tehnologiji koja služi za zlonamjerno djelovanje. Drugi problem brzog razvoja zlonamjernih tehnologija u skladu s brzim razvojem internetskih tehnologija je jednostavni pronalazak potrebnih tehnologija za zlonamjerno djelovanje na raznim izvorima unutar interneta. Jednostavnost korištenja i laka dostupnost omogućili su povećanje broja zlonamjernog djelovanja na računalne mreže i organizacije. J.M. Kizza [15] navodi kako je ovakav razvoj tehnologija doveo do sigurnosnih problema unutar organizacija jer timovi zaduženi za sigurnost teško prate sve novije trendove u napadima na sustav, i zbog toga je njihova brzina u reagiranju na napad i njegovo otklanjanje ili onemogućavanje usporena. Usporeno reagiranje na sigurnosne prijetnje sustava čine sustav ranjivim, jer uvijek postoji mogućnost da prijetnja prođe nezamijećena u moru novonastalih prijetnji s kojima se sigurnosni tim nije susreo ranije i nije siguran koja od prijetnji predstavlja veći rizik i koja ima prednost u otklanjanju. Ovakve nesigurnosti nisu dobrodošle u području sigurnosti i njihovo postojanje znači da prijetnje imaju mogućnost uzrokovanja štete unutar organizacije.

4.1.6. Poteškoće u popravljanju ranjivih mreža

Kompleksnost računalnih sustava i konstantni tehnološki napredak utječu na brzinu rješavanja problema unutar računalnih mreža. Česte promjene softverskih i hardverskih tehnologija koje se koriste unutar mreže otežavaju sigurnosnom timu da pravovremeno uoči i otkloni ranjivosti nastale unutar sustava. Prvi problem je što tim zadužen za sigurnost treba na vrijeme otkriti koje dijelovi računalne mreže predstavljaju ranjivost, a potom trebaju iz velikog broja novih tehnologija koje se brzo mijenjaju naći odgovarajuće rješenje za problem. Otkrivanje novonastalih ili starih ranjivosti otežava kompleksnost cjelokupne mreže kao i obujam zadataka koje sigurnosni tim treba odraditi uz otkrivanje ranjivosti. Otklanjanje ranjivosti je također zahtjevan posao jer je potrebno pronaći dobro hardversko ili softversko rješenje koje će u potpunosti otkloniti ranjivost, ali u isto vrijeme neće prouzročiti probleme povezane kompatibilnošću s drugim dijelovima računalnog sustava.

4.1.7. Ograničena djelotvornost reaktivnih rješenja

Dostupnost velikog broja zlonamjernih tehnologija u kombinaciji s jednostavnošću njihovog korištenja i stalnog napretka navedenih tehnologija zahtjeva kreiranje dovoljno dobrog rješenja za sprječavanje napada na računalne mreže. Prema J.M. Kizza [15], pronalazak efikasnog rješenja za određeni problem unutar velikog broja mogućih rješenja koji se nude i čiji broj raste uz napredak računalnih tehnologija, postaje težak zadatak za timove zadužene za sigurnost sustava. Doseg interneta i broj računala koja su spojena na njega raste uz minute u minutu, što stvara idealne uvijete za napade na organizacije i uređaje, jer vjerojatnost da svi uređaji prate trendove za osiguravanje sigurnosti i implementiraju ih, nije velika. Dostupnost interneta i povećanje spektra uloga u kojima se on koristi također otvara mogućnost za mnogobrojne i raznovrsne oblike napada, koji mogu prouzročiti velike štete na malim sustavima, ali i na sustavima koji su kritični za normalno funkcioniranje društva, kao što je npr. medicina.

4.1.8. Socijalni inženjering

Socijalni inženjering se, prema J.M. Kizza [15], koristi prije napada na sustav, na način da se manipulacijom i iskorištavanjem nesigurnosti dobivaju bitne sigurnosne informacije od strane osoba koje su članovi računalne mreže koju se želi napasti. Primjeri socijalnog inženjeringa su prijevare preko telefona, gdje se napadači predstavljaju kao službeno osoblje određenih institucija i time pokušavaju od osoba dobiti informacije, prijevare preko interneta, gdje se kroz ankete, lažne nagrade, formulare i na druge načine dolazi do informacija potrebnih za neovlašteni ulazak u sustav, prijevare kroz filtriranje smeća koje organizacije odbace i pronalazak bitnih informacija unutar njega, prijevare pomoću lažnog

predstavljanja kako bi se omogućio pristup tajnim informacijama i brojne druge strategije za zavaravanje stvarnih članova organizacija u svrhu dobivanja informacija ili pristupa informacijama.

4.2. Oblici prijetnja

Konstantni napredak tehnologija korištenih u računalnim mrežama, a time i napredak tehnologija korištenih u zlonamjerne svrhe, znači da raste broj mogućih prijetnji i vrste prijetnji kojima se mreže mogu izložiti. Prema J. Šehanović, Ž. Hutinski, M. Žugaj [9], većinu prijetnji je moguće klasificirati prema načinu na koji su one štetno djelovale na mrežu, i to u tri grupe: prijetnje koje su uzrokovale neautorizirano služenje informacijskim sadržajem, prijetnje koje su uzrokovale neidentificiranu promjenu informacijskog sadržaja i prijetnje koje su uzrokovale uništenje informacijskog sadržaja.

Prijetnje koje su uzrokovale neautorizirano služenje informacijskim sadržajem najčešće potječu od strane needuciranih osoba koje imaju pristup računalnoj mreži i na nenamjeran način proslijede podatke osobama koje nisu autorizirane. Ovakve prijetnje također uzrokuju osobe koje žele ostvariti neku vrstu dobiti u zauzvrat za prosljeđivanje podataka iz mreže ili prosljeđivanjem podataka koji su dio poslovne tajne žele počiniti osvetu.

Prijetnje koje uzrokuju neidentificirane promjene u podatkovnom sadržaju kojeg mreža posjeduje najčešće imaju kao motiv pad kvalitete poslovanja organizacije ili općenito onemogućavanje daljnjeg poslovanja.

Prijetnje koje uzrokuju uništenje informacijskog sadržaja su kao prvi zadatak najčešće imale prikupljanje informacija, ali zbog nemogućnosti prikupljanja sadržaja ili potrebe da sadržaj ne ostane u prvobitnoj računalnoj mreži, takav sadržaj uništavaju ili fizičkim putem sa uništavanjem fizičkih uređaja na kojima su se nalazili podaci, ili npr. kroz slanje virusa ili zlonamjernih softvera (eng. malware).

4.3. Izvori prijetnja

Izvori prijetnja računalnoj mreži govore od strane koga ili čega je nastala prijetnja računalnom sustavu. Prema J. Šehanović, Ž. Hutinski, M. Žugaj [9], izvore prijetnji računalnim mrežama moguće je grupirati i to u četiri grupe koje su redom: priroda i prirodne nepogode, čovjek s nenamjernim djelovanjem, čovjek s namjernim djelovanjem i tehničke pogreške.

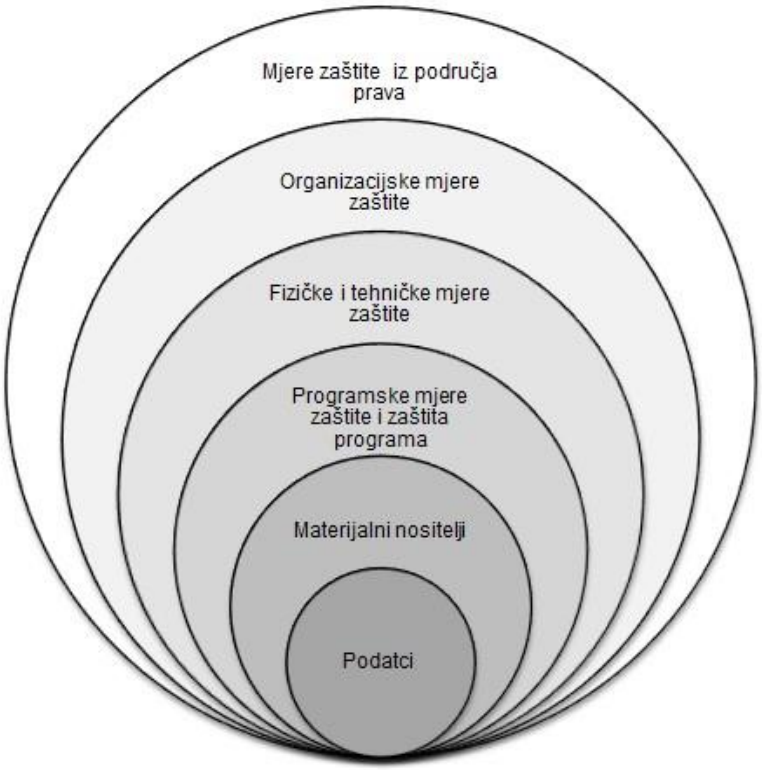
Prirodne nepogode je nemoguće spriječiti, ali je sustav moguće pripremiti kako bi se rizik od nastanka štete smanjio. Dobar primjer toga je ukoliko je poznato da na mjestu izgradnje zgrade, u kojoj se planiraju čuvati računala sa važnim informacijama, postoji velika vjerojatnost za poplavama, tada se takva računala ni u kojem slučaju neće postavljati u podrumske prostorije ili prostorije na niskim katovima koji bi bili izloženi vodi ukoliko bi došlo do poplave.

Čovjek i njegovo djelovanje predstavljaju najveći rizik za svaku računalnu mrežu i organizaciju. Kako bi se smanjio rizik za nastajanje prijetnji od strane nenamjernog ili namjernog djelovanja čovjeka, potrebno je osigurati dobru i pozitivnu radnu okolinu, poticajnu financijsku naknadu za rad, edukaciju i druge pogodnosti koje osiguravaju zadovoljstvo osobe, jer zadovoljni i educirani radnici predstavljaju puno manji rizik za računalnu mrežu od needuciranih radnika koji nenamjerno uzrokuju prijetnje ili nezadovoljnih radnika koji namjerno uzrokuju prijetnje mreži kako bi ostvarili dobit ili se osvetili za neko loše postupanje prema njima. Zlonamjerno djelovanje od strane osoba koje nemaju pristup mreži ili organizaciji može se smanjiti provođenjem sigurnosnih politika i kontroliranjem sigurnosti mreže.

Tehničke greške su prijetnje koje često nastaju u procesu izgradnje, održavanja ili izmjene računalnih mreža i praktično ih je nemoguće izbjeći, ali ukoliko postoji dobro upravljanje sigurnošću i tehničke strategije koje osiguravaju nesmetano djelovanje cijele mreže može se uvelike smanjiti rizik od posljedica ukoliko nastanu određene tehničke pogreške.

4.4. Mjere zaštite

Mjere zaštite služe za osiguranje nesmetanog funkcioniranja računalne mreže, a time i organizacija koje koriste računalnu mrežu. Mjere zaštite potrebno je prilagoditi onom dijelu mreže kojeg je potrebno zaštiti. Prema J. Šehanović, Ž. Hutinski, M. Žugaj [9], mjere zaštite moguće je grupirati prema području u kojem se one primjenjuju ili prema načinu na koje one djeluju, i tom metodom su oni naveli sljedeće metode za zaštitu: Mjere zaštite iz područja prava, organizacijske mjere zaštite, fizičke i tehničke mjere zaštite, programske mjere zaštite i zaštita programa i materijalni nositelji kao sredstvo zaštite podataka. Sve ove navedene mjere imaju važnu ulogu u pružanju zaštite za podatke koji se nalaze unutar mreže, i za koje je potrebno spriječiti neovlašteno dijeljenje, promjene nad njima i njihovo brisanje.



Slika 9: Mjere zaštite podataka (Prema: J. Šehanović, Ž. Hutinski, M. Žugaj, 2002)

Prilikom održavanja sigurnosti moguće je koristiti jedan ili više mjera zaštite, ovisno o tome što treba osigurati. Podatci koje organizacija posjeduje su njen najskupocjeniji i najznačajniji posjed, jer bez bitnih podataka je nemoguće osigurati nesmetano funkcioniranje organizacije, dok je njene druge elemente moguće na ovaj ili onaj način zamijeniti. Prema ovome podatci su temelje svake organizacije, a to je prikazano i slikom 9. Slikom 9 je predočena značajnost podataka, a ujedno i važnost da se pruži sigurnost materijalnim nositeljima podataka od strane svih dostupnih mjera zaštite, jer prema J. Šehanović, Ž. Hutinski, M. Žugaj [9], ukoliko podatci unutar organizacije ne postoje na nekom od materijalnih nositelja, tada su oni za nju trajno izgubljeni.

4.4.1. Materijalni nositelji kao sredstvo zaštite

Materijalni nositelji kao sredstvo zaštite imaju ulogu pohranjivanja i čuvanja podataka unutar organizacije. Ovisno o vrsti podataka i njihovoj značajnosti, potrebno je odabrati materijalni nositelj koji će svojim svojstvima odgovarati sigurnosnim zahtjevima za čuvanje određenih podataka. Materijalne nositelje moguće je grupirati u dvije grupe, i to: Materijalne nositelje analognog zapisa i materijalne nositelje digitalnog zapisa. Neki od analognih nositelja su papir, filmska vrpca i slični. Digitalne nositelje podataka je moguće podijeliti u

magnetske, a neki od njih su: diskete, vrpce i tvrdi disk, i optičke nositelje, u koje spadaju: DVD, CD i drugi.

4.4.2. Programske mjere zaštite i zaštita programa

Prema J. Šehanović, Ž. Hutinski, M. Žugaj [9], programske mjere zaštite i zaštitu programa je moguće podijeliti u šest kategorija, i to: mjere zaštite na razini operacijskog sustava, mjere zaštite na razini korisničke programske podrške, mjere zaštite sigurnosnog udvostručavanja sadržaja na drugim materijalnim nositeljima, mjere zaštite kriptiranja u mrežnoj komunikaciji, mjere zaštite od virusa i sličnih zlonamjernih softvera i mjere zaštite pomoću vatrozida (eng. firewall).

Mjere zaštite na razini operacijskog sustava se odnose na prepoznavanje raznih korisnika operacijskog sustava koje je potrebno međusobno odijeliti tako da se svaku pojedinu korisničku okolinu može zaštititi putem dodjeljivanja korisničkog imena i lozinke koji omogućavaju pristup skupu podataka za koje je korisnik autoriziran. Ovakvim mjerama se onemogućava pristup dijelovima operacijskog sustava osobama koje nisu ovlaštene za to.

Mjere zaštite na razini korisničke podrške omogućavaju podjelu operacijskog sustava na slojeve tako da je prilikom pristupa nekom od korisničkog programa na određenom sloju potrebno unijeti traženu lozinku za pristup korisničkom programu. Najlakši primjer ove mjere zaštite je podijeljene mogućnosti prilikom rada s podatcima, tj. za pregled, kreiranje novih, izmjenjivanje i brisanje postojećih postoje različite lozinke i ograničenja pristupa, tako da je s određenom lozinkom za pristup moguć samo pregled podataka, dok neka druga lozinka omogućava izmjenu tih podataka.

Mjere zaštite sigurnosnog udvostručavanja sadržaja na drugim materijalnim nositeljima imaju ulogu, kao što i samo ime govori, kopiranja određenog sadržaja tako da se on ne nalazi samo na jednom materijalnom nositelju. Postojanje podataka na samo jednom materijalnom nositelju predstavlja rizik za organizaciju, jer ukoliko ti nositelji prestanu postojati iz bilo kojeg razloga, tada organizacija trajno ostaje bez podataka. Spremljene podatke moguće je kopirati na način da se svi postojeći podaci kopiraju na nekoliko nositelja, na način da se kopiraju samo podaci koji su promijenjeni od zadnjeg kopiranja i koji su označeni kao oni koji se trebaju kopirati, i na način da se kopiraju samo podaci označeni kao potrebni za kopiranje. Što podaci imaju veću važnost za organizaciju, njihovo kopiranje bi se trebalo češće raditi i na više materijalnih nositelja, a podaci koji su dio poslovne tajne se često čuvaju i u papirnatom obliku jer je do njega teže doći zlonamjernim djelovanjem na računalne mreže.

Mjere zaštite kriptiranja u mrežnoj komunikaciji osiguravaju komunikacijske veze između članova računalne mreže, tj. osiguravaju neometani prijenos podataka između članova računalne mreže. Kriptografija je prema T. English [16], znanost čiji je zadatak osiguravanje podataka prilikom razmjene ili pohranjivanja. T. English [16] također napominje da je kriptiranje proces u kojem se izvodi promjena podataka na način da oni više nisu čitljivi kako bi se osigurala njihova sigurnost prilikom razmijene unutar računalne mreže. Takve promijenjene podatke je potrebno prilikom njihovog primanja dekriptirati kako bi njihov sadržaj opet bio čitljiv.

Mjere zaštite od virusa i sličnih zlonamjernih softvera imaju zadatak sprječavanja ulaska zlonamjernih softvera u računalnu mrežu organizacije i otklanjanje zlonamjernih softvera, koji su uspjeli uči u sustav, i štete koju su počinili. Brzi razvoj softverskih i hardverskih tehnologija prati i brzi razvoj raznih zlonamjernih tehnologija, zbog čega zaštita od njihovog djelovanja ima veliku ulogu u osiguranju sveukupne sigurnost organizacija. Kao prevenciju potrebno je provoditi edukaciju članova organizacije kako ne bi ugrozili sustav unosom materijalnih nositelja podataka koji sadrže skrivene zlonamjerne programe ili putem komunikacije kroz Internet, kao što je elektronska pošta. Osim toga potrebno je kontrolirati i nadzirati rad programa unutar sustava, podatke spremljene unutar mreže i promjene nad njima i komunikaciju između članova mreže. Ukoliko je već uočeno da unutar sustava postoji program koji obavlja zlonamjerne aktivnosti, potrebno je otkloniti sve uređaje unutar mreže na kojima je pronađeni zlonamjerni program kako bi se onemogućilo njegovo daljnje širenje kroz mrežu, a nakon toga potrebno je kroz razne alate otkloniti zlonamjerne programe i potom vratiti računalnu mrežu u stanje u kakvom je bila prije napada, što olakšavaju kopije podataka koje su postojale na više mjesta i time nisu bile ugrožene napadom.

Mjere zaštite pomoću vatrozida (eng. firewall) omogućavaju sigurnu komunikaciju između članova računalne mreže i uređaja koji se nalaze na nekoj drugoj mreži, kao što je npr. Internet. Prema E. Dosal [17], uloga vatrozida je da onemogući sve zlonamjerne podatke, programe ili poruke da uđu unutar mreže i da omogući nesmetani protok provjerenih podataka.

4.4.3. Fizičke i tehničke mjere zaštite

Fizičke i tehničke mjere zaštite se koriste kako bi se podatci i softverski i hardverski dijelovi mreže osigurali od fizičkih prijetnji kao što su prijetnje nastale od strane prirodnih nepogoda, npr. potresi, poplave, udari groma, požari i slično, od strane zlonamjernog fizičkog djelovanja od strane čovjeka, kao što su krađe i uništavanje fizičkim putem. Ovakve mjere najčešće uključuju sefove, razne alarme, npr. protupožarne i protuprovalne, zapošljavanje osoba zaduženih za fizičko osiguranje i slične metode. Fizičke i tehničke mjere zaštite imaju

zadatak osigurati ne samo podatke i softverske i hardverske dijelove, već i građevine u kojima se nalaze dijelovi računalne mreže osiguranjem okoline zgrade i njezine unutrašnjosti.

4.4.4. Organizacijske mjere zaštite

Organizacijske mjere zaštite su važne za pravilno funkcioniranje cjelokupne organizacije i one unutar pravilnika o sigurnosti i ostalih mjera, dokumenata i standarda osiguravaju svaku od organizacijskih jedinica i softverske, hardverske i podatkovne resurse koje ta organizacijska cjelina posjeduje. Zbog specifičnog poslovanja kojem se bave pojedine organizacije, organizacijske mjere zaštite je potrebno prilagoditi željenom sustavu, i time one nisu u cjelini pogodne za neku drugu organizaciju. Tako će se organizacijske mjere zaštite razlikovati od organizacijske jedinice do organizacijske jedinice unutar iste organizacije, i između dvije različite organizacije, npr. unutar organizacije nisu ista pravila za osiguranje financijske organizacijske jedinice i proizvodne organizacijske jedinice.

4.4.5. Mjere zaštite iz područja prava

Organizacije koje žele legalno djelovati moraju poštivati sve zakone, norme i regulative koje propisuje zemlja unutar koje one posluju, a ukoliko posluju i izvan zemlje u kojoj se nalaze, tada trebaju poštivati i pravila ostalih zemalja unutar kojih obavljaju poslovanje ili razmjenu podataka i resursa. Prema J. Šehanović, Ž. Hutinski, M. Žugaj [9], mjere zaštite iz područja prava obvezuju organizaciju da poštuje sve pravne norme donesene od strane države unutar koje djeluju, i koja predstavlja pravni okvir za ostvarivanje mjera zaštite.

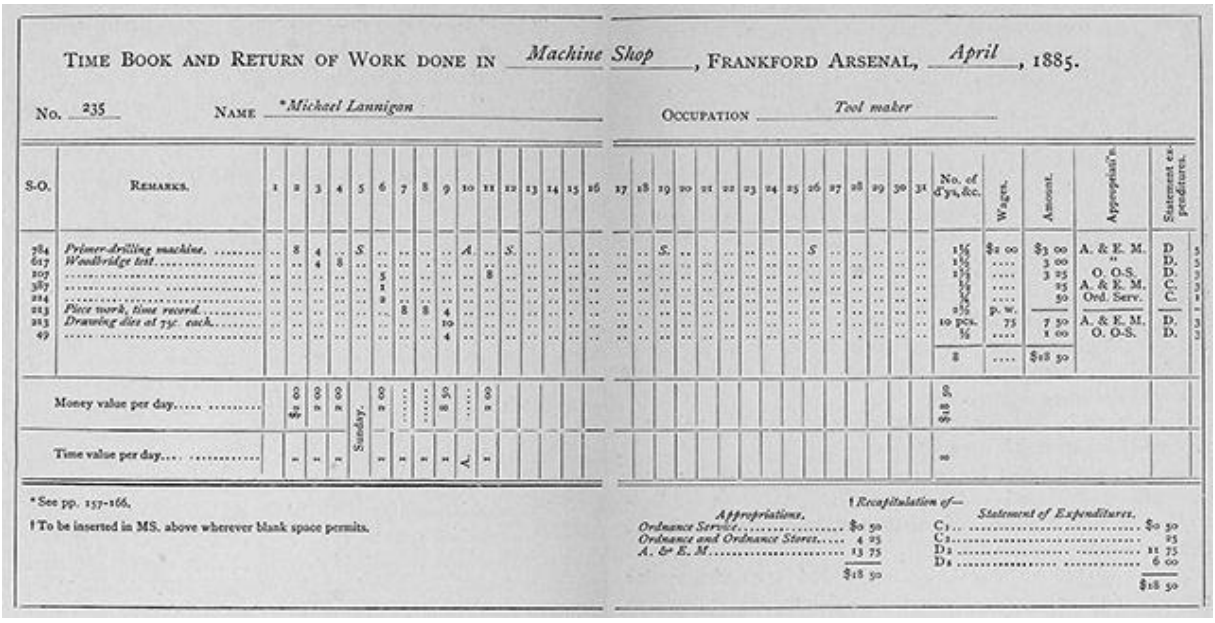
5. Mjerenje aktivnosti korisnika na krajnjem uređaju

Mjerenje aktivnosti korisnika na krajnjem uređaju se u današnje vrijeme koristi za postizanje različitih ciljeva. Mjerenje se može izvoditi kako bi se osigurala sigurnost podataka neke organizacije, kako bi se zaštitile maloljetne osobe prilikom korištenja interneta, kako bi se prikupili podaci o ponašanju korisnika na internetu i slično.

Mjerenje aktivnosti korisnika na krajnjem uređaju se unutar organizacija najčešće koristi kako bi se poslovni podaci zaštitili od neovlaštenog čitanja, mijenjanja, razmjene i brisanja, kako bi se kontroliralo pridržavaju li se zaposlenici sigurnosnih politika organizacija i općenito kako bi se spriječio nastanak prijetnji i ranjivosti unutar organizacije koje nastaju djelovanjem čovjeka.

5.1. Povijest mjerenja aktivnosti korisnika

Prvi povijesni oblik mjerenja aktivnosti korisnika bilo je mjerenje vremena kojeg su zaposlenici proveli za vrijeme obavljanja nekog posla. Prema A. Cote [19], radni list (eng. timesheet) se prvi put počeo koristiti u 19. stoljeću i na njemu su se upisivali podaci o izvršenim zadatcima, radnim danima, radnim satima i sličnim informacijama.


TIME BOOK AND RETURN OF WORK DONE IN *Machine Shop*, FRANKFORD ARSENAL, *April*, 1885.

No. 235 NAME **Michael Lannigan* OCCUPATION *Tool maker*

S-O.	REMARKS.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	No. of d'ys, &c.	Wages.	Amount.	Appropriat'n.	Statement ex-penditures.
384	*Primer-drilling machine.*	..	8	4	..	*S.*	..	..	..	..	*A.*	..	*S.*	..	..	..	..	..	..	*S.*	..	..	..	..	..	..	*S*	..	..	..	..	..	1½	$2 00	$3 00	A. & E. M.	D.
617	*Woodbridge test*	..	..	4	8	..	..	..	..	..	..	..	8	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	1½	....	3 00	"	D.
207	.....	..	..	..	..	..	5	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	1¼	....	3 75	O. O.S.	D.
387	.....	..	..	..	..	..	1	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	½	....	25	A. & E. M.	C.
214	.....	..	..	..	..	..	2	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	½	....	50	Ord. Serv.	C.
213	*Piece work, time record.*	..	..	..	..	..	..	8	8	4	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	2½	p. w.			
213	*Drawing dies at 75c. each*	..	..	..	..	..	..	..	..	10	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	10 pcs.	75	7 50	A. & E. M.	D.
49	.....	..	..	..	..	..	..	..	..	4	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	½	....	1 00	O. O.S.	D.
																																	8	....	$18 50		
	Money value per day.....		$2 00	00	00	Sunday.	00	.....	.....	50	.....	00																					$18 50				
	Time value per day.....		"	"	"		"	"	"	"	A.	"																					"				

* See pp. 157-166.

† To be inserted in MS. above wherever blank space permits.

†Recapitulation of—

Appropriations.	
Ordnance Service	$0 50
Ordnance and Ordnance Stores	4 25
A. & E. M.	13 75
	$18 50

Statement of Expenditures.	
C1	$0 50
C2	25
D2	11 75
D4	6 00
	$18 50

Slika 10: Radni list [19]

Slika 10 prikazuje radni list koji se koristio prilikom bilježenja radnih sati zaposlenika unutar organizacije. Radni listovi su se koristili kao dokaz o obavljenom radu i kao smjernica

u izračunavanju zasluženih plaća. Ovakvo bilježenje podataka o obavljenom radu je omogućilo i bolje vremensko raspoređivanje rada ovisno o težini zadatka kojeg treba napraviti i o broju radnih sati koje su radnici napravili do tada.

5.2. Metode mjerenja aktivnosti korisnika

Danas proces mjerenja aktivnosti korisnika na krajnjem uređaju uključuje široki spektar mogućih područja mjerenja i brojnih mjerila za svako od odabranih područja. Potencijalna područja iz kojih se mjere aktivnostima korisnika su aktivnosti u sustavu, na računalnoj mreži, prilikom korištenja aplikacija, ponašanje prilikom korištenja interneta, pristup podatcima na diskovima i brojna druga. Može se reći da mjerenje aktivnosti korisnika uključuje i praćenje korisnika za vrijeme dok je on unutar zgrade organizacije, što može značiti praćenje načina na koje zaposlenik koristi internet, kako i koje aplikacije koristi, koju elektronsku poštu prima i šalje, praćenje i spremanje telefonskih poziva, video nadzor, praćenje lokacije zaposlenika putem elektronskih kartica zaduženih za omogućavanje ulaska u određene prostore i druge metode.

Postoji više metoda koje se koriste prilikom mjerenja aktivnosti korisnika na krajnjem uređaju i služe za praćenje i kontroliranje aktivnosti korisnika. N. Lord [20] naveo je šest metoda za dobivanje podataka o aktivnostima korisnika na krajnjem uređaju, i to redom: snimanje sesija, kolekcije dnevnika (eng. log) i njihova analiza, pregled mrežnih paketa, spremanje zapisa sa tipkovnice (eng. keystroke logging), praćenje jezgre i uzimanje snimki zaslona (eng. screenshot) i snimki datoteka.

5.2.1. Snimanje sesija

Pojam sesije u informatičkom smislu označava neki vremenski period u kojemu se uspostavlja i odvija komunikacija između uređaja, sustava ili dijelova sustava. Sesije mogu pokrenuti sami uređaji i sustavi ili korisnik navedenih uređaja ili sustava. Snimanjem sesija se dobiva zapis uspostavljenih sesija sa uređajima ili sustavima od strane korisnika. Snimanje sesija podrazumijeva korištenje softverskog rješenja koje će zabilježiti i spremiti sesije koje korisnik pokreće. Pomoću snimanja sesija moguće je vidjeti način na koji korisnici koriste web stranice bilježenjem raznih pokreta miša, vidjeti koje web stranice su posjećivali, zabilježiti koje zaslone su korisnici otvarali na radnoj površini (eng. desktop), promatrati kako su korisnici koristili aplikacije i brojne druge aktivnosti koje su korisnici direktno izvodili korištenjem tipkovnice, miša, mikrofona, zaslona na dodir i drugih uređaja za rad sa krajnjim uređajima.

5.2.2. Kolekcije dnevnika i njihova analiza

Dnevnik (eng. log) je zapis kojeg kreiraju krajnji uređaji, operacijski sustavi, aplikacije i drugi objekti. Prema sumo logic [21], dnevnik se sastoji od nekolicine poruka koje su vremenski poredane i koje opisuju aktivnosti koje se događaju unutar sustava koji je kreirao dnevnik. Sumo logic [21] napominje kako je potrebno prikupljati dnevnike sustava, dnevnike mreže računala, tehničke dnevnike i dnevnike povezane sa kontrolom sigurnosti. Analiza dnevnika predstavlja postupak u kojemu se prikupljeni dnevnici čitaju, a podatci prikupljeni unutar njih analiziraju, a prilikom analize dnevnika potrebno je uočiti uzorke i nepravilnosti, potrebno je urediti podatke unutar dnevnika tako da budu istog formata i potrebno je dnevnike iz različitih izvora grupirati po kategorijama kako bi se lakše interpretiralo njihovo značenje.

5.2.3. Pregled mrežnih paketa

Prema C. Brook [22], prilikom pregleda mrežnih paketa potrebno je kontrolirati podatkovni dio paketa i zaglavlje paketa koji je prošao kroz kontrolnu točku unutar računalne mreže. Ovim postupkom kontroliranja sadržaja paketa koji se šalju mrežom izbacuju se paketi koji predstavljaju rizik, tj. koji nisu usklađeni sa protokolima za slanje paketa, koji predstavljaju neželjenu poštu, koji sadrže virus u podacima koje prenose, koji neovlašteno ulaze u prostor računalne mreže i bilo koji drugi paket koji nije u skladu sa sigurnosnim politikama, pravilima i strategijama koje su određeni za računalnu mrežu koja se kontrolira. Pregled računalnih mreža je zadužen i da prekidanje slanja neželjenih paketa ili njihovo preusmjeravanje.

5.2.4. Spremanje zapisa sa tipkovnice

Spremanje zapisa sa tipkovnice (eng. keystroke logging) je metoda čije ime opisuje način na koji se ona koristi. Ova metoda mjerenja aktivnosti korisnika na krajnjem uređaju radi na principu praćenja i spremanja svakog dodira na tipku tipkovnice kojeg je korisnik napravio. Prema stranici kaspersky [23], prilikom spremanja zapisa sa tipkovnice spremaju se podatci o dužini pritiska na tipku, vremenu kada je tipka pritisnuta, brzina kojom je tipka pritisnuta i ime tipke koja je pritisnuta. Prikupljanjem ovih podataka moguće je u potpunosti prisluškivati razgovore koje osoba koju se prati vodi i pratiti sve podatke i informacije koje osoba unosi putem tipkovnice. Alati koji služe za prikupljanje zapisa sa tipkovnica nazivaju se keyloggeri (eng. keylogger) i oni mogu biti softverski programi ili hardverski uređaji.

5.2.5. Praćenje jezgre operacijskog sustava

Jezgra operacijskog sustava (eng. kernel) predstavlja softversko središte uređaja čiji je ona dio. Jezgra je zaslužena za kontroliranje rada diskovnog sustava, memorije i drugih dijelova operacijskog sustava. Prema AfterAcademy [24], jezgra operacijskog sustava ima četiri uloge. Prva uloga je povezivanje korisnika i resurse sustava, a jezgra to može izvesti zato što ima pristup resursima računala, kao što su procesor, izlazno/ulazni uređaji, mrežni uređaji i drugi. Druga uloga jezgre je da resurse kojima ima pristup ravnomjerno rasporedi između postojećih procesa, tako da svaki proces dobije dio resursa koji mu je potreban. Treća uloga jezgre sustava je alokacija i dealokacija memorije kako bi procesi sustava mogli koristiti dobiveni memorijski prostor. Posljednja uloga koju jezgra ima je raspored svih uređaja koji su spojeni sa sustavom i korišteni od strane određenih procesa.

5.2.6. Uzimanje snimki zaslona i datoteka

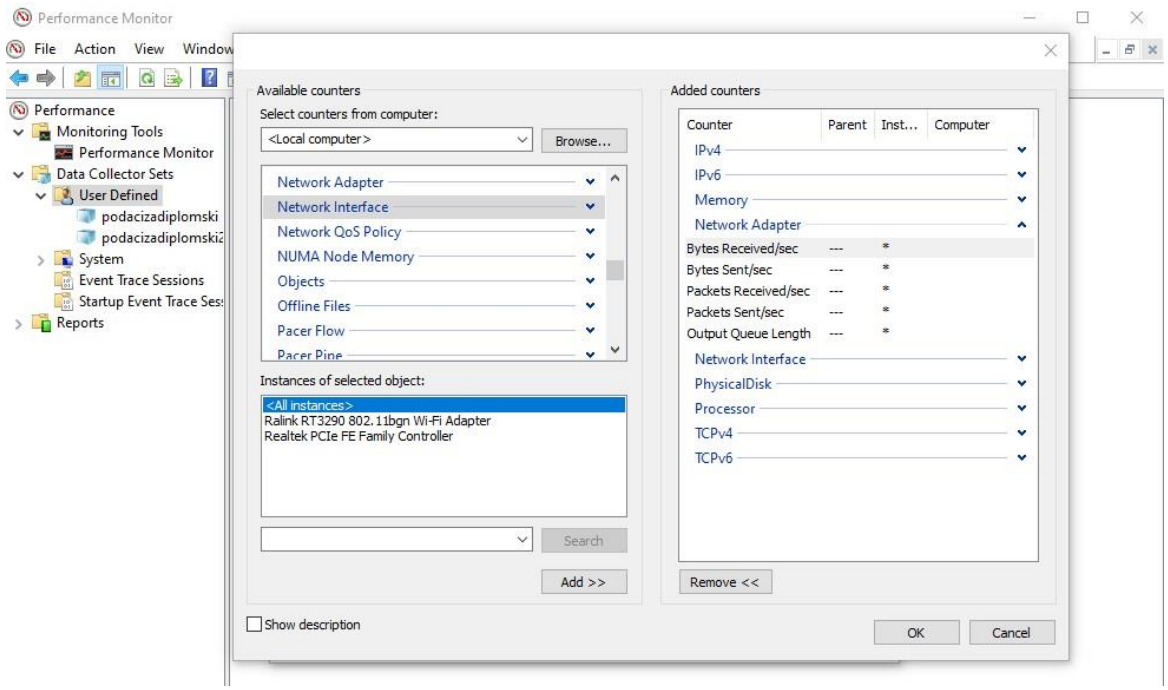
Snimke zaslona (eng. screenshot) je najlakše opisati kao spremanje trenutnog stanja zaslona uređaja u obliku slike, videa, ili nekog sličnog medija. Prema J. Simonu [25], postoji četiri vrste snimke zaslona, i to su redom nabrojane: slika zaslona, snimka zaslona, animirana slika gif formata i odljev zaslona. Slika zaslona (eng. screenshot) se dobiva uzimanjem jedne slike zaslona uređaja i spremanjem iste u obliku slikovne datoteke. Snimka zaslona (eng. screen capture) se od slike zaslona razlikuje u tome što može uhvatiti cijelo stanje zaslona uređaja, npr. ukoliko se na uređaju prikaže web stranica, slika zaslona će uhvatiti samo onaj dio web stranice koji je stao unutar zaslona, dok će snimka zaslona uhvatiti cijeli izgled web stranice koji se nije mogao odjednom vidjeti na ekranu već je bilo potrebno pomoću gumba za pomicanje pomaknuti web stranicu kako bi se vidio drugi dio nje. Animirana slika GIF formata (eng. animated GIF) prikazuje niz spremljenih slika zaslona u animiranom obliku, dok odljev zaslona (eng. screencast) predstavlja trenutno stanje zaslona uređaja spremljeno u video obliku. Svi oblici snimki zaslona pomažu prilikom uočavanja i zabilježavanja aktivnosti koje korisnik izvodi prilikom korištenja uređaja.

6. Primjer mjerenja aktivnosti korisnika

Ovo poglavlje biti će orijentirano na praktični dio rada. Prvi dio poglavlja će opisivati način prikupljanja podataka o aktivnostima korisnika na krajnjem uređaju. Drugi dio poglavlja će prikazati način na koji su dobiveni podaci uredili za daljnje korištenje. U trećem poglavlju će biti pokazan proces izrade baze podataka na temelju dobivenih podataka, a posljednji dio poglavlja će sadržavati analizu dobivenih podataka o aktivnosti korisnika na krajnjem uređaju. Potrebno je napomenuti da je korisnik o čijim aktivnostima su se prikupljali podatci autor ovog rada, dok je krajnji uređaj na kojemu su se izvodile i bilježile aktivnosti prijenosno stolno računalo u posjedu autora rada.

6.1. Prikupljanje podataka

Unutar ovog rada prikupljali su se podatci o stanju resursa sustava. Oni su prikupljeni uz pomoć programa Performance Monitor. Unutar programa bilo je potrebno kreirati set podataka (eng. data collector set). Nakon toga je trebalo odabrati koju vrstu podataka će se prikupljati, gdje se moglo birati između brojača/mjeritelj performansi, praćenju podataka o događajima i informacija o sustavskim konfiguracijama, a u slučaju ovog rada je odabran brojač performansi. Prvi korak kod odabira mjeritelja performansi bio je odabir vremenskog intervala u kojem će se mjeriti performanse, a nakon toga je trebalo dodati željene mjeritelje performansi.



Slika 11: Odabir mjeritelja performansi

Slika 11 prikazuje korak u Performance Monitor programu gdje je bilo potrebno unutar kategorija za koje se mjere performanse odabrati željene mjeritelje performansi. Kategorije za mjerenje i mjeritelji performansi koji su odabrani u sklopu ovog rada su nabrojani i objašnjeni u potpoglavljima 6.1.1, 6.1.2, 6.1.3 i 6.1.4. Drugi korak nakon odabira mjeritelja performansi je odabir formata zapisa podataka, a u slučaju ovog projekta je odabran format SQL. Nakon odabira svih željenih mjeritelja performansi i kreiranja seta podataka, potrebno je unutar glavnog izbornika programa Performance Monitor odabrati željeni kreirani set podataka i pokrenuti ga kako bi započelo prikupljanje podataka. Kada prođe određeni vremenski period u kojemu su se htjele mjerili performanse potrebno je stopirati ranije pokrenuti set podataka. Kreiranjem seta podataka unutar ovog programa kreirale su se i potrebne tablice unutar baze podataka koja je odabrana u koracima unutar potpoglavlja Izrada baze podataka.

6.1.1. Korištenje procesora

Prvi skup podataka koji je dobiven prilikom mjerenja aktivnosti korisnika na krajnjem uređaju je vezan uz podatke koji se tiču rada i korištenja procesora (eng. central processing unit ili skraćeno processor ili CPU). Procesor je dio računala koji prema N. K. Kottayil[18], obrađuje većinu uputa od strane aplikacija i hardverskih sklopova, kontrolira razmjenu podataka između različitih dijelova računala i izvršava obradu podataka. Praćenje rada i korištenja procesora je bitno za uvid u cjelokupno stanje uređaja i može ukazati na probleme povezane sa hardverskim ili softverskim dijelovima računala koji mogu utjecati na sposobnost procesora da efikasno obavlja potrebne zadatke. Prilikom prikupljanja podataka o aktivnosti korisnika na računalu odabrani su sljedeći mjeritelji performansi o radu procesora: %Privileged Time, %User Time, Interrupts/sec, %Processor Time i DPCs Queued/sec.

„%Privileged Time“ je mjeritelj performansi koji daje postotak vremena u kojemu je procesor izvršavao dretve (eng. thread) koje su koristile privilegiran način rada, tj. radile su sa podacima koji su dio resursa sustava, kao što su hardverski dijelovi i memorija, a takav rad naziva se još i način rada s jezgrom (eng. kernel mode). Ukoliko je ovaj mjeritelj većinu vremena u rasponu većem od 25% - 30% to znači da postoji problem u hardverskim dijelovima računala ili problem sa programima koji služe za korištenje određenih hardverskih dijelova (eng. driver).

„%User Time“ je mjeritelj performansi koji daje postotak vremena u kojemu je procesor izvršavao dretve (eng. thread) koje su koristile korisnički način rada, ili drugim riječima, postotak vremena u kojemu je procesor izvršavao kodove koji su dio korisničkih aplikacija. Vrijednosti ovog mjeritelja trebale bi biti ispod raspona vrijednosti od 60%-65%

kako bi procesor imao dovoljno vremena za privilegiran način rada ili za obavljanje zadataka koji ne spadaju niti u korisnički način rada niti u način rada sa jezgrom. Ukoliko ovaj mjeritelj često pokazuje vrijednosti iznad 65% tada je potrebno provjeriti koje aplikacije i procesi koriste procesor.

„Interrupts/sec“ je mjeritelj performansi koji prikazuje broj dobivenih i obrađenih prekida od strane hardvera. Ovim mjeriteljem moguće je promatrati rad uređaja, kao što su: miš, tipkovnica, programi za korištenje hardverskih uređaja (eng. driver), tvrdi disk (eng. hard disk) i drugi, jer prekidi kreiraju hardverske komponente kada izvrše neki zadatak ili zahtijevaju pozornost od strane procesora. Normalni broj prekida u sekundi ovisi o procesoru, broju mrežnih paketa i broju ulaznih i izlaznih operacija sa diska. Kod današnjih procesora normalno je da postoji do 1000 prekida unutar sekunde. Ukoliko je taj broj veći i računalo funkcionira na neuobičajeni način, to je znak da postoji problem sa hardverom i potrebno je proučiti koji uređaji ili programi stvaraju ove prekide.

„%Processor Time“ je mjeritelj performansi koji postotak vremena u kojemu je procesor radio sa dretvama i rješavao poslane zahtjeve. Kada procesor ne obavlja neki od ovih zadataka tada izvodi praznu dretvu, a to vrijeme se ne pribraja mjeritelju %Processor Time. Preporučeno je da vrijednost ovog mjeritelja u većini slučajeva ne prelazi 80%. Ukoliko je ovaj postotak često viši od 80% tada je potrebno provjeriti vrijednosti mjeritelja povezanih s korištenjem diskovnog sustava i mrežnih resursa, a ako su te vrijednosti u povoljnom rangu, tada se kod procesora radi o problemu uskog grla (eng bottleneck), što znači da on nije dovoljno brz za obavljanje traženih zadataka.

„DPCs Queued/sec“ mjeritelj performansi pokazuje broj DPC (eng. deferred procedure call) objekata koji su dodani u procesorov DPC red čekanja. DPC objekti se koriste prilikom rada s prekidima od strane hardvera i pomažu prilikom selekcije prekida na temelju važnosti, tako da se prekidi manje važnosti rješavaju od strane DPC objekata, dok prekide više važnosti rješava procesor direktno.

6.1.2. Korištenje memorije

Drugi skup podataka koji je dobiven prilikom mjerenja aktivnosti korisnika na računalu se tiče podataka vezanih uz korištenje memorije. Memorija predstavlja kratkotrajno pohranjivanje podataka unutar sustava, a problemi koji se mogu pojaviti kod memorije se najčešće otkrivaju pomoću informacija o nedostatku memorije koje procesi dobivaju za izvođenje i dokaza da je sustav došao do granice i više nema mogućnost dodjeljivanja memorije. Za ovu kategoriju podataka odabrani su sljedeći mjeritelji performansi.

„Available MBytes“ mjeritelj performansi prikazuje ukupni broj dostupne memorije u sustavu. Potrebno je odrediti minimalnu veličinu memorije potrebne za izvođenje procesa i ukoliko je količina dostupnih megabitova manja od minimuma potrebno je provjeriti koji procesi koriste memoriju.

„Pages/sec“ mjeritelj performansi pokazuje u kojoj mjeri se izvršava čitanje sa diska ili pisanje po disku u svrhu rješavanja problema tvrdih stranica (eng. hard page), tj. problema koji nastaju kada aplikacije pokušavaju koristiti dodijeljene stranice memoriju ali ju ne mogu pronaći na disku. Ukoliko ovaj mjeritelj pokazuje visoke brojeve potrebno je pronaći aplikacije koje koriste velike količine memorije.

„Page Reads/sec“ mjeritelj performansi pokazuje u kojoj mjeri se izvršava čitanje nad diskom u svrhu rješavanja problema pronalaska stranice u memoriji.

„Page Writes/sec“ mjeritelj performansi pokazuje u kojoj mjeri se izvodi pisanje po disku u svrhu rješavanja problema tvrdih stranica. Za mjerila „Pages/sec“, „Page Reads/sec“ i „Page Writes/sec“ je poželjno da izmjerene vrijednosti budu što manje.

6.1.3. Korištenje diskovnog sustava

Treći skup podataka dobiven prilikom mjerenja aktivnosti korisnika na uređaju je vezan uz podatke o korištenju diskovnog sustava. Diskovni sustav predstavlja glavno spremište podataka unutar uređaja u dugotrajnom obliku. Unutar ove kategorije prikupljeni su podaci temeljem sljedećih mjeritelja performansi.

„Avg. Disk Queue Length“ mjeritelj performansi prikazuje prosječnu dobivenu vrijednost o broju zahtjeva za čitanje i pisanje po disku koju su bili stavljeni na čekanje u odabranom periodu. Ukoliko je vrijednost ovog mjeritelja veća od 2 za svaki tvrdi disk, tada potencijalno može doći do problema uskog grla (eng. bottleneck).

„%Idle Time“ mjeritelj performansi prikazuje postotak vremena u kojemu nije bilo neriješenih zahtjeva od strane operacijskog sustava za diskovni sustav. Teži se da su vrijednosti ovog mjeritelja što veće, a postoji iznimka za manje vrijednosti ukoliko uz njih vrijedi da vrijednost mjeritelja „Avg. Disk Queue Length“ nije veća od 2. Konstantne niske vrijednosti ovog mjeritelja ukazuju na moguće povećanje aktivnosti na diskovima, dostizanje granice u mogućnostima korištenja diskova, kvar na diskovima ili lošu konfiguraciju diskova, i stoga je potrebno detaljnije pregledati diskove kako bi se otkrio i uklonio problem.

„Avg. Disk sec/Read“ mjeritelj performansi pokazuje prosječnu vremensku vrijednost potrebnu za izvršavanje naredbe čitanja sa diska. Vrijednosti ovog mjeritelja ovise o brzini kojom disk može raditi i da bi se otkrilo jesu li vrijednosti niske ili visoke za određeni disk

potrebno je prvo napraviti baznu vrijednost prilikom implementacije diska s kojom će se kasnije uspoređivati sve ostale dobivene vrijednosti.

„Avg. Disk sec/Write“ mjeritelj performansi pokazuje prosječnu vremensku vrijednost potrebnu za izvršavanje zadataka vezanih uz pisanje po disku. Kao i kod mjeritelja „Avg. Disk sec/Read“, potrebno je dobiti baznu vrijednost po kojoj će se uspoređivati kasnije dobivene vrijednosti u svrhu određivanja njihove brzine ili sporosti.

„Disk Reads/sec“ je mjeritelj performansi koji bilježi ukupan broj izlaznih zahtjeva (eng. output requests) koje disk izvrši u sekundi. Interpretacija vrijednosti ovog mjeritelja ovisi o dobivenim baznim vrijednostima o izvršavanju izlaznih zahtjeva od strane diskova.

„Disk Writes/sec“ mjeritelj performansi bilježi ukupan broj ulaznih zahtjeva (eng. input requests) koje disk izvrši u sekundi. Kao i kod mjeritelja „Disk Reads/sec“, interpretacija dobivenih vrijednosti ovisi o uzetim baznim vrijednostima koje se potom uspoređuju s kasnije dobivenim vrijednostima.

6.1.4. Korištenje mrežnih resursa

Četvrti skup podataka dobiven prilikom mjerenja aktivnosti korisnika na krajnjem uređaju je vezan uz korištenje mrežnih resursa. Mrežni resursi predstavljaju sve podatke i uređaje kojima mogu pristupit uređaji koji se nalaze unutar mreže i između kojih postoji komunikacijska veza. Od svih mrežnih resursa u ovom radu su za mjerenje odabrani Internet protokol, TCP protokol, mrežni adapter i mrežno sučelje. Za svaki od ovih mrežnih resursa odabrani su sljedeći mjeritelji performansi pomoću kojih su se prikupljali podaci o aktivnostima korisnika.

Internet protokol četvrte verzije ili skraćeno IPv4 definira i omogućava povezivanje računalnih mreža putem interneta. Internet protokol verzije 6 ili skraćeno IPv6, je novija verzija protokola za povezivanje mreža na Internet i on omogućava identifikaciju i lokaciju uređaja unutar mreže. Za prikupljanje podataka u vezi IPv4 i IPv6 su korištena dva mjeritelja performansi. Prvi mjeritelj je „Datagrams Received/sec“ i on pokazuje u kojem broju su IP datagrami dobiveni od strane mrežnog sučelja. Drugi mjeritelj je „Datagrams Sent/sec“ koji služi za mjerenje broja poslanih datagrama. Iznenadna povećanja kod bilo kojeg od ova dva mjeritelja ukazuje na mogućnost postojanja uljeza unutar mreže.

TCP protokol, gdje se skraćenica TCP dobiva od engleskog naziva „Transmission Control Protocol“, zajedno sa IP protokolom čini IP grupu protokola. TCP protokol omogućava sigurno, pouzdano i provjereno slanje podataka kroz mrežu koja koristi internet protokol za komunikaciju između uređaja. Ovisno o verziji Internet protokola unutar grupe protokola se koristi i verzija TCP protokola, pa tako postoji TCPv4 i TCPv6. Za obije verzije

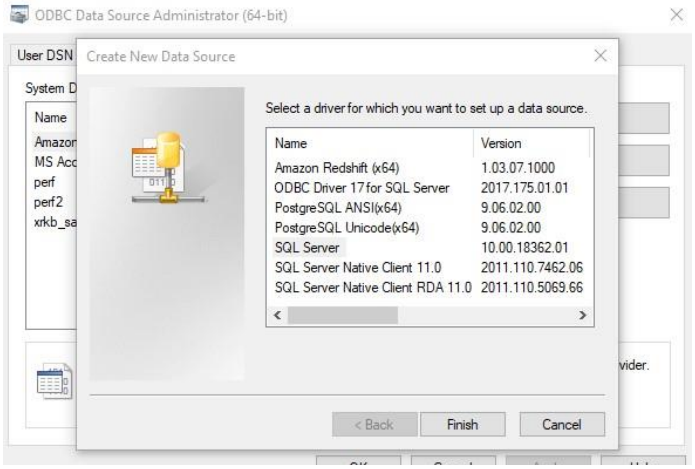
TCP protokola se prilikom prikupljanja podataka koristila tri mjeritelja performansi. Prvi mjeritelj koji se koristilo je „Segments Received/sec“, koji je dao prosječni broj TCP segmenata primljenih preko uspostavljenih veza, unutar određenog vremenskog perioda. „Segments Sent/sec“ je drugi mjeritelj koji se promatrao i koji daje prosječni broj TCP segmenata poslanih, preko uspostavljenih veza, unutar određenog vremenskog perioda. Treći mjeritelj koji se promatrao je „Segments Retransmitted/sec“ koji daje prosječni broj TCP segmenata koji su u nekom određenom periodu bili prenošeni. Da je TCP segment prenošen znači da su dijelovi nekih prethodnih segmenata ponovno korišteni u novom segmentu. Ukoliko je broj prenošenih segmenata u periodu bio veći od nula to je znak da se isti TCP segmenti šalju više puta kroz vezu, što je pokazatelj da postoji problem sa hardverskim dijelovima mreže. Naglo povećanje vrijednosti nekog od TCP mjerila može značiti postojanje uljeza u mreži.

Mrežni adapter, koji se još naziva i mrežna kartica, je uređaj koji služi za uspostavljanje veze između računala ili nekog drugog krajnjeg uređaja i računalne mreže. Za prikupljanje podataka o mrežnom adapteru odabrano je pet mjeritelja performansi. Prvi mjeritelj se naziva „Bytes Received/sec“ i služi za dobivanje ukupnog broja dobivenih bajtova poslanih u vremenu od jedne sekunde. Drugi mjeritelj je „, Bytes Sent/sec“ sa njim se dobiva ukupan broj bajtova poslanih kroz vezu unutar vremenskog perioda od sekunde. „Packets received/sec“ je treći mjeritelj i njime se dobiva broj paketa koji su dobiveni kroz uspostavljenu vezu unutar jedne sekunde. Četvrti mjeritelj služi za dobivanje broja poslanih paketa unutar jedne sekunde na uspostavljenoj vezi i naziva se „Packets Sent/sec“. Posljednji i peti mjeritelj je „Output Queue Length“ koji prikazuje dužinu reda čekanja za izlazne pakete, tj. broj paketa koji čekaju da se pošalju s adaptera u računalnu mrežu. Ukoliko je dužina reda čekanja za slanje duža od dva već neko vrijeme, tada postoji problem sa djelovanjem mreže (npr. loša mrežna kartica, problem unutar mreže i drugi).

Mrežno sučelje predstavlja softversko sučelje koje se povezuje s nekim od oblika mrežnih adaptera. Prilikom mjerenja aktivnosti korisnika je u ovom radu odabrano pet mjeritelja performansi za dobivanje podataka o mrežnim sučeljima. Prvi mjeritelj je „Bytes received/sec“ koji daje broj primljenih bajtova u sekundi za svaki mrežni adapter. Drugi mjeritelj, „Bytes Sent/sec“, prikazuje broj poslanih bajtova u sekundi preko svakog mrežnog adaptera. „Packets Received/sec“ je treći mjeritelj sa njim se dobiva broj paketa u sekundi koje prima mrežno sučelje. „Packets Sent/sec“ je četvrti mjeritelj po redu koji daje uvid u broj paketa poslanih u sekundi sa mrežnog sučelja. Posljednji mjeritelj je „Output Queue Length“ koji daje dužinu reda za čekanje za izlazne pakete. Ukoliko je vrijednost ovog mjeritelja veća od dva, tada postoje kašnjenja i problem uskog grla (eng. bottleneck) koje je potrebno otkloniti za neometano funkcioniranje računalne mreže.

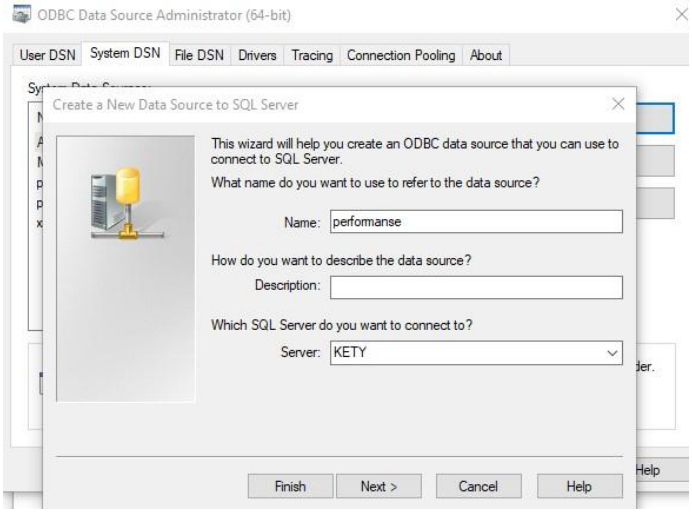
6.2. Izrada baze podataka

U slučaju ovog projekta odabrano je direktno kreiranje baze podataka na temelju dobivenog seta podataka unutar alata Performance Monitor. Kako bi se kreirala veza između alata Performance Monitor i alata Microsoft SQL Server Management Studio, tj. između podataka koji će biti dobiveni na temelju mjeritelja performansi i baze podataka unutar koje se žele zapisati dobiveni podatci, bilo je potrebno kreirati ODBC 64-bitni izvor podataka. Prvi korak prilikom kreiranja ODBC izvora podataka je bio odabir SQL Servera kao programa za kojeg će se kreirati izvor podataka.



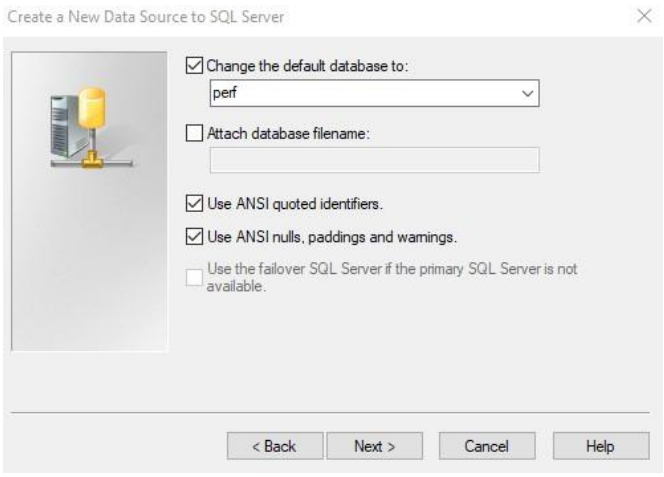
Slika 12: Odabir programa za prihvat izvora podataka

Slika 12 prikazuje prvi korak u kreiranju ODBC izvora podataka. Nakon ovog koraka je potrebno imenovati izvor podataka i odabrati SQL server na kojeg će se izvor podataka spajati.



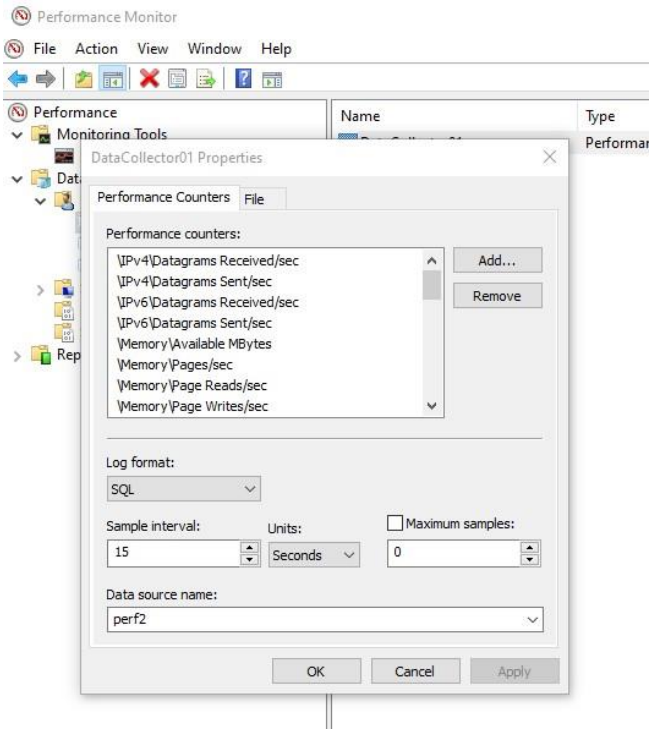
Slika 13: Imenovanje izvora podataka i odabir SQL servera

Slika 13 prikazuje zaslon za imenovanje izvora podataka i odabira SQL servera. Nakon ovoga potrebno je odabrati postojeću bazu podataka s kojom se želi spojiti izvor podataka.



Slika 14: Odabir baze podataka

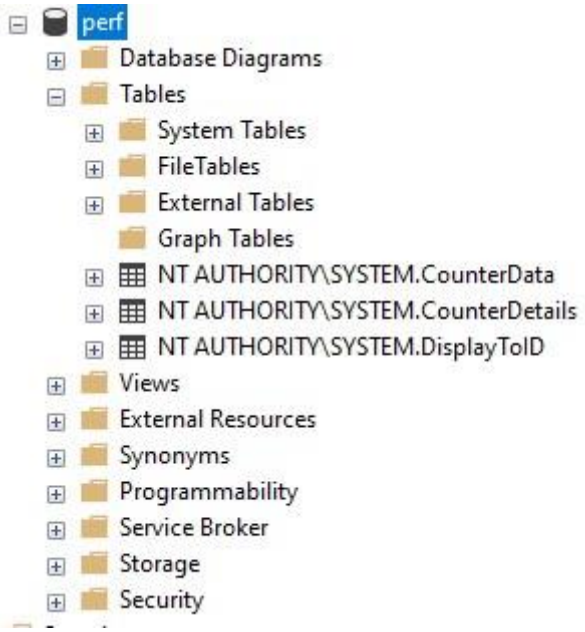
Slika 14 prikazuje kako je za potrebe ovog rada napravljena i odabrana baza podataka perf. Nakon kreiranja izvora podataka i testiranja njegove veze s bazom, potrebno ga je odabrati kao izvor podataka za set podataka koji je kreiran unutar alata Performance Monitor.



Slika 15: Odabir ODBC izvora podataka u alatu Performance Monitor

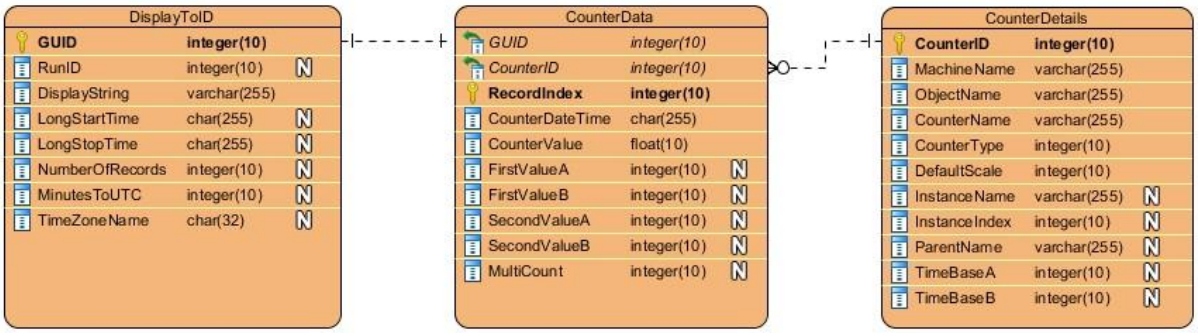
Slika 15 prikazuje da se kod uređivanja mjeritelja podataka treba u kartici za izvor podataka odabrati ranije kreirani ODBC izvor podataka.

Sljedeći korak je pokretanje skupa podataka u alatu Performance Monitor, što je objašnjeno u potpoglavlju Prikupljanje podataka. Naime pokretanjem skupa podataka se automatski kreiraju i popunjavaju tablice potrebne za pohranu podataka unutar baze podataka koja je ranije napravljena. ODBC izvor podataka se kreirao kako bi se omogućilo automatsko popunjavanje baze podataka s izradom tablica, umjesto da se prvo od skupa podataka dobivenih unutar Performance Monitor-a kreira Excel datoteka, nakon toga urede svi podatci unutar datoteke kako bi bili spremni za unos u bazu, a nakon toga napravila i uredila baza podataka kako bi se mogli unijeti podatci iz datoteke.



Slika 16: Baza podataka

Na slici 16 moguće je vidjeti izgled baze podataka kreirane unutar alata Microsoft SQL Server Management Studio. Baza sadrži tri kreirane tablice i to: CounterData, CounterDetails i DisplayToID. Tablica CounterDetails sadrži podatke o svim korištenim mjeriteljima performansi, a neki od tih podataka su kategorija iz koje dolazi mjeritelj, naziv mjeritelja, tip mjeritelja, naziv instance mjeritelja ukoliko ju on ima i drugi. Tablica CounterData sadrži podatke dobivene mjerenjem, kao što su datum, vrijeme, vrijednost mjeritelja i drugi. Treća i posljednja tablica DisplayToID sadrži podatke o samom mjerenju, kao što je vrijeme kada je mjerenje započeto, vrijeme kada je mjerenje završeno i druge podatke.



Slika 17: ERA dijagram baze podataka

Na slici 17 nalazi se ERA dijagram napravljene baze podataka gdje su vidljive veze između tablica putem vanjskih ključeva i stupci koji se nalaze u svakoj od ranije navedenih tablica.

	GUID	RunID	DisplayString	LogStartTime	LogStopTime	NumberOfRecords	MinutesToUTC	TimeZoneI
1	4BE711D7-A731-44DF-81BD-C8CB7BDE1C88	0	DataCollector01	2020-09-18 13:10:49.651	2020-09-18 14:23:26.746	292	-120	Central Eu

Slika 18: Sadržaj tablice DisplayToID

Provođenjem odgovarajućih upita za prikaz sadržaja tablice DisplayToID unutar baze podataka se dobivaju podatci koji su prikazani na slici 18. Ovdje je vidljivo kada je prikupljanje podataka od strane mjeritelja performansi započeto i kada je ono završeno, ukupni broj zapisa i druge informacije o samom prikupljanju podataka.

	CounterID	MachineName	ObjectName	CounterName	CounterType	DefaultScale	InstanceName	InstanceIndex	ParentName	ParentObjectID	TimeB
19	19	\\KETY	Processor ...	DPCs Queued/sec	272696320	0	_Total	NULL	NULL	NULL	0
20	20	\\KETY	TCPv4	Segments Received/sec	272696320	-1	NULL	NULL	NULL	NULL	10000
21	21	\\KETY	TCPv4	Segments Sent/sec	272696320	-1	NULL	NULL	NULL	NULL	10000
22	22	\\KETY	TCPv4	Segments Retransmitte...	272696320	-1	NULL	NULL	NULL	NULL	10000
23	23	\\KETY	TCPv6	Segments Received/sec	272696320	-1	NULL	NULL	NULL	NULL	10000
24	24	\\KETY	TCPv6	Segments Sent/sec	272696320	-1	NULL	NULL	NULL	NULL	10000
25	25	\\KETY	TCPv6	Segments Retransmitte...	272696320	-1	NULL	NULL	NULL	NULL	10000
26	26	\\KETY	Network A...	Bytes Sent/sec	272696576	-4	Bluetooth D...	NULL	NULL	NULL	10000
27	27	\\KETY	Network A...	Bytes Sent/sec	272696576	-4	Microsoft Ke...	NULL	NULL	NULL	10000
28	28	\\KETY	Network A...	Bytes Sent/sec	272696576	-4	WAN Minipo...	NULL	NULL	NULL	10000
29	29	\\KETY	Network A...	Bytes Sent/sec	272696576	-4	WAN Minipo...	NULL	NULL	NULL	10000
30	30	\\KETY	Network A...	Bytes Sent/sec	272696576	-4	Realtek PCI...	NULL	NULL	NULL	10000
31	31	\\KETY	Network A...	Bytes Sent/sec	272696576	-4	WAN Minipo...	NULL	NULL	NULL	10000
32	32	\\KETY	Network A...	Bytes Sent/sec	272696576	-4	VirtualBox H...	NULL	NULL	NULL	10000
33	33	\\KETY	Network A...	Bytes Sent/sec	272696576	-4	Ralink RT32...	NULL	NULL	NULL	10000
34	34	\\KETY	Network A...	Bytes Sent/sec	272696576	-4	Teredo Tun...	NULL	NULL	NULL	10000
35	35	\\KETY	Network A...	Bytes Sent/sec	272696576	-4	Microsoft IP-...	NULL	NULL	NULL	10000

Slika 19: Vrijednosti tablice CounterDetails

Slika 19 prikazuje dio podataka zapisanih unutar tablice CounterDetails koji su dobiveni za vrijeme mjerenja performansi, a tiču se informacija vezanih uz same mjeritelje. Stupac ObjectName predstavlja kategoriju iz koje potječe mjeritelj performansi, stupac MachineName prikazuje naziv uređaja za kojeg su prikupljeni sljedeći podatci, a osim ovih informacija u tablici se još vide informacije o nazivu i indeksu instance mjeritelja performansi, naziv mjeritelja roditelja ukoliko ga mjeritelj ima i druge informacije.

	GUID	CounterID	RecordIndex	CounterDateTime	CounterValue	FirstValueA	FirstValueB	SecondValueA	Secon
1	4BE711D7-A731-44DF-81BD-C8CB7BDE1C88	1	1	2020-09-18 13:10:49.651	0	54767	0	-178393779	8
2	4BE711D7-A731-44DF-81BD-C8CB7BDE1C88	1	2	2020-09-18 13:10:54.884	12,4207914188153	54832	0	-126062170	8
3	4BE711D7-A731-44DF-81BD-C8CB7BDE1C88	1	3	2020-09-18 13:11:09.886	12,9317645378714	55026	0	23956027	9
4	4BE711D7-A731-44DF-81BD-C8CB7BDE1C88	1	4	2020-09-18 13:11:24.887	12,6663728912581	55216	0	173959506	9
5	4BE711D7-A731-44DF-81BD-C8CB7BDE1C88	1	5	2020-09-18 13:11:39.889	16,530042863001	55464	0	323989365	9
6	4BE711D7-A731-44DF-81BD-C8CB7BDE1C88	1	6	2020-09-18 13:11:54.888	12,8009850784717	55656	0	473977822	9
7	4BE711D7-A731-44DF-81BD-C8CB7BDE1C88	1	7	2020-09-18 13:12:09.887	13,0014139471048	55851	0	623961509	9
8	4BE711D7-A731-44DF-81BD-C8CB7BDE1C88	1	8	2020-09-18 13:12:24.886	12,3342265780221	56036	0	773950646	9
9	4BE711D7-A731-44DF-81BD-C8CB7BDE1C88	1	9	2020-09-18 13:12:39.890	14,796002613294	56258	0	923991171	9
10	4BE711D7-A731-44DF-81BD-C8CB7BDE1C88	1	10	2020-09-18 13:12:54.885	14,6044778302659	56477	0	1073945180	9
11	4BE711D7-A731-44DF-81BD-C8CB7BDE1C88	1	11	2020-09-18 13:13:09.877	13,8076717265135	56684	0	1223861838	9
12	4BE711D7-A731-44DF-81BD-C8CB7BDE1C88	1	12	2020-09-18 13:13:24.879	14,3314338450915	56899	0	1373881719	9
13	4BE711D7-A731-44DF-81BD-C8CB7BDE1C88	1	13	2020-09-18 13:13:39.877	19,935762439534	57198	0	1523863442	9
14	4BE711D7-A731-44DF-81BD-C8CB7BDE1C88	1	14	2020-09-18 13:13:54.875	12,1344916919102	57380	0	1673849123	9
15	4BE711D7-A731-44DF-81BD-C8CB7BDE1C88	1	15	2020-09-18 13:14:09.875	12,6000399841269	57569	0	1823848647	9

Slika 20: Vrijednosti tablice CounterData

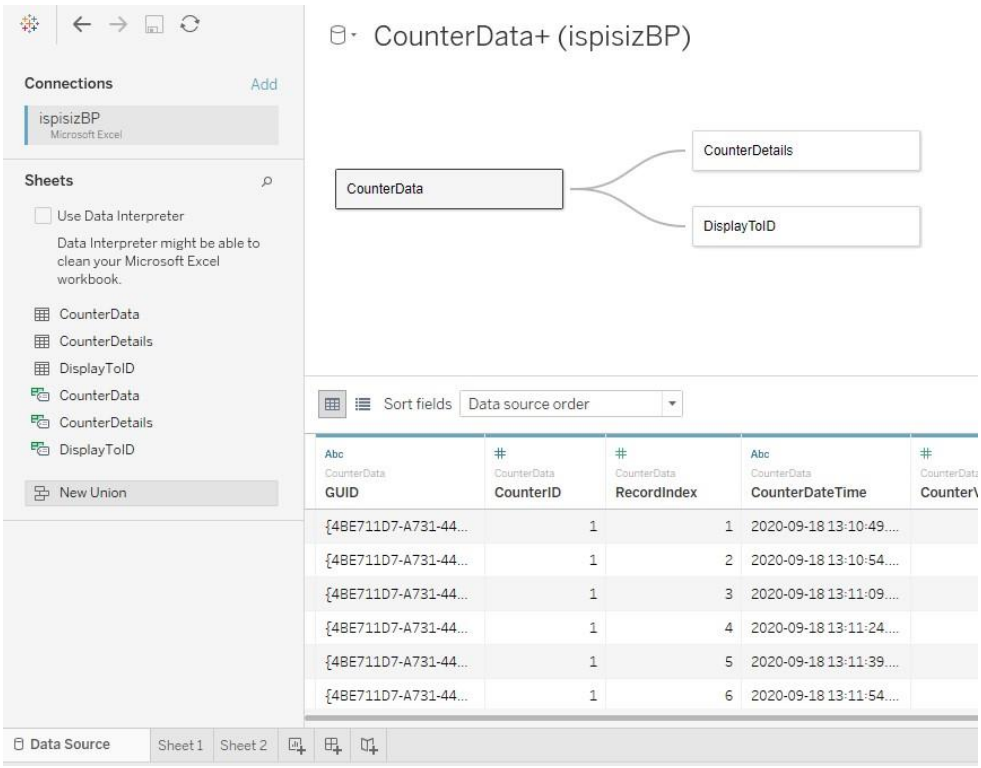
Dio podataka koji su zapisani unutar tablice CounterData vidljeivi su na slici 20. Unutar ove tablice se nalaze rezultati mjerenja za svaki pojedini mjeritelj u danom vremenskom periodu, što znači da jedan red tablice predstavlja vrijednost koju je određeni mjeritelj prikupio u zadanom periodu koji iznosi 15 sekundi.

6.3. Vizualizacija i analiza podataka

Alat Tableau je u slučaju ovog rada odabran u svrhu vizualizacije i analize podataka dobivenih mjerenjem performansi sustava. Kod Tableau Pro verzije alata moguće je željenu bazu podataka spojiti sa alatom i koristiti ju kao izvor podataka za daljnju vizualizaciju i analizu, ali u slučaju Tableau Public verzije alata, koja je besplatna za korištenje i odabrana je za izvođenje vizualizacije i analize podataka unutar ovog projekta, nije moguće direktno povezati bazu podataka kao izvor podataka. Zbog toga je bilo potrebno od ranije napravljene i popunjene baze podataka napraviti Excel datoteku koja će se koristiti za vizualizaciju i analizu podataka. Excel datoteka se je napravila pomoću čarobnjaka za uvoz i ispis podataka iz SQL servera koji je dio Microsoft SQL Server Management Studio alata, gdje je bilo potrebno odabrati potrebni SQL server na kojem se nalazi baza podataka i samu bazu podataka. Nakon toga je trebalo odabrati Excel datoteku kao željeni oblik datoteke za upis

podataka i sve tablice iz baze podataka koje se žele prenijeti u datoteku. Ovime je dobivena Excel datoteka unutar koje se nalaze podatci raspoređeni u radne listove koji predstavljaju tablice iz baze podataka.

Prvi korak nakon pokretanja alata Tableau Public je odabir Excel datoteke kao izvora podataka za daljnju obradu. Nakon odabira datoteke u alatu se otvara sljedeći zaslon u kojemu je potrebno urediti izvor podataka.

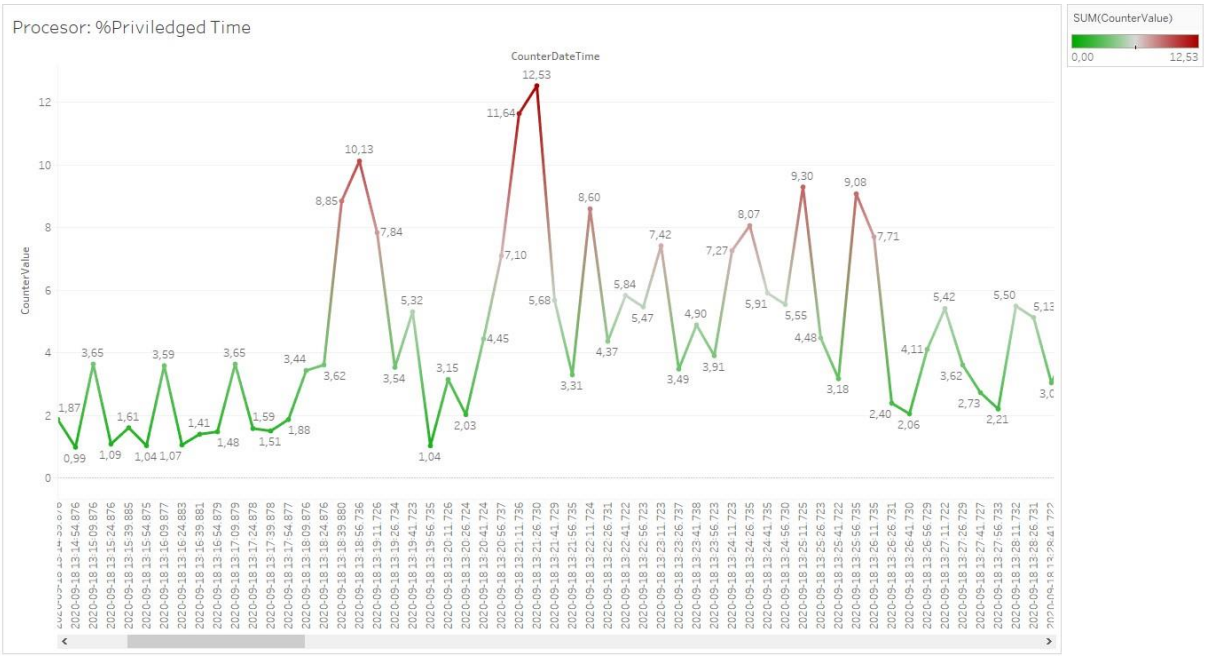


Slika 21: Uređivanje izvora podataka

Na slici 21 vidljivo je da se na lijevoj strani zaslona, koji je dio kartice sa izvorom podataka, nalaze sve tablice kreirane na temelju radnih listova iz Excel datoteke. Na temelju tih tablica potrebno je napraviti

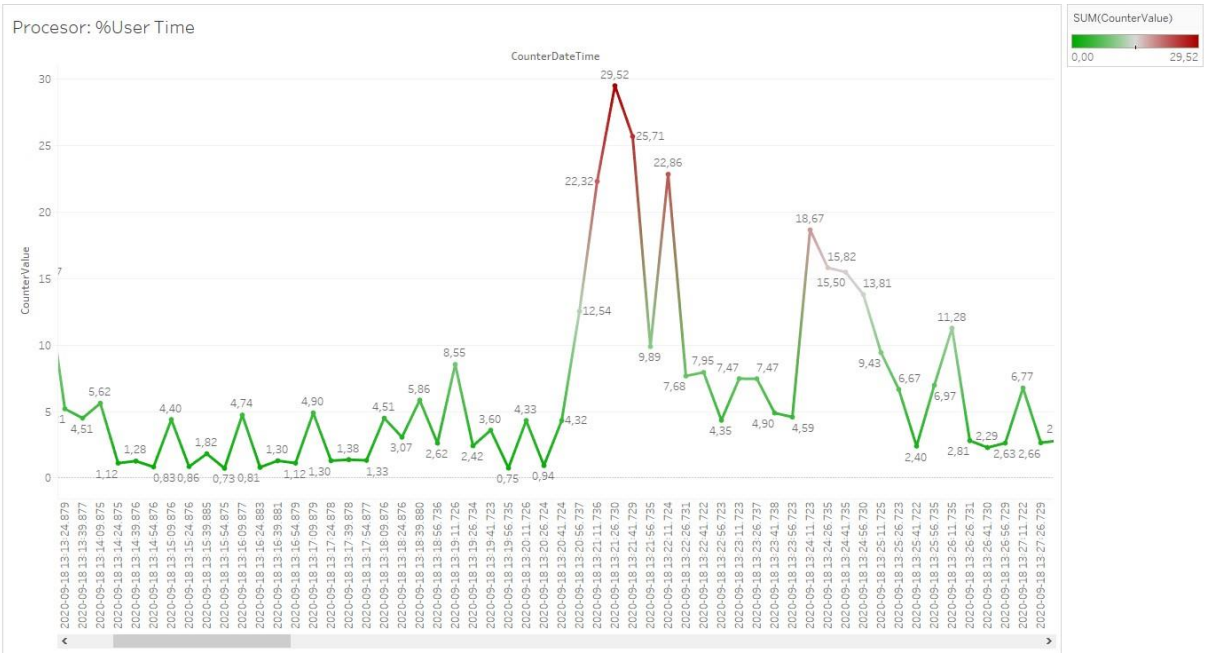
U nastavku ovog poglavlja bit će prikazani pojedini grafovi na temelju kojih će se analizirati podatci i gledati postoji li problema prilikom funkcioniranja sustava.

6.3.1. Analiza podataka vezanih uz rad procesora



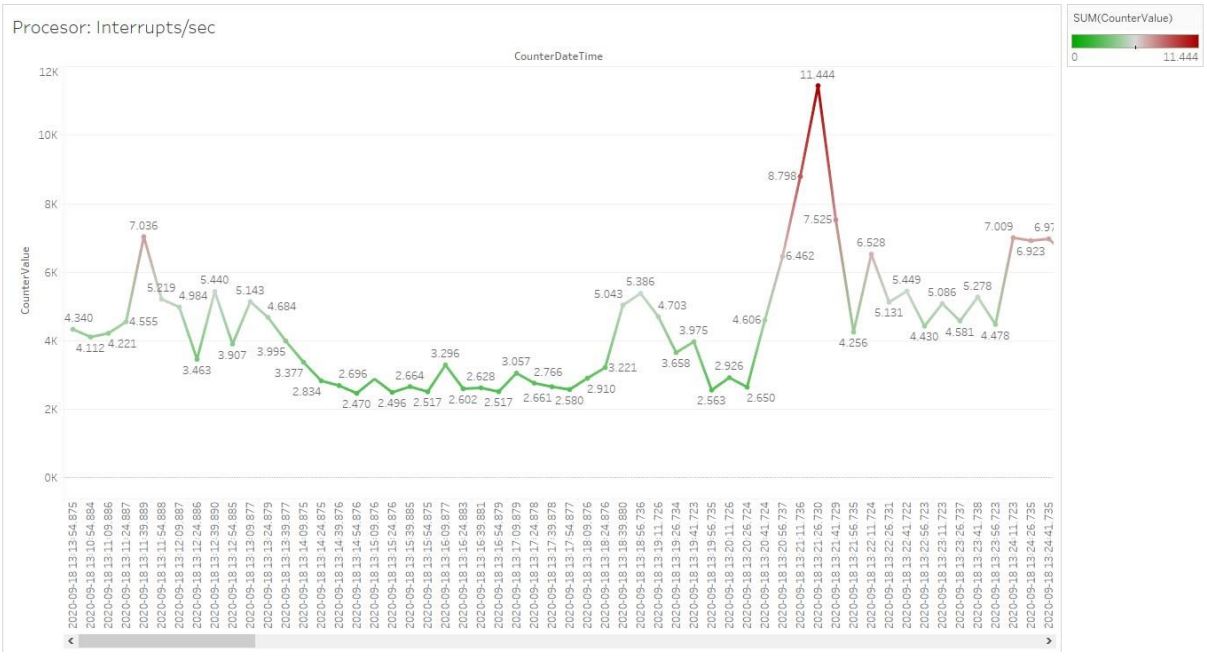
Slika 22: % Priviledged Time

Na slici 22 vidljiv je dio grafikona na kojem se nalaze podatci mjeritelja „%Priviledged Time“. Temeljem ovog grafikona moguće je zaključiti da je rad procesora u načinu rada s jezgrom operacijskog sustava u granicama normale jer ne prelazi vrijednosti od 25%, točnije najviša vrijednost iznosi 12.53%.



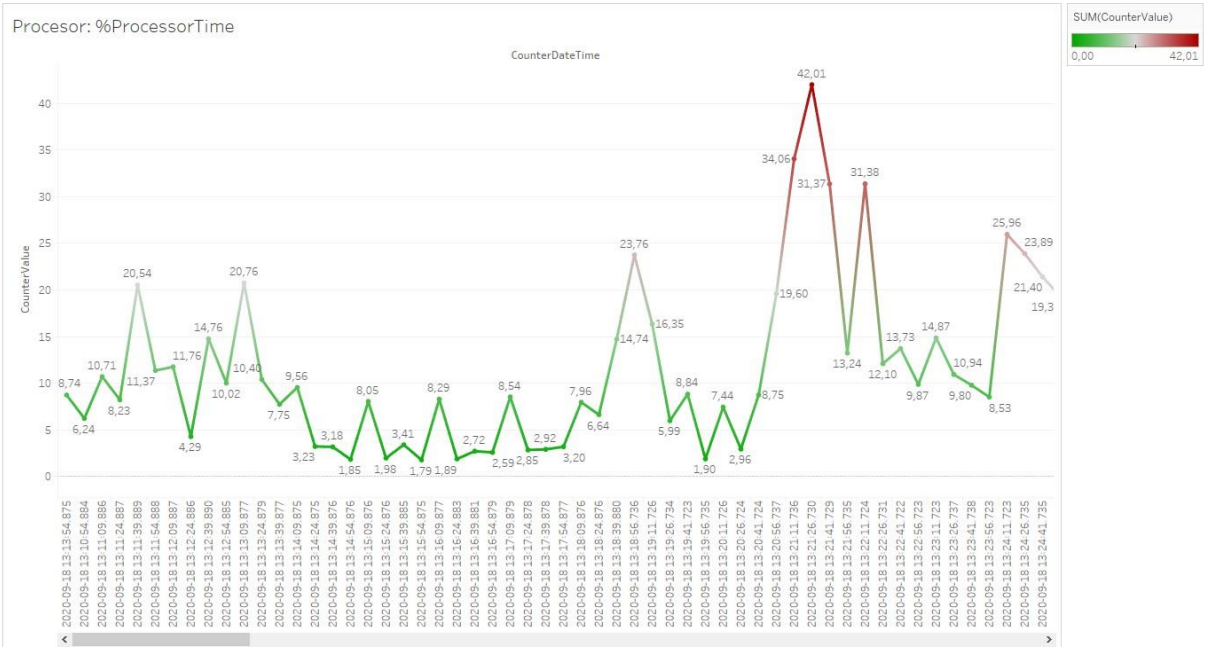
Slika 23: % User Time

Analizom podataka dobivenih od strane mjeritelja „%User Time“ koji su vizualizirani putem grafa na slici 23 može se reći da je procesor prilikom korisničkog rada funkcionirao unutar granica normale zato što vrijednost mjeritelja nikad ne prelazi granicu od 65%, tj. njegova najveća vrijednost iznosi 29.52%.



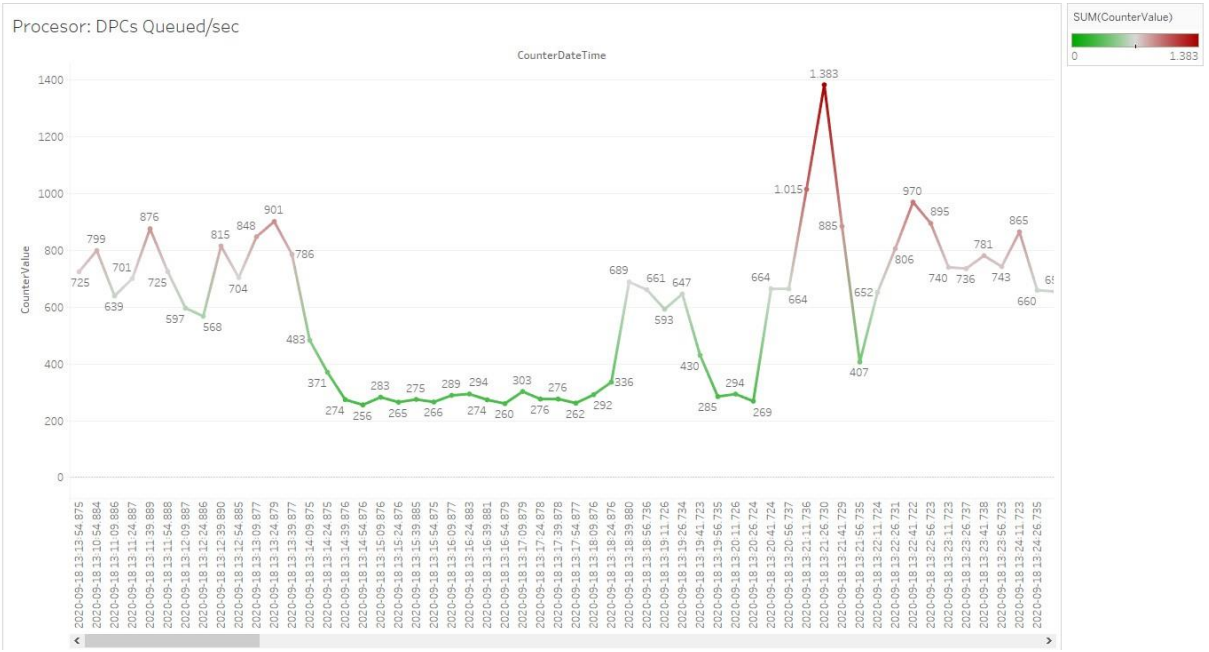
Slika 24: Interrupts/sec

Na grafikonu koji se nalazi na slici 24 vizualizirani su podatci koji predstavljaju broj prekida u sekundi, ili u slučaju grafikona, zato što je prilikom kreacije podataka bio odabran vremenski period od 15 sekundi, podatci koji predstavljaju broj prekida unutar 15 sekundi. Kako je preporučena količina prekida u sekundi do 1000 za procesore prosječne jačine, u ovom slučaju je granica normale 15,000 prekida unutar 15 sekundi, koja se niti u jednom trenutku nije prošla jer najveća vrijednost iznosi 11,444 prekida unutar 15 sekundi.



Slika 25: % Processor Time

Rezultati prikupljanja podataka od strane mjeritelja podataka „%Processor Time“ vizualizirani su na grafikonu prikazanom slikom 25. Na njemu je vidljivo da je većina vrijednosti ovog mjerila niža od preporučene granične vrijednosti mjerila koja iznosi 80%, tj. najviša vrijednost mjerila iznosi 42.01%, što znači da procesor ima dovoljno slobodnog vremena u kojemu ne radi s pravim dretvama i ne rješava poslane zadatke.

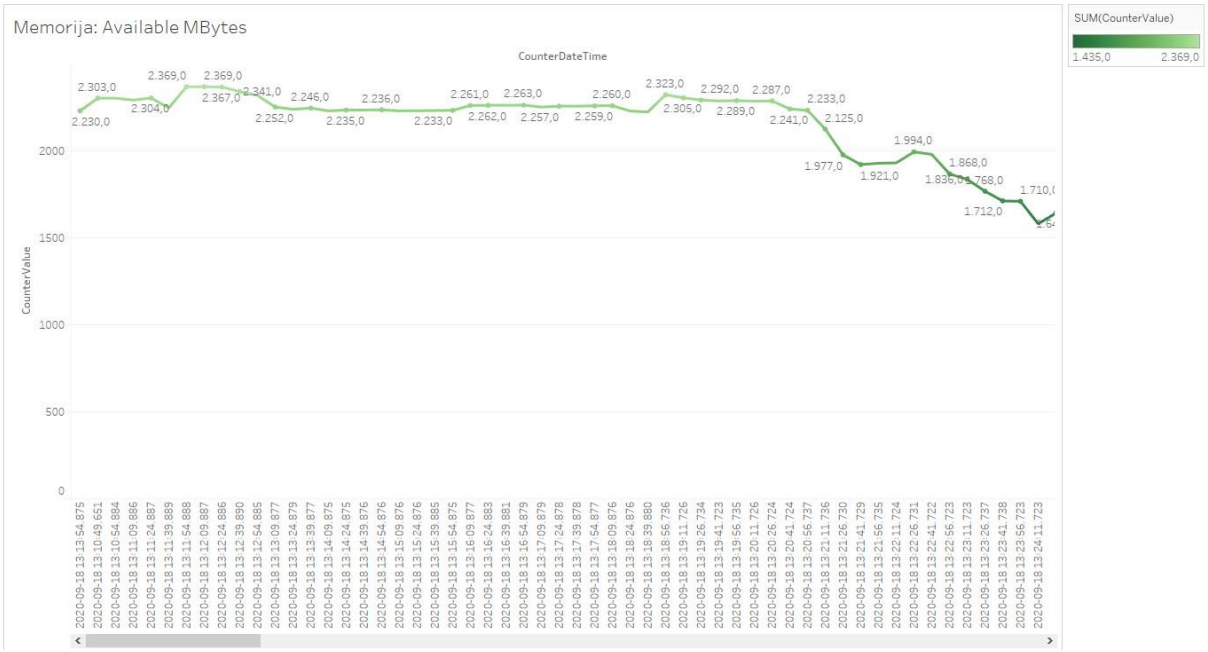


Slika 26: DPCs Queued/sec

Na slici 26 je vidljiv broj DPC objekata koji su dodani u procesorov DPC red čekanja. Najveća vrijednost ovog mjerila je iznosila 1,383 DPC objekta dodanih u red čekanja. Kad se ta vrijednost zbroji s maksimalnom vrijednošću prekida u sekundi koje procesor treba obraditi i koja iznosi 11,444, vidljivo je da ukupni broj prekida i dalje ne prelazi preporučenu granicu od 15,000 prekida u 15 sekundi.

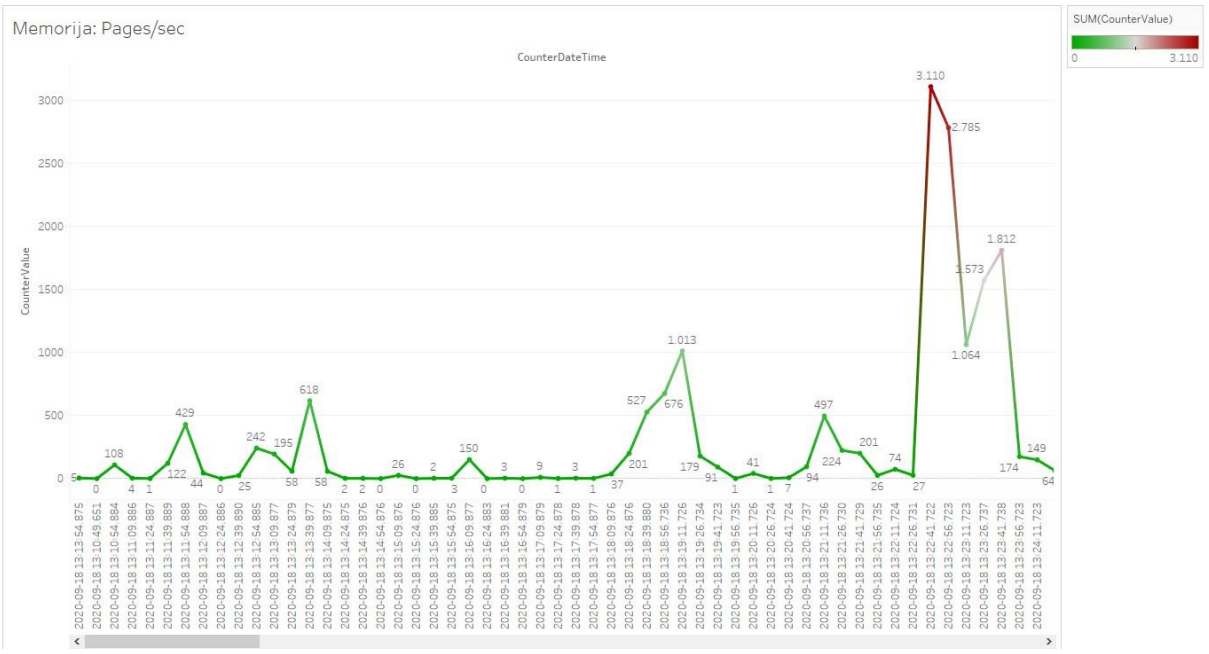
6.3.2. Analiza podataka vezanih uz korištenje memorije

Podatci vezani uz korištenje memorije dobiveni su putem 4 mjeritelja podataka, i to: „Available MBytes“, „Pages/sec“, „Page Reads/sec“ i „Page Writes/sec“.



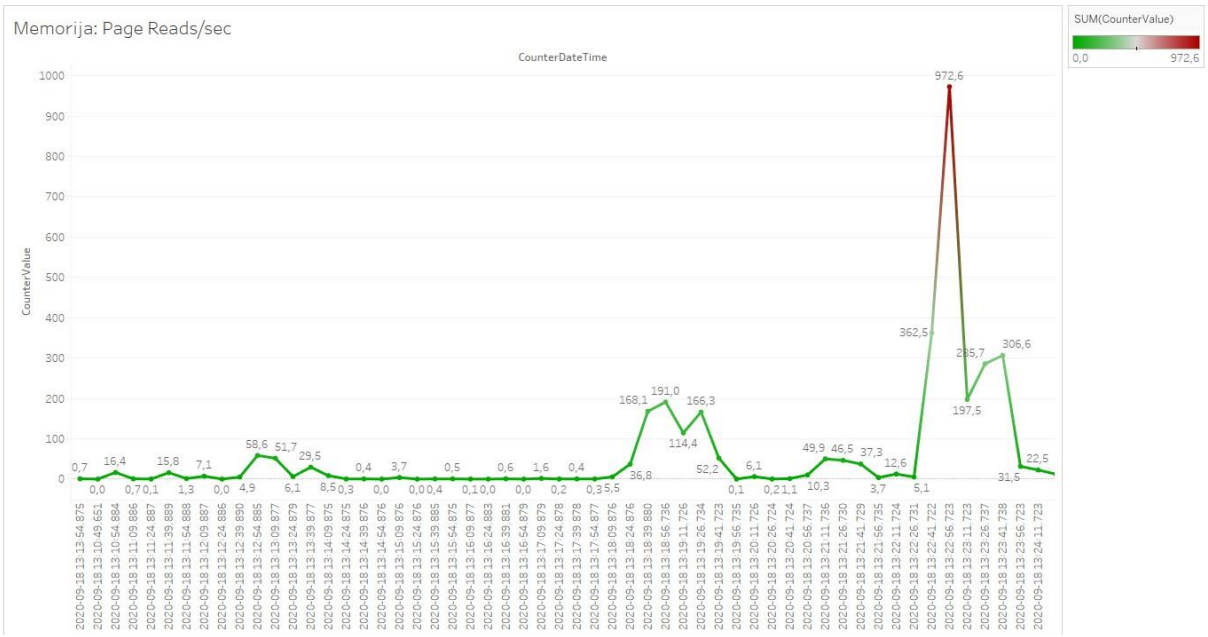
Slika 27: Available MBytes

Na slici 27 se nalaze vizualizirani podatci vezani uz mjeritelj performansi „Available MBytes“ čija je najmanja vrijednost iznosila 1,435 megabajta, a najviša 2,369 dostupnih megabajta u sustavu.



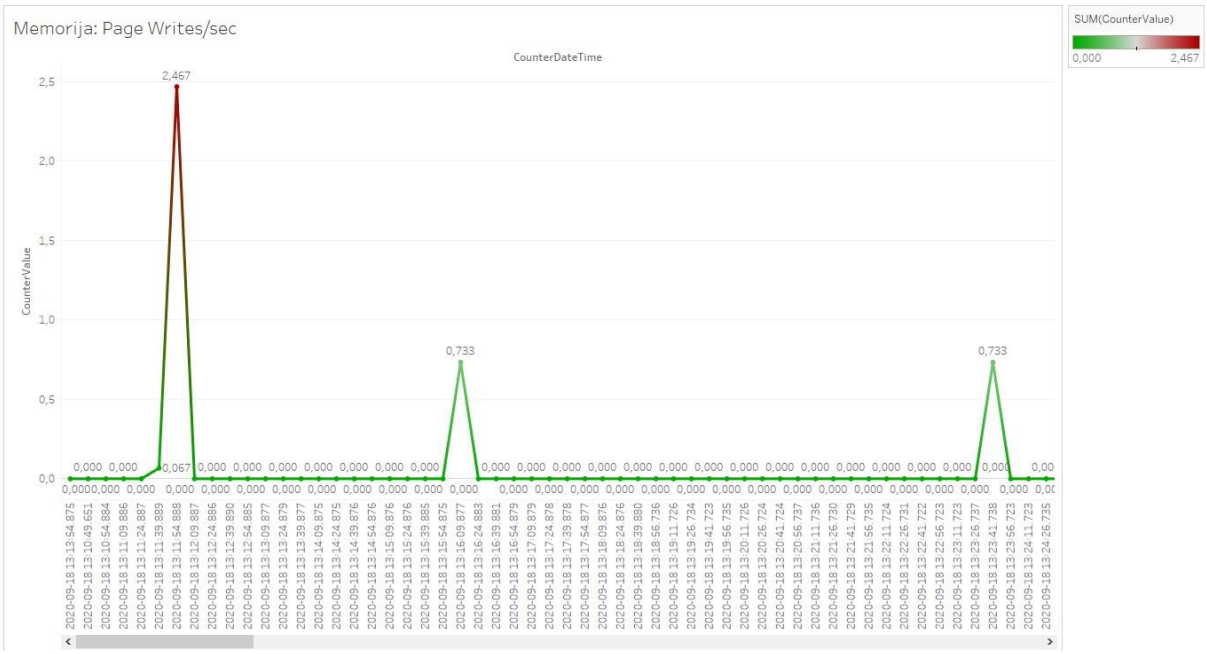
Slika 28: Pages/sec

Na slici 28 su prikazani svi podatci dobiveni od strane mjeritelja performansi „Pages/sec“ koji prikazuje broj pisanja i čitanja sa diska u sekundi, ili u ovom slučaju unutar 15 sekundi. Najveća vrijednost ovog mjeritelja iznosi 3,110 zapisa i čitanja sa diska, dok se većina ostalih vrijednosti nalazi u rasponu do 100 zapisa i čitanja unutar 15 sekundi.



Slika 29: Page Reads/sec

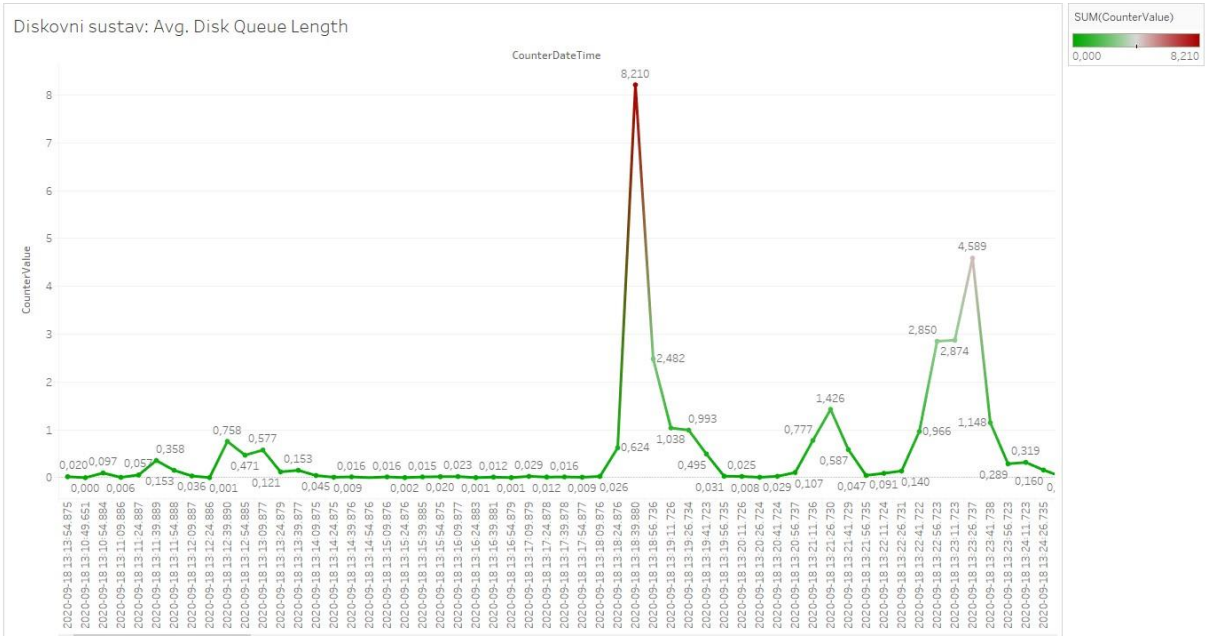
Vizualizacija podataka dobivenih mjeriteljem „Page Reads/sec“ nalazi se na slici 29, gdje je vidljivo da je najveća vrijednost mjeritelja bila 972.6 čitanja u sekundi, dok je većina vrijednosti ovog mjerila ispod 100 čitanja u sekundi.



Slika 30: Page Writes/sec

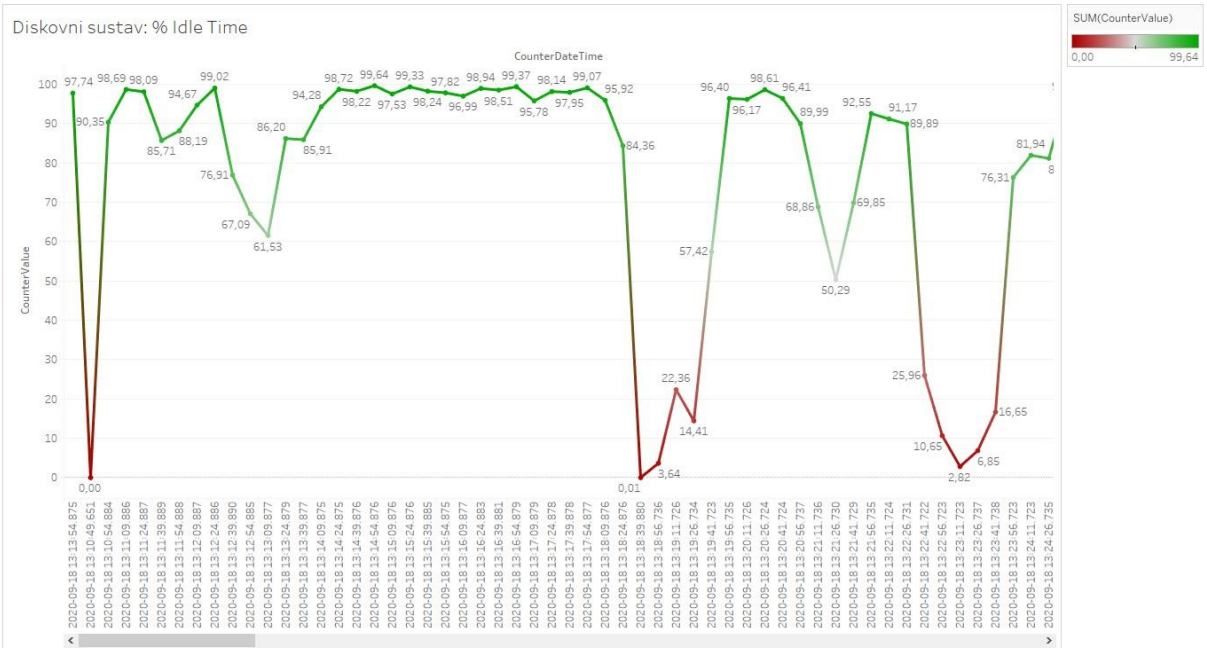
Slika 30 predstavlja vizualizaciju podataka dobivenih od strane mjeritelja performansi „Page Writes/sec“. Vidljivo je da je najveća vrijednost iznosila 2,467 zapisa dok kod većine vremenskih perioda od 15 sekundi, u kojima se mjerio broj zapisa, nema niti jednog zapisa.

6.3.3. Analiza podataka vezanih uz korištenje diskovnog sustava



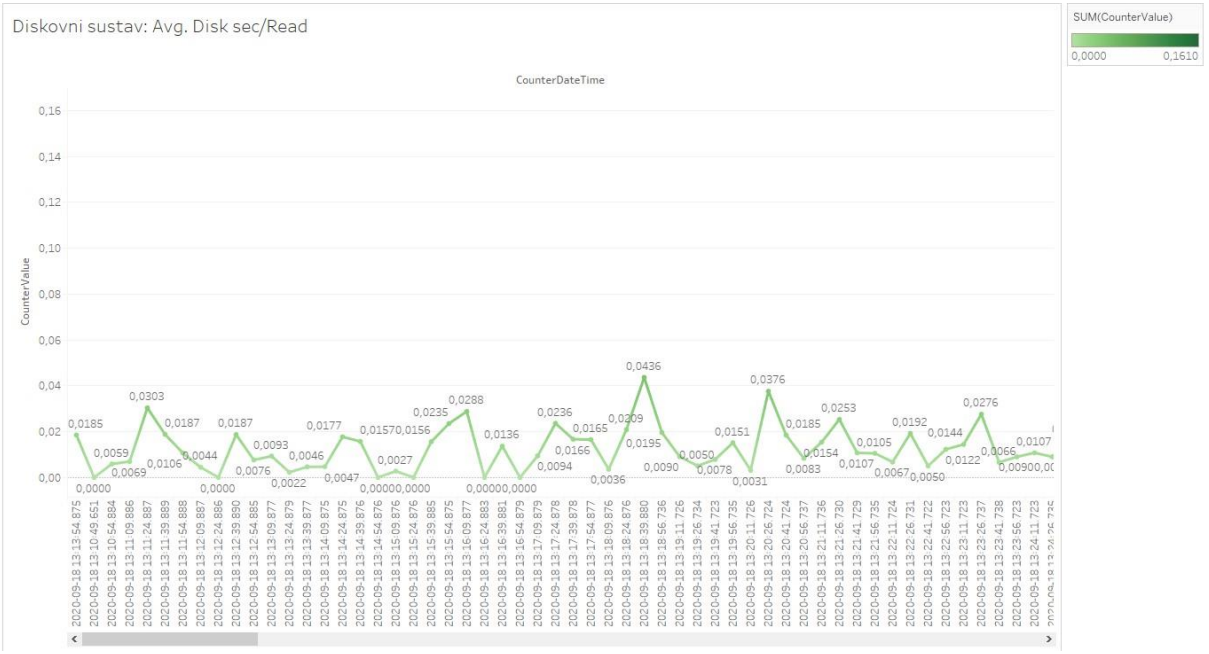
Slika 31: Avg. Disk Queue Lenght

Vrijednosti dobivene putem „Avg. Disk Queue Lenght“ mjeritelja podataka vizualizirani su na slici 31. Po ovoj slici vidljivo je da postoji problem jer je preporučeno da prosječna veličina diskovnog reda za čekanje ne prelazi vrijednosti veće od 2 do 5, a najviša zabilježena vrijednost ovog mjeritelja iznosi 8,210. Ukoliko bi takva visoka vrijednost bila duži vremenski period bilo bi potrebno provjeriti dolazi li do bottleneck problema prilikom rada sa diskovnim sustavom.



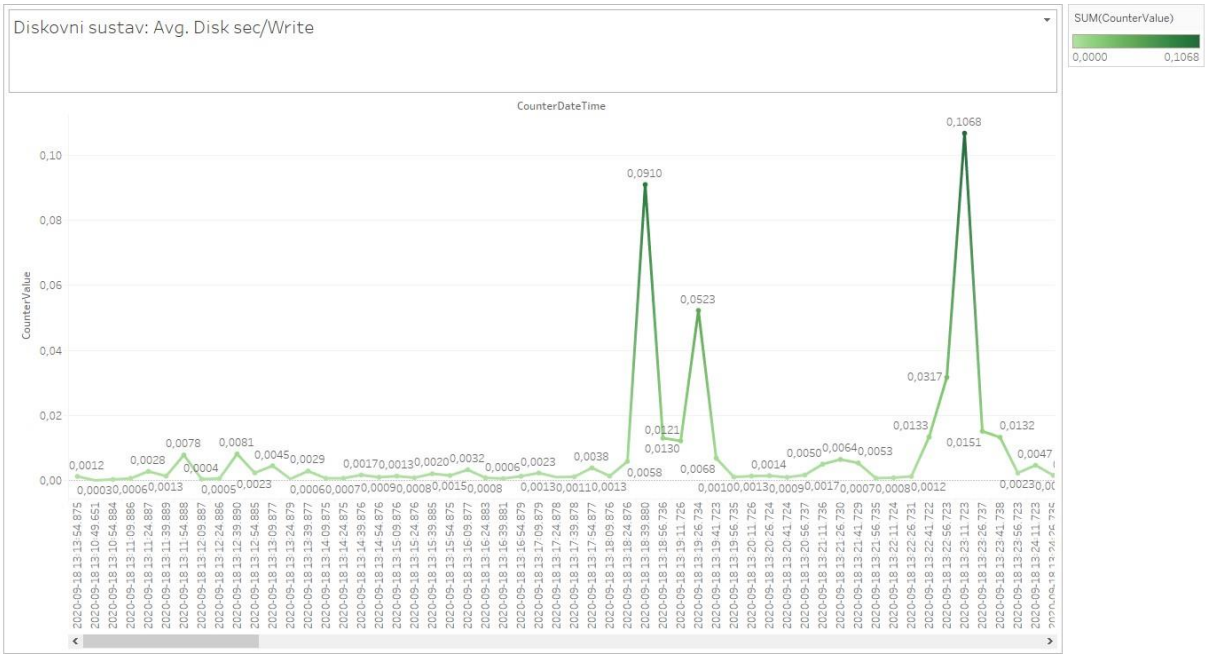
Slika 32: % Idle Time

Vizualizacija podataka dobivenih putem „%Idle Time“ mjeritelja podataka nalazi se na slici 32. Preporučljivo je da su vrijednosti ovog mjeritelja konstantno visoke, ali u ovom slučaju to nije tako. Vidljivo je da se vremena s niskom vrijednošću mjerila podudaraju s vremenom u kojem je vrijednost „Avg. Disk Queue Lenght“ mjerila bila visoka, što upućuje na neki problem sa diskovnim sustavom (kvar na njima, lošu konfiguraciju ili dosegnute maksimume diskovnog sustava).



Slika 33: Diskovni sustav: Avg. Disk sec/Read

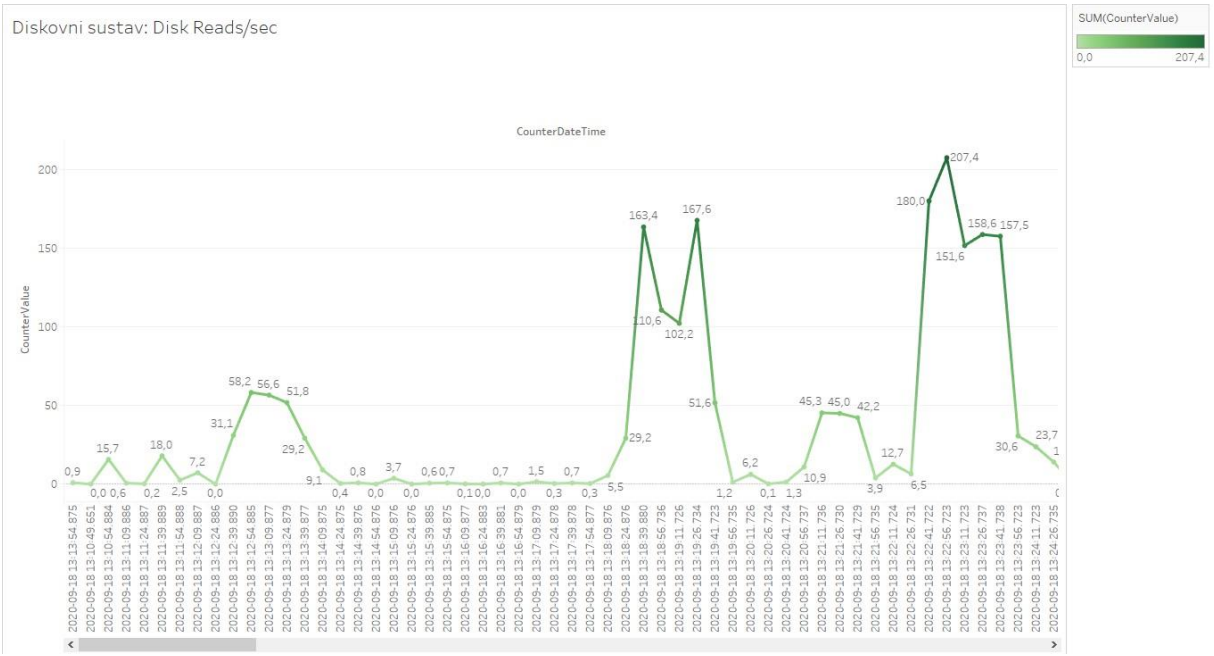
Mjeritelj „Avg. Disk sec/Read“ pokazuje prosječno vrijeme potrebno za čitanje sa diska, vizualizacija podataka dobivenih od strane njega je prikazana na slici 33. Najveća vrijednost ovog mjeritelja iznosi 0.1610 sekunde za izvođenje čitanja.



Slika 34: Diskovni sustav: Avg. Disk sec/Writes

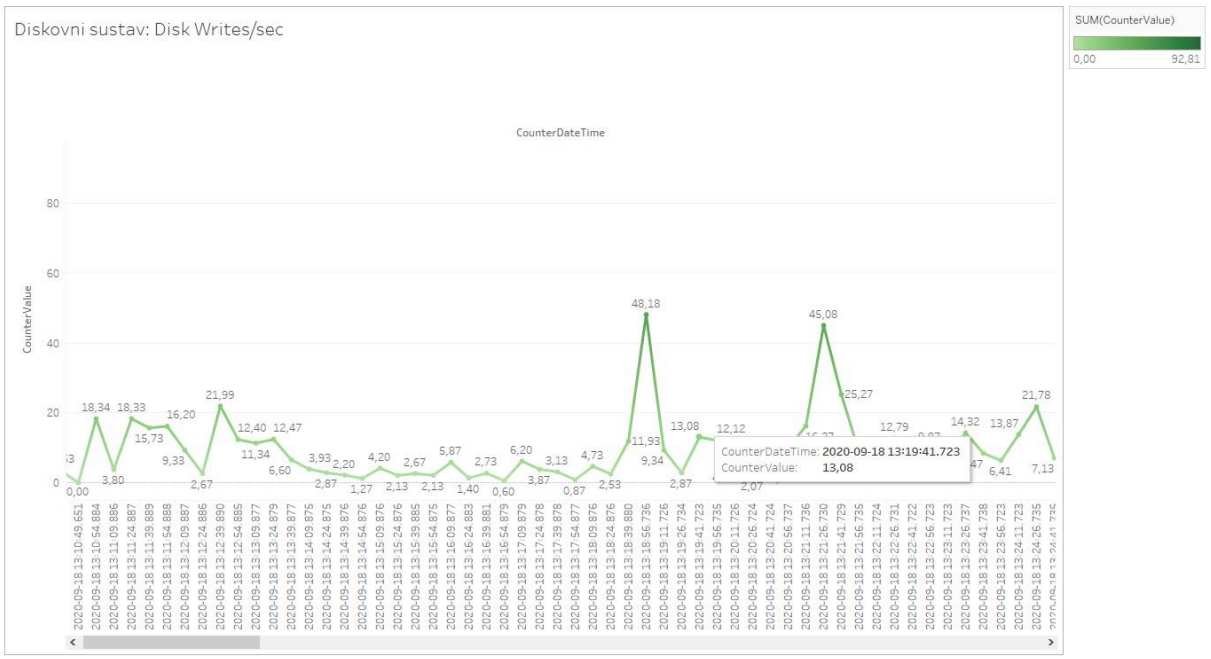
Vizualizacija podataka o prosječnom vremenu potrebnom za zapis podataka na diskovni sustav se nalazi na slici 34 i pokazuje velike razlike u vrijednostima mjeritelja, čije bi

se značenje trebalo interpretirati tako ta se dobije bazna vrijednost za funkcioniranje diskovnog sustava.



Slika 35: Diskovni sustav: Disk Reads/sec

Mjeritelj performansi „Disk Reads/sec“, za čije se dobivene vrijednosti na slici 35 nalazi njihova vizualizacija, predstavlja broj izvršenih izlaznih zahtjeva (zahtjeva za čitanje) izvršenih od strane diskovnog sustava u vremenskom periodu od 15 sekundi. Vidljivo je da je na mjestima broj zahtjeva bio puno veći od prosječne vrijednosti.

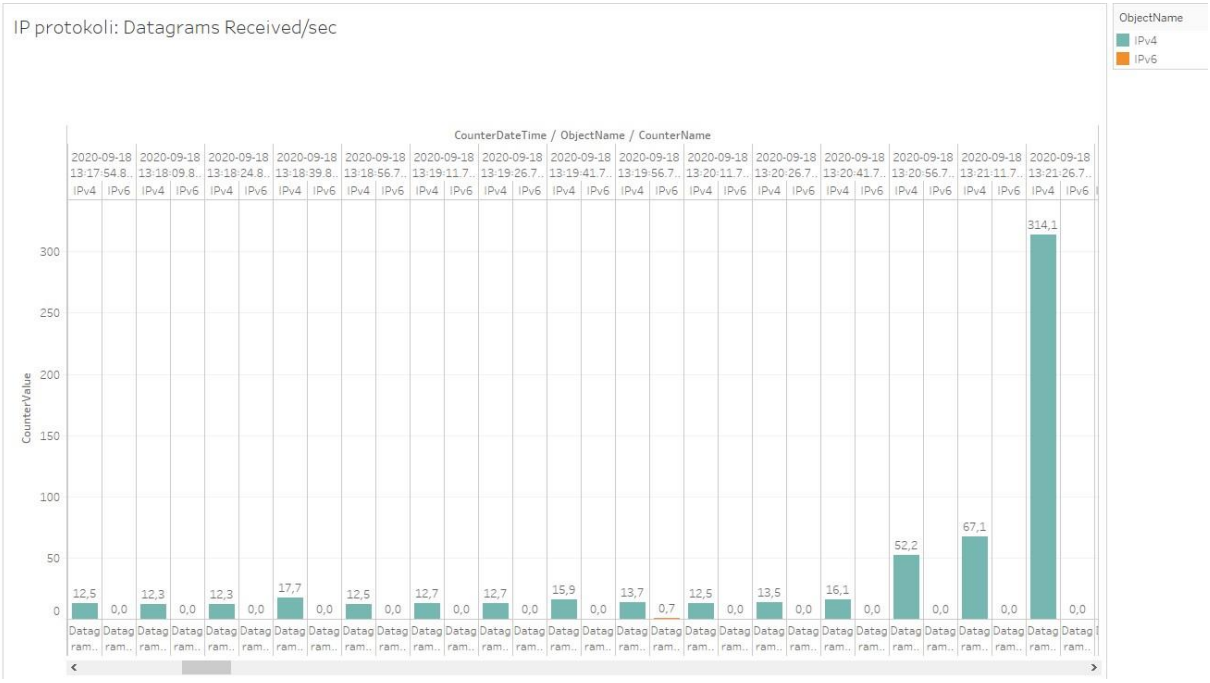


Slika 36: Diskovni sustav: Disk Writes/sec

Na slici 36 nalazi se vizualizacija podataka o broju izvršenih zahtjeva za pisanje na diskovni sustav u periodima od 15 sekundi. Vidljivo je da je u nekim vremenskim periodima broj izvršenih zahtjeva za pisanje bio puno veći nego inače.

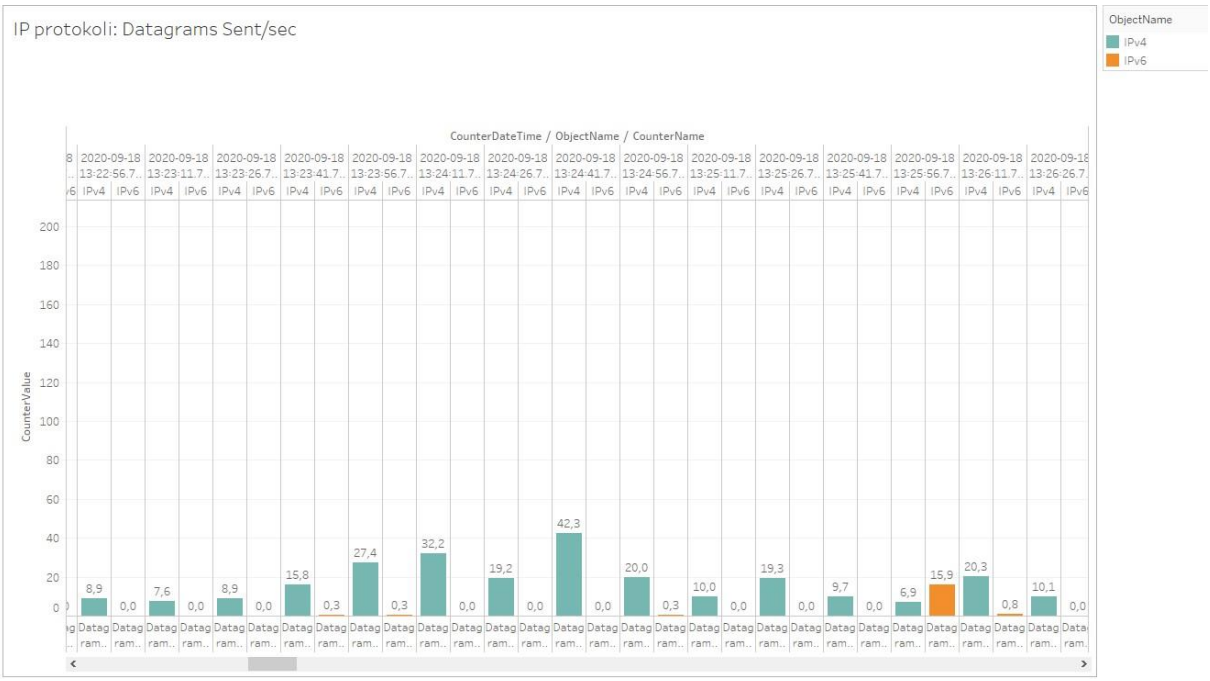
6.3.4. Analiza podataka vezanih uz korištenje mrežnih resursa

Za korištenje mrežnih resursa su se uzimali podaci iz kategorija IP protokola, TCP protokola, mrežnih adaptera i mrežnih sučelja.



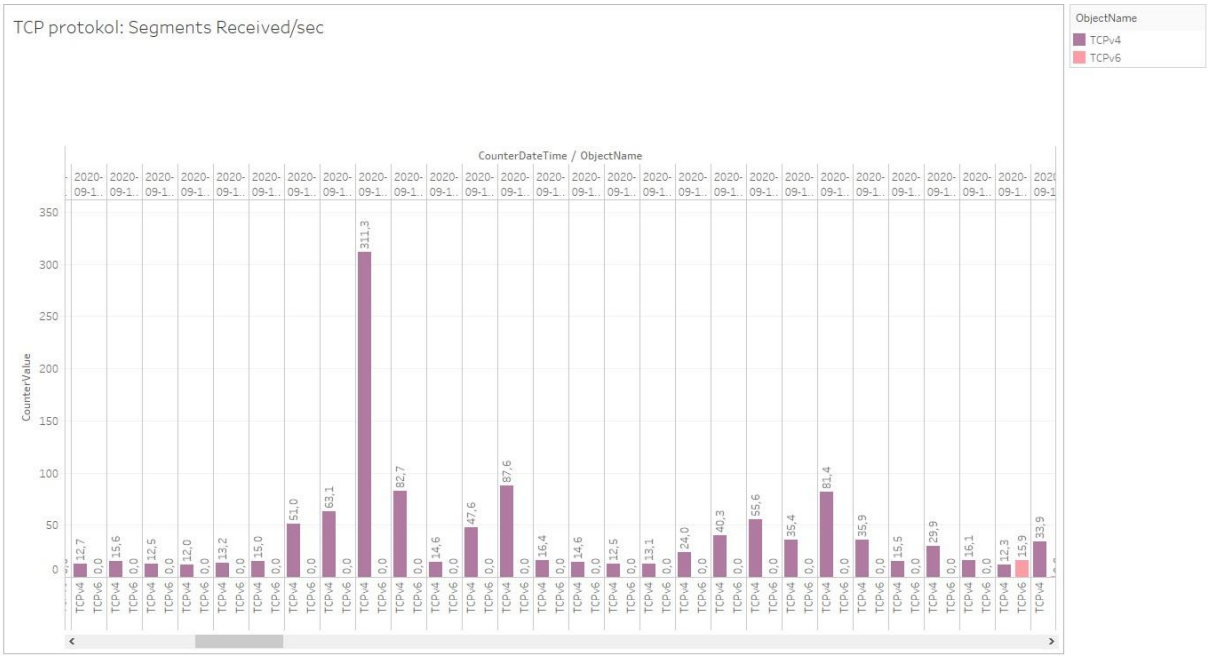
Slika 37: IP protokoli: Datagrams Received/sec

Na slici 37 su vizualizirani podatci dobiveni mjeriteljem performansi „Datagrams Received/sec“ za IP protokole četvrte i šeste verzije. Najveća vrijednost ovog mjeritelja se odnosila na IP protokol četvrte verzije i iznosila je 314.1. Velika razlika između najveće vrijednosti i ostalih vrijednosti predstavlja moguće postojanje uljeza unutar računalne mreže.



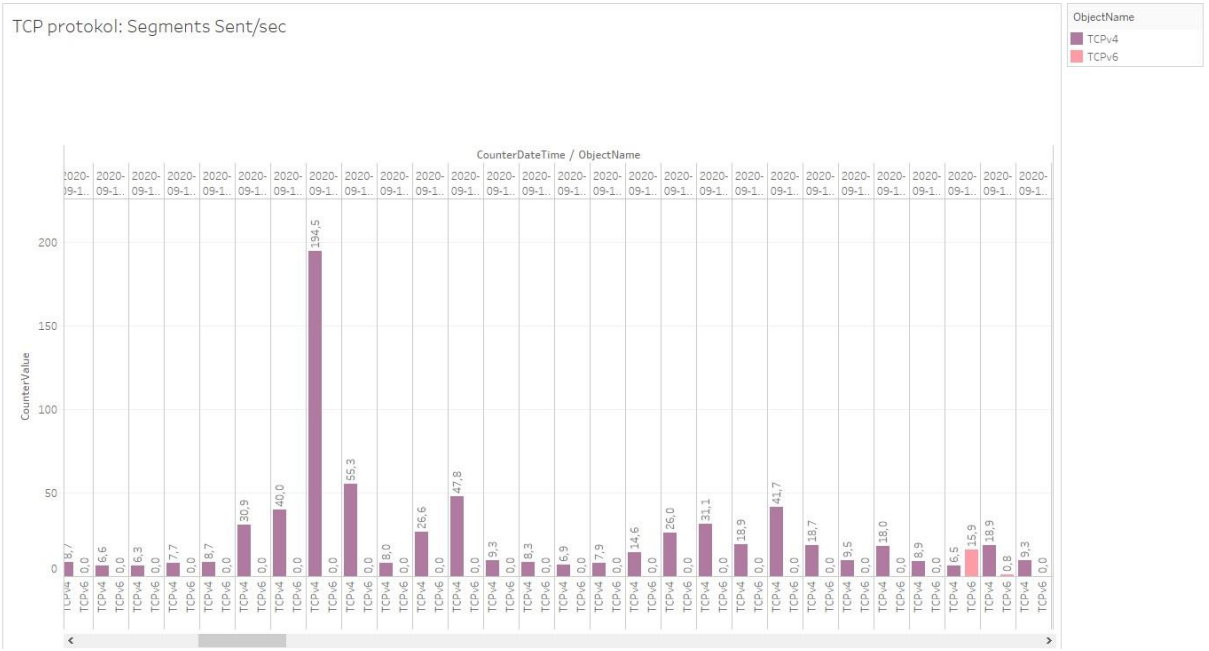
Slika 38: IP protokoli: Datagrams Sent/sec

Slikom 38 su vizualizirani podatci dobiveni mjeriteljem performansi „Datagrams Sent/sec“ koji je mjerio vrijednosti za IP protokole verzije četiri i šest. Prema napravljenom dijagramu u programu Tableau vidljivo je da je u isto vrijeme kada je bio skok primljenih datagrama kod IP protokola, je bio i skok poslanih datagrama.



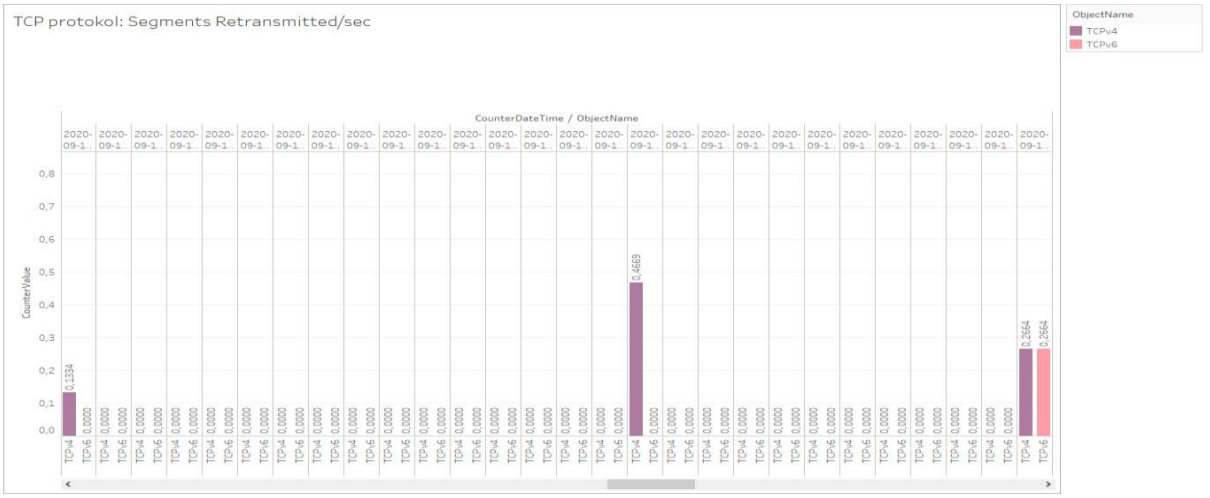
Slika 39: TCP protokoli: Segments Received/sec

Vizualizacija podataka prikazana 39. slikom predstavlja rezultat prikupljanja podataka putem mjeritelja „Segments Received/sec“ koji je prikupljao podatke za TCP protokole četvrte i šeste verzije. Temeljem ovih podataka vidljivo je nekoliko vrijednosti mjeritelja koje su znatno veće od većine ostalih dobivenih vrijednosti što bi moglo upućivati na postojanje uljeza na računalnoj mreži.



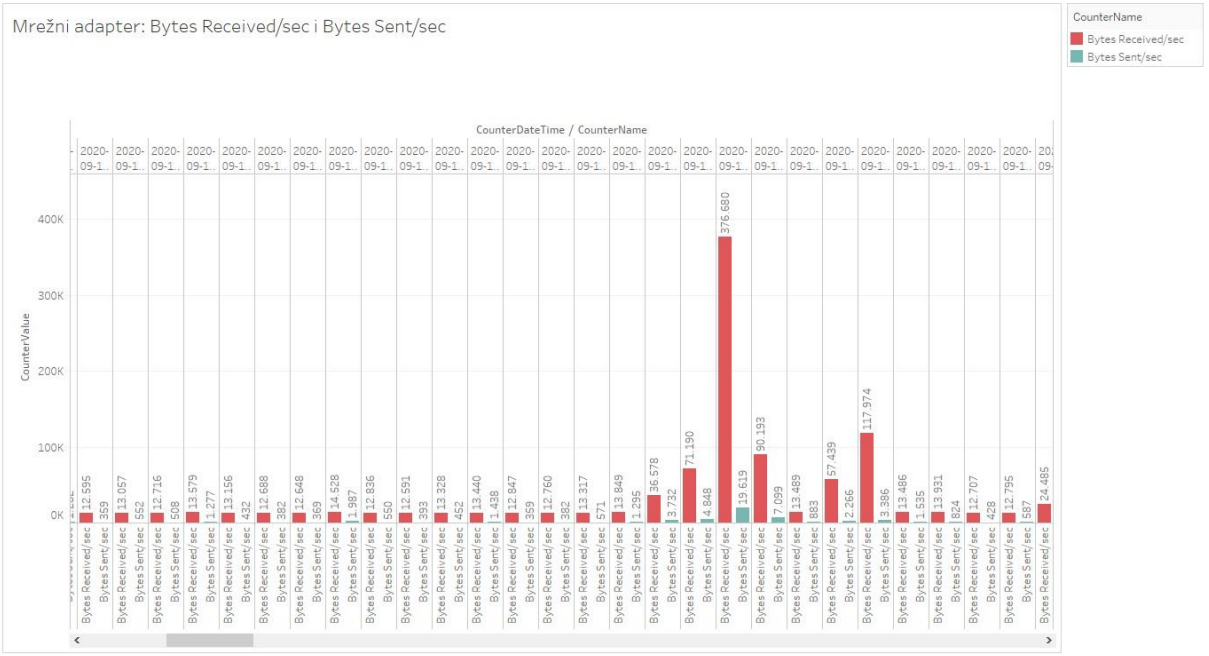
Slika 40: TCP protokoli: Segments Sent/sec

Vizualizacija vrijednosti dobivenih mjeriteljem „Segments Sent/sec“ je prikazana na slici 40 i predstavlja isti problem kao i kod IP protokola, u nekom vremenskom periodu je vrijednost mjeritelja puno veća od ostalih vrijednosti tog mjeritelja, što se događa i prilikom primanja i prilikom slanja segmenata. Ovaj problem bi mogao upućivati na postojanje uljeza.



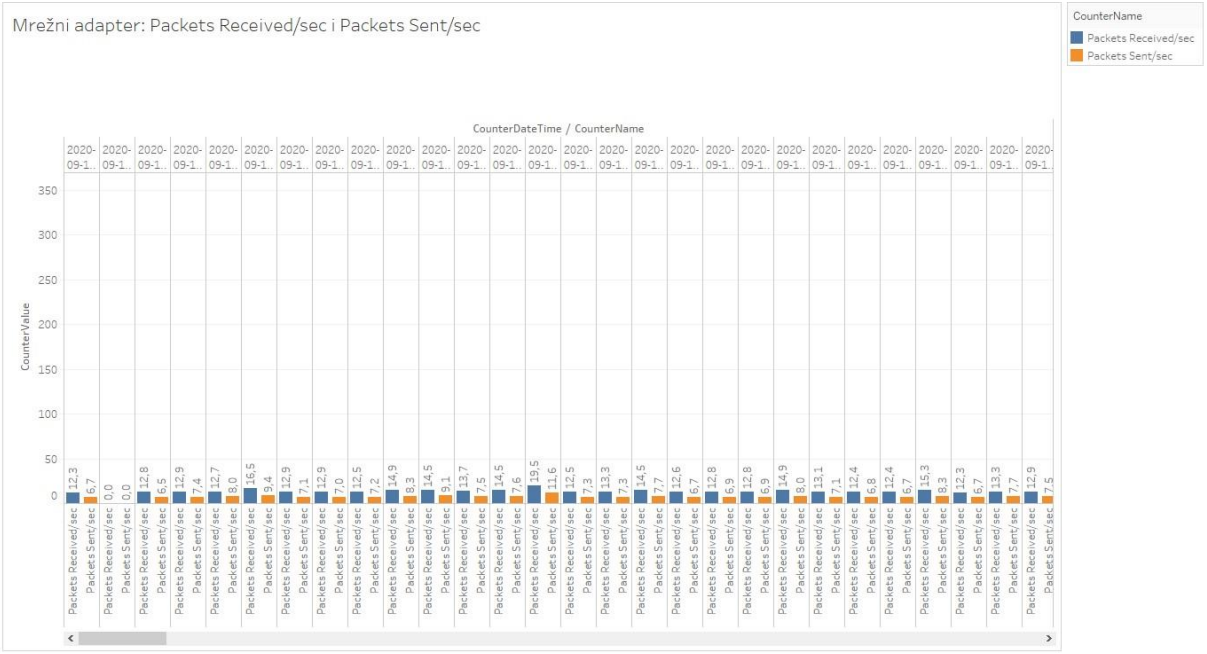
Slika 41: TCP protokoli: Segments Retransmitted/sec

Slika 41 vizualno prikazuje podatke dobivene mjeriteljem „Segments Retransmitted/sec“ na TCP protokole verzije četiri i šest. S obzirom da po pravilu broj ponovno poslanih paketa unutar vremenskog perioda ne bi trebao biti veći od nula, postojanje vrijednosti većih od nula u dobivenom skupu podataka znači da ili postoji problem s hardverskim dijelovima mreže ili da na mreži postoji potencijalni uljez.



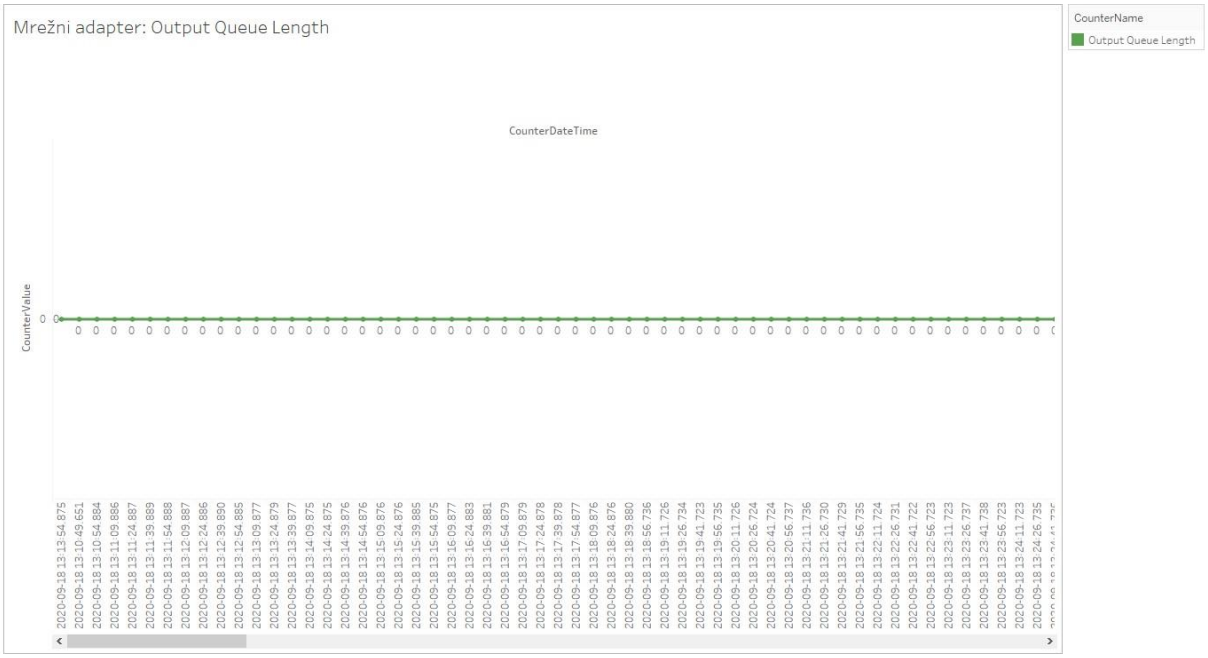
Slika 42: Mrežni adapter: Bytes Received/sec i Bytes Sent/sec

Slika 42 vizualno prikazuje podatke dobivene mjeriteljima „Bytes Received/sec“ i „Bytes Sent/sec“ za mrežni adapter. Ovakvi veliki skokovi u vrijednostima mjeritelja povezani su sa skokovima u vrijednosti mjeritelja za IP i TCP protokole i ukazuju na potencijalne probleme sa hardverskim dijelovima mreže ili na potencijalno postojanje uljeza u mreži.



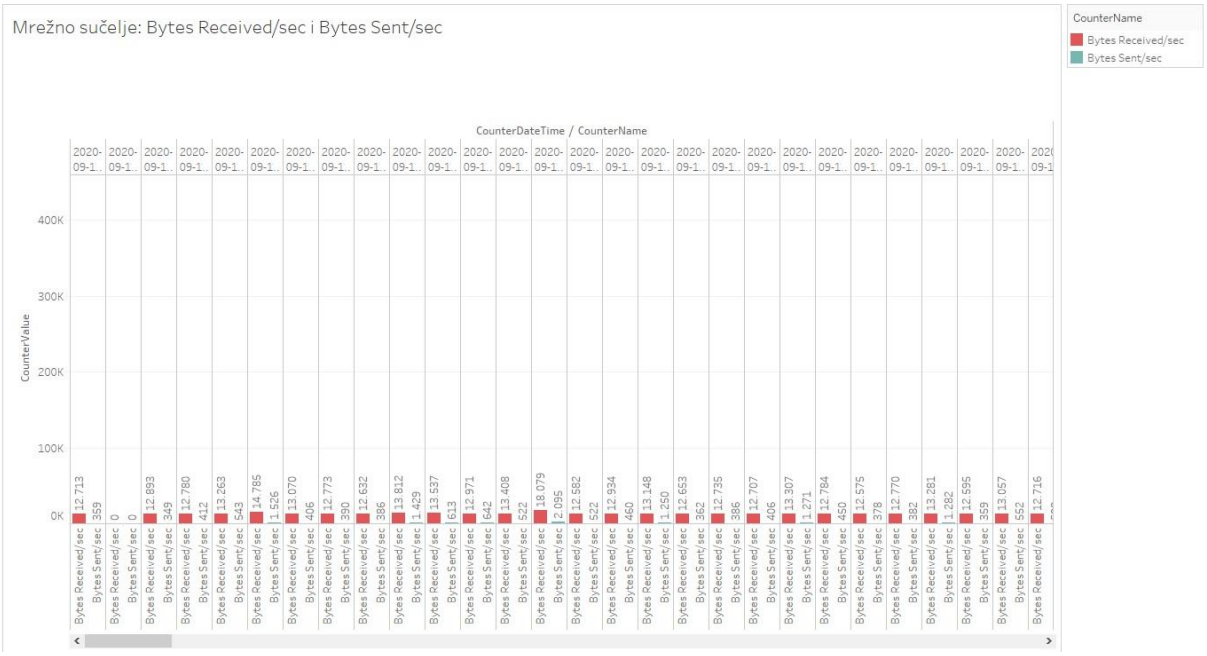
Slika 43: Mrežni adapter: Packets Received/sec i Packet Sent/sec

Vizualizacija dijela podataka dobivena mjeriteljima „Packets Received/sec“ i „Packet Sent/sec“ za mrežni adapter prikazana je na slici 43. Prema svim dobivenim podatcima od ovih mjerila je vidljivo da postoji nekoliko skokova u vrijednosti koji su veći od većine vrijednosti za ova mjerila, što se poklapa u vrijednosnim skokovima mjerila za IP i TCP protokole i mjerilima za broj primljenih i poslanih bajtova preko mrežnog adaptera.



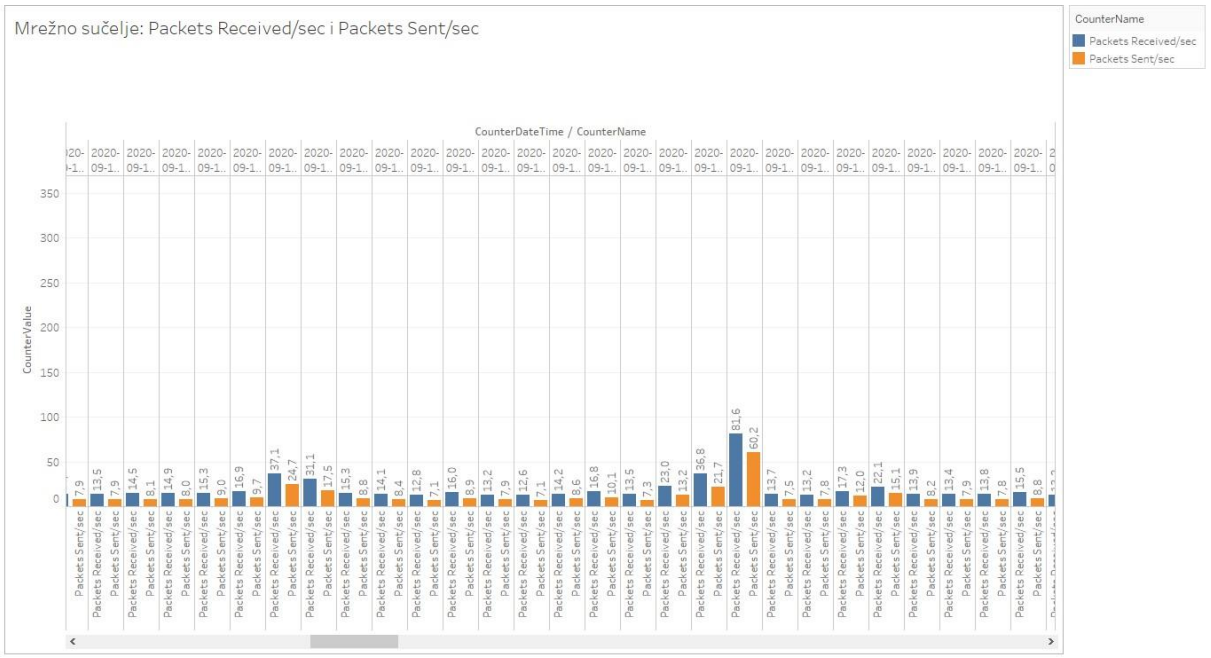
Slika 44: Mrežni adapter: Output Queue Lenght

Mjeriteljem performansi „Output Queue Lenght“ za mjerne adaptere dobivena je vrijednost 0 kod svih vremenskih perioda u kojima su se mjerile performanse što je vidljivo i na slici 44. Vrijednost 0 kod svih vremenskih perioda znači da ne postoji red čekanja kod slanja paketa s adaptera.



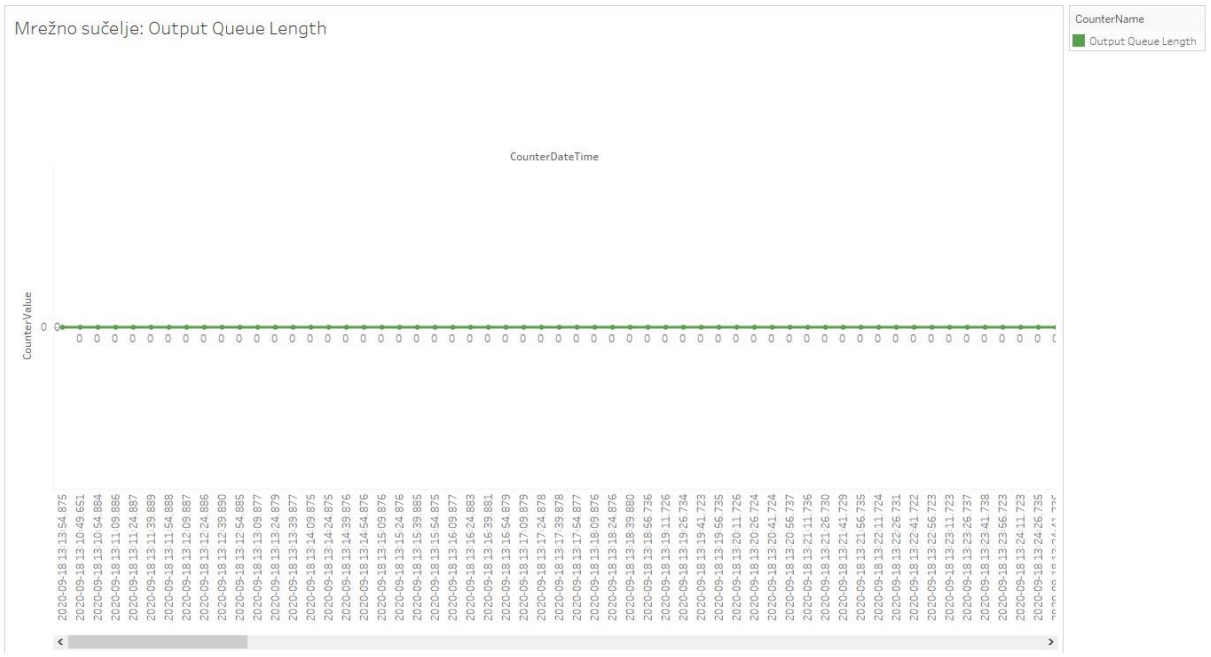
Slika 45: Mrežno sučelje: Bytes Received/sec i Bytes Sent/sec

Slika 45 prikazuje vizualizaciju podataka dobivenih od strane mjeritelja performansi Bytes Received/sec i Bytes Sent/sec, koji su u ovom slučaju mjerili podatke za mrežno sučelje. Kod mrežno sučelja postoje razlike u vrijednostima broja primljenih i poslanih bajtova ali vrijednosti tih skokova nisu drastično velike u odnosu na ostale vrijednosti.



Slika 46: Mrežno sučelje: Packets Received/sec i Packet

Podatci koji su za mrežno sučelje dobiveni od mjeritelja „Packets Received/sec“ i „Packets Sent/sec“ su vizualizirani na slici 46. Vidljivo je da su vrijednosti mjeritelja ujednačene osim nekoliko malih skokova.



Slika 47: Mrežno sučelje: Output Queue Lenght

Slika 47 prikazuje podatke dobivene mjeriteljem Output Queue Lenght za kriterij mrežnog sučelja. Za ovo mjerilo važno je napomenuti da su mu sve vrijednosti bile jednake nuli što ukazuje da ne postoji red čekanja za izlazne pakete i da ne postoje kašnjenja.

7. Zaključak

Ovim radom objašnjen je pojam krajnjeg uređaja za koji se govori da predstavlja sve uređaje koji imaju IP adresu i mogu primiti podatke s drugih uređaja ili poslati podatke drugim uređajima, a za njih se također može reći da su sastavni dio računalne mreže jer predstavljaju čvorove koji se nalaze unutar nje. Uz objašnjenje što je to krajnji uređaj navedeni su i brojni primjeri takvih uređaja kako bi se naglasile njihove važne osobine, raznolikost i svestranost, koje su im omogućile da svoju primjenu pronađu u raznim ulogama u privatnim, poslovnim, edukacijskim i drugim područjima ljudskog života. Uz pojam krajnjeg uređaja bilo je potrebno i detaljnije objasniti pojam računalne mreže zbog toga što su ta dva pojma usko povezana. Povezanost računalnih mreža i krajnjih uređaja dovela je do misli o sigurnosti računalne mreže i sigurnosti korištenja krajnjih uređaja unutar njih. Uvidom u područje sigurnosti računalnih mreža došlo se do spoznaje o važnosti osiguravanja ponašanja zaposlenika unutar organizacija, jer baš ljudsko djelovanje, nenamjerno i namjerno zlonamjerno, uzrokuje najveći broj prijetnji sustavu. Ovime se dolazi do praćenja i mjerenja aktivnosti korisnika, koji svoje korijene vuku još iz 19. stoljeća i radnih listova. Mjerenje aktivnosti korisnika na krajnjem uređaju se može izvoditi prema mnogobrojnim metodama, a neke od metoda su nabrojane i opisane u ovom radu. Nakon prolaska kroz teorijski dio, unutar praktičnog dijela rada su odabrani mjeritelji na temelju kojih će se mjeriti aktivnosti korisnika, a nakon njihovog odabira su pomoću njih prikupljeni podatci. Prema dobivenim podatcima je napravljena baza podataka koja je potom korištena za vizualizaciju i analiziranje dobivenih podataka. Za vrijeme vizualizacije i analize podataka autor ovog rada je zaključio da ima potencijalne probleme sa diskovnim sustavom i mrežnim resursima.

8. Popis literature

[1] J. Deming Burnham, „A Simple Definition: What is an 'Endpoint'?“, 2015. [Na internetu]. Dostupno: https://www.druva.com/blog/simple-definition-endpoint/ [pristupano 24.6.2020.].

[2] S. Rai, P. Chukwuma, „Beginning at the endpoint: faced with an ever changing mix of new technologies, auditors should make these devices the starting point in security reviews“, 2010. [Na internetu]. Dostupno: https://go.gale.com/ps/anonymous?id=GALE%7CA229068995&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=00205745&p=AONE&sw=w [pristupano 2.7.2020.].

[3] M. Kadrich, Endpoint Security. Boston, MA, USA: Pearson Education, Inc. 2007

[4] M. J. Bach, The design of the UNIX operating system. Englewood Cliffs, NJ, USA: Prentice- Hall, Inc. 1986.

[5] M. Maxfield, „Securing Embedded and IoT Devices from Endpoint to Cloud“, 2020. [Na interneru]. Dostupno: https://www.embedded-computing.com/guest-blogs/securing-embedded-and-iot-devices-from-endpoint-to-cloud [pristupano 2.7.2020.].

[6] M. U. Farooq, M. Waseem, S. Mazhar, A. Khairi, T. Kamal, „A Review on Internet of Things (IoT)“, International Journal of Computer Applications, sve. 113, izd. 1, ožu. 2015, [Na internetu]. Dostupno:

https://www.researchgate.net/publication/273693976_A_Review_on_Internet_of_Things_IoT [pristupano 21.7.2020.].

[7] M. Karch, „What Is Android?“, 2019. [Na internetu]. Dostupno:

https://www.lifewire.com/what-is-google-android-1616887 [pristupano 21.7.2020.].

[8] N. L. Beddall-Hill, A. Jabbar, S. Al Shehri, „Social Mobile Devices as Tools for Qualitative Research in Education: iPhones and iPads in Ethnography, Interviewing, and Design-Based Research“, sve. 7, izd. 1, str. 67-89, proljeće 2011, [Na internetu]. Dostupno:

http://eprints.hud.ac.uk/id/eprint/10507/ [pristupano 22.7.2020.].

[9] J. Šehanović, Ž. Hutinski, M. Žugaj, Informatika za ekonomiste. Pula, Republika Hrvatska: Sveučilište u Rijeci, Fakultet ekonomije i turizma dr. Mijo Mirković. 2002

[10] J. M. Kizza, Computer Network Security. New York, NY, USA: Springer Science+Business Media, Inc. 2005

[11] S. Bourgeois, „“11 Types of Networks Explained: VPN, LAN & More“, 6.10.2016. [Na internetu]. Dostupno: https://www.belden.com/blog/smart-building/network-types [pristupano 9.9.2020.].

[12] K. Pandya, „Network Structure or Topology“, sve. 1, izd. 2, srp. 2013, [Na internetu]. Dostupno: https://www.academia.edu/4185670/Network_Structure_or_Topology [pristupano 10.9.2020.].

[13] O. Bonaventure, „Computer Networking: Principles, Protocols and Practice“, 30.lis.2011. [Na internetu]. Dostupno: https://resources.saylor.org/wwwresources/archived/site/wp-content/uploads/2012/02/Computer-Networking-Principles-Bonaventure-1-30-31-OTC1.pdf [pristupano 11.9.2020.].

[14] EC-Council, „What is network security? Types of network security“, 24.ožu.2020. [Na internetu]. Dostupno: https://blog.eccouncil.org/what-is-network-security-types-of-network-security/ [pristupano 11.9.2020.].

[15] J. M. Kizza, Guide to Computer Network Security. London, England, United Kingdom: Springer-Verlag. 2015

[16] T. English, „What is Cryptography?“, 9. velj. 2020. [Na internetu]. Dostupno: https://interestingengineering.com/what-is-cryptography [pristupano 11.9.2020.].

[17] E. Dosal, „What is a Firewall“ The Different Firewall Types & Architectures“, 26. stud. 2019. [Na internetu]. Dostupno: https://www.compuquip.com/blog/the-different-types-of-firewall-architectures [pristupano 11.9.2020.].

[18] N. K. Kottayil, „Central Processing Unit (CPU)“, 14. kol. 2020. [Na internetu]. Dostupno: https://www.techopedia.com/definition/2851/central-processing-unit-cpu [pristupano 14.9.2020.].

[19] A. Cote, „What is a Timesheet?“, 4. pros. 2019. [Na internetu]. Dostupno: https://www.paymoapp.com/blog/what-is-a-timesheet/ [pristupano 15.9.2020.].

[20] N. Lord, „What is User Activity Monitoring? How it Works, Benefits, Best Practices, and More“, 12. ruj. 2018. [Na internetu]. Dostupno: https://digitalguardian.com/blog/what-user-activity-monitoring-how-it-works-benefits-best-practices-and-more#:~:text=User%20activity%20monitoring%20helps%20to,needed%20to%20improve%20security%20measures. [pristupano 15.9.2020.].

[21] sumo logic, „Log Analysis“ [Na internetu]. Dostupno: https://www.sumologic.com/glossary/log-analysis/ [pristupano15.9.2020.].

[22] C. Brook, „What is Deep Packet Inspection? How It Works, Use Cases for DPI, and More“, 5. pros. 2018. [Na internetu]. Dostupno: https://digitalguardian.com/blog/what-deep-packet-inspection-how-it-works-use-cases-dpi-and-more [pristupano 15.9.2020.].

[23] Kaspersky, „What is Keystroke Logging and Keyloggers?“. [Na internetu]. Dostupno: https://www.kaspersky.com/resource-center/definitions/keylogger [pristupano 15.9.2020.].

[24] AfterAcademy, „What is Kernel in Operating System and what are the various types of Kernel?““, 11. stud. 2019. [Na internetu]. Dostupno: https://afteracademy.com/blog/what-is-kernel-in-operating-system-and-what-are-the-various-types-of-kernel [pristupano 15.9.2020.].

[25] J. Simon, „4 Kinds of Screenshots You Need to Start Using Immediately“. [Na internetu]. Dostupno: https://www.techsmith.com/blog/4-screenshots-start-using-immediately/ [pristupano 15.9.2020.].

[26] OpenRefine, alat za uređivanje podataka. [Na internetu]. Dostupno: https://openrefine.org/download.html [pristupano 17.9.2020.].

9. Popis slika