SVEUČILIŠTE U ZAGREBU

FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI

SIGURNOST I RAČUNARSTVO U OBLAKU

DIPLOMSKI RAD

Studentica: Ivana Zovko

Mentor: dr. sc. Vedran Juričić

Zagreb, lipanj 2017.

Sadržaj

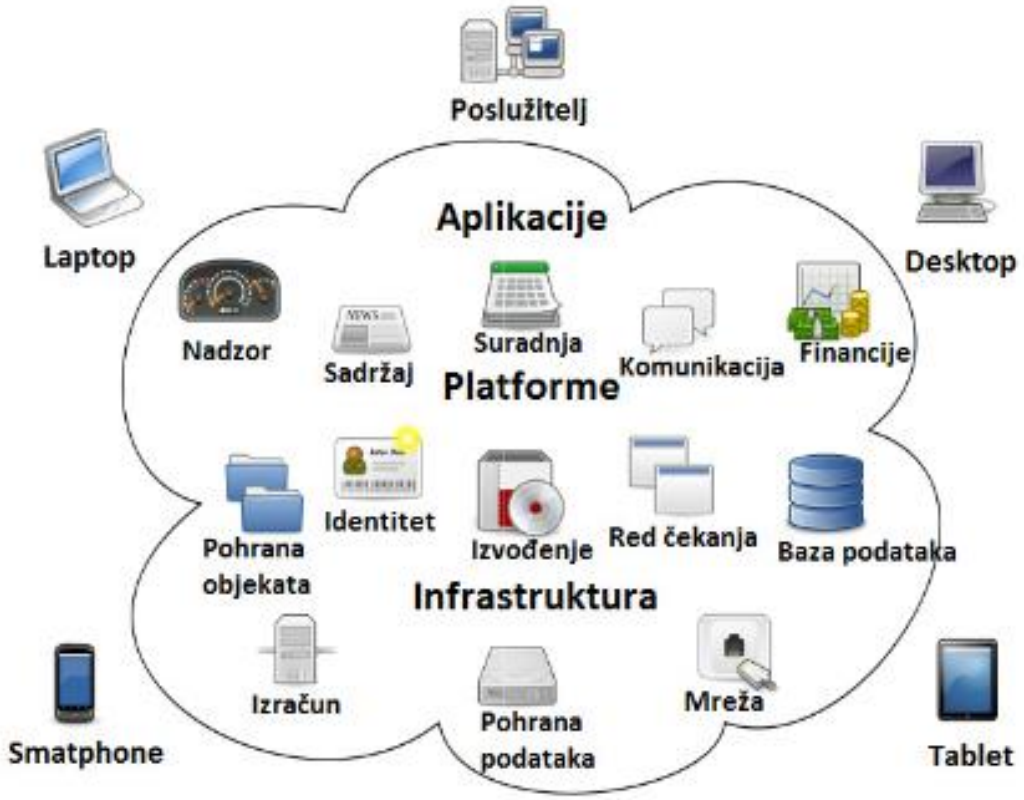
Sažetak

Računarstvo u oblaku je koncept koji se zbog niza prednosti sve više koristi od strane tvrtki i pojedinaca. Međutim, važno je obratiti pažnju na sigurnost pri korištenju oblak usluga. Budući da postoji više modela računarstva u oblaku, u radu će se prikazati kakva je sigurnost tih modela. Cilj ovoga rada jest prikazati neke od specifičnih sigurnosnih rizika, glavne prijetnje sigurnosti računarstva u oblaku te sigurnosne zahtjeve koje je poslužitelj usluge dužan osigurati. Također će se opisati aspekti sigurnosti računarstva u oblaku koji se smatraju jako važnima sa stajališta organizacija kao što su: pravna regulativa, sigurnosne kontrole i sl. Mnoge se međunarodne organizacije bave pitanjem sigurnosti računarstva u oblaku te će se u ovom radu navesti standardi koji su produkti njihova rada. Na temelju tih standarda i sigurnosnih rješenja unutar rada će se usporediti razine sigurnosti nekih od najpoznatijih oblak servisa. Osim toga, opisat će se neki od najčešćih napada ne oblak servise. Svrha rada jest prikazati na što je sve potrebno obratiti pažnju pri odabiru oblak servisa.

Ključne riječi: računarstvo u oblaku, sigurnost, oblak servisi.

1. Uvod

Računarstvo u oblaku je koncept koji se u posljednje vrijeme sve više koristi, kako od strane velikih tvrtki tako i od strane pojedinih korisnika. Postoje razne definicije navedenoga koncepta, a prema Američkom državnom institutu za standarde i tehnologiju (eng. *National Institute of Standards and Technology, NIST*) računarstvo u oblaku je model obrade podataka koji omogućuje sveprisutan jednostavan pristup djeljivih računalnih resursa poput računalnih mreža, poslužiteljskih računala, medija za pohranu podataka, aplikacija i usluga, koje je moguće konfigurirati i stavljati na raspolaganje korisnicima uz njihov minimalan osobni angažman ili uz najmanju moguću interakciju s poslužiteljem tih resursa.[1]



Slika. Računalni oblak[2]

[1] Panian, Željko. Elektroničk poslovanje druge generacije. Zagreb: Ekonomski fakultet Zagreb, 2013. Str. 172

[2] Radić, Branimir. Sigurnost u računalnom oblaku. URL: http://www.fer.unizg.hr/_download/repository/KDI%2C_Branimir_Radic.pdf (2017-04-02)

Postoje tri glavna modela usluga računarstva u oblaku:

1.) Softver kao servis (eng. *Software-as-a-Service, SaaS*) u kojem korisnik oblaka kontrolira samo konfiguracije aplikacija
2.) Platforma kao servis (eng. *Platform-as-a-Service, PaaS*) u kojoj korisnik oblaka također kontrolira hosting okruženja
3.) Infrastruktura kao servis (engl. *Infrastructure-as-a-Service, IaaS*) u kojoj korisnik oblaka kontrolira sve osim infrastrukture podatkovnih centara.

Nadalje, postoje četiri glavna modela implementacije:

1.) Javni oblak koji je dostupan široj javnosti
2.) Zajednički oblak koji služi nekoliko organizacija
3.) Privatni oblak koji je ograničen na jednu organizaciju
4.) Hibridni oblak koji je mješavina drugih.[3]

Računarstvo u oblaku koristi informatičko okruženje i informacijske sustave koji za sobom povlače pitanje sigurnosti. Za korisnike ove usluge važna je sigurnost budući da se njihovi podaci pohranjuju u oblaku. Zbog toga pružatelji oblak usluga svojim korisnicima trebaju pružiti uvid u njihov rad na tom području.

Unutar ovoga rada razrađeno je pitanje sigurnosti korištenja računarstva u oblaku. Prije svega navedeni su i opisani aspekti sigurnosti koji su vezani uz računarstvo u oblaku. Osim toga, navedeni su sigurnosni problemi i rizici kojima se korisnici izlažu pri upotrebi usluga u oblaku. Naime, problemi i rizici pri korištenju ovakvih usluga su uvijek prisutni, ali je potrebno učiniti određene korake kako bi se oni sveli na minimum. Korisnici također moraju istražiti koje sigurnosne usluge pružaju oblak servisi kako bi se mogli odlučiti kojem od njih će povjeriti svoje podatke.

U radu će se također navesti prikladna sigurnosna rješenja pomoću kojih pružatelji oblak usluga mogu korisnicima pružiti sigurnost. Mnoge međunarodne organizacije i udruženja nude različite certifikate za sigurnost i privatnost. Svaki certifikat je potvrda za

[3] Chen, Yanpei; Paxson, Vern; Katz, Randy H. What's New About Cloud Computing Security?. Electrical Engineering and Computer Sciences University of California at Berkeley, 2010. URL: http://www.utdallas.edu/~muratk/courses/cloud13s_files/what-is-new-in-cloud-security.pdf (2017-03-29)

određenu sigurnosnu značajku, a korisnik pomoću certifikata koje ima pojedini oblak servis može procijeniti koliko je on siguran za korištenje.

Na temelju određenih sigurnosnih rješenja i certifikata provedeno je istraživanje tri najpoznatija oblak servisa. Nakon prikupljenih podataka s njihovih stranica, napravljena je usporedba istraživanih oblak servisa kako bi se vidjelo koji od njih pruža korisnicima sigurno korištenje njihovih usluga te im omogućuje uvid u njihov rad na području sigurnosti. Iako se neprestano radi na pružanju i poboljšavanju sigurnosnih postavki, napadi se događaju. No svaki napad omogućuje učenje i napredovanje. U radu se navode neki od najčešćih napada na oblak servise.

2. Modeli računarstva u oblaku i sigurnost

Kao što je navedeno u uvodu, računarstvo u oblaku pruža usluge kroz tri osnovna modela (SaaS, PaaS i IaaS). Ti modeli pružaju korisniku infrastrukturne resurse, aplikacijske platforme i softversku podršku. Prema tome je ideja o individualnoj procjeni i ispitivanju platformi te pružanju individualne sigurnosti za svaku uslugu nakon njihove diferencijalne procjene prihvaćena u pružanju informacijske sigurnosti. Korisnici računarstva u oblaku prvenstveno očekuju kako će sigurnost svih pružatelja usluga biti na istoj razini.

2.1 SaaS i sigurnost

SaaS platforma je usluga kroz koju računarstvo u oblaku nudi softverske usluge svojim korisnicima. Postoji niz gotovih softverskih programa za obradu sigurno pohranjenih podataka. Dok SaaS usluga pruža korisnicima neke osnovne funkcije kao što su autentikacija (eng. *authentication*) za sigurnu komunikaciju, kontrolu autorizacije (eng. *authorization*) i sigurnu pohranu podataka, može se povezati i s korisnicima različitih usluga. Osim toga, mnogi IT odjeli i vladine agencije koriste SaaS platforme. Najvažnija točka jest razina sigurnosti poslužitelja na kojima se pohranjuju podaci korisnika. Činjenica da su vrlo povjerljivi podaci države, posebni osobni podaci ili podaci o kupcu tvrtke pohranjeni na istim poslužiteljima, potrebna je izuzetna opreznost u smislu sigurnosti informacija i privatnosti. U suprotnom je moguć pristup povjerljivim informacijama od strane neovlaštenih osoba. Zbog toga je vrlo važno čuvati sigurnost podataka na SaaS platformi.[4]

2.2 PaaS i sigurnost

PaaS je platforma na kojoj postoje aplikacije i razvojni alati za korisnike unutar računarstva u oblaku. Ova platforma nudi alate za razvoj pohrane, upravljanja i virtualnih aplikacija potrebnih korisnicima. Virtualni strojevi uključeni u PaaS moraju biti zaštićeni od zlonamjernih programa (eng. *malware*) i trojanaca (eng. *trojans*). Zaštita privatnosti podataka osigurava očuvanje integriteta sadržaja u razvijenim aplikacijama i olakšava prijenos podataka između pouzdanih mreža. Osim toga, ona također mora osigurati provjere valjanosti

[4] Yesilyurt, Murat; Yalman, Yildiray. New approach for ensuring cloud computing security: using data hiding methods. // Indian Academy of Sciences 41, 11(2016), str. 1289-1298. URL: http://web.b.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=2&sid=b3d70d07-b48e-4193-95ff-6ed17fb6cd45%40sessionmgr102&hid=118 (2017-05-21)

profila na potpuni i siguran način. Još jedna točka koju treba uzeti u obzir je provođenje pregleda u redovitim razmacima kako bi se spriječio prolazak zlonamjernih aplikacija kroz arhitekturu oblaka.[5]

2.3 IaaS i sigurnost

U prvom redu IaaS igra ulogu kao davatelj osnovnih sigurnosnih alata poput vatrozida (eng. *firewall*). Na platformi IaaS sigurnosne ranjivosti koje se mogu pojaviti u upravljanju virtualizacijom manje su uobičajene u usporedbi s ostalim platformama, a taj se proces bolje kontrolira. S druge strane, drugi važan faktor je primjenjivanje različitih tehnika kako bi se osigurala maksimalna privatnost i sigurnost uz virtualizaciju koja se primjenjuje zbog pohrane podataka u fizičkoj strukturi. Zbog razlike između modela oblak usluga, kako bi se osigurala sigurnost informacija, pružatelji usluga moraju primijeniti različite tehnike. U tom smislu, druga aplikacija koja se koristi kao sigurnosni protokol na IaaS platformi i ima mnoge prednosti u pružanju usluga računarstva u oblaku je sigurnosni protokol za automatizaciju sadržaja (eng. *security content automation protocol, SCAP*). Naglašeno je kako je važno razviti SCAP kao univerzalni sigurnosni standard.[6]

[5] Isto

[6] Isto

3. Aspekti sigurnosti računarstva u oblaku

Kada je riječ o računarstvu u oblaku, potrebno je obratiti pažnju na aspekte sigurnosti koji su vezani za njega. Postoje tri različita aspekta iz kojih je potrebno sagledati sigurnost korištenja računarstva u oblaku. Ti aspekti se odnose na pravnu regulativu, sigurnosne kontrole i federalizaciju sigurnosnih usluga.

3.1 Pravna regulativa

Pravna regulativa se odnosi na zakone i ostale pravne akte koji određuju sigurnosne zahtjeve koji su višeg prioriteta od onih funkcionalnih i tehničkih. U različitim zemljama svijeta vlast izražava svoju zabrinutost zbog sve intenzivnije primjene koncepta računarstva u oblaku u zonama njihove ingerencije. Neke zemlje su pak donijele rigorozne propise o zaštiti privatnosti koje zabranjuju pohranjivanje određenih podataka na fizičkim medijima i uređajima koji su locirani izvan zemlje. Tako pokušavaju zaštititi vlastite podatke i podatke svojih stanovnika. Na primjer, ako su podaci pohranjeni unutar teritorija Europske Unije, pružatelj usluga računarstva u oblaku iz SAD-a morat će znati europske propise koji se u nekim slučajevima uvelike razlikuju od američkih. Mnoga stručna udruženja, poslovne asocijacije i interesne grupacije razvijaju vlastitu regulativu koja nema zakonsku snagu, ali ipak ima snažan utjecaj unutar zajednice.[7]

3.2 Sigurnosne kontrole

Kada je riječ o sigurnosnim kontrolama postoji niz kontrola koje treba prakticirati u informatičkom okruženju i informacijskom sustavu pri čemu okruženje računarstva u oblaku nije nikako izuzetak. Pojedine sigurnosne kontrole koje su neophodne, danas su u velikoj mjeri standardizirane. Primjer takvih kontrola jest serija standarda ISO 27000.[8]

Postoji više sigurnosnih kontrola, a jedna od njih je upravljanje imovinom. Ona predstavlja omogućavanje upravljanja svom hardverskom mrežom i softverskom imovinom koja tvori infrastrukturu oblaka. Sljedeća je kriptografija (eng. *encryption*) tj. upravljanje ključevima i certifikatima koja uključuje primjenu kriptografskih funkcija i usluga zasnovanih na standardima za podršku sigurnosti informacija u mirovanju, ali i u pokretu. Sigurnost podataka i uređaja za pohranu jest sigurnosna kontrola koja zahtijeva omogućavanje pohranjivanja podataka u kriptografski zaštićenom formatu. Sigurnost krajnjih točaka je

[7] Panian, Željko. Nav. dj., str. 197 - 198

[8] Isto

kontrola koja konzumentima usluga u oblaku osigurava krajnje točke pristupa njihovima resursima u oblaku. Tu je svakako i revizija i izvještavanje o događajima koja kaže kako korisnici usluga oblaka moraju imati mogućnost pristupanja podacima o događajima koji su se dogodili u oblaku, osobito ako je riječ o padovima sustava i provalama sigurnosti. Pristup događajima uključuje mogućnost saznavanja proteklih događaja i obavještavanja o novim događajima odmah po njihovom zbivanju.

Jedna od sigurnosnih kontrola također je identitet, uloge, kontrola pristupa i atributi što znači kako mora biti moguće definirati identitet, uloge, ovlaštenja i ostale atribute pojedinaca i usluga na konzistentan, strojno čitljiv način. To će omogućiti učinkovito implementiranje kontrole pristupa i provođenje sigurnosnih politika prema resursima smještenim u oblaku. Sigurnosne politike osiguravaju mogućnost definiranja i primjenjivanja politike koje će pružati podršku kontroli pristupa, alokaciji resursa i ostalim odlukama na konzistentan i strojno čitljiv način. Automatizacija usluga je kontrola koja određuje obvezu postojanja autoriziranog načina upravljanja i analize sigurnosnih kontrolnih tokova i procesa kako bi se mogla provoditi revizija sigurnosti i sukladnosti. Upravljanjem radnim opterećenjem i uslugama znači kako mora biti moguće konfigurirati, koristiti i nadzirati usluge u suglasju s definiranim sigurnosnim politikama i ugovorima o licenciranju sklopljenima s klijentima.[9]

3.3 Federalizacija sigurnosnih usluga

Pod pojmom federalizacije podrazumijevamo mogućnost djelovanja većeg broja nezavisnih resursa kao jednog jedinstvenog resursa. Računarstvo samo po sebi jest primjer federalizacije resursa budući da se u njemu mnogi elementi, identiteti, konfiguracije i ostali detalji rješenja za računarstvo u oblaku moraju federalizirati kako bi oblik računarstva bio praktično primjenjiv.

Sigurnosni zahtjevi se mogu implementirati primjenom koncepta federalizacije u oblicima povjerenja, upravljanja identitetom, upravljanja pristupom, jednostrukom prijavom i odjavom, revizije i sukladnosti te upravljanja konfiguracijom. Koncept federalizacije u obliku povjerenja podrazumijeva mogućnost ostvarivanja povjerenja za dvije strane pomoću nekoga autentikacijskog autoriteta. Autentikacijski autoritet može izdavati i razumijevati potvrde o

[9] Isto

identitetu ili pak digitalne vjerodajnice u formi certifikata X.509 koje će kasnije služiti pri osiguranju poruka te za digitalno potpisivanje, najčešće prema SAML standardu.[10]

Upravljanje identitetom obuhvaća definiranje pružatelja identiteta koji prihvaća sve korisnikove digitalne vjerodajnice (poput korisničkog imena i lozinke) i vraća mu potpisanu poruku odnosno tzv. token koji jednoznačno identificira tog korisnika. Upravljanje pristupom jest mogućnost generiranja politika koje provjeravaju tokene pri upravljanju pristupom resursima u oblaku. Jednostruka prijava i odjava je mogućnost federalizacije jednostruke prijave (eng. *Single Sing-on*) za korištenje usluga oblaka koja omogućuje korisniku prijavu za korištenje jedne aplikacije, a zatim i pristup drugim aplikacijama koje vjeruju istom autentikacijskom autoritetu.

Federalizacija jednostrukih odjava (eng. *Single Sing-off*) je slična jer će u nekim situacijama korisniku biti važno da se odjavom jedne korištene aplikacije istovremeno odjavi i na drugim aplikacijama koje koristi. Revizija i skladnost označavaju mogućnost prikupljanja podataka potrebnih za reviziju i provjeru sukladnosti regulativa raspršenih po mnogim domenama, uključujući i hibridne oblake. Federalizirane revizije su neophodne kako bi se osigurala i dokumentirala sukladnost s odredbama ugovora o razini usluga i relevantnim regulatornim zahtjevima. Upravljanje konfiguracijom je mogućnost federalizacije podataka potrebnih za konfiguriranje usluga, aplikacija i virtualnih strojeva.[11]

Kada je u pitanju računarstvo u oblaku, svi pružatelji usluga bi trebali primjenjivati relevantne postojeće standarde za ostvarivanje navedenih oblika federalizacije sigurnosti. Tako bi doprinijeli sigurnom korištenju oblak usluga.

[10] Isto

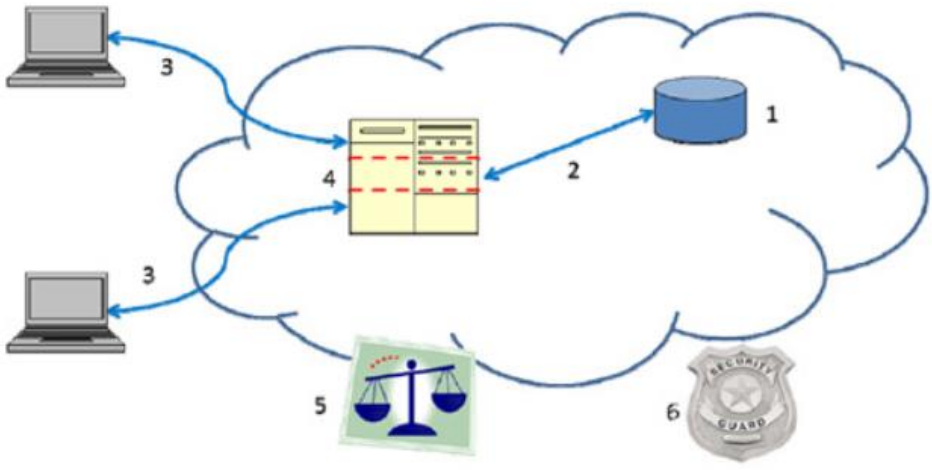
[11] Isto, str. 201

4. Sigurnosni problemi i rizici

Budući da se računarstvo u oblaku koristi informatičkim okruženjem i informacijskim sustavom, moguće je pretpostaviti kako ono obiluje sigurnosnim rizicima. Zbog toga bi svaki korisnik usluga računarstva u oblaku, prije odabira oblak servisa, trebao napraviti procjenu sigurnosti korištenja ovakve vrste usluga. To je moguće napraviti samostalnim istraživanje ili pomoću stručnih konzultanata. Računarstvo u oblaku ima jedinstvena obilježja koja zahtijevaju procjenu rizika u područjima kao što su integritet, oporavak i privatnosti. Osim toga, zahtjeva i procjenu pravnih problema u područjima poput inovacija, nadzorne usklađenosti i revizija. Postoji niz sigurnosnih rizika povezanih s računarstvom u oblaku koji moraju biti adekvatno riješeni.

Kao što je vidljivo na slici 2, postoji šest specifičnih područja oblika računarstva u oblaku gdje softver zahtijeva znatnu pažnju sigurnosti. Tih šest područja su:

1. sigurnost podataka u mirovanju
2. sigurnost podataka u tranzitu
3. autentikacija korisnika / aplikacija / procesa
4. razdvajanje podataka koji pripadaju različitim korisnicima
5. oblak pravnih i regulatornih pitanja
6. odgovor na incident.



Slika 2. Područja sigurnosnih rizika u oblak okruženju[12]

[12] Sen, Jaydip. Securitiy and privacy issues in cloud computing. URL: https://pdfs.semanticscholar.org/4dc3/70d253020947a8e66b701e12dd0233161229.pdf (2017-05-05)

Neki od specifičnih sigurnosnih rizika su: privilegirani korisnički pristup, nadzorna usklađenost, adresa podataka, odvajanje podataka te oporavljanje. Korisnici oblak servisa bi trebali prikupiti što više informacija o ljudima koji upravljaju podacima. Od davatelja usluga bi trebali zatražiti informacije o zapošljavanju i nadzoru privilegiranih administratora i provjerama ovlasti njihovih pristupa te tako smanjiti rizik privilegiranog korisničkog pristupa. Kada govorimo o riziku nadzorne usklađenosti korisnici se moraju informirati o davatelju usluga kojeg odabiru. One pružatelje usluga koji se podvrgavaju vanjskim revizijama korisnici mogu smatrati vrijednima za pružanje usluga. Pružatelj usluga mora pružiti dokaze o vlastitoj usklađenosti s relevantnim zakonima te o posjedovanju odgovarajućih certifikata. Kada su podaci u oblaku, korisnik ne zna gdje su oni točno pohranjeni. No može od davatelja usluga zatražiti pohranu podataka na točno određenoj adresi. Budući da se u oblaku podaci nalaze u zajedničkoj okolini, korisnik mora znati što je učinjeno za odvajanje podataka. Pružatelji usluga bi trebali pružiti dokaze o napravljenim shemama zaštitnog kriptiranja (eng. *encrypting*) koje su ispitane. Također korisnik mora znati što u slučaju gubitka podataka usred neplaniranih nesreća.[13]

Jedan o rizika jest činjenica da se resursima u oblaku može pristupiti s bilo kojeg mjesta na Internetu. Zbog toga se povećava potreba za utvrđivanjem korisnikovog identiteta. Snažna provjera autentičnosti i autorizacija postaju ključna briga. Važno pitanje je i zaštita podataka. Kada je riječ o podacima glavna briga je izloženost ili oslobađanje osjetljivih podataka, ali i nedostupnost ili pak gubitak podataka. Korisniku oblak usluge može biti teško provjeriti praksu rukovanja podacima te je ovaj problem pogoršan u slučajevima višestrukog prijenosa podataka (npr. između federaliziranih usluga u oblaku). Još jedan rizik predstavljaju zlonamjerne radnje ljudi koji rade unutar organizacije zbog pristupa i ovlasti koje uživaju. To je sastavni oblik računarstva u oblaku jer se takva aktivnost može dogoditi unutar klijentove organizacije ili organizacije pružatelja usluga. Još jedan rizik može biti nedostupnost usluge oblaka uzrokovane kvarovima hardvera, softvera ili komunikacijske mreže.[14]

[13] Nacionalni CERT. Cloud Computing: NCERT-PUBDOC-2010-03-193, 2010. URL: http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-03-293.pdf (2017-03-27)

[14] Cloud Standars Customer Council. Security for Cloud Computing: 10 Steps to Ensure Success, 2015. URL: http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf (2017-03-29)

5. Sigurnosna rješenja

Računarstvo u oblaku je virtualno okruženje koje zahtijeva prijenos podataka diljem oblaka. Upravo zbog toga može doći do zabrinutosti prilikom pohrane podataka. Korisnici uglavnom ne znaju gdje su pohranjeni njihovi podaci niti koji se podaci pohranjuju kolektivno s njihovima. Za održavanje podataka u oblaku ključno je ili poželjno nadmašiti razinu sigurnosti koju korisnici imaju u tradicionalnom IT okruženju. Osim toga, za osiguranje povjerljivosti podataka, provjere autentičnosti, integriteta i dostupnosti, pružatelj usluga bi trebao ispunjavati određene uvjete. Ujedno se tako približavaju svojim korisnicima te dobivaju njihovo povjerenje. Korisnici također tako mogu procijeniti je li pojedini pružatelj oblak usluga pravi za njih. Unutar ovoga poglavlja objašnjeni su nizovi koraka za korisnike oblak usluga kako bi procijenili sigurnost oblaka s ciljem ublažavanja rizika i pružanja odgovarajuće razine podrške.

Koraci koji će biti objašnjeni u nastavku:

1. Osigurati postojanje učinkovitog upravljanja, rizika i postupaka usklađivanja
2. Provjeriti operativne i poslovne procese
3. Upravljati ljudima, ulogama i identitetima
4. Osigurati odgovarajuću zaštitu podataka i informacija
5. Proširiti pravila o privatnosti
6. Procijeniti sigurnosne odredbe za aplikacije u oblaku
7. Osigurati sigurnost mreža i veza
8. Procijeniti sigurnosne kontrole na fizičkoj infrastrukturi i objektima
9. Osigurati sigurnosne uvjete u ugovoru o usluzi oblak
10. Razumjeti sigurnosne zahtjeve izlaznog procesa[15]

Za svaki pojedini korak navedeni su uvjeti i najbolje prakse. Osim toga, svaki korak uzima u obzir stvarnost današnjeg oblika računarstva u oblaku i postavlja pitanje kako će se taj prostor vjerojatno razvijati u budućnosti, uključujući važnu ulogu koju će standardi igrati kako bi poboljšali interoperabilnost i prenosivost među pružateljima usluga.

[15] Cloud Standars Customer Council. Security for Cloud Computing: 10 Steps to Ensure Success, 2015. URL: http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf (2017-03-17)

5.1 Osigurati postojanje učinkovitog upravljanja, rizika i postupaka usklađivanja

Kada je u pitanju osiguranje učinkovitog upravljanja, rizika i postupka usklađivanja većina organizacija uspostavila je sigurnosne i usklađene politike te postupke koji se koriste za zaštitu intelektualnog vlasništva i korporativne imovine, posebno u IT prostoru. Također je uspostavljena kontrola i daljnji postupci za ublažavanje rizika koji služe kao mjerilo za izvršavanje i potvrđivanje usklađenosti. Ta načela i politike, sigurnosni plan poduzeća i proces okoline za poboljšanje kvalitete predstavljaju upravljanje tvrtkom, upravljanje rizicima i model usklađenosti. Korisniku je od važnog značaja razumjeti sve uvjete vezane uz sigurnost i osigurati da ti termini odgovaraju njihovim potrebama.

Najpriznatija međunarodna norma za informacijsku sigurnost je ISO / IEC 27001. ISO ima nove standarde, ISO / IEC 27017 "Kodeks prakse za kontrolu informacijske sigurnosti temeljen na ISO / IEC 27002 za oblak usluge" i ISO / IEC 27018 "Kodeks prakse za zaštitu osobno prepoznatljivih informacije (eng. *Personally Identifiable Information, PII*) u javnim oblacima koji djeluju kao PII procesori“ koji se posebno bave problemima sigurnosti i privatnosti oblaka i koji se temelje na ISO / IEC 27001. Neke organizacije pružaju okvire i certifikate za procjenu IT sigurnosti koji se mogu primijeniti na pružatelje oblak usluga, uključujući Američki institut certificiranih javnih računovođa (eng. *American Institute of Certified Public Accountants, AICPA*) i Udrugu za reviziju i kontrolu informacijskih sustava (eng. *Information Systems Audit and Control Association, ISACA*). Druge organizacije pružaju okvire za određene usluge ili industrije kao što je Industrija platnih kartica (eng. *Payment Card Industry, PCI*) i Standard sigurnosti podataka industrije (eng. *Data Industry Security Standard, DSS*). Grupe kao što je Savez za sigurnost računarstva u oblaku (eng. *Cloud Security Alliance, CSA*) pružaju smjernice koje uključuju Matricu kontrole oblaka (eng. *Cloud Controls Matrix, CCM*), Inicijativu za procjenu konsenzusa (eng. *Consensus Assessment Initiative, CAI*) i Certifikat znanja o sigurnosti u oblaku (eng. *Certificate of Cloud Security Knowledge, CCSK*).[16]

5.2 Provjeriti operativne i poslovne procese

Tvrtke razumiju važnost revizije usklađenosti informatičkih sustava kako bi se osiguralo poštivanje njihovih korporativnih, industrijskih ili vladinih zahtjeva i pravila. Razina pristupa ključnim informacijama o reviziji ključ je razmatranja ugovora o razini usluge s bilo kojim

[16] Isto

pružateljem u oblaku. Kao dio bilo kojeg uvjeta, pružatelji oblak usluge bi trebali ponuditi pravovremeni pristup događajima revizije, prijaviti i izvještavati informacije relevantne za specifične podatke ili aplikacije klijenta.

5.3 Upravljati ljudima, ulogama i identitetima

Korištenje rješenja za oblak znači da će zaposlenici pružatelja usluga imati mogućnost pristupa korisničkim podacima i aplikacijama, kao i zaposlenici korisnika koji trebaju obavljati operacije na sustavima davatelja. Korisnici oblak usluge osiguravaju davateljima usluge procese i funkcije koje upravljaju time tko ima pristup podacima i aplikacijama korisnika. Isto tako, pružatelji oblaka moraju omogućiti klijentu dodjeljivanje i upravljanje ulogama i pridruženim razinama autorizacije za svakog svog korisnika u skladu s njihovim sigurnosnim pravilima. Ove uloge i prava autorizacije primjenjuju se na temelju resursa, usluge ili aplikacije. Na primjer, kupac u oblaku, u skladu sa svojim sigurnosnim pravilima, može imati zaposlenika čija uloga omogućuje generiranje zahtjeva za kupnju, ali druga ulogu i prava autorizacije dodjeljuje se drugom zaposleniku koji je odgovoran za odobravanje zahtjeva.[17]

5.4 Osigurati odgovarajuću zaštitu podataka i informacija

Sigurnost podatak i informacija koje se nalaze u oblaku predstavlja središte pozornosti za sve organizacije i korisnike. Pitanja koja su vezana za sigurnost podataka u oblaku odnose se na različite oblike rizika koji ju ugrožavaju. Neki od takvih rizika su: rizik od krađe ili neovlaštenog otkrivanja podataka, rizik od neovlaštenog manipuliranja ili neovlaštene izmjene podataka, rizik gubitka ili nedostupnost podataka. U oblaku "imovina podataka" može uključivati aplikacijske programe, što može predstavljati iste rizike kao i sadržaj baza podataka ili podatkovnih datoteka. Pružatelji oblak usluga trebaju brinuti o svim rizicima koji mogu uzrokovati gubitak podataka bilo zbog greške uzrokovane ljudskim faktorom ili sustavom. Prema tome oni moraju osigurati pohranjivanje redundantnih kopija korisničkih podataka kako bi se mogli nositi s bilo kojom situacijom koja bi dovela do gubitka podataka.

5.5 Proširiti pravila o privatnosti

Privatnost i zaštita podataka dobivaju važnost širom svijeta, a često uključuju zakone i propise koji se odnose na nabavu, pohranu i upotrebu osobnih podataka. Važno je napomenuti kako

[17] Isto

su sigurnost i privatnost povezani, ali i različiti. Ključna razlika je u tome što se sigurnost prvenstveno bavi branjenjem od napada, a nisu svi usmjereni na krađu podataka, dok je privatnost osobito povezana s osobnim podacima koja može biti ugrožena zbog nepažnje ili pogreške (eng. *bug*), a ne nužno zlonamjerne osobe.

Zaštita podataka zahtijeva nametanje ograničenja na korištenje i dostupnost osobnih podataka koji se temelje na politikama koje piše ne-IT osoblje, a posebno odjeli za pravo i rizik koji su u skladu s važećim propisima i zakonima, te su odobreni na najvišim razinama organizacije. Provođenje takvih ograničenja podrazumijeva pridružene zahtjeve za prikladno označavanje podataka, sigurno pohranjivanje i dopuštanje pristupa samo ovlaštenim korisnicima. To zahtijeva odgovarajuće kontrole, što može biti izazovnije kada su podaci pohranjeni unutar infrastrukture pružatelja oblak usluga. Standard ISO / IEC 27018 odnosi se na kontrole potrebne za zaštitu osobnih podataka.[18]

5.6 Procijeniti sigurnosne odredbe za aplikacije u oblaku

Organizacije moraju proaktivno zaštititi svoje poslovne aplikacije od vanjskih i unutarnjih prijetnji tijekom čitavog životnog ciklusa, od projektiranja do implementacije i proizvodnje. Jasno definirane sigurnosne politike i procesi su neophodni kako bi se osiguralo aplikacijama omogućavanje poslovanja umjesto uvođenje dodatnog rizika. Pitanje sigurnosti aplikacija predstavlja velike izazove organizacijama i kupcima. Ako je sigurnost aplikacije ugrožena, ugrožena je i sigurnost korisnika, ali i ugled organizacije.

5.7 Osigurati sigurnost mreža i veza

Mreže su klasificirane u različite vrste kao što su na primjer: zajedničke, javne ili privatne, mala ili velika mrežna područja, a svaka od njih ima niz sigurnosnih prijetnji. Kako bi se osigurala mrežna sigurnost točaka kao što su: povjerljivost i integritet u mreži, odgovarajuća kontrola pristupa i održavanje sigurnosti od vanjskih prijetnji treba uzeti u obzir pružanje sigurnosti na razini mreže. Problemi povezani s mrežnom sigurnošću su ponovljene IP adrese (eng. *reused IP address*), napadi uskraćivanjem usluga (eng. *Denial-of-service, DoS*), distribuirani napadi uskraćivanjem usluga (eng. *Distributed Denial-of-service, DDoS*), itd.[19]

[18] Isto

[19] Bhadauria, Rohit...[et. al.]. Security issues in cloud computing. // Acta Tehnica Corviniensis – Bulletin of Engineering 7, 4(2014), str. 159-177. URL:

Pružatelj oblak usluga mora omogućiti zakonit mrežni promet i blokirati zlonamjerni mrežni promet, baš kao i svaka druga organizacija povezana s internetom. Međutim, za razliku od mnogih drugih organizacija, pružatelj oblak usluga ne mora nužno znati koji mrežni promet klijenti namjeravaju poslati i primati. Ipak, korisnici bi trebali očekivati neke sigurnosne mjere vanjskih mrežnih parametara od svojih pružatelja oblak usluga.

5.8 Procijeniti sigurnosne kontrole na fizičkoj infrastrukturi i objektima

Sigurnost IT sustava također ovisi o sigurnosti fizičke infrastrukture i objekata. U slučaju računarstva u oblaku, to se odnosi na infrastrukturu i objekte pružatelja oblak usluga. Sigurnost se može osigurati putem revizijskih izvješća o procjeni koja pokazuju usklađenost sa sigurnosnim standardima kao što je ISO 27002.[20]

5.9 Osigurati sigurnosne uvjete u ugovoru o usluzi oblak

Budući da računarstvo u oblaku obično uključuje dvije organizacije, odnosno korisnika oblak usluge i davatelja oblak usluga, sigurnosne odgovornosti svake strane moraju biti jasno definirane. To se obično vrši putem ugovora o usluzi koji se odnosi na pružene usluge i uvjete ugovora između kupca i pružatelja usluga. Ugovor o usluzi trebao bi navesti sigurnosni odgovor te bi trebao uključivati aspekte kao što su izvješćivanja o kršenjima sigurnosti.

Jedna značajka ugovora o usluzi koja se odnosi na sigurnost jest da se svi zahtjevi koji se odnose na pružatelja oblaka moraju prenijeti i na one pružatelje oblak usluga u međusobnom odnosu koji davatelj usluga može koristiti kako bi pružio bilo koji dio svoje usluge. To bi trebalo biti izričito dokumentirano u ugovoru o oblak uslugama kojim davatelji moraju pravodobno obavijestiti kupce o nastanku bilo kakvog kršenja njihovog sustava, bez obzira na stranke ili podatke koji su izravno utjecali.

5.10 Razumjeti sigurnosne zahtjeve izlaznog procesa

Ukupna potreba za dobro definiranim i dokumentiranim postupkom izlaska opisana je u Praktičnom vodiču za sporazume o uslugama u oblaku (eng. *Practical Guide to Cloud Service Agreements, CSCC*). Iz sigurnosne perspektive važno je da se, nakon što kupac dovrši

---

http://web.a.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=5d9b7a3a-36a8-46f8-94d9-791561ef3a03%40sessionmgr4010&vid=0&hid=4109 (2017-05-24)

[20] Cloud Standars Customer Council. Security for Cloud Computing: 10 Steps to Ensure Success, 2015. URL: http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf (2017-03-17)

postupak prestanka, postiže "reverzibilnost" - tj. ni jedan podatak o korisniku oblak usluga ne bi trebao ostati kod pružatelja usluga. Davatelj usluga mora osigurati da se svaka kopija podataka trajno briše iz svog okruženja, gdje god da su pohranjene (uključujući rezervne lokacije, kao i internetske pohrane podataka). Imajte na umu da podaci dobiveni uslugom u oblaku koje posjeduje davatelj usluga možda trebaju "čišćenje" informacija (npr. dnevnici), premda neke jurisdikcije mogu zahtijevati zadržavanje zapisa ove vrste za razdoblja određena zakonom.

Jasno je postojanje i suprotnog problem tijekom izlaznog procesa - korisnik mora biti u mogućnosti osigurati glatki prijelaz, bez gubitka ili kršenja podataka. Stoga izlazni proces omogućava klijentu dohvaćanje vlastitih podataka u prikladnom obliku. Sigurnosne kopije moraju se čuvati za dogovorena razdoblja prije uklanjanja i pridružene dnevnike događaja, a podaci izvješćivanja moraju biti zadržani sve dok se izlazni postupak ne završi.[21]

[21] Cloud Standars Customer Council. Security for Cloud Computing: 10 Steps to Ensure Success, 2015. URL: http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf (2017-03-17)

6. Sheme certificiranja za sigurnost i privatnost

Budući da je velika pažnja posvećena sigurnosti i privatnosti informacija koje se nalaze u oblaku, neka udruženja su razvila certifikate koji osiguravaju upute za pružanje sigurnosnih postavki. To nisu zakonski okviri, ali uvelike pomažu pružateljima usluga u omogućavanju sigurne pohrane podataka. Posjedovanje jednog od navedenoga certifikata u nastavku znači rad na sigurnosnim pitanjima i briga za korisnike oblak usluga. Samim time i korisnici mogu lakše odlučiti koji oblak servis će odabrati za pohranu svojih podataka.

6.1 ISO standardi

ISO je razvio obitelj standarda za informacijsku sigurnost koji pružaju okvir organizacijama kako bi mogle razvijati procese za rješavanje pitanja vezanih uz sigurnost informacija. Kao vodeći standard u grupi ističe se najčešće priznat standard za zaštitu osjetljivih informacija od neželjene distribucije i neovlaštenog pristupa tj. ISO / IEC 27001. On opisuje kako uspostaviti neovisno ocijenjeni i certificirani sustav upravljanja informacijskom sigurnošću. To nam omogućuje učinkovitije osiguranje svih financijskih i povjerljivih podataka, čime se smanjuje vjerojatnost ilegalnog pristupanja ili pristupanja bez dopuštenja. S ISO / IEC 27001 možemo demonstrirati predanost i usklađenost s najboljom svjetskom praksom, dokazati korisnicima, dobavljačima i dionicima kako je sigurnost najvažnija. Standard prati pristup koji je uobičajen u međunarodnim standardima sustava upravljanja, što olakšava integraciju s drugim sustavima i organizacijama. Sedam osnovnih elemenata nove verzije standarda objavljenog 2013. godine su: kontekst organizacije, rukovodstvo, planiranje, podrška, rad, evaluacija i poboljšanje.[22]

Ukupno sadrži 114 kontrola te zajedno s ISO / IEC 2002 ublažava rizike vezane uz prikupljanje, pohranu i širenje informacija putem pružanja zahtjeva za učinkovit sustav upravljanja informacijskom sigurnošću, dopuštanja organizacijama pridržavanje povećane

[22] Cloud Watch. Cloud certification guidelines and recommendations. 2015. URL: http://cordis.europa.eu/docs/projects/cnect/4/610994/080/deliverables/001-D41Cloudcertificationguidelinesandrecommendationsrevisedversion.pdf (2017-04-01)

regulacije državne uprave i stroge zahtjeve specifične za pojedinu industriju te omogućavanje rasta organizacijama znajući da će sve njihove povjerljive informacije ostati sigurne.[23]

Zaštita privatnih informacija nikada nije bila veći prioritet. Mnoga nacionalna i međunarodna tijela, uključujući Međunarodnu organizaciju za standardizaciju (eng. *International Organization for Standardization, ISO*), američku vladu i Europsku uniju, poduzimaju sve korake za rješavanje ovog problema. Jedna zajednička inicijativa je međunarodni standard ISO / IEC 27018.[24]

ISO / IEC 27018 preuzima opsežan skup sigurnosnih kontrola opisanih u ISO / IEC 27002 kao bazu, a zatim ih proširuje na dva načina. Prvo, postojeće sigurnosne kontrole se proširuju u brojnim područjima kako bi se bavile dijeljenjem odgovornosti između korisnika oblak usluge i pružatelja usluga oblak. Drugo, dodaje se novi skup sigurnosnih kontrola, koje odražavaju načela privatnosti definirana u standardu zaštite privatnosti ISO / IEC 29100. ISO / IEC 27018 osigurava pružatelju oblak usluga odgovarajuće postupke za rukovanje PII-om. Također, može pomoći u izradi jačih sporazuma o uslugama u oblaku. Potencijalno izlaganje osobnih podataka nalazi se na vrhu međunarodnog dnevnog reda. Standardom se definira način na koji pružatelji oblak usluga mogu obučavati osoblje o PII-u, o tome koje su procedure dokumentacije potrebne i pružaju smjernice za njihovo praćenje. ISO / IEC 27018 ima za cilj pružiti stvarnu transparentnost za klijenta, tako da klijent razumije ono što pružatelj usluga radi s obzirom na sigurnost i zaštitu osobnih podataka.

Unutar standarda sadržano je nekoliko ciljeva među kojima je i pomoć javnom davatelju usluga da bude u skladu s primjenjivim obvezama kada se ponaša kao PII procesor, bez obzira hoće li takve obveze na PII procesor biti izravne ili putem ugovora. Postoje tri područja u kojima organizacija treba obratiti posebnu pozornost pri provedbi standarda:

1.) Postoje li zakonske odredbe koje organizacija mora slijediti, uključujući sva pravila i propise određene industrijom
2.) Podrazumijeva li pridržavanje ISO / IEC 27018 dodatne rizike za organizaciju

[23] Bsi. ISO / IEC 27108: SafeguardingPersonal Information in the Cloud. URL: https://www.bsigroup.com/Documents/iso-iec-27018/ISOIEC-27018-Safeguarding-information-in-the-cloud-whitepaperDec2015.pdf

[24] Isto

3.) Hoće li usvajanje standarda zahtijevati promjene korporativnih politika organizacije i poslovne kulture.[25]

ISO / IEC 27018: 2014 se primjenjuje na sve vrste i veličine organizacija, uključujući javne i privatne tvrtke, državne subjekte i neprofitne organizacije koje pružaju usluge obrade informacija. Smjernice iz ISO / IEC 27018: 2014 također mogu biti relevantne za organizacije koje djeluju kao kontrolori PII. Međutim, kontrolori PII mogu biti podložni dodatnim zakonima, propisima i obvezama zaštite privatnosti. ISO / IEC 27018: 2014 nije namijenjen za pokrivanje takvih dodatnih obveza.[26]

6.2 SSAE16 - SOC 1-2-3

Naziv ovoga programa je Kontrole organizacije usluga (eng. *Service Organization Controls, SOC*), a obuhvaća SOC 1, SOC 2 i SOC 3. Cilj SOC-a je pružiti korisnicima servisnih organizacija osiguran učinkovit rad IT kontrole usmjerene na rješavanje IT rizika u obradi informacija. Kako bi osigurao okvir za ispitivanje kontrola i pomoći upravljanja povezanim rizicima, Američki institut certificiranih javnih računovođa (eng. *American Institute of Certified Public Accountants, AICPA*) utvrdio je tri opcije izvještavanja o servisnoj organizaciji. U nastavku je objašnjena svaka od tih opcija.[27]

6.2.1 SOC 1

Kontrole organizacija usluga 1 (eng. *Service Organization Controls 1, SOC 1*) su kontrole relevantne za unutarnju kontrolu nad financijskim sredstvima korisnika. Angažman SOC 1 obavlja se u skladu s Izjavom o standardima za angažman ovjere (eng. *Statement on Standards for Attestation Engagement, SSAE*). SOC 1 izvješća se usredotočuju isključivo na kontrole u organizaciji koja će vjerojatno biti relevantna za reviziju financijskih izvještaja korisnika.

[25] Isto

[26] International Organization for Standardization. ISO/IEC 27018:2014: Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. URL: https://www.iso.org/standard/61498.html (2017-04-02)

[27] Cloud Watch. Cloud certification guidelines and recommendations. 2015. URL: http://cordis.europa.eu/docs/projects/cnect/4/610994/080/deliverables/001-D41Cloudcertificationguidelinesandrecommendationsrevisedversion.pdf (2017-04-01)

Korištenje izvješća SOC 1 ograničeno je na postojeće korisničke entitete, a ne potencijalne kupce. Postoje dvije vrste SOC 1 izvješća:

1.) izvješće o ispravnosti prezentacije opisa sustava usluge u organizaciji i prikladnosti dizajna kontrolnih mehanizama u svrhu postizanja opisanih ciljeva u određenom roku

2.) izvješće o ispravnosti prezentacije opisa sustava usluge u organizaciji, prikladnosti dizajna i operativne efektivnosti kontrolnih mehanizama u svrhu postizanja opisanih ciljeva kroz zadani vremenski period.[28]

6.2.2 SOC 2

Prepoznajući potrebu klijenta za osiguranjem koja se proteže izvan financijskih ciljeva, AICPA je u suradnji s Kanadskim institutom ovlaštenih računa (eng. *Canadian Institute of Chartered Account, CPA*) oblikovao Načela i kriteriji povjerenja usluge (eng. *Trust Services Principles and Criteria, TSPC*) kako bi pomogao u posredovanju povjerenja i odnosa između sve većih IT servis i obrade podataka i njegovih kupaca. TSPC pruža okvir CPA-u za izvještavanje o dizajnu i operativnoj učinkovitosti sigurnosti, povjerljivosti, dostupnosti, privatnosti i kontroli integriteta obrade. SOC 2 izvješće je slično SOC 1 izvješću.

Izvješće pruža opis sustava organizacije usluga. SOC 2 izvješća posebno se bave jednim ili više od sljedećih pet ključnih atributa sustava:

1.) Sigurnost - Sustav je zaštićen od neovlaštenog pristupa (fizički i logički)
2.) Dostupnost - Sustav je dostupan za rad i uporabu kao počinjen ili dogovoren
3.) Procesiranje integriteta - Obrada sustava je potpuna, točna, pravodobna i ovlaštena
4.) Povjerljivost - Podaci povjerljivi kao zaštićeni, počinjeni ili dogovoreni
5.) Privatnost - Osobni podaci se prikupljaju, koriste, zadržavaju, otkrivaju i zbrinjavaju.

Danas, s porastom računarstva u oblaku, potražnja za izvješćivanjem CPA tvrtki o kontrolama vezanima uz sigurnost, povjerljivost i dostupnost doživjela je ponovni procvat, a veliki pružatelji oblak usluga imaju ili su u procesu pružanja svojim klijentima SOC 2 izvješća za rješavanje ovog zahtjeva.[29]

[28] Isto

[29] Isto

6.2.3 SOC 3

SOC 3 angažmani također koriste unaprijed definirane kriterije u TSPC koji se koriste u SOC 2 angažmanu. Ključna razlika između izvješća SOC 2 i izvješća SOC 3 je da izvješće SOC 2, koje je uglavnom izvješće s ograničenim učinkom, sadržava detaljan opis testova kontrolora i rezultata testova servisa te rezultata tih testova, kao i uslugu mišljenja revizora o opisu sustava usluga organizacija. Izvješće SOC 3 je izvješće opće uporabe koja daje samo izvješće revizora o tome je li sustav postigao kriterije za usluge povjerenja (bez opisivanja testova i rezultata ili mišljenja o opisu sustav). Također dopušta organizaciji za uslugu upotrebu pečata SOC 3 na svojoj internetskoj stranici.[30]

6.3 Cloud Security Alliance Open Certification Framework

Opseg ovoga standarda jest sigurnost i privatnost. Program se naziva Sustav otvorenih potvrda - STAR (eng. *Open Certification Framework – STAR*), a standardom upravlja Savez za sigurnost računarstva u oblaku (eng. *Cloud Security Alliance, CSA*). CSA otvoreni okvir za certifikaciju može se opisati kao inicijativa industrije kako bi se omogućilo globalno, akreditirano, pouzdano certificiranje pružatelja oblaka. Program je za fleksibilnu, inkrementalnu i višeslojnu certifikaciju pružatelja oblaka u skladu s CSA sigurnosnim smjernicama. Program se integrira s popularnom procjenom treće strane (ISO27001) i izjavama o potvrđivanju (SOC2) koje su razvijene unutar javne računovodstvene zajednice kako bi se izbjeglo dupliciranje napora i troškova. CSA otvoreni okvir za certifikaciju se temelji na kontrolnim ciljevima i kontinuiranoj strukturi praćenja. Strukturiran je u tri razine kako bi se riješio različitih uvjeta uvjerenja i razine dospijeća pružatelja i potrošača. Tri razine programa OCF-a su:

1. Razina – CSA STAR Samoprocjena (eng. *CSA STAR Self-Assessment*)
2. Razina – CSA STAR Certificiranje (eng. *CSA STAR Certification*) / Razina 2 – CSA STAR Ovjeravanje (eng. *CSA STAR Attestation*)
3. Razina – CSA STAR Kontinuiranje (eng. *CSA STAR Continuous*)

STAR Samoprocjena je procjena procesa koji se temelji na najboljoj praksi upitnika inicijative za procjenu konsenzusa (eng. *Consensus Assessments Initiative Questionnaire, CAIQ*) i Matrici kontrole oblaka (eng. *Cloud Controls Matrix, CCM*). CSA STAR Certificiranje je neovisna procjena sigurnosti treće strane pružatelja oblak usluga. To je tehnološki neutralan certifikat koji koristi zahtjeve standarda ISO / IEC 27001: 2005 s CSA

[30] Isto

CCM-om. CSA STAR Ovjeravanje je postavljeno na razini dva kao i CSA STAR Certificiranje jer se radi o procjeni sigurnosti pružatelja oblak usluga pomoću treće strane. CSA STAR Kontinuiranje se temelji na kontinuiranoj reviziji/procjeni relevantnih sigurnosnih svojstava.[31]

6.4 EuroCloud Star Audit

EuroCloud Star Audit (ECSA) je shema certifikacije koja je osmišljena za procjenu sigurnosti oblak usluge. Procjenjuje usluge u oblaku prema zahtjevima revizijske sheme i obuhvaća sve sudionike oblak usluge. Ovaj certifikat je značajan alat za korisnike koji se žele koristiti i odabrati pouzdan oblak te smanjuje potrebu za obavljanjem skupe pojedinačne revizije. ESCA donosi vrijedan instrument s visokom razinom transparentnosti i smjernice za kupce i pružatelje oblak usluga. Program ECSA se temelji na:

- Detaljnoj analizi tržišta o postavljanju europskog pružatelja oblak usluga
- Modularnoj strukturi certifikacijskih stupova i dopuštanju svakom uključenom entitetu brigu o svojim područjima
- Dopuštanju djelomične certifikacije kako biste osigurali pripremljeno odobrenje za potpunu certifikaciju oblak usluge
- Snažnom angažmanu IT pravnika na uključivanju zakona i usklađenosti s određenim zemljama. EuroCloud Star Audit (ECSA) temelji se isključivo na europskom tržištu.[32]

6.5 EuroPrise: The European Privacy Seal

Standardom upravlja EuroPrise GMBH s odborom dionika uključujući i njemačku zaštitu podataka Schleswig-Holsteina. Opseg koji obuhvaća standard jest zaštita podataka. Nije specifična za oblak (baš kao i ISO 27001), ali se može primijeniti na oblak usluge, a već je dodijeljena pretraživačkoj i oglašavačkoj mreži za ponašanje. EuroPrise je europska certifikacijska shema koja potvrđuje sukladnost IT proizvoda i usluga s kriterijima koji se temelje na europskim direktivama o zaštiti podataka (95/46 / EC i 2002/58 / EZ).

Povjerljivost EuroPrisea dodjeljuje se nakon:

1.) procjene od strane nezavisnog akreditiranog revizora

2.) potvrđivanja proizvedenog evaluacijskog izvješća od strane certifikacijskog tijela Europske unije. [33]

[31] Isto

[32] Cloud Watch HUB. URL: http://www.cloudwatchhub.eu/eurocloud-%E2%80%93-star-audit (2017-05-20)

7. Organizacije za zaštitu informacija i sigurnost

Zbog sve prisutnije brige za zaštitu informacija i sigurnost korištenja usluga na Internetu razvile su se različite organizacije koje se bave tim područjem. Neke od njih su vezane isključivo za sigurnost računarstva u oblaku, a neke pak i za druge usluge koje su nam dostupne. Navedene organizacije aktivno djeluju na ovom području te pokušavaju pružiti sigurnost svim korisnicima. Njihov konstantan rad koji uključuje analize, revizije i izrade smjernica pomažu pružateljima oblak servisa stvaranje sigurnog okruženja za korisnike.

7.1 Cloud Security Alliance

Savez za sigurnost računarstva u oblaku (eng. *Cloud Security Alliance, CSA*) je neprofitna organizacija osnovana kako bi promicala uporabu najboljih načina na koje se korištenje računarstva u oblaku može učiniti što sigurnijim. Osnovana je 20. kolovoza 2008. godine. Od samoga osnutka u organizaciji djeluju stručnjaci iz različitih područja koji se bave pitanjem sigurnosti računarstva u oblaku. CSA se također bavi educiranjem korisnika o načinima uporabe računarstva u oblaku i tako pomaže u osiguravanju svih drugih oblika računarstva (mobilnog računarstva (eng. *mobile computing*), grid-računarstva (eng. *grid computing*) i mnogih drugih).

CSA čini mnoštvo stručnjaka iz različitih disciplina ujedinjenih kako bi:

- promicali međusobno razumijevanje između korisnika i pružatelja usluga računarstva u oblaku vezano za potrebne sigurnosne zahtjeve i potvrde osiguranja,
- promicali nezavisna istraživanja u područjima sigurnosti računarstva u oblaku,
- pokretali kampanje za podizanje svijesti i edukacijske programe o prikladnom korištenju računarstva u oblaku i sigurnosnim rješenjima te
- stvarali liste problema i smjernica za povećanje sigurnosti računarstva u oblaku. [34]

Osim na području edukacije djeluje i na područjima certificiranja, izgradnje standarda i istraživanja u polju računalnog oblaka. CSA je trenutno apsolutni predvodnik u integraciji na polju sigurnosti računalnog oblaka, a istraživački rad je u CSA podijeljen u dvadeset inicijativa od kojih su najznačajnije:

---

[33] Cloud Watch. Cloud certification guidelines and recommendations. 2015. URL: http://cordis.europa.eu/docs/projects/cnect/4/610994/080/deliverables/001-D41Cloudcertificationguidelinesandrecommendationsrevisedversion.pdf (2017-04-01)

[34] Nacionalni CERT. Cloud Computing: NCERT-PUBDOC-2010-03-193, 2010. URL: http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-03-293.pdf (2017-03-27)

1.) Matrici kontrole oblaka (eng. *Cloud Controls Matrix, CCM*) koja radi na definiranju sigurnosnih pravila i uputa za pružatelje oblak usluga, kao i na aktivnoj izgradnji baze znanja za korisnike kako bi bolje razumjeli sigurnosne koncepte. Također djeluje na integraciji s drugim standardima i normama.
2.) Protokol za povjerenje u oblaku (eng. *The Cloud Trust Protocol, CTP*) koji radi na razvoju mehanizma za razmjenu informacija o ugrađenim sigurnosnim mehanizmima između korisnika i CSP.
3.) Inicijativa pouzdanog oblaka (eng. *The Trusted Cloud Initiative,* TCI) koja djeluje na području upravljanja identitetima, autorizacijom (eng. a*uthorization*) i autentikacijom (eng. *authentication*).[35]

Zahvaljujući ovoj organizaciji danas se konstantno javljaju rješenja za sigurnosne probleme računarstva u oblaku. Pomoću njihovog vodiča pružatelji oblak usluga svojim korisnicima omogućavaju sigurnu pohranu podataka.

7.2 European Union Agency for Network and Information Security

Agencija Europske unije za mrežnu i informacijsku sigurnost (eng. *European Union Agency for Network and Information Security, ENISA*) je agencija kojoj je središte djelovanja mrežna i informacijska sigurnost u Europi. Agencija je osnovana 2004. godine te doprinosi visokoj razini mrežne i informacijske sigurnosti. Agencija blisko surađuje s državama članicama i privatnim sektorom kako bi pružila savjete i rješenja. To uključuje i paneuropske vještine internetske sigurnosti (eng. *cyber security*), razvoj nacionalnih internetskih sigurnosnih strategija, ali i studije o sigurnosti računarstva u oblaku, rješavanju pitanja zaštite podataka, tehnologijama za poboljšanje privatnosti.

ENISA također podupire razvoj i provedbu politike i zakona Europske unije o pitanjima koja se odnose na mrežnu i informacijsku sigurnost. ENISA radi na procjenama rizika oblak usluga prema kojima objavljuje okvir osiguranja za upravljanje rizicima informacijske sigurnosti u oblaku. Neki od tih okvira se koriste kao osnova pojedinih industrijskih inicijativa za sigurnost u oblaku. Agencija također izvješćuje o incidentima u oblaku te često ističe sigurnosne mogućnosti računarstva u oblaku. Godine 2013. ENISA je objavila rad koji analizira kako pružatelji oblaka, korisnici u kritičnim sektorima i vladine vlasti mogu postaviti sheme izvješćivanja o sigurnosnim incidentima u oblaku.

[35] Radić, Branimir. Sigurnost u računalnom oblaku. URL: http://www.fer.unizg.hr/_download/repository/KDI%2C_Branimir_Radic.pdf (2017-04-02)

ENISA je kao dio aktivnosti u okviru strategije EU-a za oblak razvila popis različitih shema certifikacije koje bi mogle biti relevantne za potencijalne korisnike računarstva u oblaku. Ovaj popis je razvila ENISA u uskoj suradnji s Europskom komisijom i privatnim sektorom. Neki od certifikata koji se nalaze na popisu su: EuroCloud Star Audit Certification, SO/IEC 27001 Certification, CSA Self Assessment - OCF Level 1, SOC 1, SOC 2, SOC 3, itd.[36]

7.3 The National Institute of Standards and Technology

Nacionalni institut za standarde i tehnologiju (eng. *The National Institute of Standards and Technology, NIST*) osnovan je 1901. godine i sada je dio Ureda za trgovinu SAD-a. NIST se ne bavi isključivo računarstvom u oblaku i njegovom sigurnosti, ali dio svoga rada posvećuje i tom području. Dugoročni cilj na tom području je pružiti vodstvo i smjernice oko paradigme računarstva u oblaku kako bi katalizirao njegovu upotrebu unutar industrije i vlade. NIST ima za cilj poticati praksu računarstva u oblaku koja podržava interoperabilnost, prenosivost i sigurnosne zahtjeve koji su prikladni i ostvarivi za važne scenarije korištenja.[37]

[36] European Union Agency for Network and Information Security. URL: https://www.enisa.europa.eu/ (2017-05-23)

[37] IEEE Cloud Computing URL: http://cloudcomputing.ieee.org/standards (2017-24-05)

8. Istraživanje sigurnosti računarstva u oblaku

Nakon što smo naveli sigurnosne probleme i rizike koji su prisutni pri korištenju računarstva u oblaku, provedeno je kratko istraživanje o sigurnosti najpoznatijih oblak servisa. Cilj i svrha istraživanja jest prikazati koliko su najpoznatiji oblak servisi sigurni te kojim se načinima osiguravanja sigurnosti koriste. Hipoteza na kojoj je temeljeno istraživanje jest da su najpoznatiji oblak servisi sigurni te svoje korisnike informiraju o načinima na koje osiguravaju sigurnost.

8.1 Metodologija

Za uzorak su odabrani Microsoft Azure, Amazon Web Services i Google Cloud Platform oblak servisi. Potrebni podaci za istraživanje prikupljane su na stranicama pružatelja oblak usluga. Za prikupljanje podataka korištena je metoda analize sadržaja. Metoda analize sadržaja pripada metodama prikupljanja primarnih podataka. Ona se može provoditi temeljem različitih izvora informacija kao što su pisani tekstovi, vizualni zapisi, audio zapisi, audio-vizualni zapisi i drugo.[38]

Posjećena je stranica svakog oblak servisa te su proučeni svi podaci koji se nalaze na njima, a vezani su uz sigurnost korištenja oblak usluga. Nakon prikupljanja potrebnim podataka, usporedba je provedena na temelju sigurnosnih elemenata koji uključuju neke od navedenih i objašnjenih kontrola. Na taj su način dobiveni rezultati koji prikazuju razlike i sličnosti sigurnosti korištenja navedenih oblak servisa.

8.2 Rezultati i rasprava

Nakon provedenoga istraživanja dobiveni rezultati (Tablica 1) prikazuju kako sva tri oblak servisa posebnu pažnju posvećuju sigurnosti svojih korisnika. Iz tablice je vidljivo kako sva tri oblak servisa imaju SOC 1, SOC 2 i SOC 3 certifikat sigurnosti. Osim toga, sva tri servisa podržavaju i djeluju prema ISO 27001 i ISO 27018 standardima. Microsoft Azure je bio prvi pružatelj oblak usluga koji je usvojio novi međunarodni standard zaštite privatnosti oblaka, ISO 27018. Kada su u pitanju CSA STAR certifikati, Amazon Web Services je jedini od tri analizirana oblak servisa koji nema taj certifikat.

[38] Tkalac Verčić, Ana; Sinčić Čorić, Dubravka; Pološki Vokić, Nina. Priručnik za metodologiju istraživačkog rada: Kako osmisliti, provesti i opisati znanstveno i stručno istraživanje. Zagreb: M.E.P. d.o.o., 2010, 90-94

Tablica 1: Rezultati istraživanja

Sigurnosni elementi	Microsoft Azure	Amazon Web Services	Google Cloud Platform
SOC 1	Da	Da	Da
SOC 2	Da	Da	Da
SOC 3	Da	Da	Da
ISO 27001	Da	Da	Da
ISO 27018	Da	Da	Da
CSA STAR certifikati	Da	Ne	Da
Kriptiranje podataka	AES-256	Na EC2 usluzi (SafeNet, S3, Glacier, EBS)	AES–256
Autorizacija pristupa	Da	Da	Da
Mrežna sigurnost	Da	Da	Da
Revizije i izvještavanje o događanjima	Da	Da	Da
Usklađenost	Da	Da	Da

Podaci su najvrjednija i nezamjenjiva imovina, a kriptiranje služi kao posljednja i najsnažnija linija obrane u višeslojnoj strategiji zaštite podataka. Za kriptiranje podataka u mirovanju Azure koristi AES–256 (Advanced Encryption Standard-256), a za podatke u tranzitu koristi standardne transportne protokole između korisničkih uređaja i Microsoftovih podatkovnih centara kao i unutar samih podatkovnih centara. Amazon nudi kriptiranje na EC2 usluzi (SafeNet, S3, Glacier, EBS). Fleksibilne opcije upravljanja ključevima, uključujući AWS Servis za upravljanje ključevima (eng. *Key Management Service*), omogućujući vam odabrati želite li da AWS upravlja ključevima za kodiranje ili da vi imate potpunu kontrolu nad ključevima. Kriptografski ključevi (eng. *encryption keys*) su pohranjeni na bazi hardvera pomoću AWS CloudHSM (AWS Cloud Hardware Security Module), čime ćete zadovoljiti zahtjeve za sukladnost. Osim toga, AWS pruža aplikacijska programska sučelja (eng. *application programming interface, API*) za integraciju kriptiranja (eng. *encryption*) i zaštite podataka s bilo kojom od usluga koje razvijete ili implementirate u AWS okruženju.

Googleova platforma oblak usluge nudi kriptiranje sadržaja korisnika koji su pohranjeni u mirovanju koristeći jedan ili više mehanizama za kriptiranje, uz nekoliko manjih iznimaka. Na primjer, svi novi podaci pohranjeni u stalnim diskovima kriptirani su AES–256 standardom, a svaki ključ za kriptiranje sam je kriptiran redovnim rotirajućim skupom glavnih ključeva. Iste politike kriptiranja, upravljanja ključevima (eng. *key management*) i kriptografske biblioteke (eng. *cryptographic libraries*) koje se koriste za vaše podatke na platformi Google Cloud koriste mnoge Googleove produkcijske usluge, uključujući Gmail.

Sva tri oblak servisa zahtijevaju autorizaciju (eng. *authorization*) pristupa te tako štite podatke pojedinih korisnika. Azure omogućuje autorizaciju s više faktora za sigurnu prijavu, uključujući specijalizirani administrativni pristup kroz upravljanje privilegiranim identitetom Azure Active Directory. Izvršava provjeru autentičnosti (eng. *authentication*), autorizacije i kontrole pristupa putem standardnih protokola poput SAML 2.0, WS-Federation i OpenID Connect. Amazon također nudi autorizaciju pristupa tj. nudi mogućnost definiranja, provođenja i upravljanja pravilima o korisničkom pristupu preko njega. To uključuje AWS menadžment za identifikaciju i pristup (eng. *Identity and Access Management, IAM*) koji omogućuje definiranje pojedinačnih korisničkih računa s dozvolama u svim resursima Amazon sustava, AWS autentikaciju više faktora (eng. *AWS Multi-Factor Authentication*) za povlaštene račune, uključujući opcije za hardverske autorizacije i AWS upravnu službu (eng. *Directory Service*) koja omogućava integriranje s korporativnim direktorijima. Kada je riječ o Googleu svaki pristup resursima reguliran je autorizacijom koja ovlašćuje druge Googleove usluge, što znači da možemo koristiti postojeće Google račune. Značajke koje su dostupne korisnicima prilikom upravljanja uključuju pravila za lozinku (eng. *password*), provođenje provjere autentičnosti i nova inovacija za povjeru autentičnosti u obliku hardverskih sigurnosnih ključeva.

Još jedan važan sigurnosni element koji ispunjavaju sva tri servisa oblak usluga jest mrežna sigurnost. Microsoft Azure ostvaruje to prvenstveno putem vatrozida (eng. *firewall*), dijeljenih lokalnih mreža (eng. *Local Area Network*) i fizičkog odvajanja poslužitelja od sučelja s javnošću. Korisnici mogu implementirati više logički izoliranih privatnih mreža, a svaka virtualna mreža izolirana je od drugih virtualnih mreža. Za lokalne klijente, Windows Server 2016 uključuje vatrozid, analizu prijetnji i brojne značajke mrežne sigurnosti. Azurov centar za sigurnost (eng. *Azure Security Center*) pruža centralizirani portal s kojeg možete osigurati resurse koje ste postavili u Azure. Kada omogućite Azure Security Center on nudi preporuke i upozorenja o pitanjima sigurnosti mreže, s centraliziranim portalom iz kojeg

možete pomoći u osiguravanju vaših Azure implementacija i spriječiti, otkriti i reagirati na prijetnje. Koristi analizu ponašanja za učinkovito otkrivanje prijetnji i pomaže vam izgraditi vremensku liniju napada za brži oporavak. Amazon također pruža nekoliko usluga za povećanje privatnosti i kontrole pristupa mreži. One uključuju mrežni vatrozid ugrađeni u Amazonov virtualni privatni oblak (eng. *virtual private cloud, VPC*) i mogućnosti vatrozida web aplikacija (eng. *AWS Web application firewall, WAF*) koje omogućavaju stvaranje privatnih mreža i kontrolu pristupa vašim aplikacijama i kodiranje u tranzitu s kriptografskim protokolom koji omogućuje siguran prijenos podataka (eng. *Transport Layer Security, TLS*) na svim uslugama. Korisnici AWS-a imaju koristi od AWS usluga i tehnologija izrađenih za postizanje otpornosti u odnosu na distribuirane napade uskraćivanjem usluga (eng. *Distributed Denial-of-service, DDoS*). Budući da je povezan s većinom pružatelja internetskih usluga (eng. *Internet Service Provider, ISP*) u svijetu, Googleova globalna mreža pomaže poboljšanju sigurnosti podataka u tranzitu. Skener sigurnosti oblaka (eng. *Cloud Security Scanner*) pomaže programerima razvojnih aplikacija da u svojim web aplikacijama identificiraju najčešće ranjivosti, posebno skriptiranje na više mjesta (eng. *Cross-site Scripting, XSS*) i mješoviti sadržaj.

Revizija i prijava događaja vezanih uz sigurnost i povezana upozorenja važna su komponenta u učinkovitoj strategiji zaštite podataka. Sigurnosni zapisnici i izvještaji pružaju vam elektronički zapis sumnjivih aktivnosti i olakšavaju otkrivanje obrazaca koji mogu ukazivati na pokušaj ili uspješan vanjski prodor mreže, kao i interni napadi. Microsoftove poslovne usluge i proizvodi pružaju vam sigurnosne revizije i mogućnosti zapisivanja kako biste lakše identificirali praznine u sigurnosnim politikama i mehanizmima. Microsoftove usluge nude neke (i u nekim slučajevima sve) sljedeće mogućnosti: centralizirano praćenje, prijavljivanje (eng. *login*) i sustave analize kako bi se osigurala kontinuirana vidljivost, pravodobna upozorenja, izvješća koja će vam pomoći upravljati velikom količinom informacija koje generiraju uređaji i usluge. Stroge revizije treće strane potvrđuju da Azure poštuje sigurnosne kontrole propisane standardima. Kod Amazona certifikacije i potvrde o sukladnosti ocjenjuju nezavisni revizori treće strane i rezultiraju certifikacijom, revizijskim izvješćem ili potvrdom usklađenosti. Google redovito posjećuje nekoliko neovisnih revizija treće strane kako bi pružio jamstvo privatnosti i usklađenosti. To znači da je neovisni revizor pregledao kontrole prisutne u njihovim podatkovnim centrima, infrastrukturi i operacijama. Googleov revizijski pristup treće strane osmišljen je tako da bude sveobuhvatan kako bi osigurao jamstvo Googleove razine informacijske sigurnosti s obzirom na povjerljivost,

integritet i dostupnost. Korisnici mogu koristiti ove revizije treće strane kako bi procijenili kako Googleovi proizvodi mogu zadovoljiti njihove zahtjeve za usklađenost i obradu podataka.

8.2.1 Ostali elementi sigurnosti

Osim sigurnosnih elemenata korištenih za usporedbu ova tri oblak servisa, zabilježeni su i neki drugi elementi koji su uočeni tijekom istraživanja. Azure svojim korisnicima daje do znanja tko ima pristup njihovim podacima. Microsoft svojim inženjerima daje pristup korisničkim podacima za obavljanje ključnih zadataka, kao što su održavanje i nadogradnje. Kooperantima je odobren pristup za obavljanje ograničenih usluga. Koriste stroge kontrole kojima upravljaju pristupom podacima o korisnicima, dodjeljuju najnižu razinu povlastica potrebnih za dovršavanje ključnih zadataka i opozivaju pristup kada više nije potreban. Osim toga, Azure pomaže u zaštiti od prijetnji zlonamjernim softverom (eng. *malicious software*) na više načina. Microsoft Antimalware izgrađen je za oblak, a dodatne zaštite od zlonamjernog softvera pružaju se u određenim uslugama. Microsoftove tehnologije za upravljanje prijetnjama pomažu u zaštiti sustava od zlonamjernog softvera, kako u oblaku tako i u lokalnim okruženjima. Zlonamjerni softver je vodeći uzrok kompromitiranja identiteta. Može se izvoditi u pozadini i prikupljati informacije, kao što su korisnička imena (eng. *user names*) i lozinke (eng. *passwords*), te ih vratiti napadaču. S ukradenim vjerodajnicama, napadač može pristupiti, mijenjati ili uništiti vrijedne podatke. Ako ugroženi račun ima administratorske ovlasti, napadač može promijeniti postavke sustava ili računa i učiniti mnogo veću štetu. Dakle, važan element u zaštiti korisničkih identiteta je zaštita od posljedica zlonamjernog softvera.

AWS pak nudi niz alata koji omogućuju usklađenost resursa u oblaku s organizacijskim standardima i najboljim praksama. To uključuje:

1.) Amazon Inspector, usluga procjene sigurnosti, koja automatski procjenjuje aplikacije za ranjivosti ili odstupanja od najboljih praksi, uključujući i utjecajne mreže, operativni sustav i priloženu pohranu
2.) Alate za implementaciju, upravljanje stvaranjem i stavljanjem u pogon AWS resursa prema organizacijskim standardima
3.) Alati za upravljanje zalihama i konfiguracijama, uključujući AWS Config, koji identificiraju resurse AWS, a zatim prate i upravljaju promjenama tih resursa tijekom vremena

4.) Alati za definiranje i upravljanje predlošcima, uključujući AWS CloudFormation za stvaranje standardnih, unaprijed konfiguriranih okruženja.

AWS također pruža alate koji vam omogućuju da vidite točno što se događa u vašem AWS okruženju. To uključuje: duboku vidljivost u aplikacijskim programskim sučeljima (eng. *application programming interface, API*) putem AWS CloudTrail, opciju agregacije zapisnika, pojednostavljivanje istraga i izvješćivanje o sukladnosti te obavijesti o upozorenjima putem Amazon CloudWatch-a kada se pojave određeni događaji. Ti alati i značajke vam pružaju vidljivost koja vam je potrebna kako biste utvrdili probleme prije nego što utječu na vas i omogućuju vam poboljšanje sigurnosti i smanjivanje profila rizika vašeg okruženja.

Googleova oblak platforma također pruža alate, kao što su Google Cloud Logging i Google Cloud Monitoring, koji olakšavaju prikupljanje i analiziranje zapisnika zahtjeva i praćenje dostupnosti vaših infrastrukturnih usluga. Ti alati također olakšavaju stvaranje prilagođenih nadzornih ploča i postavljanje upozorenja kada se problemi pojavljuju.

Prema ispitanim sigurnosnim elementima može se zaključiti kako sva ti oblak servisa zadovoljavaju sigurnosna pitanja. Naime, svi svoje usluge standardiziraju prema međunarodno priznatim certifikatima. Jedina iznimka je Amazon koji nema CSA STAR certifikat. Svaki od njih je omogućio korisnicima, i onima koji će to tek postati, jasan uvid u njihovo djelovanje i poduzete mjere po pitanju sigurnosti. To je naravno važna stavka kada biramo oblak servis. Osim međunarodnih standarda ovi oblak servisi zadovoljavaju i ostale mjere sigurnosti kao što je kriptiranje podataka, autentikacija, mrežna sigurnost, usklađenost i dr. Microsoft Azure najdetaljnije opisuje svoje korake pri osiguravanju sigurnosti. Na njihovim stranicama moguće je pronaći najviše informacija. No to ih ne čini najsigurnijim oblak servisom. Na temelju ovoga istraživanja možemo reći kako su sva tri oblak servisa relativno sigurna. Iako su sigurnosne značajke na visokoj razini, mjesta za napredak ima te je potreban neprestan rad na tom području.

9. Najčešći napadi na oblak servise

Oblak servisi nude različite dokaze o sigurnosti njihovih usluga. Raznim certifikatima korisnicima daju do znanja kako je pohrana podataka u oblaku sigurna te kako je njihov servis najbolji za njih. No unatoč tome događaju se napadi na oblak servise. Kao što je već navedeno u radu postoji mnogo različitih prijetnji sigurnosti, a neke od njih se ostvaruju i ugrožavaju korisnike. Unutar ovoga poglavlja bit će navedeni najčešći napadi na oblak servise.

9.1 Povreda podataka

Na prvom mjestu najčešćih napada na oblak servise nalazi se povreda podataka (eng. *Data Breaches*). To je incident u kojem se oslobađaju, pregledavaju, kradu ili upotrebljavaju osjetljive, zaštićene ili povjerljive informacije od strane pojedinca koji nisu ovlašteni za to. Ova vrsta napada može biti rezultat ljudske pogreške, ranjivosti aplikacije ili pak primarni cilj napada. Povreda podataka može uključivati sve informacije koje nisu bile namijenjene javnom izdavanju. Podaci koji se pohranjuju u oblaku mogu imati vrijednost napadačima iz različitih razloga. Često se traže financijski, zdravstveni i osobni podaci za provođenje različitih lažnih aktivnosti. Neki od pružatelja oblak usluga koji su doživjeli ovakav napad jesu GoGrid i Dropbox Inc. GoGrid je 2012. objavio kako je neovlaštena treća strana pregledala podatke o računima klijenata uključujući podatke o kreditnoj kartici. Pružatelj je odmah obavijestio federalne organe za provedbu zakona. Dropbox je više puta potvrdio napade u kojima su procurili podaci više od 68 milijuna korisnika. [39]

9.2 Nedostatan identitet, vjerodostojnost i upravljanje pristupom

Povrede podataka i omogućavanje napada mogu se pojaviti zbog nedostatka stabilnih sustava upravljanja identitetom, neuspjehom korištenja autentikacije, slabe lozinke i nedostatka automatske rotacije kriptografskih ključeva, lozinki i certifikata. Identitetni sustavi moraju biti mjerljivi za upravljanje životnim ciklusom za milijune korisnika. Sustavi za upravljanje identitetom moraju podržavati neposredno osiguranje pristupa resursima kada dođe do promjene kadrova, kao što je prestanak radnog odnosa ili promjena uloga. Identitetni sustavi postaju međusobno povezaniji, a povezivanje identiteta s pružateljem oblaka usluga postaje

[39]CSA. The Treacherous 12: Cloud computing top threats in 2016. URL: https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf (2017-05-30)

sve češće kako bi se olakšalo održavanja korisnika. Organizacije koje žele povezati identitet s pružateljima oblak usluga trebaju razumjeti sigurnost oko rješenja identiteta, uključujući procese i infrastrukturu.[40]

9.3 Nesigurna sučelja i API-ji

Sigurnost i dostupnost oblak usluga ovisi o sigurnosti osnovnih aplikacijskih programskih sučelja (eng. *application programming interface, API*). Od provjere autentičnosti i kontrole pristupa do enkripcije i praćenja aktivnosti, ta sučelja moraju biti dizajnirana za zaštitu od slučajnih i zlonamjernih pokušaja krađe. Organizacije se mogu graditi na tim sučeljima kako bi svojim korisnicima ponudile dodatnu vrijednost. No tu se javlja rizik od izlaganja vrijednih podataka. Jedan od primjera takvog napada jest Američka unutarnja prihodna usluga (eng. *US Internal Revenue Service, IRS*) koja je 2015. godine izložila preko 300 000 zapisa putem ranjivog API-ja.

9.4 Gubitak podataka

Mogućnost trajnog gubitka podataka (eng. *data loss*) je zastrašujući za korisnike i poslovne subjekte. Podaci pohranjeni u oblaku mogu se izgubiti iz razloga koji nisu zlonamjerni. Slučajno brisanje od strane pružatelja oblak usluga ili, još gore, fizičke katastrofe poput požara ili potresa, može dovesti do trajnog gubitka podataka o korisnicima, osim ako pružatelj ili potrošač oblak ne poduzme odgovarajuće mjere za sigurnosno kopiranje podataka. Nadalje, teret izbjegavanja gubitka podataka ne spada isključivo u pružateljeve obaveze. Ako klijent šifrira svoje podatke prije nego što ih prenese u oblak, ali izgubi ključ za šifriranje, podaci će se izgubiti. U travnju 2011. godine, Amazon EC2 pretrpio je pad koji je doveo do značajnog gubitka podataka za mnoge korisnike.[41]

9.5 Ranjivosti sustava

Ranjivosti sustava (eng. *System Vulnerabilities*) se može iskoristiti u programima koje napadači mogu koristiti za infiltriranje računalnog sustava u svrhu krađe podataka, preuzimanja kontrole nad sustavom ili ometanja servisnih operacija. Ranjivosti unutar komponenti operacijskog sustava stavljaju sigurnost svih usluga i podataka u značajni rizik. Ova vrsta prijetnje nije ništa novo. U oblaku se sustavi različitih organizacija nalaze u

[40] Isto

[41] Isto

neposrednoj blizini i daju im pristup zajedničkoj memoriji i resursima, stvarajući novu površinu napada.

9.6 Otmica računa

Metode napadanja poput krađe identiteta, prijevare i iskorištavanja softverskih ranjivosti i dalje postižu rezultate. Često se upotrebljavaju vjerodajnice i lozinke, što pojačava utjecaj takvih napada. Ako napadači dobiju pristup vjerodajnicama, oni mogu prisluškivati vaše aktivnosti i transakcije, manipulirati podacima, vratiti krivotvorene informacije i preusmjeriti svoje klijente na nelegitimne web stranice. U travnju 2010. Amazon je doživio pogrešku skriptiranja na više mjesta (eng. *Cross-site Scripting, XSS*) koja je omogućila napadačima okupljanje vjerodajnica s web mjesta. U lipnju 2014., račun za Code Spaces Amazon AWS je ugrožen kada nije uspio zaštititi administratorsku konzolu pomoću višekratne autentikacije. Sva imovina tvrtke bila je uništena.

9.7 Nedovoljna pažnja

Kada rukovoditelji kreiraju poslovne strategije, moraju se razmotriti tehnologije oblaka i pružatelji oblak usluga. Razvijanje dobrih smjernica i kontrolne liste za dubinsku procjenu prilikom ocjenjivanja tehnologija i pružatelja oblak usluga od ključne je važnosti za uspjeh. Organizacija koja želi usvojiti tehnologije oblaka i odabrati pružatelja bez obavljanja dubinske analize izlaže se bezbrojnim komercijalnim, financijskim, tehničkim, pravnim i usklađenim rizicima koji ugrožavaju njegov uspjeh. To vrijedi ako tvrtka razmišlja o preseljenju u oblaku. U 2012. javni oblak Amazon web servisa (AWS), koji se oslanja na Netflix, iskusio je prekid u regiji SAD-a zbog slučajnog brisanja podataka koji kontroliraju balansiranje opterećenja.[42]

9.8 Zlouporaba i neželjena upotreba oblak usluga

Loše osigurana implementacija oblak usluge, besplatne probne usluge u oblaku i lažne prijave računa putem prijevare otkrivaju zlonamjerne napade. Zlonamjerni glumci mogu iskoristiti resurse računalnog oblaka za ciljanje korisnike, organizacije ili druge pružatelje oblaka. Primjeri zloupotrebe resursa temeljenih na uslugama u oblaku uključuju pokretanje DDoS napada, e-mail spama i phishing kampanje, itd. Pružatelji oblak usluga moraju imati okvir odgovora na incident kako bi se riješili zlouporabe resursa, kao i način da korisnici mogu

[42] Isto

prijaviti zloupotrebu. Amazonov Elastic Cloud Computing patio je od vrlo sofisticiranog napada skupine nepoznatih hakera, koji su pronašli način za preokretanje koncepta kodova i stvorili lako dostupan ulaz za sebe u Amazonovu banku raspoložive procesorske snage.

9.9 Uskraćivanje usluge

Napadi uskraćivanjem usluga (eng. *Denial-of-service, DoS*) su napadi kojima se onemogućava korisnicima pristupiti njihovim podacima ili njihovim aplikacijama. Asimetrični DoS napadi na razini aplikacije iskorištavaju ranjivosti na web poslužiteljima, bazama podataka ili drugim resursima u oblaku, čime zlonamjerni pojedinac može izdvojiti aplikaciju s jednim iznimno malim sadržajem napada. Drugi se napadi mogu usmjeriti na jednako ograničene resurse. Ekonomski DoS ugrožava novčani tijek tvrtke, koristeći dinamičnu prirodu u oblaku kako bi prevladao sposobnost plaćanja za pokretanje. Isto tako, ljudski kapital neke organizacije može se brzo vezati za pravni posao za birokratski DoS i ostaviti tvrtku jednako nesposobnu za pružanje usluge. Pružatelj oblak usluga, Rackspace, doživio je DDoS napad na svoje usluge 2014. godine. U još jednom spektakularnom primjeru napada, Amazon EC2 suočio se s još jednim velikim DDoS napadom. Ovi napadi doveli su do prekida rada, poslovnih gubitaka te dugoročnih i kratkoročnih učinaka na poslovne procese žrtava.[43]

[43] Somani, Gouvar...[et. al]. DDoS attacks in cloud computing: Issues, taxonomy, and future directions. // Computer Communications 107, (2017), str. 30-48. URL: http://www.buyya.com/papers/DDoSCloudCC2017.pdf (2017-05-30)

10. Zaključak

Na temelju ovoga rada možemo zaključiti kako je pitanje sigurnosti pri korištenju oblak servisa jako važno. Toga su svjesni korisnici, pružatelji oblak usluga i mnoge organizacije koje su svoj rad i djelovanje posvetili sigurnosti i privatnosti informacija koje korisnici pohrane u oblaku. One propisuju određene standarde i upute kojima olakšavaju pružateljima oblak usluga oformljivanje sigurnog okruženja. Osim toga, pomoću certifikata koje dobiju svojim korisnicima pružaju dokaze kako je njihov oblak siguran za pohranu informacija. Svim korisnicima je potreban dokaza o sigurnosti njihovih informacija. Na temelju provedenoga istraživanja najpoznatijih oblak servisa zaključujemo kako se smjernice međunarodnih organizacija poštuju. Mnogim certifikatima i sigurnosnim mjerama oni dokazuju kako su informacije pohranjene u njihovim oblacima sigurne. Također, svojim korisnicima pružaju detaljne informacije o tome što se događa s njihovim informacijama u oblaku. No usprkos svim sigurnosnih mjerama, napadi se događaju. Na temelju njih oblak servisi poboljšavaju svoj rad i zaključuju što je potrebno učiniti kako se isti incident ne bi ponovio. Na kraju je potrebno reći kako je sigurnost analiziranih oblak servisa sada na zadovoljavajućoj razini, ali je mogući napredak i razvijanje na ovom području.

11. Literatura

1. Amazon Web Services. URL: https://aws.amazon.com/ (2017-04-02)

2. Bhadauria, Rohit...[et. al.]. Security issues in cloud computing. // Acta Tehnica Corviniensis – Bulletin of Engineering 7, 4(2014), str. 159-177. URL: http://web.a.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=5d9b7a3a-36a8-46f8-94d9-791561ef3a03%40sessionmgr4010&vid=0&hid=4109 (2017-05-24)

3. Bsi. ISO / IEC 27108: SafeguardingPersonal Information in the Cloud. URL: https://www.bsigroup.com/Documents/iso-iec-27018/ISOIEC-27018-Safeguarding-information-in-the-cloud-whitepaperDec2015.pdf

4. Chen, Yanpei; Paxson, Vern; Katz, Randy H. What's New About Cloud Computing Security?. Electrical Engineering and Computer Sciences University of California at Berkeley, 2010. URL: http://www.utdallas.edu/~muratk/courses/cloud13s_files/what-is-new-in-cloud-security.pdf (2017-03-29)

5. Cloud Standars Customer Council. Security for Cloud Computing: 10 Steps to Ensure Success, 2015. URL: http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf (2017-03-29)

6. Cloud Watch. Cloud certification guidelines and recommendations. 2015. URL: http://cordis.europa.eu/docs/projects/cnect/4/610994/080/deliverables/001-D41Cloudcertificationguidelinesandrecommendationsrevisedversion.pdf (2017-04-01)

7. Cloud Watch HUB. URL: http://www.cloudwatchhub.eu/eurocloud-%E2%80%93-star-audit (2017-05-20)

8. CSA. The Treacherous 12: Cloud computing top threats in 2016. URL: https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf (2017-05-30)

9. Engineering and Computer Sciences University of California at Berkeley, 2010. URL: http://www.utdallas.edu/~muratk/courses/cloud13s_files/what-is-new-in-cloud-security.pdf (2017-03-29)

10. European Union Agency for Network and Information Security. URL: https://www.enisa.europa.eu/ (2017-05-23)

11. Google Cloud Platform. URL: https://cloud.google.com/ (2017-04-02)

12. IEEE Cloud Computing URL: http://cloudcomputing.ieee.org/standards (2017-24-05)

13. International Organization for Standardization. ISO/IEC 27018:2014: Information technology -- Security techniques -- Code of practice for protection of personally identifiable

information (PII) in public clouds acting as PII processors. URL: https://www.iso.org/standard/61498.html (2017-04-02)
14. Microsoft Azure. URL: https://azure.microsoft.com/en-us/ (2017-04-03)
15. Nacionalni CERT. Cloud Computing: NCERT-PUBDOC-2010-03-193, 2010. URL: http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-03-293.pdf (2017-03-27)
16. Panian, Željko. Elektroničk poslovanje druge generacije. Zagreb: Ekonomski fakultet Zagreb, 2013. Str. 172
17. Radić, Branimir. Sigurnost u računalnom oblaku. URL: http://www.fer.unizg.hr/_download/repository/KDI%2C_Branimir_Radic.pdf (2017-04-02)
18. Sen, Jaydip. Securitiy and privacy issues in cloud computing. URL: https://pdfs.semanticscholar.org/4dc3/70d253020947a8e66b701e12dd0233161229.pdf (2017-05-05)
19. Somani, Gouvar...[et. al]. DDoS attacks in cloud computing: Issues, taxonomy, and future directions. // Computer Communications 107, (2017), str. 30-48. URL: http://www.buyya.com/papers/DDoSCloudCC2017.pdf (2017-05-30)
20. Tkalac Verčić, Ana; Sinčić Čorić, Dubravka; Pološki Vokić, Nina. Priručnik za metodologiju istraživačkog rada: Kako osmisliti, provesti i opisati znanstveno i stručno istraživanje. Zagreb: M.E.P. d.o.o., 2010, 90-94
21. Yesilyurt, Murat; Yalman, Yildiray. New approach for ensuring cloud computing security: using data hiding methods. // Indian Academy of Sciences 41, 11(2016), str. 1289-1298. URL: http://web.b.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=2&sid=b3d70d07-b48e-4193-95ff-6ed17fb6cd45%40sessionmgr102&hid=118 (2017-05-21)