



FAKULTET ZA INFORMATIKU I MENADŽMENT



Dejan Đurić

BEZBEDNOST U CLOUD COMPUTING-U

- Diplomski rad -

BEZBEDNOST U CLOUD COMPUTING-U

- Diplomski rad -

Mentor:
Prof. dr Angelina Njeguš

Student:
Dejan Đurić

Br. indeksa:
III-4V/2005



UNIVERZITET SINGIDUNUM
FAKULTET ZA INFORMATIKU I MENADŽMENT
Beograd, Bulevar Zorana Đinđića 44

Kandidat: Dejan Đurić

Broj indeksa: III-4V/2005

Smer: Projektovanje i programiranje

Tema: BEZBEDNOST U CLOUD COMPUTING-U

Zadatak:

U ovom radu ukratko je objašnjeno šta je to cloud computing i predstavljena su uputstva o bezbednosti cloud computing-a.

Datum odobrenja teme:
Beograd, _____.____.____.

MENTOR

Prof. dr Angelina Njeguš

DEKAN

Prof. dr Mladen Veinović

BEZBEDNOST U CLOUD COMPUTING-U



SADRŽAJ

1. Uvod	1
2. Šta je Cloud Computing?	2-8
2.1 Žašto je Cloud Computing upravo sada stupio na scenu?	3
2.2 Na koji način se Cloud Computing koristi danas?	3-4
2.3 Kompjuteri idu u oblake – ideja?	4-6
2.4 Teorijske osnove problema – Kako Cloud Computing radi?	6-8
2.5 Koje su tržišne mogućnosti za ovu tehnologiju?	8
2.6 Šta su najveći izazovi sa kojima se ove kompanije susreću?	8
3. Rešenje i implementacija	8-18
3.1 Cloud Computing: Evolucija Programa-kao-Servisa (Software-as-a-Service)...	8-10
3.2 Postave	10-11
3.2.1 Prva postava	10
3.2.2 Druga postava	11
3.2.3 Treća postava	11
3.3 Dobijanje oblika	11-15
3.4 Cloud Computing arhitektura	15-16
3.5 Cloud Computing aplikacije	16-18
4. Prednosti Cloud Computing-a	18-25
4.1 IBM i klijenti izvlače korist od Cloud Computinga	18-20
4.2 Centri za podatke u svetu koji se menja	20
4.3 Izazovi sa kojima se konstrukcije trenutnih centara za podatke suočavaju	20-21
4.4 Kako Cloud Computing sređuje ranjive tačke današnjeg IT okruženja	21-22
4.5 Elastična Cloud validacija: Sledeći korak u ostvarivanju elastičnosti	23
4.6 Cloud Computing u inostanstvu: Uspeh Jun platforme	23-24
4.7 Cloud Computing u Evropi	24
4.8 Osećaj sigurnosti kod IBM-ovog zapisa	24-25
5. Bezbednost u Cloud Computing-u	25-31
5.1 Adresa Cloud bezbednosti – veliki izazov	26-27
5.2 Pregled drugih modela Cloud Computing-a	27-28
5.3 Pregled IBM Sigurnosnog okvira (IBM Security Framework)	28-31
5.3.1 Bezbednost upravljanja, upravljanja rizicima i pridržavanje	29
5.3.2 Ljudi i identiteti	29
5.3.3 Podaci i informacije	29-30
5.3.4 Aplikacije i procesi	30
5.3.5 Mreža, server i krajnja tačka	30-31
5.3.6 Fizička infrastruktura	31

6. Vodič za primenu sigurnog oblaka.....	31-48
6.1 Implementacija i održavanje bezbednosnog programa.....	31-33
6.2 Izgradnja i održavanje bezbedne Cloud infrastrukture.....	33-37
6.3 Obezbediti zaštitu poverljivih podataka.....	37-41
6.4 Implementirati snažan pristup i identitet menadžmenta.....	41-42
6.5 Uspostaviti bezbednost aplikacija i okruženja.....	42-43
6.6 Sprovođenje upravljanja i revizije programa za upravljanje.....	43-44
6.7 Implementirati upravljanje programom ranjivosti i provale.....	44-45
6.8 Održavajte testiranje i validaciju okruženja.....	45-48
 7. Razumevanje IBM-ove tačke gledišta u Cloud bezbednosti.....	 48-53
7.1 Ni '' Jedna veličina odgovara svima'' za bezbednost.....	48-49
7.2 Osnovni arhitektonski model za Cloud Computing.....	50
7.3 Cloud bezbednost i SOA.....	51-52
7.4 Mogućnost da se pojednostavi kontrola bezbednosti i odbrane.....	52-53
 8. IBM-ova anketa obima i definicije.....	 53-58
 9. Zaključak.....	 59
 10. Literatura.....	 60

1 Uvod

Tokom 2008. godine cloud computing našao se u središtu zbivanja u medijima posvećenim informacionim tehnologijama.

U roku od samo nekoliko meseci, cloud computing, nekada relativno malo poznat koncept, postao je najprimamljivija tehnologija godine. Čitav niz kompanija pridružio se novom trendu, lansirajući nove usluge vezane za cloud computing. U mnogim slučajevima, radilo se samo o preimenovanju postojeće ponude kako bi se iskoristile nove okolnosti. Ukratko, radilo se o medijskoj groznici najvišeg nivoa.

Međutim, strasti se polako smiruju i IT mediji, kao i analitičari i sama informatička industrija, danas imaju u mnogo većoj meri realističan pogled na tehnologiju cloud computing-a. Na primer, Gartner ide toliko daleko da predviđa da će cloud computing proći kroz period 'razbijanja iluzija' – tj. fazu u medijskom ciklusu u kojoj nove tehnologije ne uspevaju da ispune očekivanja i brzo izlaze iz mode.

I pored toga, uprkos senzacionalizmu, i za razliku od mnogih tehnologija koje su joj prethodile, kao što su video telefonija, kancelarija bez papira i mobilna televizija, da navedemo samo neke od njih, cloud computing će sasvim sigurno ostati prisutni i evoluirati tokom godina koje slede. Oni će izmeniti način rada ljudi, kao i poslovanje kompanija, omogućavajući im da koriste usluge na ekonomičniji način.

Usluge cloud computing-a naročito su privlačne za male ili početničke kompanije koje ne mogu priuštiti velike inicijalne investicije u informatičku opremu. Ipak, nije verovatno da će veće organizacije potpuno napustiti model informatičkih aktivnosti 'na licu mesta' ili da će informatičke kapacitete koji imaju centralnu ulogu u njihovoj tržišnoj konkurentnosti zameniti uslugama cloud computing-a. Mnoge kompanije i dalje će zahtevati nivo bezbednosti, performansi ili specijalizacije aplikacija koji ne može biti dostignut korišćenjem javnih cloud computing-a. One će možda formirati sopstvenu privatnu arhitekturu cloud computing-a, skrivenu iza korporativnih firewall-a, kako bi iskoristile njihovu efikasnost, ali uz veću bezbednost i kontrolu.

Ukratko, cloud computing ne predstavlja prolaznu modu, ali ni revoluciju u elektronskom poslovanju. Umesto toga, većina kompanija verovatno će koristiti kombinovano informatičko okruženje, u kojem će aplikacije, infrastruktura i, u pojedinim slučajevima, svi poslovni procesi, biti realizovani putem javnih i privatnih cloud computing-a.

2 Šta je Cloud Computing?



Slika 1: Cloud Computing??? [4]

Danas svi govore o cloud computing-u, ali čini se da svako koristi drugačiju, iako sličnu, njihovu definiciju, u zavisnosti od svoje pozicije. Na primer, oni koji rade u oblasti usluga imaju drugačiju definiciju cloud computing-a od nekoga ko radi na sistemskoj arhitekturi.

Gartner and Forrester nudi sledeću definiciju:

„Oblast računarstva u kojoj se veoma skalabilni informatički kapaciteti obezbeđuju u vidu usluge isporučene putem interneta brojnim eksternim potrošačima.“

Daryl Plummer, Gartner⁴

„Apstrahovana, visoko skalabilna i kontrolisana kompjuterska infrastruktura koja hostuje aplikacije namenjene krajnjim korisnicima i čije se usluge naplaćuju na bazi ostvarene potrošnje.“

Forrester

Intel takođe ima sopstvenu definiciju cloud computing-a, koja uzima u obzir njegovu arhitekturu i usluge, pri čemu postoji razlika između javnih i privatnih cloud computing mreža:

Arhitektura cloud computing: usluge i podaci egzistiraju u deljenom, dinamički skalabilnom skupu resursa zasnovanom na tehnologijama virtualizacije i/ili skaliranim aplikativnim okruženjima.

Usluge cloud computing-a: servisi za potrošače ili kompanije realizuju se putem javnog interneta. Oslanjajući se na arhitekturu cloud computinga, skaliranje usluga vrši se bez intervencije korisnika i obično se naplaćuje na osnovu ostvarene potrošnje.

Privatni cloud computing: arhitektura oblaka je smeštena iza firewall-a organizacije i pruža

informatičke usluge za internu upotrebu.

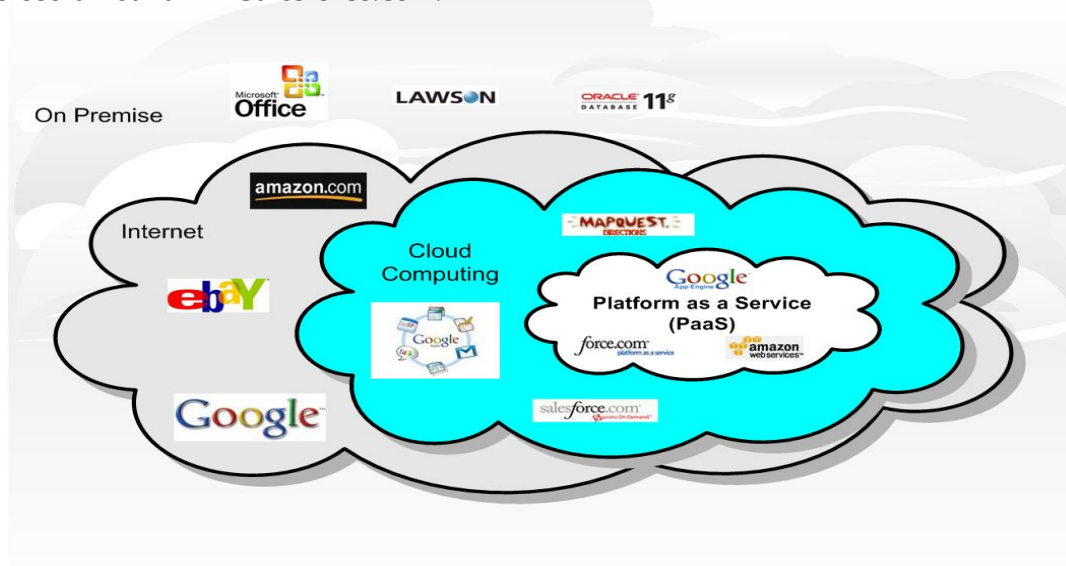
Cloud computing možemo posmatrati kao novi koncept zasnovan na ranijim modelima distribuiranih usluga koji su stvoreni tokom poslednje decenije, uključujući računarstvo u vidu usluge (utility computing), usluge na zahtev (on-demand services), mrežno računarstvo (grid computing) i softver u vidu usluge (software-as-a-service). Međutim, cloud computing od tradicionalnih internet servisa razdvaja inherentna dinamična i fleksibilna arhitektura koja omogućava korisnicima informatičkih tehnologija da plaćaju samo one usluge koje su im zaista potrebne, kao i da u kratkom vremenskom roku višestruko povećaju njihov obim.

2.1 Zašto je Cloud Computing upravo sada stupio na scenu?

Cloud computing, kako smatra Gartner, predstavljaju 'fenomen u nastajanju' – drugim rečima, fenomen koji nastupa u trenutku kada su uslovi za to povoljni i kada brojni faktori to dozvoljavaju – u ovom slučaju, orijentacija ka servisima, virtualizacija i standardizacija računarstva putem interneta. U kombinaciji sa globalnom ekonomskom krizom, cloud computing omogućavaju smanjenje određenih troškova vezanih za informatičke tehnologije.

2.2 Na koji način se Cloud Computing koristi danas?

Najveći deo arhitekture cloud computinga koji se danas koriste obuhvata javne cloud computing mreže namenjene pružanju usluga putem interneta, kao što su Google Search, Microsoft Hotmail ili Salesforce.com.



Slika 2: Prikaz javne cloud computing mreže. [4]

Veliki provajderi usluga, zajedno sa tipičnim pionirima u prihvatanju novih tehnologija kao što su finansijske usluge, superkompjuteri i farmaceutske kompanije, takođe primenjuju arhitekturu cloud computing-a prilikom implementacije privatnih cloud mreža

zaštićenih firewall-om. Ovaj način korišćenja još uvek je u početnoj fazi i očekuje se da će ostvariti dalji rast na bazi korporativnih tehnologija virtualizacije koje se već sada uvode.

Javne usluge cloud computing-a uglavnom su usmerene ka potrošačkim uslugama kao što su pretraživanje na internetu, lični email servisi, društveno povezivanje (social networking) i druge primene Interneta 2.0 (Web 2.0). Male i početničke kompanije takođe privlači koncept usluga pruženih putem cloud computing-a, s obzirom na to da on omogućava smanjenje inicijalnih investicija u informatičke tehnologije. Očekuje se da će neke od većih kompanija uvesti usluge cloud computing-a u oblasti aplikacija za koje se smatra da nemaju kritičnu važnost za poslovanje – kao što je internet softver za upravljanje rasporedom putovanja zaposlenih ili za podršku u sferi menadžmenta ljudskih resursa.

Međutim, za mnoge kompanije, informatička infrastruktura blisko je povezana sa centralnom oblašću njihovog poslovanja i eksternalizacija računarskih kapaciteta predstavljala bi veliki poslovni rizik. Bezbednost, pouzdanost, performanse i usaglašenost sa standardima predstavljaju navažnija pitanja za šefove informatičkih odeljenja prilikom procenjivanja novih tehnologija. Na primer, biotehnoška kompanija možda neće želiti da vrši modeliranje novih lekova izvan sopstvenih zidova, već će za naprednu simulaciju novih jedinjenja iskoristiti sopstvene servere. Kako bi iskoristila svu fleksibilnost i efikasnost arhitekture cloud computing-a, ta kompanija može razviti internu, privatnu cloud computing mrežu nad kojom će imati veću kontrolu i ostvariti veću bezbednost računarskih resursa.

2.3 Kompjuteri idu u oblake – ideja?



Slika 3: Kompjuteri idu u oblake – ideja? [4]

IBM, Yahoo i Google su udružili moć cloud computing-a za posao. Ovo je kratak primer kako nova tehnologija radi.

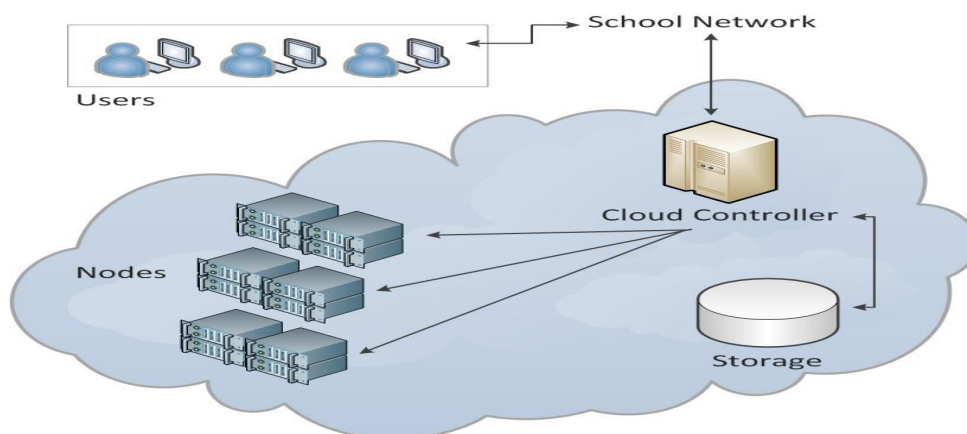
Iako je cloud computing polje u razvoju kompjuterske nauke, ideja postoji već nekoliko godina. Naziva se cloud computing zato što podaci aplikacije postoje na "oblaku" Web servera. Istraživači koji traže pametnije načine da bi obavili najkomplikovanije

kompjuterske zadatke misle da su pronašli odgovor u oblacima, ali ne one vrste koje sežu nebom i sastoje se od vodenih kapljica i smrznutih kristala. Umesto toga, okrenuli su se nečemu nazvanom cloud computing, čiji je cilj pružanje super kompjuterske moći preko Interneta.

Svake decenije, kompjuterska industrija menja prioritet za softverom koji je smešten na jednom mestu i softver koji se umesto toga nalazi na korisničkim računarima. To je uvek odluka o ravnoteži, ali današnje kombinacije visoko brzih mreža, boljih PC grafičkih procesora, i brzih jeftinijih servera i disk prostora su okrenuli inženjere prema izvršenju većeg broja obrada podataka u data centrima. U ranom delu ove decenije istraživači su se založili za sličan centralizovani pristup, nazvan "Grid Computing". Ali cloud computing projekti razvijeni u poslednjim godinama su moćniji od grid sistema.

IBM je jedna od vodećih kompanija koja objavljuje planove za korišćenje Cloud Computing tehnologije. IBM direktori u Šangaju su otkrili sistem nazvan blue cloud, koji će omogućiti bankama i drugim korisnicima distribuciju programa kroz veliki broj mašina za izvršenje brzih, komplikovanijih analiza podataka. Prvi blue cloud produkti su objavljeni u proleće 2008. godine.

Dve vrhunske internet kompanije su objavile slične projekte. Yahoo kaže da će Carnegie Mellon University i eventualno druge škole koristiti 4000 procesorski kompjuter postavljen u Web kompaniji za obavljanje softverskih istraživanja. I Google, upravljajući se efikasnošću jednog od svetskih najvećih super računara korišćen za pokretanje njihovog pretraživačkog pogona, kažu da će napraviti hiljade procesora u njihovim data centrima dostupnim školama uključujući univerezitete u Vašingtonu, Stanford univerzitetu i MIT-u da bi pomogli učenje računarskih programskih tehnologija visokih performansi.



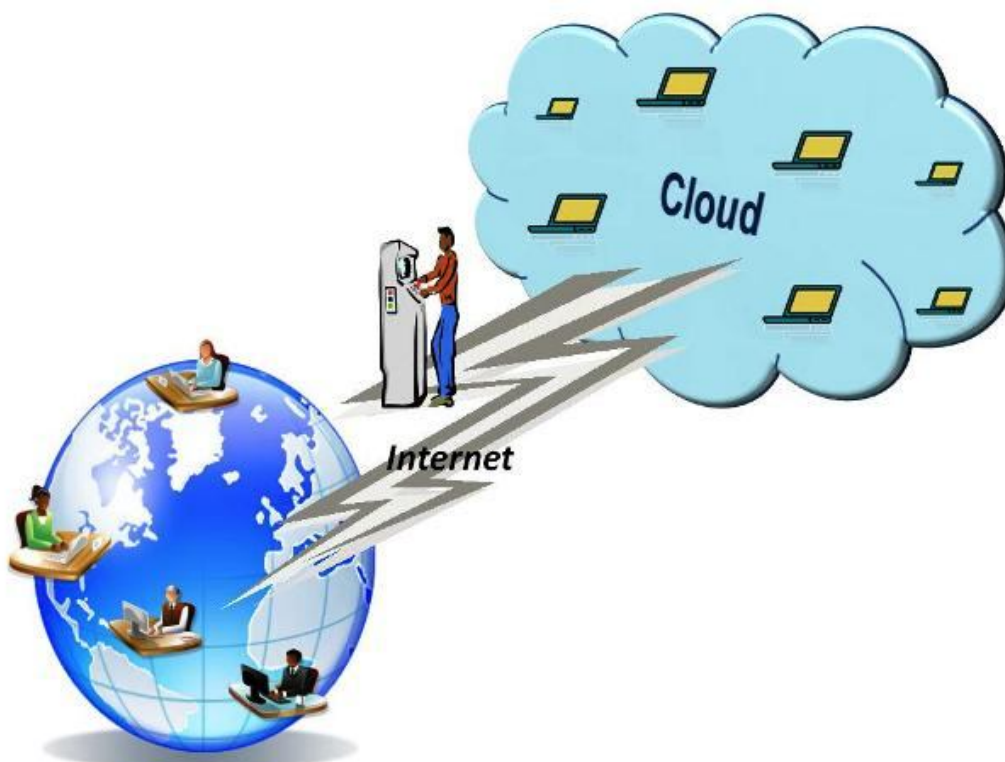
Slika 4: Prikaz korišćenja cloud computing-a od strane korisnika. [4]

Mnogi dugogodišnji istraživači super računara kažu da su ovo primeri tenzija oko cloud computing-a. Upotpunujući ovu tenziju, sledi, povećanje vrlo brzih internet konekcija, jeftiniji moćniji čipovi, jeftiniji i veći hard diskovi i razvijanje data centara koji sadrže stotine i hiljade kompjutera za brže pružanje boljih programa velikom broju korisnika. Ništa od ovoga ne bi bilo moguće decenijama ranije.

Google pretrživački pogon i produktivne aplikacije su izmedju ostalog najraniji proizvodi u pokušaju za pronalaženje moći obrade na ogromnim bankama kompjuterskih servera, umesto na jednom desktop PC-ju. Microsoft je izdao online program nazvan Windows

Live za deljenje slika, smeštanje fajlova i drugih aplikacija serviranih iz novih data centara. Yahoo je preuzeo slične korake. IBM je podvrgnuo 200 istraživača svom cloud computing projektu. I Amazon.com je skoro omogućio pristup za proizvođače softvera njihovom "Elastic Compute Cloud" servisu, koje omogućuje malim softverskim kompanijama plaćanje za pokretanje obrade koji teče iz Amazon-ovih data centra podataka.

2.4 Teorijske osnove problema - Kako Cloud Computing radi?

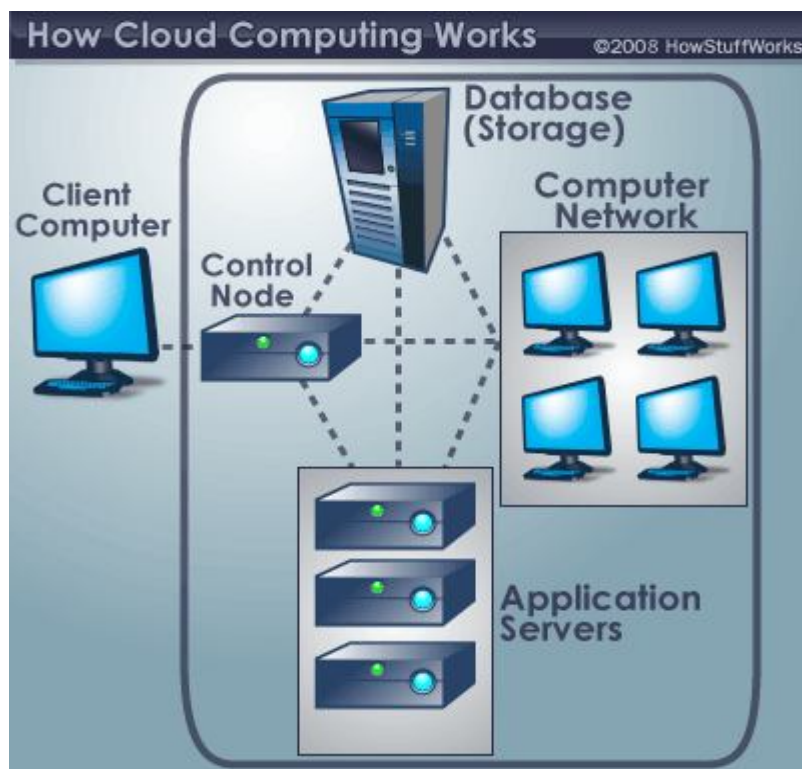


Slika 5: Cloud computing. [4]

Super računare danas uglavnom koristi vojska, vladine obavestajne službe, univerziteti, istraživačke laboratorije i velike kompanije za izvršenje ogromno kompleksnih računanja za zadatke kao što su simulacija nuklearne eksplozije, predviđanje klimatskih promena, dizajniranje aviona i analize koji proteini u telu se slažu sa potencijalnim novim lekovima. Cloud computing uspeva da pruži ovakav tip moći, izvršenje desetina trilijona računica po sekundi za probleme kao što su analiza rizika u finansijama, pružanje ličnih medicinskih usluga, čak i pokretanje zahtevnih kompjuterskih igara, na taj način da korisnici mogu koristiti kroz Web. To se radi umrežavanjem velikih grupa servera koji često koriste jeftinu potrošačku PC tehnologiju, sa specijalizovanim konekcijama za širenje obrade podataka putem njih. Poredjenja radi, novi i najaci kućni PC računari izvršavaju samo oko tri biliona računica u sekundi.

Zamislite da ste direktor velike korporacije (kompanije). Jedna od vaših odgovornosti uključuje da obezbedite da svi zaposleni imaju pravi hardver i softver koji im je potreban da bi obavljali svoje poslove. Kupovina računara za svakog nije dovoljna, takodje morate

za svakoga da naručite softver ili softversku licencu da bi zaposlenima obezbedili potrebne alate. Kada zaposlite novog radnika morate da kupite dodatni softver ili da budete sigurni da vaša trenutna softverska licenca omogućuje dodatno korišćenje softvera. Neki u šali kažu da je to toliko stresno da neće te moći mirno da spavate na velikoj količini vašeg novca. Uskoro, biće alternative za direktore. Umesto instalacije softvera na svakom računaru, treba samo da učitate jednu aplikaciju. Ta aplikacija će omogućiti radnicima da pristupe servisima zasnovane na Web-u koje hostuju sve programe koje su korisniku neophodni da bi obavio posao. Udaljeni računari u vlasništvu drugih kompanija će izvršavati sve od e-maila do obrade teksta, kao i programe za kompleksne analize podataka. To se naziva cloud computing i to može promeniti celu kompjutersku industriju.



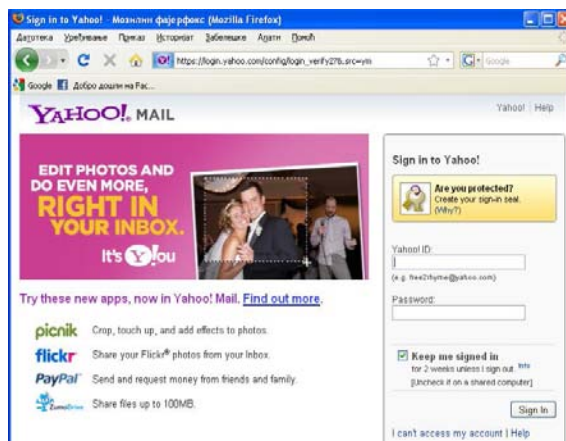
Slika 6: Kako cloud computing radi? [4]

U cloud computing sistemu postoji značajan napredak u radu. Lokalni računari ne moraju više da izvršavaju teške poslove prilikom izvršavanja aplikacija. Mreža računara koje kreira oblak obavlja te poslove umesto lokalnih računara. Hardverski i softverski zahtevi na strani korisnika se smanjuju. Jedina stvar koju korisnik računara mora da ima da bi mogao da radi u cloud computing sistemima je softverski interfejs, koji može biti običan Web Browser, a cloud computing mreža obavlja sve ostalo.

Postoje velike šanse da već koristite neku formu cloud computing-a. Ako imate e-mail nalog sa web baziranim e-mail servisima kao što su Hotmail, Yahoo!Mail ili Gmail, već imate neko iskustvo sa cloud computing-om. Umesto izvršenja e-mail programa na vašem računaru, vi prilazite web e-mail nalogu udaljenom od vas. Softver i skladišni prostor za vaš nalog ne postoji na vašem računaru, on je na servisima kompjuterskog oblaka.



Slika 7: Gmail



Slika 8: Yahoo mail

2.5 Koje su tržišne mogućnosti za ovu tehnologiju?

Dok je procenu teško pronaći, potencijalno upotreba je rasprostranjena. Umesto korišćenja relativno male grupe visoko obučanih korisnika, cilj cloud computing je da super izračunavanja omogući svima. Tehnologija može biti upotrebljena za analizu razgovora na sastancima, a zatim da predvidi šta radnicima sa podacima sledeće može zatrebati. Google i ostali takođe grade online servise za pružanje potrošačima većeg pristupa informacijama koje bi pomogle vođenju njihove brige o zdravlju.

2.6 Šta su najveći izazovi sa kojima se ove kompanije susreću?

Tehnički standardi za povezivanje različitih kompjuterskih sistema i delovi softvera potrebnih za rad cloud computinga još uvek nisu kompletno definisani. To može usporiti napredak novih proizvoda. Za široko pojasnim probojem SAD-a još uvek zaostaju mnoge zemlje u Evropi i Aziji, i bez brzih konekcija, posebno bežičnih, cloud computing servis neće biti široko dostupan. Čuvanje velike količine podataka o korisničkim indetitetima i prioritetima izaziva nove brige o zaštiti privatnosti.

3 Rešenje i implementacija

3.1 Cloud Computing: Evolucija Programa-kao-Sevisa (Software-as-a-Service)

Kada uključite toster, verovatno ne razmišljate o tome ko generiše elektrone koji ga napajaju. Isto kao što vas verovatno ne interesuje koliko daleko ti elektroni putuju do vas i šta je njihov izvor: ugalj, nuklearna energija, hidro energija, solarna ili neka druga.

Vi zaista nemate potrebe da znate detalje o snabdevanju električnom energijom. Osim toga električno napajnje je oko nas više od 100 godina, koja putuje preko mreže koja se vrlo malo promenila tokom vremena, sa retkim izuzecima, prilično možete da verujete da će te imati električnu energiju kad god vam je potrebna.

Danas, velike kompjuterske kompanije se nadaju da ste proizvođač sa sličnim odnosom prema kompjuterskom kapacitetu.

Sledeća velika nadogradnja vašeg komporativnih sistemskih odeljenja (odseka) može biti nešto što će te uvek koristiti ali nikada nećete videti. To može biti "Cloud Computing", sledeći korak u evoluciji Software-as-a-Service (SaaS) tehnologije.



Slika 9: SAAS tehnologija. [4]

Kroz SaaS, kompanije mogu da pridju aplikacijama i velikoj količini virtualne računarske moći bez kupovine istih. Umesto toga aplikacije su hostovane od strane drugih kompanija, što ih oslobađa glavobolja održavanja i većine troškova podešavanja za korisnike. Neke SaaS aplikacije mogu da funkcionišu putem konekcije izmedju samo dva ili tri računara.

Haluk Demirkan, profesor informacionih sistema na W.P.Caery poslovnoj školi kaže da cloud computing predstavlja "mnogo veću skalu implementacije". On objašnjava da "Sada pričamo o hiljadama računara" povezanih zajedno putem intereneta ili nekih drugih mreža.

Ako dobijete Gmail nalog na Google-u, vi pristupate aplikaciji putem SaaS modela. Ali, kada univerzitet Arizone sklopi ugovor sa Google-om za e-mail naloge za više od 50 000 studenata poslednje godine, igra prelazi sa SaaS na cloud computing-u. Zasto?

Google upravlja infrastrukturom i softverskim aplikacijama. Dobijate svu funkcionalnost ali nemate glavobolje izazvane radom IT infrastrukture kod vas. Nema nadogradnje, nema produženja ugovora, nema sigunosnih problema. Provajder održava vaš servis, plaćate zavisno do toga koliko koristite servis.

Zašto se ovaj model naziva cloud computing? Neki kažu da je to zato to što se kompjuterska funkcionalnost izvršava negde "u oblacima".



Slika 10: Izvršavanje operacija u oblacima. [4]

Eksperti Wikipedie tvrde da termin dolazi iz činjenice da mnogi tehnološki diagrami opisuju internet ili IP strukturu koristeći crtanje oblaka.

Po analitičarima u Gartner-u, vodećoj IT istraživačkoj kompaniji do 2011. godine, rana tehnološka usvajanja će se odreći kapitalnih troškova i umesto toga naruči će 40% njihove IT infrastrukture u vidu servisa. Povećanje brzih konekcija omogućuje praktično korišćenje infrastrukture na drugim mestima i idalje će dobijati rezultate u željenom vremenskom periodu. Preduzeća veruju da kako servisno-orijentisana arhitektura (SOA) postaje sve češća, cloud computing će se baviti odvajanjem aplikacija sa specifične infrastrukture.

3.2 Postave

3.2.1 Prva postava

IBM-a kaže da za poslovnu osobu, koja želi da razvije novu soluciju, većinu vremena i energije potroši na definisanju prave infrastrukture hardvera i softvera da bi kreirala tu soluciju. Cloud computing omogućuje ljudima da dele resurse da bi rešili nove probleme.

IBM sreće iste izazove koje sreće bilo koji biznis. Ustvari, sa oko 370 000 zaposlenih u 170 zemalja, sama kompanija je kompleksnija od poslovnih korisnika kojima služi.

Big Blue je lansirao svoju "Blue Cloud" inicijativu. Deo toga uključuje unutrašnje cloud computing okruženje, koje je Vayghan, istraživač, koristio na više projekta prošle godine. U IBM-u je povećana produktivnost, vreme potrebno za razvijanje i uručivanje solucije na nešto više od 50% u odnosu na ranije projekte zahvaljujući "Blue Cloud"-u.

Koristi se deljivo okruženje, vreme koje se potroši na bilo kom projektu za dobijanje hardvera i softvera za njihovo konfigurisanje i rukovodjenje sistemom je daleko manje, što ubrzava inovacije.

3.2.2 Druga postava

Nije cloud computing samo brži način dobijanja informacione tehnologije već je jeftinije i efikasnije.

Ako kupite server i ako on radi ceo dan ali ga vi ne koristite, ne možete da sačuvate računarski sistemski kapacitet i da ga koristite kasnije. To je gubitak, ali to se dešava kada kompanije naruče svoju IT infrastrukturu i ne koriste je 24 sata dnevno 7 dana u nedelji sa 100% iskorišćenosti. Sa cloud computing-om kompanije nemaju te troškove, i nemaju besposlene sate za traćenje njihovih IT resursa.

Kao dodatak infrastrukturnim resursima (hardver, softver, prostor) , ovi resursi uključuju ljude koji upravljaju sistemom, kao i IT obezbeđenje. Sa Cloud Computingom, troškovi IT operacija kompanija značajno opadaju.

3.2.3 Treća postava

Tu je i deljivi kapacitet ovog modela. Business week je objavila izveštaj da današnji super kompjuteri manipulišu "desetinama trilijona operacija po sekundi" i "cloud computing ima za cilj da upotrebi tu vrstu moći" u poslovnim problemima. Vrhunski "desktop PC računari obrađuju samo oko 3 biliona operacija po sekundi". Kroz cloud computing, kapacitet vašeg računara drastično raste i vi i dalje možete da se spojite na to sa vašeg PC-a koristeći internet konekciju.

3.3 Dobijanje oblika

Bez iznenadjenja, IT specijalisti nadgledaju mogućnosti u cloud computing-u. Izvršni direktor Google-a Eric Schmidh je nazvao ovakvu obradu podataka transformativnom, to je novi model kompjuterske arhitekture.

Vayghan iz IBM –a kaže "to nije nešto što će doći za dvadeset godina. Već postoji veliki broj proizvoda."

Neki proizvodi će doći iz Vayghan-ove kompanije. Zadnjih godina, IBM je obezbedio cloud computing servise kao sto su China Telecom, Wuksi Monicipal Goverment Of China, Ministarstvo nauke i tehnologije Vijatnama i druge.

IBM je takodje lansirao "Blue Code", serija cloud computing ponuda , i time je ušla u savez za cloud computing programe sa velikim brojem partnera širom sveta kao što je Google. Ove dve kompanije su se odružile da bi obezbedile hardver, softver i servise koji će unaprediti univerzitetski nastavni plan univerziteta SAD-a. Nadaju se da će njihova ulaganja pomoći istraživanje ovog razvojnog modela obrade podataka i da će obučavati sledeće generacije proizvođača aplikacija da rade sa njim.

Google se takodje udružio sa Salesforce.com za proizvodnju kombinovanog produkta koji će sadržati produktivne alate Google aplikacija i sposobnost upravljanja potrošačima koje pruža Salesforce.

Amazon takodje ulazi u cloud biznis. On sada ima novo odeljenje koje, po podacima sa kompanijinog web sajta, obezbedjuje "pristup Amazon-ovoj ogromnoj infrastrukturi lako i jeftino". Na njihovom sajtu takodje postoje informacije da je Amazon potrošio više od dva biliona dolara izgrađujući takvu infrastrukturu. Koliki broj kompanija može da uradi takvu stvar? Cloud computing će pomoći velikom broju malih i srednjih kompanija. Umesto trošenja miliona i meseca rada izgrađujući njihovu sopstvenu infrastrukturu, cloud computing omogućuje malim kompanijama da uđu u infrastrukturu gigantskih kompanija. To daje malim kompanijama istu obradu podataka koju imaju gigantske kompanije i veliki broj realnih benificija. Te benificije uključuju troškove upotrebe hardvera (kao što su upotreba po potrebi, korist obrade podataka, cloud computing, softverski orijentisana infrastruktura), softver (Software-as-a-Service, softversko orijentisana arhitektura) i poslovne procese.

Kada, šta i kako će organizacije uraditi da bi pomerili svoju IT infrastrukturu u cloud computing svet? Koji su najbolji potezi? Kako mogu da evoluiraju uspešno? To je trenutni istraživački program rada.

Trenutni krajnji rezultat:

- Software-as-a-Service evoluirao. Cloud computing je u usponu.
- Sa SaaS, cloud computing potrošači ulaze u kompjuterske resurse sa strane u drugim kompanijama. Razlika je u razmeri. Cloud computing platforme mogu kombinovati hiljade računara i mreže za skladištenje podataka kao što je Backup, između ostalih stvari.
- Benificije cloud computing-a uključuju niže cene, brži razvoj i pristup jačim računarskim resursima.
- Velike igrače u oblacima uključuju IBM, Google i Amazon Web Services.

Kako će ekspanzija Google cloud computing servisa promeniti digitalni svet?

Da bi znali kako ćete koristiti računar i Internet narednih godina, poučno je razmotriti Google-ove radnike: većina njihovih programa i podataka, od slika i videa, do prezentacija i e-mail-a, nalazi se na Webu. To predstavlja digitalne stvari koje su bitne za njih, jednako pristupačne sa kućnog računara i javnog internet kluba, ili telefona sa web mogućnostima. To čini oštećenje hard diska manje bitnim.

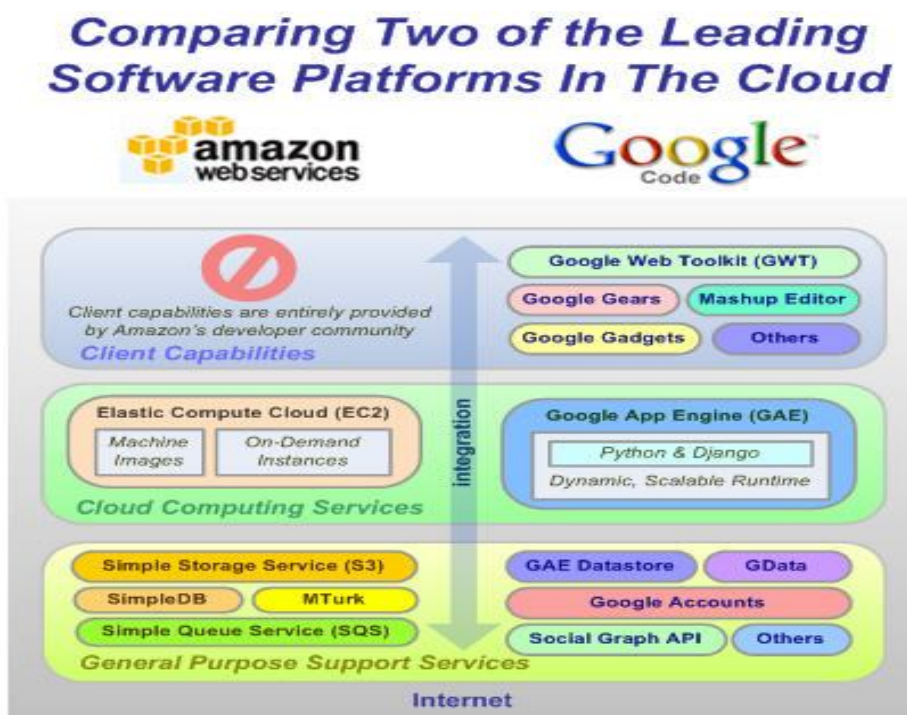
Pre izvenog vremena, Sam Shillace, direktor inženjeringa Google-a, imao je potrebu za reformatiranjem oštećenog hard diska sa računara koji je koristio najmanje 6 sati dnevno. Reformatiranje, koje kompletno briše podatke sa hard diska, izazvao bi paniku kod mnogih ljudi ali i ne kod Shillacea. On je rekao "Na njemu nema ničeg bitnog" što nije dostupno na Web-u.

Shillaceov digitalni život, najvećim delom, postoji na interenetu. Google već dozvoljava ljudima prebacivanje nekih njihovih personalnih podataka na interenet i korišćenje njihovog web baziranih programa. Google Calendar organizuje događaje, Picaso čuva slike, You Tube sadrži video, Gmail čuva e-mailove, i Google Docs sadrži dokumenta i prezentacije.

Od kompanije se očekuje mnogo više narednih godina, gde će aktivirati servis koji će ljudima omogućiti smeštanje sadržaja kompletnog hard diska online. Google je siguran da takav servis još uvek ne postoji. Kompanija kaže "Skladišni prostor je bitna komponenta izrade web aplikacije koji potrošači rado prihvataju... Mi stalno slušamo naše korisnike i

tražimo način za nadogradnju i poboljšanje naših web aplikacija, uključujući opciju smeštanja podataka, ali trenutno nemamo šta da ponudimo.” Sve do sada, mnogi ljudi u industriji veruju da će Google spojiti svoje razdvojene cloud computing ponude u veliki opšti servis, i ljudi su željni za shvatanje posledica takvog projekta.

U stvari, Google nije jedina kompanije koja investira u online skladišćenje prostora i Cloud Computing. Postoje i drugi servisi koji nude značajnu količinu softvera i prostora u oblaku. Amazonov Simple Storage Service, na primer, nudi neograničen i jeftin skladišni prostor (0,15\$ za 1GB mesečno). AOL obezbeđuje servis nazvan Xdrive sa kapacitetom od 50 GB za 9,95\$ mesečno (prvih 5GB su besplatni). Microsoft nudi Windows Live SkyDrive, trenutno u beta verziji, sa 1GB besplatnog skladišnog prostora.



Slika 11: Poređenje između dve softverske platforme u cloud-u. [4]

Google je u boljoj poziciji od drugih za puštanje cloud computing-a u javnosti, izjavljuje Thomas Vander Wal, osnivač Infocloud Solutions, cloud computing savetnik. Prvo, milioni ljudi već koristi Google online servise i čuva podatke na njegovim serverima kroz softver. Drugo, Vander Wal kaže da kultura u Google omogućava njegovom timu da lakše spoji delove cloud computing, a koji danas deluju prilično razbacano. On napominje da Yahoo, Microsoft i Apple takodje imaju veliku količinu personalnih informacija i online aplikacija, ali da postoji barijera unutar svake organizacije koja može usporiti proces integracije tih delova. Po rečima Vander Wala ”to može značiti da je Google prešao ivicu u kojoj se svi drugi ostaju zaglavljani neko vreme”.

Jedno od mesta gde Google, posebno, može ostvariti veliki uticaj je integracija cloud computing-a u mobilne uređaje. Kompanija je u skorije vreme objavila Android, platforma koja omogućuje ljudima izgradnju softvera za razne mobilne uređaje. Savez može podstaći kreiranje mobilnih aplikacija okrenutih ka cloud computing-u. Ljudi žele da bezbolno prebace podatke između računara, weba i telefona. Ako je Google počeo sa rešavanjem ovog dela problema, ovo može imati uticaj zbog toga što to još uvek niko nije uradio.

Objedinjena teorija cloud computinga nije tako prosta kao pisanje softvera, postoji veliki broj socijalnih i legalnih problema koji mogu da budu rešeni. Jimmy Lin, profesor računarskih nauka na Maryland univerzitetu kaže da je najveći problem privatnost korisnika. To će postati veoma bitno ukoliko Google bude prikazivao reklame vezane za personalne informacije kao što rade u Gmail-u. Zavisno od informacija korišćenih za izbor reklama neki ljudi se mogu osećati nelagodno. Različiti ljudi se osećaju različito u vezi bezbedonosnih faktora, ljudi se i dalje osećaju nelagodno u vezi ovoga. Osim toga, Google mehanizmi enkripcije nisu bez mane. Postoje priče da su ljudi pristupali u Gmail-u i koristili tuđe naloge. Uverenje nije dovoljno za rešavanje ljudskih strahova. Sve što je potrebno je jedan incident da bi ljudi bili nezadovoljni.

Osim toga tu je razgraničavanje autorskih prava u cloud computing-u. Jedna od prednosti cloud computing-a je što smešteni podaci mogu lako biti deljeni sa drugim ljudima, ali deljenje fajlova kao što su muzika i filmovi sa autorskim pravima je generalno ilegalna. Lin tvrdi da je u nekim slučajevima nejasno da li prosto čuvanje informacija u cloud computing-u narušava autorska prava. Na primer, nad podacima koji se koriste za istraživanja postojí zabrana kopiranja na računare izvan Maryland univerziteta. Tu je problem u kome je pravna politika zaista ostala u pozadini.

Takođe tu su sumnjivi problemi konstantne veze: online podaci nisu korisni ukoliko nije moguće ostvariti internet konekciju, ili ako je veza loša. Internet postaje sve pristupačniji non stop, ali se kompanije ipak plaše današnjih tehničkih izazova obezbeđivanja servisa web aplikacijama bez prekida. To je glavni problem, ali postoji nekoliko načina za rešavanje tog problema. Google nudi softver za preuzimanje po imenu Gears koji se ponaša kao keš za podatke kada osoba koristi web aplikacije offline. Kada osoba ostvari internet pristup, Gears automatski izvršava sinhronizaciju i snima rad na server. Tim ljudi radi na integrisanju ove vrste mogućnosti u Google Docs.

Microsoft izbliza nadgleda Google poteze, i ima sopstveni pristup za koji misli da je bliži rešavanju nekih cloud computing izazova. To nije samo online svet, to treba da bude online-offline kombinacija, i solucija koja pobeđuje je ona koja oba posla uradi najbolje. Microsoft gradi softver, koji će omogućiti ljudima da čuvaju neke od njihovih fajlova na hard diskovima, čuvajući privatnost, dok će istovremeno omogućiti udaljeni pristup tim fajlovima. Navodno, količina skladišnog prostora neće biti toliko bitna kao doživljaj korisnika.



Slika 12: Microsoft google cloud. [4]

Ipak, postoji osećaj da Google verzija cloud computing-a poziva na jednostavnost, uprkos trenutnim izazovima. Pomerajući podatke i aplikacije na internet, Google pomaže nestajanje računara. Svaka generacija aplikacija odvaja jedan sloj kompjutera. Ljudi su u početku radili na računaru koristeći komandne linije, a zatim koristeći grafički interfejs, sada ljudi mogu da rade većinu posla u web browseru, koji može biti na personalnom računaru ili malom ručnom uređaju. Radi se o odbacivanju računara da bi mogli da radimo sa drugim ljudima i da delimo informacije.

3.4 Cloud Computing arhitektura

Kada pričamo o cloud computing sistemima, lakše nam je da izvršimo podelu u dve sekcije: front end i back end. Međusobno su konektovani putem mreže, najčešće internetom. Front end je strana korisnika kompjutera, odnosno klijenta. Back end je "Cloud" sekcija sistema.

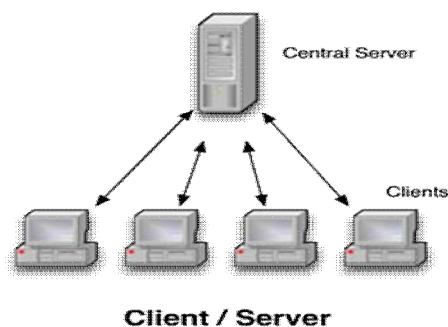
Front end uključuje klijentski računar (ili računarsku mrežu) i aplikaciju neophodnu za pristup cloud computing sistemu. Nemaju svi cloud computing sistemi isti interfejs. Servisi kao web bazirani e-mail programi koriste postojeće web browsere kao što su Internet Explorer ili Mozilla Firefox. Drugi sistemi imaju jedinstvene aplikacije koje obezbeđuju mrežni pristup klijentu.

Većinu vremena serveri ne rade u punom kapacitetu, to znači da postoji neiskorišćena procesorska snaga. Moguće je prevariti fizički server da se ponaša kao da su upitanju više servera, od kojih svaki izvršava sopstveni operativni sistem. Ta tehnika se naziva server virtualizacija. Povećavajući rezultat individualnih servera, server virtualizacija smanjuje potrebu za više fizičkih računara (mašina).

Na Back End-u nalaze se razni računari, serveri i sistemi za skladištenje podataka koji kreiraju "Cloud (oblak)" računarskih servisa. U teoriji, cloud computing sistem može sadržati bilo koji kompjuterski program koji možete da zamislite, od obrade podataka do video igara. Često, svaka aplikacija ima sopstveni namenski server.

Centralni server upravlja sistemom, nadgleda saobraćaj i klijentske zahteve da bi obezbedio da sve funkcioniše stabilno. Sledi set pravila, nazvanim protokolima i koristi specijalnu vrstu softvera nazvanog Middleware. Middleware omogućuje mrežnim računarima međusobnu komunikaciju.

Ako cloud computing kompanija ima veliki broj klijenata, verovatno će biti velikih potreba za velikim prostorom za skladištenje podata. Neke kompanije zahtevaju stotine uređaja za skladištenje podataka. Cloud computing sistemi zahtevaju dva puta veći broj uređaja za skladištenje podataka za čuvanje klijentskih informacija. To je zato što se ovi uređaji kao i računari, često kvare. Cloud computing sistem mora praviti kopiju svih klijentskih informacija i čuva je na drugim uređajima. Te kopije omogućuju centralnom serveru pristup rezervnim mašinama za dobijanje podataka koje drugačije nebi bili dostupni. Kreiranje kopije podataka u vidu rezerve kopije se naziva redudancija.

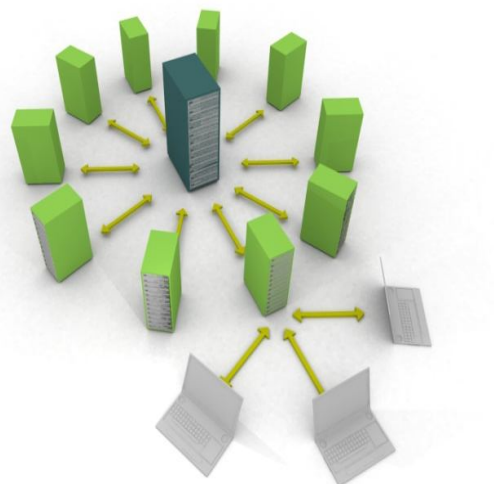


Slika 13: Centralni server [4]

Cloud computing je tesno vezan za grid computing i utility computing. U grid computing sistemu mrežni računari su u mogućnosti da pristupaju i koriste resurse svakog računara u mreži. U cloud computing sistemu to se jedino često dešava u Back End-u. Utility computing je poslovni model u kome jedna kompanija plaća drugoj kompaniji za pristup računarskim aplikacijama ili skladištenju podataka.



Slika 14: Grid computing [4]



Slika 15: Utility computing [4]

3.5 Cloud Computing aplikacije

Aplikacija cloud computing-a su praktično ne ograničene. Sa pravim Middleware programima, cloud computing sistem može izvršiti sve programe kao i normalan računar. Potencijalno, sve od generičkih programa za obradu teksta do računarskih programa dizajniranih po specifičnim potrebama kompanije.

Neke od kompanija koje istražuju su najveće kompanije kompjuterske industrije. Microsoft, IBM, Google investiraju milione dolara u razvoj. Neki ljudi misle da Apple može istražiti mogućnosti proizvodnjom interfejsnog hardvera za cloud computing sisteme.

Zašto bi bilo ko želeo da se osloni na druge računarske sisteme za izvršenje programa i čuvanje podataka?

Iz sledećih razloga:

-Klijenti bi mogli da pristupe njihovim aplikacijama i podacima sa bilo kog mesta u bilo kom trenutku. Oni mogu da pristupe cloud computing sistemu koristeći bilo koji računar povezan na Internet. Podaci ne bi bili vezani za hard disk računara korisnika kao ni za internu mrežu kompanije.



Slika 16: Dostupnost cloud computing-a. [4]

-To može smanjiti cenu hardvera. Cloud computing sistemi mogu smanjiti potrebu za naprednim hardverom na klijentskoj strani. Vi nećete imati potrebu da kupite najbrži računar sa najvećom količinom memorije, zbog toga što će cloud computing sistem preuzeti brigu o tome umesto vas. Umesto toga kupićete jeftini računarski terminal. Terminal uključuje monitor, ulazne uređaje kao što su tastatura i miš i sasvim onoliko (i računar dovoljan za izvršenje) procesorske moći koliko je potrebno za izvršenje Middleware-a, potrebnog za konektovanje na cloud computing sistem. Neće vam trebati veliki hard disk jer će svi vaši podaci biti sačuvani na udaljenom računaru.



Slika 17: Smanjenje troškova. [4]

-Korporacije koje se oslanjaju na računare moraju da budu sigurne da poseduju adekvatan softver za postizanje svojih ciljeva. Cloud Computing sistemi daju tim kompanijama širok pristup računarskim aplikacijama. Te kompanije ne trebaju da kupuju set softvera ili softverskih licenci za svakog radnika. Umesto toga, kompanije plaćaju honorarne troškove cloud computing kompanijama.

-Serveri i uređaji za čuvanje podataka zauzimaju prostor. Neke kompanije iznajmljuju fizički prostor za čuvanje servera, zbog toga što nemaju dovoljno prostora kod sebe. Cloud computing daje tim kompanijama opciju čuvanja podataka na tuđem hardveru, uklanjajući potrebu za fizičkim prostorom kod tih kompanija.



Slika 18: Serverska prostorija. [4]

-Kompanije mogu uštedeti novac na IT podršci. Hardver u cloud computing sistemu, u teoriji, ima manje problema od mreže heterogenih računara i operativnih sistema.

-Ukoliko back end cloud computing sistema predstavlja grid computing sistem, klijenti mogu koristiti prednost cele mreže računara. Često, naučnici i istraživači rade sa toliko kompleksnim kalkulacijama da bi individualnim računarima bile potrebne godine da kompletiraju kalkulacije. Na grid computing sistemu, klijent može poslati kalkulaciju na obradu cloud computing-u. Cloud sistem će iskoristiti moć svih dostupnih računara čime će značajno ubrzati kalkulaciju.

Cloud computing može pretvoriti kućne računare u proste terminale. Na neki način to je korak unazad. Prvi računari su uključivali korisničke terminale povezane kablovima. Svaki terminal je imao računarski monitor i tastaturu, ali su oni služili samo za pristup glavnom računar. Nije bilo načina za čuvanje informacija na terminalu.

4 Prednosti Cloud Computing-a

4.1 IBM i klijenti i izvlače korist od Cloud Computinga

IT-rukovodiocima danas može biti oprošteno ako ih optuže da su njihove glave u oblacima. To je zato, jer oblaci koji interesuju IT rukovodioce danas nisu meteorološki, oni su oblaci računarstva. Rasprostranjena zainteresovanost i čak nepostiđena pobuda o cloud computing-u proizilazi iz firmi, vladinih agencija i drugih organizacija koje traže više dinamičnije, elastičnije i ekonomičnije IT sisteme nego što je prethodna generacija tehnologije to dozvoljavala.

Iako termin "oblak" može označiti prolaznim kvalitetom tip računara koji on opisuje, prednosti cloud computing-a klijentima su veoma stvarni. Sam IBM, kao i klijenti širom

sveta usvajaju cloud computing prepoznavajući njegov potencijal u uvođenju u novu eru pouzdanosti, efektivnosti i efikasnosti u IT isporuci usluga.

Cloud computing je stil računarstva čiji temelj je isporuka usluga, softver i kapacitet procesa koristeći privatne ili javne mreže. Fokus cloud computing-a je korisničko iskustvo, a suština je da izdvoji isporuku računarskih usluga iz osnovne tehnologije. Iza korisničkog interfejsa, tehnologija iza cloud-a ostaje nevidljiva za korisnika, što čini cloud computing neverovatno prijateljski nastrojeno ka korisniku. Cloud computing je pristup u nastanku deljenoj infrastrukturi u kojoj se u veliki delovi sistema međusobno povezani u privatne ili javne mreže radi pružanja IT usluga. Potreba za takvim sredinama je podstaknuta dramatičnim rastom povezanih uređaja, tokovima podataka u realnom vremenu i usvajanjem servisno-orijentisana arhitekture i web2.0 aplikacija, otvorene saradnje, društvene mreže i mobilne trgovine.

Konstantni napredak u performansama digitalnih komponenata rezultira masivnim porastom u obimu IT okruženja, izražavajući potrebu da se upravlja njima, kao jedinstvenim oblakom. Cloud computing predstavlja sledeću fazu u logičnoj evoluciji u isporuci IT usluga, gradeći na prethodnim inovacijama koje uključuju grid computing, utility computing i computing na zahtev koji su prvi osmišljeni od strane IBM-a.

U početku, IBM je prepoznao potencijal cloud computing-a da dramatično poboljša ne samo način kako predati svojim klijentima IT usluge, već i kako bi cloud computing modernizovao i poboljšao način na koji IBM-a ispunjava svoje unutrašnje zahteve za IT resursima. Kao rezultat toga, IBM je delovao agresivno i uspešno u sopstvenom poslovanju za implementaciju cloud computing-a kroz svoju organizaciju.

Zahvaljujući cloud computing-u, IBM je u stanju da brzo odgovori na potrebe kupaca na mnogo isplativiji način. Na primer, cloud computing je omogućio IBM-u da ponudi kupcima izuzetno fleksibilno, skalabilano rešenje za vrhunske periode prilikom obrade zahteva koji daleko prevazilaze ono što interni resursi kupaca mogu da smeste. Ovo je IBM računarstvo na zahtev usluga u kojoj clouds omogućavaju IBM-u da se snadbe serverima, skladištima i umrežavajućim mogućnostima u roku od par sati od kupčevog zahteva za kapacitetom. Zahvaljujući cloud computing-u, IBM računarstvo na zahtev služba je izašla u susret potrebama kupaca više nego što je to ranije bilo moguće.

Slično tome, IBM je bio u mogućnosti da značajno unapredi produktivnost svog Evropske Benchmark centra, koji omogućava korisnicima da testiraju da li se novi IT resursi ponašaju kao što bi trebalo. Sa cloud computing-om, obezbeđivanje resursa za korisnike Benchmark Centra je zgusnuto u jedan dan umesto sedmice ili više. Ovo je drastično uvelo kapacitet centra i znatno je skraćen ciklus prodaje, direktno doprinoseći krajnjoj liniji IBM-a.

IBM-ov Watson I Ciriški istraživački centri prihvatili su cloud computing da bi rasporedili i kompletirali mnogo više projekata nego što bi to ranije bili u mogućnosti da preduzmu. Umesto uobičajenih dve nedelje potrebnih za zahtev, raspored i odredbu posebnog softvera za istraživački projekat, cloud computing dozvoljava im da rezervišu IBM resurse u brojnim udaljenim lokacijama u deliću vremena. Ovaj pogon je bolje korišćenje resursa, konsolidacija budžeta kapitala, kao i veća produktivnost.

Dolazak cloud computing-a ne dolazi prerano. Model za savremeni centar za podatke, koji je služio potrebama informacionih tehnologija organizacija godinama unazad, se suočava sa izazovima.

4.2 Centri za podatke u svetu koji se menja

Većina IT-rukovodioca prepoznaje da su osnovni principi organizovanja današnjih centara za podatke nadživela svoju korisnost i da je nova paradigma u nastajanju. Veoma su svesni određenih ranjivih tačaka u osnovi IT infrastrukture, ali se često toliko zauzeti sa trenutnim problemima tako da nemaju vremena i sredstava da formulišu rešenje na duže staze. Prema Gartner istraživanju od 2007 od 70 odsto od 1.000 globalnih organizacija očekuju da će morati značajno da promene svoje centre podataka pre 2012.

4.3 Izazovi sa kojima se konstrukcije trenutnih centara za podatke suočavaju:

- **Povećani troškovi radne snage** - IT-budžeti su veoma zategnuti zbog rastuće cene osoblja potrebnog za održavanje i upravljanje centara podataka. Administrativni troškovi za servere su skočili za 400 odsto od 1996, a sada čine najveće troškove u okviru centara podataka.
- **Visoka potrošnje energije** – Napajanje i troškovi za hlađenje centara podataka su porasli za 800 odsto od 1996, a eskalacijama troškova nema kraja na vidiku, a ipak resursi centra podataka imaju nisku iskorišćenost (ispod 20 odsto) . U narednih pet godina, industrije za nadzor predviđaju da će SAD centri za obradu podataka trošiti dvostruko više na troškove energije, kao i na hardver i dvaput onoliko koliko su do sada trošili na server za upravljanje i administrativne troškove. Štaviše, mnogi centri za podatke shvataju, da čak i ako su spremni da plate za više energije, ograničenja kapaciteta na startu znači da dodatna snaga nije dostupna.
- **Rastući zahtevi korisnika** - Danas se na zahtev društva pretpostavlja skoro univerzalni pristup podacima u realnom vremenu i analiza u elastičnom, bezbednom okruženju. Ništa manje od tog standarda je neprihvatljivo. Ovi zahtevi su vođeni povećanjem izvora podataka, mobilnih uređaja, sistema za identifikaciju radio-frekvencija, ujedinjenih komunikacija, web 2.0 servisom i tehnologijom, kao što je Mashups. Ovaj rast očekivanja takođe stvara zahteve centara za podatke koji IT administratori moraju zadovoljiti.
- **Haotični silosi podataka** – Previše često, današnji centri podataka su slučajni skupovi više hardverskih sistema, operativnih sistema i aplikacija koje su akumulirane tokom godina kao odgovor na zahteve različitih internih poslovnih jedinica. Ovi različiti sistemi su rasli bez preduzimljivog pristupa centru podataka koji je bio zasnovan na zajedničkom skupu ciljeva i standarda. Umesto toga,

sistemi su često bili posvećeni da izađu u susret specifičnim potrebama jedne poslovne jedinice ili funkcije procesa bez prikaza operativnosti sa ostatkom centra podataka ili potreba drugih delova organizacije. Često je rezultat centar podataka sa više verzija baze podataka, operativnih sistema i hardvera od različitih poslodavaca. Ovo okruženje može lako rezultirati hiljadama različitih sistema u centru podataka. Ovaj visoki stepen kompleksnosti ne samo da u velikoj meri povećava broj posvećenog tehničkog osoblja potrebnog da se reše problemi, takođe povećava rizik od prekida servisa.

- **Eksponencijalni rast obima podataka** - Porast broja uređaja, neotpornost, poboljšane performanse sistema, online trgovina i povećanje replikacije do sekundarne ili rezervne lokacije doprinosi dupliranju godišnje količine informacija koja se prenese preko interneta, prema istraživaču tržišta IDC-u. Svetska informacija, sirovina za baze podataka, je predviđena da se duplira svakih 11 sati dva puta do 2010 godine. Kao rezultat toga, više od trećine centara podataka u 2006. u bazi ima prijavljeno prekoračenje veće od terabajt veličine.

Skriveni troškovi u rešavanju ovih bolnih tačaka su poslovna inovacija. Pošto je potrebno da provedu veći deo svog dana popravljajući probleme to sprečava IT profesionalce da posvete vreme i sredstva razvojnim aktivnostima koje mogu istinski da promovišu inovacije i pravi potencijal centra podataka da guraju posao napred u nepredviđenim pravcima. Da bi se krenulo napred, prvo se mora drugačije sagledati kako infrastruktura sama sebi može da pomogne gurajući inovacije u poslovnu jedinicu. IT-rukovodioci moraju da promene svoj položaj u lidere koji mogu da donesu svojoj organizaciji novi nivo performansi i efikasnosti kroz IT, a takođe se fokusira na poboljšanje usluga, smanjenje troškova i upravljanje rizicima u porastu sve povezanijeg sveta.

IBM nudi kohezivnu strategiju za razvoj dinamičke infrastrukture, koja će podržati veliki broj zahteva koji dolaze na IT danas, dok se ujedno postavlja osnova za vrlo brzim, agilnim poslovnim okruženjem koje može da utiče ne različite vrste cloud computing-a. Cloud computing stvarno poboljšava poslovnu vrednost. Sa cloud computing-om, IT profesionalci mogu da posvete više energije za unapređenje vrednosti korišćenja IT za svoja preduzeća, a manje na dnevne izazove za IT.

4.4 Kako Cloud Computing sređuje ranjive tačke današnjeg IT okruženja

Cloud computing oslobađa organizacije isporuke IT usluga kao nikada pre.

Cloud omogućava dinamičku dostupnost IT aplikacija i infrastrukture, bez obzira na lokaciju.

Brže pružanje usluga rezultira mogućnostima od orkestriranja zadataka do kreiranja, konfigurisanja, snabdevanja i dodavanja računarske snage u IT podršku i poslovne usluge mnogo brže nego što bi bilo moguće sa današnjim računarskim infrastrukturama.

Poboljšana usluga ojačava napore za zadržavanje kupaca, kraće vreme na tržištu i horizontalno proširenje tržišta.

Cloud computing može da poboljša SOA, upravljanje informacijama i inicijativama za upravljanje servisom, koji takođe podržavaju inicijativu pružanja usluga.

Cloud computing takođe promoviše IT optimizaciju tako da su IT resursi konfigurisani za maksimalnu dobru cenu. To je moguće zato što cloud computing podržava velike skalabilnosti da zadovolji periode potražnje izbegavši produžene periode za iskorišćenje IT kapaciteta. Sa klikom miša, usluga se može brzo proširiti ili sažeti kao i remontovati bez potrebe za popravkom jezgra centra podataka. Prednosti uključuju niže troškove vlasništva, što vodi do veće profitabilnosti, omogućavajući vam da lakše ponovo uložite u infrastrukturu i odgovarajući na pitanje: "Kako da uradim više sa manje resursa?"

Cloud computing podstiče poslovne inovacije omogućavajući organizacijama da brzo i efikasno istraže potencijal novih IT omogućenih poslovnih poboljšanja koja mogu da rastu uz nezapamćene razmere.

Ne samo da cloud computing isporučuje veliki povratak uložene potrošnje na IT opremu, već i promoviše efikasnije i efektivnije korišćenje tehničkog osoblja. IT troškovi radne snage predstavljaju 70 posto informatičkog operativnog budžeta. Sa veoma autonomnim karakterom, cloud computing eliminiše mnogo vremena tradicionalno potrebnog za trebovanja i pružanje IT resursa.

Cloud computing takođe daje značajne uštede u troškovima za nepokretnosti potrebnim za centar podataka, kao i troškove napajanja i hlađenja. Zahvaljujući virtuelizaciji i cloud-ovoj sposobnosti za iskorišćenjem resursa (bilo kroz privatni cloud ili iskorišćenjem javno dostupnih cloud izvora), centri podataka mogu da smanje nemilosrdan pritisak i da prošire svoj fizički prostor. Taj prostor se prevodi u štednju smanjenja potrošnje energije, što je važno razmatranje u svetlu činjenice da su napajanje i troškovi za hlađenje centara podataka porasli osam puta u proteklih 12 godina. Studije su dokumentovale da cloud computing može sačuvati 80 odsto na površini i 60 odsto na energiji, dok bi se korišćenje imovine utrostručilo.

Sa cloud-s kao konstrukcijom IBM-a, sigurnost podataka je ugrađena u cloud. IBM-a uključuje sledeće generacije bezbednosti i cloud tehnologije za upravljanje servisom, kao i pojednostavljeno upravljanje bezbednosti i primene, nudeći kupcima preduzeća iste vrednosti i poštovanje garancija koji su ekvivalentni ili bolji od onoga što mogu da očekuju u tradicionalnom računarskom okruženju. Izgrađena na IBM-ovoj velikoj industriji bezbednosti rukovodstva, IBM bezbednost okolnih cloud-a se fokusira na razvijanje poverenja virtuelnih domena, autentifikaciju, upravljanje izolacijom, politiku i integritet menadžmenta i tehnologije kontrole pristupa dizajnirane specifično za cloud computing.

4.5 Elastična Cloud validacija: Sledeći korak u ostvarivanju elastičnosti

Baš kao što mogu usvojiti bezbednosne funkcije da izađu u susret zahtevima najzahtevnijih servisa, cloud-i takođe mogu biti projektovani tako da budu suštinski čvrsti. IBM-a nudi program za elastičnu cloud validaciju da biste potvrdili elastičnost bilo koje kompanije isporuku aplikacija i usluga klijentima u cloud okruženju. Kao rezultat, korisnici mogu brzo i lako da identifikuju pouzdane provajdere koji su prošli rigorozne procene, omogućavajući im da brže i samouvereno ubiraju korist iz poslovanja cloud servisa. Na ovaj način, korisnici mogu biti sigurni da su oni izbegli nepredvidive performanse i potencijalno visoko vreme zastoja i ishoda oporavka koji može doći sa drugim cloud servisima.

IBM pomaže novim klijentima da se premeste u oblak. Jedna od Hjustonovih najvećih i najbrže rastućih ljudsko-uslužnih neprofitnih agencija, Centri susedstva, koja služi više od 200.000 građana u Jugozapadnom Teksasu, zavisi od IBM- cloud servisa, servera podrške i računara distribuiranih podataka iz okruženja koji čuvaju podatke na sigurnom mestu nepoznate lokacije. Kao davalac osnovne društvene uslugeu u preko 20 objekata, Centri susedstva nisu mogli tolerisati isključivanja kada je naleteo uragan Ike koji ih je pogodio. Sa cloud-om, Centri susedstva nisu pretrpeli prekide poslovanja i uživali su u visokom kvalitetu zaštite podataka. Elastičnost i fleksibilnost su omogućene od oblaka su omogućile neprofitnima dobijanje novog ugovora.

IBM primenjuje stečeno znanje i uvid od stotine sličnih angažmana u cloud tehnologije. IBM direktno radi sa klijentima da stvore repliciran, cloud-isporučeni, industrijski-specifičan servis kao što su Lender Biznis process servis ili Servis zdravstvene usluge ili usluge kao što su horizontalne poslovne usluge kao CRM i upravljanje lancem snabdevanja.

4.6 Cloud Computing u inostranstvu: Uspeh Jun platforme

U Kini, IBM upravlja novorazvijenim cloud-om računarske platforme, kodnog imena Jun projekat što na kineskom znači "oblak", za kompanije da pristupe poslovnim servisima. Platforma je dizajnirana da izvrši selekciju i implementaciju novih cloud usluga vrlo jednostavno, kao da birate stavku iz padajućeg menija. Bez potrebe za potpornim rezervisanjem, IBM platforma nastoji da dramatično smanji vreme potrebno za isporuku novih usluga. Jun platforma raspoređuje skladištenje, servere i mrežne resurse za korisničku primenu bez ljudskog dodira, postizući vrhunske performanse, dostupnost i iskorišćenost energije.

Jedan od najvećih prodavaca Kine pozdravlja više od 10 miliona klijenata dnevno; Wang Fu Jing Robna kuća prihvatila je i raspodelila nekoliko ključnih cloud-a iz ProJekat Jun usluge, uključujući i rešenje za upravljanje lancem snabdevanja zbog ogromne mreže maloprodajnih objekata, da bi se lako delile informacije lanca snabdevanja kao i izvršenje B2B poslovnih procesa sa hiljadama svojih SMB dobavljača preko cloud-a.

Da zadovolji rastući apetit kupaca za uslugama cloud computing-a, IBM je izgradio više od desetak centara cloud computing-a za kupce širom sveta. Na primer, u Kini, Wuksi cloud

centar pruža na zahtev virtuelne računarske resurse koji omogućavaju da i do 200.000 izdavača softvera dele troškove i IT okruženje iz njihovih računara ili drugih računarskih uređaja. Ovaj pristup stimuliše ekonomski rast i stvara više srodnih IT poslova.

4.7 Cloud Computing u Evropi

U Evropi, IBM je pomogao Softver kao servis (SaaS) provajder u stvaranju računarskih resursa sa sigurnošću, kontinuitetom, poštovanjem i brzom isporukom potrebnim da zadovolji zahteve kupaca, uz održavanje niskih troškova. IBM cloud tehnologija, sa jakim mogućnostima upravljanja uslugama, opremljena je pouzdanim, elastičnim resursima koji su usklađeni sa promenama poslovnih pravila i propisa. Ovaj provajder se sada može proširiti do novih segmenata klijenata, dok takođe stvara nova radna mesta istovremeno poboljšavajući zadovoljstvo kupaca.

IBM ne pruža samo viziju koja omogućava IT profesionalcima da se fokusiraju više na inovacije u okviru svojih IT sistema i manje na dnevne IT probleme, već takođe pruža pristup čija je osnova u iskustvu stvarnog sveta zasnovana na otvorenim standardima i pojačana ekosistemom tehnologija partnera. Nijedan drugi provajder se fokusira na proces transformacije centra podataka na svim nivoima, od tehnologije, konsultantske usluge i strategije poslovnih procesa poput IBM-a. Rezultat je stvaranje vrednosti u svakoj fazi procesa.

4.8 Osećaj sigurnosti kod IBM-ovog zapisa

Ukrotiti remećenu tehnologiju i opremiti je da radi za klijente nalazi se u IBM-ovom DNK. IBM zapis za prelazak centara podataka na novi nivo pouzdanosti i performansi kroz hiljade angažmana u svetu je dobro dokumentovan. Da li je to bilo pionirsko rukovodstvo sa Linuks-om, e-poslovanje, ili mreže računara, IBM je sarađivao sa klijentima za primenu više dinamičke infrastrukture i popločao put za inovacije preduzeća za klijente koji su postali suparnici unutar industrije.

Rezultati su vidljivi i smisleni. U sopstvenom centru za transformaciju podataka, IBM-ova IT investicija u poslednjih pet godina doneli je kumulativni napredak od 4,1 milijardi dolara, dok u realnom vremenu omogućava integraciju informacionih i poslovnih usluga. IBM želi da udvostruči svoj kapacitet računara do 2010 ne planirajući povećanje potrošnje energije ili ugljeničnog otiska.

Podupret dubokim tehničkim mogućnostima, veštine bez premca i jasnim putokazom procene i rešenja po kojima klijenti mogu da postupaju, IBM nudi ključne gradivne blokove za ostvarivanje mogućnosti cloud computing-a. Jedan od kamena temeljca u sledećoj generaciji osnovnih IBM sistema Z10. Novi sistem Z10 predstavlja decenije IBM inovacije i saradnje sa najmodernijim klijentima IBM-a. To omogućuje do 100 odsto veće performanse i do 100 odsto iskorišćenosti troškova i potencijal uštede od 80 odsto ili više u odnosu na konkurentska IT okruženja. IBM-Z10 sistem je najmoćnije sredstvo na raspolaganju klijentima za smanjivanje troškova i kompleksnosti u njihovim centrima podataka.

Najveći deo vrednosti IBM-ovog poduhvata počiva na njegovoj posvećenosti saradnji sa klijentom, koja je omogućila IBM-u da identifikuje najbolje postupke za implementaciju dinamičke infrastrukture, vodeći napred nove nivoe IT optimizacije i transformacije. Sa fokusom na proces, kao i na tehnologiju transformacije, IBM je identifikovao vodeći najbolji postupak za IT optimizaciju i transformaciju. Ovo omogućava IBM-u da obezbedi korisnicima dokazani, disciplinovani, strateški putokaz i implementaciju pristupa obuhvatajući konsolidaciju, virtuelizaciju, fleksibilnu IT infrastrukturu i "IT kao set usluga," bez obzira na trenutno stanje centara podataka korisnika.

Cloud computing obezbeđuje novu sredinu koja omogućava organizacijama da obuhvati nove tehnologije koje adresiraju rastuće poslovne izazove i da postavi njihova preduzeća da budu konkurentnija na isplativ način. Sa iskustvom na svim nivoima, od tehnologije, konsultantske usluge do strategije poslovnih procesa, IBM je jedinstveno pozicioniran da sarađuje sa klijentima i omogućava im da žanju značajnu korist od cloud computing-a.

U konačnoj analizi, cloud computing ne govori samo o tehnologiji centra za podatke. Reč je o racionalizaciji poslovnih procesa koja čini da organizacije i ljudi budu više strateški orijentisani, sa više odgovornosti za promene i više orijentisani na pružanje usluga. Ne postoji provajder sa više uspeha i iskustva u ostvarivanju ovoga za klijente od IBM-a.

5 Bezbednost u Cloud Computing-u

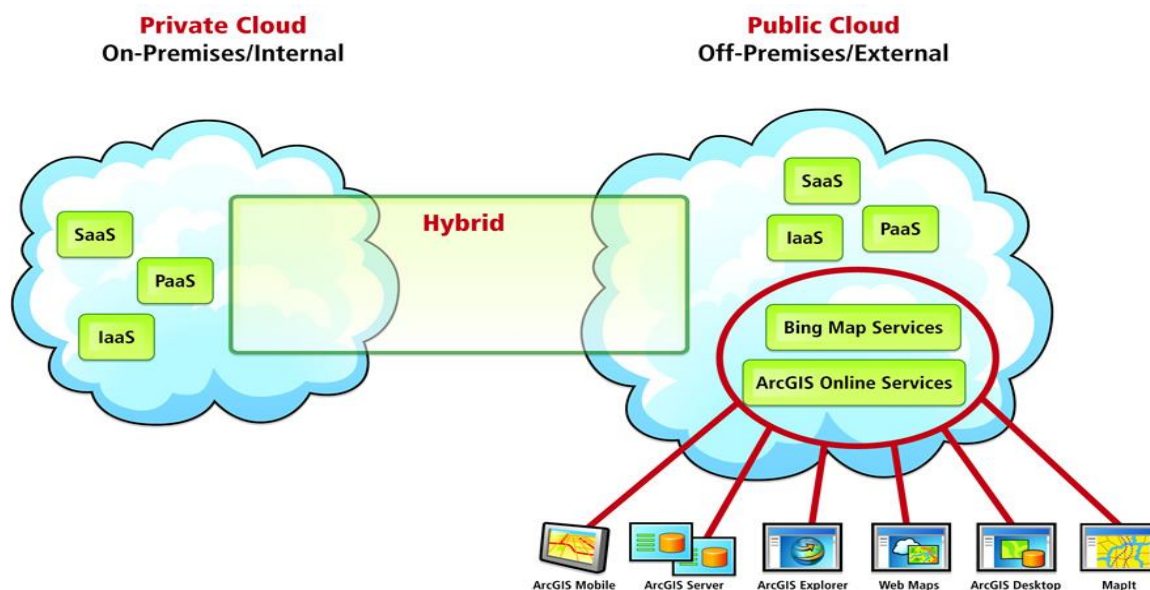
Cloud computing je fleksibilna, ekonomična i proverena platforma za isporuku i pružanje poslovnih ili potrošačkih IT usluga putem interneta. Cloud resursi se mogu brzo razvijati, i lako se postepeno smanjivati, sa svim procesima, aplikacijama i servisima pribavljenim „na zahtev“, bez obzira na lokaciju korisnika ili uređaja.

Kao rezultat, cloud computing daje organizacijama šansu da povećaju efikasnost servisnih isporuka, unapredi IT menadžment, i bolje uskladi IT usluge sa dinamičkim poslovnim zahtevima. Na mnogo načina cloud computing nudi "najbolje od oba sveta", obezbeđuje solidnu podršku glavnim poslovnim funkcijama uz sposobnost razvijanja novih i inovativnih servisa.

Kao dodatna prednost, cloud computing poboljšava korisničko iskustvo bez povećanja složenosti. Korisnici ne moraju da znaju ništa o korišćenim osnovnim tehnologijama ili implementacijama.

I javni i privatni cloud modeli su sada u upotrebi. Dostupni su svakome sa internetom, javni modeli uključuju Softver kao servis (SaaS) cloud kao što je IBM LotusLive, Platforma kao servis (PaaS) cloud kao što je IBM Računarstvo na zahtev, i Bezbednost i zaštita podataka kao servis (SDPaaS) cloud kao što je IBM Menadžment servis ranjivosti.

Privatni cloud poseduje i koristi jedna organizacija. Oni nude mnogo istih pogodnosti kao javni cloud, a daju vlasniku organizacije veću fleksibilnost i kontrolu. Osim toga, privatni cloud može da obezbedi manje kašnjenje od javnih clouds tokom perioda najjačeg saobraćaja. Mnoge organizacije prihvataju i javni i privatni cloud computing integrišući dva modela u hibridni cloud.



Slika 19: Hibridni cloud. [4]

Ovi hibridi su dizajnirani da zadovolje specifične poslovne i tehnološke zahteve, pomažući optimizaciju bezbednosti i privatnosti uz minimalne investicije u fiksne IT troškove.

Kako su prednosti cloud computinga jasne, tako je jasna i potreba za razvijanjem bezbednosti za cloud implementacije. Sledeće stranice daju pregled ključnih bezbednosnih pitanja u vezi cloud computing, zaključno sa IBM-Point of View na sigurnosnoj cloud arhitekturi i okruženju.

5.1 Adresa Cloud bezbednosti - veliki izazov

Pored standardnih izazova razvoja bezbednih informacionih sistema, cloud computing predstavlja dodatni nivo rizika, jer su osnovne usluge često dostupne trećoj strani. "Spoljašnji" aspekt dostupnosti čini težim za održavanje integriteta i privatnosti podataka, podrške podataka i dostupnosti servisa, i pokazivanja elastičnosti.

Efektivno cloud computing premešta veći deo kontrole nad podacima i operacijama sa klijentske organizacije na njihove cloud provajdere, gotovo na isti način na koji organizacije povere deo svojih IT poslovanja spoljnim preduzećima. Čak i osnovni zadaci, kao što su primena zakrpe i konfigurisanje zaštitnog zida, može postati odgovornost cloud provajdera servisa, a ne krajnjeg korisnika. Kao rezultat toga, klijenti moraju da uspostave odnos poverenja sa svojim provajderima i da budu svesni rizika da njihovi provajderi izvršavaju, primenjuju i upravljaju bezbednosti u njihovo ime. Ovaj "Veruj, ali proveri" odnos između cloud provajdera usluga i klijenata je kritična, jer klijenti su i dalje su u krajnjoj liniji odgovorni za istinitost i zaštitu svojih važnih podataka, čak i ako je taj posao odgovornost cloud provajdera. U stvari, neke organizacije odabiraju privatne ili hibridne modele umesto javnih cloud-s zbog rizika u vezi sa spoljnim servisima.

Drugi aspekti o cloud computing takođe zahtevaju veliko preispitivanje sigurnosti i rizika. Unutar cloud-sa, teško je fizički locirati mesto gde se čuvaju podaci. Bezbednosni procesi koji su nekada bili vidljivi su sada skriveni iza izdvojenih slojeva. Ovaj nedostatak vidljivosti može izazvati više sigurnosnih i problema istinitosti.

Pored toga, masivno deljenje infrastrukture sa cloud computing-om stvara značajnu razliku između cloud bezbednosti i bezbednosti u više tradicionalnom IT okruženju. Korisnici povezuju različite korporacije i nivoe poverenja često komunicirajući sa istim setom kompjuterskih resursa. U isto vreme, ravnoteža posla, promena servisnog nivoa sporazuma (SLAs) i drugih aspekata današnjeg dinamičkog IT okruženja stvaraju još više mogućnosti za dekonfiguraciju, otkrivanje podataka i zlonamerno ponašanje.

Infrastruktura deljenja poziva na visok stepen standardizacije i automatizacije procesa, a to može poboljšati sigurnost eliminišući rizik od greške operatera i previda. Međutim, rizici nerazdvojni od masovne deljene infrastrukture znače da cloud computing modeli moraju i dalje naglasiti značaj izolacije, identiteta i istinitosti.

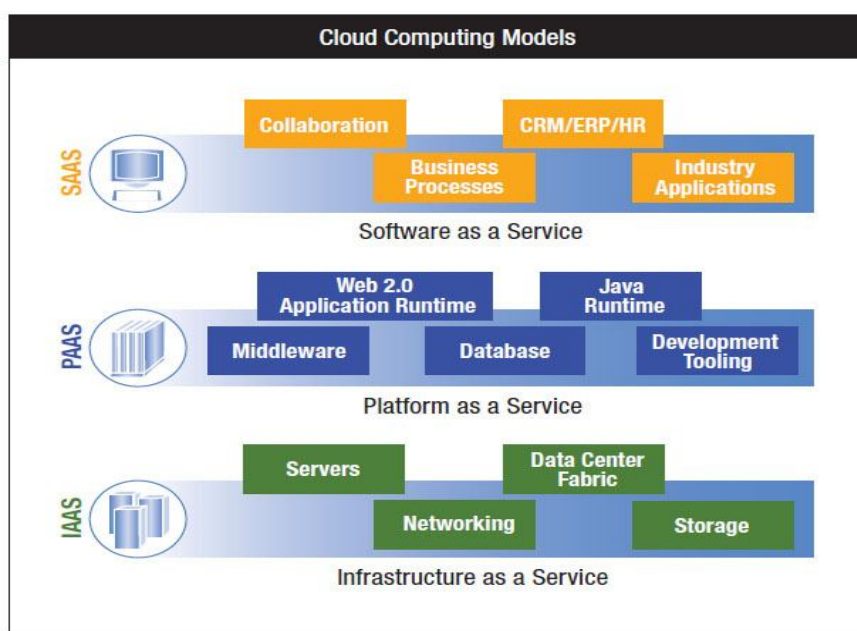
5.2 Pregled drugih modela Cloud Computing-a

Različiti modeli cloud computing-a imaju različite načine za prikazivanje njihove osnovne infrastrukture korisnicima. Ovo utiče na stepen direktne kontrole nad upravljanjem računarske infrastrukture i raspodelu odgovornosti za upravljanje njene bezbednosti.

Kod SaaS modela, većinu odgovornosti za bezbednost upravljanja pružima cloud provajder. SaaS obezbeđuje više načina za kontrolu pristupa web portala, kao što su upravljanje identitetima korisnika, aplikacija na nivou konfiguracije i mogućnost da ograničite pristup određenim IP adresama opsega ili geografskog područja.

Cloud model platforma kao servis (PAAS) omogućava klijentima da preuzmu više odgovornosti za upravljanje konfiguracijom i bezbednošću baze podataka i softverskih aplikacija.

Infrastruktura kao servis (IAAS) model prebacuje još više kontrole i odgovornosti za bezbednost od cloud provajdera ka klijentu. U ovom modelu, dozvoljen je pristup operativnom sistemu koj podržava virtualne slike, umrežavanje i skladištenje.



Slika 20: SAAS, PAAS, IAAS modeli. [1]

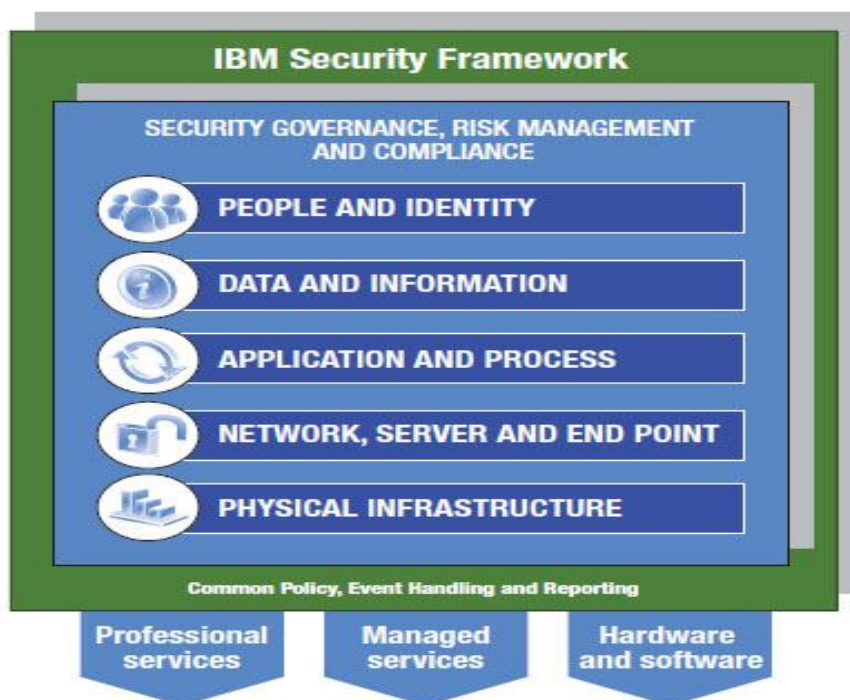
Organizacije su zaintrigirane ovim modelima cloud computing-a zbog njegove fleksibilnosti i isplativosti, ali su takođe zabrinuti za bezbednost. Poslednje cloud studije usvojene od strane industrijskih analitičara i članaka u štampi su potvrdile ove probleme, navodeći nedostatak vidljivosti i kontrole, brige o zaštiti poverljivih informacija i čuvanje informacija u deljivom, spolja upravljanom okruženju.

Masovno usvajanje spoljašnjih, masovno deljenih i potpuno otvorenih cloud platforma za kritične računarske IT servise će izgleda biti još uvek nekoliko godina daleko.

U bliskoj budućnosti, većina organizacija će tražiti načine da poveže usluge spoljnih cloud provajdera. Ovi cloud-si bi se koristili prvenstveno za opterećenja sa niskim profilom rizika, sa jedna-veličina-odgovara-svemu pristupom bezbednosti sa nekoliko garancija prihvatljivosti, i gde je cena glavna razlika. Za opterećenja sa srednjim i visokim stepenom rizika profila uključujući visoko regulisan ili zakonom zaštićenu informaciju, organizacije biraju izbor privatnog i hibridnog clouds-a koji omogućavaju značajan nivo kontrole i sigurnosti. Ova opterećenja će biti premeštena u spoljne clouds-e kad počnu nuditi jaču i fleksibilniju bezbednost.

5.3 Pregled IBM Sigurnosnog okvira (IBM Security Framework)

IBM-bezbednosni okvir je razvijen da opiše bezbednost u smislu resursa poslovanja koji moraju biti zaštićeni, i posmatra različite resurse domena sa poslovne tačke gledišta. Zasnovan na IBM-bezbednosnom okviru i informisan obimnim razgovorima sa klijentima IBM-a, sledeći odeljak daje listu bezbednosnih zahteva u preduzetničkoj klasi cloud computing-a danas.



Slika 21: IBM Security Framework [1]

5.3.1 Bezbednost upravljanja, upravljanja rizicima i pridržavanje

Organizacija zahteva uvid u bezbednosno stanje svojih clouds-a. Ovo uključuje široki uvid u promene, imidž i upravljanje incidenta, kao i izveštavanje incidenata za članove i specifične logove članova i reviziju podataka.

Vidljivost može biti posebno kritična po istinitost. Sarbanes-Oxley-akta, Zakon zdravstvenog osiguranja o prenosivosti i odgovornosti (HIPAA), Evropski zakoni o privatnosti i mnogi drugi propisi zahtevaju sveobuhvatne revizije mogućnosti. Pošto su javni cloud-si po definiciji "crna kutija" za pretplatnika, potencijalnom cloud pretplatniku neće biti u stanju da pokaže istinitost (Privatni ili hibridni cloud, sa druge strane, može biti konfigurisan da ispuni te zahteve).

Pored toga, od provajdera se ponekad zahteva da podrži kontrolu treće strane, a njihovi klijenti mogu biti usmereni na podršku elektronskog otkrića i sudske istrage, kada se sumnja na proboj. Ovo dodaje još više značaja za pravilno održavanje vidljivosti u cloud-u.

U principu, organizacije često navode potrebu za fleksibilnim SLAS koji se može prilagoditi na svoje specifične situacije, izgrađenim na svojim iskustvima sa strateški tradicionalnim vođenjem usluga.

5.3.2 Ljudi i identiteti

Organizacije moraju da se uvere da ovlašćeni korisnici preko svojih preduzeća i lanca snabdevanja imaju pristup podacima i alatima koji su im potrebni, kada su im potrebni – a sve to dok blokiraju neovlašćeni pristup. Cloud okruženja obično podržavaju veliku i raznovrsnu zajednicu korisnika, tako da su ove kontrole još više kritične. U prilog tome, cloud-s uvode nove dužnosti privilegovanih korisnika: administratore koji rade za cloud provajdera. Privilegovani korisnički nadzor, uključujući i aktivnosti logovanja, postaje važan zahtev. Ovaj nadzor treba da obuhvati fizički nadzor i pozadinsku kontrolu.

Identitet federacije i brzorastuće mogućnosti ulaska moraju biti dostupne da bi koordinirale proveru identiteta i autorizaciju sa pomoćnim preduzećem ili nezavisnim sistemom. Standardizovana, jedinstvena mogućnost prijavljivanja je potrebna da se pojednostavi za prijavljivanje krajnjih korisnika na interno hostovane aplikacije i cloud-s, omogućavajući korisnicima da lako i brzo iskoriste cloud usluge.

5.3.3 Podaci i informacije

Većina organizacija navodi zaštitu podataka, kao njihov najvažniji sigurnosni problem. Tipični koncepti obuhvataju način na koji se podaci skladište i na koji im se pristupa, pridržavanje i reviziju zahteva, i poslovnih problema koji uključuju troškove povrede podataka, obaveštenje o zahtevima i oštećenja vrednosti brenda. Svi osetljivi ili regulisani podatci treba da budu pravilno odvojeni na cloud strukturi skladištenja, uključujući i arhivirane podatke.

Kriptovanje i upravljanje ključevima za šifrovanje podataka u prenosu do cloud ili ostatka servisa u provajderskom centru za podatke su od ključne važnosti za zaštitu podataka i

saglasnosti u skladu sa mandatima. Enkripcija mobilnih medija i mogućnost da bezbedno dele ključeve za enkripciju između cloud provajdera servisa i potrošača je veoma važna i često prevedena potreba. Budući da kretanje velike količine podataka brzo i jeftino preko interneta još uvek nije praktično u mnogim situacijama, u mnogim organizacijama moraju da pošalju mobilne medije, kao što je arhiv traka, do cloud provajdera. Veoma je važno da podaci budu šifrovani i da samo cloud provajder i klijent imaju pristup šifrovanim ključevima.

Značajna ograničenja u pogledu grupisanja podataka mogu nastati sa oblakom računara, u zavisnosti od lokacije organizacije, tipa podataka koji se obrađuje i prirodi svog poslovanja. Nekoliko članica Evropske unije (EU), na primer, izričito zabranjuju da privatni lični podaci svojih građana napuste granice države. Određen broj američkih vladinih institucija ne dozvoljavaju da privatni lični podaci svojih zaposlenih budu poslani u spoljni svet.

Pored toga, razvijanje cloud-a može povećati pitanja kršenja zakona vezanih za šifrovane informacije, i razvoj može potencijalno izložiti intelektualne svojine ozbiljnim pretnjama. Pravni savetnik organizacije mora izvršiti detaljan pregled svih zahteva pre primene oblaka, kako bi organizacija mogla da održi kontrolu nad geografskoj lokaciji podataka u infrastrukturi provajdera.

U oblastima koje uključuju korisnike i podatke sa različitim klasama rizika koje su izričito identifikovane (kao što su javne i finansijske usluge), organizacija treba da održi rasprostranjenu klasifikaciju podataka. Klasifikacija podataka će odrediti ko ima pristup, kako su ti podaci šifrovani i arhivirani, i kako se koriste tehnologije za sprečavanje gubitka podataka.

5.3.4 Aplikacije i procesi

Klijenti obično podrazumevaju cloud primenu bezbednosnih zahteva u pogledu bezbednosti slika. Svi zahtevi tipičnih primena bezbednosti i dalje važe za aplikacije u cloud-u, ali su takođe preneti i na slike koje hostuju te aplikacije. Cloud provajder treba da prati i podržava siguran proces razvoja. Pored toga, cloud korisnici zahtevaju podršku za poreklo slike i za izdavanje dozvola i kontrolu upotrebe. Suspendovanje i uništavanje slika mora da se sprovodi pažljivo, vodeći računa da osetljivi podatci sadržani u tim slikama ne budu izloženi.

Definisanje, verifikacija i održavanje položaja bezbednosti slika Vis-a-Vis klijent-specifične bezbednosne politike je važan uslov, posebno u visoko regulisanim industrijama. Organizacije treba da obezbede da web servisi koje objave u cloud-u budu sigurni, usaglašeni i da zadovolje njihovu poslovnu politiku. Zahvaljujući sigurnom razvoju najbolja praksa je ključni uslov.

5.3.5 Mreža, server i krajnja tačka

U zajedničkoj cloud sredini klijenti žele da osiguraju da su svi domeni članova pravilno izolovani i da ne postoji mogućnost da podaci i transakcije procure iz jednog članskog

domena u sledeći. Da bismo ovo postigli, klijentima je potrebna mogućnost da konfigurišu sigurnosne virtuelne domene ili pravilno bazirane sigurnosne zone.

Kako se podaci kreću dalje od kontrole klijenta, oni očekuju sposobnost sistema nametanja, otkrivanja i sprečavanja da se ugradi u okruženje. Briga nije samo upada u klijentov sigurnosni virtuelni domen, već i potencijal za curenja i "istiskivanja" podataka – to jest, zloupotreba domena klijenta da omogući napad na treća lica. Premeštanje podataka ka spoljnim servisima stvara dodatne brige o unutrašnjim i internet baziranom uskraćivanju usluga (DOS), ili distribuiranog uskraćivanju usluga (DDOS) napadima.

U deljenoj sredini, sve strane se moraju složiti oko svojih obaveza da bi dali kritičnu ocenu podataka i sprovesti ove kritike na redovnoj osnovi. Organizacija mora preuzeti vođstvo u pogledu ugovora o upravljanju za bilo koju procenu rizika ili primenu kontrole koja se ne obavlja direktno.

Gde su kataloške slike obezbeđene od strane cloud provajdera, klijenti žele da ove slike budu bezbedne i adekvatno zaštićene od korupcije i zloupotrebe. Mnogi klijenti očekuju ove slike da budu kriptografski sertifikovane i zaštićene.

5.3.6 Fizička infrastruktura

Cloud infrastruktura, uključujući servere, rutere, uređaje za skladištenje, napajanja i ostale komponente koje treba da podrže operacije – moraju biti fizički bezbedne. Zaštitne mere uključuju adekvatnu kontrolu i praćenje fizičkog pristupa koristeći biometrijsku kontrolu pristupa i zatvorenog kruga video (CCTV) monitoringa. Provajder treba da jasno objasni kako funkcioniše fizički pristup serverima koji hostuju klijentske radove i da podržavaju klijentske podatke.

6 Vodič za primenu sigurnog oblaka

Sledeće mere bezbednosti predstavljaju generalno najbolje praktične implementacije za cloud bezbednost. Istovremeno, one se ne mogu tumačiti kao garancija za uspeh. Posavetujte se sa svojim IBM-predstavnikom bezbednosnih službi da identifikujete najbolje praktične smernice za primenu specifičnih implementacija.

6.1 Implementacija i održavanje bezbednosnog programa

Bezbednosni program može da obezbedi strukturu za upravljanje bezbednosti informacija, kao i rizicima i pretnjama za ciljnu sredinu. U slučaju kršenja bezbednosti, bezbednosni program može da pruži ključne informacije, kao na primer, kako je cloud zaštićen, odgovori na pretnje, i iscrta odgovornosti za upravljanje događajima.

1. Razmatranja o implementaciji programa bezbednosti

Kada gradimo bezbednosni program, sledeće preporuke treba uzeti u obzir:

- 1.1 Oceniti i dokumentovati kulture organizacije u povezanosti sa opštom sigurnošću:
 - a. Procenite trenutne industrijske i organizacijske posebne zahteve u uspostavljanju najbolje prakse za bezbednu infrastrukturu. Na primer, u SAD, organizacija u industriji zdravstvene zaštite može da se kvalifikuje kao zaštićena suština pod zdravstvenim osiguranjem Zakona o prenosivosti i odgovornosti (HIPAA).
 - b. Ako poslovne tajne predstavljaju osnovu za konkurentsku prednost preduzeća, korporativni bezbednosni program mora odrediti zahteve saglasnosti.
 - c. Ako se kontrola izvoza primenjuje na podatke preduzeća, važno je odrediti određenu usklađenost metodologije za podatke.
 - d. Ocenjuje svaku predloženu cloud aplikaciju za dobrobit cloud razvijanja. Pažljivo razmatranje potreba kompanije sa cloud provajderom ili sa graditeljem bezbedne infrastrukture mogu biti korisni u procenjivanju da li i koji tip cloud ponude bi mogao raditi.
- 1.2 Poredati prioritete bezbednosne attribute, koji odgovaraju tvojoj cloud implementaciji, po značaju.
- 1.3 Kreirati i održavati pravila i postupke u odnosu na to kako će organizacija adresirati razna razmatranja cloud sigurnosti.
 - a. Politika treba da identifikuje pretnje cloud životnoj sredini i njihov sadržaj, što znači da moraju da budu održavani tako da mogu adresirati aktuelne pretnje.
 - b. Politika treba da identifikuje ključne merne jedinice za praćenje, i frekvencije na kojima trebaju biti ocenjivane; ove metrike i merenja mogu biti diktirane od strane industrije propisa ili najbolje prakse.
 - c. Politika treba da odredi strukturu za odgovornosti.
 - d. Politika treba da da preporučeni odgovor u slučaju događaja.
 - e. Preporučena reakcija treba da identifikuje ključne akcije, osoblje i eskalaciju postupaka u određenom vremenskom periodu.
- 1.4 Raditi sa rukovodstvom ili izvršnim timom koji je odgovoran za sprovođenje cloud implementacije da bi obezbedili razumevanje i podršku inicijativi.
- 1.5 Sprovoditi organizacijski široko-edukativni program za komunikaciju sa politikom bezbednosti i zbog opšteg shvatanja politike.
 - a. Obezbediti da sve osobe sa administrativnim ulogama kompletiraju potrebnu obuku.

- b. Obezbediti da politika bude objavljena na lokaciji koja je lako dostupna svima onima koji su odgovorni za sprovođenje politike i upravljanje.

1.6 Implementirati sistem da se obezbedi transparentnost i sigurnost statusa anomalije događaja.

1.7 Uspostaviti program za reviziju.

1.8 Implementirati prinudni model da se obezbedi dozvola za komunikaciju događaja i odgovornosti.

1.9 Kreirati obaveštajni program da komunicira sa odgovarajućim osobljem u slučaju bilo kakvog nepravilnog događaja, koji će biti blizak realnom vremenu koliko je to razumno moguće.

6.2 Izgradnja i održavanje bezbedne Cloud infrastructure

Bezbedna infrastruktura pomaže da se obezbedi elastičnost oblaka i poverenje da su podaci koji se nalaze u cloud-u adekvatno zaštićeni. Tokom procesa, organizacija mora da obezbedi da prodavac ispuni sve poslovne zahteve, pokazuje razumevanje svih pravnih, regulatornih, industrijskih, i specifičnih zahteva klijenata, i ima kapacitet da ispuni te zahteve na zadovoljavajući način.

2. Instaliranje i održavanje podešavanja zaštitnog zida

Podešavanja zaštitnog zida treba da se instaliraju i održavaju prateći sledeće preporuke:

2.1 Uspostaviti konfiguraciju zaštitnog zida koja sadrže sledeće uslove:

- a. Formalni proces upravljanja promenama za zaštitni zid koji rezultira formalnim odobravanjem i prihvatanjem promena konfiguracije.
- b. Zaštitni zid treba da se postavi na svaki interfejs spoljne mreže, a između svake bezbednosne zone unutar cloud-a.
- c. Dijagram mrežnog interfejsa i mesta koja su povezana sa protokom informacija i plasmana zaštitnog zida, mora razmotriti aktiviranje virtuelnih okruženja, kao i rešenja mekog zaštitnog zida.
- d. Dokumentovana i održavana lista portova i usluga neophodnih za poslovanje operacije i kontinuitet. Podrazumevane postavke za portove zaštitnog zida treba da odbiju pristup.
- e. Opravdanost i procena rizika za svaki protocol zaštitnog zida ili anomalije definicije dizajna.
- f. Opis grupa, uloga i definicja za logičko upravljanje mrežom.
- g. Kvartalne procene konfiguracije rutera i zaštitnog zida i pravila postavljanja.
- h. Standarde za podešavanja zaštitnog zida i konfiguraciju rutera.

- 2.2 Izgraditi i razviti zaštitni zid koji uskraćuje pristup iz "nepouzdatih" izvora ili aplikacija, i koji adekvatno loguje ove događaje.
- 2.3 Izgraditi i razviti zaštitni zid koji ograničava pristup sistemima koji imaju direktnu spoljnu vezu spoljne i onima koje sadrže poverljive podatke ili konfiguracije podataka.
Konfiguracija treba da obuhvati sledeće:
 - a. Specifična ograničenja saobraćaja između navedenih filtera portova i adresa.
 - b. Da sprečava direktan pristup spoljnih interfejsa u ograničenu mrežnu zonu.
 - c. Implementacija dinamičkog filtriranja paketa.
 - d. Ograničenje svih ulaznih i izlaznih prometa na te informacije navedenih u dokumentovanoj i održavanoj listi portova i servisa.
 - e. Prevencija direktnog bežičnog pristupa cloud infrastrukturi.
 - f. Prevencija direktnog pristupa unutrašnje adrese spoljnim interfejsima.
- 2.4 Instalirati parameter zaštitnog zida između poverljivih i konfiguracijskih podataka i eksternog interfejsa koje podržava cloud host.
- 2.5 Instalacija ličnog zaštitnog zida, rešenjima na eksternim uređajima, kao što su računari, mobilni računari, mobilni uređaji, i tako dalje, da interfejs sa cloud okruženjem bude podržan od host cloud-a.
- 2.6 Implementiranje IP-maske da spreči unutrašnje sisteme budu predstavljeni i identifikovani sa spoljnim entitetima.
- 2.7 Implementirati zaštitni zid da bi se izolovale poverljive informacije, i da obezbedi da su svi poverljivi podaci sačuvani iza zaštitnog zida.

3. Ne koristiti podrazumevane vrednosti prodavaca za lozinke i druge bezbednosne parametare

Prodavac isporučuje podrazumevane parametre za bezbednost, poput lozinki, koje ne treba koristiti.

- 3.1 Uvek promenite lozinku koju prodavac isporučuje i bezbednost parametara pre aktiviranja servera, ili pre stvaranja virtuelne mašine.
- 3.2 Razviti cloud standarde konfiguracije i smernice za organizaciju. Dokumentovati ove standarde i obezbediti da vaše cloud okruženje bude u skladu. Uverite se da su ovi standardi u skladu sa smernicama industrije.
- 3.3 Obezbediti da svaka virtuelna mašina primenjuje samo jednu primarnu funkciju.
- 3.4 Proverite da li postoje nepotrebne funkcije ili aktivni procesi.
- 3.5 Uklonite sve nepotrebne aplikacije, skripte, ili module iz virtuelnih sistema.

4. Zaštititi administrativni pristup

Svi administrativni pristupi treba da budu pravilno zaštićeni pristupnim kontrolama i sigurnom mrežom.

- 4.1 Koristiti sigurne mrežne protokole za sve administrativne radnje (ssh, SSL, IPSEC, i VPN), uz dvosmernu proveru identiteta.
- 4.2 Zahtevati dvostruku kontrolu za sve pristupe provajdera resursima potrošača (autentifikacij i autorizacija kupca i provajdera za operacije).
- 4.3 Održavati trag revizije administrativnih postupaka.
- 4.4 Host cloud treba da razvije i objavi smernice upravljanja konfiguracijom.
- 4.5 Implementirati mehanizam za otkrivanje resursa da bi se otkrili resursi u upotrebi u ciljnoj sredini.
- 4.6 Redovno pregledajte mape resursa da bi ste razumeli resurse u cloud sredini.
- 4.7 Održavati konfiguraciju skladišta podataka da bi se omogućilo kontrolisanje i razumevanje opšte sigurnosti.

5. Obezbediti zakrpe

Implementacija programa zakrpa treba da bude osigurana.

- 5.1 Cloud host treba da razvije i objavi zakrpe i promeni upravljanje programski menadžmentom
- 5.2 Razviti pre-produkcijski menadžment sistem zakrpa kako bi omogućili elastičnost poslovanja.
- 5.3 Osigurati da logovanje bude omogućeno za sve procese zakrpa, i razvijati odgovarajuću dokumentaciju.
- 5.4 Uverite se da svi sistemi i aplikacije koriste poslednju verziju prodavčeve zakrpe i ispravke u okviru određenog perioda kao što je navedeno u zakrpi i upravljanjem promenama programa. Uverite se da je uspostavljen odgovarajući vremenski okvir.
- 5.5 Uspostaviti proces ili koristiti nezavisnog proizvođača da očuva svest o najnovijoj ranjivosti bezbednosti.

6. Implementirati sigurnosni plan fizičkog okruženja.

Bezbednosni plan za fizičko okruženje treba biti sproveden.

- 6.1 Uverite se da objekat ima odgovarajuće fizičke bezbednosne kontrole kako bi se sprečio neovlašćeni pristup kritičnim oblastima u okviru objekata i pristup fizičkim sredstvima i sistemima od uljeza i neovlašćenih korisnika.
- 6.2 Osigurati da svi zaposleni sa direktnim pristupom sistemu imaju punu pozadinsku proveru.
- 6.3 Uverite se da svi nezavisni provajderi imaju pravila i procedure da izdvoje zaposlene od posetilaca.
- 6.4 Uverite se da hosting servis ima adekvatnu zaštitu od prirodnih nepogoda.

7. Zaštitite hibridnu komunikaciju

Komunikacije između daljinske i korporativne infrastrukture treba da budu pravilno zaštićene.

- 7.1 Uverite se da je pristup korporativnoj infrastrukturi moguć samo preko bezbedne komunikacije.
- 7.2 Uverite se da su sve komunikacije između daljinske i korporativne infrastrukture šifrovane.
- 7.3 Obezbediti da komunikacija može da potiče samo od korporativne infrastrukture.
- 7.4 Obezbedite da je korporativna infrastruktura zaštićena sigurnosnim zidom.
- 7.5 Uverite se da sve komunikacije između daljinske i korporativne infrastrukture mogu da dođu samo preko određenih mrežnih cevi.
- 7.6 Ograničiti broj korisnika sa administrativnim pristupom i na korporacije i na daljinsku infrastrukturu.

- 7.7 Napraviti adekvatne odredbe za zaštićenu komunikaciju van opsega u slučaju vanrednog stanja.

6.3 Obezbediti zaštitu poverljivih podataka

Zaštita podataka je osnovni princip informacione bezbednosti. Sve rasprostranjene informacije bezbednosnih propisa i standarda, kao i glavnicu najboljih industrijskih izvedbi, zahtevaju da osetljive informacije budu zaštićene na adekvatan način kako bi se očuvala poverljivost. Tajnost tih podataka je potrebna bez obzira gde da se podaci nalaze u lancu nadzora, uključujući i cloud okruženja.

8. Zastita ličnih identifikacionih podataka (PII)

Sa PII treba pažljivo rukovati i treba ih zaštititi.

- 8.1 Razviti i objaviti pravila za nastanak, prikupljanje, rukovanje, prenos, skladištenje i odlaganje PII podataka.
- 8.2 Konsultujte se sa pravnim savetnikom za potrebe primenjive na vas / vašu industriju.
- 8.3 Razviti strategiju obaveštavanja PII Politike proboja i politike za komunikaciju proboja informacija, u skladu sa nacionalnim, državnim i saveznim zakonom, kao i industrijskih regulativa i najboljih praksi.
- 8.4 Razviti PII inventar podataka i klasifikaciju šeme.
- 8.5 Čuvajte PII skladište podataka na minimumu usvajanjem sledećih pravila:
 - a. Razviti i primeniti politiku zadržavanja podataka.
 - b. Sigurno uništiti sve nesusštinske PII podatke

9. Sigurno uništiti sve nesusštinske PII

PII informacije koje nisu od suštinske važnosti za poslovanje treba da bude bezbedno uništene.

- 9.1 Maska prikazuje PII informacije kada je to potrebno (na primer, prikaz podskup Brojeva socijalnog osiguranja).
- 9.2 Prikazati PII nepročitane informacije kad god su skladištene.
- 9.3 Uverite se da je PII informacija u memoriji nečitljiva i neadresirana od strane klijentove tehnologije.
- 9.4 Uverite se da PII informacije nisu snimljene u log fajlovima ili u drugim sistemske datoteke.
- 9.5 Obezbediti prijavljivanje svih PII informacija da se ublaži curenje podataka.

10. Zaštititi poverljive i kritične poslovne podatke

Razviti i primeniti politiku da zaštiti poverljive i kritične poslovne podatke.

- 10.1 Razviti PII strategiju kršenja politike i politike za komunikaciju obaveštavanja proboja informacija, u skladu sa nacionalnim, državnim i saveznim zakonom, kao i industrijskom regulativom i najboljom praksom.
- 10.2 Razvijati i održavati inventar poverljivih podataka i klasifikaciju šema.
- 10.3 Zadržati poverljive informacije za skladištenje na minimum usvajanjem sledećih pravila:
 - a. Razviti i primeniti politiku zadržavanja podataka.
 - b. Sigurno uništiti sve nesusštinske PII podaci (regulatorni zahtevi se mogu primeniti).
- 10.4 Izvršiti procenu udara podataka pre primene podataka na cloud, koja bi trebalo da se sastoji od dokumentacije i procene rizika tolerancije.
- 10.5 Ne dozvoljavati čuvanje poverljivih informacija pre autentifikacije korisnika.

11. Zaštiti intelektualnu svojinu

Razvoj i primena politike za zaštitu intelektualne svojine.

- 11.1 Pre primene bilo kog javnog cloud-a, procena rizika organizacije bi trebalo da obuhvati intelektualnu svojinu koja može biti izložena.
- 11.2 Kada koristite javne cloud-se, generalni savetnik organizacije treba da obezbedi da SLA sporazumi pokrivaju zaštitu intelektualne svojine.
- 11.3 Kada se primenjuju na javni cloud, organizacije bi trebalo da pokušaju da prikriju intelektualne svojine što je više moguće kroz šifrovanje, ili druge mehanizme, koji stvaraju teškoće zlonamernim korisnicima da iskoriste informacije.

12. Ključevi za šifrovanje štite od zloupotrebe ili otkrivanja

Proverite da li su ključevi za šifrovanje sigurni, da bi ste sprečili zloupotrebu ili otkrivanje.

- 12.1 Dokument u potpunosti sprovodi ključ za upravljanje programom za skladištenje, uključujući i sledeće:
 - a. Generisanje ključeva minimalne snage smernica i politike.
 - b. Dostava sigurnog ključ dostave i metodologije za upravljanje.
 - c. Minimalno, periodična godišnja reciklaža ključeva.
 - d. Metodologija za uništenje starog ili neaktivnog ključa.
 - e. Mehanizam koji omogućava pravilno odlaganje i brzu zamenu sumnjivih kompromitovanih ključeva.
 - f. Proces za obaveštenja o sumnjivim kompromitovanim ključnim događajima.
 - g. Sprečavanje neovlašćene zamene ključeva.
 - h. Podela znanja i uspostavljanje kontrole nad dvostrukim ključevima.
 - i. Pravila u vezi zapisa informacija moraju biti dokumentovana i odgovarajući arhivski mehanizam mora biti stavljen na svoje mesto.
- 12.2 Sprovođenje ključnih programa za upravljanje:
 - a. Primenite princip na najmanje-privilegovan pri davanju pristupa ključevima.
 - b. Redovno pregledajte korisnička prava pristupa ključevima.
 - c. Čuvati ključeve na nekoliko mesta ako je moguće.
 - d. Prijavite sve pristupe ključevima.

13. Siguran prenos podataka.

Sprovođenje bezbedne politike komunikacije podataka.

- 13.1 Dokumentovati i objaviti smernice za značenje i uslove za komunikaciju podataka.
- 13.2 Koristiti jaku kriptografiju i bezbednosne protokole, kao što su SSL / TLS i IPSEC, radi zaštite osetljivih informacija.
- 13.3 Nikada ne slati nezaštićene PII ili poverljive informacije putem e-pošte.
- 13.4 Koristite sigurnosni protokol prilikom povezivanja na mrežu zbog sigurnog skladištenja informacija.
- 13.5 Uverite se, da se koristi bezbedan transport prilikom stvaranja arhiva.

14. Implementiranje mehanizma koji sprečavanja gubljenja podataka

Implementiranje mehanizma koji sprečava gubljenje podataka (DLP) radi sprečavanja curenja podataka

- 14.1 Implementirati DLP-mehanizam da spreči nenamerno ili namerno curenje informacije.
- 14.2 Uverite se da DLP-mehanizmi daju odgovarajuće izveštavanje.
- 14.3 Uverite se da je vaše DLP rešenje integrisano sa bezbednosnom politikom.

15. Zaštita aplikacije podataka.

Obezbediti da aplikacije štite informaciju koju obrađuju.

- 15.1 Implementirati pregled kodova svih klijentskih kodova koji upravljaju osetljivim ili ličnim podacima i dokumentovati i vrste sačuvanih informacija.
- 15.2 Uverite se da su sve PII ili poverljive informacije sačuvane u nečitljivom formatu.
- 15.3 Uverite se da sve PII ili osetljive informacije sačuvane u “kolačićima” šifrovan i u nečitljivom formatu.
- 15.4 Sprečili čuvanje ključeva za šifrovanje u lokalnim sistemima.
- 15.5 Sprečili keširanje za PII ili osetljive informacije.

- 15.6 Kada pokazujete PII ili osetljive informacije, uverite se da se maskiranje realizuje za polja za prikaz podataka.
- 15.7 Ne dozvoliti skladištenje osetljivih podataka kao stalno promenljivih u aplikaciji.
- 15.8 Redovno skenirati web aplikacije zbog ranjivosti.

6.4 Implementirati snažan pristup i identitet menadžmenta

Pristup i upravljanje identitetom su kritični za cloud bezbednost. Oni ograničavaju pristup podacima i aplikacijama za ovlašćene i odgovarajuće korisnike.

16. Primeniti najmanje privilegovan model.

Uverite se da su korisničke privilegije pristupa odgovarajuće, i da je bezbedan mehanizam pristupa na mestu.

- 16.1 Redovno procenite listu pristupa korisnika kako bi se obezbedilo da se odobravaju samo odgovarajući nivoi pristupa, kao i da samo ovlašćeno osoblje ima pristup sistemima.
- 16.2 Uspostaviti politiku za sisteme koji imaju više korisnika, ograničenjem pristupa zasnovanom na potrebnom znanju.
- 16.3 Obezbedite da sistem prekontroliše i proveriti identitete svih korisnika zbog liste dozvoljenog pristupa da bi odobrio ulaz.
- 16.4 Uverite se da je odobreni mehanizam za autentifikaciju na mestu.
- 16.5 Implementirati više faktora autentikacije za pristup svim sistemima i administrativnim sistemima.
- 16.6 Za pristup administrativnim funkcijama, primeniti tehnologije kao što su biranje i daljinska VPN-autentikacija (SSL / TLS i IPsec) sa individualnim sertifikatima.
- 16.7 Enkriptovati sve lozinke tokom prenosa i skladištenja.
- 16.8 Da bi ste osigurali pravilnu autentifikaciju i funkcije upravljanja lozinkom na svim sistemima elemenata, koristite kao sledeće smernice:
 - a. Kontrola upravljanja korisnikovog ID akreditiva i ostale ID informacije.
 - b. Potvrditi identitet korisnika pre poništenje ili promene lozinke.
 - c. Zahtevati da korisnici menjaju svoju lozinku nakon prvog ulaska u aplikaciju.

- d. Hitno opozvati pristup za ograničene korisnike.
- e. Uklanjati neaktivne račune najmanje svakih 30 dana.
- f. Obezbediti dokumentaciju lozinki i ID politike, i obuku zaposlenih u uputstvima.
- g. Uverite se da su preduzimač i hosting lozinki omogućeni samo tokom održavanja rasporeda.
- h. Ne dozvolite grupne, deljene, ili generičke naloge ili lozinke.
- i. Zahtevati od korisnika da menjaju lozinke u određenom vremenskom intervalu (30, 60 ili 90).
- j. Zahtevati kompleksne lozinke za korisnike koje sadrže alfa i numeričke znakove
- k. Ograničiti prepisivanje brojeva iste lozinke (na primer, onemogućiti ponovnu upotrebu poslednje 3 lozinke).
- l. Ograničiti broj pokušaja kod neuspele lozinke, korisnik može pokušati pre nego što se zaključa sistem.
- m. Postaviti neaktivni period isteka za sve sisteme u slučajevima kada poverljivi podatci zahtevaju od korisnika da ponovo potvrdi autentikaciju sistema.
- n. Primeniti pravilo-zaključavanja koje ili ima ograničenje vremena, ili da zahteva ponovno aktiviranje servisa.

17. Implementirati ujedinjeni menadžment identiteta.

Sjedinjeni identiteti treba da budu raspoređeni tako da bezbedno razmenjuju informacije identiteta.

- 17.1 Uverite se da je sjedinjeni menadžment identiteta implementiran kada je sprovedena cloud sredina.
- 17.2 Uverite se da kada se sjedinjuju identiteti poverenje sistem identiteta se sprovodi da spreči varku identiteta.

6.5 Uspostaviti bezbednost aplikacija i okruženja

U centralno upravljanoj cloud okruženju, neophodno je automatsko obezbeđivanje funkcionalnosti na mestu.

18. Sprovođenje programa za obezbeđivanje aplikacija

Dizajnirati i primeniti programe za obezbeđivanje slika i aplikacija.

- 18.1 Obezbediti da odobreni proces za obezbeđivanje virtuelne slike bude na mestu.
- 18.2 Obezbediti da se sistem obezbeđivanja odnosi na prava pristupa za vreme obezbeđivanja.
- 18.3 Uverite se da menadžment obezbeđivanja ima odgovarajuće bezbednosne

kontrole i ovlašćenja.

18.4 Obezbediti da obezbeđivanje aplikacija i virtuelnih slika budu prijavljene.

18.5 Obezbedite da sve promene pristupu virtuelnim slikama i aplikacijama budu prijavljene.

18.6 Redovno pregledajte menadžment sistem obezbeđivanja pristupa kako bi se obezbedilo da se samo privilegovana pravila primenjuju.

18.7 Uverite se da je mehanizam na mestu koji reguliše uništavanje zastarelih ili nevažećih virtuelnih slika.

6.6 Sprovođenje upravljanja i revizije programa za upravljanje

Da bi se pripremili za regulatorne ili interne revizije, potrebno je da imate program koji definiše kada, kako i gde da se prijavite i pregledate prikupljene informacije.

19. Sprovođenje privatnosti programa upravljanja.

19.1 Implementirati program za privatnost menadžmenta sledećim atributima:

- a. Napravite razumevanje onoga zbog čega PII i poverljive informacije postoje.
- b. Prioritetizovati PII i poverljive informacije u odnosu na rizik i regulatorni uticaj.
- c. Napišite politiku upotrebe, zadržavanja, modifikacije i brisanja PII i podataka.
- d. Raditi sa izvršnim i rukovodstvenim timom za validaciju programa.
- e. Sprovođenje procesa za nadgledanje poštovanja pravila i izuzetaka.
- f. Kreirati program obrazovanja srodan sa politikom.
- g. Kreiranje programa za reviziju politike.
- h. Kreiranje pravila za sprovođenje i praćenje politike.
- i. Kreirati program / proces za notifikaciju odgovarajuće strana u slučaju kršenja.

19.2 Dodati PII podatke mapi referentnih podataka da bi dozvolili revizorima i administratorima da identifikuju opasnosti u cloud sredini.

20. Implementirati mehanizme za reviziju snimanja i upravljanja

Sprovođenje revizije upravljanja zapisima i programa za upravljanje.

20.1 Raditi sa pravnim savetnikom da se identifikuju i dokumentuju svi važeći i zakonski i regulatorni zahtevi za svaki cloud.

- 20.2 Na osnovu navedenog, stvoriti politiku za hvatanje i zadržavanje pravnih i regulatornih dokumenata.
- 20.3 Sprovesti redovan pregled zadržanih informacija.
- 20.4 Implementirati program za reviziju da se osigura da revizija za snimanje i zadržavanje politike jeste sprovedena.
- 20.5 Obezbediti prikupljanje svih pravnih i regulatornih dokumenata po potrebi.

21. Zaštita i elastičnost dokumenata preko granice

Dokumentovati, pregledati i sprovesti politiku koja obezbeđuje da se podaci obrađuju i čuvaju u skladu sa propisima i vangraničnim zahtevima za zaštitu.

- 21.1 Sve važeće regionalne, nacionalne i međunarodne zakone treba preispitati sa pravnim savetnikom zbog razumevanja zahteva vezanih za prenos i korišćenje prostora od strane cloud potrošača i domaćina.
- 21.2 Dokumentovati politiku i procedure povezane sa međunarodnim, nacionalnim, regionalnim zakonima i propisima koji utiču na poslovanje, uključujući:
 - a. Gde podaci moraju biti uskladišteni na osnovu sadržaja i podataka potrošača.
 - b. Ko ima pristup podacima na osnovu sadržaja i podataka potrošača.
 - c. Koje zaštite (šifrovanje, segregacije, i tako dalje) se moraju staviti na mesto da zaštite podatke na osnovu navedenih regionalnih, nacionalnih i međunarodnih zakona i propisa koji utiču na poslovanje.
- 21.3 Redovno pregledanje različitih propisa i zakona sa pravnim savetnicima koji mogu biti primenjeni na kreiranje, skladištenje, prenos, i uništavanje podataka kao što se odnosi na vangraničnu zaštitu.
- 21.4 Uveriti se, da u slučajevima kada je potrebna saglasnost, zapis se održava da potvrdi, da su podaci koje je osoba dala ispravni.
- 21.5 Proveriti da li su podaci o procesorima svesni aktivnosti i ograničenja koja se primenjuju u vezi sa osetljivim informacijama.

6.7 Implementirati upravljanje programom ranjivosti i provale

U sigurnom cloud okruženju, morate da primenite stroge programe za upravljanje ranjivosti i mehanizme kao što su sistemi za otkrivanje upada (IDS) i sistemi za

sprečavanje upada (IPS-) da se osigura da su IT resursi (serveri, mrežne infrastrukture komponente i uređaji) stalno praćeni zbog propusta i kršenja.

22. Implementirati i redovno ažurirati antivirusnu / anti-spajver i IDS / IPS zaštitu

Mehanizmi za skeniranje ranjivosti, antivirusi, i mehanizmi za otkrivanje i sprečavanje upada moraju biti razvijeni za zaštitu okruženja.

- 22.1 Instalirajte antivirusni softver podržan na svim sistemima koji bi mogli biti izloženi virusima ili napadima špijunskih softvera.
- 22.2 Obezbediti da izabrani programi mogu identifikovati, izolovati, ili ukloniti i zaštititi od zlonamernog softvera i procesa.
- 22.3 Razviti politiku za mašinsku klasifikaciju u odnosu na antivirusne menadžment protokole
- 22.4 Uverite se da su svi mehanizmi zaštite trenutni i aktivno rade, a sposobni su za generisanje logova.
- 22.5 Koristiti mreže i host baziranu detekciju upada ili sistem za sprečavanje upada da prati aktivnosti u cloud okruženju i upozorava osoblje na sumnjive događaje.
- 22.6 Držite sve sisteme za otkrivanje i sprečavanja upada apdejtovanim.
 - a. Potvrdite korišćenje sistema za otkrivanje upada ili sistema za sprečavanje upada i da se sav saobraćaj u cloud sredini prati .
 - b. Potvrditi da su IDS i IPS konfigurisani da upozore osoblje na sumnjive događaje.

6.8 Održavajte testiranje i validaciju okruženja

Da biste održali netaknuto cloud IT okruženje, morate upošljavati različite mehanizme za testiranje i proveru validacije.

23. Implementirati upravljanje promenama procesa

Dokumentovati i implementirati proces upravljanja promenama

- 23.1 Uveriti se da postoji dokumentovana konfiguracija za upravljanje promenama procesa u prostoru.

- 23.2 Pratite proces promene konfiguracije za sisteme upravljanja i softvera unutar cloud. On treba da sadrži sledeće:
- a. Promena logovanja na zahtev.
 - b. Izjava o izvršenom udaru.
 - c. Pre-proizvodni rezultati testa i odjavljivanje.
 - d. Proces za vraćanje u prethodno stanje.

24. Implementirati enkripciju podataka i pristupni program.

Implementirati program koji će testirati da li su uskladišteni podaci pravilno zaštićeni.

- 24.1 Testirati bazu podataka i ostale medije za skladištenje kako bi se osiguralo da su adekvatno zaštićeni, i da se primenjuje odgovarajući nivo šifrovanja.

25. Implementiranje programa za bezbedno testiranje i razvoj aplikacija

Razvoj bezbedonosnih aplikacija i programa za testiranje treba da bude sproveden.

- 25.1 Razviti softverske aplikacije na osnovu najbolje prakse, gde je sigurnost svesni deo inicijative komponente.
- a. Validacija svih bezbednosnih zakrpa pre proizvodnje.
 - b. Uverite se da su test i proizvodno okruženje odvojeni.
 - c. Osigurati razdvajanje dužnosti između test, razvojnih i administracijskih kadrova.
 - d. Nemojte koristiti podatke proizvodnje koji sadrže poverljive ili PII informacije u test okruženju.
 - e. Obezbediti uklanjanje svih administrativnih test podataka i informacija iz testa okruženja pre konverzije u proizvodnju.
 - f. Uverite se da su svi test računari i privatni računari uklonjeni pre aktiviranja proizvodnje.
 - g. Obavljati sigurnosnu recenziju kodova na sve kodove pre puštanja u proizvodnju.
- 25.2 Razviti sve web bazirane aplikacije pomoću sigurne smernice kodiranja, kao što su one proizvedene od IBM-a, bezbednosni projekat otvorene web aplikacije, i tako dalje. Redovno pregledajte kod zbog zajedničkih sigurnosnih propusta. Uključiti sledeće:
- a. Devalidizaciju ulaza.
 - b. Prekinuta ili neefikasna kontrola pristupa.
 - c. Prekinuta ili neefikasna autentičnost i menadžment sesije.
 - d. Ranjivost ukrštene skripte.
 - e. Propusti zasnovani na uvođenju, kao što su SQL-a, i LDAP...
 - f. Nepravilno ili nepostojeće rukovanje.
 - h. Nesigurna metoda ili tehnologija skladištenja.
 - i. Nesigurno upravljanje konfiguracijom.
 - j. Osetljivost na odbijanje servisnih napada.

- 25.3 Uverite se da su tragovi i izjave o otklanjenim greškama su uklonjeni iz proizvodnog koda.
- 25.4 Uverite se da aplikacija nema spisak imena grešaka.
- 25.5 Uverite se da su sve web izložene aplikacije zaštićene od napada poznatih po jednom od sledećih mehanizama:
 - a. Instalacija aplikacije zaštitnog zida.
 - b. Imati pouzdano treće mišljenje o aplikaciji zbog bezbednostnih propusta.
- 25.6 Sprovođenje programa za nadgledanje mreže i testiranje.
- 25.7 Obezbediti da se svaki proces povezuje sa jedinstvenim ID sa svim aktivnostima, a posebno onim aktivnostima koje se odnose na administrativne poslove.
- 25.8 Obezbediti da je revizija putanje omogućena za sve događaje, a naročito za sledeće:
 - a. Pogrešni pokušaji logovanja.
 - b. Svaki pokušaj sa administrativnim pristupom.
 - c. Svaki događaj koji uključuje pristup poverljivim podacima, PII podacima.
 - d. Svaki pristup funkcijama sistema ili revizorske staze.
 - e. Aktiviranje ili prestanak funkcije sistema ili procesa.
 - f. Sve administrativne aktivnosti.
 - e. Svako aktiviranje ili prestanak rada virtuelnih sistema.
- 25.9 Snimati sledeće informacije na minimum:
 - a. Korisnički ID.
 - b. Vreme događaja.
 - c. Opis događaja.
 - d. Poreklo događaja, ako je potrebno.
 - e. Uspeh ili neuspeh događaja.
 - f. Uticaj na entitet.
- 25.10 Proverite da li su osigurane sve revizije putanja.
- 25.11 Ograničiti pristup administrativnim funkcijama.
- 25.12 Ako je moguće, enkriptovati revizije putanja.
- 25.13 Osigurati da su revizije staza regularno bekapovane.
- 25.14 Koristiti praćenje i detekciju da bi se odredile neovlašćene izmene datoteka.
- 25.15 Osigurati da su satovi sinhronizovani.
- 25.16 Čuvati istoriju putanje revizije najmanje godinu dana, ili u skladu sa važećim regulatornim zahtevima.

- 25.17 Testirati bezbednosnu kontrolu zbog validnosti usklađivanjem alata za verifikaciju krajnjih tačaka protiv pretnji.
- 25.18 Testirati prijave pre primene usklađivanjem komercijalnih aplikacija i alata za proveru valjanosti servisa.
- 25.19 Obavljati testiranja penetracije najmanje jednom u 90 dana da se utvrdi da li su propusti uvedeni u svom cloud okruženju.
- 25.20 Razviti praćenje rešenja integriteta datoteka da se identifikuje uvođenje zlonamernog koda.

7 Razumevanje IBM-ove tačke gledišta u Cloud bezbednosti

IBM-a nudi perspektivnu informisanost o cloud sigurnosti na osnovu dugogodišnjeg iskustva u projektovanju, implementaciji i podršci rešenja cloud computing-a preko opsega vertikalnih industrija.

7.1 Ni "Jedna veličina odgovara svima" za bezbednost

Ne postoji jedna-veličina-odgovara-svima model za cloud bezbednost. Organizacije imaju različite bezbednosne zahteve koji su određeni jedinstvenim karakteristikama poslovnog opterećenje koje oni nameravaju da prenose u cloud.

Organizacije imaju mnogo različitih zahteva za integraciju između cloud okruženja i njihovih pomoćnih sistema. Neke organizacije u potpunosti razvijaju nove aplikacije i spremne su da izgrade svoju cloud okolinu da bude nezavisna od bilo koje postojeće operacije, ali većina klijenata preduzeća će početi sa hibridnim ili privatnim cloud-om gde je integracija sa sistemima preduzeća glavni zahtev.

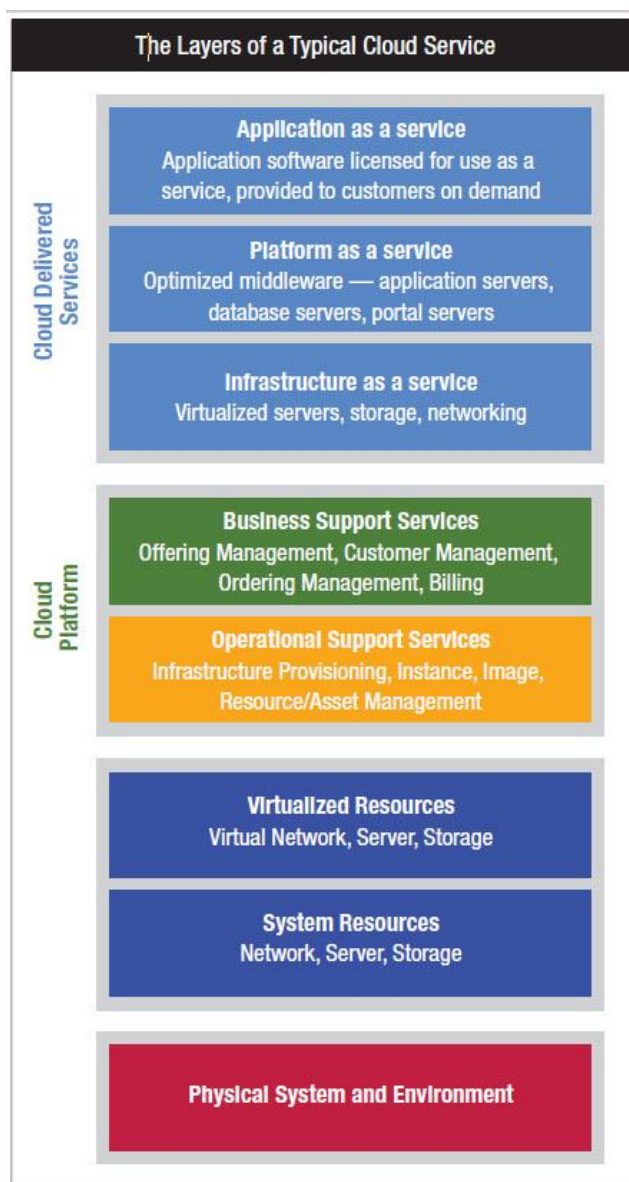
U tom kontekstu, lakoća sa kojom postojeći bezbednosni menadžment infrastrukture može biti produžen u cloud i, naročito, upotreba ujedinjenih protokola- su važne potvrde za uspešnu primenu. Identitet saveza protokola kao što su Open ID I Security Assertion Markup Language (SAML) dobijaju veliku pažnju javnosti i igraju važnu ulogu za javne cloud-se, ali u preduzeću niz drugih protokola treba da bude podržan. Ovi protokoli imaju za cilj da brzo prenose podatke iz pomoćnog sistema preduzeća u privatni ili hibridni cloud.

Različite vrste opterećenja zahtevaju različite nivoe sigurnosti. Jedan od glavnih zahteva je potreba za spoljnom bezbednosnom provere ili validacijom, i vlada čak izražava potrebu za formalnu validaciju i sertifikaciju. Snaga provere identiteta, da se uverite da su korisnici koji se prijavljuju na servis zaista oni koji tvrde da su i snaga mehanizama autentikacije će varirati u zavisnosti od tipa opterećenja. Kao odgovor, novi javni servisi za verifikaciju identiteta koji se postavljaju, nude različit nivo kvaliteta usluga.

Potrebe za senkrijom se veoma razlikuju od jednog do drugog klijenta. Određeni klijenti nalažu korišćenje određenih kriptu-algoritama i zahtevaju veoma visoka ograničenja o tome ko može imati pristup ključevima, dok ostali klijenti mogu da zahtevaju enkripciju samo za određene podatke i mogu ovlastiti da ključem upravlja pouzdani cloud provajder.

Postoji velika varijacija u raspoloživosti mogućnosti, uključujući i dozvoljeno vreme za provajdera da reaguje i da se oporavi od neuspeha. Zahtevi se razlikuju za intervale u kojima se vrši provera bezbednosti i uslužnosti.

To je IBM tačka gledišta da provajder preduzeća cloud klase usluge mora da podržava niz bezbednosnih i usluga na nivou mogućnosti, kao i industrijske standarde zasnovane na bezbednosnoj infrastrukturi, što ih čini lakim za integraciju sa postojećim operacijama. Pored toga, provajder servisa mora da se integriše sa i proširi mogućnosti klijentove cloud bezbednosti prema potrebi.



Slika 22: Slojevi tipičnih cloud servisa1. [1]

7.2 Osnovni arhitektonski model za Cloud Computing

Osnovni arhitektonski model za cloud computing se sastoji od gomile slojevitih servisa:

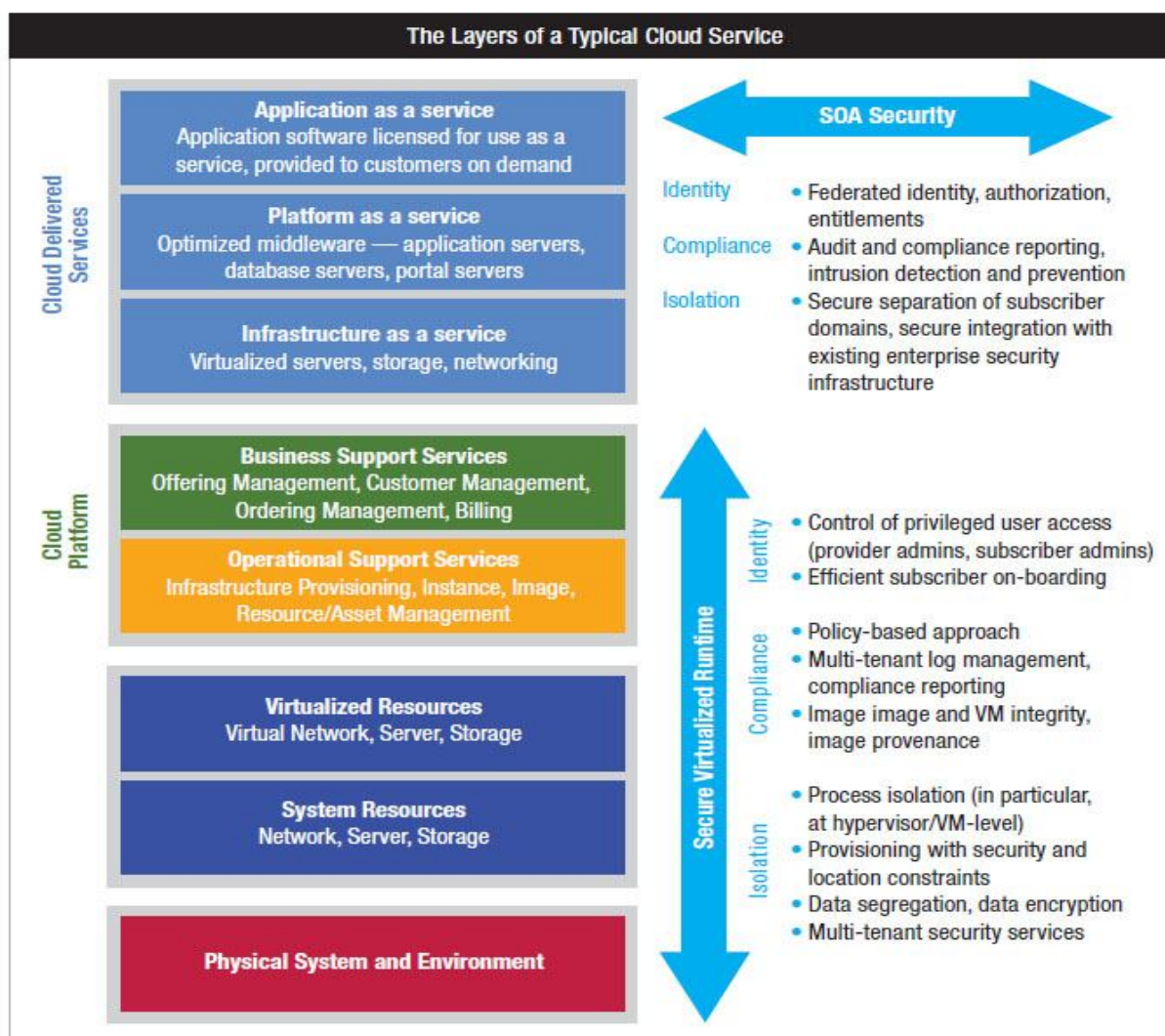
-Sloj fizičkog sistema opisuje normalne zahteve centra podataka, nalaže kontrolu pristupa i monitoring mera objekta.

-Sloj resursa sistema upravlja mrežnom , serverima i infrastrukturom skladištenja.

-Sloj virtuelnih izvora predstavlja snažnu izolaciju kao glavnu vrednost virtuelizacije bezbednosti: izoluju procese kroz hipervizore i podatke odvajanja.

Sledeći slojevi su operativne službe podrške (OSS) i usluge poslovne podrške (BSS) koji definišu platformu cloud menadžmenta. Na vrhu su razni cloud dostavni servisi ,Infrastruktura kao servis, Platforma kao servis, i Aplikacija kao servis.

Bezbednosni zahtevi postoje na svakom sloju ove arhitekture, a izuzetno je važno da se održi konzistentnost između ovih slojeva. Na primer, ako sigurnosna politika na najvišem nivou definiše da korisnička informacija ne sme da napusti zemlju, onda na nižem nivou fizičkih resursa, prostor na disku mora biti označen u zemlji koja će sačuvati te podatke.



Slika 23: Slojevi tipičnih cloud servisa2. [1]

7.3 Cloud bezbednost i SOA

Cloud arhitektura opisana ovde nam omogućava da izgradimo vrlo jednostavan model cloud bezbednosti koji se sastoji od dva glavna koncepta: SOA bezbednosni sloj koji se nalazi na vrhu novog Sigurnog Virtuelnog Trajnog sloja.

Sloj cloud servisa za isporuku je kompleksno, distribuirano SOA okruženje. Različiti servisi se mogu širiti kroz različite oblake u okviru preduzeća. Usluge mogu biti u različitim administrativnim i bezbednosnim oblastima koje se povezuju zajedno da bi formirali jednu cloud aplikaciju. SOA bezbednosti model se u potpunosti primenjuje na oblak. web servisi protokol predstavlja osnov za SOA bezbednost, i dakle, i za oblak bezbednosti. Ovaj sigurnosni model je u potpunosti podržan preko IBM softvera. Rešenje, kao što su IBM Tivoli® Federalni identitet menadžer obezbeđuje široku, standardizovanu podršku za povezivanje različitih domena bezbednosti da dostavi objedinjen pristup korisnika do cloud servisa usluga. Ovo je posebno važno kod vezivanja unutrašnjih IT resursa zajedno sa spoljnom cloud uslugom u hibridni cloud model, ili kod pakovanja nekoliko spoljnih usluga u brendiran i ponuđen krajnjim kupcima.

Jedan od ključnih aspekata SOA je sposobnost da lako integriše različite servise od različitih provajdera. Cloud computing gura ovaj model jedan korak dalje od većine preduzeća SOA okruženja, jer oblak ponekad podržava veliki broj članova, usluga i standarda. Ova podrška je predviđena za veoma dinamičan i agiln način rada, i pod vrlo složenim odnosima poverenja. Konkretno, SOA cloud nekad podržava velike i otvorene korisničke populacije, i to ne može da preuzme unapred uspostavljena veza između provajdera i cloud pretplatnika.

Mnoge cloud implementacije se fokusiraju na određene protokole, kao što je Otvoreni ID na identitet federacije, i omiljene specifične arhitektonske stilove, kao što je reprezentativni državni prenos (REST). IBM-ova je tačka gledišta da preduzeće cloud klase računara ne sme da ograničava svoje korisnike na protokol ili određeni stil, već ponudi fleksibilnost i izbor. Iako IBM podržava REST-bazirani interfejs i protokole, gde je potrebno, SOA bezbednosti je potreban čitav niz bezbednosnih službi kao što je opisano u SOA bezbednosnom Referentnom modelu.

Standardom zasnovana provera, upis i autentifikacija korisnika cloud servisa predstavljaju samo vrh ledenog brega sigurnosti da pravi korisnici imaju pravo pristupa pravim resursima. Konzistentna politika za prava i kontrolu pristupa su potrebne da se obezbedi da se sve osnovne komponente cloud servisa pridržavaju održavanju poverljivosti podataka i poštovanja propisa. Na primer, medicinska istraživačka aplikacija vuče podatke iz kliničkih i servisa za plaćanje iz više bolnica, tako da ime pacijenta i druge lične informacije moraju biti uklonjene iz svih izvora. Centralizovano pravno upravljački servis, kao što je IBM Tivoli Security Policy Manager, može da pomogne osiguranju da se zajednička politika definiše i sprovodi da zaštitimo poverljivost pacijenata u svim cloud servisima.

Cloud provajderi mogu podržati i SaaS i IAAS unutar i između cloud-a. Provajder treba da se pridržava najbolje praktične implementacije i klijentima obezbedi maksimalnu vidljivost u sigurnost i poštovanje položaja cloud servisa. IBM Rational® AppScan® portfolio može da pomogne u podršci bezbednosti aplikacije. IBM Tivoli Security Information i menadžer događaja obezbeđuju konsolidovane stavove evidencije bezbednosti i revizije izveštaja koji

se mogu koristiti da se pokaže usklađenost napora i identifikuju pretnje od privilegovanih insajdera. Sposobnost da prati i odgovori na pretnje od strane privilegovanih IT administratora zauzima veliki značaj u javnom cloud modelu, gde nezavisni administratori imaju pristup podacima iz različitih organizacija.

Sigurni virtuelni trajni sloj (Secure Virtualized Runtime layer) na dnu je virtuelnih sistema koji pokreće procese koji pružaju uvid u podatke o skladištima podataka. Ovaj run-time sistem se razlikuje od klasičnog run-time sistema koji radi na virtuelnoj mašini slike pre nego na pojedinačnim aplikacijam. On pruža bezbednosne usluge kao što su antivirusi, introspekcija i spoljni sigurnosni servisi oko virtualne slike.

Iako temelj Secure Virtualized Runtime postoji pre SOA bezbednosti i izgrađen je na decenijama iskustva sa glavnim arhitekturama, razvoj Secure Virtualized Runtime je i dalje veoma u toku. IBM kontinuirano ulaže u istraživanje i razvoj jače izolacije na svim nivoima mreže, servera, hipervizora, procesa i infrastructure skladištenja da podrži masivni zakupni prostor.

Obezbeđivanje virtuelnih sredstava primorava domen bezbednosti i ograničenja lokacije. Virtuelna sredstva moraju biti grupisani na osnovu politike, i automatizacija upravljanja bezbednosne konfiguracije obezbeđuje konzistentnost.

U okviru Secure Virtualized Runtime, bezbednosne službe su takođe rastući iskorišćene kroz SOA usluge, pružanja identiteta, revizije, upravljačkih ključeva, politiku i druge usluge. IBM® Proventia Mrežna virtuelna bezbedonosna platforma je prostrana virtuelna platforma koja obezbeđuje sigurnost od pretnji kao što su sprečavanje upada, zaštita web aplikacija i zaštita mreže za sprovođenje politike.

7.4 Mogućnost da se pojednostavi kontrola bezbednosti i odbrane

Iako se na cloud computing često gleda kao na povećanje bezbednosnih rizika i pretnji uvođenja novih vektora, on takođe predstavlja uzbudljivu priliku da se poboljša bezbednost. Karakteristike cloud-a, kao što su standardizacija, automatizacija i povećanje vidljivosti u infrastrukturu može dramatično povećati nivo bezbednosti.

Na primer, upotrebom definisanog skupa cloud interfejsa, zajedno sa centralizovanim identitetom i politikom kontrole pristupa, smanjuje se rizik od korisničkih pristupa do nepovezanih izvora. Pokretanje računarskih servisa u izolovanim oblastima, pružanje podrazumevanih enkripcija podataka u kretanju i u mirovanju, kao i kontrola podataka kroz virtuelno skladištenje su postali aktivnosti koje mogu unaprediti odgovornost i smanjiti gubitak podataka.

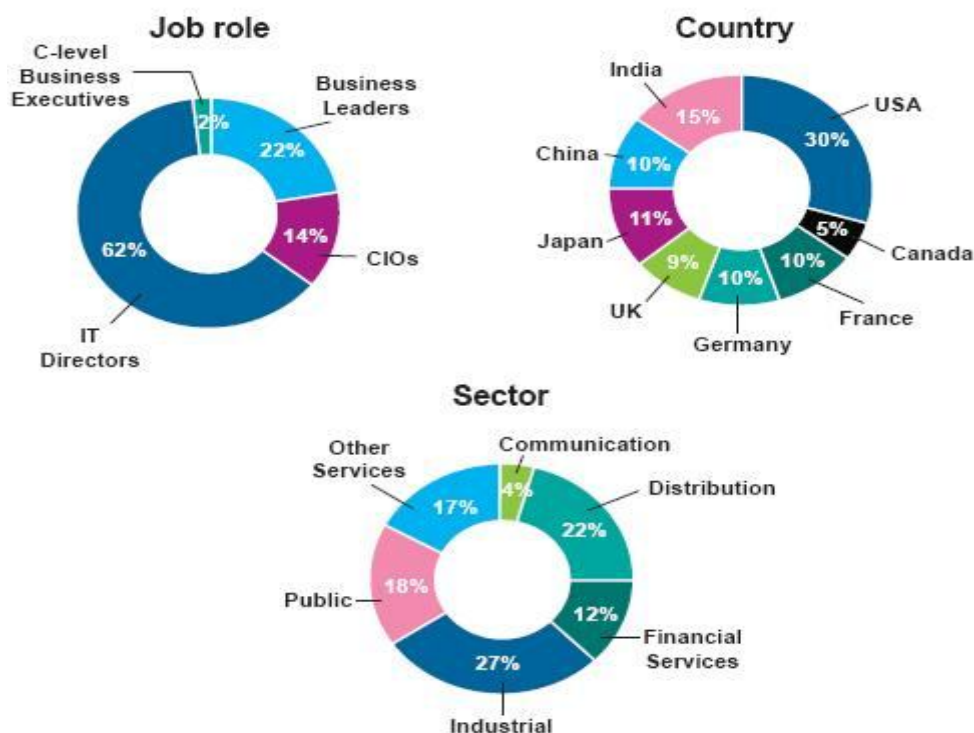
IBM-istraživači, programeri i bezbednosni stručnjaci širom sveta su dobili nagrade za više od 3.000 patenata bezbednosti i upravljanja rizikom.

IBM-a nudi neuporedivu sposobnost da se fokusira na upravljanje poslovnim inovacijama i obezbeđivanje operativnih procesa u svim rizičnim domenima. Njegova sveobuhvatna rešenja i usluge omogućavaju organizacijama da smanje kompleksnost bezbednosti u okviru svojih preduzeća i da primenjuju holističku strategiju menadžmenta bezbednosti.

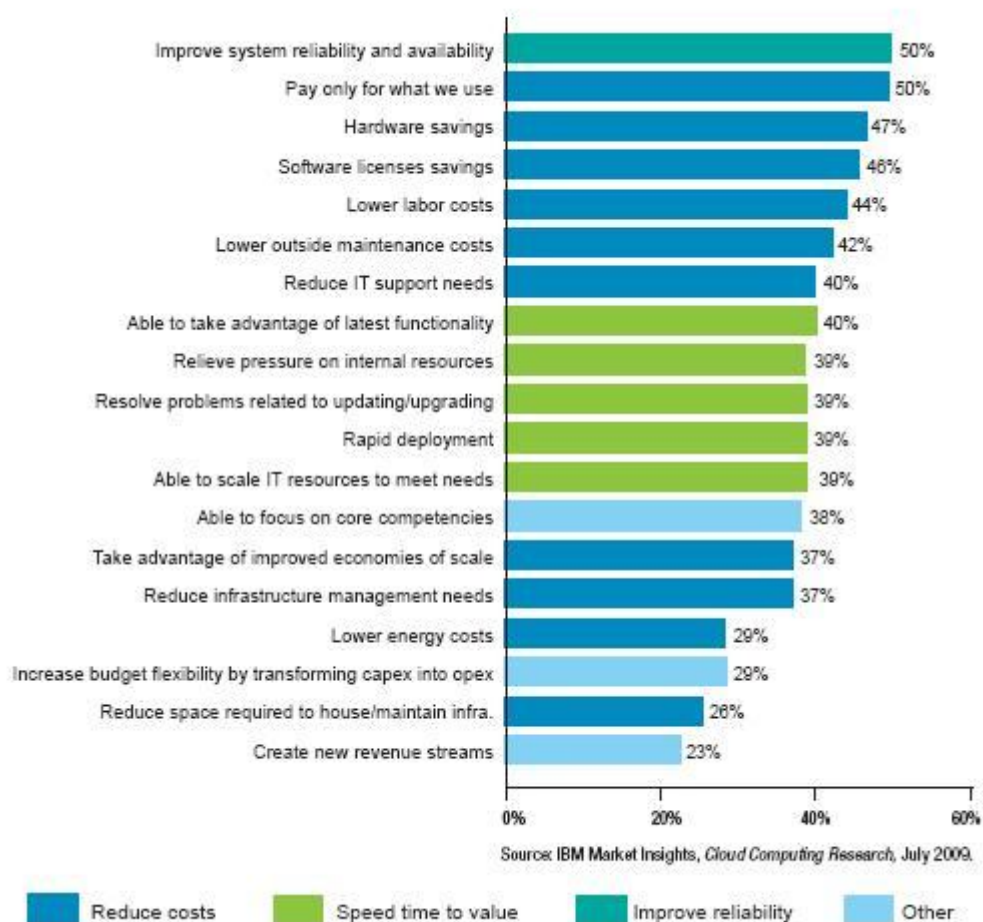
Sa IBM-om, organizacija može da razvije sveobuhvatna, skalabilna, standardizovana rešenja u okviru preduzeća, podržavajući njihove bezbednosne potrebe i sada i u narednim godinama.

8 IBM-ova anketa obima i definicije

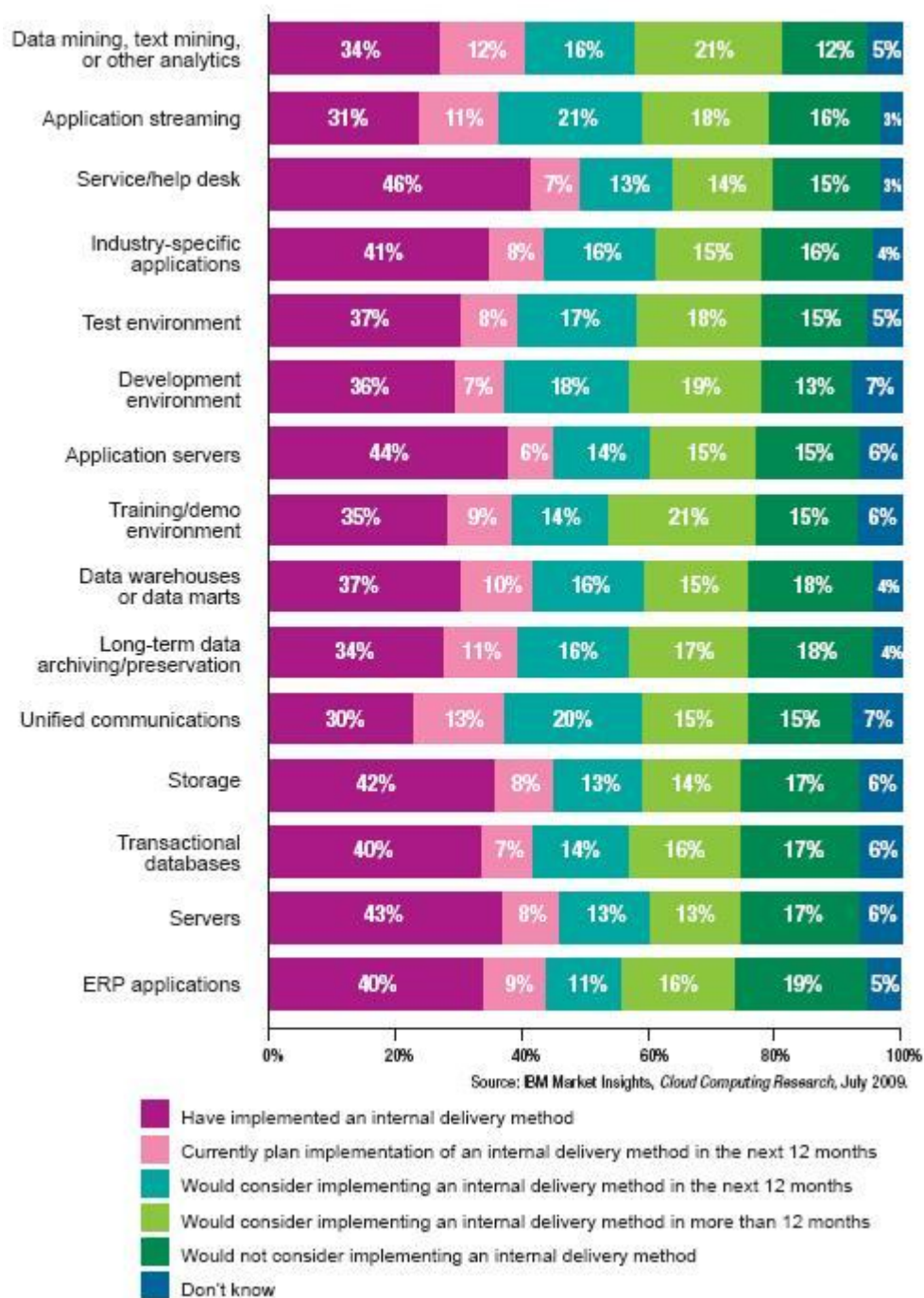
Popularnost cloud computing-a i njegov potencijal da transformiše isporuku usluga doveo je do toga da sve veći broj organizacija implementira cloud computing za jedno ili više opterećenja, a mnoga druga ga aktivno razmatraju. Anketirane su IT i linije poslovanja donosilaca odluka širom SAD, Kanade, Francuske, Italije, Nemačke, Velike Britanije, Japana, Kine i Indije. Većina anketiranih su iz kompanija koje imaju između 1.000 i 9.999 zaposlenih (videti sliku 1). Anketirani su zastupljeni u raznim industrijama, uključujući javni sektor, komunikacije, distribuciju, finansijske usluge i drugo.



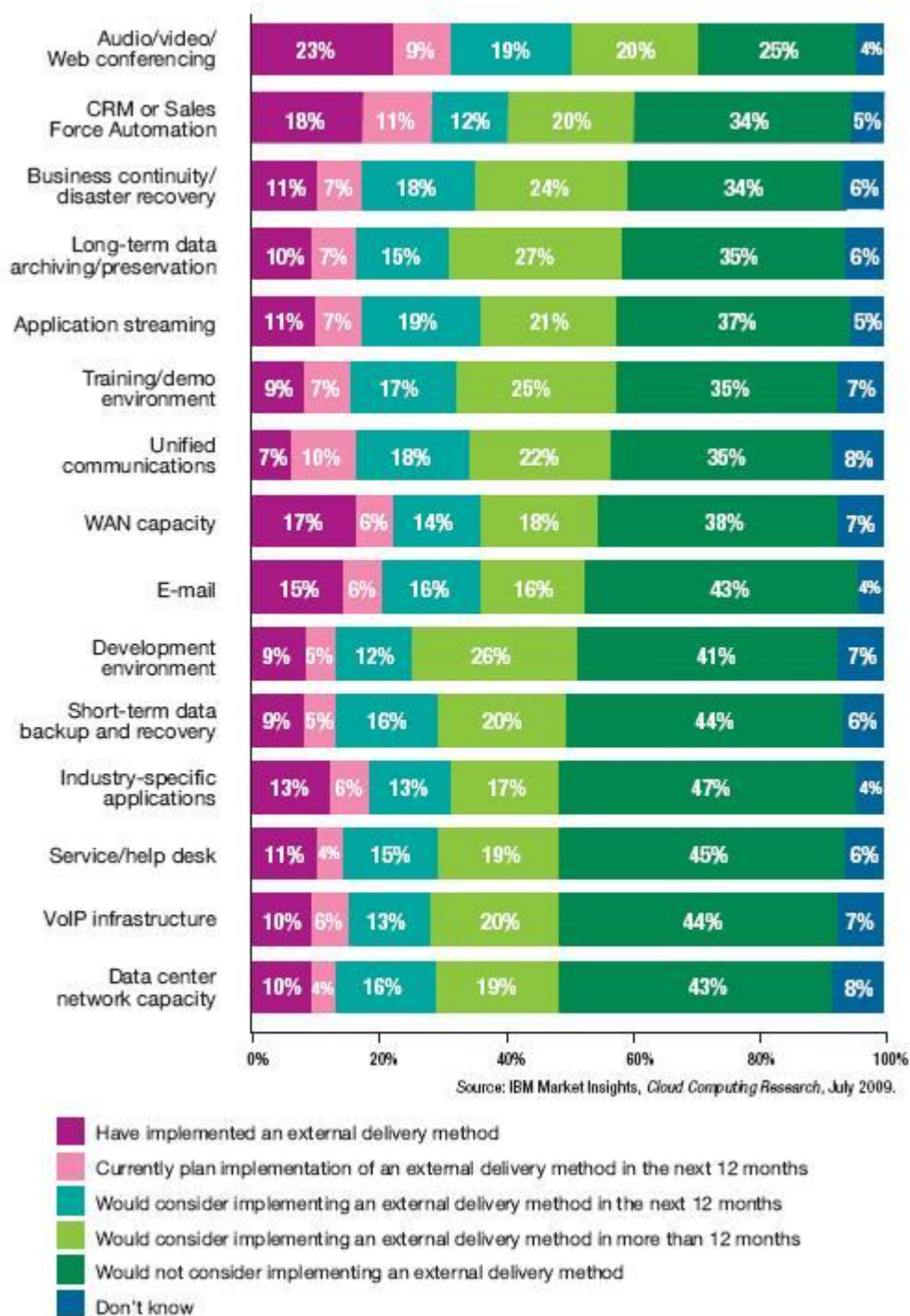
Slika 24: Demografija ankete. Pokazuje IBM-ovu cloud computing anketu koja uključuje IT i donosiocce poslovnih odluka iz 8 zemalja, predstavljajući presek industrije i veličine kompanije. [3]



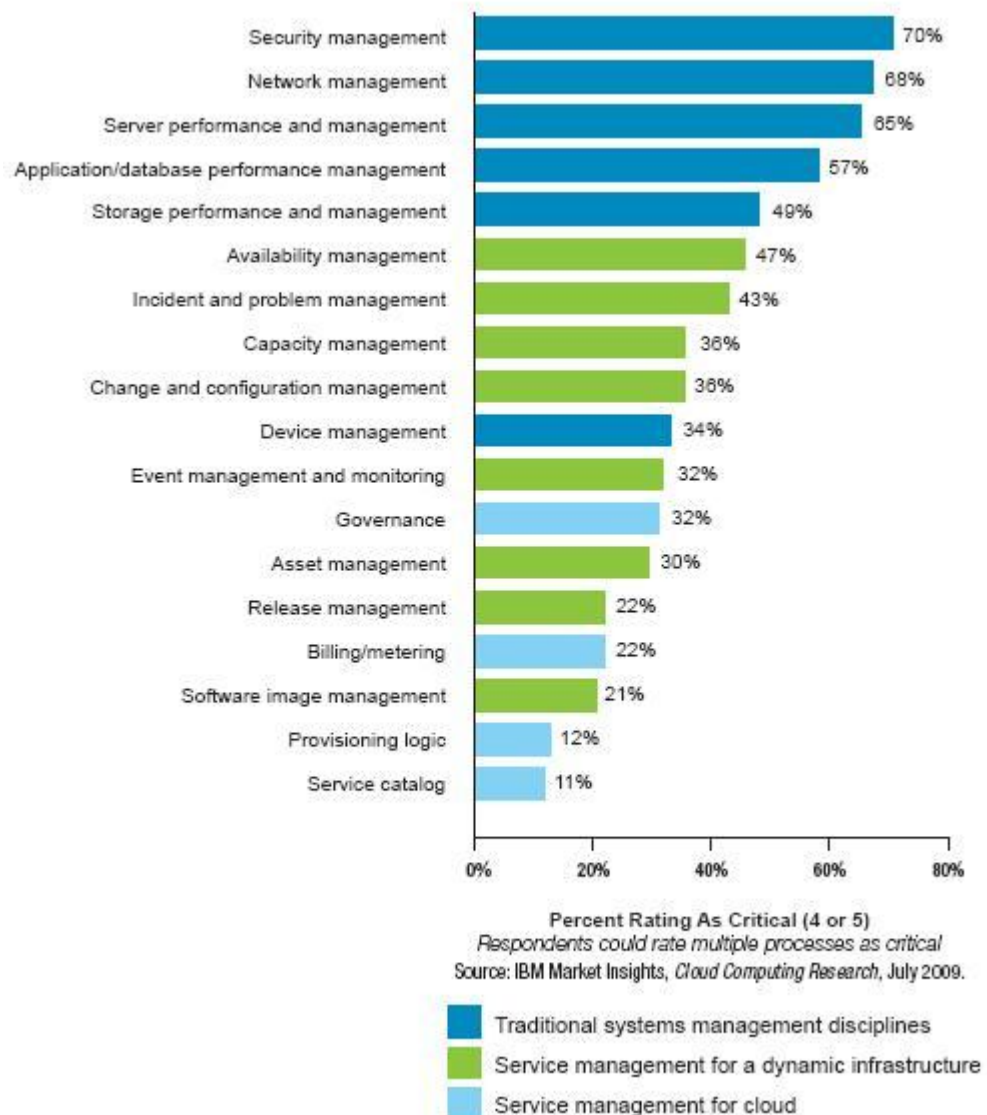
Slika 25: Ušteda, vreme za proračun vrednosti i poboljšanje dostupnosti su vodeće atrakcije za korišćenje javnog cloud servisa. [3]



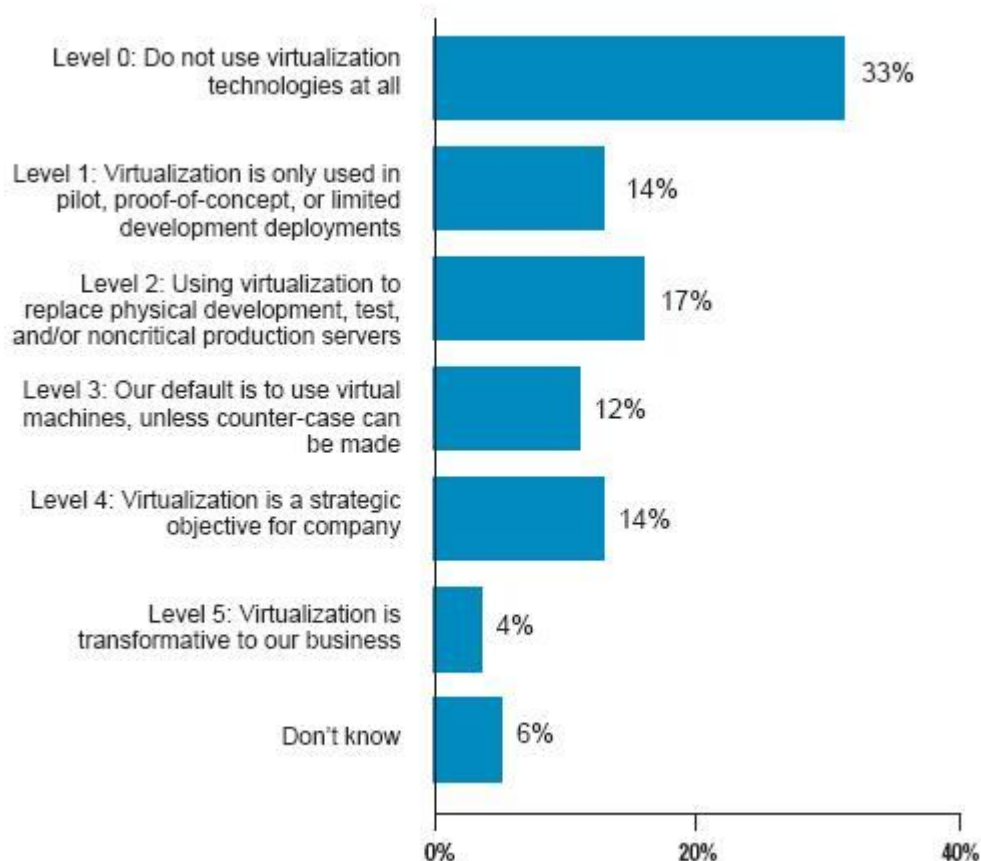
Slika 26: Poželjnija privatna cloud opterećenja. Analitika, strimovanje aplikacija, usluga / službe pomoći, specifične aplikacije industrije i testiranje i razvoj su najviše zastupljeni za privatni cloud. [3]



Slika 27: Poželjnija privatna cloud opterećenja. Konferencije i CRM ili prodajna automatizacija su na vrhu liste prioriteta javnih cloud opterećenja. [3]



Slika 28: Kritičnost upravljanja menadžment servisom. Odgovori pokazuju nedostatak značaja dat menadžment servisu koji je bitan za pružanje usluga preko cloud-a. [3]



Slika 29: Upotreba tehnologije virtualizacije. Samo 18 odsto ispitanika navelo da virtualizaciju smatra strateškim ciljem ili transformacionom tehnologijom za svoje organizacije. [3]

9 Zaključak

Cloud computing obezbeđuje efikasan, skalabilan i isplativ način za današnje organizacije da dostave poslovne ili potrošačke IT usluge preko Interneta. Različiti modeli cloud computing-a su na raspolaganju, pružaju i solidnu podršku za osnovne poslovne funkcije i fleksibilnost da isporuče nove usluge.

Međutim, fleksibilnost i otvorenost modela cloud computing-a stvorili su veliki broj bezbednosnih problema. Ogromne količine IT resursa se dele među mnogim korisnicima i bezbednosti procesa su često skrivene iza slojeva apstrakcije. Cloud computing se često nudi kao usluga, tako da se kontrola podataka i operacija prebacuje na nezavisnog provajdera servisa, zahtevajući da njihovi klijenti uspostave odnos poverenja sa svojim provajderima i razviju rešenja za sigurnost koja ovaj odnos uzima u obzir.

U ovom radu predstavili smo uputstva o bezbednosti cloud computing-a. Ispitan je veliki broj bezbednosnih izazova za cloud provajdere i njihove klijent, i razgovarano je o konkretnim uputstvima za sprovođenje kontrole sigurnosti cloud-a koja se baziraju na priznatim bezbednosnim okvirima industrije i najbolje prakse.



Slika 30: Jedan klik za cloud [4]

10 Literatura

- [1] IBM Corporation (International Business Machines Corporation) 2010.
<http://www.redbooks.ibm.com/redpapers/pdfs/redp4614.pdf>
- [2] IBM Corporation (International Business Machines Corporation) 2010.
http://linux1.beausanders.com/whitepapers/Benefits_of_Cloud_Computing.pdf
- [3] IBM Corporation (International Business Machines Corporation) 2010.
<ftp://ftp.software.ibm.com/common/ssi/sa/wh/n/ciw03062usen/CIW03062USEN.PDF>
- [4] Google.com (Google Inc.) 2010.
http://images.google.com/images?hl=sr&source=hp&q=cloud+computing&gbv=2&aq=f&aqi=g10&aql=&oq=&gs_rfai=