UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

ZAKLJUČNA STROKOVNA NALOGA VISOKE POSLOVNE ŠOLE

VARNOST INFORMACIJSKIH REŠITEV V OBLAKU V EVROPI

Ljubljana, september 2017 MATJAŽ ŽULIČ

IZJAVA O AVTORSTVU

Podpisani Matjaž Žulič, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom Varnost informacijskih rešitev v oblaku v Evropi, pripravljenega v sodelovanju s svetovalcem red. prof. dr. Tomažem Turkom

IZJAVLJAM

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 _____ Podpis študenta:_____

KAZALO

KAZALO SLIK

UVOD

Računalništvo v oblaku (angl. *Cloud Computing*) je v zadnjih letih vse bolj razširjen pojav na področju računalništva. Danes se uporablja veliko storitev v oblaku, kar pa predstavlja velik pomen v svetu računalništva. Računalništvo v oblaku se tudi pogosto imenuje kot »oblak«, ki predstavlja prenos računalniških virov na zahtevo preko interneta na osnovi uporabe.

Namen zaključne strokovne naloge je podrobneje spoznati prednosti in slabosti uporabe oblačnih sistemov z vidika varnosti ter s kakšnimi izzivi se evropsko okolje sooča in opredeliti vzroke za nastanek varnostnih problemov v oblaku.

Cilj naloge je narediti pregled varnostnih vidikov oblačnih sistemov pri shranjevanju podatkov v evropskem okolju. Za izbiro teme zaključnega strokovnega dela sem se odločil na podlagi zanimanja za računalništvo v oblaku ter same uporabe teh storitev. Hotel sem izvedeti več glede varnosti teh storitev in raziskovati področja oblačnih sistemov. Zanimalo me je tudi evropsko okolje ter njegova vpletenost pri varnosti shranjevanja podatkov v oblaku.

Zaključna strokovna naloga je razdeljena na več poglavji s podpoglavji, ki vključujejo prikaz osnovnih značilnosti oblaka, varnosti shranjevanja v oblaku in varnosti oblačnih sistemov v Evropi. Uvodno poglavje vsebuje področje predstavitve oblaka in opredeljuje značilnosti oblaka. Za osrednji del pa je predstavljen empirični del, ki na podlagi povzema znanstvenih člankov in njihovih raziskav opredeljuje pogodbene pogoje oblaka, varnostne probleme v oblaku, varnost in zasebnost podatkov, varnost shranjevanja podatkov, varnost osebnih podatkov in standarde in predpise. V zadnjem oz. sklepnem poglavju pa je predstavljena analiza na podlagi raziskav v Eurostatu, ki kažejo, kakšna je varnost uporabe shranjevanja podatkov v evropskem okolju.

1 RAČUNALNIŠTVO V OBLAKU

1.1 Zgodovina

Računalništvo v oblaku je šlo skozi številne spremembe v preteklosti, kar je omogočilo, da so ljudje lažje in bolj dostopno dostopali do vsebin. Kot mnoge druge stvari je pomembno razumeti, kakšno je bilo računalništvo v oblaku v preteklosti, da lahko govorimo o prihodnosti razvoja le-tega. Trenutno stanje računalništva v oblaku temelji na močni podpori uporabe interneta, ampak včasih ni bilo tako. Danes je oblak pomemben del mnogih poslovnih infrastruktur informacijske tehnologije (v nadaljevanju IT), zaradi česar so elementi virtualizacije in storitveno usmerjenih arhitektur še pomembnejši. Če

pogledamo, kakšen je bil razvoj oblaka v preteklih letih, bomo lažje razumeli, kako je oblak pomemben sestavni del sodobnih informacijskih rešitev (Harrell, 2014).

1.1.1 Začetki računalništva v oblaku

Začetki računalništva v oblaku so se začeli že v 60. letih prejšnjega stoletja, kjer so podjetja preko »velikega računalnika« zagotavljala več uporabnikom dostop do istih sredstev. Včasih so bili veliki računalniki nameščeni v šolah, vladnih organizacijah in velikih podjetjih, saj so bili edini kraji, kjer so lahko imeli te stroje. Potem se je v 70. letih pojavila implementacija virtualnih strojev, ko je podjetje IBM izdalo operacijski sistem Navidezni računalnik (angl. *Virtual Machines – VM*). S tem je podjetje IBM poskrbelo za več ločenih računalnikov v istem okolju, kar je vodilo do interakcij, ki jim pravimo virtualizacija. To pomeni, da ima vsak posameznik oziroma uporabnik svoj računalnik, vendar so sredstva deljena z drugimi. Takšna vrsta računalništva je pokazala podjetjem, da lahko začnejo z omrežnimi rešitvami, ne da bi dejansko povečali njihove strojne infrastrukture. To je pomenilo, da so razbremenili omrežje in zagotovili boljše storitve svojim strankam (Harrell, 2014).

1.1.2 Prihod interneta

Telekomunikacijske rešitve so bile sestavni del razvoja računalništva v oblaku, kar je postalo možno s komercializacijo interneta. Mreža, na katerem temelji, je bila postavljena v 60. letih, ko so razvili Omrežno agencijo za napredne projekte (angl. *Advanced Research Projects Agency Network,* v nadaljevanju ARPANET). To je sčasoma postal predhodnik sodobnega interneta. Ta ideja, da bi povezovali ljudi po vsem svetu, je postala resnična možnost, kjer bi omogočili dostop do programov in podatkov iz različnih lokacij na svetu. Leta 1971 je ameriško obrambno ministrstvo poslalo prvo e-pošto, kar je pomenilo, da je s tem uspehom nadaljevalo razvijanje ARPANET-a v današnji internet. V poznejših letih pa so se različna podjetja oblikovala kot ponudniki storitev za gostovanje interneta. V letu 1993 je brskalnik Mosaic omogočil uporabnikom grafični prikaz vsebine, kar je pomenilo lažjo uporabo interneta. Kmalu zatem je tudi prišel brskalnik Netscape in podjetji Amazon ter eBay, ki sta začela s prodajo preko spleta (Harrell, 2014).

1.1.3 Sodobnejša zgodovina

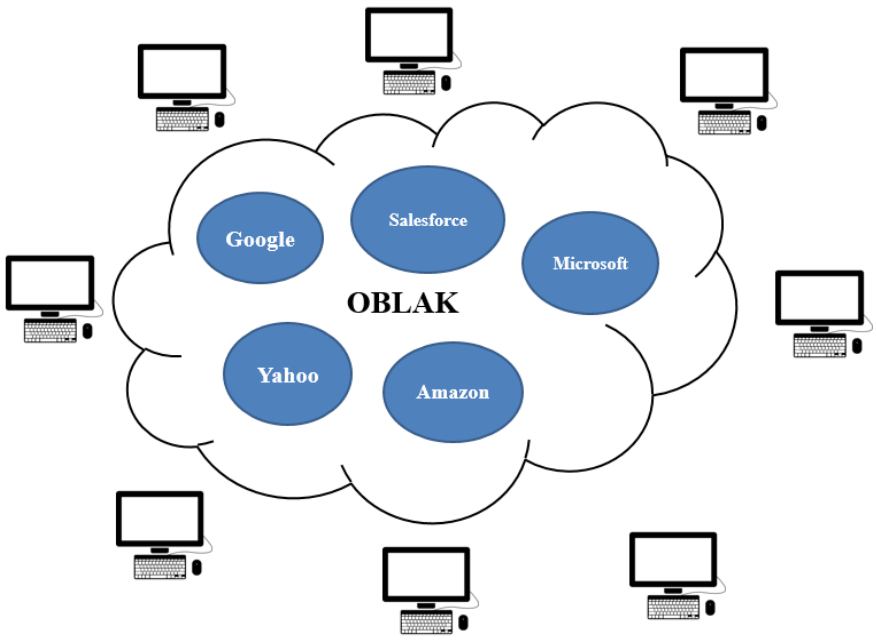
Začetki niso bili lahki za računalništvo v oblaku, saj so šele v letu 2000 podjetja morala razmisliti o spremembi poslovnih načrtov. Podjetje je še zmeraj moralo imeti trden poslovni načrt na dolgi rok, če je hotelo dobiti velike investicije od vlagateljev. Z iskanjem novih metod trženja interneta so se mnoga podjetja začela zavedati, da lahko zagotavljajo storitve uporabnih rešitev in virov. Podjetje Salesforce.com je bilo prvo na tem področju, ki je začelo s konceptom zagotavljanja aplikacij preko spletnega mesta. V letu 2002 je podjetje Amazon izdalo svoje spletne storitve (angl. *Amazon Web Services – AWS*), ki je

dalo uporabnikom možnost dostopa do shrambe podatkov, računanja rešitev in drugih aplikacij preko interneta. V letu 2006 pa so šli še dalje z elastičnim oblakom (angl. *Elastic Compute Cloud – ECC*), ki je omogočalo najem prostora na računalnikih za shranjevanje in zagon aplikacij. To je ponudilo celotno infrastrukturo, ki deluje kot storitev. Od leta 2009 pa so podjetja, kot sta Microsoft in Google, uspešno zagotovila programsko opremo za povprečnega potrošnika, kot tudi podjetjem v obliki enostavnih in dostopnih storitev. Stalna prisotnost oblaka je omogočila podjetjem, da jim ni treba iti do tretjih oseb, da uporabljajo te storitve. Tehnologija se je razvila do te mere, da lahko podjetja učinkoviteje razporejajo zasebne in hibridne oblake, namesto da se opirajo javnih oblakov. To lahko potencialno poveča učinkovitost in zmanjša nekatere stroške na tem področju (Harrell, 2014).

1.2 Opredelitev računalništva v oblaku

Definicija računalništva v oblaku je v večini pogledov zelo različna, zato moramo vedeti, da enotne definicije praktično ni mogoče najti. V nadaljevanju bom navedel nekaj definicij, ki so bile najdene iz različnih virov. Računalništvo v oblaku izhaja tudi iz spodnje shematske Slike 1, ki predstavlja upodobitev interneta, kar pa enako velja za oblak.

Slika 1: Shema računalništva v oblaku



Povzeto in prirejeno po U. Mesejedec, Oblaki prihodnosti, 2009.

Računalništvo v oblaku ali na kratko »oblak« je računalniški model, ki ga sestavljajo avtonomni in mrežni IT-viri (strojna in programska oprema). Ponudniki storitev v oblaku

ponujajo vnaprej določeno kakovost storitve preko interneta kot enostavno za uporabo, prilagodljivo in poceni storitev za stranke na podlagi različnih naročnin (Mesojedec, 2009).

Pri podjetju Salesforce so oblak definirali kot boljši način vodenja in delovanja podjetja. Poudarjajo pomen, da programske opreme delujejo na skupnih podatkovnih centrih namesto na infrastrukturi. Za potrebe zagona programske opreme pa je potrebna samo prijava v sistem in delo lahko poteka v podjetju. To je bistvena moč in prednost računalništva v oblaku (Salesforce, 2017).

NIST oz. Ameriški nacionalni inštitut za standarde in tehnologijo (angl. *US National Institute of Standards and Technology,* v nadaljevanju NIST) ima svojo razlago za računalništvo v oblaku, ki pravi, da je oblak način enostavnega dostopa oz. model za omogočanje dostopnosti do omrežja preko deljenih računalniških virov, kot so računalniško omrežje, strežniki, prostor za shranjevanje, programska oprema in storitve. Ti računalniški viri pa so lahko hitro oskrbovani, izdani z minimalnim naporom vodstva in z majhno interakcijo posameznega ponudnika storitev (NIST, 2011).

Spodaj so določene značilnosti, ki opredeljujejo računalništvo v oblaku (Qusay, 2011):

- Oblak na zahtevo – podjetjem ni potrebno, da so lastniki svojih podatkovnih centrov, s čimer bi imeli zagotovljene potrebe po IT-virih. Podjetja lahko najamejo zunanjega ponudnika, ki jim bo omogočal dostop do ogromnih baz podatkov na podoben način kot dostop do javnih podatkov.
- Avtonomnost − nekatere stranke se ne zavedajo tehničnih kompleksnosti ponujenih storitev. Od tega vidika so vključeni tehnologija, lokacija, omrežje in človeški viri za upravljanje storitev.
- Kakovost storitev − ponudniki storitev navajajo pogoje v pogodbah, da seznanijo svoje stranke o pričakovani ravni storitev. V pogojih kakovosti storitev lahko stranke izbirajo iz razpoložljivih ponudnikov in izberejo tistega, ki bo najbolj izpolnjeval njihove tehnične potrebe.
- Temelječe na internetu − iz oblike oblaka je prvotno prišlo poimenovanje računalništva v oblaku, ki pa se pogosto uporablja na področju informacijskih tehnologij ter predstavlja internet. To je zagotovilo, da vse storitve v oblaku gostijo in so zunaj meja strank ter so posredovane preko interneta.
- Enostavno za uporabo − ponudniki ponujajo vmesnike, ki so enostavni za uporabo in omogočajo strankam uporabo njihovih storitev. Ponudniki tudi omogočajo različne grafične uporabniške vmesnike za administratorje in razvijalce, kar jim omogoča lažjo uporabo teh vmesnikov.
- Prilagodljivost − pri tej lastnosti pa stranke niso omejene s fiksnimi zneski sredstev, vendar namesto tega se lahko uporaba prilagodi glede na potrebe. To dosežejo s

pomočjo metod, ki omogoča strankam, da dinamično ustvarjajo, prenašajo in nameščajo svoje podatke preko kode ali grafičnega vmesnika.
- Cenovna ugodnost − oblak daje malim in srednje velikim podjetjem možnost nižjih stroškov, če si podjetje ne more privoščiti lastnih podatkovnih centrov. Za podjetja to pomeni, da so sredstva v lasti ponudnikov, ki imajo v skupni rabi več strank, namesto tega, da imajo samo izključno za določeno stranko.
- Temelječe na naročniškem modelu − stranke se odločijo za ponudnika in mu za svoje storitve plačujejo uporabo. Strošek uporabe se zaračuna predvidoma na koncu meseca, vendar je odvisno od pogodbe, ki jo ponudnik in stranka skleneta.

Kot vidimo, so različne definicije za računalništvo v oblaku. Nekatere definicije dajejo poudarek na vidik uporabnika, druge pa na vidik infrastrukture. Glavni cilj poglavja je analizirati obstoječe definicije računalništva v oblaku s pomočjo analiz vsebine in prizadevanje za vzpostavitev skupne podlage, kaj točno je celovita opredelitev računalništva v oblaku (Gojčič, b.l.a).

1.3 Modeli računalništva v oblaku

1.3.1 Storitveni modeli računalništva v oblaku

Pri storitvenih modelih računalništva v oblaku govorimo predvsem o arhitekturi oblaka. Pri tem modelu oblaka združujemo infrastrukturo, platformo in programsko opremo kot storitev. To storitev pa zagotavlja ponudnik, ki omogoča uporabnikom, da lahko preko računalnika ali mobilnih naprav dostopajo do oblaka (Erl, Mahmood, & Puttini, 2013).

Glede na vsebino ločimo tri glavna področja oziroma platforme, ki določajo storitveni model oblaka (Erl et al., 2013):

- infrastruktura kot storitev – IaaS (angl. *Infrastructure as a Service*, v nadaljevanju IaaS),
- platforma kot storitev − PaaS (angl. *Platform as a Service*, v nadaljevanju PaaS),
- programska oprema kot storitev – SaaS (angl. *Software as a Service*, v nadaljevanju SaaS).

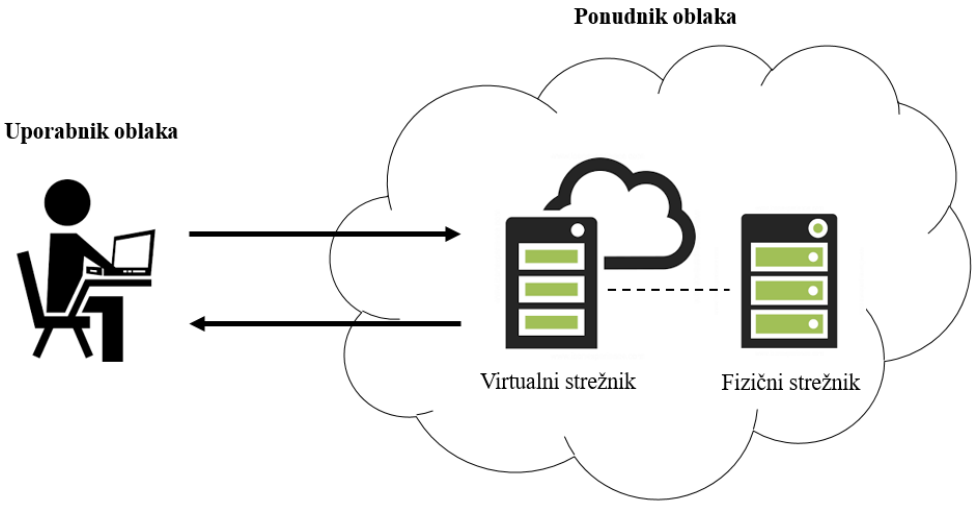
1.3.1.1 Infrastruktura kot storitev

Za infrastrukturo je značilno, da omogoča uporabo virtualiziranih virov, kot so procesorski čas, pomnilnik in prostor za shranjevanje. Storitev temelji na najemu računalniške infrastrukture (strežnik, prostor za shranjevanje in mrežna kapaciteta), ter nudi storitev v obliki računskih zmogljivosti, blokovnih shramb in omrežnih zmogljivosti. Uporabniki pa so sistemski administratorji. Glavni namen IaaSa je, da omogoča uporabnikom visoko

stopnjo nadzora in odgovornosti nad svojo konfiguracijo in uporabo. Sredstva, ki jih IaaS uporablja, na splošno niso vnaprej nastavljena, kar daje administrativno odgovornost neposredno na uporabnika. Vrste informacijskih virov, ki jih ponuja IaaS, se pri različnih ponudnikih razlikujejo. Informacijski viri, ki so ponujeni s strani IaaSa, so na splošno na voljo kot virtualni primeri. Osrednji in primarni vir informacijske tehnologije v tipičnem okolju IaaSa je virtualni strežnik. Virtualni strežniki zakupijo zahtevane strojne opreme strežnika, kot so procesorska kapaciteta, pomnilnik in lokalni prostor za shranjevanje (Gojčič, b.l.b).

Na spodnji Sliki 2 je prikazana shema, kako uporabnik oblaka uporablja virtualni strežnik v okolju IaaS.

Slika 2: Shema infrastrukture kot storitev



Povzeto in prirejeno po T. Erl et al., Cloud computing: Concepts, Technology & Architecture, 2013.

Za pomembnejše ponudnike infrastrukture, kot storitve so Oracle, IBM, Microsoft, Amazon ECC itd.

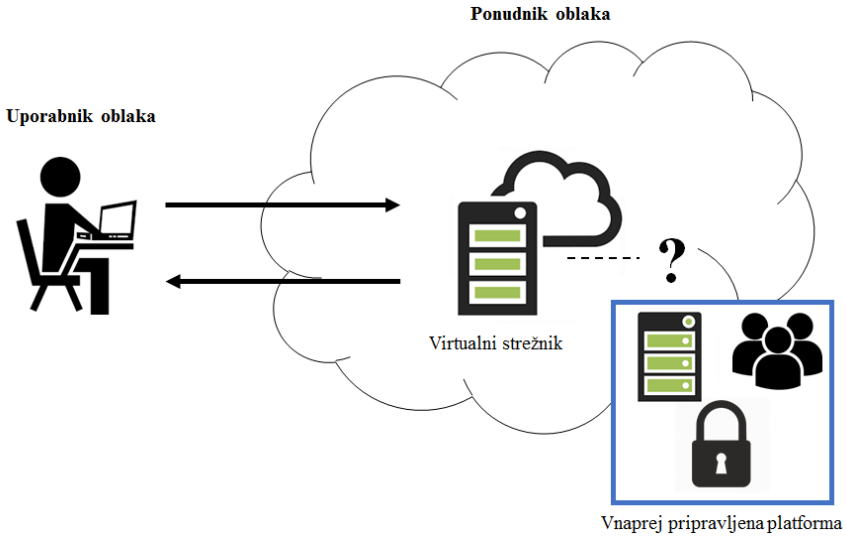
1.3.1.2 Platforma kot storitev

Pri tem storitvenemu modelu posredovanje določene platforme omogoča delovanje programske opreme. Platforma kot storitev omogoča razvoj, obratovanje in upravljanje programske opreme z orodji, ki vključujejo izvedbeno okolje, okolje varnosti, upravljanje podatkov in uporabnikov. Platforma omogoča postavitve različnih programskih oprem, ki se razvijejo s pomočjo programskih jezikov in orodij, ponujenih s strani ponudnika. PaaS vsebuje orodja za razvoj in testiranje računalniške programske opreme naročnika. Ponuja tudi storitve izvajalnega okolja, podatkovnih baz, objektnih hramb, sporočilnih vrst in

upravljanja z identitetami. V tej storitvi so uporabniki razvijalci. Na tej platformi lahko uporabnik razvija programsko opremo in tako uporablja rešitve za svojo korist. Omogoča razvoj in uporabo programske opreme brez potrebe po nakupu in vzdrževanju lastne strojne in programske infrastrukture, kar pomeni, da uporabnik ne upravlja oziroma nadzira z infrastrukturo (omrežje, shrambo, operacijski sistem itd.), ampak ima nadzor nad programsko opremo in gostujočim okoljem (Gojčič, b.l.b).

Vnaprej pripravljena platforma uporabniku prihrani administrativno breme vzpostavitve in vzdrževanja infrastrukture informacijskih virov. Na spodnji Sliki 3 pa znak vprašaj predstavlja uporabnikovo nižjo raven nadzora nad osnovnimi informacijskimi viri, ki gostijo zagotavljanje platforme (Erl et al., 2013).

Slika 3: Shema platforme kot storitev



Povzeto in prirejeno po T. Erl et al., Cloud computing: Concepts, Technology & Architecture, 2013.

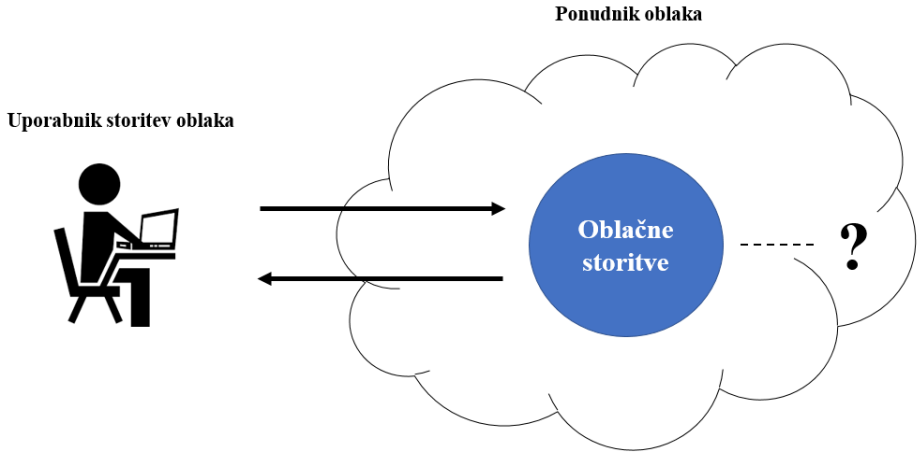
Ponudniki platforme kot storitve so Google (angl. *App Engine*), Microsoft (angl. *Azure Services Platform*), IBM PaaS, Oracle PaaS, Amazon (angl. *Amazon's Web Services*) itd.

1.3.1.3 Programska oprema kot storitev

Za zadnjo raven pa je izpostavljena programska oprema kot storitev, kar pomeni, da je ni treba nameščati oziroma zagnati na računalniku, in prav tako se nam ni treba ukvarjati z vzdrževanjem in nadgrajevanjem aplikacij, ki jih ponuja storitev. Pri tem lasten razvoj aplikacij ni možen, saj so aplikacije že razvite preko enostavnega spletnega vmesnika in omogočajo uporabo aplikacij na daljavo preko uporabe internetne tehnologije. Za takšno obliko oblaka uporabnik običajno potrebuje samo brskalnik in dostop do interneta, za ostalo pa poskrbi ponudnik storitve. Programska oprema temelji na infrastrukturi ponudnikov storitev v oblaku, kar omogoča dostop večjim odjemalcem hkrati, kar s

spletnim brskalnikom. Storitev tudi omogoča programske rešitve kot rešitve za komunikacijo, spremljanje, sodelovanje ipd. Pri tem pa so uporabniki storitev končni poslovni uporabniki. Pri ponudnikih storitev v oblaku gre za kompleksne, distribuirane računalniške sisteme, ki jih po navadi ne upravlja en subjekt, ampak celotna skupina. Uporabniki teh storitev pa praviloma ne poznajo strukture teh sistemov, temveč poznajo samo ključne parametre storitev, z najemom oziroma uporabo. Največja prednost tega sistema pa je zaračunavanje glede na uporabo aplikacij oz. plačilo na uporabo (angl. *pay-per-use*), kar pomeni, da s tem prinašajo tudi nove načine delovanja in se kaže z bistveno večjo stopnjo medsebojne integracije v primerjavi s klasičnimi aplikacijami (Gojčič, b.l.b).

Slika 4: Shema programske opreme kot storitev



Povzeto in prirejeno po T. Erl et al., Cloud computing: Concepts, Technology & Architecture, 2013.

Na zgornji Sliki 4 je predstavljen dostop uporabniku do storitev v oblaku, pri katerem znak vprašaj pomeni, da uporabnik ne dostopa do podrobnosti o izvajanju storitev.

1.3.2 Izvedbeni modeli računalništva v oblaku

1.3.2.1 Javni oblak

Javni oblak je javno dostopen oblak, ki je v večinoma v lasti ponudnikov. Informacijski viri v javnem oblaku so običajno zagotovljeni preko prej opisanih storitvenih modelov in so običajno na voljo uporabnikom po neki določeni ceni ali pa se prodajajo na druge načine, kot so oglasi itd. Ponudnik javnega oblaka je odgovoren za oblikovanje in tekoče vzdrževanje javnega oblaka in njegovih informacijskih virov. Velik pomen je tudi v odnosu med ponudniki in potrošniki IT-sredstev preko javnega oblaka. Organizacije lahko igrajo vlogo potrošnika pri dostopu do storitev oblaka in IT-virov, ki jih ponujajo različni ponudniki (Erl, et al., 2013).

Podjetja, kot so Google, Amazon, Apple itd., ponujajo storitve javnega oblaka, kar pomeni da delujejo na nizkocenovnemu modelu plačilo na poti (angl. *pay-as-you-go*) in večji prilagodljivosti na zahtevo (Erl et al., 2013).

1.3.2.2 Oblak skupnosti

Oblak skupnosti je zelo podoben javnemu oblaku, vendar je razlika v tem, da je njegova dostopnost omejena na določeno skupnost v oblaku. Oblak je lahko v lasti članov skupnosti ali pa je ponudnik oblaka tretja oseba, ki določa omejitve dostopa. V večini potrošniki oblaka delijo odgovornost za razvijanje oblaka skupnosti. Potrebno članstvo v skupnosti ni nujno, da zagotovimo dostop ali nadzor vseh IT-virov v oblaku. Osebe izven skupnosti nimajo dovoljenja do dostopa v oblak, razen če jim skupnost dovoli (Erl et al., 2013).

1.3.2.3 Zasebni oblak

Organizacije imajo v lasti zasebne oblake, saj omogočijo uporabo oblaka kot sredstvo za centralizacijo dostopa do informacijskih virov po različnih oddelkih in lokacijah. Pri uporabi zasebnega oblaka je možno spremeniti, kako organizacijske in meje zaupanja določamo in uporabljamo. Dejanska uporaba zasebnega oblaka se lahko izvaja preko notranjega in zunanjega osebja. Pri zasebnem oblaku je lahko ista organizacija potrošnik in ponudnik storitev v oblaku. Za razliko teh vlog imamo oddelke znotraj organizacije, ki običajno prevzamejo vlogo odgovornosti zagotavljanja IT-sredstev, in oddelke, ki zahtevajo dostop do zasebnega oblaka, kjer vlogo prevzamejo kot potrošniki. Zasebni oblak lahko prebiva v prostorih organizacije, vendar so gostujoči IT-viri lahko še vedno temelječi na osnovi oblačnih storitev tako dolgo, kot so na daljavo dostopni do potrošnika oblaka (Erl et al., 2013).

1.3.2.4 Hibridni oblak

Ta oblika oblaka je sestavljena iz dveh ali več različnih izvedbenih modelov oblaka. Kot primer lahko potrošnik odloči, kako bo razporedil storitve v oblaku za obdelavo občutljivih podatkov v zasebni oblak in druge manj občutljive v javni oblak. Arhitektura hibridnega oblaka je lahko zapletena in zahtevna za vzdrževanje zaradi potencialnih razlik v okolju oblaka in dejstva, da je upravljanje nalog po navadi razdeljeno med ponudnikom zasebnega in javnega oblaka (Erl et al., 2013).

1.4 Prednosti in slabosti računalništva v oblaku

V tem poglavju je poudarjen pomen prednosti in slabosti oblaka, ki je prinesel veliko novosti za računalništvo v oblaku.

1.4.1 Prednosti računalništva v oblaku

Oblak lahko popolnoma spremeni način, kako podjetje uporablja tehnologijo za storitve strankam, partnerjem in dobaviteljem, ki jim daje novo možnost okretnosti. Ponuja tudi številne prednosti, ki so (Ishita, 2014):

- Večja izkoriščenost strežnika − večina podjetij izkorišča svoje strežnike preko oblaka, tako da zagotavlja uporabljanje sredstev na najboljši možni način, saj se delijo med končnimi uporabniki na optimalen način.
- Stroškovna učinkovitost − oblak prinaša velike prihranke pri stroških za podjetje, saj jim ni treba kupiti vseh strojnih in programskih oprem. Za lažjo interpretacijo vzemimo primer velikega podjetja, ki zagotavlja, da imajo vsi zaposleni vse potrebne strojne in programske opreme, kar pa prinaša ogromne stroške, pri tem je oblak najboljša rešitev za takšno podjetje.
- Prilagodljivost − v primeru, če se podjetje želi razširiti mora vlagati še naprej v strojne in programske licence, ki vključujejo velike stroške. Pri tem pa oblak ponuja dodatno prednost, saj po nizkih stroških ponuja obdelavo podatkov brez vlaganja v kapital.
- Krajši programski čas razvoja − oblak uporablja storitveno usmerjeno arhitekturo, ki temelji na razvoju programske opreme, v katerem razvijalci aplikacij uporabljajo storitve v oblaku preko spleta. Nova programska oprema se lahko razvije preko spleta z večkratno uporabo skupaj.
- Krajši čas za izvedbo − oblak omogoča obdelavo procesov, podatkov in ima večjo zmogljivost, kar pomeni da s tem prihrani veliko časa, da bi dobili vse potrebne vire za izvedbo.

1.4.2 Slabosti računalništva v oblaku

Pri slabostih je treba paziti na različne probleme, ki pridejo z računalništvom v oblaku, kot so (Ishita, 2014):

- Varnostni problemi – v oblaku se shranjujejo podatki končnih uporabnikov in ne v uporabnikovi strojni opremi, kar pomeni veliko skrb za varnost podatkov. Pri tem varnostni programi oblaka zagotavljajo ustrezno varnost podatkov za uporabnika. Vendar imajo nekateri ponudniki manjšo preglednost kot drugi glede na njihove varnostne politike.
- Odvisnost od omrežja – pri oblaku je velikega pomena internet, saj storitve v oblaku brez internetnega dostopa ne morejo delovati na isti ravni, kot pa če bi delovale z internetom.
- Lokacija podatkov – omogoča strežnikom, da se lahko nahajajo kjerkoli, kar pomeni da uporabnik ne more vedeti, kje je fizična lokacija podatkov. V tem vidiku to ni

relativnega pomena, vendar je pomembno v primeru upravljanja podatkov v vladnih organizacijah.

- Obnovitev podatkov – za podjetja je zelo skrb vzbujajoče, saj so njihovi podatki lahko raztreseni po različnih strežnikih. V tem primeru lahko ponudnik oblaka najame zunanje izvajalce za proces obnovitve.
- Skupna raba programske opreme – velika skrb obstaja tudi za podatke v oblaku, ki so združeni in se nahajajo na različnih strežnikih. Tako je programska oprema v skupni rabi med končnimi uporabniki. V tem primeru je varnost velikega pomena.

2 VARNOST SISTEMOV V OBLAKU ZA SHRANJEVANJE PODATKOV

Oblak je v današnjih časih povsem odvisen od interneta, kjer se uporabniški podatki shranjujejo in vzdržujejo v podatkovnih centrih ponudnika oblaka. Arhitektura oblaka zagotavlja računalniške storitve preko interneta in brez fizične pridobitve, ki se uporablja za dostop do skupnih virov, kot so omrežja, hramba podatkov in strežniki. Tako pa prihranimo stroške upravljanja in čas za organizacijo. Varnost računalništva v oblaku postaja prostor za raziskovalna dela v študijskih vodah, kar pomeni, da se postavlja veliko vprašanj glede varnosti, kajti potrošnik nima veliko nadzora nad storitvijo in mora povsem zaupati ponudniku storitve. V tem poglavju se bomo osredotočili na varnost oblačnih sistemov pri shranjevanju podatkov in nevarnosti, ki pretijo pri tem (Singh, 2014).

2.1 Pravila in pogoji za oblačne storitve

Oblačne storitve so posebej primerne za uporabnike, ki imajo spremenljivo povpraševanje, kjer se ekonomija obsega doseže s pomočjo nekaterih ponudnikov, kar pa zagotavlja ekonomsko spodbudo za uporabo storitev oblaka ali pa infrastrukture. Ko se stranka oziroma uporabnik odloči za oblačne storitve pri ponudniku za zagotavljanje različnih programskih oprem, infrastruktur ali različnih storitev, so elementi nadzora do neke mere izven rok strank. Pri tem pa so pogoji, ki jih ponudnik postavlja, lahko vprašljivi, ko pride do dostopa do programske opreme in podatkov, ki so pomembni za delovanje. Varnost podatkov in sposobnost, da izpolnijo ureditvene potrebe o usklajevanju pravnih sredstev v odnosu do storitve, sta ključnega pomena ter jih morajo upoštevati ponudniki in potrošniki (Vincent, Hart, & Morton, 2011).

V večini primerov potrošniki neradi izkoriščajo storitve v oblaku bodisi zato, ker so pogodbe nejasne ali pa neuravnotežene v korist ponudnikov storitev. Obstoječi predpisi pogodbenega prava niso prilagojeni storitvam v oblaku, kar pomeni tudi več pomanjkljivosti pri pravnih pogojih oblačnih storitev. Varstvo osebnih podatkov v oblaku je treba tudi obravnavati in pri tem prilagoditi pogodbeno pravo, ker je pomembno za računalništvo v oblaku (European Commision, b.l.).

Kot primer pravil in pogojev ponudnika v oblačnih storitvah bi izpostavil podjetje Google, ki so, kot sledi (Google Inc., 2014):

- **Uporaba storitev:**
  - storitev se ne zlorablja,
  - potrošnik si ne more lastiti intelektualne lastnine na storitvah.
- **Google račun:**
  - za uporabo storitev lahko uporablja potrošnik samo ponudnikov račun.
- **Zaščita zasebnosti in avtorskih pravic:**
  - uporaba podatkov skladno z njihovimi pravilniki o zasebnosti,
  - postopki pri kršitvi avtorskih pravic potrošnika.
- **Potrošnikova vsebina je v Googlovih storitvah:**
  - kar je v lasti potrošnika, tudi ostane v njegovi lasti.
- **Programska oprema:**
  - omogoča prenos in uporabo programske opreme, vendar pa potrošnik ne sme kopirati, spremeniti, prodati ali dati v najem storitve.
- **Spreminjanje in ukinitev storitev:**
  - storitve se stalno spreminjajo ali ukinjajo, kar pomeni, da se potrošnik lahko kadarkoli preneha z uporabo storitve.
- **Jamstva podjetja in zavrnitev odgovornosti:**
  - nobenih posebnih obljub glede storitev, razen če so navedena izrecno v pogojih.
- **Odgovornost za storitev:**
  - ponudnik je odgovoren do mere, ki jo dovoljuje zakonodaja.
- **Poslovna uporaba storitev:**
  - uporaba storitev v imenu podjetja, če podjetje soglaša s temi pogoji.

2.2 Varnostni problemi povezani z računalništvom v oblaku

Obstaja veliko varnostnih izzivov, ki so povezani z oblakom, ki jih lahko razdelimo na različne razsežnosti. Preden uporabniki oblaka izberejo ponudnika, se morajo pozanimati o naslednjem (Chen & Zhao, 2012):

- ali imam privilegiran dostop do podatkov,
- ali ponudnik dela skladno s predpisi,
- kje je lokacija podatkov,
- kakšna je ločitev oz. segregacija podatkov,
- kako poteka obnovitev podatkov,
- kakšna je podpora pri preiskovanju zlorabe podatkov,
- kakšna je dolgoročna stabilnost ponudnika.

Strokovnjaka na področju računalništva v oblaku Subashini in Kavitha sta naredila raziskavo o varnosti oblaka na področju storitvenega modela ter podala podrobno analizo in oceno za vsak varnostni problem. Pozneje so še drugi strokovnjaki podali varnostne izzive glede arhitekture, značilnosti oblaka in deležniki v oblaku. Menili so, da sta še posebej dva vidika do neke mere nova in bistvenega pomena za oblak. To sta kompleksnost zaupanja večstranskega vidika oblaka in možnost revizije. Pri tem poudarjajo tudi nekaj novih priložnosti v varnosti oblaka (Chen & Zhao, 2012).

2.3 Varnost podatkov in zaščita zasebnosti

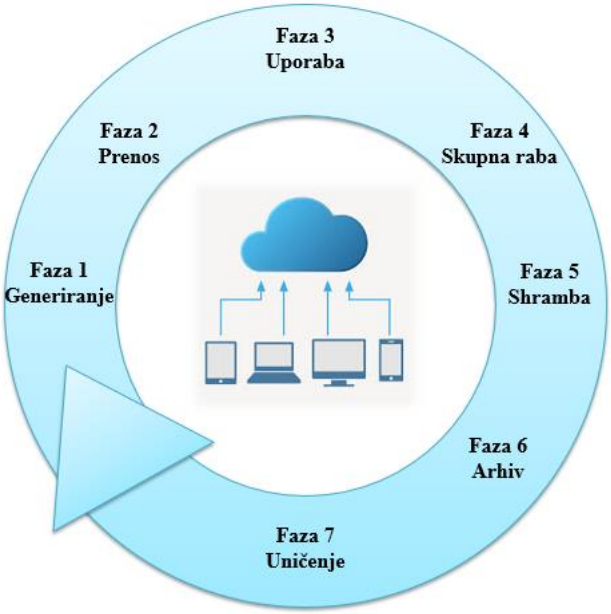
Pri varnosti podatkov in zaščiti zasebnosti v oblaku ni velike razlike od tradicionalne varnosti podatkov in zasebnosti, kajti je prisotno v vsaki fazi življenjskega cikla podatkov. Vendar ima varnost vsebine svoje posebnosti zaradi odprtosti in različnih značilnosti oblaka (Chen & Zhao, 2012)

Zasebnost se v različnih državah razlikuje glede na državo, kulturo ali pristojnosti, ki so na določenem območju. Različne organizacije imajo svojo opredelitev glede zasebnosti. Sprejela jo je tudi Organizacija za gospodarsko sodelovanje in razvoj (angl. *Organization for Economic Cooperation and Development – OECD*), ki pravi: »Vse informacije so v zvezi z določeno ali določljivim predmetom podatka.« Opredelitev, ki ga podata Ameriški inštitut registriranih računovodij (angl. *American Institute of Certified Public Accountants – AICPA*) in Kanadski inštitut licenciranih računovodij (angl. *Canadian Institute of Chartered Accountants – CICA*) v okviru standarda splošno sprejetih računovodskih načel (angl. *Generally Accepted Privacy Principles – GAPP*), pravi: »Pravice in obveznosti posameznika v organizaciji v zvezi z zbiranjem, uporabo, zadrževanjem in razkritjem osebnih informacij.« Če govorimo na splošno, je zasebnost povezana z zbiranjem, uporabo, razkritjem, shrambo in uničevanjem podatkov. Za identifikacijo zasebnih informacij je odvisno od specifičnega zakona in je primarna naloga za zaščito zasebnosti (Chen & Zhao, 2012). V nadaljevanju je analiza varnosti podatkov in zasebnosti v oblaku glede življenjskega cikla podatkov.

2.3.1 Življenjski cikel podatkov

Za življenjski cikel podatkov je značilno, da se nanaša na celoten proces, ki poteka od generiranja do uničenja podatkov. Pri tem je življenjski cikel sestavljen iz sedmih faz, ki so v nadaljevanju predstavljene. Na spodnji Sliki 5 so predstavljene faze življenjskega cikla podatkov (Chen & Zhao, 2012).

Slika 5: Življenjski cikel podatkov



Povzeto in prirejeno po D. Chen & H. Zhao, Data Security and Privacy Protection Issues in Cloud Computing, 2012.

2.3.2 Generiranje podatkov

Pri generiranju podatkov je vključeno lastništvo podatkov, saj si v informacijskem okolju uporabniki ali organizacije običajno lastijo podatke ter z njimi upravljajo. V primeru, če so podatki v oblaku, potem je treba upoštevati, kako ohraniti lastništvo glede podatkov. Pri osebnih podatkih imajo lastniki podatkov pravico vedeti, kakšni osebni podatki se shranjujejo in zbirajo ter če pride do zlorabe, da se ustavi zbiranje in uporaba osebnih podatkov (Chen & Zhao, 2012).

2.3.3 Prenos podatkov

Prenos podatkov je običajno znotraj meja organizacij in ne zahteva šifriranja ali pa imajo samo preproste ukrepe šifriranja. Da bi se preprečilo izkoriščanje in ponarejanje podatkov nepooblaščenim uporabnikom v organizacijah, bi za prenos podatkov preko organizacij morale organizacije povečati zaupnost podatkov. Kar pomeni, da samo šifriranje ni dovolj, ampak je treba tudi zagotoviti podatkovno integriteto. Zaupnost in integriteta prenosa podatkov morata zagotoviti ne le skladiščenja podatkov med organizacijami in shranjevanjem v oblaku, ampak tudi med različnimi storitvami shranjevanja v oblaku (Chen & Zhao, 2012).

2.3.4 Uporaba podatkov

Z uporabo preproste storitve za shranjevanje je šifriranje podatkov izvedljivo, vendar pa za podatke, ki temeljijo v oblaku platforme in programske opreme kot storitve je šifriranje podatkov v mnogih primerih neizvedljivo. Zato bo šifriranje podatkov povzročilo težave glede poizvedb v preprostih storitvah shranjevanja, kar pa za podatke, ki temeljijo v oblaku, ni težav, saj v splošnem niso šifrirani. V IT-okolju, kjer se podatki obravnavajo, skoraj noben ni šifriran za vsak program. Glede na funkcije več najemnikov v oblačnem modelu, pri čemer se podatki obdelujejo s programsko opremo, ki temelji na oblaku in se shranjujejo skupaj s podatki od drugih uporabnikov. Kar pa za nešifrirane podatke pomeni, da so v tem procesu resno ogroženi glede varnosti (Chen & Zhao, 2012).

2.3.5 Skupna raba podatkov

Lastniki podatkov lahko dovolijo dostop do podatkov subjektu, kar pomeni, da subjekt lahko nadaljuje z deljenjem podatkov na druge osebe brez soglasja lastnikov podatkov. Izmenjava podatkov širi obseg uporabe podatkov in naredi dovoljenje o uporabi bolj zapleteno. Zato morajo pri izmenjavi podatkov lastniki še posebej biti pozorni pri skupni rabi s tretjo osebo, saj morajo zagotoviti, ali bo tretja oseba ohranjala varnostne ukrepe in omejitve uporabe. Vsi podatki ali delni podatki so odvisni od politike skupne rabe podatkov in delitve podatkov vsebine. Za transformacijo podatkov je potrebna izolacija občutljivih podatkov od izvirnih podatkov, kar pomeni, da pri tem postopku podatki niso pomembni za lastnike podatkov (Chen & Zhao, 2012).

2.3.6 Shramba podatkov

Shranjeni podatki v oblaku so skladiščeni enako kot tisti, ki so shranjeni v drugih oblikah, zato morajo upoštevati tri vidike informacijske varnosti, kot so: zaupnost, integriteto in razpoložljivost. Za zaupnost podatkov je skupna rešitev šifriranje podatkov, pri tem pa bi zagotovili učinkovitost šifriranja, tako da se uporabi algoritem šifriranja in moč ključa. V okolju oblaka, kjer so vključene velike količine prenosa, shranjevanja in obdelave podatkov, je treba upoštevati tudi hitrost obdelave podatkov in učinkovitosti šifriranja velike količine podatkov (Chen & Zhao, 2012).

Obstaja še ena težava pri šifriranju podatkov, in to je upravljanje s ključi. Običajno so upravitelji ključa lastniki podatkov, zato ker sami uporabniki nimajo dovolj znanja za upravljanje z ključi, kar pa pomeni, da zaupajo ponudnikom storitev z upravljanjem ključev. Za ponudnike pa to pomeni vzdrževanje ključev za veliko število uporabnikov, kar pa je vedno bolj zapleteno in težko (Chen & Zhao, 2012).

Poleg zaupnosti podatkov je treba biti pozoren tudi na integriteto podatkov, ko uporabniki dajo več podatkov v oblak, je težko vedeti, kje točno se njihovi podatki shranjujejo. Selitev

v oblak ali izven njega porabi veliko uporabnikovega omrežja in časa. V nekaterih primerih ponudniki, kot so Amazon, zaračunajo uporabnikom za prenos podatkov, v bistvu kako neposredno preveriti integriteto podatkov, brez da se jih prenese in potem naloži nazaj, je velik izziv, saj so podatki dinamični v oblaku, kar pa pomeni, da niso tako učinkoviti. Pri IT-okolju je glavna nevarnost razpoložljivost podatkov, ki prihajajo iz zunanjih virov. Poleg nevarnosti, ki prihajajo iz zunanjih virov, so tukaj še druge nevarnosti, ki bodo ogrozile razpoložljivost podatkov, kot so razpoložljivost storitev v oblaku, nadaljnje delovanje ponudnikov storitev in zagotavljanje varnostnih kopij za shranjevanje v oblaku (Chen & Zhao, 2012).

2.3.7 Arhiviranje podatkov

Za arhiviranje podatkov je poudarek na shranjevanju v medij, ki pa je zagotovljeno shranjevanje na drugem mestu in trajanju skladiščenja tega medija. V primeru, če so shranjeni podatki na prenosnem mediju, potem je lahko nevarnost, da bodo podatki uhajali izven meja nadzora. Zato morajo ponudniki storitev zagotoviti drugo mesto za arhiviranje podatkov. Če je trajanje shranjevanja v skladu z zahtevami arhivskih, potem ni nevarnosti, vendar v nasprotnem primeru lahko pride do resnih groženj pri razpoložljivosti in zasebnosti podatkov (Chen & Zhao, 2012).

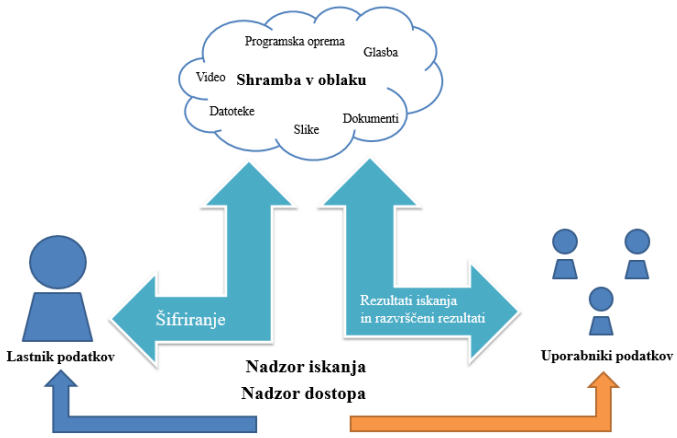
2.3.8 Uničenje podatkov

Podatki so lahko uničeni ali pa se jih ne potrebuje več. Pri fizikalnih lastnostih medija so lahko podatki, ki so bili izbrisani, še vedno obstoječi in jih je možno obnoviti. Vendar v tem primeru lahko povzroči nenamerno uhajanje občutljivih podatkov (Chen & Zhao, 2012).

2.4 Varnost shranjevanja podatkov v oblaku

Kot izziv shranjevanja v oblaku je zagotavljanje nadzora nad shranjenimi podatki v podatkovnih centrih oblaka. Pri tem imajo ponudniki storitev v oblaku popoln nadzor nad podatki, kar pomeni, da z njimi lahko opravljajo različne naloge, kot so kopiranje, spreminjanje, uničevanje itd., kar pomeni, da zaradi tega pomanjkanja nadzora nad podatki vodi k večjim varnostnim problemom, kot pa pri generičnem modelu oblaka, ki je izpostavljen na spodnji sliki. V tem primeru niti šifriranje ne daje popolnega nadzora nad shranjenimi podatki, vendar pa daje še vedno boljši nadzor kot nad golimi podatki (Vurukonda & Thirumala Rao, 2016).

Slika 6: Model oblaka za shranjevanje podatkov



Povzeto in prirejeno po N. Vurukonda & B. Thirumala Rao, A Study on Data Storage Security Issues in Cloud Computing, 2016.

Shranjevanje podatkov v oblaku se sooča z različnimi problemi v zvezi z integriteto, zasebnostjo in razpoložljivostjo podatkov. Kot vidimo na spodnji Sliki 7, so predstavljeni različni problemi shranjevanja podatkov v oblaku.

Slika 7: Problemi shranjevanja podatkov

Povzeto in prirejeno po N. Vurukonda & B. Thirumala Rao, A Study on Data Storage Security Issues in Cloud Computing, 2016.

2.4.1 Zasebnost in integriteta podatkov

Za oblak je značilno, da zagotavlja manj stroškov z upravljanji virov, vendar pa še vedno ima določene varnostne izzive. Kot je bilo že prej omenjeno, je oblak najbolj ranljiv v primerih, ko pride do zagotavljanja integritete, zaupnosti, zasebnosti in razpoložljivosti podatkov. Samo zaradi oblakove enostavnosti je programska oprema v oblaku zelo pogosta, kar pa pomeni, da te razmere vodijo k večji nevarnosti za potrošnike oblaka. V

primeru, če je napad na podatkovno bazo uspešen, potem lahko pride do vdora v zasebnost ter so vsi uporabniški podatki v bazi ogroženi s strani vdiralcev (angl. *hacker*). To pomeni, da sam oblak izgubi večnajemniški pomen. Za ponudnike programske opreme kot storitve je lahko tudi nevarnost, da izgubijo podatke in posledično tudi obstaja nevarnost pri shranjevanju teh podatkov. Poleg vseh teh nevarnosti obstaja še nevarnost obdelave podatkov za različne uporabnike. Nevarnost obstaja tudi pri virtualizaciji, kjer se več fizičnih virov deli med uporabnike, kar pa lahko povzroča napade zlonamernih notranjih uporabnikov. Te okoliščine notranjim uporabnikom omogočajo izvedbo napadov na shranjene podatke drugih uporabnikov preko obdelave njihovih podatkov. Obstajajo še druge nevarnosti, kot so podatki, preneseni v hrambo tretji osebi preko ponudnika oblačnih storitev. Upravljanje s ključi za varnost oblaka še ni povsem na ravni, kot bi moralo biti, kar pa pomeni, da brez standardnega šifriranja algoritma ne zagotavlja dobrega upravljanja oblaka s ključi. S tem pa šifriranje potencialno ogroža varnost za oblak (Vurukonda & Thirumala Rao, 2016).

2.4.2 Obnovitev in občutljivost podatkov

Oblak uporabnikom zagotavlja dinamično oskrbovanje virov po meri preko združevanja podatkov. Različni viri, ki so bili dodeljeni uporabnikom, so lahko v kasnejši časovni točki dodeljeni drugih uporabnikom. Če pride do primera shranjevanja virov, lahko zlonamerni uporabniki izkoristijo proces obnovitve, s katerimi bi lahko pridobili podatke predhodnih uporabnikov. Obnovitev pa lahko povzroči veliko nevarnost za občutljive podatke uporabnika (Vurukonda & Thirumala Rao, 2016).

2.4.3 Nepravilno prečiščevanje nosilca za shranjevanje

Pri nepravilnem prečiščevanju nosilca za shranjevanje obstaja velika nevarnost za shranjene podatke v oblaku. Razlogi za prečiščevanje nosilca so naslednji (Vurukonda & Thirumala Rao, 2016):

- disk je treba zamenjati z drugim diskom,
- diska ni treba vzdrževati in
- prenasičenost je storitev za shranjevanje v nosilca.

Vse podatke, ki so v večnajemniškem oblaku, je nemogoče prečistiti, ker so že najemniški s strani uporabnikov. Za večnajemniški oblak je značilna arhitektura, v kateri aplikacija služi več strankam oz. najemnikom. V tem imajo najemniki možnost, da prilagodijo nekatere dele v aplikaciji, kot so pogled uporabniškega vmesnika ali postavitev, vendar ne morejo prilagoditi kode programske opreme (Vurukonda & Thirumala Rao, 2016).

2.4.4 Varnostno kopiranje podatkov

V primeru, ko pride do naključnih oz. namernih nesreč pri izgubi podatkov, potem pride v poštev varnostno kopiranje podatkov. Za ponudnike oblačnih storitev pomeni, da morajo redno opravljati varnostno kopiranje shranjenih podatkov, da se zagotovi dostopnost podatkov. Varnostno kopiranje podatkov mora imeti določene varnostne smernice za preprečevanje zlonamernih dejavnosti, kot so nedovoljeni posegi in nepooblaščeni dostop uporabnikov (Vurukonda & Thirumala Rao, 2016).

2.4.5 Varnostne rešitve za shranjevanje podatkov v oblaku

Na podlagi znanstvenega članka »Študija o varnostnih izzivih shranjevanja podatkov v oblaku« (angl. *A Study on Data Storage Security Issues in Cloud Computing)* je narejena študija za različne varnostne protokole od različnih raziskovalcev. Kot prvi je *SecCloud*, ki je varnostni protokol za shranjevanje uporabniških podatkov, kar pa pomeni, da varuje shranjene podatke. Protokol uporablja šifriranje za shranjene podatke v varnem načinu. Šifrirani podatki so poslani s preverjenim podpisom v podatkovni center oblaka. Nato oblak s prejemom šifriranih podatkov dešifrira podatke, preveri digitalni podpis in shrani izvirne podatke v določenem mestu v oblaku. Protokol *SecCloud* preveri, ali so podatki shranjeni na določenem mestu ali niso (Vurukonda & Thirumala Rao, 2016).

Naslednji protokol, ki je bil povzet v študiji je protokol Zagotovljenost izbrisa datotek (angl. *File Assured Deletion*, v nadaljevanju FADE), ki zagotavlja upravljanje ključev s podatkovno integriteto in zasebnostjo podatkov. Pri tem protokolu je značilno, da je preprost, uporablja hkrati asimetrični in simetrični ključ za šifriranje podatkov. Protokol je zaščiten z algoritmom Shamir, ki ščiti simetrične in asimetrične ključe. Različni skrbniki podatkov uporabljajo protokol FADE, ki jih ščiti pred nevarnostmi udora. Tako imenovani *policy file* je datoteka Ameriške standardne kode za izmenjavo informacij (angl. *American Standard Code for Information Interchange – ASCII*), ki se lahko sestavi z urejevalnikom besedil ali pa z orodjem (angl. *Policy Tool*), kar prihrani tipkanje in odpravlja napake. *Policy file* ohranja podrobnosti, preko katerega so datoteke dostopne, kar pomeni, da za naložitev podatkov uporabnik zahteva ključ od tretje osebe, ko pošlje *policy file*. Skrbnik ključa pošlje javne in zasebne ključe do uporabnika preko *policy fila*. S tem se naložena datoteka šifrira z naključnimi znaki, ki so narejeni s simetričnim ključem. To šifrirano datoteko dešifrirajo z javnim ključem, ki je bil generiran s ključi. Z kontrolo dostopa do medijev (angl. *Media Access Control – MAC)* pa je tudi generiran s preverjeno podatkovno integriteto. Z obratnim procesom bo sprejemnik dobil nazaj prvotne podatke (Vurukonda & Thirumala Rao, 2016).

Šifriranje na atributu (angl. *Attribute-based encryption – ABE*) je uporabljeno v naslednji rešitvi, ki temelji na časovnem šifriranju. Ta shema omogoča varno izmenjavo podatkov med skupinami uporabnikov s kontroliranim pristopom. Shema *TimePRE* zagotavlja, da

posredovani podatki varno dosežejo uporabnika v skupini in ohranja uporabnikovo možnost preklica. Časovno obdobje je povezano z vsakim uporabnikom in lahko jo uporabnik sam prekliče ali pa je preklicano s strani ponudnika oblačnih storitev. V tej shemi lahko uporabniki delijo ključe predhodno s ponudniki ali pa ponudniki ustvarjajo nove ključe na zahtevo uporabnika. Shema omogoča nadzor dostopa po preučitvi atributov in ne identitete. *TimePRE*-shema zagotavlja zasebnost in razpoložljivost podatkov med skupinami, vendar pa se ne osredotoča na integriteto podatkov (Vurukonda & Thirumala Rao, 2016).

Za zadnjo rešitev bi poudaril metodologijo za varnost rezidenčnih podatkov, ki z verjetnostnim vzorčenjem zmanjšuje redundanco podatkov za varno in učinkovito upravljanje ključev. Skupina ali posameznik mora vzdrževati ključe, kar pomeni, da morajo standardne algoritme uporabiti za šifriranje ter zavreči šibke algoritme (Vurukonda & Thirumala Rao, 2016).

Za najboljšo varnost upravljanja s ključi in programsko opremo je uporaba legitimne programske opreme, ki zagotavlja varnost za shranjevanje podatkov v oblaku. Vsi uporabniki morajo ohraniti učinkovito upravljanje ključev. V primeru, če je zasnova protokola napačna, potem lahko proces šifriranja nadzoruje pretok podatkov z zunanjimi uporabniki. Za šifriranje je značilno, da samo po sebi ne preprečuje pretoka podatkov na zunanje uporabnike, ampak ga zmanjša na minimalno raven. Če pa pride do izpostavljenosti šifriranega ključa, potem lahko to vodi do uhajanja podatkov, kar je velik problem v okolju oblaka. Za reševanje problema je možno kombiniranje overitelja (angl. *authenticator*) in naključnega maskirnega postopka (angl. *masking process*). V spodnji sliki 8 so grafično predstavljene rešitve oz. zagotovila za varnost shranjevanja podatkov v oblaku glede na različne lastnosti (Vurukonda & Thirumala Rao, 2016).

Slika 8: Varnostne rešitve pri shranjevanju podatkov

	SecCloud Varnost oblačnih podatkov	**FADE** Zasebnost podatkov in integriteto	**TimePRE** Shema za varno skupno rabo podatkov	Metodologija za varnost rezidenčnih podatkov
Zasebnost	✓	✓	✓	✗
Integriteta	✓	✓	✗	✓
Razpoložljivost	✗	✗	✗	✓
Zaupnost	✓	✓	✓	✓

Povzeto in prirejeno po N. Vurukonda & B. Thirumala Rao, A Study on Data Storage Security Issues in Cloud Computing, 2016.

2.5 Varnost osebnih podatkov

Vrste oblaka so razdeljene na zasebni, javni in hibridni oblak. Po oblaku potujejo podatki uporabnika, ki se obdelajo in shranijo v zasebni oblak. Za razliko od zasebnih oblakov je javni oblak sredstvo, v katerem so podatki uporabljeni istočasno od različnih uporabnikov, kar pomeni, da zato prihaja do problema uhajanja podatkov med uporabniki. V tem primeru pa nastopi hibridni oblak, ki je tudi bil podrobneje predstavljen v prejšnjem poglavju. Različna varnostna zagotovila so prisotna pri oblaku, kot so zaupnost, integriteta in razpoložljivost, kar pa pri varnosti osebnih podatkov predpostavlja spoštovanje teh načel, ki so opredeljena z mednarodnimi sporazumi, zakonodajnimi akti, priporočili mednarodnih organizacij in z nacionalnimi zakonodajami (Fal & Kozak, 2014).

2.5.1 Pravice in obveznosti potrošnika

Potrošnik oblaka sprejema odločitve glede prenašanja vseh funkcij obdelave osebnih podatkov ali vsaj del na zunanjega upravitelja. Upravljanje osebnih podatkov je v potrošnikovih rokah, kar pomeni odgovornost pri spoštovanju zakonodaje o varovanju podatkov. Pri tem pa lahko potrošnik zaupa ponudniku z nalogo tehničnih in organizacijskih ukrepov, ki pridejo v poštev v zakonodaji varnosti podatkov (Fal & Kozak, 2014).

2.5.2 Pravice in obveznosti ponudnika

Ponudnik oblačnih storitev je glavna osrednja enota za osebne podatke. V nekaterih primerih je tudi ponudnik lahko upravljalec osebnih podatkov. V kompleksnem okolju obdelave podatkov so vključene različne kontrolne enote osebnih podatkov, kjer je treba odgovornost pri spoštovanju ali kršenju pravil natančno porazdeliti, pri tem pa preprečiti nastanek »lukenj« v primeru, če nobena kontrolna enota osebnih podatkov ne izvaja svojih obveznosti (Fal & Kozak, 2014).

Ponudniki v praksi morajo sami oblikovati pogoje za svoje storitve, kar pa pomeni, da morajo paziti na potrošnikove zahteve v pogodbah. Vendar potrošnika ne reši pred problemi pri varstvu osebnih podatkov. Če želi ponudnik načrtovati pogodbe za osebne podatke, potem mora kontrolnim enotam osebnih podatkov omogočiti svoje zahteve glede na ustrezno obdelavo podatkov, ki so zapisane v pogodbah (Fal & Kozak, 2014).

2.5.3 Zakonitost osebnih podatkov

Upoštevanje temeljnih pravnih načel pri varstvu osebnih podatkov je temelj za zakonitost obdelave osebnih podatkov, kjer se jamči preglednost za predmete osebnih podatkov, načela specifikacij cilja in omejitev ter uničenja osebnih podatkov zaradi nesmiselnega shranjevanja. Zagotovitev ustrezne ravni varstva podatkov je možna z ustreznimi

tehničnimi in organizacijskimi ukrepi. Za preglednost v oblaku je potrebna potrošnikova obveščenost o vseh podizvajalcih, ki so vključeni v sodelovanje pri opravljanju storitev oblaka, ter da je obveščen o lokaciji podatkovnih centrov, v katerem so obdelani podatki uporabnika. Načelo specifikacij ciljev in omejitev mora biti za osebne podatke zbrano za zakonite namene, prav tako pa se mora preprečiti kakršnekoli druge metode, ki niso v skladu s temi cilji. Za nastanek možnosti nezakonitih obdelav osebnih podatkov je treba postoriti vse, da ne pride do teh nezakonitih dejavnosti. Za uničenje osebnih podatkov je predpostavljeno, da se uničijo različni nosilci podatkov in izbris podatkov na način ponovnega zapisovanja na nosilce. Za zagotovitev varnosti osebnih podatkov je pomembna vsebina pogodb, ki so sklenjena med ponudnikom in potrošnikom v oblaku ter ponudnikovim podizvajalcem (Fal & Kozak, 2014).

2.5.4 Priporočila za varnost osebnih podatkov

Obstajajo različna priporočila za boljšo varnost osebnih podatkov za potrošnike in ponudnike (Fal & Kozak, 2014):

- potrošnik predhodno pridobi seznam skladiščenja ali obdelave podatkov s strani ponudnika v času veljavnosti pogodbe,
- potrošnik ima pravico pooblaščati tretje osebe za opravljanje nadzora podatkov,
- ponudnik ne more uporabiti podatkov za lastne potrebe,
- potrošnik mora oceniti tveganje, povezano z obdelavo osebnih podatkov pri določenem ponudniku,
- ponudnik mora zagotoviti pravico do dostopa podatkov potrošniku ter da odpravi napake.

Ponudniki oblačnih storitev v Ukrajini so se morali spopasti s problemom varstva osebnih podatkov v primeru potrošnikov iz držav Evropske unije (v nadaljevanju EU). Za pogodbo s potrošnikom oblačnih storitev je treba odražati zgornja priporočila, ki temeljijo na standardnih pogodbenih določbah, ki jih je odobrila Evropska komisija za ponudnike v tretjih državah (Fal & Kozak, 2014).

2.6 Standardi in predpisi

Pri ponudnikih, ki ponujajo različne metode za shranjevanje podatkov, je treba prav tako zagotavljati visoke stopnje varovanja podatkov. Pri varovanju podatkov so prisotni različni varnostni standardi in predpisi, kar pa ponudniku omogoča uveljavljanje najboljše prakse varovanja. Določeni standardi in predpisi pomenijo, da imajo ponudniki že določene pristope glede zaupnosti, razpoložljivosti in integritete varnosti podatkov (de Hert, Papakonstantinou, & Kamara, 2016).

V EU poznamo različne standarde in predpise, v tem primeru pa bi rad izpostavil standard ISO/IEC 27018 in njegov vpliv na zakonodajo EU o varstvu podatkov.

2.6.1 Standard ISO/IEC 27018

Standard ISO/IEC 27018 je bil predstavljen leta 2014, ki sta ga skupaj objavila organizaciji Mednarodna organizacija za standardizacijo (angl. *International Organisation for Standardisation*, v nadaljevanju ISO) in Mednarodna komisija za elektrotehniko (angl. *International Electrotechnical Commission*, v nadaljevanju IEC) za namen varnosti podatkov. Standard je kazalnik slabosti računalništva v oblaku, kjer je skrb za potrošnike oblaka velik problem, predvsem pri pomanjkanju zaupanja in preglednosti, kar pa z razvojem nadzora in predlogi ponudnika oblaka omogoča boljšo varnost v oblaku. Poleg tega pa omogoča ponudnikom večjo preglednost in odgovornost pri ravnanju s podatki v oblaku. Pod EU direktivo je standard opredeljen kot »tehnična specifikacija«, kar pomeni, da organ uporablja standard za večkratno ali stalno uporabo z namenom prepoznavnosti kakovosti standarda celotni javnosti. ISO/IEC-standard je postavljen na dveh prejšnjih standardih. To sta standard ISO/IEC 27001 in ISO/IEC 27002. Prejšnja standarda sta podobno kot ISO/IEC 27018 temeljila na varnosti podatkov. ISO/IEC 27001 zagotavlja sistem za identifikacijo nevarnosti podatkov in njenemu reševanju nevarnosti. ISO/IEC 27002 pa nadzira varnost glede zaupnosti, integritete in razpoložljivosti podatkov (de Hert et al., 2016).

3 VARNOST OBLAČNIH SISTEMOV V EVROPI

3.1 Načrti in strategija Evropske komisije

Politika Evropske komisije je postavljena v okviru strategije za enotni digitalni trg v Evropi (angl. *Digital Single Market Strategy*), ki igra ključno vlogo glede ključnih vprašanj, povezanih z lastništvom, dostopom, prenosljivostjo in preklapljanjem med ponudniki oblačnih storitev. Ta strategija bi do leta 2020 omogočila sprostitev potencialnosti oblaka v Evropi in bi z različnimi ukrepi povečala število delovnih mest na 2,5 milijona ter letno povečala za 160 milijard evrov bruto domačega proizvoda (*BDP*). Zasnovana je bila za pospešitev in povečanje uporabe oblaka v vseh gospodarskih sektorjih, kjer bi omogočila lažjo pridobitev delovnih mest. Ustanovili do tudi delovne skupine, ki bi omogočile lažje sodelovanje z interesnimi skupinami (European Commission, 2014).

Načrt strategije vključuje tri različne glavne ukrepe, ki bi izvajali strategijo Evropske komisije za izboljšanje stanja oblaka v Evropi (European Commission, 2014):

- Pogodbeni pogoji, ki so pravični in varni ter imajo cilj razviti model pogodbenih pogojev, ki bi urejal vprašanja glede lastništva podatkov, integritete, prenosa, lokacije, ohranitve podatkov po izteku pogodbe in spremembe pogodbe s ponudnikom in podizvajalci. S tem bo Evropa povečala zaupanje potrošnikov v ponudnike, saj bo z najboljšo prakso z novim modelov pogodbenih pogojev zaživelo novo obdobje oblačnih storitev.
- Hitro in učinkovito zmanjšanje standardov je ukrep, ki omogoča zmanjšanje nepreglednih standardov, pri tem pa je cilj, da imajo uporabniki boljšo izkušnjo pri prenosljivosti in popravljivosti podatkov. Evropska komisija je sodelovala z Evropsko agencijo za varnost omrežja in informacij (angl. *European Union Agency for Network and Information Security – ENISA*), kjer so razvili EU prostovoljne sheme za izboljšanje standardov.
- Ustanovitev Evropskega partnerstva v oblaku omogoča združitve zasebnega in javnega sektorja, da delajo na skupnih dejanjih v oblaku v odprtem in preglednem načinu. Evropska komisija je usmerjena v trajnostno gospodarsko rast, inovativnost in stroškovno učinkovitost javnih in zasebnih storitev v oblaku. Javni sektor ima pomembno vlogo glede oblaka, vendar je zaradi razdrobljenosti javnega sektorja integracija storitev nizka, kar za državljane pomeni, da ne dobijo najboljše storitve v državi. V pomoč pri tem problemu pride iniciativa oblak za Evropo (angl. *Cloud for Europe – C4E*), ki je usmerjena k pomoči javnemu sektorju za boljše zaupanje in storitev v oblaku.

3.2 Raziskava varnosti uporabe oblačnih sistemov v Evropi

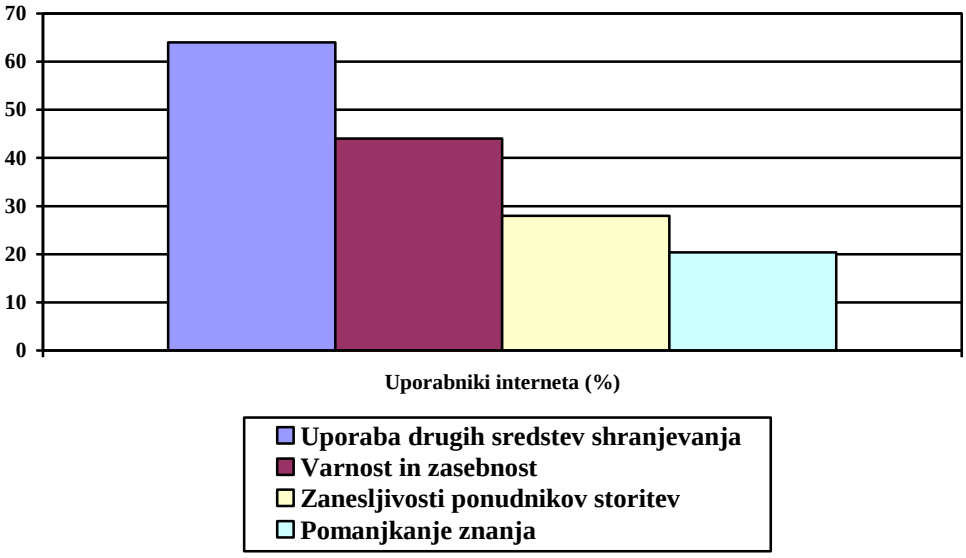
V raziskavi je uporabljen portal Statističnega urada Evropske unije Eurostat, ki je v letih 2014 in 2016 objavil raziskavo o uporabi in varnosti oblačnih storitev glede posameznikov in podjetji v EU. Raziskava o uporabi in varnosti oblačnih sistemov glede posameznikov je temeljila na odgovorih 150.427 gospodinjstev in na 211.325 posameznikih, starih med 16 in 74 let po celotni EU. Raziskava o uporabi in varnosti oblačnih sistemov glede podjetji pa je bila objavljena leta 2016 in je vsebovala 148.000 podjetij od 1,6 milijona vseh podjetij v EU. Od teh podjetji je bilo 83 % majhnih podjetij, 14 % je bilo srednje velikih in 3 % je bilo velikih podjetij (Seybert & Reinecke, 2014).

3.2.1 Raziskava o varnosti uporabe oblačnih sistemov glede posameznika

Shranjevanje podatkov na oblačni prostor je bilo v letu 2014 prisotno pri enemu od petih posameznikov v EU, starih od 16 do 74 let. Večina od teh posameznikov je uporabljala dostop do podatkov preko naprav iz različnih lokacij, vendar pa se večina še vedno ne zaveda oblačnih storitev, kljub temu da uporabljajo internet. Tisti uporabniki, ki so se zavedali oblačnih storitev, so bili zaskrbljeni glede varnosti in zasebnosti, kar jim je tudi onemogočilo uporabo takšnih storitev (Seybert & Reinecke, 2014).

V raziskavi so ugotovili, da je bila glavna ovira glede varnosti in zasebnosti podatkov zaskrbljenost o uporabi oblačnih storitev. V Sliki 9 so prikazani podatki uporabnikov, ki so uporabljali internet in se tudi zavedali, da oblačne storitve obstajajo. V večini uporabnikov je shranjevalo podatke na lastnih napravah Od tega je 44 % vprašanih odgovorilo, da jih skrbita varnost in zasebnost v oblačnih sistemih, kar pomeni tudi neuporabo teh storitev. Naslednji dejavnik (28 %) je zaskrbljenost glede zanesljivosti ponudnikov storitev, preostali dejavnik (22 %) pa je pomanjkanje znanja za uporabo oblačnih storitev (Seybert & Reinecke, 2014).

Slika 9: Glavne ovire za neuporabo oblačnih storitev



Povzeto in prirejeno po H. Seybert & P. Reinecke, Internet and cloud services – statistics on the use by individuals, 2014.

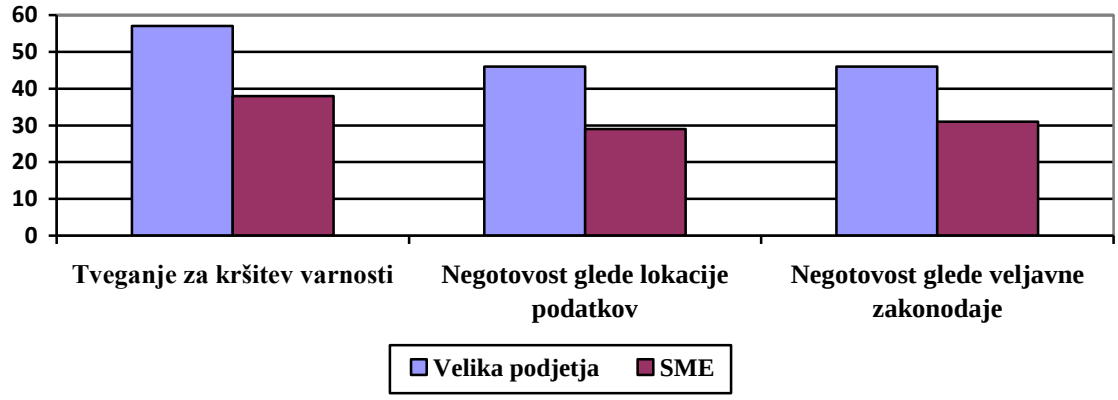
3.2.2 Raziskava o varnosti uporabe oblačnih sistemov glede podjetji

Pri podjetjih vplivajo številni dejavniki, zaradi katerih je omejitev uporabe oblačnih storitev večja. Za najvišje tveganje je izpostavljena kršitev varnosti izdaje podatkov tako za velika kot mala in srednje velika podjetja (angl. *Small and Medium Enterprises,* v nadaljevanju SME) (57 % in 38 %). Iz poslovnega vidika bi lahko odgovornost za kršitev varnosti preložili morda na ponudnika storitev ali pa le na tehnične težave, ki so prisotne pri oblačnih sistemih (Giannakouris & Smihily, 2016).

Podjetja, ki uporabljajo oblak, morda ne poznajo lokacije o svojih podatkih, kajti ponudniki storitev lahko uporabljajo podatkovne centre po vsem svetu, kar povzroča skrb velikim podjetjem (46 %) in SME-jem (29 %). Problemi nastanejo tudi v primeru spora in negotovosti med podjetjem in ponudnikom glede veljavnih zakonodaj ter njihovih pravnih

pristojnosti. Pri tem sta oba dejavnika povzročila manjšo uporabo oblaka; še posebej je to razvidno za velika podjetja, ki so že uporabljala oblačne storitve (46 %). Pri SME-podjetjih pa je ta omejitev manjša (31 %) (Giannakouris & Smihily, 2016). Na spodnji Sliki 10 vidimo omejitvene dejavnike uporabe oblačnih storitev glede na velikost podjetja.

Slika 10: Omejitveni dejavniki uporabe oblačnih storitev glede na velikost podjetja



Povzeto in prirejeno po K. Giannakouris & M. Smihily, Cloud computing – statistics on the use by enterprises, 2016.

SKLEP

V zaključni strokovni nalogi so predstavljene značilnosti na področju varnosti oblačnih sistemov za shranjevanje podatkov v evropskem okolju. Oblak je ustvarjen za večjo učinkovitost in fleksibilnost pri shranjevanju podatkov. Prinaša tudi nižje stroške IT-virov, hitrejšo odzivnost na zahtevo in dostopnejše storitve za podjetja in posameznike. Ti oblačni sistemi zagotavljajo določen nivo varnosti shranjevanja podatkov, vendar tudi tukaj ni povsem brez nevarnosti, ki pretijo na vsakem koraku. Pri varnosti shranjevanja podatkov je za ponudnika in potrošnika pomembnega pomena, kajti pri obeh je nujna varnost pri zlorabi podatkov. Ponudniki morajo poskrbeti za svoje stranke, kajti oni so tisti, ki ponujajo storitve v oblaku ter morajo zagotoviti določeno varnost oblačnih sistemov. Potrošniki oz. stranke v oblaku pa želijo najboljšo varnost za njihove podatke, vendar ni vse na strani ponudnikov. Tudi preko potrošnikovih napak lahko pride do zlorabe podatkov. Obstajajo tudi različne rešitve, ki se upirajo nevarnostnim v oblaku. To so različni protokoli, ki preprečujejo zlonamernim škodljivcem, da vdirajo v oblačne sisteme. V oblačnih sistemih je velik potencial, da se bo njihova uporaba v prihodnje širila. Vendar z razvojem različnih storitev in večje uporabe se bo vedno pojavila nevarnost za napade v oblačnih sistemih. Mnoga podjetja se zato pred izpostavljenimi nevarnostmi angažirajo na področju standardov in predpisov, ki jim omogoča večjo stabilnost pri varnosti v oblaku. Kar se tiče uporabnikovega znanja glede oblaka pa bo potrebnih še veliko izkušenj ter dodatnega znanja za boljšo izkušnjo uporabe oblačnih storitev.

LITERATURA IN VIRI

1. Chen, D., & Zhao, H. (2012, 23. april). Data Security and Privacy Protection Issues in Cloud Computing. *IEEE Xplore*. Najdeno 10. maja 2017 na spletnem naslovu http://ieeexplore.ieee.org/document/6187862/
2. de Hert, P., Papakonstantinou, V., & Kamara, I. (2015, 24. december). The cloud computing standard ISO/IEC 27018 through the lens of the EU legislation on data protection. *Computer Law & Security Review*, *32*(1), 16–30.
3. Erl, T., Mahmood, Z., & Puttini, R. (2013). Cloud Computing: Concepts, Technology & Architecture. *WhatIsCloud*. Najdeno 15. aprila 2017 na spletnem naslovu http://whatiscloud.com/cloud_delivery_models/index
4. European Commission. (2014, 24. marec). *European Cloud Strategy*. Najdeno 28. maja 2017 na spletnem naslovu https://ec.europa.eu/digital-single-market/en/european-cloud-computing-strategy
5. European Commission. (b.l.). *Cloud Computing Contracts*. Najdeno 7. maja 2017 na spletnem naslovu http://ec.europa.eu/justice/contract/cloud-computing/index_en.htm
6. Fal, O. M., & Kozak, V. F. (2014). Personal Data Protection Problems Associated with Cloud Computing. *Cybernetics and Systems Analysis; New York*, *50*(5), 768–773.
7. Giannakouris, K., & Smihily, M. (2016). Cloud computing – statistics on the use by enterprises. *Eurostat*. Najdeno 9. junija 2017 na spletnem naslovu http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises
8. Google Inc. (2014, 14. april). *Googlovi pogoji storitev*. Najdeno 7. maja 2017 na spletnem naslovu https://www.google.com/policies/terms/
9. Gojčič, I. (b.1.a). Računalništvo v oblaku – zgodovina, definicije. *Gemini*. Najdeno 7. aprila 2017 na spletnem naslovu http://www.geministyle.si/print/racunalnistvo/splosno/racunalnistvo-v-oblaku-2.html
10. Gojčič, I. (b.1.b). Modeli računalništva v oblaku. *Gemini*. Najdeno 7. aprila 2017 na spletnem naslovu http://www.geministyle.si/print/racunalnistvo/splosno/racunalnistvo-v-oblaku-4.html
11. Harrell, J. (2014, 4. junij). The History and Development of Cloud Computing. *AeroFS*. Najdeno 4. aprila 2017 na spletnem naslovu https://www.aerofs.com/blog/the-history-and-development-of-cloud-computing-md/
12. Ishita, V. (2014). Cloud Computing: A study of Benefits and Challenges. *International Journal of Advanced Studies in Computers, Science and Engineering; Gothenburg, 1*(1), 14–17.
13. Mesojedec, U. (2009, 28. april). Oblaki prihodnosti. *Monitor*. Najdeno 6. aprila 2017 na spletnem naslovu http://www.monitor.si/clanek/oblaki-prihodnosti/123624/?xURL=301
14. NIST – National Institute of Standards and Technology. (2011). *The NIST Definition of Cloud Computing*. Najdeno 6. aprila 2017 na spletnem naslovu http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

15. Qusay, H. F. (2011). Demystifying Cloud Computing. *Crosstalk, 24*(1), 16–21.
16. Salesforce. (2017). *What is cloud computing?*. Najdeno 6. aprila 2017 na spletnem naslovu https://www.salesforce.com/cloudcomputing/
17. Seybert, H., & Reinecke, P. (2014). Internet and cloud services – statistics on the use by individuals. *Eurostat*. Najdeno 9. junija 2017 na spletnem naslovu http://ec.europa.eu/eurostat/statisticsexplained/index.php/Internet_and_cloud_services_-_statistics_on_the_use_by_individuals
18. Singh, S. (2014). Security in Cloud Computing. *International Journal of Computer Applications Technology and Research, 3*(8), 488–493.
19. Vincent, M., Hart, N., & Morton, K. (2011, 5. april). *Cloud Computing Contracts White Paper, A Survey of Terms and Conditions*. Avstralija. Australian Federation of Intellectual Property Attorneys.
20. Vurukonda, N., & Thirumala Rao, B. (2016, 11. avgust). A Study on Data Storage Security Issues in Cloud Computing. *Procedia Computer Science, 92*, 128–135.

PRILOGA

PRILOGA 1: Seznam uporabljenih kratic

IT	Informacijska tehnologija
VM	(angl. *Virtual Machines*); Navidezni računalnik
IBM	(angl. *International Business Machines*)
ARPANET	(angl. *Advanced Research Projects Agency Network)*; Omrežna agencija za napredne projekte
AWS	(angl. *Amazon Web Services)*; Amazonove spletne storitve
ECC	(angl. *Elactic Compute Cloud)*; Elastični računski oblak
NIST	(angl. *US National Institute of Standards and Technology)*; Ameriški nacionalni inštitut za standarde in tehnologijo
IaaS	(angl. *Infrastructure as a Service)*; Infrastruktura kot storitev
PaaS	(angl. *Platform as a Service*); Platforma kot storitev
SaaS	(angl. *Software as a Service)*; Programska oprema kot storitev
OECD	(angl. *Organization for Economic Cooperation and Development)*; Organizacija za gospodarsko sodelovanje in razvoj
AICPA	(angl. *American Institute of Certified Public Accountants)*; Ameriški inštitut registriranih računovodij
CICA	(angl. *Canadian Institute of Chartered Accountants)*; Kanadski inštitut licenciranih računovodij
GAPP	(angl. *Generally Accepted Privacy Principles)*; Standard splošno sprejetih računovodskih načel
FADE	(angl. *File Assured Deletion*); Zagotovljenost izbrisa datotek
MAC	(angl. *Media Access Control)*; kontrola dostopa do medijev
ASCII	(angl. *American Standard Code for Information Interchange*); Ameriška standardna koda za izmenjavo informacij
ABE	(angl. *Attribute-based encryption*); šifriranje, ki temelji na atribut
EU	Evropska unija
ISO	(angl. *International Organisation for Standardisation)*; Mednarodna organizacija za standardizacijo
IEC	(angl. *International Electrotechnical Commission)*; Mednarodna komisija za elektrotehniko

BDP	Bruto domači proizvod
ENISA	(angl. *European Union Agency for Network and Information Security)*; Evropska agencija za varnost omrežja in informacij
C4E	(angl. *Cloud for Europe)*; Oblak za Evropo
SME	(angl. *Small and Medium Enterprises)*; majhna in srednje velika podjetja