UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

ANALIZA SELITVE TEHNOLOŠKE ARHITEKTURE V OBLAK V OSNOVNI ŠOLI MILANA ŠUŠTARŠIČA

Ljubljana, oktober 2020 MATJAŽ PUCELJ

IZJAVA O AVTORSTVU

Podpisani Matjaž Pucelj, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom Analiza selitve tehnološke arhitekture v oblak v osnovni šoli Milana Šuštaršiča, pripravljenega v sodelovanju s svetovalcem red. prof. dr. Tomažem Turkom

I Z J A V L J A M

1. da sem predloženo delo pripravil samostojno;

2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;

3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbel, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani;

4. da se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;

5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;

6. da sem pridobil vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označil;

7. da sem pri pripravi predloženega dela ravnal v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobil soglasje etične komisije;

8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;

9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu preko Repozitorija Univerze v Ljubljani;

10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi.

V Ljubljani, dne 2. 10. 2020 Podpis študenta: _____

KAZALO

KAZALO TABEL

KAZALO SLIK

SEZNAM KRATIC

angl. - angleško
AaaS – (angl. Application as a Service); aplikacij kot storitev
ARNES – (angl. Academic and Research Network of Slovenia); Akademska in raziskovalna mreža Slovenije
ARP – Address Resolution Protocol
ARPANET – (angl. Advanced Research Projects Agency Network); Omrežje agencije za napredne projekte
AWS – Amazon Web Services
BS3 – Bežigrajska soseska 3
EC2 – Elastic Compute Cloud
CaaS – (angl. Compliance as a Service); upravljanje skladnosti kot storitev, (angl. Communication as a Service); komuniciranje kot storitev, (angl. Computing as a service); računalništvo kot storitev
CSA – Cloud Secutiry Alliance
CRaaS – (angl. Customer Relationship as a Service); odnos s strankami kot storitev
CRM – (angl. customer relationship management); upravljanje odnosov s strankami
DHCP – Dynamic Host Configuration Protocol
DSaaS – (angl. Data Storage as a Service); podatkovna hramba kot storitev
EDUROAM – education roaming
EU – Evropska unija
FRI – Fakulteta za računalništvo in informatiko Ljubljana
GDPR – (angl. General Data Protection Regulation); splošna uredba Evropske unije o varstvu podatkov
IaaS – (angl. Infrastructure as a Service); infrastruktura kot storitev
IDaaS – (angl. Identity as a Service); identiteta kot storitev
IKT – informacijsko komunikacijska tehnologija
IoT – (angl. Internet of Things); internet stvari
IP Address – (angl. Internet Protocol Address); naslov internetnega protokola
IPv4 – (angl. Internet Protocol version 4); internetni protokol verzije 4
IPv6 – (angl. Internet Protocol version 6); internetni protokol verzije 6
IS – informacijski sistem
ISO – (angl. International Standards Organisation); Mednarodna organizacija za standarde
IT – informacijska tehnologija
MaaS – (angl. Monitoring as a Service); nadzorovanje kot storitev
MIT – Massachusetts Institute of Technology
NaaS - (angl. Network as a Service); omrežje kot storitev

NIST - (angl. National Institute of Standards and Technology); Nacionalni inštitut za standarde in tehnologijo
OŠ – osnovna šola
PaaS – (angl. Platform as a Service); platforma kot storitev
RAM – delovni spomin
RFID – Radio-frequency identification
SaaS – (angl. Software as a Service); programska oprema kot storitev
SLA – (angl. service-level agreement); sporazum o ravni storitev
StaaS – (angl. Storage as a Service); skladiščenje kot storitev
UPS – (angl. Uninterruptible Power Supply); brezprekinitveno napajanje
VPN – Virtual Private Network
XaaS – (angl. X as a Service); karkoli kot storitev

UVOD

Delovanje organizacij je pogojeno z delovanjem njihovega informacijskega sistema. Vsaka organizacija ima svojo naravo dela. Tako se informacijska infrastruktura prilagaja naravi dela in potrebam uporabnikom, v določenih primerih pa tudi obratno, kjer se mora organizacija zaradi tehničnih omejitev prilagajati informacijski infrastrukturi. Investicije v samo opremo za zagotavljanje delovanja tehnološke arhitekture lahko tako pomenijo visok vložek za vzpostavitev delovanja okolja.

V današnjem času smo v obdobju, ko se je računalništvo v oblaku razvilo že do te mere, da se sistemi počasi selijo v različne modele oblakov in nadomeščajo različne računalniške sestave iz organizacije v gostovanje k ponudnikom oblačnih storitev. Kdaj bo organizacija selila storitev iz lastnih strežnikov, je zapisano v članku, ki je lahko v pomoč pri oceni stroškov sistemov, ki temeljijo na oblaku (Kratzke, 2012; Chang, Hsu, Huang & Chen, 2019). Pomembno se je zavedati tveganja zlorabe podatkov pri ponudniku storitve v oblaku, saj je tu možnost zlorabe višja (Aleem & Sprott, 2013). Ne glede na rast in razcvet ponudbe storitev računalništva v oblaku so avtorji v ameriških raziskavah glede zaupanja še vedno nezaupljivi in verjamejo, da bodo v prihodnosti same oblačne rešitve bolj zaupanja vredne in bodo lahko nadomeščale trenutne sisteme (Kajiyama, Jennex & Addo, 2017).

Ne glede na dvome o varnosti storitve in tehnologijo oblaka obstajajo različni izračuni, kako lahko izobraževalne organizacije privarčujejo na proračunu (Pardeshia, 2014). Potrebe po hitrem spreminjanju strojne in programske opreme ga s pomočjo tehnologij računalništva v oblaku olajšajo prilagajanju razmeram. Institucije, ki so se odločile za premik v oblak, tako pričakujejo, da bodo privarčevale tudi do 20 % namenskih stroškov. To predstavlja velik premik v pristopu organizacijske učinkovitosti, izboljšanja agilnosti in spodbujanju inovacij. Poleg vsega naštetega pripomorejo tehnologije tudi pri posodobitvi in poenotenju izobraževalnih vsebin ter boljšemu sodelovanju med izobraževalnimi zavodi (Pardeshia, 2014).

Za potrebe javne uprave sta slovenska avtorja (Dečman & Vintar, 2013) proučevala možnosti za centralno skladiščenje podatkov znotraj okvirjev oblaka. Oblak skupnosti se tako dobro prilega ideji centraliziranega zaupanja vrednega skladišča za digitalno shranjevanje vsebin. Ta shramba podatkov bi tako bila namenjena vsem javnim institucijam in predstavlja organizacijski premik v procesih upravljanja digitalnih zapisov in dokumentov. Sistem naj bi omogočal pregleden in varen ter takojšen dostop do dokumentov glede na potrebe po dostopu do lastnih ali morebiti tudi vsebin drugih institucij, odvisno od ustreznosti politik dostopa. Da bi takšen koncept sistema lahko kdaj v resnici zaživel, je ključnih več dejavnikov, ki pa so odvisni od vodstvenih organov države, ki bi morali zagotoviti ustrezna finančna sredstva, oblikovati strategije in standarde, ki temeljijo na dobrih praksah in ustrezni obstoječi zakonodaji, ki bi potrebovala verjetno tudi nekaj

sprememb (Dečman & Vintar, 2013). Čeprav so možnosti enega skupnega centralnega skladišča za podatke v državi v fazi raziskovanja in oblikovanja, imajo države v Evropski uniji in tudi Sloveniji že predloge za rešitve ter vpeljane nekatere storitve v oblaku oz. oblikovano infrastrukturo računalništva v oblaku. Avtorja (Ujčič & Florjančič, 2017) ugotavljata težave z neobstojem pravnega okvira, pomanjkanjem ustreznih standardov in smernic za računalništvo v oblaku. Javna uprava sicer ima vzpostavljen državni računalniški oblak, ki pa je namenjen storitvam javne uprave. Ta temelji na prenovi državnih informacijskih sistemov.

Znanje o računalništvu v oblaku po slovenskih raziskavah (Ujčič & Florjančič, 2017) v javni upravi je zelo pomanjkljivo in je podobno kot v tujini. Ljudje imajo še vedno premalo zaupanja v sisteme v oblaku, ko se sprašujemo po zagotavljanju varnosti in možnostjo izgube ali zlorabe podatkov. To je še vedno najbolj pogosti negativni vidik možnosti uporabe računalništva v oblaku. Kot prednosti uporabniki izpostavljajo večjo interoperabilnost programskih rešitev in podatkov ter standardiziranje informacijskih sistemov. Za lažjo uporabo bi bilo treba zagotoviti ustrezen sistematični pristop izobraževanja, da lahko uporabniki lažje razumejo koncept in prednosti delovanja oblačnih arhitektur, saj se veliko ljudi o tem izobražuje samoiniciativno in je lahko preveč površinsko in pomanjkljivo. Ne glede na ugotovitve o pomanjkljivostih o znanju in možnih dvomov o varnosti pretehtajo pozitivni učinki o računalništvu v oblaku in predstavljajo pravo smer nadaljnjega razvoja slovenske državne informatike in tako sledijo trendom po svetu (Ujčič & Florjančič, 2017).

S širitvijo omrežne infrastrukture oblak zagotavlja nov način shranjevanja in dostopa do virov na zanesljiv, udoben in že omenjen cenovno dostopen tehnološki način. Populariziran in uveljavljen je v številnih inovacijah in močno vpliva na trend upravljanja poslovnih procesov, predvsem virov v skupni rabi. Zaradi pozitivnih lastnosti oblaka in prilagodljive uporabe je v razvoju interneta stvari (angl. Internet of Things – IoT) tehnologija oblaka postala podatkovno in obdelovalno središče. Pri tem se postavlja vprašanje z realizacijo, saj je ta močno odvisna od napredka v razvoju tehnologije in uporabe ter vprašanj o zagotavljanju varnega okolja. Na tem mestu je v prvi vrsti razvoj zagotavljanja varnosti oblaka, saj so podatki običajno občutljive narave. Glede na lastnosti oblaka: razširljivost, fleksibilnost, uporabnost, se predvideva prevladovanje storitev v oblaku, saj bo omogočala visoke hitrosti prenosa in s tem lažjega dostopa in selitve podatkov v oblak. Oblak bo tako komuniciral s tehnologijami ter se tako internet stvari prilagodil okolju oblaka (Viswanatham, 2016).

Pomembno vlogo pri selitvi v oblak igrajo tudi stroški, ki vplivajo tako na razvoj nadaljnjih storitev, saj se pogosto kot prednost računalništva v oblaku omenja prav varčevanje pri vlaganju v primerjavi s staro obstoječo lokalno arhitekturo. Pri tem moramo biti pozorni, saj se nam lahko predvidevanja hitro porušijo. Treba je biti pozoren, kako izračunati resnične stroške selitve v oblak. Poznati je treba trenutne stroške infrastrukture informacijske tehnologije (v nadaljevanju IT), izračunati moramo ocenjene stroške infrastrukture v oblaku. Pomembno je oceniti stroške izvedbe v oblak, ki je odvisna tako od vrste kot tudi modela

oblaka. Ko smo enkrat arhitekturo že selili v oblak, predstavljajo pomembne stroške tudi stroški, povezani po selitvi v oblak, navezujejo se lahko tako v nadaljnji razvoj novih aplikacij, ki so prilagojeni novim sistemom ali pa vzdrževanja delovanja v oblaku. Nastanejo lahko tudi različni nepredvidljivi stroški same infrastrukture v oblaku. Ko so vsi stroški sešteti, se lahko te stroške primerja z materialnimi in nematerialnimi koristmi in hitra računica izpostavi dobre lastnosti storitev v oblaku in tudi nižje stroške (Chan, 2017). Ne glede na pozitivne posledice, ki naj bi jih prinašal oblak, obstajajo tudi potencialna tveganja migracije. Ta se navezujejo na občutljivost podatkov in vzrok selitve v oblak. Ko je enkrat sistem postavljen v oblaku, predstavlja selitev k drugemu ponudniku lahko velik izziv, saj sistemi običajno med seboj niso kompatibilni. To je omenjenih le nekaj potencialnih tveganj migracije, ki jih obravnavajo avtorji v članku *Tveganja in koristi migracij v oblaku* (Cook, 2019).

Migracije je mogoče izvesti na več načinov, izpostavi se štiri fazni Microsoftov in Amazonov šest fazni pristop. Ker ima vsak od predlaganih izvedb migracij določene pomanjkljivosti, ki jih avtorja (Dukarić & Jurič, 2011) v članku *Migracija obstoječih aplikacij in platforme za računalništvo v oblaku* proučita, zato predlagata svoj pristop. Ta predvideva tri različne faze s podprocesi in v grobem predvideva fazo raziskave, preizkusa in izvedbe. Podprocesi prvega koraka so tako izbira ustreznega ponudnika, analiza trenutnega stanja ter načrtovanje. V drugem koraku se izvede evalvacijo stroškov, varnosti, zakonodaje in tehničnih lastnosti. Nato sledi izdelava pilotnega testnega projekta, kjer v oblaku testiramo naše aplikacije, če zadeva deluje v skladu z našimi pričakovanji, da se lahko prepričamo o ustreznosti karakteristik tehnološke arhitekture. Za tretji korak so opredeljeni naslednji postopki: najprej se izvede migracijo podatkov v oblak, sledi migracija aplikacij in na koncu optimizacija glede na prednosti oblaka, da se lahko izboljša delovanje samega sistema in zmanjšamo stroške (Dukarić & Jurič, 2011).

Oblak modela arhitekture infrastruktura kot storitev (angl. Infrastructure as a Service, v nadaljevanju IaaS) je najbolj obsežena storitev. Uporabnik dobi v uporabo pomnilniške in procesorske kapacitete ter prostor za hrambo, sam pa vzpostavit celotno sistemsko arhitekturo. Zagotavljanje varnosti v tem modelu oblaka je predvsem zaradi kompleksnosti arhitekture samega sistema zelo zapleten proces. Varnost je treba zagotavljati na dveh nivojih, administratorji arhitekture IaaS in tudi administratorski uporabniki oblaka. Pomembno je, da ponudnik storitve, ki vzdržuje strojno in programsko opremo za delovanje oblačnih storitev, poskrbi za ustrezno varovanje in arhiviranje sistema. Pomembno je tudi, da napadalcu preprečimo, da ne uspe pridobiti pravic in dostopov v sistem, saj lahko v najslabšem primeru prevzame nadzor nad celotno arhitekturo oblaka, s tem pa tudi do vseh podsistemov, ki jih upravljajo uporabniki sami. Drugi pomembni nivo je zagotavljanje varnosti na nivoju uporabnika oblaka infrastrukture kot storitve. Vsak uporabnik ima svoj oblak, kjer ima svoj samostojen sistem. Napad v sistemu virtualnega okolja, če je sistem zadostno varovan s strani ponudnika, se ne razširi na ostala okolja in tudi ne na sam virtualizator oz. sistem za zagotavljanje oblačne storitve. Uporabnik mora poskrbeti za

ustrezno varovanje svojega okolja. Uporabljati morajo dovolj močna gesla, ustrezno avtentikacijo in ostale pripomočke za zagotavljanje zadostne varnosti. Pred začetkom uporabe sistema je pomembno, da si zastavimo ustrezna varnostna vprašanja v smislu uporabe in izpostavljenosti tveganja, saj le tako dobimo predstavo, kako močno je priporočljivo varovati sistem. Ker je arhitektura oblaka modela infrastrukture kot storitve obsežna in zajema različne sisteme, so pripravljeni za zagotavljanje celostnega varovanja varnostni kontrolni seznami, ki opomnijo uporabnika, kje vse je treba zagotoviti zaščito, da bi bili sistemi ustrezno varovani (Chawkia, Ahmed & Zakariaea, 2018).

Na migracijo v storitve oblaka tako vpliva veliko različnih omenjenih dejavnikov, zato moramo biti na selitev dobro pripravljeni in imeti pripravljene tudi rezervne načrte. Vsi postopki načrtovanja morajo biti večkrat preverjeni. Stroške selitve v oblak je treba dobro predvideti in biti pripravljen tudi na dodatne investicije v samo vzpostavitev. Lahko se izkaže, da določenih sistemov niti ni mogoče trenutno še preseliti v oblak. Za to je lahko kriva tudi lokalna mrežna povezava, ki trenutno še ne omogoča ustreznih željenih hitrosti povezave, s tem pa to pomeni ustavitev prenosa. Da sistemi v oblaku delujejo, je lahko hitrost odzivanja ključnega pomena, saj neodzivne aplikacije pomenijo neuspešen proces migracije. Možne so sicer selitve najprej samo manjših delov sistema v oblak in s tem postopno migracijo, vseeno pa je treba biti dovolj informiran o tem, če je delna izpeljava sploh smiselna.

Za magistrsko nalogo sem si zastavil raziskovalno vprašanje na realnem primeru. Sprašujem se, kako v organizaciji, kjer sem trenutno zaposlen, nadomestiti lokalni strežnik s strežnikom v oblaku z infrastrukturo kot storitvijo, ki podpira poslovni informacijski sistem šole ter tiskalniški strežnik in poiskati najbolj primeren način izvedbe.

Lokalni infrastrukturi, kjer trenutni sistemi delujejo, se počasi izteka življenjska doba. Računalništvo v oblaku pa je ena iz med možnosti, ki bi nam lahko ponujala ustrezno rešitev za zamenjavo obstoječe arhitekture.

Cilji magistrskega dela, ki jih želim doseči, so:

- proučiti trenutno stanje tehnološke arhitekture v organizaciji, ki jo želimo seliti v oblak;
- ugotoviti, katere rešitve računalništva v oblaku ustrezajo željam in zahtevam organizacije, da uspešno izpeljemo selitev v oblak, če je to seveda sploh mogoče;
- raziskati varnostna tveganja in omejitve ter poskrbeti za pripravo ustreznih varnostnih rešitev, ki bodo varovala sistem, primerno občutljivosti podatkov, ki se bodo obdelovali v oblaku (varovanje sistema, podatkov in skladnost s splošno uredbo Evropske unije o varstvu podatkov);
- preveriti različne domače in tuje ponudnike, ki ponujajo infrastrukturo kot storitev, ki naj bi uporabili pri selitvi v oblak;
- preveriti finančne prednosti s selitvijo v oblak v primerjavi z nakupom nove računalniške opreme;

- vzpostavitev testnega okolja, kjer se preveri odzivnost in delovanje sistema. Na podlagi tega se nato odloči za izvedbo selitve v oblak;
- izvedba selitve in vzpostavitev delujoče tehnološke arhitekture v oblaku, vzdrževanje;
- preučiti, raziskati možnosti za nadaljnji razvoj in nadgradnjo.

Teoretični del magistrskega dela bo temeljil na raziskovanju teme selitve tehnološke arhitekture v oblak s pomočjo kvalitativne metode. Značilnost te metode je, da se sestavi celota iz več različnih virov podatkov, pri tem pa manj pomembne informacije spustimo, naš fokus pa ostane na tistih, ki so za nas pomembnejši (Patton, 2002). Pregledal bom domačo in tujo literaturo, ki obdela različna področja računalništva v oblaku. Poudarek je selitev v oblak, varnost in tudi finančne prednosti. Proučil bom različne podatke in poglede, ki se nanašajo na računalništvo v oblaku, ter tudi teoretske vidike, ki opisujejo različne situacije in stanja. S to kombinacijo različnih virov si bom zagotovil celovitejši vpogled v moj problem (Lobe, 2006).

Sledila bo izvedba analize stanja. Analiziral bom trenutno stanje tehnološke arhitekture v organizaciji in raziskal potrebe organizacije. Za to bom opravil razgovore z uporabniki, ki so najbolj odvisni od uporabe poslovno-informacijskega sistema in strežnika za tiskanje ter tudi odgovornimi vodstvenimi osebami. Na podlagi pridobljenih informacij bom oblikoval predlog potreb, te pa primerjal z ustreznostjo ponudnikov, ki so na razpolago. Izpeljati bo treba tudi finančno analizo selitve infrastrukture v oblak in izvesti primerjavo z nakupom nove računalniške opreme. Priprava na selitev predvideva pripravo testnega okolja za testiranje in smiselnost selitve k izbranemu ponudniku. V primeru uspešnega testnega preizkusa sledi selitev, ki bi se izvedla postopoma po delih, saj je organizacija različno odvisna od komponent tehnološke arhitekture. Na koncu sledi še analiza uspešnosti izvedbe ter predlogi za nadaljnjo nadgradnjo in vzdrževanje.

1 PREDSTAVITEV OSNOVNE ŠOLE MILANA ŠUŠTARŠIČA

Osnovna šola Milana Šuštaršiča je javni vzgojno-izobraževalni zavod, ki ga je leta 1980 ustanovila Mestna občina Ljubljana. Šola se v Ljubljani nahaja v neposredni bližini naselja bežigrajska soseska 3 (BS3) za Bežigradom. V šolski okoliš je vključeno omenjeno naselje, ulice v okolici šole do Dunajske ceste ter območje Stožic med Dunajsko cesto in hipodromom Stožice. Ker je oddaljenost nekaterih učencev od šole daljša, šola tem zagotavlja tudi prevoz.

Šolo trenutno obiskuje več kot 550 učencev, ki so razporejeni v 25 oddelkov od 1. do 9. razreda. Za nemoteno izvajanje vzgojno-izobraževalnega procesa tako skrbi več kot 80 zaposlenih.

Šolski prostor je omejen z ograjo, kjer imajo učenci prostor za izvajanje različnih dejavnosti. Poleg velike travnate površine je na šolskem prostoru več igrišč, stez in zarisanih poligonov ter učilnica na prostem. Šolski objekt sestavljajo učilnice in kabineti, od leta 2018 nov

prizidek za prve razrede, garderobe, večja in manjša telovadnica, knjižnica, zbornica, šolska kuhinja in prostor vodstva šole.

1.1 Delovanje in organiziranost šole

Šolo upravljata ravnateljica in svet šole, ki ga zastopajo predstavniki Mestne občine Ljubljana, delavcev šole in staršev. Strokovni organ šole zastopa učiteljski zbor, oddelčni učiteljski zbori, razredniki in strokovni aktivi.

Za organizirano uresničevanje interesov staršev je v šoli odgovoren svet staršev. Sestavljen je tako, da ima v njem vsak oddelek po enega predstavnika, ki ga starši izvolijo na roditeljskem sestanku oddelka.

Učenci so organizirani v oddelčne skupnosti. Za uveljavljanje svojih interesov se oddelčne skupnosti povezujejo v šolsko skupnost učencev in v šolski parlament učencev.

V šolski knjižnici šola hrani, obdeluje in izposoja knjižnično gradivo ter z referenčnimi pogovori knjižničarka svetuje pri izbiri gradiva učencem šole, ki so poleg zaposlenih na šoli uporabniki knjižnice. Učenci si lahko izposojajo knjižna gradiva, multimedijske in serijske publikacije pa so na voljo samo za uporabo v prostorih knjižnice, tako z leposlovno kot poučno tematiko.

Šola omogoča učencem, da si izposodijo učbenike iz učbeniškega sklada. Učbeniški komplet si izposodijo tisti učenci, ki so oddali soglasje za vsa leta šolanja.

V šolskem skladu se zbirajo sponzorska sredstva, prostovoljni prispevki staršev, sredstva, pridobljena na sejmih in prireditvah. Upravni odbor šolskega sklada zbrana sredstva porabi za sofinanciranje dejavnosti socialno ogroženim učencem, za nagrade učencem, za nabavo in organizacijo nadstandardnih storitev za učence in podobno. Namensko donirana sredstva pa se porabijo za namen, za katerega so bila pridobljena.

Šola zagotavlja štiri obroke, na katere se učenci lahko naročijo. Poleg malice šola zagotavlja še zajtrk za učence, ki obiskujejo jutranje varstvo, kosilo in popoldansko malico za tiste učence, ki ostajajo v podaljšanem bivanju.

Predmetnik učencev je sestavljen iz osnovnih predmetov, ki so obvezni za vse učence. Šola ponuja tudi dodatne neobvezne predmete za učence od 4. do 6. razreda in obvezne izbirne predmete za učence od 7. do 9. razreda. Vsi predmeti se ocenjujejo z ocenami od 1 do 5, od 3. razreda naprej, učenci 1. in 2. razreda pa so ocenjeni z opisno oceno.

V sklopu pouka imajo učenci poleg osnovnih, obveznih in neobveznih predmetov, na izbiro tudi različne interesne dejavnosti internih in zunanjih izvajalcev. Šola sodeluje v različnih projektih, tudi mednarodnih. Povezana je z različnimi šolami v tujini, kjer med njimi potekajo različne interdisciplinarne dejavnosti.

Pouk je organiziran od predure, ki se začne ob 7.30 in se zaključi najkasneje do 16.05, ko se končajo zadnje interesne dejavnosti. Večina pouka se običajno zaključi do 13.35. Šola staršem učencev nižjih razredov omogoča tudi jutranje varstvo od 6.30 ure dalje in tudi po pouku podaljšano bivanje oz. popoldansko varstvo do 17. ure (Osnovna šola Milana Šuštaršiča, 2019).

1.2 Uporaba informacijskih sistemov

Za Osnovno šolo Milana Šuštaršiča sta za nemoteno delovanje pomembna dva informacijska sistema, to sta Lo.Polis in SAOP iCenter.

Lo.Polis je informacijski sistem, ki zajema celoten spekter pedagoškega dela. Sestavlja ga več modulov. Osnovni modul Lo.Polisa je namenjen pedagoškim delavcem za izvajanje pedagoške dejavnosti. V portalu se vnašajo podatki o učencih, ocene, vpisi, komentarji, opravila in naloge, dnevnik, urnik, izpisi in druge dejavnosti. Pripravijo se lahko različni izpisi, tudi na tiskane obrazce, kot so na primer spričevala ali ostala potrdila. Sistem je enoten za vse delavce znotraj organizacije in dostopajo do istih podatkov, glede na dodeljene pravice. Po vnosu lahko do teh podatkov dostopajo vsi pooblaščeni udeleženci. Program omogoča staršem vpogled v elektronsko redovalnico in prejem elektronskih sporočil.

Z modulom za prehrano ima vodja kuhinje pregled nad številom prijavljenih in odjavljenih obrokov in tudi nad realizacijo izdanih obrokov. Organizator šolske prehrane v tem modulu ureja abonente in pripravlja podatke za pripravo obračunavanja obrokov.

Modul za elektronsko dokumentacijo omogoča evidentiranje dokumentiranega gradiva v elektronski obliki, ki je opremljen z revizijsko sledjo, kar pomeni samodejno beleženje zapisov, ogledov in sprememb podatkov. Usklajen je z enotnimi tehnološkimi zahtevami Arhiva Republike Slovenije, Zakonom o varstvu dokumentarnega in arhivskega gradiva ter arhivih, Uredbi o varstvu dokumentarnega in arhivskega gradiva in Uredbi o upravnem poslovanju. Evidentirani dokumenti so povezani z rokom hrambe, ki je določen s klasifikacijskim načrtom. Ko dokumentu poteče rok hrambe, se s pomočjo programa izvede proces odbiranja ali izločanja gradiva.

Evidentiranje delovnega časa je modul, ki je oblikovan za vodenje evidence delovnega časa zaposlenih v osnovnih in srednjih šolah. Pred uporabo je treba postaviti obseg dela v skladu s šolskim koledarjem in zakonodajo, ki opredeljuje delovno in učno obveznost strokovnih delavcev. Ko je obseg dela pripravljen, zaposleni v sistem vpišejo podatke o realizaciji. Ta na podlagi vpisov in ostalih pogojev izračunava delovno obvezo.

Lo.Polis aplikacija je pred časom delovala samo kot program, nameščen na računalnik, ki je za delovanje nujno potreboval internetno povezavo za komunikacijo s strežniki podjetja Logos (lastnik Lo.Polisa), saj so podatki gostovali pri njih. V letu 2018 so ustvarili spletno aplikacijo, do katere se lahko dostopa z vsemi mobilnimi napravami, prek spletnega portala.

Vsi moduli še ne delujejo prek spleta, zato je možno nekatere module uporabljati izključno še po starem načinu, s pomočjo nameščenega programa na računalnik.

Informacijski sistem SAOP iCenter je poslovno-informacijski sistem in je prilagojen javnim zavodom. Namenjen je različnim ustanovam, kot so vrtci, osnovne šole, srednje šole ter ostalim javnim zavodom.

Javni zavodi imajo predpisane postopke delovanja, zato so funkcionalnosti programa optimizirane in prilagojene različnim organizacijam. Program je prilagojen za delo različnih služb, saj pri svojem delu uporabniki dostopajo in uporabljajo samo tiste funkcionalnosti, ki jih potrebujejo za svoja opravila.

Šola običajno uporablja funkcionalnosti programa za obdelavo podatkov, kot so glavna knjiga z davčno knjigo, plačilni promet in obračun obresti, osnovna sredstva in drobni inventar, obračun plač z obračunom dohodnine, obračun storitev, spremljanje plačil računov, knjiga prejetih računov z javnimi naročili malih in velikih vrednosti, blagajniško poslovanje, kadrovska evidenca, potni nalogi, materialno skladišče, fakturiranje storitev v šoli, naročanje materiala prek spleta in registracija prisotnosti zaposlenih.

Več o programu, kako je program nameščen in kako uporabniki dostopajo do storitve poslovno-informacijskega sistema, bom obravnaval v naslednjih podpoglavjih.

1.3 Pregled infrastrukture računalniškega omrežja

Objekt osnovne šole je opremljen z žičnim omrežjem v vseh učilnicah, kabinetih in ostalih prostorih, tako da se lahko vsak uporabnik poveže na računalniško omrežje s kablom.

Hitrost omrežne povezave je trenutno do 1 Gb/s, kar zadošča za vsa opravila, ki jih uporabniki opravljajo. Tudi v času, ko je omrežje bolj obremenjeno z večjim številom uporabnikov, ta deluje zadovoljivo in ne povzroča izpadov komunikacije.

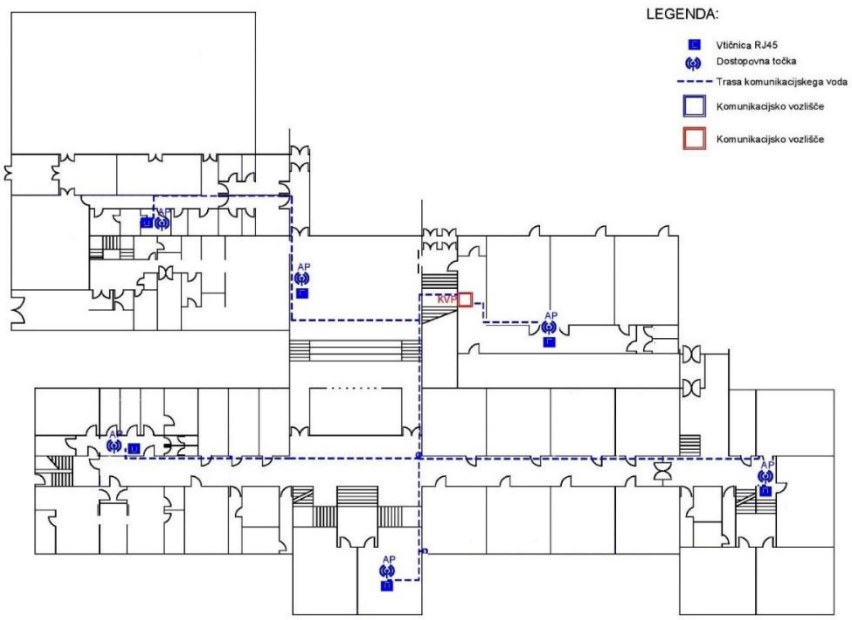
Organizacija bo v kratkem pridobila novo hitrejšo internetno povezavo, in sicer do hitrosti 10 Gb/s. Trenutno se izvajajo dela nadgradnje povezovalnih linij z optičnimi vlakni med komunikacijskimi vozlišči, ter čaka dobavo ustrezne nove opreme, ki bo omogočala tako visoke hitrosti prenosov podatkov.

Na objektu je nameščena tudi oprema za brezžično internetno povezavo. Trenutna oprema je stara skoraj 10 let in se bo, vzporedno z nadgradnjo internetne povezave in dograditvijo linij, dodalo tudi nove žične povezave za dodatne brezžične internetne dostopne točke. Trenutno šola razpolaga z opremo za brezžično omrežje, ki je lastno, centralizirano in upravljano iz krmilnika v glavnem vozlišču ter je povezano z vsemi osmimi brezžičnimi dostopnimi točkami. Tako je šola zadovoljivo preskrbljena z brezžično internetno povezavo v dobri polovici prostorov, določeni prostori imajo manjšo obremenitev ali pa je uporaba

prilagojena razpoložljivemu stanju s pogojno dobro povezavo, ostali prostori pa so odvisni od žične povezave za nemoteno delovanje prek internetne povezave.

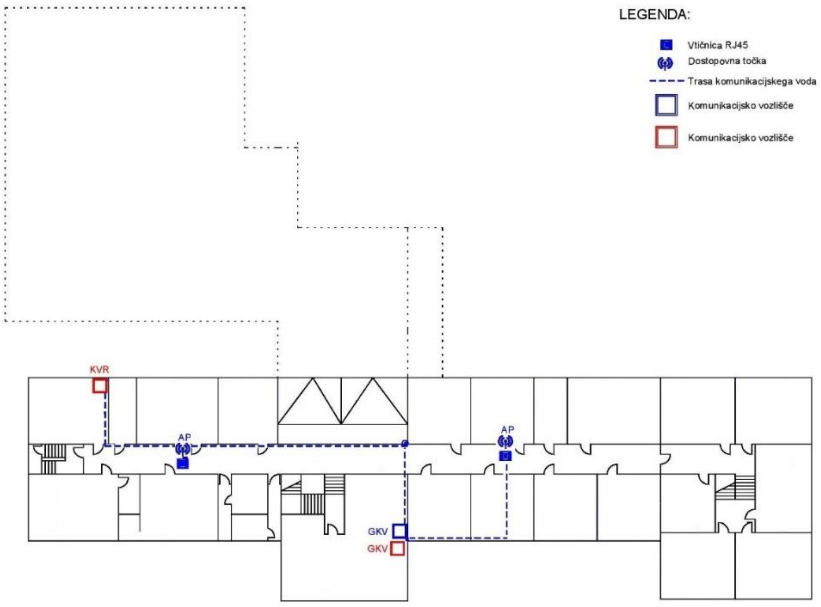
Sliki 1 in 2 prikazujeta shemi načrta trenutnega stanja brezžičnega omrežja na šoli, v pritličju in nadstropju šole.

Slika 1: Trenutno stanje brezžičnega omrežja v pritličju šole



Vir: lastno delo.

Slika 2: Trenutno stanje brezžičnega omrežja v nadstropju šole

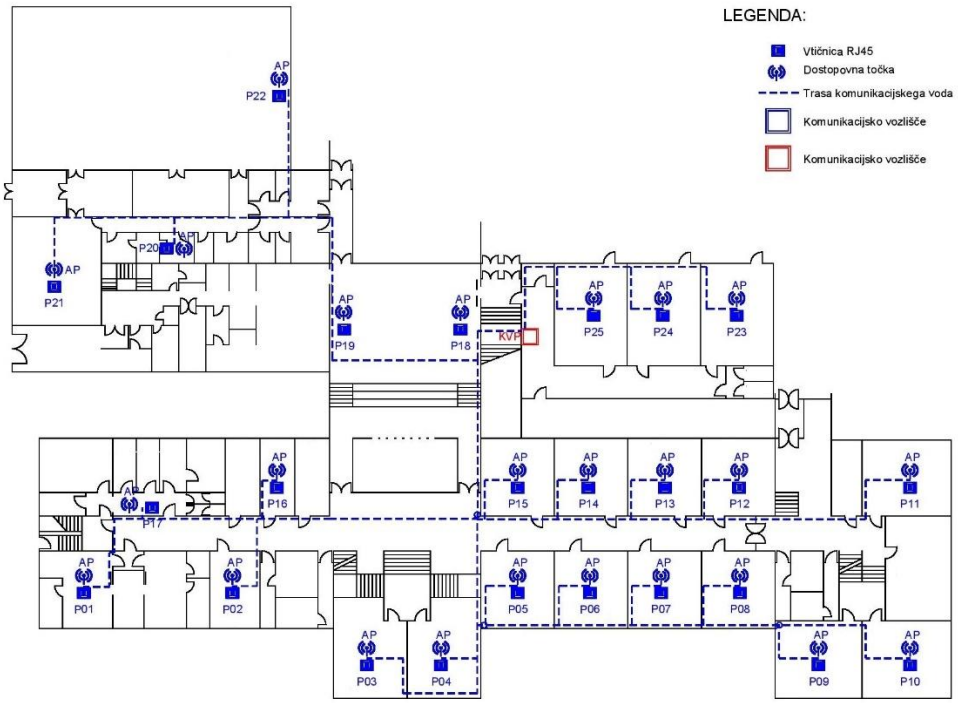


Vir: lastno delo.

Kot je bilo že omenjeno, bo nadgradnja omrežja omogočala višje hitrosti prenosa podatkov. Nadgradnja žičnega omrežja za brezžično omrežje bo po zaključenih delih zagotavljala priklop 44 dostopnih točk in popolno pokritost z brezžičnim omrežjem v vseh prostorih šole. Upravljanje dostopnih točk bo upravljano s pomočjo organizacije Akademska in raziskovalna mreža Slovenije (angl. Academic and Research Network of Slovenia, v nadaljevanju Arnes), ki tudi zagotavlja visoke hitrosti internetne povezave.

Sliki 3 in 4 prikazujeta shemo načrta novega brezžičnega omrežja in lokacijo vseh dostopnih točk.

Slika 3: Novo predvideno stanje brezžičnega omrežja v pritličju šole



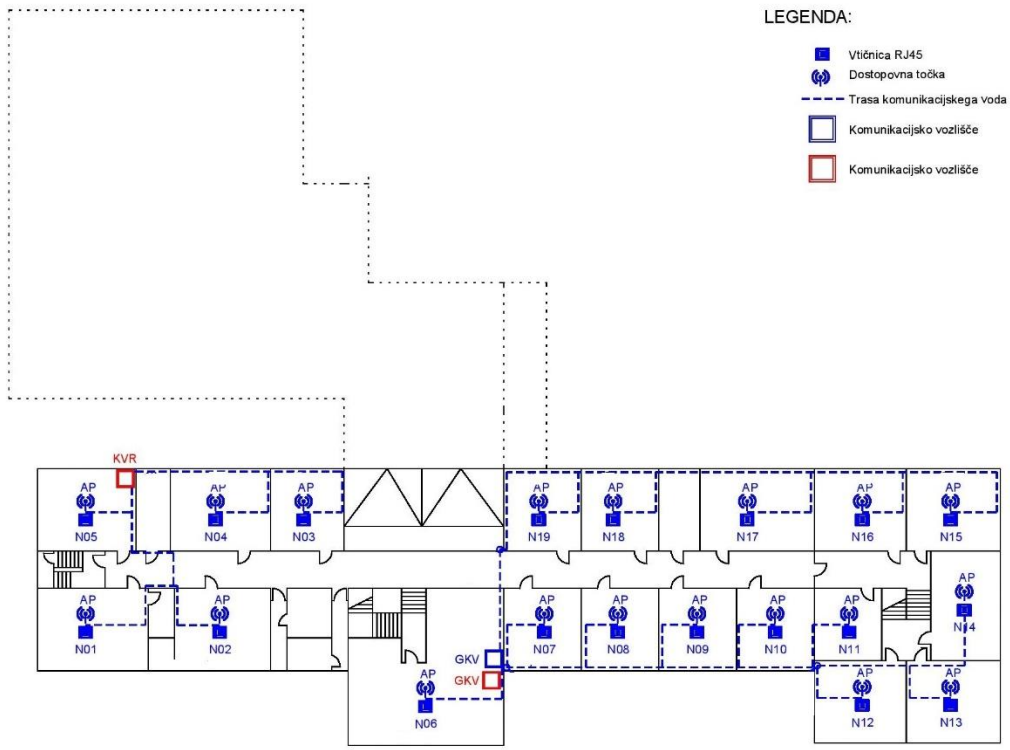
Vir: lastno delo.

Komunikacijska vozlišča so najpomembnejše točke za zagotavljanje internetne povezave. Šola ima zaradi svoje specifičnosti urejena 3 vozlišča, enega glavnega, kjer vstopi zunanja povezava z internetnim omrežjem, in še dva manjša.

V glavnem vozlišču, kot je bilo že omenjeno, je dovod zunanje povezanosti z internetom. Ta je zagotovljena po optični povezavi, ki jo zagotavlja organizacija Arnes. V to vozlišče komunikacijske omare so pripeljane povezave iz večine učilnic, razen tistih najbolj oddaljenih, za katere sta urejena pomožna vozlišča. Tu je pripeljana tudi dovodna povezava za telefonsko linijo, ki je prav tako zagotovljena s pomočjo optične povezave. Naprave, ki so nameščene, so glavno stikalo internetne povezave, ki jo zagotavlja Arnes, dodatna druga stikala za ustrezno zagotavljanje internih povezav po šoli, krmilnik za upravljanje dostopnih točk, povezave z dostopnimi točkami ter nadomestno napajanje (angl. Uninterruptible Power

Supply – UPS) za celotno komunikacijsko omaro, ki za nekaj ur, v primeru izpada, zagotavlja električno energijo za vse priključene naprave.

Slika 4: Novo predvideno stanje brezžičnega omrežja v nadstropju šole



Vir: lastno delo.

Dve manjši vozlišči sta urejeni zaradi večjega števila žičnih povezav na bolj oddaljenem koncu objekta in tako v tem delu zagotavljata povezanost v internetno omrežje. Oba manjša vozlišča sta trenutno z glavnim povezana z navadnim internetnim ožičenjem, saj ta še omogoča prenos podatkov do hitrosti, ki so trenutno omogočene. Ko bodo dela nadgradnje omrežja po šoli zaključena, bo med pomožnima vozliščema z glavnim delovala optična povezava. Da bo sistem prek optične povezave deloval nemoteno, bo treba zamenjati tudi nekatera obstoječa stikala, ker ta ne omogočajo optične povezave.

Šola ima urejena različna internetna podomrežja, ki so odvisna od namembnosti uporabe. Trenutno sta v delovanju aktivna dva različna, tretji pa bo aktiven, ko bo dokončana nadgradnja omrežja. Prvo podomrežje je namenjeno pedagoškemu delu, drugo pa delu za administracijo. Tretje, ki je še neaktivno, bo na voljo uporabnikom, ki imajo urejen eduroam dostop.

Vse naprave, priklopljene v različna podomrežja, tako delujejo neodvisno in tudi ne morejo ena do druge dostopati, če ni drugače konfigurirano. V podomrežje za pedagoško dejavnost so priključeni računalniki iz učilnic, kabinetov ter tudi brezžično omrežje za brezžične naprave. V tem podomrežju lahko uporabniki dostopajo do strežnika, kjer je skupni prostor

za izmenjavo datotek in tudi možnost tiskanja s tiskalnikov. Naprave, na katerih lahko uporabniki tiskajo, delujejo v odvisnosti od tega, v katerem podomrežju je naprava priklopljena.

Uporabniki administrativnega podomrežja imajo na voljo na enak način svoje brezžično in tudi žično omrežje za naprave. To je manjše in je namenjeno predvsem vodstvu in pisarnam, ki opravljajo administrativna in nepedagoška dela, povezano z organizacijo in vodenjem ustanove. V tem podomrežju imajo uporabniki omogočen dostop do strežnika, kjer je na voljo skupen prostor za nalaganje podatkov, in tudi dostop do tiskalnikov, ki delujejo le v tem podomrežju. V sklopu administrativnega delovanja naprav imajo uporabniki omogočen tudi dostop do poslovno-informacijskega sistema šole za vodenje in upravljanje. Do tega dostopajo računovodska služba, tajništvo in vodstvo šole.

1.4 Uporaba strežnika

Strežnik je računalnik, naprava ali program, ki je namenjen upravljanju omrežnih virov. Podatke s strežnika posreduje drugim napravam po lokalnem omrežju ali internetu oz. širokopasovnem omrežju. Strežniki so pogosto namenski, ker so namenjeni izvajanju namenskih nalog. Obstaja več kategorij strežnikov, in sicer tiskalniški strežniki, datotečni strežniki, omrežni strežniki in strežniki z bazami podatkov.

Strežnik je v organizaciji pomembna naprava, od katere je organizacija odvisna in v primeru izpada delovanja, pomeni nedostopnost do veliko različnih podatkov. Na njem se hranijo pomembni podatki in tudi različni sistemi, s katerimi se zagotavlja izvajanje različnih procesov.

Šola ima za ta namen poseben računalnik, ki je v stanju delovanja ves čas. Sistem je vzpostavljen na operacijskem sistemu Microsoft Windows Server. Na tem sistemu je nameščena namenska programska oprema Hyper-V, ki omogoča ustvarjanje navideznih oz. virtualnih računalnikov, zato se ta računalnik imenuje tudi virtualizator. Za zagotavljanje ustreznega prostora za podatke ima računalnik posebno diskovno polje, na katerem je priključenih 6 trdih diskov. Zaradi zagotavljanja neprestanega delovanja je za primere, če bi kateri od diskov prenehal delovati, vzpostavljen sistem treh paralelnih zapisovanj na dva diska hkrati. Tako so aktivni »le« trije diski, ostali trije pa so varnostna kopija. Operacijski sistem virtualizatorja tako teče na svojem diskovnem paru.

S pomočjo virtualizatorja sta tako ustvarjena še dva navidezna računalnika, prav tako z operacijskim sistemom Microsoft Windows Server. Preden se ustvarijo navidezni računalniki, se v virtualizatorju določi, koliko bodo zmogljivi ti navidezni računalniki. Zmogljivost teh računalnikov je tako odvisna od kapacitet, ki jih premore virtualizator. Zaradi različne namembnosti navideznih računalnikov sta ta dva po konfiguraciji popolnoma različna. Eden je namenjen delovanju kot datotečni, tiskalniški in domenski strežnik, drugi pa je namenjen za delovanje poslovno-informacijskega sistema. Več o delovanju teh dveh

navideznih računalnikov pa sledi v naslednjih dveh podpoglavjih Strežnik za izmenjavo podatkov in tiskanje ter Poslovno-informacijski sistem šole.

1.4.1 Strežnik za izmenjavo podatkov in tiskanje

Eden od virtualnih oz. navideznih računalnikov je namenjen bolj splošnemu oz. pedagoškemu delu. Ta je namenjen datotečnemu, tiskalniškemu in domenskemu strežniku.

Domena strežnika organizaciji omogoča, da lahko uporablja domenska uporabniška imena na različnih napravah, pri tem pa ima ta vedno dostopne vse svoje podatke, ki so shranjeni na strežniku. Uporabniki, ustvarjeni na domenskem strežniku, se urejajo s pomočjo enotne politike pravic. Uporabniška imena se lahko uporabljajo tudi za zagotavljanje ustreznih dostopov do podatkov ali storitev, ki so na strežniku na voljo. Tako je urejen poseben dostop samo za uporabo datotečnega sistema v skupni rabi. Uporabniki, ki imajo pravice za to storitev, lahko dostopajo in urejajo zgolj mape in datoteke. Sem lahko prenesejo, shranijo, ustvarijo, odstranijo mape in ostale datoteke. Taka uporaba se imenuje storitev datotečnega strežnika oz. strežnik za izmenjavo podatkov. Za preprečevanje pred izgubo podatkov se ti skupni podatki tudi redno kopirajo v oddaljeno napravo za arhiviranje. Tako je mogoče s programom za arhiviranje iz druge naprave pridobiti izgubljeno vsebino.

Isti virtualni računalnik se uporablja tudi za uporabo tiskalniškega strežnika. To pomeni, da so tiskalniki priključeni v računalniško omrežje in povezani s strežnikom. Povezani tiskalniki se upravljajo prek strežnika in tudi vsa opravila, ki jih izvedejo, se izvedejo iz strežnika. Tiskanje na določeni napravi se izvaja v eni čakalni vrsti za vsako napravo ločeno, tako v primeru več zahtevkov za tiskanje sledi časovno odvisno zaporedje, kdaj se bo katero opravilo izvedlo. Da lahko uporabniki uporabljajo storitve tiskalniškega strežnika, morajo prav tako kot pri datotečnem strežniku na svoji napravi uporabiti dostop do strežnika z uporabo domenskega uporabniškega imena. Ta ima omogočene pravice, da se naprava in tiskalnik med seboj povežeta. Ko je povezava uspešno vzpostavljena, programi omogočajo izbiro tiskalnika, povezanega prek strežnika. V tem primeru lokalni računalnik pošlje dokument za tiskanje na strežnik, ta ga tam prejme, doda v čakalno vrsto za tiskanje in ko pride na vrsto izvede tiskanje.

1.4.2 Poslovno-informacijski sistem šole

Osnovna šola Milana Šuštaršiča uporablja poslovno-informacijski sistem SAOP. Zaradi zahtevnosti programske rešitve je delovanje urejeno z ločenim virtualnim računalnikom. Temu je dodeljen ločen prostor za podatke in večja računalniška zmogljivost za namen obdelave podatkov.

Podatki iz sistema so za ustanovo ključnega pomena za vodenje in upravljanje. Z uporabo programskih modulov šola upravlja različna sredstva in svoje premoženje. V uporabi so

različna finančna orodja za prejem in izdajo računov, vodenje plačilnega prometa, vodenje in upravljanje sredstev in drobnega inventarja. Zelo pomemben je modul za izračunavanje plač, ki se posodablja in usklajuje z aktualnimi zakonskimi predpisi. Sistem vodi tudi kadrovsko evidenco z vsemi ustreznimi in pomembnimi podatki. Prek sistema se izdajajo tudi potni nalogi, ki se kasneje ustrezno obračunavajo, ter vsa ostala druga pomembna opravila.

Poseben dodaten modul je tudi modul za vodenje evidence delovnega časa oz. registrator delovnega časa. Ta deluje s pomočjo oddaljene enote za registracijo, prek katere uporabniki z uporabo radio frekvenčne identifikacije (angl. Radio-frequency identification – RFID) registrira svoj prihod na delovno mesto in odhod z delovnega mesta.

Poslovno-informacijski sistem šole obdeluje veliko občutljivih podatkov. Zaradi preprečevanja dostopa do strežnika večjemu številu uporabnikov je ta povezan v ločeno administrativno podomrežje. Do njega dostopa manjše število uporabnikov, ki imajo dodeljene ustrezne pravice in so urejene prek domenskih uporabnikov. Tako je ta virtualni računalnik povezan s prvim virtualnim računalnikom, prek katerega se ureja možnost uporabe. Uporabniki z neustreznimi pravicami nimajo dostopa.

Za dostop do podatkov je treba na delovnih postajah oz. računalnikih zaposlenih namestiti aplikacijo, ki interpretira različne podatkovne baze in prikazuje podatke za obdelovanje. Aplikacija dostopa do podatkov na strežniku prek lokalnega omrežja, zato je delovanje omejeno na delo v organizaciji. Delo v aplikaciji na daljavo je možno pod posebnimi pogoji. Uporabniki, ki želijo uporabljati aplikacijo na ta način, morajo imeti urejeno povezavo s strežnikom prek virtualne zasebne omrežne (angl. Virtual Private Network – VPN) povezave. Na ta način se povežejo v lokalno omrežje organizacije, kjer je možno uporabljati aplikacijo. Ta dostop je omogočen le ključnim uporabnikom v organizaciji.

Vstop v aplikacijo je zaščiten z uporabniškim imenom in geslom. Uporabniki imajo omogočene različne pravice do uporabe modulov glede na to, katero delo v organizaciji opravljajo. Vse pravice za uporabo modulov upravlja administrator poslovno-informacijskega sistema.

Programska rešitev SAOP se zaradi spreminjanja zakonodaje redno posodablja. Vzdrževanje in podporo redno zagotavlja ponudnik storitve.

2 RAČUNALNIŠTVO V OBLAKU

Računalništvo v oblaku je dobava različnih storitev prek interneta. Viri vključujejo različna orodja in aplikacije za shranjevanje podatkov, strežnike, podatkovne baze in različno programsko opremo. Uporabniki namesto shranjevanja podatkov na lastnih lokalnih napravah, podatke shranijo v oddaljeno podatkovno bazo. Podatki so dosegljivi toliko časa, dokler ima naprava omogočen dostop do spleta. Računalništvo v oblaku je priljubljen način

uporabe storitev tako za posameznike kot podjetja, za kar obstaja več razlogov, med drugim tudi prihranki s stroški za vzpostavitev arhitekture, višjo produktivnostjo, hitrostjo in učinkovitostjo, uspešnostjo in tudi varnostjo.

Ime storitev računalništva v oblaku je poimenovano tako, ker se shranjeni in naloženi podatki, do katerih uporabnik dostopa, nahajajo se v oddaljenih strežnikih oz. virtualnem okolju. To pomeni, da uporabniku ni treba biti na določenem mestu ali napravi, da bi do podatkov dostopal, ampak omogoča delo na daljavo. Razvoj tehnologije in spletnih storitev omogoča veliko opravil prek storitev na internetu, s tem pa internet postane oblak. Tako so podatki, delo in aplikacije dosegljive na katerekoli napravi in lokaciji, le da imamo omogočeno povezavo na splet.

Računalništvo v oblaku je lahko javno ali zasebno. Javne storitve v oblaku zagotavljajo različni ponudniki tako brezplačno kot tudi za plačilo. Zasebne storitve računalništva v oblaku se izvajajo lokalno in do njih dostopa samo omejeno število ljudi. Obstajajo tudi različni hibridni sistemi, ki pa združujejo elemente javnih in zasebnih storitev.

Kot je bilo že omenjeno, si lahko računalništvo v oblaku razlagamo glede na pomen. Najpogostejše se nanaša na oddaljeno izvajanje procesov prek interneta v podatkovnem centru ponudnika storitve, ki ga lahko poimenujemo tudi javni oblak. Ponudniki so Amazon Web Services (v nadaljevanju AWS), sistem za upravljanje odnosov s strankami (angl. customer relationship management – CRM) Salesforce in Microsoft Azure. V današnjem času uporabniki večinoma uporabljajo več kot eno storitev računalništva v oblaku.

Druga možna razlaga se nanaša na računalništvo v oblaku, kako deluje od virtualizirane zbirke virov, računalniške performanse in funkcionalnosti aplikacij, ki so na voljo na zahtevo. Porabniki naročijo storitev v oblaku, ponudnik pa izpolni njihove zahteve (InfoWorld & Knorr, 2018).

Tako se opazi, da se računalništvo v oblaku ne nanaša vedno na določeno tehnologijo, ampak na koncept, ki obsega niz kombiniranih tehnologij (OECD, 2017).

2.1 Opredelitev računalništva v oblaku

Različni viri se do računalništva v oblaku opredeljujejo na več načinov, zato sem izbral dva, ki sta večkrat omenjena in uporabljena v različnih člankih. Različne opredelitve so se oblikovale prav zaradi različnih konceptov, ki se nanašajo na obseg nabora kombiniranih tehnologij in ne na določeno tehnologijo.

Izpostavljena in večkrat uporabljena je opredelitev Nacionalnega inštituta za standarde in tehnologijo (angl. National Institute of Standards and Technology, v nadaljevanju NIST), ki govori o tem, da je računalništvo v oblaku model za omogočanje vseprisotnega, priročnega omrežnega dostopa na zahtevo do skupnih in nastavljivih računalniških virov (omrežja,

strežniki, shramba, aplikacije in storitve), ki so zagotovljeni na zahtevo in sproščeni z minimalnim upravljanjem ali posredovanjem ponudnika storitve (Mell & Grance, 2011).

Avtorji članka kalifornijske univerze v Berkeleyju so računalništvo v oblaku opredelili na naslednji način: Računalništvo v oblaku se nanaša na aplikacije, ki so na razpolago kot storitev prek interneta in strojno, ter programsko opremo v podatkovnih centrih, ki zagotavljajo delovanje storitev. Storitve se imenujejo programska oprema kot storitev (angl. Software as a Service, v nadaljevanju SaaS), strojna in programska oprema v podatkovnih centrih pa se imenuje oblak (Armbrust in drugi, 2009).

Ti dve definiciji so razvili po obsežni razpravi in posvetovanju ter opisujeta na celovit način glavne vidike koncepta (Mell & Grance, 2011; Armbrust in drugi, 2009).

Prva opredelitev se tako bolj osredotoča na namen računalništva v oblaku, druga pa je osredotočena na komponente računalništva v oblaku. Obe kažeta na to, da je računalništvo v oblaku mogoče razumeti kot model storitev, ki temelji na naboru računalniških virov, do katerih se dostopa na prilagodljiv in elastičen način z malo upravljanja.

Slovenska avtorja knjige *Javna uprava v računalniškem oblaku* (Ujčič & Florjančič, 2017) opredelitev računalništva v oblaku proučujeta skozi več avtorjev. Pomembna je objava podatka, da je direktor Googla Eric Schmidt leta 2006 na panožni konferenci govoril, da bodo storitve in arhitektura »nekje na internetu, nekje v oblaku«. Drugi v knjigi omenjeni avtorji opisujejo še različne druge opredelitve, kjer navajajo uporabo različnih znanih tehnologij in virtualizacije. Skozi analizo trditev so opredelili računalništvo v oblaku, kjer so zapisali, da je računalništvo v oblaku zaloga uporabljivih in dosegljivih virtualiziranih virov, ti pa so nastavljivi dinamično v odvisnosti od obremenitev, kar omogoča optimalno izrabo. Uporabnik pa plačuje uporabljene vire glede na rabo, ki ima s ponudnikom infrastrukture podpisan prilagojen dogovor za zagotavljanje določene ravni storitve (angl. Service Level Agreement – SLA). Poleg že omenjene opredelitve NIST se je s tem ukvarjala tudi Mednarodna organizacija za standarde (angl. International Standards Organisation, v nadaljevanju ISO), ki je leta 2014 izdelala dva standarda: ISO/IEC 17788:2014, Information technology – cloud computing overview and vocabulary (ISO 2014a) in ISO/IEC 17789:2014, Information technology – cloud computing reference architecture (ISO 2014b). S tema standardoma opredelijo računalništvo v oblaku kot razvijajočo se paradigmo, kjer določijo sedem storitev v oblaku, med drugim je omenjeno omrežje kot storitev (angl. Network as a Service, v nadaljevanju NaaS) in podatkovna hramba kot storitev (angl. Data Storage as a Service – DSaaS) (Ujčič & Florjančič, 2017).

2.2 Razvoj računalništva v oblaku

Za lažje razumevanje, kako je potekal razvoj do okolja v oblaku, je treba razumeti razvoj celotnega računalništva. To pokaže že sam razvoj računalniške strojne opreme od prve do četrte generacije računalnikov, kjer je bila strojna oprema le del evolucijskega procesa.

Vzporedno s strojno opremo se je razvijala tudi programska oprema. Ko so se razvijala računalniška omrežja, so se razvili tudi prvi protokoli za komunikacijo med računalniki, saj so prav ti protokoli veliko pripomogli k razvoju internetne programske opreme.

Vzpostavitev skupnega internetnega protokola je neposredno pripeljala do hitre rasti števila uporabnikov na spletu. Rast števila uporabnikov je povzročila nadaljnji razvoj tehnologije in oblikovanje novih protokolov. Trenutno je za naslavljanje v uporabi poleg internetnega protokola verzije 4 (angl. Internet Protocol version 4, v nadaljevanju IPv4) tudi internetni protokol verzije 6 (angl. Internet Protocol version 6, v nadaljevanju IPv6), s katerim so se razširile možnosti za večje število dodeljevanja naslovov internetnih protokolov (angl. Internet Protocol Address – IP Address) napravam za medsebojno komunikacijo po internetu. Sčasoma se je skozi izboljšave strojne in programske opreme razvila tudi sposobnost gradnje enotnega univerzalnega internetnega vmesnika. Uporaba spletnih brskalnikov je privedla do selitve s tradicionalnega modela podatkovnega centra na model v oblaku. Uporaba tehnologij, kot so virtualizacija strežnika, vzporedna obdelava, vektorska obdelava, simetrična večprocesorska obdelava in množična vzporedna obdelava je pripeljala do korenitih sprememb (Rittinghouse & Ransome, 2009).

Izvor idej, povezanih z računalništvom v oblaku, je mogoče zaslediti približno v petdesetih letih prejšnjega stoletja, ko je John McCarthy, oblikoval »teorijo časovnega zakupa« (angl. »theory of time-sharing«). S »časovnim zakupom« se je skliceval na operacijski sistem, ki je več uporabnikom omogočal možnost delovanja in upravljanja na način, kot da bi ti upravljali računalnik. »Časovni zakup« se zato pogosto šteje za prvotni temelj koncepta, ki ga danes poznamo kot računalništvo v oblaku.

V petdesetih letih so bili računalniki zelo dragi. Ker so že velika podjetja težko zagotavljala uporabo računalnikov vsem zaposlenim, je bilo revolucionarnega pomena odkritje, da glavni računalnik delijo uporabnikom na način, da ti do njega dostopajo z uporabo terminala, ki omogoča delo na glavnem računalniku. Zaradi visoke cene glavnega računalnika si že manjša podjetja niso mogli priskrbeti računalnika in tako je nastala ideja, da bi lahko s »časovnim zakupom« računalnika večja podjetja manjšim podjetjem omogočila cenovno ugoden najem za uporabo velikih računalnikov.

V šestdesetih letih je J. C. R Licklider razvil mrežo ARPANET, kjer je bila njegova vizija razviti globalno računalniško omrežje tako, da bi lahko uporabniki do programov in podatkov dostopali od kjerkoli. V tem času pa je John McCarthy zapisal, da bi se nekoč lahko računalništvo organiziralo kot javni pripomoček.

V poznih šestdesetih letih je razvoj napredoval do te mere, da so uporabniki že dostopali do aplikacij v gostovanju s pomočjo terminala. To je delovalo tako, da sta terminal in glavni računalnik med seboj komunicirala po protokolu glede na znano in prejeto zahtevo.

V 70. letih je prišlo do pomembnega razvoja, ki je temeljil na konceptu delitve časa. Ustvarjanje virtualnih strojev je omogočilo uporabnikom, da je na eni fizični platformi hkrati delovalo več operacijskih sistemov.

V devetdesetih letih so začela telekomunikacijska podjetja s ponudbo virtualnih zasebnih omrežnih storitev. V podjetjih so zgradili omrežno infrastrukturo, ki je več uporabnikom omogočala enak dostop do storitev. Organizacija je lahko svoj trud in vire usmerila v izboljšanje učinkovitosti pasovne širine in z nižjimi stroški zagotovila enako raven kakovosti storitev. Leta 1997 je profesor Ramnath Chellapa z Univerze Emory in Univerze Južna Karolina oblikoval eno prvih definicij računalništva v oblaku. Računalništvo v oblaku je označil kot »računalniško paradigmo, kjer bodo meje računalništva določena z ekonomsko utemeljitvijo in ne samo s tehničnimi omejitvami.«

Slika 5: Zgodovina oblaka

Vir: Prirejeno po Times of Cloud (brez datuma).

V obdobju med letoma 1999 in 2009 so se zgodili naslednji pomembnejši mejniki:

- 1999: Salesforce.com: omogočijo uporabo preprostega spletnega mesta na internetu za prenos poslovnih aplikacij;
- 2002: Spletne storitve Amazon: predstavijo več storitev v oblaku, ki so omogočale shranjevanje in obdelavo podatkov;
- 2006: Amazonov Elastic Compute Cloud (EC2) – prvi komercialni oblak: Amazon majhnim podjetjem omogoči najem računalnikov, ki gostujejo in poganjajo lastne aplikacije;
- 2006: Google zažene Google Dokumente: končni uporabniki so lahko neposredno uporabljali oblak za izmenjavo dokumentov;

- 2007: Dropbox: študent na Univerzi Massachusetts Institute of Technology (MIT) ustvari storitev za gostovanje datotek, ki omogoča shranjevanje in sinhronizacijo z računalnikom;
- 2009: Google Apps – primeri poslovnih aplikacij, ki temeljijo na uporabi spletnega brskalnika in Windows Azure – Microsoftova platforma oblaku;

Med letoma 2008 in 2009 je bila industrija osredotočena na zasebne oblake. Zasebni oblak pomeni, da je infrastruktura (strojna oprema, prostor za podatke in omrežje) v celoti namenjena eni sami organizaciji. Glavna pomanjkljivost zasebnega oblaka je, da je podjetje odgovorno za vse upravljanje in vzdrževanje infrastrukture. To je v nasprotju z javnim računalništvom v oblaku, v katerem lahko vsaka organizacija kupi del strežnika, ki je v skupni rabi z drugimi strankami. Podjetje v teh razmerah ni odgovorno za nobeno upravljanje podatkov, vendar se pojavljajo pomisleki glede varnosti podatkov (Hoopes, Bogel, Sunga, Kocis & Nicu; bcs - The Chartered Institute fo IR, 2019).

2.3 Virtualizacija

Izraz virtualizacija se na področju informacijsko komunikacijske tehnologije (IKT) uporablja za označevanje abstraktnih in navideznih računalniških virov, saj gre pri tem za nadomeščanje strojne opreme z navidezno oz. programsko opremo. Virtualizacija se izvaja na različnih nivojih, na nivoju strojne opreme, operacijskega sistema in na nivoju aplikacij. Ko se omenja virtualiziranje strojne opreme, je ta običajno namenjena gostovanju operacijskih sistemov in delovanju več samostojnim neodvisnim navideznim računalnikom. Za te potrebe se virtualizira delovni spomin, prostor za podatke in omrežje, da lahko ustrezni program ustvari virtualni računalnik. Virtualiziranje na nivoju operacijskega sistema omogoča več uporabnikom hkrati, z različnimi uporabniškimi računi, dostopati do istega operacijskega sistema z uporabo sistema oddaljenega namizja. V tem primeru se uporabljajo virtualna namizja računalnikov in map za podatke. Virtualiziranje aplikacijskega nivoja se osredotoča na izvajanje znotraj gostiteljskega operacijskega sistema, ki omogoča namizno virtualizacijo, da oddaljeni računalnik na lastnem namizju uporablja program iz strežnika. Tako lahko uporabnik prek lokalnega odjemalca upravlja podatke na strežniku z uporabo aplikacije, nameščene na svojem računalniku (Mahmood & Hill, 2011).

Z virtualizacijo se delovanje IT-infrastrukture optimizira (delovne postaje, strežniki, sistemi za hrambo in drugi viri), saj naj bi optimalno razporejala informacijske vire in optimizirala organiziranje IT-procesov. S tem, ko se vzpostavi virtualizacija, se na eni strojni opremi vzpostavi več virtualnih okolij, ki so odvisna od razpoložljivosti virov ter se tako optimizira izkoriščenost strojne opreme (Barrett & Kipper, 2010).

Za vzpostavitev navideznega računalnika za uporabo je potrebna posebna programska oprema na glavnem računalniku oz. strežniku, ki simulira razpoložljivo navidezno strojno opremo. Na teh navideznih računalnikih delujejo od gostitelja neodvisni operacijski sistemi, do teh pa se dostopa s programom za oddaljeni dostop. Prednosti uporabe virtualizacije računalnikov je manj strojne opreme, centralizirano upravljanje programske in strojne

opreme, dobra izkoriščenost in optimizacija sistemskih virov, prihranki pri energiji, strojni opremi in njenem vzdrževanju, razširljivost, prilagodljivost, večja razpoložljivost, dostopnost ter dosegljivost. Prednost virtualizacije računalnika je tudi selitev iz enega fizičnega računalnika na drugega, vendar pa je ob enem to tudi slabost, saj je v določeni meri odvisna od samega virtualizacijskega programa, v katerem je bil ustvarjen navidezni računalnik in mora tudi drugi računalnik v primeru selitve podpirati format navideznega računalnika, ki migrira. Slabost uporabe navideznih računalnikov je tudi odvisna od internetne omrežne povezave (Rittinghouse & Ransome, 2009).

2.4 Značilnost računalništva v oblaku

Glede na opredelitev računalništva v oblaku je NIST določil pet ključnih značilnosti, ki so skupne vsem storitvam računalništva v oblaku (Mell & Grance, 2011):

- *Samopostrežba na zahtevo*: Uporabnik ima na razpolago storitve računalništva v oblaku brez dodatnega posredovanja, računalniške zmogljivosti strežniškega časa, prav tako je omrežna shramba vedno omogočena glede na potrebe uporabnika in se izvaja samodejno.
- *Širok dostop do omrežja*: Razpoložljive storitve v oblaku so na voljo prek računalniškega omrežja in so dostopne za uporabo z različnimi napravami (računalniki, tablice, telefoni in druge naprave), ki omogočajo uporabo standardnih protokolov.
- *Združevanje virov*: Računalniški viri ponudnika oblačnih storitev so združeni iz več podatkovnih centrov skupaj in na razpolago vsem odjemalcem glede na potrebe. Fizični in virtualni viri so dodeljeni dinamično, odvisno od porabe uporabnikov, kar pripelje do občutka o lokacijski neodvisnosti, kjer uporabnik nima nadzora nad lokacijo ponudnikovih virov. Uporabnik nima podatka, kam se shranjujejo podatki, saj so ti lahko porazdeljeni in se nahajajo v različnih podatkovnih centrih ali tudi različnih državah pri velikih ponudnikih.
- *Hitra prilagodljivost/Elastičnost:* Ta zagotavlja računalniško zmogljivost odvisno od povpraševanja. Računalniška zmogljivost se prilagaja potrebam, če je treba tudi samodejno. Uporabnik dobi občutek neomejene razpoložljivosti zmogljivosti virov in se lahko uporabljajo kadarkoli in v katerikoli količini.
- *Merjena storitev*: Oblačni sistemi samodejno nadzirajo in optimizirajo uporabo virov z merjenjem zmogljivosti na ravni abstrakcije, ki ustreza vrsti storitve (npr. shranjevanje, obdelava podatkov, pasovna širina in aktivni uporabniški računi). Porabo virov je mogoče spremljati, nadzorovati in poročati, kar zagotavlja preglednost tako za ponudnika kot uporabnike storitve.

2.4.1 Prednosti

Računalništvo v oblaku ponuja številne prednosti tako končnim uporabnikom kot tudi podjetjem različnih velikosti. Velika prednost je, da ni treba skrbeti za razvoj, vzdrževanje in podporo infrastrukture, kot je bilo treba pred uporabo oblaka, saj za to poskrbi ponudnik

storitve in se zato uporabniki lahko osredotočijo na svojo osnovno dejavnost (Tsagklis, 2013).

Stroškovna učinkovitost. To je največja prednost računalništva v oblaku, saj se uporabnik izogne naložbi v samostojno programsko opremo ali nakup strežnika. Z uporabo oblaka lahko uporabniki prihranijo pri stroških, povezanih s shranjevanjem podatkov, posodobitvami programske opreme, upravljanjem itd. Stroškovno je oblak veliko ugodnejša rešitev kot tradicionalna rešitev z lokalnim strežnikom. Stroškovna učinkovitost se poveča tudi zaradi modela plačevanja storitve, saj se zaračunava po sistemu glede na to, koliko virov se uporabi, kar naredi oblak še veliko bolj zanimiv za uporabnike.

Udobnost in stalna razpoložljivost. Predvsem javni oblaki ponujajo storitve, ki so vedno na voljo, ne glede na lokacijo uporabnika, da lahko enostavno dostopa do informacij. Kot posredna storitev je prednost tudi ta, da lahko uporabniki spreminjajo dokumente in datoteke v realnem času, kar prispeva k učinkovitejšemu delovanju. Razpoložljivost storitev v oblaku je 24 ur na dan, tudi v »konjicah« obremenitve sistemi ne odpovejo, saj so vzporedno vzpostavljeni rezervni strežniki, ki v primeru izpada zagotovijo pravočasen preklop in preprečijo izpad zagotavljanja storitve ali pa je ta, kar se le da, kratek.

Varnostne kopije in obnovitev. Podatki, ki gostujejo v oblaku in ne na lokalnem računalniku ali strežniku, imajo zagotovljeno varnostno kopiranje in obnovitev podatkov. V določenih primerih se oblak uporablja samo za varnostno kopiranje in shranjevanje podatkov z lokalnega računalnika.

Okolju prijazen oblak. Informacijska infrastruktura oblaka je na splošno bolj učinkovita od lokalne, saj deluje bolj energetsko učinkovito. Za primer, ko strežnik ne deluje z vsemi razpoložljivimi viri, ta prilagodi porabo energije trenutni porabi in tako zmanjša porabo energije.

Odpornost in redundanca. Arhitektura oblaka je robustno zgrajena, kar uporabnikom zagotavlja dodatno odpornost in redundanco arhitekture. Oblak tako poskrbi za samodejno preklapljanje med strojno opremo v primeru izpadov, poleg tega pa omogoča tudi obnovitvene sisteme.

Razširljivost in zmogljivost. Razširljivost je lastnost oblaka, ko prilagaja razpoložljive kapacitete glede na potrebe uporabnika. Porabljeni viri se obračunavajo glede na porabo. Poleg razširljivosti oblaka igra pomembno vlogo tudi elastičnost, saj se oblak prilagaja potrebam, ki jih zahtevajo sistemi. Za zagotavljanje ustrezne zmogljivosti sistemi uporabljajo porazdeljeno arhitekturo, ki zagotavlja visoko hitrost delovanja. V primeru, da želi uporabnik povečati zmogljivost svojega sistema, lahko to uredi prek nadzorne plošče, kjer najame dodatne vire za izboljšanje delovanja sistema.

Hitra postavitev in enostavna integracija. Ključna prednost oblaka je, da je sistem v oblaku mogoče hitro vzpostaviti, prav tako hitro pa ga osvojijo tudi uporabniki, ki ga uporabljajo.

Integracija programske opreme se izvaja samodejno pri namestitvi oblaka, uporabniki pa si pred tem izberejo storitve in aplikacije, ki jih potrebujejo. Poenostavljeno je tudi nadaljnje prilagajanje in nameščanje aplikacij.

Velika podatkovna skladišča. V oblak se lahko shrani veliko več podatkov, kot se lahko shranjujejo na lokalne strežnike, kjer je uporabnik odvisen od prostorske kapacitete. Tako ponuja skoraj neomejene prostorske zmogljivosti za shranjevanje podatkov, to pa odpravlja skrbi glede pomanjkanja prostora, saj skrbnikom lokalne infrastrukture ni treba nadgrajevati prostorskih kapacitet, kar pripelje do zmanjševanja IT-stroškov.

Dostopnost in lokacijska neodvisnost. Dostop do storitev v oblaku je mogoč z vseh naprav, ki imajo omogočen dostop do interneta, tako za računalnike, tablične računalnike, pametne telefone in druge osebne naprave. Uporaba storitev v oblaku tudi ni omejena na lokacijo, od kje se dostopa do storitev, saj je dosegljiva kjerkoli po svetu in je omejena zgolj na internetno povezavo.

Manjša krivulja učenja. Aplikacije v oblaku imajo običajno manjšo krivuljo učenja, saj se ljudje nanje hitreje navadijo. Uporabniki jih lažje sprejmejo in pridejo v uporabo veliko hitreje. Primer tega so storitve Googla, npr. elektronska pošta Gmail in storitev za urejanje dokumentov Google Docs.

2.4.2 Slabosti

Računalništvo v oblaku je orodje, ki uporabnikom ponuja številne koristi, vendar pa se srečuje tudi s težavami, ki povzročajo neučinkovito uporabo. V nadaljevanju bodo izpostavljene najpomembnejše pomanjkljivosti in slabosti (Tsagklis, 2013).

Varnost in zasebnost. Varnost je ena od ključnih skrbi vsakega uporabnika in ponudnika storitve v oblaku. Z uporabo storitve oblaka na daljavo uporabnik daje svoje zasebne podatke in podatke, ki so lahko občutljivi in zaupni. Te podatke mora ponudnik storitve ustrezno zaščititi pred morebitno zlorabo, za kar je sama zanesljivost ponudnika zelo pomembna. V primeru zlorabe podatkov podjetja je lahko ogrožen obstoj podjetja, za kar pa je treba proučiti vse morebitne alternativne možnosti, preden se zgodi selitev v oblak. Enako je tudi za posamezne uporabnike, saj zaupajo svoje podatke tretji osebi. Tudi zasebnost je pod velikim vprašajem, saj morajo podjetja in posamični uporabniki verjeti, da je ponudnik storitve zaščitil podatke pred nepooblaščeno uporabo. Zaradi zgodb iz medijev, ko poročajo o izgubi podatkov in uhajanju gesel, so nekateri uporabniki še vedno skeptični ter se ne poslužujejo storitev v oblaku, saj je pristno nezaupanje zaradi možnosti zlorab.

Odvisnost od ponudnika. Ena od glavnih pomanjkljivosti računalništva v oblaku je implicitna odvisnost od ponudnika, kar se v industriji računalništva v oblaku imenuje »zaklepanje ponudnika« (angl. »vendor lock-in«). V primeru, da želi uporabnik migrirati k drugemu ponudniku storitve, je to praktično zaradi različnosti sistemov skoraj neizvedljivo.

Ko pa se vseeno odločijo za migracijo, pa je to dolgotrajen in naporen postopek zaradi prenašanja vseh podatkov od starega k novemu ponudniku. Prav zaradi selitev drugam je pred sklenitvijo pogodb o uporabi dobro preveriti, kakšne so možnosti razširitve in uporabe arhitekture, saj je selitev zapleten postopek.

Tehnične težave in izpadi. Različni uporabniki so zagotovo zadovoljni z uporabo storitve, ko se jim ni treba ukvarjati s tehničnimi težavami infrastrukture, vendar pa se vseeno zgodijo različne motnje v delovanju in različni izpadi delovanja. Izpadi storitev, tudi največjih in najzanesljivejših ponudnikov storitev v oblaku, so možni. Zavedati se je treba, da je uporabnik odvisen od internetne povezave, zato bodo kakršnekoli težave na internetnem omrežju pripeljale do najrazličnejših težav s povezljivostjo, kar povzroča, da je storitev nedosegljiva. Izpad uporabe storitve, ki je sicer relativno kratek, se zgodi tudi v primeru težav na strežniku oblaka, saj se preklop delovanja na vzporeden sistem ne more zgoditi čisto neopazno.

Omejen nadzor in prilagodljivost. Aplikacije in storitve se izvajajo v oddaljenem virtualnem okolju, zato imajo uporabniki omejen nadzor nad delovanjem in izvajanjem strojne ter programske opreme. Zaradi oddaljenega dostopa je omejeno tudi delovanje funkcionalnosti programske opreme v primerjavi z delovanjem lokalno nameščene programske opreme.

Povečana ranljivost. Oblačne rešitve so izpostavljene internetu in javnemu dostopu ter tako tarča različnih zlonamernih uporabnikov in napadalcev. Nikjer na internetu ni mogoče zagotoviti popolne varnosti, kar trpijo tudi največji ponudniki storitev računalništva v oblaku, saj so deležni različnih vdorov in izkoriščanja varnostnih lukenj za namerno povzročanje različne škode.

Kljub pomanjkljivostim in dejstvu, da je računalništvo v oblaku še relativno mlado, ima še veliko potenciala za prihodnost. Njegova uporabniška baza nenehno raste, največ jih privabljajo veliki in zaupanja vredni ponudniki, ki znova in znova ponujajo boljše in bolj prilagojene storitve ter rešitve uporabnikom. Želja je le, da se bodo prednosti še povečale in pomanjkljivosti zmanjšale, saj se zdi, da je računalništvo v oblaku poenostavilo IT (Tsagklis, 2013).

2.5 Storitveni modeli

Po opredelitvi NIST-računalništva v oblaku so določeni trije storitveni modeli (Mell & Grance, 2011), ki bodo opisani v nadaljevanju tega poglavja, in sicer: infrastruktura kot storitev, platforma kot storitev (angl. Platform as a Service, v nadaljevanju PaaS), programska oprema kot storitev. Storitveni modeli določajo, kako se viri podredijo bistvenim lastnostim oblaka in kako viri sledijo storitvenemu modelu oblaka, kar na skladu storitev IT (angl. IT stack) omogoča postavitev mejne črte med klasičnim IT-pristopom in oblakom.

Slika 6 prikazuje storitvene modele SaaS, PaaS in IaaS ter njihove glavne komponente, ki jih mora zagotavljati ponudnik: IaaS ponudnik poskrbi za strežnike in shranjevanje, požarni zid omrežja in varnost ter podatkovni center; PaaS ponudnik mora dodatno poskrbeti še za operacijske sisteme in razvojna okolja, upravljanje podatkovnih baz in poslovno analitiko; SaaS ponudnik pa poleg že naštetega ponudi uporabnikom storitve končno aplikacijo za uporabo.

Slika 6: Storitveni modeli

Vir: Prirejeno po Microsoft Azure (brez datuma).

Avtorja knjige (Ujčič & Florjančič, 2017) in prispevka na spletu s Fakultete za računalništvo in informatiko Ljubljana (Neznan avtor na FRI) omenjata tudi druge novejše oblike storitvenih modelov, ki se pojavljajo v kombinaciji z imenovanjem karkoli kot storitev (angl. X as a Sevrice, v nadaljevanju XaaS), in bodo predstavljeni na koncu poglavja.

2.5.1 Infrastruktura kot storitev

Osnovni storitveni model računalništva v oblaku je infrastruktura kot storitev. Ta kot osnovo ponuja najem strojne opreme oz. računalniške infrastrukture, ki podpira ostala koncepta računalništva v oblaku, in sicer tako PaaS kot SaaS.

NIST opredeljuje IaaS kot storitev, kjer ima uporabnik zagotovljene procesorske, prostorske, omrežne in druge vire, ki jih lahko poljubno porazdeljuje, si uredi poljubno programsko opremo ter namešča in upravlja aplikacije. Značilnost infrastrukture kot storitve je, da je prilagodljiva in omogoča različne inovativnosti in prilagoditve glede na zahtevnost uporabnikov. Uporaba te storitve omogoča razvoj in uporabo najrazličnejših novosti, vendar lahko privede tudi do omejitev uporabe, predvsem zaradi pomanjkanja znanja in neprestanega razvoja novih tehnologij (Kavis, 2014).

Izpostavljene prednosti modela IaaS (povzeto (Grohar, Ciglarič, Pančur & Horvat, 2013)):

Nižji stroški. Ti so s poslovnega vidika ena od glavnih prednosti uporabe storitev oblaka. V primeru uporabe javnega oblaka uporabnik zakupi dostop do informacijske tehnologije, ki jo upravlja ponudnik storitve. Stroški investicije so eliminirani in se zamenjajo za operativne

stroške, saj se zaračunajo zgolj toliko, kot se viri porabljajo, in se plačujejo mesečno, kar pa zmanjša vrednost celotnih stroškov.

Poslovna agilnost. Različni poslovni procesi, predvsem prodaja, uporabniška podpora, razvoj in notranja komunikacija je močno odvisna od informacijske tehnologije ter računalniških omrežij. Za odzivanje na različne poslovne priložnosti potrebujejo različni uporabniki dinamično IT infrastrukturo, pri tem IaaS omogoča tudi zagotavljanje konsistentne IT vpeljave med različnimi lokacijami in zagotavlja neprekinjenost operacij. Z IaaS se med drugim pohitri tudi čas vstopa na tržišče in čas do ustvarjanja prihodkov, interno pa se osebje ukvarja predvsem s ključnimi poslovnimi dejavnostmi in manj z vzpostavitvijo infrastrukture.

Hitro razširjanje zmogljivosti, elastičnost, skalibilnost. IaaS zmanjša čas za nabavo in vpeljavo enotne strojne opreme, kar omogoča, da se uporabnik osredotoči na poslovne projekte in razvoj ter postavitev poslovnih rešitev. Oblačna storitev IaaS omogoča, da uporabniki prilagajajo vire specifičnim opravilom, pri tem pa lahko viri tudi skalirajo. Povečanje inovativnosti, zniževanje stroškov in povečanje prihodkov vpliva tudi na dejstvo, da ni več pomanjkanja v infrastrukturi z viri ali njihovim omejevanjem.

Konsolidacija in centralizacija IT sistemov. S tehnološkega vidika lahko IaaS zamenja obstoječo infrastrukturo in neizkoriščene strežnike s standardizirano infrastrukturo za delovanje in nadgradnjo aplikacij. Enotni viri IaaS lahko služijo kot razširitev internih strežniških zmogljivosti ali kot oddaljen sistem za reševanje pred izpadom delovanja internih storitev.

2.5.2 Platforma kot storitev

Storitveni model platforma kot storitev je naslednja stopnja storitve v oblaku in na enak način, kot je IaaS storitev za infrastrukturo, je PaaS storitev za aplikacije. PaaS je nad IaaS in povzema večino standardnih funkcij na ravni aplikacij in jih zagotavlja kot storitev. PaaS uporabniki imajo pripravljeno ogrodja modulov in se osredotočajo le na razvoj poslovne logike aplikacije. Ta storitev je kot razvojno okolje, ki ga ponudniki ponujajo za razvoj aplikacij brez dodatnih stroškov za nakup osnovne strojne in programske opreme, upravljanja in zagotavljanja zmogljivosti gostovanja. Storitev je v celoti dostopna prek interneta in se plačuje toliko, kot jo uporabnik uporablja, za uporabo pa je pripravljeno razvojno okolje z orodji, ki bistveno pocenijo in pohitrijo razvoj (Kavis, 2014).

Izvajanje storitve je mogoče na vseh vrstah oblakov, in sicer v javnem, zasebnem in tudi hibridnem oblaku. Prvotno so današnji ponudniki ponujali storitev na nivojih IaaS (Amazon, VMware) in SaaS (SalesForce), kasneje pa so rešitve konvergirale proti PaaS. Tako je nastala različna ponudba PaaS rešitev, kjer ponudniki različno propagirajo opredelitev PaaS storitev, zaradi česar se je pojavilo pet tipov ponudnikov platform (povzeto (Grohar, Ciglarič, Pančur & Horvat, 2013)):

- *za nalaganje celotnega okolja*, kjer se naloži sliko pripravljenega okolja. Tako se lahko poganja zastarele računalniške sisteme (Amazon EC2);
- *za nalaganje prevedene aplikacije*, saj že zagotavlja predpripravljeno okolje in je treba nanj naložiti prevedeno aplikacijo, ki je podprta za PaaS okolje;
- *za nalaganje aplikacij s pomočjo namestitvenega paketa,* ki so vsebniki z določenimi omejitvami, ki zahtevajo striktno strukturo oblikovanja kode (Google App Engine);
- *za nalaganje kode,* ki omogoča nalaganje izvorne kode na PaaS, ki se najprej prevede, kar omogoča boljši pregled nad kodo ter posledično lažje dodeljevanje virov (Herouk);
- *z vgrajenim razvojnim okoljem,* ki dejansko omogočajo razvoj v samem oblaku in izvajajo specifično programsko kodo, kjer se prek razširitev lahko dodaja funkcionalnosti. Takšne aplikacije so osredotočene predvsem na SaaS nivo (Salesforce.com).

Storitev platforma kot storitev zajema veliko različnih lastnosti, ki jih sicer ne zagotavlja vsak ponudnik, saj so te odvisne od prej omenjenih tipov platform. Lastnosti, ki jih zajema PaaS, so (povzeto (Grohar, Ciglarič, Pančur & Horvat, 2013)):

- *razvoj, testiranje, nameščanje, gostovanje in vzdrževanje aplikacij v enotnem integriranem okolju:* PaaS ima podporo celotnega razvojnega cikla v istem integriranem okolju. Na preprost način je mogoče izvesti kopije aplikacije, kar prihrani čas in trud, zagotavlja pa tudi celovito okolje za nadzor programske kode, testiranje na interaktiven način z več uporabniki in ponastavljanje in sledenje spremembam uporabnikov;
- *dodatna orodja za nastavitve in razvoj: t*o je odvisno od ponudnika, nekateri omogočajo tudi razvoj vmesnikov, modeliranje poslovnih procesov in druge funkcionalnosti. Na voljo so tudi rešitve za vizualno grajenje uporabniških vmesnikov;
- *zagotavljanje skalabilnosti, zanesljivosti in varnosti:* platforma PaaS zagotavlja hkratno uporabo več uporabnikom – večodjemni model, zato je poskrbljeno s samodejnim upravljanjem sočasnega dostopa, skalibilnostjo, nadomestnim načinom delovanja in varnostjo, kar je zagotovljeno vsem razvijalcem;
- *integracija spletnih storitev in podatkovnih baz:* s podporo vmesnikom SOAP in REST PaaS omogoča integracijo obstoječih storitev, dostopa do podatkovnih baz in uporabo lokalnih storitev, za kar ponudniki zagotovijo storitveno vodilo (angl. Enterprise Service Bus), na osnovi katerega se vrši integracija storitev;
- *podpira skupinski razvoj:* sistem omogoča deljenje izvorne kode med razvijalce, oblikovanje urnikov, postavljanje ciljev, oblikovanje skupine, dodelitev odgovornosti ter opredelitev različnih vlog;
- *podpira spremljanje dogodkov:* to je omogočeno z zagotovitvijo nadzornih plošč, prek katerih je možno spremljati različne aktivnosti, kot so: poraba virov, zmogljivosti, napovedovanje konic, spremljanje dnevnikov napak in prestrezanje nepredvidenih dogodkov. Te platforme imajo tudi vgrajene mehanizme za obračunavanje porabe storitev, kar olajša finančno planiranje porabe sredstev.

»Uporaba PaaS modela v organizaciji lahko prinaša nekatere poslovne prednosti. Poznavanje teh prednosti nam omogoča boljše prilagajanje arhitekture rešitve na PaaS modelu ter boljši izkoristek zmožnosti, ki nam jih ta ponuja« (Grohar, Ciglarič, Pančur & Horvat, 2013).

Izpostavljene poslovne prednosti modela PaaS (povzeto (Grohar, Ciglarič, Pančur & Horvat, 2013)):

Hitrejši razvoj novih poslovnih zmogljivosti. Vzpostavitev novih razvojnih kapacitet, z namenom izboljšanja delovanja sistemov ali postavitve novih poslovnih komponent zahteva svoj čas, kar posledično predstavlja potencialno izgubo poslovanja in dobička. Podobno velja tudi za razvoj aplikacij, ki so v razvoju, saj traja tudi več mesecev, preden je nared za uporabo. Skrajševanje časa razvoja in vzpostavitve delovanja pomeni hitrejši prihod na tržišče in zmanjševanje poslovnih izgub. Razvoj s PaaS krajša čas prihoda na tržišče, saj je okolje za postavitev aplikacije predpripravljeno, ne da bi bilo treba dodatno čakati na zagotavljanje ustreznih virov. To predstavlja zmanjševanje potencialne izgube poslovanja.

Manj tvegane poslovne inovacije. Za uspeh so ključnega pomena inovacije, saj organizacija brez ponudbe novih storitev ne zadovolji stranke, to pa lahko stori konkurenca. Same inovacije so tvegane, saj jih je večina neuspelih, to pa predstavlja tveganje in stroške organizaciji, kar posledično omejuje tudi inovativnost. Tako ima organizacija, v odvisnosti od vložka, tudi sorazmerno veliko poslovno tveganje. Storitev PaaS zniža stroške in posledično tudi tveganje pri razvoju, saj se vsak razvoj zažene kot eksperiment, s čim cenejšimi stroški in čim manjšimi obveznostmi. Storitev se v oblaku plačuje glede na porabo sistemskih virov in v začetku predstavlja zaradi majhnosti aplikacije tudi nizke stroške financiranja v inovacijo. V primeru neuspeha inovacije se aplikacija enostavno odstrani in preneha s plačevanjem, v nasprotnem primeru, ob uspehu aplikacije, pa se jo lahko skalira in zagotovi ustrezne vire za povečanje obsega aplikacije, kar prinese manj poslovnega tveganja pri razvoju novosti in poveča uspešnost inovativnosti organizacije.

Globalno skaliranje in globalni doseg. Če organizacija razvije aplikacijo, ki se izkaže, da jo uporablja veliko uporabnikov, se lahko zgodi pomanjkanje zagotavljanja ustreznih virov za delovanje. V tem primeru se aplikacija seli v arhitekturo oblaka, kjer je zagotovljena skalibilnost aplikacij in tako ustrezni viri. V oblaku je možno skaliranje navzgor pa tudi navzdol, odvisno od obremenitve konice aplikacije. Organizacija ima lahko svoje aplikacije, nameščene v različnih podatkovnih centrih po svetu, in medsebojno sinhronizacijo ter tako zagotavlja ustrezne hitrostne odzivnosti delovanja. Na podoben način se rešuje delovanje aplikacije v primerih izpadov delovanja podatkovnega centra, ko je omogočen dostop za uporabo z druge lokacije. V standardnih podatkovnih centrih mora organizacija za vse to poskrbeti sama, v primeru storitve PaaS, pa je to zagotovljeno s strani ponudnika in je na voljo tudi manjšim najemnikom storitve. Globalni doseg in globalno skaliranje omogoča organizacijam hitrejše odkrivanje novih priložnosti na tržišču.

Inteligentnejša razporeditev sredstev za IT. Sredstva, ki so namenjena za IT, so običajno razdeljena v dve kategoriji, in sicer: sredstva za osnovno infrastrukturo in sredstva za inovacije. Optimizacija sredstev z uporabo PaaS pripomore k plačevanju storitev glede na porabo, kar pomeni, da ni treba investirati v strojno in programsko opremo ter njuno vzdrževanje. Vzdrževanje platforme aplikacije postane operativni strošek in ne več kapitalni, kar pripomore k učinkovitejši izrabi sredstev. Ker ponudnik storitve zaračunava stroške po porabi, ima organizacija dober pregled nad vložkom in tako lažje odločanje o nadaljnjih vložkih ali ukinitvah pri doseganju zastavljenih ciljih. Odvisno od poslovanja organizacije je uporaba oblačne arhitekture za gostovanje aplikacij lahko cenejša kot gostovanje aplikacij v lastnem podatkovnem centru. PaaS model ne sme predstavljati popolne zamenjave tehnološke-infrastrukture organizacije, saj je ta še vedno lahko potrebna, vseeno pa je postavitev prilagojenih aplikacij v oblak v večini primerov boljša izbira.

2.5.3 Programska oprema kot storitev

Storitveni model, programska oprema kot storitev, je raven oblaka za uporabo aplikacij, saj se aplikacije ne nameščajo ali zaganjajo na lokalnem računalniku in tudi ni treba skrbeti za vzdrževanje in nadgrajevanje. Razvoj lastnih aplikacij prek storitve SaaS ni mogoč, saj gre v tem primeru za dostopanje do že ustvarjenih aplikacij prek spletnega vmesnika. Dostop je mogoč z uporabo internetne povezave in deluje s pomočjo različnih odjemalcev prek internetnega brskalnika ali prek programskega vmesnika, ki omogoča uporabo aplikacij. Za uporabo in delovanje teh storitev je običajno potreben le internetni brskalnik, vse ostale vire za zagotavljanje delovanja pa zagotovi ponudnik storitve. Uporabnik nima možnosti upravljanja ali nadzorovanja infrastrukture računalniškega oblaka, razen v primerih, ko se prilagajajo posebne nastavitve uporabniškega vmesnika.

Ponudnik modela SaaS poskrbi za strojno in programsko opremo ter vzdrževanje, da sistem deluje. Plačevanje uporabe te storitve je samo za primer storilnosti, ne plačuje pa se za aplikacijo, da bi bil uporabnik njen lastnik. Aplikacija deluje po principu večkratne najemne arhitekture, kjer lahko več odjemalcev uporablja isto instanco aplikacije. Ta model je običajno tudi največkrat opažen v SaaS storitvenem modelu (Kavis, 2014).

Svetovni trg na področju SaaS doživlja hitro rast, saj se pojavlja vedno več aplikacij, ki temeljijo na tem modelu storitve. Avtor (Jamcracker, 2020) se sprašuje, ali so res vse aplikacije modela SaaS ali le zlorabljajo to oznako v tržni namen, za kar izpostavi ključne lastnosti in značilnosti programske opreme kot storitve (povzeto (Jamcracker, 2020)):

Večnajemniški model. To je programska arhitektura, ki jo lahko uporablja hkrati več uporabnikov oz. najemnikov. Vsak najemnik lahko dobi možnost prilagajanja nekaterih delov aplikacije, saj so zasnovane tako, da se za vsakega najemnika ustvari ločena podatkovna baza oz. shema znotraj ene baze podatkov in so med njimi podatki strogo ločeni in medsebojno nedosegljivi.

Samodejno zagotavljanje storitve. Dostop do storitev SaaS je vedno na voljo in se zagotavlja samodejno. SaaS aplikacije se običajno uporabljajo v poslovne namene ter mora omogočati in ustvarjati dostope na podlagi zahtev in tudi možnost odstranitve na enak način, na zahtevo.

Enotna prijava. Enoten sistem prijave omogoča več dostopov do storitev z enim uporabniškim imenom in geslom. Uporabniško ime in geslo je vezano na pravice za dostopanje in prijavo do različnih aplikacij, ki so na voljo in glede na prednastavljene politike omogoča uporabo teh storitev.

Obračunavanje na podlagi naročnine. Cena aplikacije SaaS ne zajema stroškov licenc in nadgradnje, ampak se za uporabo zaračunava naročnina, kar uporabnikom omogoča zakup dostopa na zahtevo, kadar aplikacijo potrebujejo. Na enak način se naročnina tudi prekine, ko uporabnik aplikacije ne potrebuje več, in sicer s prekinitvijo naročnine. Običajno so naročnine po tedenskih, mesečnih, četrtletnih, polletnih in letnih naročniških ciklih, le v manjšini primerov pa se zaračunava glede na dejansko uporabo.

Visoka dostopnost. Dostopnost do aplikacij SaaS mora biti zagotovljena 24/7, kjerkoli na svetu. Obstajala naj bi tudi aplikacija za upravljanje in spremljanje razpoložljivosti aplikacij. Aplikacija mora omogočati veliko število prijav uporabnikov v sistem hkrati.

Elastičnost infrastrukture. Uporaba SaaS aplikacij na splošno ni predvidljiva, zato se lahko poraba virov hitro spremeni, kar mora v ozadju omogočati dovolj zmogljiva infrastruktura, da zagotovi ustrezno količino virov za omogočanje nemotenega delovanja aplikacije.

Varnost podatkov. Podatki in poslovne informacije so zaščiteni pred nepooblaščenimi dostopi, določeni podatki morajo biti glede na stopnjo tveganja tudi dodatno šifrirani, kar pa je odvisno tudi od samega najemnika aplikacije. Da so podatki ustrezno varovani, mora imeti ponudnik storitve urejen okvir pravic za upravljanje s ključi za dostope do aplikacij, saj podatki ne smejo biti dostopni drugemu najemniku.

Varnost aplikacije. Aplikacije morajo biti zaščitene pred različnimi ranljivostmi, zagotovljen mora biti tudi močan nadzor identitete, s katero uporabnik vstopa. Storitev SaaS je varna tudi zaradi zaščite seje, ki jo uporabnik vzpostavi ob vstopu v aplikacijo in varuje pred krajo, prav tako prepoznava nepooblaščene seje, uporabo piškotkov, ki ne shranjujejo pomembnih podatkov, omogoča več nivojsko preverjanje vstopa in zaščito pred napadi porazdeljene ohromitve storitev.

Revizija. Aplikacije SaaS so opremljene z zagotavljanjem revizijskih dnevnikov poslovnih transakcij, kar uporabnikom omogoča oblikovanje poslovne strategije z uporabo načrtov poslovne inteligence, ki pa naj bi bile sposobne upoštevati tudi različne državne predpise in notranjo politiko organizacije.

2.5.4 Karkoli kot storitev

Avtorja knjige (Ujčič & Florjančič, 2017) omenjata tudi druge novejše oblike storitvenih modelov, ki se pojavljajo v kombinaciji s poimenovanjem XaaS. Pri tem črka X pomeni oznako različnih možnosti uporabe in kot kombinacija XaaS predstavlja dobavo informacijske tehnologije kot storitve skozi računalniški oblak in se nanaša na eno storitev ali na kombinacijo več obstoječih storitev, ki so bile prej ločene v zasebnih ali javnih oblakih, zdaj pa postajajo pregledne in celostne (Ujčič & Florjančič, 2017).

XaaS se je pojavil kot nov operacijski model storitve, ko so vodje informatike iskali cenejše in učinkovitejše načine za začetek uporabe IT-infrastrukture in so začeli uporabljati različne storitve skupaj v oblaku, in sicer pošto, portale za upravljane s strankami in vizualizacijo poslovne inteligence ter shranjevanje podatkov. XaaS se opredeljuje kot storitev po naročilu (Boulton, 2018).

Sledi omemba le nekaj možnosti in kombinacij, ki so izpeljane iz storitve XaaS, in sicer: upravljanje odnosov s strankami kot storitev (angl. Customer Relationship as a Service – CRaaS), upravljanje z identitetami kot storitev (angl. Identity as a Service – IDaaS), upravljanje skladnosti kot storitev (angl. Compliance as a Service – CaaS), nadzorovanje kot storitev (angl. Monitoring as a Service – MaaS), komuniciranje kot storitev (angl. Communication as a Service – CaaS), dostop do aplikacij na zahtevo (angl. Application as a Service – AaaS), računske storitve za podatkovne centre (angl. Computing as a service – CaaS), storitev hrambe (angl. Storage as a Service – StaaS) in omrežje kot storitve (angl. Network as a Service – NaaS).

Karkoli kot storitev še vedno izhaja iz treh glavnih modelov storitev, in sicer IaaS, PaaS in SaaS. Vse ostale storitve so le hibridi rešitev različnih storitev in vrst oblakov, javnih in zasebnih, ki so prilagojeni različnim potrebam uporabnikov.

2.6 Vrste oblakov

NIST (Mell & Grance, 2011) razlikuje računalniške oblake tudi glede na lastništvo in pravico do dostopa in opredeljuje naslednje vrste računalniških oblakov:

- zasebni računalniški oblak,
- oblak skupnosti,
- javni oblak,
- hibridni oblak.

Imena oblakov ne pomenijo nujno vezave glede lokacije oblaka, saj sta tako zasebni kot tudi javni dosegljiva po medmrežni povezavi. Tip oblaka, ki ga bo uporabljala organizacija, je odvisen predvsem od namena, za kaj ga bodo uporabljali. Običajno se za testne in raziskovalne namene uporabljajo javni oblaki, ki so cenejši in enostavnejši, za večje stabilne

in občutljivejše obdelave pa uporabljajo ostale vrste oblakov, zasebne, hibridne ali oblak skupnosti.

2.6.1 Zasebni oblak

Po opredelitvi NIST (Mell & Grance, 2011) in povzemanju slovenskih avtorjev (Ujčič & Florjančič, 2017) je infrastruktura zasebnega oblaka namenjena izključno uporabi znotraj ene organizacije in njenih poslovnih enot. Lahko je v lasti, upravljanju in delovanju znotraj organizacije, tretje strani ali njune kombinacije in je lahko nameščena znotraj ali zunaj poslovnih prostorov organizacije.

Zasebni oblak je rešitev, namenjena za organizacije ali uporabnike, ki želijo imeti omogočen dostop do podatkov na zahtevo, vendar pa ne morejo podatkov hraniti v javnem oblaku, kar je lahko posledica varnostne politike, finančnega proračuna ali predpisov, ki ne dovoljujejo iznosa podatkov iz lokalnega okolja. Da se podatki ustrezno zaščitijo, uporabljajo tudi različne šifrirne protokole in požarne zidove. Prednost zasebnega oblaka je tudi, da obravnava slabosti javnega oblaka, kot so nadzor nad podatki, regulativne težave in konfiguracije.

Običajno so zasebni oblaki nameščeni lokalno v organizacijah, ki ga uporabljajo, lahko pa so postavljeni tudi v najetih podatkovnih centrih pri zunanjem ponudniku. Ne glede na to ali je sistem v zasebnem ali najetem lastništvu, se končni uporabniki v oblaku pri ponudniku storitve med seboj ne morejo povezati, saj so podatki med seboj strogo izolirali. Pri lokalni zasebni namestitvi oblaka uporabniki storitev sami nadzorujejo in upravljajo podatkoven center in tudi sami odločajo o tem, kakšne konfiguracije bodo na oblaku tekle, saj sami upravljajo tudi strojno opremo.

To uporabnikom zagotavlja več nadzora in varnosti, vendar stane več kot uporaba računskih virov v večplastnem javnem oblaku. Zasebni oblak zmanjšuje nekatera regulativna tveganja v zvezi z lastništvom podatkov, zasebnostjo in varnostjo zaradi narave modela, kar pa v tem primeru tudi škoduje nekaterim glavnim prednostim računalništva v oblaku, in sicer zmanjšanju elastičnosti, omejenemu združevanju virov in plačevanje virov po porabi.

Zasebni oblak končnemu uporabniku omogoča uporabo skupnih virov, vendar so ti viri omejeni na velikost in upravljanje lokalne infrastrukture, kar pa je v nasprotju s pravilom računalništva v oblaku, ki zagotavlja navidezno neskončno uporabo računalniških virov za širitev. Posledično se povečajo stroški in zmanjša okretnost infrastrukture, saj morajo notranji upravljalci fizične oblačne infrastrukture zagotoviti in poskrbeti za ustrezno nadgradnjo potreb po virih, ki so v pomanjkanju. V primerih, ko so presežene zmogljivosti, se uničuje model plačevanja »toliko kot porabiš«, saj je končni uporabnik že plačal najete količine, ne glede na to, ali jih uporablja ali ne (Kavis, 2014).

2.6.2 Javni oblak

Po opredelitvi NIST (Mell & Grance, 2011) in povzemanju slovenskih avtorjev (Ujčič & Florjančič, 2017) je infrastruktura javnega oblaka namenjena vsakršni uporabi celotne javnosti. Lahko je v lasti, upravljanju in delovanju poslovnih uporabnikov, akademskih ali državnih organizacij ali njihovi kombinaciji. Lokacija nameščene infrastrukture je pri ponudniku storitve javnega oblaka.

Javni oblak je večnamensko okolje, v katerem uporabnik oz. najemnik plačuje za storitve, ki jih ponujajo ponudniki in so na voljo za uporabo. Uporabniki ne poznajo fizične lokacije, kjer se nahaja in deluje programska oprema, poleg tega, da lahko poznajo lokacije podatkovnih centrov ponudnika. Fizično strojno opremo povezuje abstrakcijski sloj storitve oblaka in deluje kot aplikacija končnemu uporabniku, ki se uporablja za ustvarjanje virtualnih računskih sredstev, ki so na voljo velikemu številu uporabnikov.

Prednosti javnega oblaka (povzeto po Kavis, 2014):

Cene uporabnosti. Uporabnik plača samo za vire ali storitve, ki jih porabi. To uporabniku pomaga tako, da ko potrebuje več različnih storitev iz oblaka, te tudi najame in po potrebi tudi zmanjša, ko jih ne potrebuje več. Uporabniku ni treba več skrbeti za strojno opremo.

Elastičnost. Uporabnik ima na videz neskončen nabor virov in lahko konfigurira svoje programske rešitve tako, da dinamično poveča ali zmanjša količino računskih virov, ki jih potrebuje za obvladovanje nepričakovanih preobremenitev. To uporabniku omogoča, da se v realnem času odzove na nepričakovane konice prometa, kjer bi moral uporabnik v zasebnem lokalnem oblaku ali na klasični strežniški infrastrukturi imeti v pripravljenosti možen zakup ali povečanje po potrebnih virih, da bi lahko upravljal z nepredvidenimi preobremenitvami.

Ključne kompetence. Z uporabo javnega oblaka uporabnik izvozi v upravljanje svoje podatke in infrastrukturo na infrastrukturo ponudnikovega javnega oblaka. S tem uporabnik porabi manj časa za upravljanje infrastrukture in ima več časa, da se osredotoči na svojo osnovno dejavnost.

Poleg prednosti ima javni oblak tudi pomanjkljivosti, ki prinašajo določena tveganja. Ta se nanašajo na sam nadzor, regulativna vprašanja in omejitve pri uporabi infrastrukture javnega oblaka (povzeto po Kavis, 2014):

Upravljanje. Uporabnik mora poznati sporazum o ravni zagotavljanja storitev, ki jih ponuja ponudnik glede delovanja sistema. Če ima ponudnik javnega oblaka izpad storitve, uporabnik pa na ta izpad ni pripravljen, je ponudnik storitve dolžan opraviti obnovitev storitve, kar lahko pripelje do izgube podatkov.

Regulativna težava. Predpisi, kot so standard o varovanju podatkov plačilnih kartic, prenosljivost in dostopnost do zdravstvenih podatkov in težave z osebnimi podatki, predstavljajo velike izzive javnim oblakom. Za zagotavljanje teh predpisov je pogosto potrebna hibridna rešitev, čeprav obstajajo podjetja, ki te težave rešujejo v javnem oblaku z uporabo certificiranih SaaS, kar predstavlja rešitev za tiste komponente, ki jim je težko zagotavljati revizijo v javnem oblaku.

Omejena konfiguracija. Javni ponudnik oblaka ima standardni nabor infrastrukturnih konfiguracij, ki ustrezajo potrebam splošne javnosti. Včasih je za reševanje kompleksnejših težav potrebna specifična strojna oprema, ki pa je v takšnih primerih javni oblak pogosto ne zagotavlja, saj ponudnik storitve kompleksnejše infrastrukture preprosto ne zagotavlja.

2.6.3 Hibridni oblak

Po opredelitvi NIST je infrastruktura hibridnega oblaka sestavljena iz kombinacije dveh ali več infrastruktur (zasebni, skupnostni ali javni oblak), ki ostajajo samostojni subjekti, povezani s standardizirano ali lastno tehnologijo, kar omogoča prenosljivost podatkov in programske opreme (npr. širjenje oblaka zaradi prerazporejanja obremenitev med oblaki) (Ujčič & Florjančič, 2017; Mell & Grance, 2011).

Najboljši izkoristek zasebnega in javnega oblaka uporabljajo številne organizacije z uporabo tako imenovanega hibridnega oblaka. Kot je že bilo omenjeno v prejšnjem odstavku, je to kombinacija dveh ali več infrastruktur oblakov, ki tvorijo eno novo celoto, ki je povezana z javno in zasebno infrastrukturo, ki omogoča prenosljivost podatkov in aplikacij. Dobra praksa za uporabo hibridnega oblaka je, da se čim bolj izkoristijo prednosti javnega oblaka, kot sta elastičnost in združevanje virov ter zasebni oblak za zmanjšanje tveganja na področju lastništva podatkov in zasebnosti, kar je lahko v javnem oblaku kritično (Kavis, 2014). Ena od prednosti je tudi okretnost, saj je potreba po hitri prilagoditvi in spremembam v poslovanju temeljno načelo digitalnega poslovanja. Podjetje mogoče potrebuje ali želi združitev javnih, zasebnih in lokalnih virov, da bi pridobili na spretnosti, ki jo organizacija potrebuje za konkurenčno prednost. Ostale prednosti hibridnega oblaka so: skalibilnost, saj je omogočenih skoraj neskončno virov zaradi virov na zahtevo; nižji investicijski stroški v opremo za infrastrukturo; višja zanesljivost zaradi razpršenosti podatkov po več podatkovnih centrih; varnost podatkov in aplikacij, sploh občutljivih podatkov, saj je v zasebnem oblaku ta višja; večji nadzor in prilagodljivost infrastrukture po željah uporabnika; prilagodljivost in sposobnost premikanja neobčutljivih podatkov v javni oblak, da so viri zasebnega oblaka na voljo v primeru povečane obremenitve infrastrukture (Lucidchart Content Team, brez datuma; NetApp, brez datuma).

Hibridni oblak ima tudi slabosti oz. pomanjkljivosti. Ne glede na prednost o varnosti se pojavlja tudi slabost pri zagotavljanju varnosti, saj so podatki na različnih lokacijah in nimamo nadzora, kje se podatki obdelujejo. Prav tako se povečujejo operativni stroški glede na zmogljivost sistema, potrebna pa je tudi začetna investicija za nakup določene opreme.

Uporabnik tudi prevzema odgovornost za upravljanje in vzdrževanje lastne infrastrukture, tako strojne kot tudi programske opreme in njeno kompatibilnost ter varnosti, prisotna je tudi zmanjšana prožnosti infrastrukture pri povečanju ali zmanjševanju potreb po virih (Lucidchart Content Team, brez datuma; NetApp, brez datuma).

2.6.4 Oblak skupnosti

NIST opredeljuje, da je infrastruktura računalniškega oblaka skupnosti namenjena izključno uporabi določene skupnosti uporabnikov ene ali več organizacij, ki imajo enake interese (npr. isto poslanstvo, varnostne zahteve, politike ali skladnostne zahteve). Tako kot zasebni računalniški oblak je tudi oblak skupnosti lahko v lasti, upravljanju in delovanju ene ali več organizacij skupnosti, tretje strani ali neke vrste njihove kombinacije ter je lahko nameščen znotraj ali zunaj poslovnih prostorov (Ujčič & Florjančič, 2017; Mell & Grance, 2011).

Oblak skupnosti je različica modela zasebnega oblaka, ki zagotavlja celovito rešitev v oblaku za določene poslovne skupnosti. Podjetja si delijo infrastrukturo in programsko-razvojno opremo, ki je zasnovana za skupne potrebe. Vsako podjetje ima pri tem svoj zasebni prostor v oblaku in ima tako zagotovljeno varnost in zasebnost za interno delovanje ter tudi okolje skupnosti, do katerega imajo dostop tudi drugi sodelujoči. Oblak skupnosti je privlačen za uporabo v organizacijah, ki imajo skupne interese in značilnosti, kot so dejavnosti, varnostne zahteve in politika podjetja. Primerni so tudi za upravljanje skupnih projektov, saj se lahko kombinirajo različne vrste oblakov z različnimi modeli storitev in podjetjem nudijo privlačne rešitve v oblaku, ki ustrezajo trenutnim skupnim potrebam. Oblak lahko upravlja in nadzoruje skupina v oblaku skupnosti ali pa tudi ponudnik storitve (AbacusNext, brez datuma).

3 ZAGOTAVLJANJE VARNOSTI V MODELU OBLAKA INFRASTRUKTURA KOT STORITVE

V tem poglavju magistrske naloge se bom osredotočil na pomembne dejavnike pri zagotavljanju varnosti modela oblaka infrastruktura kot storitve. Kot je bilo že opisano v preteklih poglavjih, je oblak infrastruktura kot storitev eden najbolj temeljnih modelov zagotavljanja storitev računalništva v oblaku. Sestavljen je iz širokega spektra virtualiziranih informacijsko-tehnoloških virov in je na voljo kot storitev na zahtevo. Bistvo tega modela je virtualizacijska platforma, kjer lahko uporabnik upravlja svoje okolje na oddaljenem fizičnem strežniku s pomočjo internetne povezave.

Ne glede na to, da ponudniki storitev zagotavljajo visoko stopnjo varnosti podatkov, imajo uporabniki še vedno dvome v varnostne mehanizme, posledično pa ne zaupajo svojih podatkov v oblačne storitve. Za zagotavljanje varnosti oblaka infrastrukture kot storitve je v veliki meri odgovoren tudi uporabnik sam, pri tem pa mora preprečiti različna varnostna tveganja. Da je varovanje infrastrukture ustrezno, mora poskrbeti za ustrezne varnostne

ukrepe, si postaviti ustrezna varnostna vprašanja in predvideti različne grožnje, ki jim je infrastruktura lahko izpostavljena.

Široka dostopnost do storitev v oblaku je med pomembnejšimi razlogi, da začne organizacija uporabljati storitve za različne namene. Pri tem pa se pojavi vprašanje nadzora nad podatki in varnostjo, saj se z najemom storitve v oblaku in migracijo ti premaknejo iz varnega okolja, kjer so bili pred tem ustrezno varovani. Ponudnik storitve v oblaku mora pri tem prevzeti del odgovornosti, da zagotovi zaščito podatkov in varen dostop, del odgovornosti pa je odvisen od storitvenega modela, kjer ima najmanj odgovornosti pri modelu IaaS, kjer nosi odgovornost sam najemnik storitve.

Pri zagotavljanju varnosti se je treba tudi prepričati, ali je preprosta avtentikacija ustrezen način varovanja, saj se napadalec z ukradenim geslom ali drugim avtentikacijskim sredstvom prebije do širokega nabora storitev in podatkov v oblaku. Zaradi nestandardiziranih oblik delovanja oblakov, ti delujejo različno in predstavljajo različne rešitve, med katerimi izbirajo uporabniki. Na ta način so uporabniki kasneje tudi »obsojeni« uporabljati izbrano rešitev, kar je bilo opisano v prejšnjih poglavjih in pomeni »lock-in« na enega ponudnika, saj je prehod drugam običajno preveč zapleten za izvedbo zaradi medsebojne nekompatibilnosti in je potrebna ponovna postavitev infrastrukture pri drugem ponudniku (Božič, 2011).

Ali so podatki bolj varni ali ne z uporabo oblaka ni samoumevno vprašanje v primerjavi z zagotavljanjem lastnega nadzora, da je tudi varnejše. Pri tem gre predvsem za zaupanje v operacijski sistem, strojno opremo, programsko opremo in podobno tudi zaupanje ponudniku storitve računalništva v oblaku. Vseeno se pojavlja ena razlika pri tem, če imaš računalniške zmogljivosti pod svojim nadzorom, kjer skrbiš za različne varovalne mehanizme in zunanjim ponudnikom. Zunanjemu ponudniku je treba v celoti zaupati, pri tem pa se ne zaupa samo v varnostne postopke in ukrepe, ampak tudi v zanesljivost, dostopnost in stanovitnost delovanja. Pri lastnem izvajanju ni prevelike skrbi, da bi diskovna polja kupil konkurent, kar pa je lahko pri najemu storitve v oblaku težava, saj si v trenutku odvisen od plačevanja najemnine konkurenci za svoje podatke, in je priporočljivo, da ima najemnik storitve urejene ustrezne varnostne kopije. Pri zagotavljanju varnosti in pred varnostnimi tveganji predstavljajo težavo tudi lokacije podatkov, shranjevanje podatkov različnih uporabnikov ter vprašljivost zagotavljanja podatkov le lastnikom teh podatkov. Obstajajo tudi varnostna tveganja napadov spremljanja podatkov, ki lahko zlorablja aktivno ali pa pasivno (Tomšič, 2011).

3.1 Sestavni deli oblaka infrastruktura kot storitev

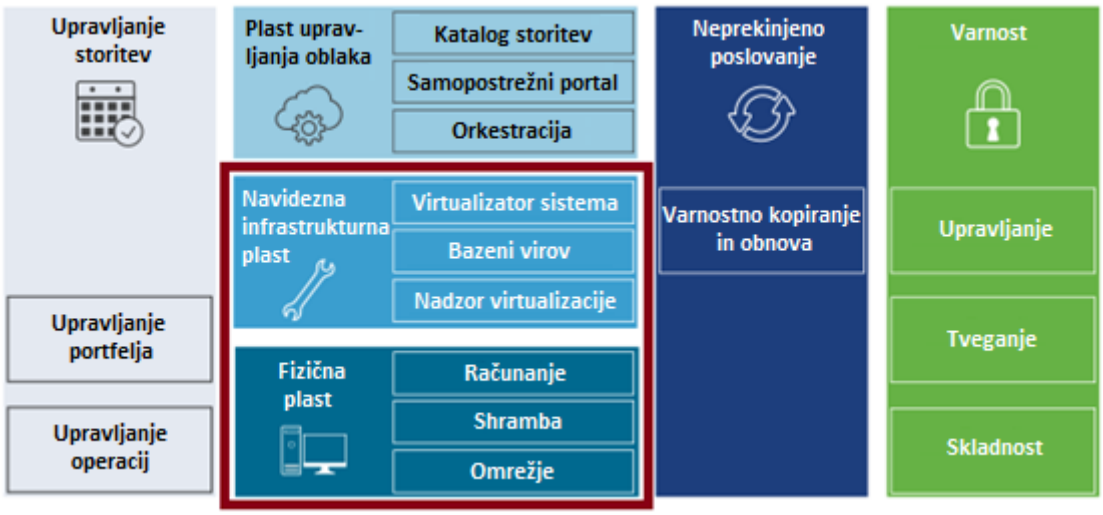
Storitev oblaka infrastruktura kot storitev uporabniku zagotavlja navidezni računalnik, na katerega nato nalaga lastni operacijski sistem, pri tem pa ima zagotovljeno vso osnovno računalniško infrastrukturo, tj. pomnilnik, prostor za podatke in omrežje. Če pa se postavimo v vlogo ponudnika storitve, je ta zadolžen za vzpostavitev celotne strojne računalniške in programske opreme. Celotna strojna in programska oprema ponudnika storitve

infrastruktura kot storitev je sestavljena iz tako imenovanih dveh najpomembnejših plasti, in sicer iz fizičnega nivoja in virtualnega infrastrukturnega nivoja. Zaradi lažjega razumevanja zagotavljanja ustrezne zaščite sistema, bodo v tem podpoglavju magistrske naloge predstavljeni in opisani obe omenjeni plasti in tudi ostale, ki so vidne na Sliki 6 (Chawkia, Ahmed & Zakariaea, 2018; vmware, 2019).

Fizična plast je najnižja plast rešitve v oblaku, ki je sestavljena iz strojne opreme. Ta zajema računalniške komponente za zagotavljanje računske zmogljivosti oz. procesorske zmogljivosti, kjer tečejo strežnik, prostorske komponente za zagotavljanje ustrezne velikosti podatkovnih centrov in komponente za zagotavljanje omrežne povezljivosti.

Navidezna infrastrukturni plast se nahaja nad fizično plastjo in je bistvena za ustrezno delovanje fizične plasti v dodeljevanju virov uporabnikom. Navidezna infrastrukturna plast nadzira dostope do osnovne fizične infrastrukture in nadzoruje ter dodeljuje vire za upravljanje in delovanje potreb najemnikov. Upravljanje delovne obremenitve je sestavljeno iz navidezne infrastrukturne plasti, v veliko pomoč pri delovanju pa so še plast za upravljanje oblaka, plast za upravljanje storitev, plast kontinuitete poslovanja in varnostna plast.

Slika 7: Arhitektura IaaS



Vir: Prirejeno po VMware (2019).

Plast upravljanja oblaka je nad virtualno plastjo. Skrbi za usklajeno izvajanje procesov na nižji plasti za dodeljevanje virov, katerih potrebo sprožijo najemniki storitve.

Plast upravljanja storitev skrbi za zagotavljanje dnevnih storitev, predvsem upravljanje operacij, monitoring, opozorila in upravljanje dnevnikov.

Plast za upravljanje operacij v realnem času spremlja fizično infrastrukturo, virtualno upravljanje in delovanje sistema, ki se beleži v podatkovnih bazah in dnevnikih dogodkov.

Plast kontinuitete poslovanja skrbi za podporo za neprekinjeno poslovanje z zagotavljanjem varnostnih kopij in obnovitve podatkov.

Varnostna plast zagotavlja varnost sistema in preprečuje notranje ali zunanje zlorabe.

3.2 Varnostne zahteve

Upravljanje varnosti je zapletena naloga, ki vključuje več različnih komponent in delov infrastrukture oblaka. Za razumevanje varnostnega tveganja pri modelu IaaS je treba pred tem razumeti in znati oceniti tveganja, ki jim je izpostavljen uporabnik in ponudnik storitve. To je v veliki meri odvisno od tega, za kakšne namene bo uporabnik oz. organizacija storitev uporabljala, saj je veliko bolj izpostavljena v primerih, ko je ta vplivnejši igralec med konkurenti na trgu. V teh primerih se lahko pričakuje povečanje verjetnost za zlorabe ter mora uporabnik sam poskrbeti, da svoje podatke in sistem, ki ga uporablja v oblaku, ustrezno zaščiti. V primeru manj vplivnih uporabnikov storitve je sam uporabnik izpostavljen manjšim tveganjem, vendar je prav tako priporočljivo, da se ustrezno zaščiti pred nepooblaščenimi dostopi do podatkov. Visoka tveganja pred nepooblaščenimi vdori lahko predstavljajo tudi ponudniki storitev, ki so prav tako odvisni od vplivnega deleža svoje storitve na trgu in so izpostavljeni različnim napadom.

Tabela 1: Varnostne lastnosti, ki se zahtevajo pri komponentah modela IaaS s strani uporabnika (U) ali ponudnika oblačnih storitev (P).

Varnostne zahteve	Avtentikacija	Šifriranje	Integriteta/ celovitost	Razpoložljivost	Nadzor dostopa
Strojna oprema	P	-	-	P	-
Virtualizacija	P / U	-	P / U	P	P / U
Shranjevanje podatkov	-	P / U	U	P	P / U
Mrežno povezovanje	-	-	-	P	P / U
Programska oprema oblaka	P	-	-	P	-
Uporabni računalništvo	-	-	P	-	P
Sporazum o ravni storitev	-	-	-	P	P

Vir: Chawkia, Ahmed & Zakariaea (2018).

Napadi na ponudnika storitve so lahko še bolj občutljivi, saj v primeru, da se napadalec uspešno prebije v jedro sistema oblaka ponudnika, lahko posledično zlorabi podatke uporabnikov. Tudi na tem nivoju mora ponudnik storitve poskrbeti za ustrezno varovanje in

zaščito, ki omogoča uporabo storitev le pooblaščenim osebam in ne omogoča dostopa do podatkov brez ustreznih nivojev varovanja. Za zagotavljanje ustrezne varnosti ima ponudnik storitev v oblaku omejeno odgovornost. Ponudnik storitve ima popoln nadzor nad spodnjimi plastmi infrastrukture, kjer se nahaja virtualizacija sistema in zagotavljanje storitev uporabnikom, medtem ko pa je nivo virtualnega okolja, kjer uporabniki uredijo lastno virtualno okolje, prilagojeno svojim potrebam, uporabnik dolžan urediti in zagotoviti sam.

Avtorji članka (Chawkia, Ahmeda & Zakariaea, 2018) so raziskovali varnostna tveganja oblaka IaaS. Skozi tabelo 1 so prikazane komponente modela oblaka IaaS, ki so v relaciji z varnostnimi zahtevami, ki jih je treba zagotoviti s strani uporabnika in ponudnika storitve v oblaku, da bi bilo zagotovljeno dobro delovanje celotne arhitekture na vsaki komponenti z ustreznim ravnanjem odgovornih udeležencev. Iz te je razvidno, da je v veliki meri za zagotavljanje ustreznih varnostnih pogojev soodgovoren tako ponudnik kot tudi uporabnik storitve. Obstaja področje, kjer je uporabnik sam odvisen od svojega upravljanja določenih delov podatkov pri izpolnjevanju varnostnih zahtev ter tudi področja, kjer je za samo zagotavljanje in izpolnjevanje varnostnih zahtev odgovoren izključno ponudnik storitve.

3.3 Varnostna vprašanja

Vprašanje o varnosti in zagotavljanja ustrezne zaščite podatkov pred nepooblaščeno uporabo je pomemben dejavnik, še preden se uporabnik ali organizacija odločijo za najem storitve ponudnika. Pogodba o zagotavljanju storitev je ena od takšnih, kjer ponudnik uporabniku razkrije svoj način varovanja in upravljanja s podatki. Ta naj bi vključevala vse ključne točke, ki so potrebne, da naj bi imel sam uporabnik ustrezno varovane podatke. S to pogodbo se ponudnik storitve tudi zavezuje k zagotavljanje predpisane razpoložljivosti storitve. Skozi več raziskav se je izkazalo, da različni ponudniki storitve ne opredeljujejo vseh pogojev uporabe in zagotavljanja sredstev, s čimer tako med seboj na trgu tekmujejo in poudarjajo svoje konkurenčne prednosti pred ostalimi ponudniki, da bi lažje privabili nove najemnike storitve. Ob tem, da vsak poudarja samo svoje prednosti, pa skrivajo svoje pomanjkljivosti, ki jih običajno zamolčijo oz. jih poizkušajo skriti. S standardizirano enotno pogodbo bi uporabniki storitve predstavili vsa svoja močna in šibka področja storitve, vendar pa takšna pogodba ne obstaja in ima vsak ponudnik storitve svojo individualno pogodbo.

Zapleten koncept arhitekture računalništva v oblaku predstavlja ponudniku velike izzive pri zagotavljanju zadostnih količin računalniških virov v oblaku, pri tem pa mora poskrbeti tudi za nadzor delovanja storitev in uporabnikovo uporabo. Zloraba sistema s strani napadalcev se zgodi iz različnih razlogov. Nekateri želijo pridobiti podatke, spet drugi pa želijo škodovati le delovanju sistema tako, da onemogočajo delovanje in povzročajo izpad dostopa, s tem pa posledično škodujejo uporabnikom, saj te ne morejo uporabljati najete infrastrukture.

Platforma za virtualizacijo je občutljiva na različne napade, ki se lahko zgodijo na različnih slojih. Tako avtorji (Chawkia, Ahmed & Zakariaea, 2018) izpostavljajo dva nivoja

izpostavljenosti pred napadi v infrastrukturi oblaka IaaS. Prvi nivo napada je napad na gostiteljski nivo znotraj virtualnega oblaka oz. napad na uporabnika storitve IaaS, drugi nivo pa predstavlja napad na samo infrastrukturo oblaka IaaS oz. napad na ponudnika oblačne storitve. V primeru prvega je napad izveden le znotraj virtualnega okolja in razen podatkov tega okolja, ostali naj ne bi bili v nevarnosti pred zlorabo, pod pogojem, da ponudnik storitve zagotavlja ustrezno infrastrukturo, to je zagotavljanje ustrezne izolacije virtualnih okolij najemnikov storitve. V drugem primeru, ko se zgodi napad na samo infrastrukturo IaaS pri ponudniku storitev, pa je ogroženost podatkov višja. Napadalec lahko onemogoči dostope, pridobi podatke uporabnikov storitve, dostope do virtualnih okolij, migrira podatke ali celo prevzame nadzor nad samim sistemom delovanja. Iz opisanih razlogov in še številnih drugih mora ponudnik storitve skrbno načrtovati načine varovanja in izpolnjevanje varnostnih kriterijev, da se ustrezno ubrani pred morebitnimi zlorabami. Virtualizator sistema (angl. hypervizor) poskrbi tudi za zagotavljanje prilagodljivosti sistema. Virtualizacija omrežja je občutljiva tudi na nivoju medsebojnega povezovanja virtualnih okolij. Najpogosteje se napadi izvedejo na virtualizacijo omrežja s pregledovanjem prometa (angl. Sniffing attack) in napadom s ponarejanjem (angl. Spoofing attack).

Zagotavljanje varnosti v omrežju v modelu infrastruktura kot storitev je zaradi zapletenosti arhitekture, težko popolno zagotoviti. Avtentikacija, napadi v zakulisje in kraja seje so glavne varnostne grožnje pri skalibilnosti omrežja. Raziskave na temo varnostnih tveganj predlagajo ustrezno ureditve omrežnega sistema, ki bi preverjal stanje v omrežju in zaznaval vdore z zagotavljanjem nadzora omrežnega prometa (Chawkia, Ahmed & Zakariaea, 2018).

3.4 Izpostavljene grožnje oblaka

Vodilna svetovna organizacija Cloud Secutiry Alliance (CSA) skrbi za opredelitev računalništva v oblaku in za ozaveščanje o najboljših praksah med uporabniki za zagotavljanje varnega računalniškega okolja v oblaku. Organizacija pridobiva informacije na podlagi poročil strokovnjakov iz različnih okolij, kjer delujejo, tj. industrije, različnih združenj, vlad ter njihovih korporacij ter posameznikov, ki zagotavljajo raziskovalna izobraževanja, različna certificiranja in storitve računalništva v oblaku. Glede na njihove izkušnje in znanje s tega področja so leta 2016 izpostavili najpogostejše grožnje za računalništvo v oblaku (Chawkia, Ahmed & Zakariaea, 2018):

Zloraba osebnih podatkov. Dostop do občutljivih, zaščitenih ali zaupnih podatkov s strani nepooblaščenih oseb, ki jih pregledujejo ali uporabijo na različne načine, so posledica človeške napake ali slabe varnostne prakse. Predlagana rešitev za zaščito so ustrezni kriptografski mehanizmi za shranjevanje in kopiranje podatkov, ki bodo onemogočali prosti dostop.

Neustrezno upravljanje z identitetami, poverilnicami in dostopi. Uporabniki bi morali uporabljati unikatne identitete, ki bi ustrezale varnostnim zahtevam. Da se uporabnika pred zlorabo ustrezno zaščiti, je treba poskrbeti za preverjanje prisotnosti in nadzor dostopa na

nivoju virtualizacije. To se zagotovi z večstopenjskimi gesli in mehanizmi za preverjanje prisotnosti.

Nevarni vmesniki in aplikacije. Odprtokodna narava storitev, vmesnikov in aplikacij pogosto uporablja anonimne ali nezaščitene dostope in povzroča ranljivost računalništva v oblaku. Da bi se izognili morebitnim zlorabam, mora ponudnik storitve poskrbeti za ustrezno preverjanje prisotnosti, šifriran prenos podatkov na ravni omrežja in kompleksne mehanizme za nadzore dostopa in overjanje.

Sistemska ranljivost. Povzročajo jo različne napake, ki jih napadalci izkoristijo za infiltracijo v računalniški sistem za krajo podatkov, prevzem nadzora ali motenje delovanja. Zaščita pred sistemsko ranljivostjo je uporaba zaupanja vrednih storitev pod nadzorom in spremljanje storitev.

Kraja uporabniškega dostopa ali storite. Vzrok za ranljivost je lahko slaba varnost infrastrukture ali uporaba zlonamernih trikov za nepooblaščeno pridobitev podatkov. Zaščita pred oškodovanjem je ustrezna zagotovitev mehanizmov za preverjanje prisotnosti in uporaba varnih komunikacijskih kanalov.

Zlonamerni notranji strokovnjaki. To so ljudje, ki so bili kakorkoli povezani z organizacijo in jo želijo oškodovati na različne načine. Za zaščito v teh primerih je treba poskrbeti za ustrezne pogodbe, ki opredeljujejo ukrepanje glede na kršitve in zagotavljajo varnost ter pregledno upravljanje.

Napredni napadi. Napadalec se infiltrira v sistem žrtve s pomočjo različnih namenskih programov ali še neznanih varnostnih lukenj, ki pripomorejo pri uhajanju podatkov iz različne intelektualne lastnine. Zaščita pred temi napadi se zagotavlja z ustreznimi sistemi za zaznavanje vdorov, ki kontrolirajo odhodni promet in predvidevajo morebitne grožnje na končnih točkah.

Izguba podatkov. Lastništvo podatkov, šifriranje in prenos, operativne napake, brisanje podatkov ter razpoložljivost podatkov v okolju oblaka predstavljajo različne izzive. Poskrbeti je treba za ustrezno zasebnost in varnost podatkov ter možnost shranjevanja in varnostnega kopiranja.

Skrbnost dobrega gospodarja. Poskrbeti je treba za razvoj dobrega načrta in kontrolnega seznama za preverjanje delovanja tehnologije, kar je ključno za uspešno upravljanje. Upravljanje s tveganji morajo prevzeti le administratorji v oblaku in odgovorne osebe.

Zlorabe in škodljiva uporaba storitev v oblaku. Zaradi anonimnosti pri uporabi nekaterih storitev te izkoriščajo tudi različne kriminalne združbe za izvajanje različnih nelegalnih procesov in kraj. Da bi se ponudnik zaščitil pred takimi zlorabami, je treba poskrbeti za ustrezno overjanje in nadzorovanje stanja omrežja z zagotavljanjem robustnih tehnik, ki uporabljajo omenjeno overjanje.

Izpad storitve. Pomanjkanje »neomejenih« omejenih sistemskih virov lahko povzroča izpad delovanja storitev in razpoložljivosti, kar je lahko tudi posledica premočnih preverjanj prisotnosti in avtorizacije, ki za izvajanje potrebujejo procesorske, pomnilniške in diskovne kapacitete.

Tehnologija deljenja virov. Deljenje virov in storitev med več različnimi najemniki povečuje odvisnost od logične segregacije in drugih kontrol, da je zagotovljena medsebojna izolacija podatkov in varnostnih kopij. Uporabniki med seboj ne morejo posegati v varnost drugih uporabnikov, za kar se uporabljata močno avtentikacijo in nadzor dostopa, ki zagotavljata ustrezno neodvisnost.

Načinov, kako se napadalci prebijejo do koristnih in nepooblaščenih informacij znotraj infrastrukture v oblaku IaaS, je še veliko več, kar predstavlja tudi dodatna tveganja in grožnje. V tem podpoglavju je bilo izpostavljenih le 12 najpogostejših, ki jih izpostavlja organizacija CSA kot največkrat zasledene in omenjene iz različnih okolij in uporabnikov, ki se srečujejo z uporabo te storitve. Da bi se zagotavljalo, kar se le da ustrezno zavarovano in nadzorovano infrastrukturo, tako s strani najemnikov kot tudi s strani ponudnika storitve, bo v naslednjem podpoglavju predstavljen kontrolni list, ki je v pomoč pri zagotavljanju želenega ustreznega nivoja varnosti, da bi se preprečilo ali otežilo izvajanje različnih zlorab znotraj ali zunaj infrastrukture oblaka IaaS.

3.5 Varnostni seznami za zagotavljanje varnosti v modelu infrastruktura kot storitev

Pred začetkom uporabe oblaka infrastruktura kot storitev je pomembno, da si zastavimo ustrezna varnostna vprašanja v smislu uporabe in izpostavljenosti tveganja, saj le tako dobimo ustrezen pogled na to, kako močno je priporočljivo varovati celoten sistem. Ker je arhitektura oblaka modela IaaS obsežna in zajema različne sisteme, so pripravljeni za zagotavljanje celostnega varovanja varnostni kontrolni seznami, ki pomagajo pri zagotavljanju ustrezne zaščite, da bi se ustrezno zavarovali pred kibernetskimi napadi. Avtorji kontrolnih seznamov (Heder in drugi, 2016) so te oblikovali na podlagi modelov groženj in pogostih varnostnih vprašanj.

Varnost spletnih vmesnikov in zagotavljanje ustrezne varnosti je zelo pomembno. Preden se začne uporabljati storitev IaaS je treba, da se opravijo testiranja, tako na ponudnikovi kot tudi na najemnikovi strani, ter da je zagotovljena ustrezna varnost dostopa uporabnikov.

Varnostni seznam za spletni vmesnik v oblaku:

- Bistvenega pomena je, da spletni vmesniki uporabljajo varno povezavo (https);
- Bistvenega pomena je, da so spletni vmesniki zaščiteni z uporabo certifikata, ki mu zaupajo uporabniki;
- Pomembno je, da certifikatom na strežniku zaupajo brskalniki;

- Pomembno je, da uporabniki uporabljajo certifikate;
- Pomembno je, da imajo skrbniki oblaka in najemniki ločene strani za administracijo;
- Pomembno je, da je zagotovljena večnivojska overitev uporabnikov z višjimi ravnmi dostopa.

Upravljanje varnostnih posodobitev virtualnih virov lahko predstavlja različna varnostna tveganja, saj v primeru starih predpripravljenih virtualnih strojev predstavljajo, ob morebitnih neposodobljenih programskih rešitvah, potencialno varnostno tveganje. Možno je uporabljati tudi neuporabljene virtualne računalnike, ki se neprestano posodabljajo in tako zmanjšajo varnostno tveganje, vendar v primeru podvojitve, če niso programi predpripravljeni, lahko pripelje do izgube podatkov v primeru prepisovanja stare verzije z novo.

Varnostni seznam za upravljanje posodobitev varnosti virtualnih virov:

- Bistvenega pomena je, da je predloga virtualnega računalnika nastavljena tako, da ob prvem zagonu poišče in namesti vse najnovejše varnostne posodobitve;
- Pomembno je, da je predloga virtualnega stroja nastavljena tako, da blokira dohodne povezave, dokler se ne zaključijo vse varnostne posodobitve;
- Pomembno je, da se primarni virtualni računalnik posodobi takoj, ko so na voljo nove posodobitve za operacijski sistem. Iz posodobljenega virtualnega računalnika se nato ustvarjajo replike;
- Pomembno je, da lahko sistemski administrator izvede revizije na pretekle verzije stanja virtualnih računalnikov (vračanje sistema na prejšnjo verzijo, varnostne kopije);
- Pomembno je, da je uporabnik seznanjen s tveganji v primeru vračanja na pretekle verzije sistema in morebitne izgube.

Posodabljanje infrastrukture IaaS predstavlja veliko tveganje v primeru nedelovanja. Pomembno je, da so izpadi kratki ali pa se celo ne dogajajo, vendar obstajajo določeni postopki nadgradnje, v katerih brez popolnega izklopa tega ni mogoče izvesti.

Varnostni seznam za upravljanje varnostnih posodobitev programske opreme IaaS:

- Bistvenega pomena je, da so na voljo orodja za ponovno vrnitev sistema;
- Bistvenega pomena je, da so komponente vedno funkcionalne, tudi ko je omrežje nedostopno;
- Pomembno je, da so viri za posodobitve preverjeni;
- Pomembno je, da je zagotovljena vzporedna rešitev za preklop v primeru izpada komponente;
- Pomembno je, da je omogočena selitev virtualnih računalnikov v času, ko ti delujejo;
- Pomembno je, da so na voljo navodila za izvajanje postopkov.

Virtualne slike računalnikov morajo biti ustrezno urejene in ustvarjene, da ne vsebujejo pomembnih podatkov, ki bi kakorkoli lahko pomagali napadalcem, da bi lažje vstopili v sistem. To je pomembno predvsem v primerih, ko se ustvarjajo duplikati že ustvarjenih računalnikov in ti vsebujejo varnostne pomanjkljivosti.

Varnostni seznam za zaščito slik virtualnih mašin:

- Bistvenega pomena je, da predloga virtualnega računalnika ne vsebuje podatkov, ki bi jih lahko izkoristil nekdo, ki ima dostop do iste virtualne predloge (SSH-ključi, SSL-potrdila, gesla, požarni zid in pravila);

- Bistvenega pomena je, da je predloga, ki jo ustvari uporabnik, ločena od predpripravljene predloge IaaS;
- Pomembno je, da so ob izbiri predloge vidni tudi podatki o ustvarjalcu, času nastanka in varnostnih pregledih.

V primeru izbrisa virtualnega računalnika je treba zagotoviti, da se izbrisani podatki nikakor ne morejo povrniti ali kasneje prebrati, da bi jih lahko novo nastali virtualni računalniki pridobili in prebrali. Treba je poskrbeti za ustrezno čiščenje in onemogočanje kakršnegakoli restavriranja izbrisanih podatkov.

Varnostni seznam za ponovno uporabo virov in razveljavitev:

- Bistvenega pomena je, da se diskovni bloki nikoli ne dodelijo brez predhodnega prepisa podatkov;
- Bistvenega pomena je, da se ob zagonu virtualnega računalnika delovni in ostali pomnilniki počistijo;
- Pomembno je, da je omogočeno kriptiranje virtualnih računalnikov.

Varovanje omrežja v IaaS pri virtualnih računalnikih igra pomembno vlogo, kjer je treba zagotoviti ustrezno omrežno izolacijo in filtriranje prometa, ki onemogoča morebitne napade znotraj omrežja.

Varnostni seznam za varnost v omrežju oblaka:

- Bistvenega pomena je, da je nadzor podatkovnega omrežja ločen od omrežja virtualnih računalnikov;
- Bistvenega pomena je, da sta Address Resolution Protocol (ARP) in Dynamic Host Configuration Protocol (DHCP) onemogočena, razen če je zahtevek iz veljavnega vira;
- Bistvenega pomena je, da napadalni virtualni računalnik ne more pridobiti IP-naslova druge virtualnega računalnika. Pakete prejema in pošilja samo preverjeni virtualni računalnik;
- Bistvenega pomena je, da se elementi oblaka IaaS ne morejo izvajati v oblaku IaaS;

- Bistvenega pomena je, da se migracija virtualnih računalnikov izvaja v ločenem omrežju, izoliranem od ostalih;
- Pomembno je, da so zagotovljeni enaki varnostni ukrepi za IPv4 in tudi za IPv6;
- Pomembno je, da so na voljo tako naslovi IPv4 kot tudi IPv6;
- Pomembno je, da se naslovi IPv6 ne dodeljujejo v naprej, razen če to ni zahtevano;
- Pomembno je, da dobi vsak uporabnik na virtualnem računalniku svoje podomrežje.

Dnevniki dogodkov zagotavljajo večji pregled nad delovanjem in tako izboljšujejo varnostno stanje sistema. V primeru gostovanja najemnik običajno nima vpogleda v vse dnevniške podatke o infrastrukturi, ampak le njemu namenjene pomembne informacije o delovanju.

Varnostni seznam za dostop do dnevnikov in podatkov dostopa:

- Pomembno je, da ima uporabnik omogočen vpogled v nastavitve virtualizacije;
- Pomembno je, da lahko uporabnik vidi verzijo programske opreme, podatke operacijskega sistema, jedra in arhitekturo virtualizacije;
- Pomembno je, da ima uporabnik na voljo dnevnike svojih virtualnih računalnikov;
- Pomembno je, da ima uporabnik omogočen vpogled v varnostni dnevnik omrežja svojega virtualnega računalnika.

Za preprečevanje prekomerne uporabe virov ali prednastavljenih kvot je treba zagotoviti ustrezne mehanizme za opozarjanje in omejevanje delovanja, ki po potrebi zaustavijo storitve, ko so doseženi limitni pogoji.

Varnostni seznam za reševanje izrabljenosti dodeljenih virov:

- Pomembno je, da dobi uporabnik opozorilo o vnaprej določenih omejitvah uporabe;
- Pomembno je, da lahko uporabnik opredeli pravilnike uporabe, npr. na največjo porabo v časovnem obdobju ali največjo porabo na odjemalca (na podlagi dodeljenega IP naslova).

4 SKLADNOST S SPLOŠNO UREDBO EVROPSKE UNIJE O VARSTVU PODATKOV

Vse več uporabnikov in podjetij seli storitve v oblak, saj ta omogoča optimizacijo IT-virov, ki so prilagodljivi in skoraj neomejeni. Ponudnik storitve v oblaku tako v imenu najemnika obdeluje osebne podatke, ki so shranjeni v podatkovnih centrih in strežnikih. Ponudnik storitve v oblaku ne sme uporabiti podatkov, razen če dobi navodilo najemnika, drugače pa morajo ostati pod nadzorom najemnika. Uporaba storitev računalništva v oblaku vseeno predstavlja izzive pri zagotavljanju zasebnosti in zagotavljanju skladnost s splošno uredbo Evropske unije o varstvu podatkov (angl. General Data Protection Regulation, v nadaljevanju GDPR). Tudi občutljive informacije lahko uporabniki hranijo v storitvah oblaka, vendar pri tem povečajo tveganje za nenadzorovano distribucijo tretjim osebam, za

katere ne želijo, da dobijo dostop do teh podatkov. Težavo predstavljajo tudi geografske lokacije obdelovanih podatkov storitve računalništva v oblaku, saj so ti podatki o lokaciji zabrisani zaradi različnih podatkovnih centrov in rednega prenašanja med lokacijami za zagotavljanje ustreznih varnostnih korakov ponudnikov storitev. To predstavlja uporabnikom in najemnikom velike izzive, da zadostijo zahtevam s predpisi in zakoni. Izziv predstavlja tudi eksternalizacija zasebnosti, saj najemniki želijo, da ponudnik storitve izvaja pogoje zasebnosti, ki so jih sprejeli znotraj organizacije, te pa želijo izvajati tudi pri ponudniku storitve računalništva v oblaku.

GDPR predstavlja specifične izzive. Eno od določil navaja, da se osebni podatki ne smejo hraniti dlje, kot je predpisano glede na namen podatkov. Po pretečenem obdobju je treba zagotoviti ustrezen izbris z vseh lokacij, če ponudnik podatke hrani na različnih lokacijah, prav tako je potreben izbris varnostnih kopij. Zaradi navedenega je potreben dober pregled nad zaščito varnostnih kopij in nad upravljanjem hranjenja podatkov s strani ponudnika storitve.

Obveznost obveščanja o kršitvah in določila o protokolih morajo biti vključeni v sporazume o obdelavi podatkov s ponudniki oblakov. V pogodbi mora biti opredeljena kršitev ter opisan postopek, s katerim mora ponudnik brez odlašanja obvestiti najemnika o kršitvah. V primeru, da pride do zlorabe oblaka in je pri tem oškodovanih več najemnikov storitve, mora imeti uporabnik omogočeno zunanjo podporo reševanja kršitev.

V primeru obdelave podatkov zunaj evropskega prostora je treba sprejeti posebne zaščitne ukrepe, če pred tem niso urejeni pogoji upravljanja s podatki, kar je odvisno od politike države, kjer se ti hranijo. Ponudniki storitve imajo lahko namreč podatkovne centre na več lokacijah, ki so tudi zunaj evropskega prostora, kjer pa uredba GDPR ne velja.

Omogočena mora biti prenosljivost podatkov, da lahko te podatke uporabnik prenese k drugemu ponudniku. V primeru hranjenja podatkov v oblaku lahko uporabnik te podatke pridobi v datotečni strukturi, ki jih posreduje v nadaljnje hranjenje drugemu ponudniku. Ponudnik storitve naj bi v skladu z možnostjo dogovora poskrbel za tehnično sposobnost, tako da lahko najemnik storitve te podatke uporablja na novi storitvi.

Podobno je z lastništvom podatkov, saj mora najemnik storitve kot upravljavec nad podatki ohraniti nadzor in lastništvo, kar se opredeli v pogodbi, ta pa mora biti usklajena z zakoni držav gostiteljic, da lahko podjetje obdrži lastništvo nad svojimi podatki.

Za upravljanje s tveganji mora imeti ponudnik storitve v oblaku opredeljene predpise upravljanja s tveganji tretjih oseb. Za določitev tveganj, ki lahko nastanejo pri uporabi storitve v oblaku, se lahko izvede ocena učinka na varstvo podatkov in varnostna ocena. Pri tem mora biti v pogodbi omogočena tudi pravica do revizije podatkov, kjer je treba poleg ustreznega revizijskega načrta poskrbeti tudi za kontrolni okvir zasebnosti ter ukrepe za nadzor zasebnosti.

Upoštevati je treba tudi načelo najmanjšega obsega podatkov in vidnost metapodatkov. Uporabnik, ki želi začeti uporabljati storitev v oblaku, mora po pogodbi poznati, katere metapodatke bo ponudnik storitve zbiral. Zbira lahko le minimalno količino zahtevanih podatkov, pri tem pa je treba preveriti raven zaščite metapodatkov, lastniške pravice, pravice o preklicu zbiranja ali distribucije podatkov in predvidene uporabe metapodatkov.

Varnost zasebnosti je pomembna, saj uporabnik nima nadzora nad okoljem ponudnika oblaka in se mora zanašati na varnostne kontrole, ki jih zagotavlja ponudnik. Zato je potrebno presoditi, v kolikšni meri je ponudnik sposoben izpolnjevati zahteve uporabnika glede varnosti. To se lahko preveri s postopkom upravljanja tveganj s strani tretjih oseb, pri tem pa je treba presoditi tudi, kakšne vrste ukrepov izvaja ponudnik storitve za varovanje infrastrukture in zasebnosti. Ponudnik storitve v oblaku lahko skladnost z varnostjo in zasebnostjo zagotavlja na več načinov: z oceno učinka na varstvo podatkov, s certifikatom ISO 27001, ki določa standard za pomoč podjetjem in organizacijam po vsem svetu za vzpostavitev in vzdrževanje najboljšega sistema upravljanja informacijske varnosti ali s certifikatom ISO 27018, to je mednarodni kodeks ravnanja z zaščito osebnih podatkov (angl. Personally Identifiable Information, v nadaljevanju PII) v javnih oblakih, ki deluje kot procesor PII in temelji na najboljših praksah, ki so določene v standardu ISO 27002, ter vzpostavlja nekatere nove kontrole za zasebnost podatkov v oblaku (Tolsma, brez datuma).

Uporabniki storitve v oblaku morajo tako imeti dober pregled nad podatki v infrastrukturi, vedeti, kje so podatki shranjeni, kako jih je mogoče prenesti k drugemu ponudniku in kakšne so možnosti za dostop do teh podatkov, saj je pomembno, kje se podatki nahajajo, da zadostijo veljavni zakonodaji. Najemnik storitve naj bi imel možnost preveriti, ali ponudnik zagotavlja ustrezne in zadostne varnostne ukrepe, ki so določeni v pogodbi ter da je omogočena revizija, ki je lahko dober ukrep za oceno varnostnih ukrepov (Jamšek, 2018; Informacijski pooblaščenec, 2017a; Informacijski pooblaščenec, 2017b; Evropska unija, 2016).

5 PONUDNIKI RAČUNALNIŠTVA V OBLAKU INFRASTRUKTURE KOT STORITVE

Računalništvo v oblaku se hitro širi in na trgu je vse več različnih ponudnikov storitve in tudi modelov. V magistrski nalogi se bom osredotočil predvsem na ponudnike storitve IaaS, saj se naloga navezuje na storitev oblaka infrastrukture kot storitev. Najemniki storitve uporabljajo infrastrukturo oblaka za najrazličnejše načine, tudi najkompleksnejše procese.

5.1 Tuji ponudniki

Raziskovalci pri Gartnerju redno preverjajo svetovne vodilne ponudnike storitve IaaS, kjer zanje tudi izdelajo t. i. magični kvadrant in je razdeljen na štiri kvadrante: izzivalce, vodje, nišne igralce in vizionarje (Hein, 2019).

V levem zgornjem kvadrantu se nahajajo izzivalci (angl. Challengers), ki dajejo poudarek na ponudbo infrastrukture kot storitvi, ki pa še ni točno umeščena v tržno nišo, saj je njihova vizija še nedodelana in iščejo najemnike svoje storitve.

V desnem zgornjem kvadrantu se nahajajo vodilni ponudniki storitve (angl. Leaders), ki imajo jasno opredeljene ter zastavljene cilje in tudi vizijo za razvoj v nadaljevanju. Ponujajo najboljšo in najnaprednejšo infrastrukturo in sisteme. Že več let je vodilni ponudnik storitve Amazon Web Service, v isti kvadrant pa sta se uvrstila še Microsoft in Google.

V levem spodnjem kvadrantu se nahajajo nišni igralci (angl. Niche Players). Ponudniki običajno ponujajo storitve v sodelovanju z drugimi partnerji in se osredotočajo na manjši segment poslovanja.

V desnem spodnjem kvadrantu se nahajajo vizionarji (angl. Visionaries). Njihova vizija je dodelana, vendar nimajo popolne ponudbe. Vložki ponudnika storitve so usmerjeni v prihodnost, da bodo lažje sledili zastavljeni viziji.

Kateri ponudniki se nahajajo v katerem kvadrantu, je razvidno s Slike 8, izpostavil pa bom vodilne 3.

Slika 8: Magični kvadrat za ponudnike oblaka IaaS

Vir: Prirejeno po Gartner (2019).

Amazon Web Service je na trgu že od leta 2006 in je začetnik storitve IaaS, ob tem pa je tudi največji ponudnik oblakov. Storitev IaaS ponudnika Amazon je po mnenju Gartnerja tisti ponudnik, ki naj bi bil vzgled, kako naj bi storitve v virtualnem okolju oblaka potekale. AWS je vodilni ponudnik, ki mu zaupajo milijoni strank po svetu. Širi se v več smereh, eno od ključnih področij pa je trg baz podatkov. Poleg prednosti raziskovalci opozarjajo na pomanjkljivosti in pri tem izpostavljajo ceno najema, ki se kljub znižanju cen strojne opreme še vedno ni znižala. Ker je storitev AWS vodilni ponudnik storitve v oblaku, se dogaja, da se uvajajo novitete, ki imajo v izvirniku veliko pomanjkljivosti in za zanesljivo delovanje zahtevajo veliko izboljšav in posodobitev (Targett, 2019; Dignan, 2019).

Microsoft Azure je drugi najmočnejši ponudnik za AWS in za njim zaostaja predvsem pri zagotavljanju zanesljivosti izvajanja. Uporabniki Microsoft Azura so predvsem tisti uporabniki, ki se odločijo razširiti svojo infrastrukturo z nadgradnjo svoje obstoječe Microsoftove tehnologije. Integracija z Microsoftovimi orodji za razvoj je brezhibna, prav tako tudi strojno učenje in shranjevanje podatkov. Največja težava je že omenjena zanesljivost delovanja, saj je imel ponudnik storitve v letu 2018 več incidentov z izpadom delovanja storitve in tudi zagotavljanjem ustrezne podpore uporabnikom. Veliko je Microsoft pridobil z integracijo orodij s programskimi rešitvami Dynamics 365 in Office 365 (Targett, 2019; Dignan, 2019).

Google Cloud je tretji najuspešnejši tuj ponudnik storitve infrastruktura kot storitve in je po mnenju Gartnerja dobra izbira za uporabnike, ki želijo ustvarjati aplikacije v domačem oblaku. Primeren naj bi bil predvsem za startup podjetja, saj zajema različne tehnologije na področju analitike in strojnega učenja. Uporablja inovativen odprtokodni pristop in je platforma za aplikacije, ki so osredotočene na podatke. Srečuje se s pomanjkljivostmi pri zagotavljanju stabilnosti, saj še niso razvili v celoti procesov za reševanje poslovnih računov. Pogodbe, popusti, licenciranje in integracija povzročajo uporabnikom različne preglavice, s temi pa se srečuje tudi ponudnik storitve Google prek različnih infrastrukturnih izpadov storitev. Ne glede na težave predstavlja Google Cloud dobro protiutež Microsoftu Azuru in AWS-ju, saj krepijo partnerstvo s ponudnikom SAP, kar bi lahko povzročilo večjo povezanost s tradicionalnimi podjetji (Targett, 2019; Dignan, 2019).

5.2 Domači ponudniki

Ponudba storitve IaaS v oblaku v Sloveniji je v razvoju in je v primerjavi s tujim tržiščem zelo skromna in praktično še v začetni fazi razvoja. Ponudniki razvijajo svoje različne inovativne ideje in storitve ter tako poudarjajo svojo konkurenčno prednost pred drugimi ponudniki. O tem, kateri so največji ponudniki storitve IaaS v Sloveniji, po raziskovanju različnih virov nisem odkril. Po lastni presoji bom tako izpostavil nekaj ponudnikov, za katere menim, da igrajo na slovenskem trgu relativno pomembno vlogo pri zagotavljanju oblačnih storitev.

Po podatkih avtorice (Crnkovič, 2014) prevladujeta v Sloveniji ponudbi storitev v oblaku SaaS, PaaS, medtem ko je ponudba storitev IaaS manj razširjena. Slovenski ponudniki naj bi po mnenju avtorice oblačno identiteto še iskali. Ponudniki storitev se ločijo na razvijalce in preprodajalce ter ponudnike SaaS in IaaS/PaaS. Izrazitega razvijalca do leta 2015 v Sloveniji na področju PaaS/IaaS niso opredelili, kasnejših analiz pa prek literature ni bilo zaslediti. Kljub temu pa lahko sklepamo, da se tudi na tem področju ustvarjajo rešitve, ki bodo prišle v širšo uporabo in bodo prevzeli primat med ponudniki IaaS (Crnkovič, 2014).

Izpostavljam nekaj ponudnikov, ki naj bi bili med bolj priljubljenimi v Sloveniji in prevzemajo večje deleže storitve v oblaku.

NIL je slovenski pionir računalništva v oblaku in inovator na področju virtualizacije ter podatkovnih središč oblačnih storitev. Storitve naj bi prinašala zniževanje stroškov IT in višjo prilagodljivost uporabe. Rešitev Flex IT iz ponudbe NIL HyperCenter, ki je namenjena tako javnim kot tudi zasebnim oblakom. Ponudnik storitve navaja visoko odzivnost storitve in kontinuiteto delovanja. Za storitev so pridobili tudi certifikata ISO 9001 in ISO 27001. Stroški storitve se obračunavajo na mesečni ravni najema. Ponudnik storitev NIL ponuja za najem tudi uporabo omrežnih storitev, pomoč pri zagotavljanju IT-varnosti, uporabnih orodij in svetovanje ter pomoč pri snovanju arhitekture.

Pošta Slovenije (brez datuma) PosiTa IaaS (VS) je osnovna infrastrukturna storitev v oblaku, ki temelji na partnerskem sodelovanju s podjetjem Microsoft in HPE, ki na izbiro ponuja različne operacijske sisteme, in sicer operacijski sistem Linux ali operacijski sistem Microsoft Windows. HPE Helion CloudSystem je celovita rešitev strojne in programske opreme za razvoj in upravljanje rešitev v oblaku s poudarkom na optimizaciji in pospeševanju rasti poslovanja, ki prinaša poenostavitev, pridobitev nadzora, večjo produktivnost in agilnost pri razvoju in poslovanju v oblaku s hibridnimi rešitvami v oblaku za razvoj, lansiranje in upravljanje programske opreme. Na razpolago je tudi Microsoft Azure Stack Hub, ki prinaša možnost, da se storitve poganjajo znotraj lastnega okolja, v okviru podatkovnega centra, zasebnega ali gostovalnega oblaka. Storitve se lahko poganjajo za testiranje ali produkcijo. Upravljanje je preprosto, prek nadzorne plošče, in prinaša več storitev na enem mestu. Lokacija podatkovnih centrov se nahajajo v Ljubljani in Mariboru in so fizično visoko zavarovani. Obračunavanje storitev je lahko mesečno ali po porabi na dan.

Telekom Slovenije ponuja različne storitve v oblaku, kot so: digitalna identiteta, mobilna pisarna Microsoft Office 365, e-blagajna, različni najemi storitev in aplikacij ter tudi najem strežnika. Najem prilagojenega virtualnega strežnika je možen preko različnih paketov, kjer je zagotovljena tudi tehnična podpora, možen pa je tudi začasen najem. Obračunavanje storitev je na mesečnem nivoju. Strežniki se nahajajo v varni sobi, ki je zavarovana pred požarom, potresom, poplavo in drugimi nevarnostmi. Podprta je namestitev operacijskih sistemov Windows, kot tudi ostalih odprtokodnih operacijskih sistemov.

Arnes je javni zavod, ki gradi, vzdržuje in upravlja infrastrukturo, ki povezuje univerze, inštitute, raziskovalne laboratorije, muzeje, šole, baze podatkov in digitalne knjižnice. Svojim uporabnikom nudi enake storitve kot nacionalne akademske mreže iz drugih držav, s katerimi sodeluje v projektih Evropske komisije pri testiranju, razvoju rešitev in vpeljavi novih internetnih protokolov in storitev. Opravlja tudi storitve, ki jih komercialne organizacije ne opravljajo, a so predpogoj za delovanje interneta v Sloveniji. Arnes ponuja svojim članicam na uporabo strežnik po meri, ki omogoča platformo za gostovanje strežnika. Na strežniku po meri delujeta tako operacijski sistem Windows kot tudi Linux. Lokacija strežniške infrastrukture ponudnika je v Sloveniji in je za članice organizacije brezplačna, za vzpostavitev pa je potrebno izvesti naročilo storitve, s katerim ponudnik administratorju lokalne organizacije omogoči začetek upravljanja s strežnikom po meri (Arnes, brez datuma).

V Sloveniji so prisotni še drugi različni ponudniki infrastrukture kot storitve, kot so: mojoblak.si (Optimus IT), Complete-datacenter.si (FMC Group), Domovanje.com, ingrammicrocloud.com, UNISTAR PRO, itd.

6 SELITEV TEHNOLOŠKE ARHITEKTURE V OBLAK

Priprava na selitev tehnološke arhitekture v oblak se bo izvedla v več korakih, ki so odvisni eden od drugega, in le uspešno izpeljava korakov je pogoj za uspešno izpeljan proces. Konec leta 2019 se je na Kitajskem pojavil novi koronavirus, ki se je iz meseca v mesec zelo hitro razširil po celem svetu, zaradi česar je bila razglašena svetovna pandemija SARS-CoV-2 (COVID-19), ki je v sredini marca zajela tudi Slovenijo in praktično ohromila življenje ter ustavila večino dela v klasični obliki, z delom na delovnih mestih v pisarnah podjetij, ter prisilila družbe, da praktično čez noč organizirajo delo od doma in delo na daljavo. Prav tako je močno vplivala na učni proces v izobraževalnih ustanovah, kjer so učenci, dijaki in študentje po svojih najboljših močeh začeli z delom in učenjem od doma na daljavo. Tako so se vrata osnovne šole, kjer smo imeli načrt izpeljati selitev, zaprla in ni bilo dovoljeno izvajati drugih dejavnosti, razen nujnih popravil in vzdrževanja pod strogimi varnostnimi pravili po priporočilih Nacionalnega inštituta za javno zdravje. Posledično so bili na osnovni šoli zaustavljeni vsi projekti in nadgradnje na področju omrežja kot tudi ostalega dela v šoli. Načrtovana izvedba del za posodobitev omrežja je bila načrtovana že pred marcem leta 2020, vendar je dana situacija dela zaustavila in se je gradnja omrežne infrastrukture zaustavila vse do junija 2020. Vseeno je bilo opravljenih nekaj korakov za ureditev infrastrukture v oblaku, vendar v veliko manjšem obsegu kot po prvotnem načrtu, saj ni bilo mogoče izvajati nobenega realnega testa in delovanja pripravljene infrastrukture.

Zaradi že omenjenega stanja epidemije v državi se je veliko procesov zaustavilo in še niso bili izvedeni. Želja je bila, da bi izpeljali selitev lokalne strežniške infrastrukture v strežniško infrastrukturo v oblaku. Še pred razmerami epidemije smo na šoli pripravili testno strežniško okolje pri ponudniku storitve Arnes. Vzroki za takšno odločitev organizacije bodo

utemeljeni in opisani v naslednjih poglavjih. Tako je bilo vzpostavljeno tesno okolje za podatkovni in tiskalniški strežnik, ki pa je že v fazi testiranja in ga testira manjša skupina uporabnikov v organizaciji, ki imajo različne potrebe po sami uporabi za tiskanje in podatkovni rabi strežnika. Uporaba testne infrastrukture ni na ustreznem nivoju, saj organizacija še nima urejenih in zagotovljenih hitrosti prenosa podatkov, kar posledično vpliva na odzivnost in uporabnost delovanja storitev na strežniku. Ob ustrezni nadgradnji povezave bomo dokončno testirali odzivnost okolja na storitve in sprejemali nadaljnje odločitve. Sama odzivnost je pomembna tudi pri nadaljnji vzpostavitvi strežnika za poslovno-informacijski sistem in nadaljnje oblikovanje infrastrukture.

6.1 Pregled trenutnega stanja sistema

Trenutno organizacija uporablja lokalni strežnik, na katerem delujeta dva virtualna računalnika. Ta je v uporabi že več kot 8 let, med uporabo pa so se že začele pojavljati prve težave z odpovedjo določene strojne opreme oz. predvsem diskovnega polja, ki ga rešuje redundantno polje za vzporedno delovanje. Vse bolj intenzivno organizacija razmišlja o posodobitvi infrastrukture in proučuje možnosti selitve strežnika v oblak pa tudi tehta možnosti za zamenjavo strojne opreme. Na strežniku za virtualizacijo sta urejena dva virtualna računalnika, ki se uporabljata za dva različna namena. Prvi se uporablja za podatkovni strežnik za podatke v skupni rabi ter tiskalniški strežnik (»Strežnik1«), drugi pa je namenjen administrativnemu in vodstvenemu delu organizacije za uporabo poslovnega informacijskega sistema in upravljanjem z njim (»Strežnik2«). Vsak od teh dveh navideznih računalnikov ima dodeljene računalniške vire, ki jih potrebujeta za zagotavljanje ustreznega nivoja delovanja storitev. »Strežnik1« potrebuje veliko manj računalniških virov kot »Strežnik2«, ki potrebuje za delovanje poslovnega informacijskega sistema veliko več virov. Do virtualnih naprav dostopajo različni uporabniki, ki imajo omogočene specifične uporabniške račune in pravice, ki omogočajo uporabo različnih storitev, kot so npr. samo podatki v skupni rabi, dostop do tiskalniškega strežnika in dostop do poslovno informacijskega strežnika. Obstajajo tudi še drugi uporabniški dostopi, ki so specifični glede na profil učitelja v šoli, vendar so storitve uporabnikov že zastarele in niso več v uporabi.

Sam strežnik deluje v dveh različnih omrežjih, ki sta ločeni po namembnosti za administrativno osebje in pedagoško osebje. Da sistem deluje v obeh omrežjih, ima strežnik dve mrežni kartici, ki sta povezani vsaka s svojim omrežjem in tako omogoča dostop do storitev z različnih omrežij. Uporabniki, ki se nahajajo v pedagoškem omrežju, nimajo pravice dostopati do storitev virtualnega računalnika, namenjenega za poslovno informacijski sistem, saj je ta namenjen administrativni in vodstveni uporabi.

Redundantno polje opravlja varnostno kopiranje vse vsebine v primeru izpada enega od trdih diskov računalnika. Tako imata virtualna računalnika in virtualizator za delovanje na voljo tri pare vzporednih diskov, da v primeru izpada enega, nalogo prevzame drugi. Menjava nedelujočega trdega diska v strežniku se lahko izvede v času delovanja, saj diskovno polje

omogoča odstranitev nedelujoče naprave in priklop nove delujoče, tako da se nato neopazno preslikajo podatki iz obstoječega na novi nosilec podatkov.

Za strežnik je urejeno tudi varnostno kopiranje, ki se izvaja periodično na drugo napravo, iz katere je možno pridobiti zadnje stanje podatkov ob morebitnem izpadu delovanja primarnega strežnika.

6.2 Ključni dejavniki za odločitev selitve v oblak

Sprejemu odločitve, da se strežniška infrastruktura preseli v oblak, je botrovalo več dejavnikov in jih organizacija proučuje že nekaj časa. Zavedati se je treba staranja fizičnih komponent, ki se jim življenjska doba počasi izteka in je treba imeti strategijo, v katero smer razvoja in posodobitev naj se organizacija usmerili. V zadnjih nekaj letih se je že zgodilo, da je prišlo do okvare na diskovnih pogonih v taki meri, da je bilo delovanje strežnika onemogočeno. V danem položaju je organizacija reševala podatke in uspešno popravila okvaro. Takšna okvara je povzročila ohromljenost v delovanju poslovnega in pedagoškega procesa.

Kasneje so se začele pojavljati težave z odzivnostjo strežnika, ki so bile posledica nadgradenj aplikacij in sistemskih programov. Začasno se je strežni nadgradil z delovnim pomnilnikom, vseeno pa je procesorsko še vedno šibek in se težave z neodzivnostjo še vedno dogajajo, saj zmanjka fizične procesorske moči za računanje.

Organizacija je proučevala različne možnosti, kako posodobiti strežniško infrastrukturo, na voljo pa so bile tri različne rešitve: obnovitev in posodobitev obstoječega strežnika, nakup novega strežnika in selitev v oblak. Obnovitev in posodobitev obstoječega strežnika v vsakem primeru pomeni, da bi določene komponente ostale še vedno stare, kar pa pomeni večje tveganje za odpoved delovanja. Nakup novega strežnika pomeni naložbo v novo opremo, v katero bi bili prisiljeni, če organizacija ne bi imela druge izbire. V tem primeru bi za zagotavljanje ustreznega viška računalniških virov morali investirati vsaj 4.500 EUR za nakup nove strojne opreme. Testiranje okolja v oblaku se je tako izkazalo za eno bolj premišljenih potez, saj trenutna obstoječa infrastruktura še vedno deluje, vzporedno pa je mogoče premišljeno pripravljati novost in pravočasno vzpostaviti novo infrastrukturo. Zaradi zanesljivosti delovanja in brezplačnega najema storitve se poglobljene finančne analize ni pripravilo in sprejelo odločitev za nadaljnje testiranje storitve računalništva v oblaku.

Računalništvo v oblaku je v današnjem času postalo del vsakdana, kar pomeni veliko različnih produktov, ki za delovanje uporabljajo oblačne storitve. Organizacija Arnes za šole in ostale organizacije pod svojim okriljem skrbi na več področjih, med drugim tudi za zagotavljanje brezplačne hitre optične internetne povezave. Omogočajo tudi brezplačen najem storitev strežnika po meri v oblaku, kjer dobi organizacija strežniške kapacitete za vzpostavitev lastne strežniške infrastrukture.

6.3 Opredelitev potreb

Organizacija za delovanje potrebuje storitev, ki bo zagotavljala visoko razpoložljivost delovanja. Predvsem je pomembno, da storitev brezhibno deluje v dopoldanskem času, ko se strežnik uporablja za potrebe pouka in hkrati za potrebe poslovanja ter vodenja. Samo novo okolje, kjer bo sistem deloval, naj bi bilo hitrejše in odzivnejše, kot je bilo dosedanje. Pomembna je zagotovitev varovanja podatkov pred izgubo in urejevanje ustreznih varnostnih kopij na več lokacij ter tudi vzdrževanje in tehnična podpora pri zagotavljanju storitve v primeru nastalih težav.

Finančne sposobnosti šole so pomemben dejavnik pri odločitvi, ali je investicija finančno sprejemljiva. Pri tem je še vedno pomembno, da se ne glede na stroške, odloči preudarno, četudi za dražjo investicijo, le da bo ta ustrezala in zagotavljala ustrezno delovanje različnih storitev, saj so storitve, ki jih trenutno zagotavlja strežnik, bistvenega pomena za obratovanje organizacije.

Zaradi zagotavljanja ustreznega varovanja podatkov v skladu z zakoni v Republiki Sloveniji si organizacija želi, da se v primeru selitve storitve v oblak, podatki nahajajo in hranijo v Sloveniji. Organizacija je del državne javne uprave in pri upravljanju s podatki je treba upoštevati vse zakonske predpise, ki se navezujejo na področje upravljanja in obdelovanja podatkov, s tem pa se tudi zmanjša tveganje za nastanek napak.

Ker ima organizacija na področju računalništva le enega zaposlenega, je za šolo pomembno, da ponudnik storitve zagotavlja zunanjo podporo in pomoč za upravljanje storitve.

6.4 Analiza in ocena storitve ponudnika

Po proučitvi možnosti med nadgradnjo, nakupom novega strežnika ali selitvijo v oblak je bila možnost, da bi izvedli selitev v oblak, najugodnejša rešitev. Sam način zagotavljanja storitve je sicer popolnoma različen, in sicer ali se bo ta izvajala interno ali pa se bo izvajala pri zunanjem ponudniku. Zaradi zaupanja v zagotavljanje storitev, saj ponudnik storitev Arnes zagotavlja že več drugih storitev pri delu, je šoli Arnesova ponudba strežnika po meri v oblaku najbolj ustrezala.

Za pridobitev več informacij o zagotavljanju delovanja storitve je šola najprej kontaktirala z Arnesom, kjer je pridobila informacije o sami infrastrukturi in njihovem delovanju. Ker so za začetek v ponudbi pripravljeni »paketi« računalniških virov, je bilo treba pridobiti tudi informacije o tem, če je možno in za koliko je mogoče povečati razpoložljive vire virtualnih procesorjev, delovnega pomnilnika in prostora za hranjenje podatkov.

Kot zaključek projekta si želi šola urediti celotno infrastrukturo v oblaku, zato je za dodatne informacije kontaktirala tudi ponudnika informacijskega sistema SAOP o možnostih in

delovanju njihovih aplikacij v oblaku. Poizvedelo se je tudi o možnosti vzpostavitve testnega okolja in podatkov o tem ali se na ta način informacijski sistem že uporablja.

Pomisleki so nastali pri zagotavljanju odzivnosti, saj je strežnik v primeru najema na oddaljeni lokaciji. Pojavil se je tudi pomislek pri zagotavljanju ustrezne internetne povezave. Za dostop do storitve v oblaku je treba imeti omogočeno stalno internetno povezavo, ki pa mora biti tudi dovolj hitra, da procesi tečejo normalno. Pri tem je bila glavna olajševalna okoliščina dograditev in ureditev nove še hitrejše internetne optične povezave, ki bo tako zagotavljala manjše zastoje v prometu podatkov v času, ko bo računalniško omrežje na šoli bolj obremenjeno. Negativna lastnost strežnika v oblaku je prekinjena zunanja internetna povezava, saj posledično storitev ni na voljo za delovanje. V tem primeru je možnost postavitve lokalnega strežnika v prednosti, saj so storitve dosegljive, četudi je internetna povezava prekinjena.

Pojavili so se tudi varnostni pomisleki za zagotavljanje ustrezne vernosti infrastrukture. Urediti je treba ustrezne profile z omejitvami dostopa, ti imajo podeljene pravice za uporabo, glede na vlogo pri uporabi storitev. Vsi morajo uporabljati ustrezna varnostna priporočila za zagotavljanje ustreznih varnostnih ukrepov, da ne pride do zlorabe.

Pri zagotavljanju ustreznega varnostnega kopiranja ima ponudnik storitve možnost uporabiti tudi dodatne shrambe, kjer se shranjujejo varnostne kopije sistema ter so zaščitene pred morebitnimi izgubami podatkov iz strežnika. Varnostno kopiranje je mogoče urediti tudi z oddaljene lokacije v organizacijo na napravo za arhiviranje podatkov ter ima tako šola podatke s strežnika vedno tudi pri sebi.

6.5 Potrditev storitve ponudnika in sklenitev pogodbe

Pri izbiri ponudnika in odločitvi za selitev strežnika v oblak odločitev ni bila samoumevna. Po zbiranju informacij in ponudb za nov namenski strežnik se je pokazalo, da je investicija glede na trenutne finančne zmožnosti organizacije visok zalogaj, zaupanje v storitev oblaka pa povzroča dvom v zagotavljanje ustreznega varovanja. Zbiranje informacij iz različnih virov je pretehtalo možnost, da se organizacija usmeri v storitev v oblaku in začne načrtovati projekt selitve tehnološke arhitekture v oblak. Informacije s strani Arnesa o zagotavljanju storitve oblaka po meri so presenetile s ponudbo in kakovostjo na papirju, informacije, kako bodo sistemi delovali v realnem času, pa so bili še pod vprašajem, saj šola še nima izkušenj z upravljanjem in delom v oblaku na tem nivoju storitev. Pomembna informacija, ki jo je šola dobila, je prišla s strani ponudnika informacijskega sistema SAOP, ko so sporočili, da organizacije na ta način storitev strežnika v oblaku že uporabljajo in je po njihovih izkušnjah delovanje sistema zadovoljivo in stabilno. To je bila ključna informacija, da se nadaljujejo priprave za selitev v storitev Arnesa.

Urejanje pristopne pogodbe je za organizacije, ki že uporabljajo storitve Arnes, poenostavljeno in se uredi prek namenskega portala. Ureditev je preprosta in hitro urejena,

vseeno pa je možno storitev naročiti prek klasičnega načina z uporabo predpripravljenega obrazca, ki ga organizacija izpolni in posreduje. Naročilo izvede odgovorna oseba ali pooblaščenec, ki odda vlogo z uporabo uporabniškega imena in gesla, ki ga odgovorni že uporablja za urejanje drugih Arnesovih storitev. Po uspešno izpeljanem postopku dobi naročnik za uporabo »osnovni paket« strežniških virov. Za povečanje osnovne kvote je treba posebej zaprositi, ta pa mora biti ustrezno argumentirana. Ker je osnovni paket virov za delovanje strežnika na osnovi operacijskega sistema Windows komaj zadosten za delovanje osnovnega programskega paketa, je organizacija, takoj po uspešni sklenitvi pogodbe, zaprosila za povečanje kvote, ki bo ustrezala potrebam za tekoče delovanje strežnika v oblaku. Ker je bila argumentacija s strani šole ustrezno podana, je Arnes prošnjo uspešno sprejel in povečal količine, s tem pa je bila realizacija za vzpostavitev testnega okolja korak bližje izvedbi.

6.6 Priprava za prehod v okolje oblaka, prilagajanje in testiranje

Sistem za ustvarjanje strežnika po meri je prilagojen uporabnikom različnega računalniškega predznanja, saj bodo lahko tudi tisti s šibkejšim znanjem in z malo pomoči uredili virtualni strežnik v oblaku. Da uporabnik sploh lahko začne pripravljati strežniško okolje, je treba imeti urejeno ustrezno uporabniško ime in geslo z omogočenimi pravicami, prek katerega se prijavi na portal. Ta je namenjen upravljanju s strežnikom v oblaku in ustvarjanju novih virtualnih računalnikov. Glede na dogovor s ponudnikom storitve ima šola omogočeno večjo kvoto za začetne potrebe testiranja, delovnega pomnilnika in število procesorjev.

Koraki izdelave in vzpostavitve delujočega virtualnega strežnika za izmenjavo podatkov in tiskanje:

- *Opredelitev virov za potrebe strežnika*. Dodeljene vire strežnik potrebuje za delovanje strežniške infrastrukture. Ob tem je treba predvideti maksimalno količino virov, ki jih bodo sistemi potrebovali, da bo zagotovljeno optimalno delovanje. Kasneje, seveda, če so ti na razpolago, se jih lahko dodatno dodeljuje in ureja.

- *Potrditev in kreiranje virtualnega strežnika*. S potrditvijo, ob ustvarjanju virtualnega strežnika, se za to virtualno napravo rezervirajo kvote računalniških virov, ki so na voljo za uporabo le tej virtualni napravi za delovanje. Tako je ustvarjen virtualni računalnik s pred nastavljenimi specifikacijami.

- *Zagon virtualnega strežnika in namestitev operacijskega sistema*. Pred zagonom virtualnega strežnika ima sistem strežnika po meri pred pripravljene različne operacijske sisteme, ki so na voljo za namestitev. V primeru, da ni željene serije programske opreme na voljo, je le to mogoče tudi še dodatno namestiti, vendar je pred tem treba kontaktirati Arnes, ki lahko omogoči dodatne različice osnovnega operacijskega sistema. Šola je za svoje potrebe namestila operacijski sistem Windows Server, ki je že omogočen v naboru za izbor in ga je uporabljala tudi že do sedaj na lokalnem strežniku. Nameščanje

operacijskega sistema se začne po potrditvi programske opreme in vklopu virtualne naprave. Sama namestitev poteka na enak način kot poteka na ostalih napravah, bodisi na strežniku, bodisi na osebnem računalniku. Vse skupaj lahko uporabnik administrator upravlja in spremlja prek konzole strežnika po meri, saj v času nameščanja še ni mogoč oddaljen dostop do programske opreme.

- *Ureditev dostopa do virtualnega strežnika.* Kot je bilo že omenjeno, se namestitev opravi prek konzole v spletnem brskalniku. Njeno delovanje je zagotovljeno na Strežniku po meri s pomočjo Javascripta, ki pa je počasno in povzroča časovne zamike pri prikazovanju slike sistema. Tudi zaradi boljšega in odzivnega delovanje je zato priporočljivo čim prej urediti in omogočiti oddaljeni dostop do strežnika. Tega se opravi s programom za dostop do oddaljenega namizja, ki je že vključen v zbirki programov operacijskega sistema Windows. Da pa to deluje, je treba omogočiti takšen način delovanja operacijskega sistema ter ureditev IP-naslova računalnika in ureditev ustreznih uporabniških pravic, ki omogočajo uporabo računalnika na daljavo. Ko so nastavitve urejene, se lahko na strežnik prijavi z uporabo programa oddaljenega namizja. Na računalniku, s katerim želimo dostopati, odpremo program oddaljenega namizja in se prijavimo na virtualni strežnik z uporabo IP-naslova in ustreznega uporabniškega imena. S tem programom oddaljeni dostop ne deluje več prek Javascripta in odzivnost virtualnega strežnika je v realnem času.

- *Konfiguracija strežnika: posodobitve, aplikacije, uporabniki, zaščita pred vdori in požarni zid.* Sledi urejanje virtualnega strežnika. Poskrbeti je treba za posodobitve operacijskega sistema, ki z zadnjimi varnostnimi paketi odpravljajo ranljivost sistema. Ker deluje virtualizator Strežnik po meri v ozadju na osnovi na operacijskega sistema Linux, je treba za ustrezno delovanje namestiti še dodatne komponente in gonilnike, ki jih je pripravil ponudnik storitve Arnes. Oblikovati je treba uporabnike, podatkovne mape za skupno rabo in urediti aplikacije, ki jih strežnik potrebuje. Namestiti je treba protivirusno zaščito in urediti požarni zid za preprečevanje nepooblaščenih vstopov do strežnika.

Najprej se je šola odločila za kreiranje strežnika za izmenjavo podatkov in tiskanje. Za dostop do podatkov v skupni rabi je urejenih več uporabniških računov, ki pomenijo nivoje in imajo dostope do različnih map in možnost medsebojne izmenjave. Namenjeni so uporabnikom glede na profil uporabe, ali je ta namenjen pedagoškim ali administrativnim in vodstvenim delavcem, saj se narava teh podatkov zelo razlikuje in je pomembno, da so med seboj ločeni.

Konfiguracija virtualnega računalnika za deljenje tiskalnikov v skupni rabi je pripravljena tako, da je ustvarjen uporabniški dostop, prek katerega uporabniki pridobijo pravice za namestitev in povezavo do naprave. Uporabnik opravi namestitev tiskalnika na lokalni računalnik, da se poveže na strežnik s pomočjo IP-naslova strežnika. Ko se uspešno poveže, si »z dvoklikom« namesti povezavo in gonilnik tiskalnika na lokalni računalnik, ki ga želi uporabljati. Da pa se lahko uporabnik poveže na tiskalnik, ki je dosegljiv v internetnem omrežju, je treba poskrbeti za ustrezne namestitve tiskalnikov na strežnik in zagotoviti

ustrezne gonilnike za računalnike uporabnikov. Namestitev mora biti urejena tako, da omogoča skupno rabo in določene pravice, kateri uporabniški računi lahko dostopajo do naprave in imajo s tem omogočeno namestitev in tiskanje dokumentov.

Takoj ob uvedbi testnega tiskalniškega strežnika je bila pozornost usmerjena na to, da lahko do naprav dostopajo in jih uporabljajo uporabniki iz različnih omrežij, ki so na voljo v organizaciji. Pri tem je bilo tudi pomembno, da obstaja omejitev, ki ne bo omogočala vsesplošnega prostega dostopa, da ne bi prišlo do zlorabe pri uporabi naprav. Strežnik je v javnem omrežju in če ni določenih omejitev, lahko do virtualnega računalnika dostopa kdorkoli, kar pa lahko na daljavo v organizaciji povzroči nemalo nevšečnosti, zato je treba omejiti dostop na organizacijo in IP-naslove, ki pripadajo podomrežjem znotraj ustanove. Še bolj pomembno je, da do podatkov ne morejo dostopati uporabniki v primeru podatkovnega strežnika, saj bi to pomenilo veliko tveganje za zlorabo in krajo podatkov na strežniku za izmenjavo. Naprava naj bi bila po politiki uporabe namenjena izključno interni uporabi znotraj organizacije za hitro izmenjavo podatkov ali hranjenje manj občutljivih podatkov.

Testiranje virtualnega strežnika traja že od februarja 2020 in do konca junija 2020, z manjšim številom uporabnikov, ki za potrebe testiranja tiskajo dokumente prek strežnika v oblaku. Testiranje odzivnosti tiskanja v oblaku se izvaja tako, da se preizkuša tiskati različno zahtevne in obsežne dokumente, tudi iz različnih aplikacij ali programov, ter se primerja odzivnost tiskanja v primeru, ko se izvede tiskanje z uporabo lokalnega strežnika in primerja z uporabo strežniškega tiskalnika. Vzrok za tako dolgo časovno obdobje je posledica koronavirusa v Sloveniji, saj je bil šola zaprta skoraj tri mesece in nihče ni uporabljal strežnika niti za tiskanje niti za izmenjavo ali hranjenje datotek. V začetku junija, ob vrnitvi zaposlenih in šolarjev k pouku, pa izvedbe obsežnejšega testiranja ni bilo mogoče izvesti zaradi prezasedenosti učiteljev, ter tako niso mogli preizkušali storitev tiskanja v novi preobleki.

Uporabniki so imeli za zdaj le manjše pripombe, ki so se navezovale na poimenovanje naprave. Preimenovati je bilo treba naprave, da bi bile bolj očitno prepoznavne.

Testiranje strežnika za izmenjavo datotek še ni bilo izvedeno med uporabniki, saj je še pred začetkom uporabe prišlo do prekinitve izvajanja pouka v organizaciji, tako da so bile z začetkom pouka na daljavo vse načrtovanje dejavnosti preklicane.

6.7 Načrt za prihodnost

V načrtu za prihodnost so različna opravila, ki bodo opisana skozi naslednja podpoglavja. Zaradi razmer v organizaciji je treba izvesti še obsežnejše testiranje za tiskalniški strežnik, preizkusiti delovanje podatkovnega strežnika za izmenjavo datotek, vpeljati sistem v uporabo in izvesti izklop stare storitve. Nato sledi še zahtevnejši del selitve, ki se navezuje na poslovno-informacijski sistem šole, ki potrebuje neodvisni virtualni računalnik, testiranje

delovanja, prenos podatkov in zagon v živo, priprava navodil za uporabo, obveščanje in izobraževanje uporabnikov ter skrb za vzdrževanje in podporo.

6.7.1 Priprava dodatnega strežnika, testiranje in selitev

Naslednji korak bo priprava novega samostojnega virtualnega računalnika, ki bo namenjen poslovno-informacijskemu sistemu šole. Treba bo poskrbeti za vse že opisane postopke, tako pri strežniku za tiskanje kot podatkovnemu strežniku. Poskrbeti bo treba za ustrezne nastavitve, pravice do uporabe in tudi omejitve dostopa. Predhodno pa je treba poskrbeti, da bo namenski virtualni računalnik imel dovolj virov za zagotavljanje ustreznega delovanja poslovno-informacijskega sistema. Zagotavljati mora dovolj delovnega spomina in diskovnih kapacitet za obdelovanje ter hranjenje podatkov.

Ko bodo izpolnjeni vsi pogoji za delovanje programa, je na vrsti vzpostavitev testnega okolja, kjer se bo preverjala odzivnost delovanja v primerjavi z lokalnim strežnikom, in sicer najprej z manjšo podatkovno bazo, kasneje pa na obsežnejših podatkih, da bo lahko pridobljeno realno stanje delovanja programa. V primeru uspešno izpeljanega testnega obdobja je na vrsti selitev podatkovne baze in vzpostavitev delovanja s pravimi podatki, kjer pa je prav tako pomembno, da se preizkusi delovanje in uredi celoten sistem za optimalno delovanje. Po uspešni selitvi bo treba preurediti vse dostope uporabnikom, ki uporabljajo ta sistem. Izklop starega lokalnega strežnika z nameščenim poslovnim informacijskim sistemom se bo lahko zgodil šele takrat, ko bodo v šoli prepričani, da vse deluje, kot je bilo predvideno, in ne bodo potrebovali več nobene interakcije z lokalnim strežnikom.

Poskrbeti bo treba tudi za dodatni prostor in ustrezno arhiviranje podatkov. Za samo arhiviranje je smiselno, da se uredi na vsaj dva načina. Najprej bo izvedeno samo arhiviranje podatkovnih baz poslovno-informacijskega sistema, da bodo podatki varno shranjeni na drugi lokaciji in zaščiteni pred izgubo, sledil bo še drugi način arhiviranje celotnega virtualnega računalnika, prav tako na oddaljeno lokacijo. S tem se v primeru izpada zagotovi varnostna kopija celotnega sistema, ki omogoča, da se lahko z zadnjo varnostno kopijo na relativno preprost način zagotovi obnovitev vseh nastavitev računalnika, za primer okvare operacijskega sistema ali ob morebitnem virusnem napadu na računalniško infrastrukturo.

Glavno vlogo pri celotni odzivnosti v upravljanju virtualnih naprav nosi hitra in odzivna internetna povezava, ki jo bo treba še pred vsemi zaključnimi testiranji urediti, saj bosta v primeru nestabilne in počasne internetne povezave strežnika v oblaku še bolj neodzivna, kot bi bila sicer in ne bosta prinašala želenih rezultatov.

6.7.2 Obveščanje in izobraževanje uporabnikov

Obveščanje in izobraževanje uporabnikov je naslednji korak za vzpostavitev novega okolja. Ko bo delovanje strežnika v oblaku omogočalo uporabo sistema v taki meri, da bo to

delovalo nemoteno, se bo začel postopek obveščanja uporabnikov o prenovljeni storitvi. Pozvani bodo k preklopu na nov način uporabe, hkrati pa bo določen tudi rok, do kdaj bodo stare storitve še na voljo.

Za uporabo prenovljenega načina bo treba pripraviti navodila, ki bodo opisala postopke, da se bodo lahko uporabniki povezali do prenovljenih storitev in tudi navodila, kako stare povezave odstraniti.

Obveščanje uporabnikov bo potekalo v več korakih, da bodo zagotovo ustrezno seznanjeni o pridobitni novega sistema:

- *Obveščanje preko elektronske pošte.* Najprej bodo uporabniki obveščeni prek elektronske pošte, da je na voljo prenovljena storitev, v katero se lahko povežejo s priloženimi navodili. Navodila bodo morala biti ločeno pripravljena za uporabnike, ki bodo uporabljali tiskalniški in podatkovni strežnik, ter ločeno za poslovno-informacijski sistem.

- *Predstavitev prenovljene storitve in delovanje, prednosti in vzroki za spremembe*. Po krajšem časovnem obdobju, največ teden dni, pa je predvidena predstavitev prenovljene storitve in delovanja ter tudi prednosti in vzroki, zakaj se je organizacija usmerila v novo storitev. Ob tej priložnosti bo tudi prikazan postopek za uporabnike, ki so imeli ob prehodu morebitne težave, da jih odpravijo in se uspešno povežejo v prenovljene storitve.

- *Preverjanje delovanja pri uporabnikih in odprava morebitnih težav uporabnikov*. Kasneje je načrtovano preverjanje delovanja in uporabe po uporabnikih in morebitnih težavah, ter da se te odpravijo.

- *Individualna izobraževanja in svetovanje.* Ker pa uporabljajo uporabniki različne naprave, se pričakuje, da bo treba uporabnikom omogočiti tudi individualno izobraževanje in svetovanje, saj so ti različnega računalniškega predznanja in razumevanja okolja, pri nekaterih pa tudi strah pred možnostjo, da bi s postopkom povzročili okvaro v računalniškem sistemu. Z individualno pomočjo se bodo tako odpravile morebitne posameznikove težave pri uporabi storitev.

Pomembno je tudi, da bodo uporabniki takoj ob vpeljavi nove infrastrukture obveščeni o prehodnem časovnem obdobju ter tudi o tem, kdaj bo stara strežniška infrastruktura prenehala delovati. S tem imajo uporabniki dovolj časa, da se prilagodijo uporabi novih storitev in sprejmejo nov način uporabe in delovanja pri uporabi z delom na računalniku.

6.7.3 Vzdrževanje in podpora

Za potrebe vzdrževanja bo treba zaradi samostojnega operacijskega sistema v celoti poskrbeti za ustrezno posodobitev in nadgradnjo vseh programov in aplikacij, ki bodo tekle na virtualnem strežniku. Pozornost bo potrebno usmeriti tudi v sisteme, ki bodo zahtevali ustrezno kompleksnost dostopov, saj se s tem oteži različnim napadalcem, da si prilastijo

podatke o uporabniških računih za vstop do strežnika. Treba bo poskrbeti, da se bodo gesla uporabnikov redno menjavala, saj se s tem poveča odpornost sistema proti vdorom.

Varnostne kopije podatkov poslovno-informacijskega sistema in na sploh virtualnih računalnikov bo potrebno redno shranjevati in hraniti več revizijskih izvodov za primere, ko pride do izgube ali poškodovanja osnovnega sistema. Te varnostne kopije se morajo hraniti na neodvisni lokaciji, ki ni povezana z lokacijo strežnika, saj je v primeru nesreče manjša verjetnost, da bi bili lahko vsi podatki hkrati uničeni.

Obsežnost uporabe obeh virtualnih strežnikov zajema skupaj do osemdeset uporabnikov. Tiskalniški strežnik bodo uporabljali vsi uporabniki, ki bodo potrebovali tiskalnike, strežnik s poslovno-informacijskim sistemom pa le vodstvo in uprava šole. Vsi uporabniki bodo imeli poleg pripravljenih navodil, kako v osnovi vzpostaviti povezavo s pomočjo pisnih navodil, v šoli na voljo skrbnika sistema, ki bo poskrbel, da bo delovanje infrastrukture potekalo kar se le da nemoteno in tekoče. V primeru težav bo skrbnik sistema na šoli prvi, ki bo začel odpravljati težave na sami strežniški infrastrukturi, na nivoju višje pa bo lahko zaprosil za dodatno pomoč pri ponudniku storitve v oblaku Arnes ali pa pri ponudniku programske rešitve SAOP za težave v zvezi z njihovim programom. Težave bo administrator reševal po različnih komunikacijskih kanalih, in sicer v živo, po telefonu, prek elektronske pošte ali s pomočjo programov oddaljene pomoči. Na enak način bo stopil v kontakt za zunanjo pomočjo, ki jo nudijo ponudniki storitev, saj vsak odgovorni najbolje pozna svoje storitve in najhitreje odpravlja težave.

SKLEP

V današnjem času je uporaba storitev v oblaku možna alternativa, ki lahko nadomešča obstoječe lokalne strežnike. Pred tem je treba storitev proučiti in analizirati kot ob vsaki investicijski odločitvi, povezani z informacijsko tehnologijo. Osredotočanje je le še vprašanje vsebine in cene storitve ter izvedljivosti prehoda v njihovo uporabo (Varga, 2017). V primeru, da je oblačna rešitev bolj primerna oz. ugodna, tako ni več zadržkov za selitev. Pri tem vseeno nastanejo težave s skladnostjo s platformo, ki jo organizacija najema ter je potrebno prilagajanje novim pogojem delovanja in usklajevanje z možnostmi, ki jih ponuja rešitev v oblaku.

Migracije je mogoče izvesti na različne načine, avtorja (Dukarić & Jurič, 2011) predlagata svoj pristop, ki v grobem predvideva fazo raziskave, preizkusa in izvedbe. Podprocesi prvega koraka so izbira ponudnika, analiza trenutnega stanja ter načrtovanje. V drugem koraku je na vrsti evalvacija stroškov, varnosti, zakonodaje in tehničnih lastnosti, ter izdelava pilotnega testnega projekta, kjer se v oblaku testira aplikacije, ki morajo ustreznosti karakteristikam tehnološke arhitekture. V tretjem koraku so opredeljeni postopki migracije podatkov v oblak, migracija aplikacij in optimizacija za izboljšanje delovanje sistema in

zmanjšanja stroškov (Dukarić & Jurič, 2011). Omenjeni koraki so bili tudi v veliko oporo, ko smo se v šoli odločali in urejali vse v zvezi s selitvijo tehnološke infrastrukture v oblak.

V današnjem času pretehtajo prednosti računalništva v oblaku pred slabostmi, ko se odločamo o selitvi storitve v oblak. Storitev v oblaku in konkurenčni trg je ponudnike storitve prisilila do so negativne lastnosti računalništva v oblaku, kar se le da minimalne. Še vedno pa ostaja ena od glavnih negativnih lastnosti računalništva v oblaku to, da je tehnologija odvisna od internetne povezave. Poleg tega je treba biti vedno pozoren tudi na zagotavljanje ustrezne varnosti.

Pri storitvi oblaka infrastruktura kot storitev ima uporabnik na voljo za uporabo navidezni računalnik, ki ga v celoti upravlja sam, ponudnik storitve pa mu zagotavlja računalniško infrastrukturo. Da lahko ponudnik storitve zagotavlja ustrezne kapacitete, mora imeti njegova infrastruktura dovolj fizičnih virov, ki se zagotavljajo za virtualne vire. Oblak infrastruktura kot storitev je sestavljen iz dveh glavnih plasti, to sta fizična in navidezna. Prva je najnižja in zajema strojno opremo, druga pa upravlja s fizičnimi viri, ki jih virtualno dodeljuje in nadzira za nadaljnjo uporabo (Chawkia, Ahmed & Zakariaea, 2018).

Omenjena ustrezna varnost se navezuje na ponudnika kot tudi najemnika storitve. Oba morata upoštevati varnostne zahteve, da je možna ranljivost storitev minimalna. Pri tem si mora vsak pri sebi zastaviti določena varnostna vprašanja, ki se navezujejo na ustrezno zaščito podatkov pred nepooblaščenimi dostopi do informacij ali vsebine. Za boljše zagotavljanje varnosti je treba poznati morebitne grožnje, ki nas kot uporabnike storitve lahko najbolj ogrožajo in v skladu s tem proučiti dodatne možnosti za zagotavljanje ustrezne varnosti. Ker je varnostnih nastavitev veliko, obstajajo različni varnostni seznami za preverjanje zagotavljanja ustreznih varnostnih mehanizmov in protokolov ter tudi upoštevanja predpisov o varovanju osebnih podatkov.

Na trgu so različni ponudniki storitev v oblaku, vendar se je šola odločila za storitev v oblaku organizacije Arnes, ki je javni zavod in zagotavlja omrežne storitve organizacijam s področja raziskovanja, izobraževanja in kulture ter omogoča njihovo povezovanje in medsebojno sodelovanje ter sodelovanje s sorodnimi organizacijami v tujini. Prek zavoda ima šola zagotovljeno brezplačno uporabo storitve računalništva v oblaku s polno podporo pomoči, glavna prednost pred ostalimi ponudniki pa je brezplačnost in visoka zanesljivost delovanja.

Šola je vključena v projekt, kjer se posodablja in gradi internetna infrastruktura, ki bo izboljšala delovanje internetne povezljivosti. Ker bodo nove hitrosti internetne povezave občutno hitrejše, je namen to izkoristiti s tehnologijo storitve v oblaku. Uporaba najema strežnika v oblaku pri Arnesu bo tako lahko nadomestila starejši strežnik, na katerem tečejo storitve za poslovno-informacijski sistem, tiskalniški strežnik in tudi strežnik za izmenjavo podatkov. Na strežniku so se že začele pojavljati prve odpovedi strojne opreme, ki se je do sedaj uspešno servisirala, ob enem pa se je začela proučevati možnosti za zamenjavo. Selitev strežnika v oblak v času, ko strežnik še deluje, ob enem pa se pripravlja novo okolje, kot

kažejo trenutne ugotovitve, ko so postopki še v fazi testiranja, bo privarčevala na investicijskih stroških za novo strežniško opremo, saj se predvideva, da bodo vsi procesi v oblaku lahko nadomestili trenutno lokalno infrastrukturo. Preden se bodo lahko začele uporabljati vse storitve, je treba opraviti še zaključna dela na internetni infrastrukturi ter uspešno zaključiti testiranja tiskalniškega in podatkovnega strežnika. Dela trajajo že od začetka leta 2020, saj je izvedbo preprečila prisotnost koronavirusa, kar je zaustavilo vsa opravila in tako je posledično preloženo dokončanje za vsaj šest mesecev.

V nadaljevanju je predvidena postavitev strežniškega okolja za poslovno-informacijski sistem, ki ga je treba obsežno testirati in proučiti možnosti za optimizacijo delovanja. Ob uspešno izvedenem testiranju je planirana selitev, predstavitev prenovljene storitve ter izobraževanje za uporabo prenovljene storitve. Čez čas bo treba na strežnikih v oblaku upravljati storitve posodabljanja programske opreme in vzdrževati visoke standarde zagotavljanja varnosti. Za potrebe zagotavljanja podpore uporabnikom bo na voljo v šoli administrator, ki bo skrbel za nemoteno delovanje storitev. V primeru večjih težav se bo ta obrnil po dodatno pomoč na ponudnika storitve v oblaku Arnes ali za bolj tehnično programsko pomoč, ki se navezuje na poslovno-informacijski sistem, na administratorje ponudnika SAOP.

Koronavirus je organizacije prisilil v vse večjo uporabo računalništva v oblaku. V objavi prispevka (MarketWatch, 2020) navajajo, da so v času koronavirusa v porastu transakcije za rešitve gostovanja v oblaku, ki so razširljive in ne motijo poslovanja. Organizacijam izboljšujejo sposobnost preučevanja podatkov, povečujejo odzivnosti in tudi produktivnosti dela. Storitve v oblaku so ene od ključnih za uporabnike, ki delajo na daljavo, saj imajo zaposleni na voljo večino orodij za nemoteno izvajanje dejavnosti. Računalništvo v oblaku je v pomoč tudi pri podpori telemedicine, saj postaja dostop do zdravnikov in zdravstvenih delavcev na daljavo vse pomembnejši. Potreba po računalništvu v oblaku je postala ob izbruhu virusa še očitnejša, saj podjetja niso mogla izvajati dejavnosti brez rešitev v oblaku, integracija oblačnih rešitev pa je omogočila in zagotovila stabilnost spletnih platform in storitev.

LITERATURA IN VIRI

1. AbacusNext. (brez datuma). *What's the Difference between Public, Private, Hybrid, and Community Clouds?* [objava na blogu]. Pridobljeno 25. maja 2020 iz https://www.abacusnext.com/blog/whats-difference-between-public-private-hybrid-and-community-clouds/
2. Abu Saed, K., Aziz, N., Jadid Abdulkadir, S., Hafizah Hassan, N. & A Aziz, I. (2018). Data Governance Cloud Security Checklist at Infrastructure as a Service (IaaS). *(IJACSA) International Journal of Advanced Computer Science and Applications*, *9*(10), 279-306.
3. Aleem, A. & Sprott, C. R. (2013). Let me in the cloud: analysis of the benefit and risk assessment of cloud platform. *Journal of Financial Crime, Emerald*, *20*(1), 6-24.

4. Anisetti Marco, A. A. (2019). Cost-effective deployment of certified cloud composite services. *Journal of Parallel and Distributed Computing, 135*(2020), 203-218.
5. Anthony D., J., Božič, G., Mešić, J., Porenta, J., Tomšič, A. & drugi. (2011). Kaj nam prinaša računalništvo v oblaku? Zbornik člankov. *Konferenca Arnes 2011.* Kranjska gora: Arnes.
6. Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., . . . Zaharia, M. (2009, 10. februar). *Above the Clouds: A Berkeley View of Cloud*. California: Electrical Engineering and Computer Sciences University of California at Berkeley
7. Arnes. (brez datuma). *Strežnik po meri*. Pridobljeno 8. junija 2020 iz https://www.arnes.si/storitve/splet-posta-strezniki/streznik-po-meri/
8. Barrett, D. & Kipper, G. (2010). Cloud Computing Service. V *Virtualization and Forensics 1. izd.* Rockland, Massachusetts: Syngress.
9. bcs - The Chartered Institute fo IR. (2019, 19. marec). *History of the cloud*. Pridobljeno 5. maja 2020 iz https://www.bcs.org/content-hub/history-of-the-cloud/
10. Boulton, C. (2018, 25. september). CIO. *What is XaaS? A way to inject agility into your digital business*. Pridobljeno 25. maja 2020 iz https://www.cio.com/article/3308418/what-is-xaas-a-way-to-inject-agility-into-your-digital-business.html
11. Božič, G. (2011). Ali je kaj trden vaš oblak? *Konferenca Arnes* (str. 9-10). Kranjska gora: Arnes.
12. Catteddu, D. & Hogben, G. (2009). *Cloud Computing: Benefits, risks and recommendations for information security.* ENISA.
13. Chan, M. (2017). *How to calculate the true cost of migrating to the cloud.* NetworkWorld. Pridobljeno 28. januarja 2020 iz https://www.networkworld.com/article/3164444/how-to-calculate-the-true-cost-of-migrating-to-the-cloud.html
14. Chang, Y.-W., Hsu, P.-Y., Huang, S.-H. & Chen, J. (2019). Determinants of switching intention to cloud computing in large enterprises. *Data Technologies and Applications, Emerald, 54*(1), 16-33.
15. Chawkia, E. B., Ahmed, A. & Zakariaea, T. (2018). IaaS Cloud Model Security Issues on Behalf Cloud Provider and User Security Behaviors. *Procedia Computer Science 134*(2018), 328-333.
16. Cloud Flare. (brez datuma). *What Is Cloud Migration? | Cloud Migration Strategy.* Pridobljeno 25. januarja 2020 iz https://www.cloudflare.com/learning/cloud/what-is-cloud-migration/
17. Cloud Security Alliance. (2011). *SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V3.0.* Seattle, Washington: Cloud Security Alliance.
18. Cook, J. (2019). Cloud Academy. *Cloud Migration Risks & Benefits* [objava na blogu]. Pridobljeno 25. januarja 2020 iz https://cloudacademy.com/blog/cloud-migration-benefits-risks/

19. Crnkovič, M. (november 2014). *Analiza slovenskega trga ponudnikov storitev v oblaku za podjetja.* Pridobljeno 5. junija 2020 iz https://www.slideshare.net/masacrnkovic/storitve-v-oblaku-masa-crnkovic
20. David, L. (2017). InfoWorld. *Calculate your cloud costs with this simple formula.* Pridobljeno 23. januarja 2020 iz https://www.infoworld.com/article/3182492/calculate-your-cloud-costs-with-this-simple-formula.html
21. Dečman, M. & Vintar, M. (2013). A possible solution for digital preservation of e-government. *Aslib Proceedings: New Information Perspectives, 65*(4), 406-424.
22. Dignan, L. (2019, 18. julij). *Google Cloud gains in Gartner's 2019 cloud infrastructure Magic Quadrant*. Pridobljeno 1. junija 2020 iz https://www.zdnet.com/article/google-cloud-gains-in-gartners-2019-cloud-infrastructure-magic-quadrant/
23. Doherty, E., Carcary, M. & Conway, G. (2015). Migrating to the cloud. *Journal of Small Business and Enterprise Development, Emerald*, 512-527.
24. Dolenc, T. (2019). Osebni podatki in njihova obdelava v omrežju Arnes. *Mreža znanja 2019.* Ljubljana: Arnes.
25. Dukarić, R. & Jurič, M. B. (2011). Migracija obstoječih aplikacij na platforme za računalništvo v oblaku. *Uporabna informatika, 19*(3), 136-146.
26. Evropska unija. (4. maj 2016). *UREDBA (EU) 2016/679 EVROPSKEGA PARLAMENTA IN SVETA*. Pridobljeno 25. maj 2020 iz EUR-Lex: https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX%3A32016R0679
27. Flat World Solutions. (brez datuma). *CLOUD MIGRATION - ADVANTAGES, DISADVANTAGES, AND HOW TO MITIGATE RISKS.* Pridobljeno 14. januarja 2020 iz https://www.flatworldsolutions.com/IT-services/articles/cloud-migration-advantages-disadvantages-risk-mitigation.php
28. Flisar, J. & Hölbl, M. (2014). Varovanje podatkov v storitvi. *Uporabna informatika, 22*(1), 38-47.
29. Grohar, M., Ciglarič, M., Pančur, M. & Horvat, M. (maj 2013). Gradivo za pristop k izpitu za pridobitev certifikata »Certified Cloud Computing Engineer«. Pridobljeno 20. maj 2020 iz https://www.slideshare.net/kcdemo/test-30335793
30. Pardeshia, V. H. (2014). Cloud Computing for Higher Education Institutes: Architecture, Strategy and Recommendations for Effective Adaptation. *Procedia Economics and Finance 11*, 589-599.
31. H´eder, M., Bisztray, F., Lakatos, G., Malasits, G., Ormos, P., Prunk-´Eger, E., . . . Rig, E. (2016). *Security checklist for IaaS cloud deployments*. ResearchGate.
32. Han, Y. (2012). IaaS cloud computing services for libraries: cloud storage and virtual machines. *OCLC Systems & Services: International digital library perspectives, 29*(2), 87-100.
33. Harr, P. (2019). How To Migrate To The Cloud With Ease In 2019. *Forbes*. Pridobljeno 26. januarja 2020 iz

https://www.forbes.com/sites/forbestechcouncil/2019/03/05/how-to-migrate-to-the-cloud-with-ease-in-2019/#11c0f5663c91

34. Heder, M., Bisztray, F., Lakatos, G., Lakatos, G., Ormos, P., Prunk-Eger, E., . . . Rigo, E. (8. marec 2016). *Security checklist for IaaS cloud deployments*. ResearchGate.
35. Hein, D. (2019, 4. marec). *What's Changed: Gartner's 2019 Magic Quadrant for Public Cloud Infrastructure Professional and Managed Services, Worldwide*. Pridobljeno 1. junija 2020 iz https://solutionsreview.com/cloud-platforms/whats-changed-gartners-2019-magic-quadrant-for-public-cloud-infrastructure-professional-and-managed-services-worldwide/
36. Hoopes, M., Bogel, R., Sunga, A., Kocis, E. & Nicu, D. (brez datuma). *History of Cloud Computing*. Pridobljeno 5. maja 2020 iz https://cloudcomputing521.wordpress.com/2017/05/01/history-of-cloud-computing/
37. Hugos, M. & Hulitzky, D. (2011). *Business in the Cloud.* Canada: John Wiley & Sons, Inc.
38. Informacijski pooblaščenec. (2017a, 14. september). *KAJ MORAMO GLEDE GDPR STORITI SEDAJ? TOP 10*. Pridobljeno 28. maja 2020 iz https://www.ip-rs.si/fileadmin/user_upload/Pdf/GDPR/GDPR_TOP10_14sep2017.pdf
39. Informacijski pooblaščenec. (2017b, 25. maj). *Kaj prinaša nova Splošna uredba (EU) o varstvu podatkov?* Pridobljeno 28. maja 2020 iz https://www.ip-rs.si/fileadmin/user_upload/Pdf/pripombe/Splosna_uredba_o_varstvu_podatkov-letak_maj_2017.pdf
40. InfoWorld & Knorr, E. (2018). InfoWorld. *What is cloud computing? Everything you need to know now.* Pridobljeno 5. maja 2020 iz https://www.infoworld.com/article/2683784/what-is-cloud-computing.html
41. Jamcracker. (2020, 29. januar). *What are the Features and Characteristics of Software as a Service (SaaS)?* [objava na blogu]. Pridobljeno 20. maj 2020 iz https://www.jamcracker.com/blogs/features-characteristics-software-as-a-service-saas
42. Jamšek, B. (2018, 20. november). Mladi podjetnik. *GDPR: Uredba o varstvu podatkov*. Pridobljeno 28. maja 2020 iz https://mladipodjetnik.si/novice-in-dogodki/novice/gdpr-uredba-o-varstvu-podatkov
43. Kajiyama, T., Jennex, M. & Addo, T. (2017). To cloud or not to cloud: how risks and threats are affecting cloud adoption decisions. *Information & Computer Security, 25*(5), 634-659.
44. Kavis, M. (2014). *Architecting the Cloud.* Hoboken, New Jersey: John Wiley & Sons.
45. Khorraminia, M., Lesani, Z., Ghasvari, M., Rajabion, L., Darbandi, M. & Hassani, A. (2019). A model for assessing the impact of cloud computing on the success of customer relationship management systems (case study: agricultural companies). *DIGITAL POLICY, REGULATION AND GOVERNANCE*, 461-475.
46. Kocha Fernando, D. A. (2015). Optimising resource costs of cloud computing for education. *Future Generation Computer Systems, 55*, 473-479.

47. Kratzke, N. (2012). *Cloud Computing Costs and Benefits: An IT Management Point of View* (str. 185-203). Lübeck: Lubeck University of Applied Sciences.
48. Lanich, Z. (2017). The Benefits Of Moving To The Cloud. *Forbes*. Pridobljeno 27. januarja 2020 iz https://www.forbes.com/sites/forbestechcouncil/2017/05/19/the-benefits-of-moving-to-the-cloud/#18283cfd4733
49. LinkTek. (2017). *On Moving Your Data to the Cloud: "Resistance is Futile" and Unnecessary.* Pridobljeno 20. januarja 2020 iz https://linktek.com/resisting-pressure-to-moving-your-data-to-the-cloud/
50. Lo.Polis. (brez datuma). *Uvedba Splošnih pogojev zasebnosti - GDPR*. Pridobljeno 28. maj 2020 iz https://novi.lopolis.si/Home/SecurityPolicy
51. Lobe, B. (2006). Združevanje kvalitativnih in kvantitativnih metod – stara praksa v novi preobleki? *Družboslovne razprave, XXII*, 55-73.
52. LOGOS.SI. (brez datuma). *Lo.Polis Opisi Modulov.* Kranj: LOGOS.SI d.o.o.
53. LOGOS.SI. (brez datuma). *Lo.Polis Predstavitev.* Kranj: LOGOS.SI d.o.o.
54. Lucidchart Content Team. (brez datuma). *Benefits of switching to a hybrid cloud infrastructure* [objava na blogu]. Pridobljeno 25. maj 2020 iz https://www.lucidchart.com/blog/hybrid-cloud-benefits
55. Mahmood, Z. & Hill, R. (2011). *Cloud Computing for Enterprise Architectures.* London: Springer.
56. MarketWatch. (2020, 19. maj). *COVID-19 Impact on Cloud Computing Market 2020: Comprehensive Analysis, Technological Advancement, Business Growth, Size, Share, Industry Share with Regional Forecast to 2024*. Pridobljeno 10. junija 2020 iz https://www.marketwatch.com/press-release/covid-19-impact-on-cloud-computing-market-2020-comprehensive-analysis-technological-advancement-business-growth-size-share-industry-share-with-regional-forecast-to-2024-2020-05-19?tesla=y
57. Mell, P. & Grance, T. (september 2011). *The NIST Definition of Cloud Computing.* Gaithersburg: National Institute of Standards and Technology (NIST).
58. NetApp. (brez datuma). *What Is Hybrid Cloud?* Pridobljeno 25. maja 2020 iz https://www.netapp.com/us/info/what-is-hybrid-cloud.aspx
59. Neznan avtor na FRI. (brez datuma). Računalništvo v oblaku. Pridobljeno 15. maja 2020 iz https://moodle.lusy.fri.uni-lj.si/pluginfile.php/1752/mod_resource/content/2/Ra%C4%8Dunalni%C5%A1tvo%20v%20oblaku.pdf
60. NIL d. o. o. (brez datuma). *IT-INFRASTRUKTURA ZA BOLJŠO ODZIVNOST VAŠEGA POSLA*. Pridobljeno 8. junija 2020 iz https://www.nil.com/sl/podatkovni-center-in-racunalnistvo-v-oblaku/
61. OECD. (2014). *Cloud Computing: The Concept, Impacts and the Role of Government Policy*. Pariz: OECD publishing.
62. OECD. (2017). *Cloud computing*. Pariz: OECD Observer.
63. Osnovna šola Milana Šuštaršiča. (2010). *Bilten ob 30-letnici osnovne šole Milana Šuštaršiča.* Ljubljana: Osnovna šola Milana Šuštaršiča.

64. Osnovna šola Milana Šuštaršiča. (2019). *Publikacija z beležko za šolsko leto 2019/2020.* Ljubljana: Osnovna šola Milana Šuštaršiča.
65. Patton, M. Q. (2002). *Qualitative Research & Evaluation Methods* (3. izd.). Thousand Oaks: Sage Publications.
66. Pošta Slovenije d. o. o. (brez datuma). *Storitve v oblaku (IaaS) - Rešitve.* Pridobljeno 8. junija 2020 iz https://www.posita.si/storitve/storitve-v-oblaku-(iaas)/pregled
67. Predavatelji na konferenci Arnes. (2011). Kaj nam prinaša računalništvo v oblaku? *Konferenca Arnes 2011.* Arnes.
68. Qadri, M. N. & Quadri, S. (2018). Mapping cloud computing in university e-governance system. *International Journal of Intelligent Computing and Cybernetics, Emerald, 11*(1), 141-162.
69. Raj, P. (2013). *Cloud Enterprise Architecture.* New York: CRC Press.
70. Rittinghouse, J. & Ransome, J. (2009). *Cloud Computing: Implementation, Management and Security.* CRC Press.
71. Saop d. o. o. (brez datuma). *iCenter, Osnovna šola potrebuje zanesljiv informacijski sistem.* Šempeter pri Gorici: Saop d. o. o.
72. Slack, C. (2019). Blue Silver Shift. *10 Reasons that so many business are moving to the cloud.* Pridobljeno 25. januarja 2020 iz https://www.bluesilvershift.com/why-are-so-many-businesses-moving-to-the-cloud-2/
73. Targett, E. (2019, 22. julij). Computer Business Review. *IaaS Magic Quadrant: Gartner Gets the Claws Out*. Pridobljeno 1. junija 2020 iz https://www.cbronline.com/news/cloud-iaas-gartner
74. TechTerms.com. (brez datuma). *TechTerms, Server Definition.* Pridobljeno 23. aprila 2020 iz https://techterms.com/definition/server
75. Teck Soon, H. & Syed A. Kadir, S. L. (2017). The drivers for cloud-based virtual learning environment. *Internet Research, 27*(4), 942- 973.
76. Telekom Slovenije, d. d. (brez datuma). *NAJEM STREŽNIKA*. Pridobljeno 8. junija 2020 iz https://www.telekom.si/poslovni-uporabniki/ponudba/it-resitve/storitve-v-oblaku/najem-streznika
77. Tolsma, A. (brez datuma). Deloitte. *GDPR and the impact on cloud computing*. Pridobljeno 28. maj 2020 iz https://www2.deloitte.com/nl/nl/pages/risk/articles/cyber-security-privacy-gdpr-update-the-impact-on-cloud-computing.html
78. Tomšič, A. (2011). Zasebnost v oblaku. *Arnes konferenca* (str. 15-19). Kranjska gora: Arnes.
79. Tsagklis, I. (2013, 23. april). *Advantages and Disadvantages of Cloud Computing – Cloud computing pros and cons*. Pridobljeno 20. maja 2020 iz https://www.javacodegeeks.com/2013/04/advantages-and-disadvantages-of-cloud-computing-cloud-computing-pros-and-cons.html
80. Ujčič, A. & Florjančič, V. (2017). *Javna uprava v računalniškem oblaku*. Koper: Znanstvena monografija, Založba Univerze na Primorskem.
81. Varga, M. (2017, 10. februar). Ni več ključno vprašanje, oblak da ali ne, ampak kako čim hitreje tja. *Delo*. Pridobljeno 8. junija 2020 iz

https://www.delo.si/gospodarstvo/podjetja/ni-vec-kljucno-vprasanje-oblak-da-ali-ne-ampak-kako-cim-hitreje-tja.html
82. Viswanatham V., M. (2016). Cloud Computing: Goals, Issues, SOA, Integrated Technologies and Future-scopes. *Ambient Science*, *3*(2).
83. vmware. (21. februar 2019). Architecture Overview for Consolidated SDDC. Pridobljeno 25. maja 2020 iz https://docs.vmware.com/en/VMware-Validated-Design/4.3/com.vmware.vvd-sddc-consolidated-design.doc/GUID-724CB1A5-11DD-4525-A510-A9272CDC29E9.html
84. Walterbusch, M., Martens, B. & Teuteberg, F. (2013). Evaluating cloud computing services from a total cost of ownership perspective. *Management Research Review*, *36*(6), 613-638.
85. Zainab, A., Chong, C. & Chaw, L. T. (2013). Moving a repository of scholarly content to a cloud. *Library Hi Tech*, *31*(2), 201-215.