Udaljeno održavanje informacijsko-komunikacijskih sustava

Mlinar, Antun

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 6. travnja 2020.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Računalne mreže**

ZAVRŠNI ZADATAK br. 5774

Pristupnik: **Antun Mlinar (0135245503)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Udaljeno održavanje informacijsko-komunikacijskih sustava**

Opis zadatka:

U završnom radu analizirat će se problematika održavanja informacijsko-komunikacijskih sustava. Opisat će se značajke udaljenog održavanja informacijsko-komunikacijskih sustava. Analizirat će se programski alati za udaljeno održavanje informacijsko-komunikacijskih sustava i sigurnost udaljenog održavanja informacijsko-komunikacijskih sustava. Navest će se primjena udaljenog održavanja informacijsko-komunikacijskih sustava.

Mentor:

doc. dr. sc. Ivan Grgurević

Predsjednik povjerenstva za završni ispit:

Sveučilište u Zagrebu

Fakultet prometnih znanosti

ZAVRŠNI RAD

UDALJENO ODRŽAVANJE INFORMACIJSKO-KOMUNIKACIJSKIH SUSTAVA

REMOTE MAINTENANCE OF INFORMATION AND COMMUNICATION SYSTEMS

Mentor: Doc. dr. sc. Ivan Grgurević, dipl. ing.

Student: Antun Mlinar, 0135245503

Zagreb, rujan 2020.

UDALJENO ODRŽAVANJE INFORMACIJSKO-KOMUNIKACIJSKIH SUSTAVA

SAŽETAK

U današnje vrijeme nezamislivo je voditi tvrtku bez informacijskog sustava. Napretkom tehnologije mnoge prednosti proizlaze iz korištenja Interneta i svega što ga sačinjava. U završnom radu obrađuje se termin udaljenog održavanja koji omogućuje vođenje velikog sustava s jednog mjesta koristeći određeni terminalni uređaj. Objašnjene su značajke udaljenog pristupa u funkciji održavanja informacijsko-komunikacijskog sustava, te kako je omogućeno pojednostavljenje poslovanja uz prateće sigurnosne aspekte koji pružaju poslovanju pouzdanost i efektivnost. U radu su opisani programski alati koji se koriste za udaljeno održavanje, te je prikazano kakvu primjenu takvi sustavi imaju u današnjici.

KLJUČNE RIJEČI: Informacijsko-komunikacijski sustav; udaljeno održavanje; udaljeni pristup; korisnik; usluga

REMOTE MAINTENANCE OF INFORMATION AND COMMUNICATION SYSTEMS

SUMMARY

Nowadays, it is unthinkable to run a company without an information system. With the advancement od technology, many advantages come from using the Internet and everything that makes it up. The final paper deals with a remote maintenance that allows the management of a large system from one place using one terminal device. The features of remote access are explained in the function of maintaining information and communication system, as well as how business simplification is enabled with a corresponding security aspects that provide business with reliability and efficiency. The paper describes program tools that implement the use of maintenance services and it can be seen what is the use of those services today.

KEYWORDS: Information-communication systems; remote maintenance; remote access; user; service

Sadržaj

1. UVOD

Udaljeno održavanje informacijsko-komunikacijskih sustava je zahvaljujući brzom napretku tehnologije postalo jedan od osnovnih načina održavanja i vođenja različitih sustava. Brojne su prednosti koje udaljeno održavanje omogućava poslovanju. Znatno smanjenje troškova popravaka, dijagnostike i održavanja stvorili su novu granu upravljanja tehnologijom koja je svoju primjenu pronašla u brojnim tvrtkama. Mnogi su načini korištenja usluge udaljenog održavanja. Pretežito pronalazi svrhu u sustavima s velikim brojem osjetljivih uređaja kojima je potrebno redovito održavanje kako bi bili što efektivniji i pouzdaniji.

Svakim danom svjedoči se sve većem broju napada na informacijske sustave, kako u Hrvatskoj tako i u svijetu. Pravilnim vođenjem poslovanja udaljenog održavanja takvi se slučajevi pokušavaju svesti na minimum korištenjem ažuriranih aplikacija i svođenja na što detaljnije autentifikacije korisnika. Uočeno je da je stav korisnika prema terminu udaljenog pristupa računalu dosta skeptičan jer se osoba s pristupom u osobno računalo fizički ne može vidjeti.

Cilj završnog rada je prikazati načine korištenja usluge udaljenog pristupa, istaknuti načine pravilne uporabe u svrhu prevencije od mogućih problema poput krađe podataka, krađe identiteta i nedozvoljenog pristupa udaljenim računalima. Također je objašnjen aspekt sigurnosti takvih sustava. Svrha završnog rada je predočiti prednosti koje donosi korištenje udaljenog održavanja informacijsko-komunikacijskih sustava na poslovanje tvrtki. Promjene u vođenju poduzeća/tvrtki koristeći takvu uslugu mogu biti značajne za uspjeh poslovanja.

Završni rad je podijeljen na sedam (7) logičko povezanih cjelina:

1. Uvod
2. Problematika održavanja informacijsko-komunikacijskih sustava
3. Značajke održavanja informacijsko-komunikacijskih sustava
4. Programski alati za održavanje informacijsko-komunikacijskih sustava
5. Sigurnost udaljenog održavanja informacijsko-komunikacijskih sustava
6. Primjena udaljenog održavanja informacijsko-komunikacijskih sustava
7. Zaključak

U uvodnom poglavlju se upoznaje čitatelja s temom završnog rada. Prikazuje se struktura rada, te njena svrha i cilj.

U drugom poglavlju navedeni su osnovni pojmovi za bolje shvaćanje rada. Objašnjava se termin udaljenog održavanja te je iznesena problematika usluge udaljenog održavanja.

U trećem poglavlju je opisan način funkcioniranja udaljenog održavanja. Opisano je kojim se prijenosnim medijima može ostvariti, te s kojim sigurnosnim protokolima se omogućuje pouzdano slanje podataka kroz mrežu. Također se raščlanilo udaljeno održavanje na četiri osnovne funkcije koje omogućuju potpuno provođenje i definiranje usluge.

U četvrtom poglavlju prikazani su programski alati koji omogućuju uslugu udaljenog održavanja. Programski alati se prvenstveno odnose na vođenje i kontroliranje većeg broja različitih uređaja, a omogućavaju sustavni pregled nedostataka i potrebnih ažuriranja uređaja u mreži.

Petim poglavljem je objašnjen sigurnosni aspekt vođenja i korištenja usluga udaljenog održavanja. Opisana je sigurnost iz aspekta poslovanja i sigurnost iz aspekta mogućih prijetnji s Interneta.

U šestom poglavlju izneseni su primjeri (tvrtki) koji unutar svog poslovanja koriste udaljeno održavanje, dijagnostiku i/ili popravljanje. Na primjerima je objašnjen način korištenja takvih usluga.

U zaključnom poglavlju iznesena je trenutna situacija i mogućnosti razvoja korištenja usluge udaljenog pristupa te su komentirani čimbenici koji su utjecali na porast broja korisnika udaljenog održavanja.

2. PROBLEMATIKA ODRŽAVANJA INFORMACIJSKO-KOMUNIKACIJSKIH SUSTAVA

Problematika udaljenog održavanja informacijsko-komunikacijskih sustava je u tome što korisnicima takvih usluga pristup nepoznatih ljudi koji su fizički udaljeni predstavlja nepovjerenje u sigurnosnom aspektu. Kako bi se uopće počela razmatrati problematika održavanja informacijsko-komunikacijskih sustava, potrebno je prvo definirati osnovne pojmove i dijelove sustava.

2.1. Osnovni pojmovi

Za shvaćanje pojma informacijski sustav, prvo je potrebno definirati što je sam sustav. Sustav je uređen skup od više elemenata koji zajedno čine cjelinu. Elementi komuniciraju međusobno preko sučelja. Razlikujemo zatvorene i otvorene sustave. Za razliku od otvorenih, zatvoreni ne razmjenjuju informacije, energiju i materiju sa svojim okruženjem. Svaki sustav je podsustav nekog većeg sustava. Okruženje u kojem se sustavi nalaze zove se okolina, te se sustavi podvrgavaju promjenama kako bi bili sukladni s okolinom. Na slici 1. nalazi se poopćeni prikaz sustava i na koja sve pitanja sustav daje odgovor, [1].

Slika 1. Opći model sustava, [1]

Informacijski sustav je dio nekog tehnološkog i/ili organizacijskog stvarnog sustava čija je svrha opskrbljivanje potrebnim informacijama svih razina njegovog upravljanja i odlučivanja. Sastoji se od skupine postupaka koji djeluju zajedno kao

jedna koherentna cjelina da bi izvršio određen zadatak. Provodi svoje temeljne aktivnosti poput prikupljanja, obrade, pohranjivanja i distribucije informacija. Na tablici 1. prikazani su ciljevi informacijskog sustava koji su različiti za različite radne razine, [1].

Tablica 1. Ciljevi informacijskog sustava

Razina funkcija organizacijskog sustava	Cilj informacijskog podsustava
IZVOĐENJE procesi osnovne djelatnosti	povećanje **produktivnosti** rada
UPRAVLJANJE razina odgovorna za organiziranje, praćenje uspješnosti, otklanjanje smetnji	povećanje **učinkovitosti**
ODLUČIVANJE razina odgovorna za postavljanje poslovnih ciljeva	osiguranje **stabilnosti** rasta i razvoja

Izvor: [1]

Postoji više vrsta informacijskih sustava ovisno o različitim kriterijima podjele. Osnovne podjele su prema konceptualnom ustroju poslovodstva, prema modelu poslovnih funkcija u poslovnom sustavu i prema namjeni. Prema konceptualnom ustroju informacijski sustavi se dijele na:

- Sustav potpore odlučivanju – Strateški nivo ustroja;
- Izvršni informacijski sustav – Taktički nivo ustroja i
- Transakcijski sustavi – Operativni nivo, [1].

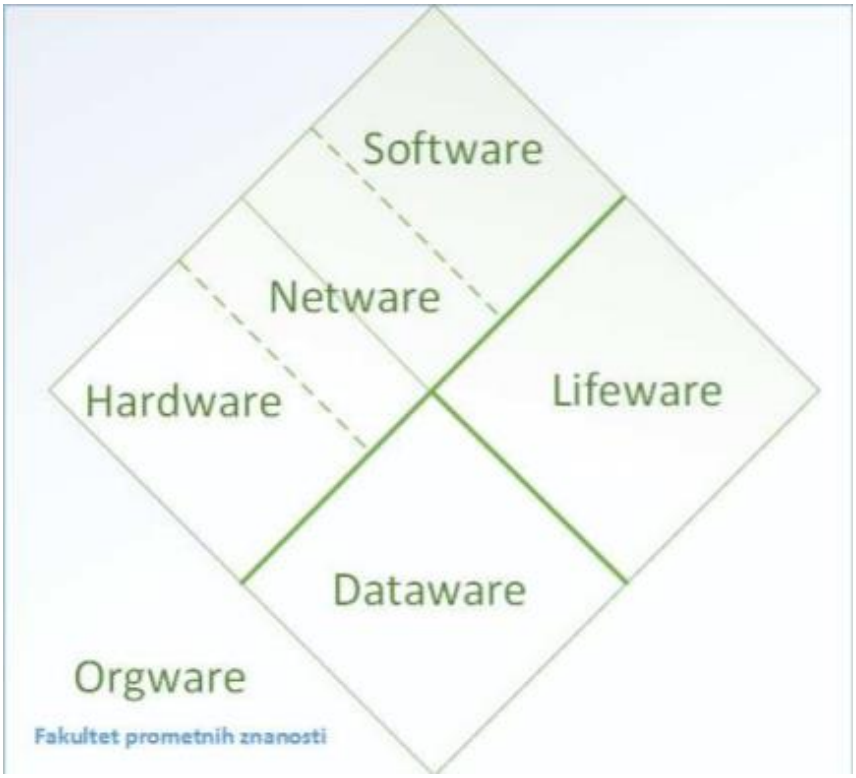
Prema modelu poslovnih funkcija informacijski sustavi se dijele na:

- Operativne sustave;
- Potporne sustave;
- Strateške sustave i
- Izgledne sustave, [1].

Prema namjeni informacijske sustave dijelimo na:

- Sustave obrade podataka - unos, obrada i pohranjivanje;
- Sustave podrške uredskom radu - administrativni poslovi i ljudsko komuniciranje;

- Sustave podrške u odlučivanju - informacije za odlučivanje, podrška pojedincu i grupi te
- Ekspertne sustave - podrška stručnjacima i ekspertima za rješavanje problema, [1].



Slika 2. Osnovni elementi informacijskog sustava, [1]

Osnovni elementi informacijskog sustava su:

- *Hardware* - fizička komponenta koja čini materijalnu osnovicu računala;
- *Software* - skup programa koji upravljaju računalom;
- *Orgware* - organizacijski dio računala;
- *Lifeware* - oznaka za ljudski faktor u sustavu;
- *Netware* - označava komunikacijsko povezivanje elemenata i predstavlja hardversko - softversku komponentu;
- *Dataware* – organizacija baze podataka i informacijskih resursa, [1]

Slikom 2. prikazana je povezanost osnovnih elemenata informacijskog sustava čija je kvalitetna interakcija uzrok ostvarivanja ciljeva sustava.

Komunikacijski sustav je sustav koji opisuje razmjenu informacija između dvije točke. Proces prijenosa i primanja informacija naziva se komunikacija. Glavni elementi komunikacije su odašiljač informacija, prijenosni medij komunikacije i prijamnik informacija. Dva osnovna načina prijenosa podataka komunikacijskim sustavom su analogni i digitalni prijenos.

Informacijsko-komunikacijski sustav služi za prikupljanje, obradu, memoriranje i distribuciju informacija, te njihovu razmjenu između dvije točke. Takav sustav se sastoji od povezanog i organiziranog skupa ljudi, programa, metoda i drugih elemenata radi obavljanja informacijske aktivnosti, [2].

2.2. Udaljeno popravljanje, dijagnostika i održavanje sustava

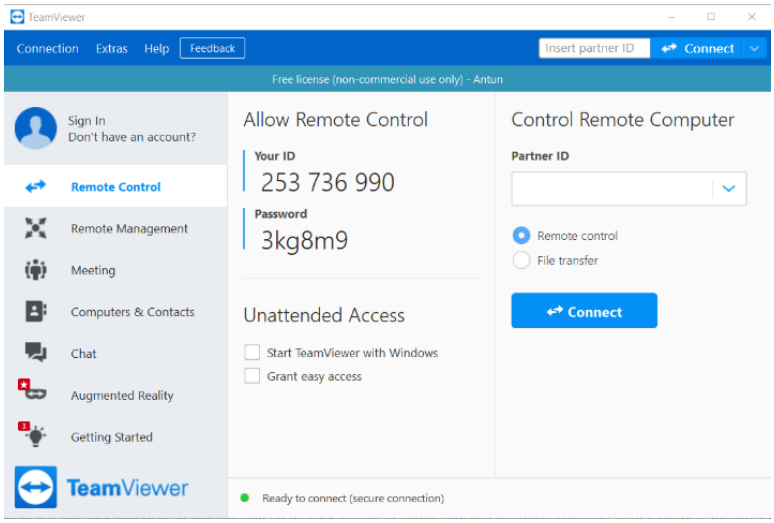
U prošlosti se vođenje sustava izvodilo većinom fizički, to jest inženjeri su popravke tehnologije i vođenje sustava obavljali ručno pri čemu se dosta novaca i vremena trošilo na putovanja. Razvojem tehnologije dolazi do masovnog korištenja Interneta u svrhu poslovanja tvrtki što je rezultiralo razvojem udaljenog popravljanja, dijagnostike i održavanja sustava (engl. *Remote repair, diagnostics and maintenance* – RRDM).

RRDM je termin koji obuhvaća razne tehnologije i aplikacije. To može biti od običnog telefonskog poziva preko kojeg se navodi osobu kako ukloniti kvar na uređaju, pa sve do integriranih računalnih i mrežnih aplikacija koji nadziru sustav, te alarmiraju tehničare ukoliko dođe do kvara. Proizvođači uređaja i tvrtke koje pružaju mrežne usluge mogu značajno profitirati korištenjem RRDM-a kao uslužnog alata, [3].

2.2.1. Udaljeno popravljanje

Udaljeno popravljanje je moguće izvršiti putem poziva gdje se razgovorom korisnika navodi na rješavanje problema ili putem povezivanja na Internet gdje tehničar ima pristup terminalnom uređaju koji je u kvaru. Ukoliko je problem jednostavan koristi se navođenje korisnika, no ukoliko je problem kompleksniji onda je potrebno instalirati

program poput *TeamViewer*-a[1] uz prethodno autoriziranje lozinkom. Svrha udaljenog popravljanja također može biti nadograđivanje sustava i ažuriranje istog u svrhu boljeg poslovanja korisnika, [4].



Slika 3. Povezivanje uređaja korištenjem alata *TeamViewer*

Slikom 3. prikazano je povezivanje klijenta i tehničara korištenjem alata *TeamViewer*. Takav alat daje potpuni pristup tehničaru u korisnički uređaj, pri čemu klijent može na svom ekranu nadzirati što točno tehničar izvodi na njegovom računalu. Ovakav oblik davanja udaljenog pristupa je siguran jer zahtjeva tehničara identifikacijski broj i šifru koji su generirani na korisnikovom računalu, te bez korisnikove suradnje tehničar ne može udaljeno pristupiti tuđem uređaju, [5].

2.2.2. Udaljena dijagnostika

Udaljena dijagnostika[2] je trend koji je usko povezan s razvojem IoT (engl. *Internet of Things*) infrastrukture. IoT je baziran na samostalnom funkcioniranju uređaja na rubu mreže koji senzorima generiraju podatke iz ljudske svakodnevnice. Najkorišteniji termin IoT-a je termin pametne kuće[3] koja unaprjeđuje život uporabom

[1] *TeamViewer* – programski alat / *softver koji* omogućuje tehničaru potpuni pristup svim programima na udaljenom računalu
[2] Udaljena dijagnostika – omogućuje pronalazak kvara na uređaju udaljenim načinom
[3] Pametna kuća (engl. *Smart House*) – pojam kuće kao jedinstvenog integriranog sustava pomoću napredne tehnologije

tehnologije. Takvi senzori imaju dug životni vijek zbog svoje jednostavnosti i male potrebe za napajanjem, no kvarovi su uvijek mogući što se najlakše kontrolira korištenjem udaljene dijagnostike nad krajnjim uređajima kako bi se omogućila pouzdanost sustava. Najveći problem poslovanja nastaje ukoliko kvar zahvati više sustava. Bez kvalitetno implementirane udaljene dijagnostike, takav problem može biti skup i dugotrajan što može kobno naštetiti poslovanju, [6].

Osim u IoT infrastrukturi, udaljena dijagnostika je postala bitan čimbenik u auto industriji. Moderna vozila imaju u sebi ugrađena računala koja bilježe sve podatke što se događa unutar vozila. Ti podaci se koriste kao izvor znanja o kvaliteti i ispravnosti vozila, te se još nazivaju dijagnostika vozila. Obično su dostupni samo proizvođaču vozila, no korištenjem odgovarajuće opreme moguće je preuzeti te podatke bez potrebe za odlaskom u radionicu što se naziva udaljeno održavanje vozila. Svrha te funkcije je predviđanje kvarova u svrhu jednostavnijeg popravka i izbjegavanja nesreća. Ukoliko je vozač upućen u moguće kvarove u bližoj budućnosti ima vremena preduhitriti neželjeni kvar, [6].

Slika 4. Udaljena dijagnostika u vozilima

Izvor: [7]

Slikom 4. prikazane su funkcije vozila koje je moguće pratiti udaljenom dijagnostikom što je bitna funkcija za tvrtke koje se primjerice bave iznajmljivanjem i posjeduju veći broj vozila radi lakšeg kontroliranja kvarova i povećanja kvalitete usluge.

2.2.3. Udaljeno održavanje

Udaljeno održavanje se izvodi putem Interneta korištenjem virtualne privatne mreže (engl. *Virtual Private Network* – VPN). Dodatnu razinu sigurnosti omogućava vatrozid[4] integriran na uređaju koji održava sustav. Načini povezivanja uređaja s glavnim uređajem mogu biti putem lokalne mreže (engl. *Local Area Network* – LAN), bežične lokalne mreže (engl. *Wireless Local Area Network* – WLAN) i mobilnim mrežama UMTS (engl. *Universal Mobile Telecommunications System*) i LTE (engl. *Long Term Evolution*). Svrha udaljenog održavanja je s jednog mjesta pratiti, nadgledati i unaprjeđivati svaki element sustava. Koristi se pri vođenju velikih tvrtki koje se sastoje od velikog broja povezanih uređaja, dok ga nerijetko koriste i manje tvrtke u svrhu poboljšanja kvalitete poslovanja, [3].

Slika 5. Koraci uspostavljanja udaljenog održavanja

Izvor: [8]

[4] Vatrozid (engl. *Firewall*) – Vatrozid je mrežni sigurnosni uređaj koji nadzire dolazni i odlazni mrežni promet i dopušta ili blokira podatkovne pakete na temelju skupa sigurnosnih pravila.

Slikom 5. prikazan je najjednostavniji način korištenja usluge udaljenog održavanja. Prvenstveno je potrebno imati *hardversku* podlogu na kojoj je potrebno dizajnirati korisničko sučelje. Zatim konfiguracija upravitelja stranice (engl. *Site Manager*) koju je potrebno povezati s logičkim programskim upravljačem (engl. *Programmable Logic Controller* – PLC), te je sustav spreman za upotrebu putem Interneta.

Uvođenjem politike BYOD (engl. *Bring Your Own Device*), organizacije omogućuju korištenje privatnih uređaja za spajanje na poslovna područja. Takvim pristupom poslovanja podigla se produktivnost zaposlenika za 16 %. Problem korištenja takve politike je sigurnosni aspekt jer se na istom uređaju miješaju podaci osjetljivog značaja za tvrtku s privatnim podacima zaposlenika. To niti malo ne ide u prilog udaljenom održavanju jer uređaj koji se nadgleda ne koristi se više samo za poslovne svrhe, nego se nadgledanjem može narušiti zaposlenikova privatnost. Udaljeno održavanje se u globalu ne poklapa s politikom BYOD koja je u današnje vrijeme rastuća. I dalje mnogo tvrtki inzistira na odvajanju poslovnog i privatnog života, no korištenjem BYOD politike u doba buktajućeg rasta obavljanja posla od kuće, pristup udaljenog održavanja nailazi na prepreku.

3. ZNAČAJKE UDALJENOG ODRŽAVANJA INFORMACIJSKO-KOMUNIKACIJSKIH SUSTAVA

Generalno gledajući udaljeno održavanje informacijsko-komunikacijskih sustava je skup svih postupaka kojima je u cilju zadržavanje uređaja ili cijelog sustava u stanju u kojem može obavljati namijenjenu funkciju. Ti postupci se najviše odnose na rješavanje problema sustava i adaptacije na promjenu okoline. Održavanje se dijeli na:

- **Preventivno** održavanje – odnosi se na mogućnost djelovanja sustava na pogreške prije nego se one dogode;
- **Korektivno** održavanje – omogućavanje vraćanja oštećenih uređaja ili sustava u prvobitno stanje;
- **Aktualno** održavanje – ažuriranje uređaja ili sustava;
- **Adaptivno** održavanje – prilagođavanje softverskih komponenata na promjenu okoline, [9].

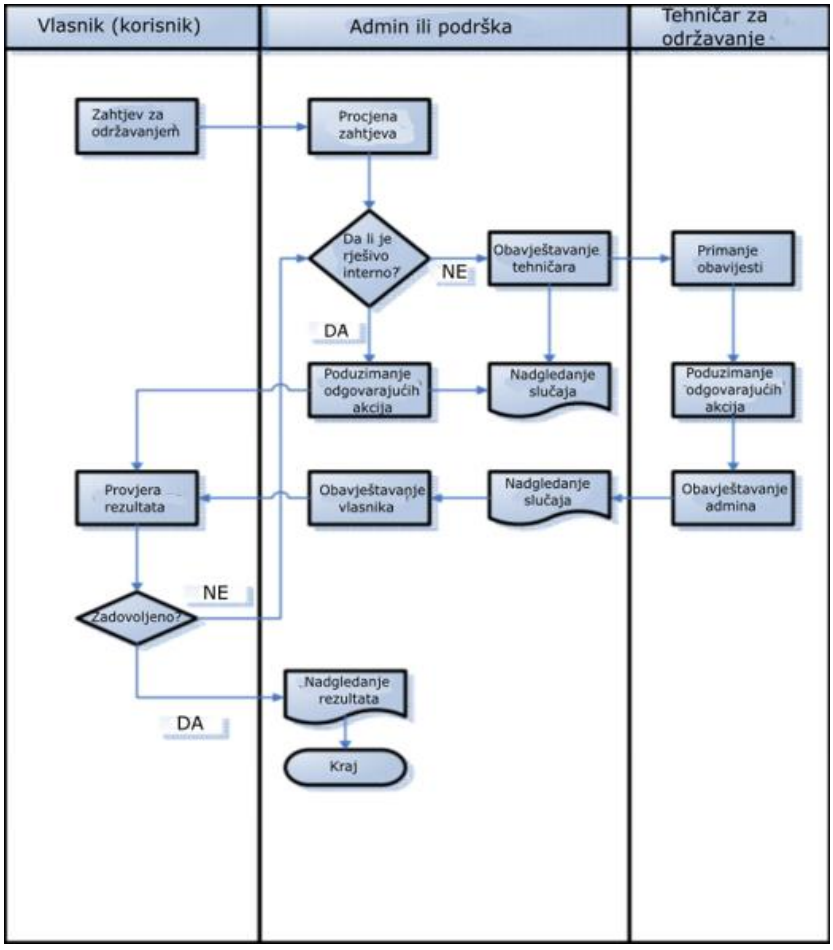
Preventivno i korektivno održavanje su dvije glavne stavke u očuvanju dostupnosti i performansi sustava. Troškovi preventivnog održavanja bi za idealno poslovanje trebali iznositi 4 %, a korektivnog poslovanja 21 % u odnosu na ukupne troškove udaljenog održavanja. Preventivno održavanje se koristi nakon što se novi softverski produkt implementira na sustav kako bi se uvidjele moguće greške i kvarovi, dok se korektivno održavanje koristi nakon što su greške već pronađene kako bi sustav i dalje nesmetano funkcionirao. Ključan faktor za sustav je vrijeme odziva podrške[5], [9].

Aktualno održavanje je dio uspješnog životnog ciklusa sustava. Odnosi se na sve nadogradnje izvan osnovnih specifikacija poput implementacije novih softverskih modula ili operativnih sustava kojima je cilj poboljšati funkcionalnost redefiniranjem, brisanjem i dodavanjem svojstava. Nekad je potreban i dodatni hardver koji mora moći popratiti ažuriranja softvera. Unatoč promjeni funkcioniranja sustava, aktualno održavanje također može promijeniti izgled sučelja što će biti prije zapaženo od strane korisnika nego neka promjena u samom kodu, te se radi toga korisnicima pruža

[5] Vrijeme odziva podrške – uklanjanje poteškoća u što kraćem vremenu.

mogućnost slanja povratne informacije i komuniciranje s dostupnom podrškom. Okvirni troškovi za ovaj oblik održavanja iznose 50 % u odnosu na ukupne troškove održavanja. Postotak je poprilično visok zbog toga jer aktualno održavanje zahtjeva uvođenje velikog broja noviteta u sustave, [9].

Adaptivno održavanje se pretežito koristi u institucijskim i tehničkim okruženjima jer su takva područja dinamično promjenjiva. Takav tip održavanja koristi *ad-hoc*[6] svojstva što znači da su telekomunikacijski sustavi povezani mrežom koja omogućuje direktno spajanje pri čemu se čvorovi ponašaju kao usmjerivač (engl. *router*). Troškovi za idealno poslovanje adaptivnog održavanja su okvirno 25 % u odnosu na sveukupne troškove udaljenog održavanja, [9].



Slika 6. Ad-hoc proces održavanja

Izvor: [9]

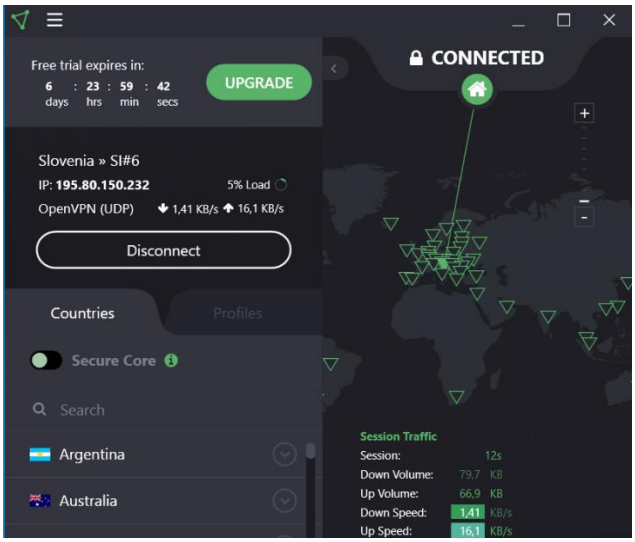
[6] *Ad-hoc* - sustavi su dizajnirani za specifične probleme ili zadatke, te se ne koriste u druge svrhe.

Primjer *ad-hoc* sustava je prikazan slikom 6. gdje se prikazuje tok komunikacije korisnika i podrške u svrhu rješavanja problema. Dva su moguća ishoda. Jedan je da je problem rješiv unutar okvira administratora ili podrške, dok je drugi ishod zahtijevanje tehničara za održavanje da pronađe način rješavanja problema. Razlika je u tome što se tehničarom za održavanje smatra cijela organizacija koja pruža usluge održavanja sustava što je zasnovano ugovorom.

3.1. Mrežne značajke

Udaljeno održavanje se postiže kombinacijom hardvera, softvera i mrežnog povezivanja. Tradicionalni daljinski pristup se ostvarivao pomoću softvera za emulaciju[7] terminala koji je kontrolirao pristup preko hardverskog modema povezanog na telefonsku mrežu. Danas se daljinski pristup ostvaruje putem Interneta sigurnijim softverskim rješenjima poput virtualne privatne mreže preko žičanog mrežnog ili bežičnog sučelja (engl. *Wireless Fidelity* – Wi-Fi). VPN stvara sigurnu kriptiranu konekciju preko manje sigurne mreže poput Interneta, tj. omogućava dvjema mrežama povezivanje preko mreže širokog područja (engl. *Wide Area Network* – WAN) pritom zadržavajući sigurnosne beneficije privatne mreže. VPN tehnologija je razvijena u svrhu omogućavanja udaljenim korisnicima prijavu na privatne mreže tvrtki da bi mogli pouzdano i sigurno koristiti aplikacije, podatke i ostale resurse. Način na koji VPN osigurava komunikaciju je taj što se korisnikov promet kriptira prije nego što se dostavi na Internet. VPN server, koji je lociran na rubu ciljane mreže dekriptira sadržaj i šalje ga unutar privatne mreže, [10].

[7] Emulacija – informacijski proces prilikom kojeg se jedno računalo, uređaj ili program u svim relevantnim aspektima ponaša kao neko drugo računalo, uređaj ili program.



Slika 7. Sučelje programskog alata ProtonVPN

Slika 7. prikazuje sučelje programskog alata ProtonVPN koji omogućava korištenje VPN mreže. Sa slike 7. može se vidjeti da je dodijeljena nova IP adresa[8] računalu s područja Slovenije. Konekcija je ostvarena UDP (engl. *User Data Protocol*) protokolom i prikazane su brzine uzlazne i silazne veze.

Širokopojasni prijenos nudi udaljenim korisnicima mogućnost brzog povezivanja s poslovnim mrežama i Internetom. Nekoliko je vrsta prijenosa, a to su:

- **Digitalna pretplatnička linija** (engl. *Digital Subscriber Line* – DSL) – omogućuje prijenos digitalnih podataka preko bakrene parice;
- **Optičko vlakno** – omogućuje prijenos podataka putem svjetlosnih zraka;
- **Kabelski modem** – omogućuje prijenos podataka koristeći koaksijalni kabel kojem je također funkcija dostavljanje slike i zvuka televizijskom prijamniku;
- **Bežični prijenos** – omogućuje prijenos podataka putem elektromagnetskih valova;
- **Satelit** – oblik bežičnog prijenosa koji je koristan za rijetko naseljena mjesta, [10].

[8] IP adresa – decimalni broj koji definira podatke o usmjeravanju paketa.

3.2. Protokoli udaljenog pristupa

Protokoli udaljenog održavanja su odgovorni za upravljanje vezom između udaljenog računala i poslužitelja udaljenog servera. Oni su neophodni za stvaranje usluge udaljenog pristupa. Velik je broj protokola koji obavljaju funkcije u udaljenom održavanju. Razvojem tehnologije i informacijskih sustava, neprestano se pojavljuju novi protokoli s drugačijim funkcijama, kao što su RADIUS[9], TACACS[10] i RAS[11]. Primarni protokoli današnjice su:

- **PPP** (engl. *Point-to-Point Protocol)* – protokol udaljenog održavanja koji omogućava povezivanje uređaja putem direktnih dediciranih linkova. Najčešće se koristi za udaljeno povezivanje lokalnih mreža s davateljem internetske usluge (engl. *Internet Service Provider* – ISP). Bazira se po TCP/IP[12] modelu. PPP koristi LCP (engl. *Link Control Protocol*) koji testira poveznicu između klijenta i PPP domaćina te specificira korisničku konfiguraciju kako bi se uskladili za komunikaciju. LCP omogućava PPP-u pregovore o autentifikaciji povezivanja koristeći kompresiju i enkripciju podataka između klijenta i domaćina pomoću enkripcijskog kontrolnog protokola (engl. *Encryption Control Protocol* – ECP) i kompresijskog kontrolnog protokola (engl. *Compression Control Protocol* – CCP). PPP je generalno smatran kao jednostavan protokol za konfiguraciju jer čim se usmjerivač spoji na PPP, automatski mu se dodjeljuju ostali TCP/IP parametri. Tu funkciju obavlja protokol dinamičke konfiguracije (engl. *Dynamic Host Configuration Protocol* – DHCP), a riječ je o parametrima subnetirane maske[13], sustav domene (engl. *Domain Name System* – DNS) i IP adrese domaćina. Prednost korištenja PPP-a je što ga je moguće koristiti kroz razne fizičke medije i što omogućuje funkciju provjere pogrešaka, dok mu je nedostatak što nije kompatibilan sa starijim konfiguracijama. Slikom 8 prikazan je tok zahtjeva za stvaranje PPP povezivanja između klijenta i servera, [11];

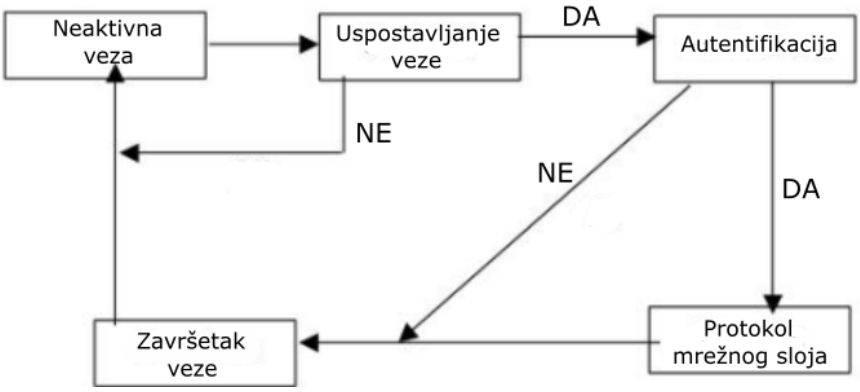
[9] RADIUS – omogućuje poslužiteljima udaljenog pristupa komunikaciju sa središnjim poslužiteljem radi provjere autentičnosti dial-in korisnika.

[10] TACACS - omogućuje poslužiteljima udaljenog pristupa prosljeđivanje korisničke lozinke na poslužitelj za provjeru autentičnosti.

[11] RAS – omogućuje konfiguraciju modema samo za dial-out i dial-up.

[12] TCP/IP (engl. *Transmission Control Protocol / Internet Protocol)* – skup standardiziranih pravila koji omogućavaju povezivanje na mrežu poput Interneta.

[13] Subnetirana maska (engl. *Subnet Mask)* – 32 ili 128-bitni broj koji segmentira postojeću IP adresu u TCP/IP mreži. Dijeli IP adresu na mrežnu adresu i adresu domaćina.



Slika 8. Dijagram PPP protokola
Izvor**:** [11]

- **PPTP** (engl. *Point-to-Point Tunneling Protocol)* – Baziran je na PPP-u kreiran od strane tvrtke Microsoft. Za korištenje PPTP protokola, prvo je potrebno ostvariti PPP vezu između servera i klijenta. Nakon što je ta sesija uspostavljena, kreira se nova sesija koja koristi prvotnu sesiju za sigurniji prijenos podataka. Implementacija PPTP-a se obavlja na dva načina. Prvi način je postavljanje servera u ulogu uređaja za mrežni prolaz[14] do Interneta. *Gateway* je odgovoran za sav prijenos podataka. Tim načinom se ne zahtjeva od baznih stanica dodatna konfiguracija. Ovaj način se koristi ukoliko je cilj povezivanje cijele mreže. Zatim drugi način implementacije je da se konfigurira jedna bazna stanica povezivanjem preko ISP-a, dok se klijent povezuje na mrežu preko VPN servera. PPTP je prvenstveno koristio MSCHAP-v2[15] koja je napretkom *cyber* prijetnji postala nepouzdana. Posljedica toga je uvođenje proširenog autentifikacijskog protokola (engl. *Extensible Authentification Protocol* – EAP) koji je sigurniji za upotrebu, no zahtjeva korištenje pametnih kartica i certifikata što PPTP čini kompliciranijim za uporabu. PPTP koristi MPPE (engl. *Microsoft Point-to-Point Encryption*) s ključem generiranim od MSCHAP-v2 ili EAP-TLS[16] autentifikacijskog procesa i zahtjeva TCP (engl. *Transmission Control Protocol*) port 1723 i IP protokol 47 za korištenje bez problema s vatrozidom, [11];

[14] Mrežni prolaz (engl. *Gateway)* – mrežni hardver koji se koristi kao čvor u telekomunikacijskim mrežama. Omogućava protok podataka iz jedne mreže u drugu.
[15] MSCHAP-v2 – autentifikacijski protokol PPTP protokola
[16] EAP-TLS (engl. *Transport Layer Security)* – osigurava autentičnost klijenta i mreže na temelju certifikata.

- **SLIP** (engl. *Serial Line Internet Protocol)* – koristi podatkovni i fizički sloj OSI referentnog modela[17], a služi za emitiranje TCP/IP preko serijskih konekcija. Za stvaranje SLIP udaljenog povezivanja potreban je SLIP račun na uređaju domaćina, te skripta ili dokument na baznoj stanici. Funkcija skripte je unošenje parametara nakon što se računom poveže na udaljeno mjesto. Nedostatak SLIP-a je što ne adresira poslane pakete i što nema opciju provjere greški, [12].

- **L2TP** (engl. *Layer Two Tunneling Protocol*) – VPN protokol koji ne nudi enkripcijsku autentifikaciju za promet koji prolazi kroz poveznicu, ali u kombinaciji s IPsec (engl. *Internet Protocol Security*) čini L2TP/IPsec protokol koji koristi certifikate za autentifikaciju krajnjih točaka komunikacije. Također se upotrebljavaju unaprijed dodijeljeni ključevi, iako oni zahtijevaju ručnu konfiguraciju. L2TP/IPsec zahtjeva UDP port 500 i IP protokol 50 za korištenje bez problema s vatrozidom, [13].

[17] OSI referentni model – konceptualni model koji karakterizira i standardizira komunikacijske funkcije sustava.

4. PROGRAMSKI ALATI ZA UDALJENO ODRŽAVANJE INFORMACIJSKO-KOMUNIKACIJSKIH SUSTAVA

Programski alati za udaljeno održavanje pružaju mogućnost nadziranja, dijagnosticiranja i upravljanja udaljenim uređajima u mreži. Omogućuju davateljima upravljanih usluga (engl. *Managed Service Providers* – MSP) rješavanje problema i upravljanje udaljenim uređajima mnogo efikasnije nego što se postiže korištenjem usluga lokalnih tehničara.

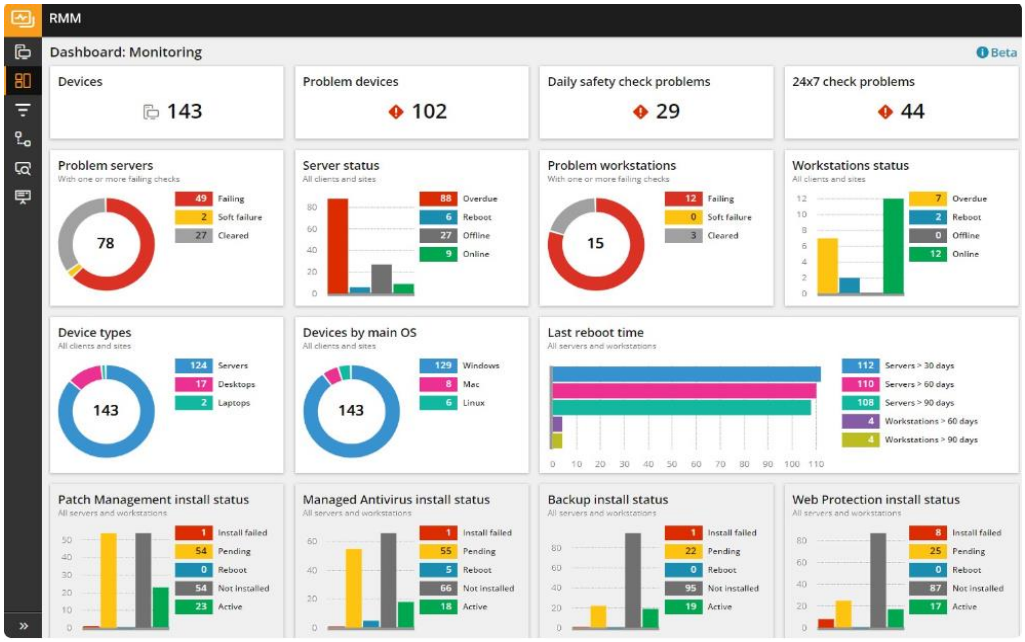
Neki od najkvalitetnijih programskih alata za udaljeno održavanje su:

- SolarWinds RMM
- Ninja RMM
- Atera
- TeamViewer
- Paessler PRTG Network Monitor
- Site24x7
- ConnectWise Automate
- Pulseway
- Kaseya VSA
- ITarian
- Domotz Pro i dr.

Programski alati koji su analizirani u radu su *SolarWinds*, *NinjaRMM* i *Itarian*. Oni su opisani zbog raznolikosti pružanja usluge održavanja informacijsko-komunikacijskih sustava. *SolarWinds* se smatra programskim alatom za vođenje računalnih sustava, dok je *NinjaRMM* alat omogućen i na mobilnim uređajima. Razlog opisivanja *Itarian* alata je zbog mogućnosti besplatnog korištenja što zasigurno utječe na povećanje broja korisnika.

4.1. SolarWinds RMM

Programski alat SolarWinds RMM (engl. *Remote Maintenance Monitoring*) je prvenstveno dizajniran u svrhu zaštite od gubitka podataka izradom sigurnosnih kopija. Također održava antivirusni sustav korisnika i prevenira *cyber* napade[18] od strane nepoznatih izvora. Uz funkcije izrade sigurnosnih kopija, kontrole rizika poslovanja, *SolarWinds* RMM također omogućuje pohranu podataka na računalni oblak[19] čime se štedi na prostoru za pohranu podataka. Koristi funkcije otkrivanja i reagiranja krajnjih točaka sustava koje pomažu pri praćenju prijetnji u udaljenom okruženju. Datoteke se skeniraju neprekidno u stvarnom vremenu kako bi se pojačala sigurnost zaštite podataka. Ukoliko dođe do probijanja zlonamjernog sadržaja na mrežu, strojno učenje omogućuje brzo i efikasno rješenje na nastali problem. Značajka *NetPath*[20] je još jedan koristan dodatak. Njime se mogu pratiti mrežne performanse da bi se vidjelo postoje li problemi u povezivanju među uređajima. Funkcionira kao alat *Traceroute*[21] kojem je funkcija preciziranje gdje se problem s izvedbom nalazi u mreži, [14].



Slika 9. Sučelje programskog alata SolarWinds RMM, [14]

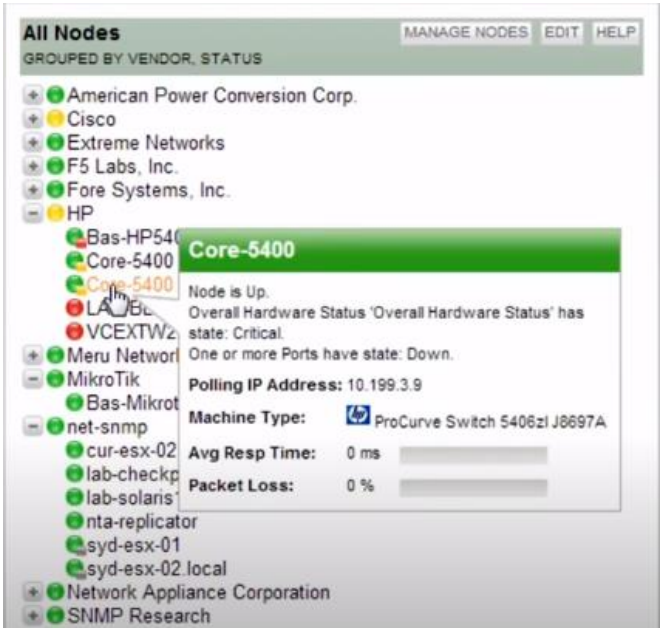
[18] Cybernapadi – Napadi na računala preko Interneta.
[19] Računalni oblak (engl. Cloud) skup računalnih usluga uključujući pohranu podataka i umrežavanje putem Interneta.
[20] *NetPath* - *NetPath* mjeri karakteristike performansi svakog mrežnog čvora i veze uočavanjem usporavanja.
[21] *Traceroute* – alat koji se koristi za praćenje putanje paketa u stvarnom vremenu. Također bilježi vrijeme potrebno za svaki skok koji paket napravi na ruti do odredišta

Slikom 9. prikazan je izgled programskog sučelja alata *SolarWinds RMM*. Dijagramom su prikazani brojevi problematičnih servera i baznih stanica. Također se mogu nadzirati vrste uređaja spojenih na programski alat, njihovo zadnje podizanje sustava, status instalacije sigurnosne kopije, *Web* zaštite i upravljanje zakrpama, [14].

Funkcija mrežnog nadzora performansi (engl. *Network Performance Monitor* NPM) programskog alata *SolarWinds* omogućuje uvid korisniku u povijest kvarova, mjerenje performansi mreže, kvalitetu i stanje harvera i dubinski pregled i analizu paketa. Alat koristi tri protokola, a to su:

- **ICMP** (engl. *Internet Control Message Protocol*);
- **SNMP** (engl. *Simple Network Management Protocol*) i
- **WMI** (engl. *Windows Management Instrumentation*), [14]

Odmah nakon instalacije NPM-a ugrađena mreža automatski pronalazi sve prespojnike, usmjernike, vatrozide, bežične pristupne točke i servere. Prvo programsko sučelje do kojeg korisnici dođu koristeći NPM je sučelje na kojem je moguće vidjeti stanje mreže i omogućava korisnicima brzo identificiranje problema u njihovom okruženju. Zatim moguće je vidjeti status svih čvorova koji se nadziru, kao i njihov status što je prikazano slikom 10.



Slika 10. Praćenje mrežnih čvorova programskim alatom SolarWinds, [14]

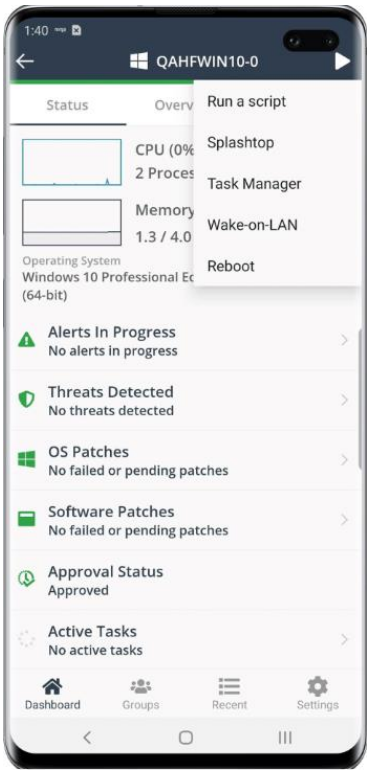
Čvorovi mogu biti grupirani po prodavaču, vrsti uređaja, lokaciji ili bilo kojim drugim specifikacijama definiranim od korisnika. Pritiskom na čvor se vide detaljnije informacije poput gubitaka paketa, prosječnog vremena reagiranja, vrsti uređaja i IP adrese. Čvorovi žute i crvene boje zahtijevaju intervenciju.

4.2. Ninja RMM

Ninja RMM je kvalitetno RMM rješenje koje omogućava nadzor u stvarnom vremenu za Windows i Mac računala. Glavna funkcija je omogućavanje korisnicima automatizaciju zakrpa na udaljenim mrežama. Također bitna funkcija Ninja RMM-a je upravljanje sigurnošću krajnje točke mreže. Sigurnost se postiže implementacijom *Webroot-a*[22] u cijeloj mreži. Ukoliko je datoteka maliciozna, mali lokalni program briše datoteku i preokreće radnje prouzrokovane tom datotekom. Ovaj oblik obrane od virusa je dosta neobičan, no testiranjem se pokazalo da je pouzdano, [15].

Ninja RMM podržava preko 120 aplikacija, uključujući Dropbox i Javu. Jedna od velikih prednosti je ta što je razvijena Ninja RMM mobilna aplikacija čime je omogućen pregled kritičnih upozorenja u pokretu. Podržava Android i iOS sustave, [15].

[22] *Webroot* - sustav koji nadgleda nepoznate datoteke sve dok glavni program koji se nalazi na oblaku ne donese odluku da li je datoteka maliciozna.



Slika 11. Sučelje programskog alata Ninja RMM

Slika 11. prikazuje sučelje aplikacije Ninja RMM za sustav Android koja je postavljena na tržište 30. studenog 2019. godine. Slikom su prikazane opcije pregleda znakova za uzbunu, detektiranje prijetnji, zakrpe sustava OS[23], zakrpe softvera, statusa potrebnih odobrenja i aktivnih zadataka.

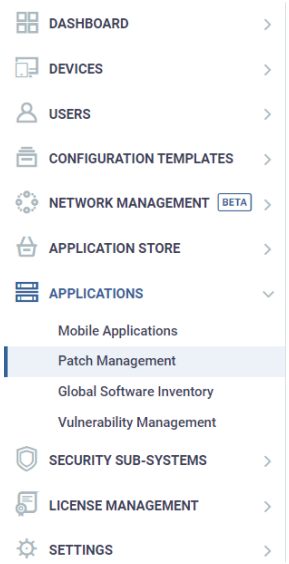
4.3. Itarian

Itarian je RMM programski alat koji omogućava daljinsko nadziranje krajnje točke, mreže i korisničkog računala. Pomoću RMM-a, MSP-ovi mogu daljinski uvoditi zakrpe i ažuriranja, instalirati i konfigurirati softver, rješavati probleme i sl. Moguće je povezivanje različitih vrsta uređaja s različitim operativnim sustavima. Bitna stavka udaljenog održavanja je upravljanje zakrpama. Itarian alatom je vidljiv točan broj potrebnih novih zakrpa za svaki uređaj na popisu uređaja, zatim je moguće detaljnije

[23] OS (engl. Operating system) – Operativni sustav

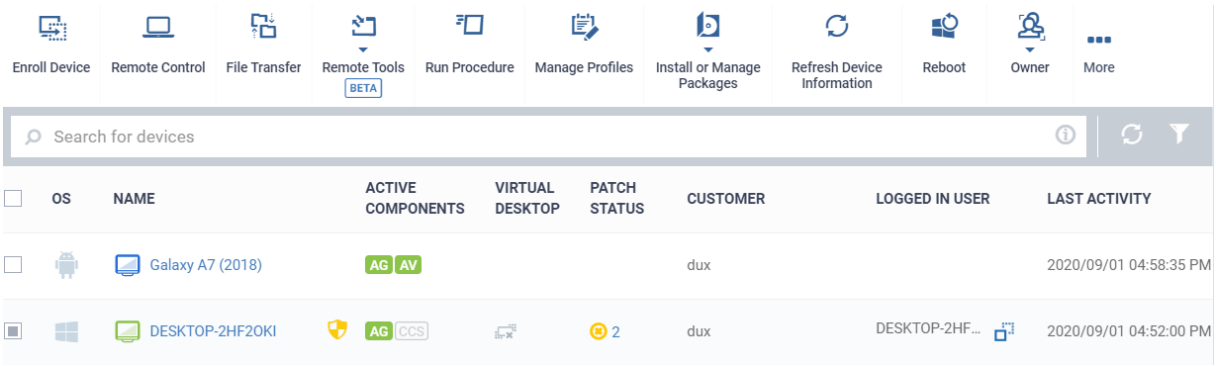
vidjeti o kojim se zakrpama radi. Također raspodjeljuje zakrpe po razini kritičnosti po uređaj.

Itarian sadrži alat za automatsko otkrivanje i postavljanje datoteka na udaljeni uređaj. Funkcija tog programskog alata je da se pošalju datoteke uređaju ili većem broju grupiranih uređaja preko platforme u oblaku. Mobilnim uređajima putem *Itarian* platforme nije moguće pristupiti, nego ih je samo moguće konfigurirati, upravljati aplikacijama i pratiti mrežni promet. Također je uređajima moguće poslati poruku u svrhu obavještavanja za potrebna sigurnosna ažuriranja, moguće je udaljeno uključiti alarm, te postaviti datum i vrijeme aktiviranja alarma što je prikladno ukoliko je potrebno naznačiti korisniku obavljanje funkcije u točno vrijeme.



Slika 12. Glavni padajući izbornik programskog alata *Itarian*

Slikom 12. prikazane su osnovne opcije programskog alata Itarian. Pritiskom na kontrolnu ploču (engl. *Dashboard*) dobiva se revizija o izvješćima, usklađenosti i obavijestima generiranih od korisničkih aktivnosti. Moguće je vidjeti aktivnost uređaja u proteklom danu, da li je detektiran virus na nekim uređajima, da li uređaji sadrže aplikacije koje se smatraju sigurnosno opasnima, stanje antivirusnih programa i sl.



Slika 13. Funkcije upravljanja uređajima programskim alatom *Itarian*

Pritiskom klika na inačicu „uređaji“ (engl. *devices)* prikazan je popis povezanih uređaja kojima je moguće udaljeno pristupiti, slati datoteke, udaljeno ih popravljati, instalirati i upravljati zakrpama, ponovno pokrenuti uređaj i brojne druge manje bitne funkcionalnosti (Slika 13.).

Slika 14. Funkcije upravljanja korisničkim računima programskim alatom *Itarian*

Klikom na inačicu „korisnici“ (engl. *Users*) otvara se sučelje prikazano slikom 14 u kojem je moguće upravljati korisničkim računima uređaja. Jedan korisnički račun može upravljati više uređaja u sustavu tako da promjenom nekih od postavki jednog korisnika može zahvatiti više uređaja. Opcije koje se nude su dodavanje novog korisničkog računa, upravljanje profilima, slanje e-pošte u svrhu promjene zaporke, promjena zaporke, brisanje korisničkog računa, resetiranje 2FA tokena[24] i dr.

Brojne su druge opcije korištenja *Itarian* programskog alata. *Itarian* omogućava konfiguraciju predložaka, upravljanje mrežnim značajkama, pregled aplikacija preuzetih na promatrane uređaje gdje je moguće zabraniti korištenje nekih aplikacija

[24] *Token* – predstavlja niz bitova koji kruže mrežom. Kad jedan od mrežnih sustava ima token, može slati informacije na druga računala. Budući da postoji samo jedan token za svaku mrežu prstenova, samo jedan uređaj može istovremeno slati podatke.

uređajima. Zatim ima mogućnost upravljanja sigurnosnim podsustavima uređaja gdje je najviše naznaka na korištenju vatrozida i njegovo redovito ažuriranje.

Prednost *Itarian* programskog alata je što je besplatan u okvirima osnovnog korištenja. S velikim brojem mogućnosti konkurentan je vodećim programskim alatima u udaljenom održavanju koje za razliku od *Itariana* nisu besplatne.

Slika 15. Zadovoljstva korisnika koristeći programske alate *SolarWinds i Ninja RMM, [16]*

Slikom 15 prikazana je usporedba zadovoljstva korisnika koristeći *SolarWinds* i *NinjaRMM* alate za udaljeno održavanje. U ocjenjivanju je sudjelovala 1141 osoba, a raspon ocjena je bio od 1 do 5. Usporedbom je prikazano da je iz korisničkog aspekta programski alat *NinjaRMM* kvalitetniji i jednostavniji za uporabu od programskog alata *SolarWinds*.

5. SIGURNOST UDALJENOG ODRŽAVANJA INFORMACIJSKO-KOMUNIKACIJSKIH SUSTAVA

Sigurnost udaljenog održavanja je glavni prioritet prilikom pružanja usluga korisnicima. Pojam sigurnosti je proporcionalan veličini korištenja usluga udaljenog održavanja jer današnji pristup Internetu je nepouzdan upravo zbog raznih prijetnji koji se nalaze na njemu. Sigurnost se može podijeliti u dvije osnovne kategorije, a to su sigurnost iz aspekta poslovanja i sigurnost od prijetnji.

5.1. Sigurnost iz aspekta poslovanja

Davatelji usluga udaljenog održavanja informacijsko-komunikacijskih sustava se raznim načinima osiguravaju od mogućih problema prilikom pohranjivanja korisničkih podataka, održavanja tuđih sustava i odgovaranja za nastale smetnje. Iz aspekta poslovanja davatelji usluga su precizirali suzbijanje mogućih problema tako što su definirali podkomponente koje zajedno čine sustav pouzdanim i korisnim. Sigurnost udaljenog održavanja se može raščlaniti na nekoliko grana što je prikazano slikom 15.

Slika 16. Sigurnost iz aspekta poslovanja

Izvor: [9]

Pod operativnu sigurnost udaljenog održavanja sustava spada postupak upravljanja promjenama. One se odnose na unaprjeđenje informacijskih sustava i mrežnih uređaja, te na fizičke promjene na uređajima. Kontroliraju se i nadgledaju kroz formalni postupak kontrole promjena. Također se primjenjuju nakon implementacije kako bi se osiguralo da djeluju kako je planirano. Efikasno praćenje sustava je esencijalna stavka za udaljeno upravljanje. Praćenje se odnosi na performanse hardvera i softvera što je prvi korak prilikom odabira modela udaljenog održavanja. Pravilno održavanje zadržava sustav aktualnim što u krajnjem slučaju omogućuje uzimanje u obzir podataka za buduće poslovne procese i praćenje troškova. Najčešće se za praćenje jednostavnih sustava koriste tehnike poput proračunskih tablica i prilagođenih baza podataka, dok se za kompleksnije sustave koriste integrirani alati za upravljanje, [9].

Idući korak u održavanju sigurnosti poslovanja je kvalitetna i detaljna dokumentacija. Dokumentiranje cijele arhitekture i njenih elemenata je isključivo bitno za održavanje softvera. Cilj je stvoriti strukturirano održavanje sustava, te izbjeći nestrukturirano. Razlika je u tome što se nestrukturirano održavanje direktno veže na izvor koda i radi promjene bazirane samo na tome, dok strukturirano održavanje modificira i proučava originalan dizajn, te obnavlja kod tako da odgovara sustavu, [10].

Bitan čimbenik poslovanja je ugovaranje usluge. Ugovor se može potpisati s opskrbljivačem usluge ili s trećom stranom koja posjeduje adekvatnu infrastrukturu. U ugovoru se najviše pažnje posvećuje preventivnom i korektivnom održavanju sustava, dok se adaptivno i aktualno održavanje rješava ugovorima kad dođe za to predviđeno vrijeme. Stavke koje sačinjavaju ugovor su:

- Minimalna zaliha hardverskih dijelova (matična ploča, memorija i sl.);
- Mogućnost mrežnog upravitelja pristupanju udaljenim računalima;
- Sati podrške (dani u tjednu / sati u danu);
- Planiran prekid rada;
- Maksimalno prihvatljivo trajanje neplaniranog prekida rada sustava;
- Penali za nepridržavanje ugovora, [9].

U kritičnim okruženjima s visokim zahtjevima za dostupnošću sustava poželjno je imati zamjensku zalihu kritičnih dijelova kako bi se smanjilo trajanje pada sustava

ukoliko dođe do toga. Svaki sustav mora prekinuti s radom u jednom trenutku radilo se to o unaprjeđenju sustava ili poteškoćama. Prekid rada može dovesti poslovanje do značajnih troškova, zato je bitno dobro isplanirati trenutak kada će troškovi biti najmanji. Penali za nepridržavanje ugovora se najviše odnose za poteškoće s prekidom rada sustava. Dostupnost sustava se može izračunati uzevši u omjer radne sate bez perioda u kojem sustav nije radio s radnim satima tijekom jedne godine. Što je dostupnost sustava manja u odnosu na ugovorom dogovorenu dostupnost, to su penali veći. Penali su još definirani kao postotak troškova kupnje i održavanja uređaja koji je u kvaru. Ukoliko dođe do kvara jednog uređaja, svi ostali uređaji koji ovise o njemu su također smatrani izvan funkcije što može rezultirati visokim penalima kad prekid rada pređe planirano trajanje, [9].

5.2. Sigurnost od prijetnji

Opasnost od prijetnji s Interneta je jedno od najučestalijih briga korisnika udaljenog pristupa. Većina ljudi koji posjeduju terminalni uređaj su se suočili sa situacijom da im uređaj zahtijeva popravak tehničara. Nema velike razlike omogućavanju pristupa osobi koja je fizički prisutna i osobe koja udaljeno obavlja popravak. Velik je broj mjera opreza koje su razvijene u svrhu pouzdanog omogućavanja udaljenog pristupa. Jedna od tih mjera je već spomenuta u radu, a odnosi se na VPN mrežu koja omogućuje sigurno povezivanje s javnim mrežama bez mogućnosti praćenja IP lokacije. Takvo pristupanje mreži onemogućava napadaču pristup osobnim podacima. Relativno nova mjera opreza u udaljenom pristupanju je dva faktora autentifikacije (engl. *Two-Factor Authentication* – 2FA). 2FA je drugi sloj sigurnosti, obično je dodatak šifri za pristup računu ili sustavu. Preuzima ga se u obliku aplikacije i povezuje se na *Google* račun ili broj mobilnog uređaja korisnika. Funkcionira na način da generira nasumične pinove koje je potrebno unijeti za pristup računu ili serveru u kratkom vremenskom intervalu nakon upisivanja šifre. Nakon korištenja 2FA, korisnik dobiva informaciju od kud je pristupano i kojim modelom uređaja je pristupano računu ili sustavu. Slikom 16 prikazano je pristupanje uređaju putem 2FA autentifikacije, [17].

Slika 17. Korištenje 2FA autentifikacije

Izvor: [17]

Prijetnje koje zahvaćaju udaljeni pristup su u oblicima krađe podataka, krađe identiteta, nedozvoljen pristup udaljenim uređajima i korištenje kamera i mikrofona. Jedan od takvih zlonamjernih softvera je trojanski virus udaljenog pristupa (engl. *Remote Access Trojan* – RAT). RAT je klasa zlonamjernog softvera koji napadaču omogućuje izravan interaktivni pristup osobnom računalu žrtve, omogućavajući napadaču krađu privatnih podataka pohranjenih na uređaju, špijuniranje žrtve u stvarnom vremenu preko kamere i mikrofona i izravno komuniciranje sa žrtvom putem dijaloškog okvira. Funkcionira na način da napadač prvo hakira uređaj, te zatim nadzire žrtvu čekajući priliku za krađu osjetljivih podataka. Budući da je komplicirano uočiti zahvaćanje RAT-a za uređaj, cilj je onemogućiti prijenos podataka natrag napadaču. Različiti oblici pristupa RAT-a računalu predstavljaju mrežne karakteristike virusa po čemu se može dizajnirati sustav detekcije virusa. Problem se nalazi u tome što slične mrežne karakteristike generiraju uobičajene aplikacije. Da bi se mogao razlikovati promet nastao od uobičajenih aplikacija i virusa uzima se kratak period praćenja značajki zaražene mreže, te se pomoću umjetne inteligencije uči sustav na koji način prepoznati prisutnost RAT virusa, [18].

6. PRIMJENA UDALJENOG ODRŽAVANJA INFORMACIJSKO-KOMUNIKACIJSKIH SUSTAVA

Sustav za udaljeno održavanje se ugrađuje na zadani hardverski uređaj s ugrađenim senzorom koji prikuplja podatke o kvaru hardverskog uređaja bez ometanja njegovog rada. Podaci se dobivaju iz unaprijed određenih kritičnih točaka i analiziraju se uz pomoć stručnjaka za dijagnostiku sustava. Stručnjak pronalazi i izolira porijeklo kvara hardvera. Također nadzor uređaja može uključivati podatke grešaka pariteta koji se koriste za definiranje anomalije testiranog hardvera. Mnoštvo senzorskih implantata se može dodati odgovarajućim uređajima u svrhu dobivanja pouzdanijih podataka distribuiranih sustava velikih razmjera. Transparentno sučelje senzora sprječava operativne smetnje u distribuiranom sustavu. Senzore je također moguće nadograditi u svrhu mogućnosti praćenja starijih uređaja koji nemaju ugrađenu tehnologiju ispitivanja. Kontinuirano praćenje sustava s takvim uređajima u stvarnom vremenu u kombinaciji s dijagnostičkom analizom omogućava pronalazak povremenih kvarova što olakšava održavanje sustava velikih razmjera, [19].

Područje tehnologije koje je postalo dio suvremene industrijske automatizacije je robotika[25]. Prvi robot proizveden je 1960. godine, a 1985. godine u Sjedinjenim Američkim Državama je već radilo oko 16 000 industrijskih robota. U današnje vrijeme robotizam je zamijenio čovjeka u gotovo svim aspektima industrijskog procesa jer su analize pokazale da roboti uvećavaju produktivnost za 20 do 30 %. Prouzrokovano globalnim valom korištenja internet stvari, moderni industrijski roboti su zadobili veliku ulogu u fleksibilnoj manufakturi. Troškovi kompleksnih struktura i održavanja su značajno smanjeni korištenjem udaljenog održavanja. Od tehničara je očekivano detektiranje grešaka i kontrola uređaja, te slanje informacija korisnicima o problemima koje je za očekivati. Kao pomoć nadziranju takvih sustava razvio se termin rubnog računalstva[26] koji ima iduće funkcije:

- Predobrada, filtriranje i zaštita podataka;

[25] Robotika – interdisciplinarno područje koje uključuje dizajniranje, konstrukciju, rad i upotrebu robota. Cilj robotike je dizajnirati inteligentne sustave koji mogu pomoći u ljudskoj svakodnevici.

[26] Rubno računalstvo (engl. Edge Computing) Računalstvo na rubu mreže je otvorena IT arhitektura koja sadrži decentraliziranu procesorsku snagu omogućavajući IoT tehnologiju. U rubnom računanju podatke obrađuje sam uređaj ili poslužitelj.

- Podržava pristup oblaku;
- Podržava VLAN (engl. *Virtual Local Area Network)* funkciju;
- Prima naredbe iz oblaka i obavještava uređaje na rubu mreže;
- Podrška sigurnim tunelima za udaljeno uklanjanje pogrešaka, [19].

Slika 18. Udaljeno održavanje u robotici

Izvor: [20]

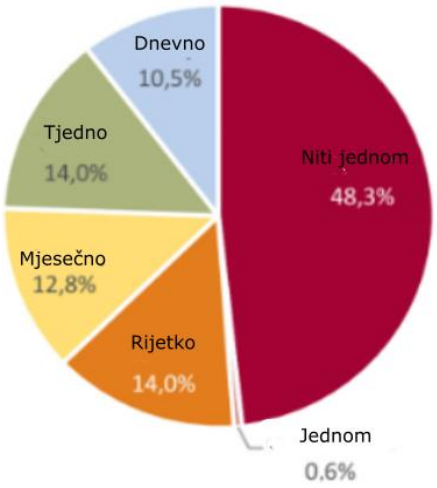
Slikom 18. prikazano je proizvodno mjesto koje se sastoji od robota, ručnog terminala i upravljačkog sustava. Kroz brzi *Ethernet*[27], sustav upravljanja jezgrom povezan je s baznom stanicom na rubu mreže koja prikuplja podatke o statusu rada strojeva poput temperature, brzine okretnog momenta osovine, brzine povratne sprege osi i sl. Obrađeni se podaci šalju na platformu u oblaku pomoću često korištenih IoT protokola HTTP (engl. *Hyper-Text Transfer Protocol*) i MQTT (engl. *Message Queuing Telemetry Transport*). Preko platforme se može daljinski nadzirati status uređaja i provoditi preventivno održavanje, [20].

Termin udaljenog održavanja je u porastu uporabe što je prouzrokovano situacijom vezanom za virus COVID-19. Mnoge tvrtke su osposobile obavljanje poslova korištenjem udaljenih servera na koje se zaposlenici spajaju. Organizacije koje su najviše zahvaćene promjenom poslovanja korištenjem udaljenog održavanja su zdravstvene organizacije i obrazovne ustanove.

U nastavku su prikazani rezultati istraživanja autora [21] koje je provedeno na djelatnicima zdravstvenih organizacija, a vezano za korištenje udaljenih sustava zbog epidemije COVID-19. U istraživanju je sudjelovalo 172 ispitanika iz 35 zemalja.

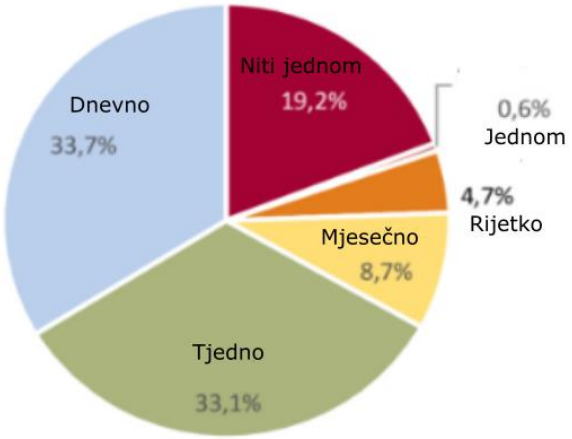
[27] Ethernet metoda povezivanja uređaja u lokalnu mrežu.

Tijekom epidemije, 84,6 % ispitanika uključenih u akademske aktivnosti transformiralo je svoje tečajeve u mrežno učenje. Istraživanjem se usporedilo korištenje udaljenog pristupa u Kini, Francuskoj i Italiji. Rezultati su pokazali da je prije epidemije COVID-19 korištenje udaljenog pristupa bilo znatno više u Kini nego u Francuskoj i Italiji, dok je za vrijeme epidemije COVID-19 ta razlika manje izražena, [21].



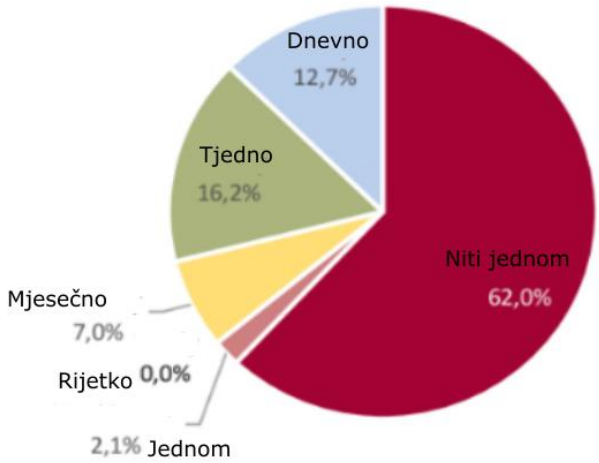
Grafikon 1. Uporaba udaljenog pristupa u poslovne svrhe prije epidemije COVID-19, [21]

Frekvencija korištenja udaljenog pristupa u poslovne svrhe prije epidemijske situacije vezane za COVID-19 nastale u prvoj polovici 2020. godine, prikazana je grafikonom 1.



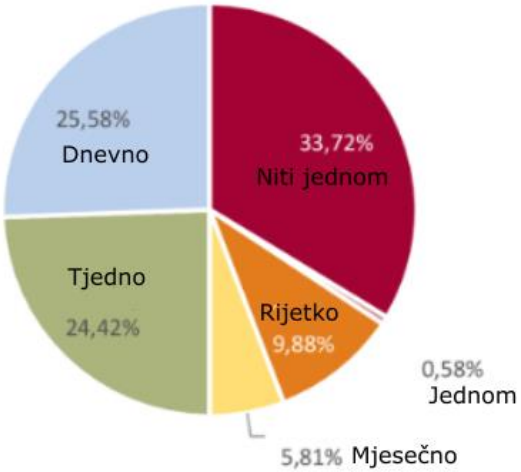
Grafikon 2. Uporaba udaljenog održavanja u poslovne svrhe za vrijeme epidemije COVID-19, [21]

Frekvencija korištenja udaljenog pristupa u poslovne svrhe za vrijeme epidemije COVID-19 prikazana je grafikonom 2. U usporedbi s grafikonom 1. vidljivo je da se broj ispitanika koji nikad nisu koristili udaljeni pristup smanjio za 29,1 %.



Grafikon 3. Uporaba udaljenog pristupa u privatne svrhe prije epidemije COVID-19, [21]

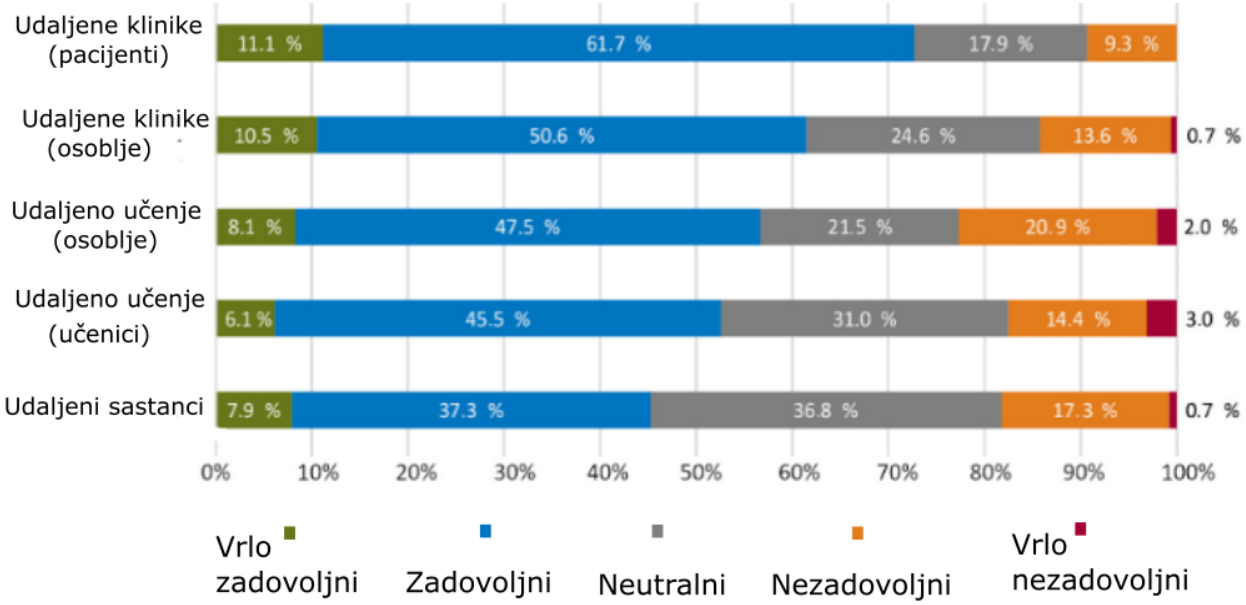
Frekvencija korištenja udaljenog pristupa u privatne svrhe prije epidemije COVID-19 prikazana je grafikonom 3.



Grafikon 4. Uporaba udaljenog pristupa u privatne svrhe za vrijeme epidemije COVID-19, [21]

Frekvencija korištenja udaljenog pristupa u privatne svrhe za vrijeme epidemijske situacije je prikazana grafikonom 4. U usporedbi s grafikonom 3. je vidljivo da se broj ispitanika koji nikad nije koristio udaljen pristup smanjio za 28,28 %.

Također su se ispitivale recenzije usluge udaljenog pristupa koja je prikazana grafikonom 5.



Grafikon 5. Prikaz recenzija koristeći udaljeni pristup, [21]

S grafikona 5. može se očitati da je malen broj korisnika vrlo nezadovoljan, dok je velika većina zadovoljna uslugom udaljenog pristupa.

7. ZAKLJUČAK

Temelj informacijsko-komunikacijskih sustava je pouzdanost, povjerljivost i efikasnost obavljanja funkcija za koje su predviđeni. Kroz završni rad je objašnjeno na koji način udaljeno održavanje poštuje ta načela u provođenju usluge preko mreže. Opisan je proces omogućavanja povezivanja korisnika i davatelja usluga s visoke sigurnosne razine koristeći višerazinske alate identifikacije.

U završnom radu objašnjeno je funkcioniranje udaljenog pristupa, što se odnosi na udaljeno održavanje, udaljenu dijagnostiku i udaljeno popravljanje. Objašnjeno je kakvu korist od takvih usluga ima ukupno poslovanje odnosno poslovni sektor i na koji način. Uporaba udaljenog održavanja ne samo da pojednostavljuje upravljanje sustavima, nego i značajno smanjuje troškove.

Gledajući sa sigurnosnog aspekta, sustavi djeluju pouzdano zahvaljujući napretku sigurnosnih sustava, dodatnih identifikacija korisnika koja pridonose razvoju u tehničkom okruženju. Brojni su programski alati koji omogućavaju korištenje usluge udaljenog održavanja. Korištenje takvih alata omogućuje detaljno i pregledno vođenje organizacija.

Smatra se da će udaljeno održavanje napredovati dolaskom mlađih generacija koja su odrasla uz Internet. Također sve je veći broj korisnika terminalnih uređaja i korisnika koji obavljaju poslove putem udaljenog pristupa što je još jedan znak napretka takvih usluga.

U bliskoj prošlosti dogodilo se mnogo promjena koje su utjecale na razvoj udaljenog održavanja. Termin udaljenog pristupa doživio je procvat u nastaloj epidemijskoj situaciji virusa COVID-19 jer su mnogobrojne organizacije prisiljene obavljati funkcije poslovanja putem Interneta. Samim time održavanje je postalo puno kompleksnije zbog povećanja broja povezanih uređaja i samim time zahtjevaju sveći resursi - hardverski, softverski i prateće informacijsko-komunikacijske opreme.

Mnoge tvrtke prelaskom na udaljeno poslovanje su ostvarile porast produktivnosti zaposlenika za značajan postotak. Vjerojatno je da će, kad dođe do ublažavanja situacije s virusom COVID-19, brojne tvrtke zadržati način poslovanja putem Interneta, te takva usluga može samo napredovati. Smatra se da će u budućnosti usluge udaljenog pristupa predvoditi kao glavni oblik poslovanja.

LITERATURA

[1] Peraković, D., Periša, M., Forenbacher, I.: Autorizirana predavanja, Informacijski sustavi mrežnih operatora, Fakultet prometnih znanosti, Zagreb, 2018.

[2] Hagen, L., Breugst, M., Magedanz, T.: *Impacts of mobile agent technology on mobile communication system evolution, IEEE Personal communications*, *5*(4), 56-69., 1998.

[3] Biehl, M., Prater, E., Mcintyre J.: *Remote repair, diagnostics and maintenance*. 2004;47(11): 100-106

[4] Drugarin, C. A., Draghici, S., Raduca, E., *Team Viewer Technology for Remote Control of a Computer*, *Analele Universitatii'Eftimie Murgu'*, 2016., *23*(1), 61-66

[5] Advanced Technology. Preuzeto sa: https://advancedtechnology.com.au/remote-it-repair/ [Pristupljeno: srpanj 2020.]

[6] Macaulay T., RioT Control: Understanding and Managing Risks and the Internet of Things, Elsevier, Cambridge, United States, Morgan Kaufmann, 2016; 13(8): 141-155

[7] FleetGO. Preuzeto sa: https://fleetgo.com/kb/telematics/remote-diagnostics/ [Pristupljeno: srpanj 2020.]

[8] Br-Automation. Preuzeto sa: https://www.br-automation.com/sv/foeretaget/press-room/5-easy-steps-to-remote-maintenance-01-01-1970/ [Pristupljeno: srpanj 2020.]

[9] ICT Standards. Preuzeto sa: http://www.moct.gov.sy/ICTSandards/en_pdf/21.pdf [Pristupljeno: kolovoz 2020.]

[10] SearchSecurity: Preuzeto sa: https://searchsecurity.techtarget.com/definition/remote-access [Pristupljeno: kolovoz 2020.]

[11] Celestix. Preuzeto sa: https://www.celestix.com/client-based-remote-access-vpn-protocol-overview/ [Pristupljeno: kolovoz 2020.]

[12] Valencia, A. J.: *U.S. Patent No. 6,487,598. Washington, DC: U.S. Patent and Trademark Office*, 2002

[13] Comstock, D. R.: *U.S. Patent No. 6,452,920. Washington, DC: U.S. Patent and Trademark Office*, 2002

[14] SolarWinds. Preuzeto sa: https://www.solarwindsmsp.com/products/rmm?_ga=2.104317888.1728639749.1596210507-419578850.1596210507 [Pristupljeno: kolovoz 2020.]

[15] NinjaRMM. Preuzeto sa: https://www.ninjarmm.com/rmm/mobile-app/ [Pristupljeno: kolovoz 2020.]

[16] NinjaRMM. Preuzeto sa: https://www.ninjarmm.com/compare/solarwinds-alternative/?utm_source [Pristupljeno: rujan 2020.]

[17] Learning Hub. Preuzeto sa: https://learn.g2.com/two-factor-authentication [Pristupljeno: kolovoz 2020.]

[18] IEEE Xplore. Preuzeto sa:https://ieeexplore.ieee.org/abstract/document/7098042 [Pristupljeno: kolovoz 2020.]

[19] Google Patents. Preuzeto sa: https://patents.google.com/patent/US5123017A/en [Pristupljeno: kolovoz 2020.]

[20] InHand Networks. Preuzeto sa: https://www.inhandnetworks.com/solutions/industrial-robot-remote-monitoring.html [Pristupljeno: kolovoz 2020.]

[21] ScienceDirect. Preuzeto sa: https://www.sciencedirect.com/science/article/pii/S1525505020305552 [Pristupljeno: kolovoz 2020.]

POPIS ILUSTRACIJA

POPIS SLIKA

POPIS TABLICA

POPIS GRAFIKONA

POPIS KRATICA

KRATICA	PUNI NAZIV
2FA	(engl. *Two Factor Authentication*) Drugi faktor autentifikacije
BYOD	(engl. *Bring Your Own Device*) Termin korištenja osobnog uređaja u poslovne svrhe
CCP	(engl. *Compression Control Protocol*) Kompresijski kontrolni protokol
DHCP	(engl. *Dynamic Host Configuration Protocol*) Protokol dinamičke konfiguracije
DNS	(engl. *Domain Name Server)* Decentralizirano dodjeljivanje imena sustava
DSL	(engl. *Digital Subscriber Line*) Digitalna pretplatnička linija
EAP	(engl. *Extensible Authentification Protocol*) Protokol proširene autentifikacije
ECP	(engl. *Encryption Control Protocol)* Protokol kontrole enkripcije
HTTP	(engl. *Hyper-Text Transfer Protocol)* Protokol za pristup podacima postavljenima na Internetu klikom na poveznicu
ICMP	(engl. *Internet Control Message Protocol*) Protokol Internetske kontrolne poruke
IoT	(engl. *Internet of Things)* Internet stvari
IPsec	(engl. *Internet Protocol Security)* Sigurnosni Internet protokol
ISP	(engl. *Internet Service Provider*) Davatelj internetske usluge
L2TP	(engl. *Layer Two Internet Protocol*) Protokol tuneliranja u svrhu pružanja podrške virtualnoj privatnoj mreži
LAN	(engl. *Local Area Network)* Lokalna mreža
LCP	(engl. *Link Control Protocol*) Protokol kontrole linka

LTE	(engl. *Long Term Evolution)* Mobilna 4G mreža
MPPE	(engl. *Microsoft Point-to-Point Encryption)* Microsoft enkripcija od točke do točke
MSP	(engl. *Managed Service Provider*) Davatelj usluge upravljanja
MQTT	(engl. *Message Queuing Telemetry Transport*) Protokol koji omogućava prijenos i prevođenje poruke između uređaja
NPM	(engl. *Network Performance Monitor*) Praćenje mrežni performansi
PLC	(engl. *Programmable Logic Controller)* Logički programski upravljač
PPP	(engl. *Point-to-Point Protocol)* Protokol od točke do točke
PPTP	(engl. *Point-to-Point Tunneling Protocol*) Protokol tuneliranja od točke do točke
RAT	(engl. *Remote Access Trojan)* Trojanski virus udaljenog pristupa
RMM	(engl. *Remote Maintenance Monitoring*) Udaljeno praćenje održavanja
RRDM	(engl. *Remote Repair, diagnostics and mainteance)* Udaljeno popravljanje, dijagnostika i održavanje
SLIP	(engl. *Serial Line Internet Protocol*) Enkapsulacija Internet protokola za rad preko serijskih portova
SNMP	(engl. *Simple Network Management Protocol*) Protokol za upravljanje jednostavnom mrežom
TCP	(engl. *Transmission Control Protocol*) Protokol kontrole transmisije
UDP	(engl. *User Data Protocol*) Komunikacijski protokol
UMTS	(engl. *Universal Mobile Telecommunications System)* Mobilna 3G mreža

VPN	(engl. *Virtual Private Network)* Virtualna privatna mreža
WAN	(engl. *Wide Area Network*) Mreža širokog područja
WI-FI	(engl. *Wireless Fidelity*) Bežična lokalna mreža
WLAN	(engl. *Wireless Local Area Network)* Bežična lokalna mreža
WMI	(engl. *Windows Management Instrumentation*) Protokol za instrumentaciju upravljanja sustavom Windows

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

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

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

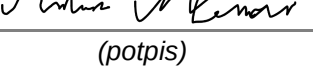
Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog rada pod naslovom **Udaljeno održavanje informacijsko-komunikacijskih sustava**

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

Student/ica:

U Zagrebu, 7.9.2020.



(potpis)