

Inovativni projekti za poboljšanje kvalitete života

Sigurnost u oblaku



Poslovanje u oblacima (Cloud computing) ima potencijala biti tehnologija koja će znatno promijeniti način kako tvrtke koriste informacijsku tehnologiju, odnosno ulogu i rad inženjera u tvrtkama. biti korisni cijeloj društvenoj zajednici neke su od osnovnih ideja djelovanja te zagrebačke tvrtke. Krajem je prošle godine tvrtka krenula s dva specifična i inovativna projekta.

Tehnološka platforma na kojoj počiva ideja poslovanja u oblacima je virtualizacija, a korisnici cloud uslugu koriste kroz web-preglednik preko javne ili privatne visokopropusne mreže. Za očekivati je znatan rast upotrebe cloud usluga putem mobilnih uređaja.

Cloud computing na tržištu nudi virtualne slojeve informatičkoga sustava kao uslugu; aplikacije kao uslugu, platformu kao uslugu, infrastrukturu kao uslugu.

Cloud aplikacije su gotove desktop aplikacije opće namjene, odnosno specijalizirane poslovne aplikacije poput praćenja odnosa s kupcima, sve smještene u oblaku. Cloud programske platforme omogućuju razvoj i smještaj korisničkih aplikacija u cloud okruženju, a cloud infrastruktura zamjenjuje stvarnu korisničku fizičku infrastrukturu (poslužitelje, diskove, baze podataka, uređaje za osiguranje sigurnosti).

Pravo cloud computing okruženje mora zadovoljiti sljedeće uvjete:

- 1.** Neograničena skalabilnost (po potrebi kapacitet usluge se dinamički skalira)
- 2.** Naplata prema korištenju (plaća se samo ono što se koristi i koliko se koristi)
- 3.** Bez naplate uspostave usluge (trenutačna, besplatna uspostava usluge, samo operativni troškovi)
- 4.** Korisnik ne mora održavati sustav (samoposluga, održavanje se svodi na administriranje korisnika i praćenje korištenja usluge)

Po istraživanjima glavni je uzrok za zabrinutost kod uvođenja cloud compu-

tinga u tvrtke sigurnost i to najviše zbog gubitka kontrole. Prihvaćanjem javne cloud computing usluge, velik dio mreže, računalnih sustava, aplikacija i podataka dolazi pod kontrolu treće osobe, davatelja usluge cloud computinga.

Svaka je od značajki cloud computinga mogući sigurnosni problem i treba ju ocijeniti preko osnovnih mjerila informacijske sigurnosti: povjerljivosti, nepovjerljivosti i raspoloživosti.

Skalabilnost i povoljna cijena usluge postiže se dijeljenjem resursa među korisnicima. Upitan je način na koji su odvojeni korisnici koji dijele isti resurs. Izolacija i fizička separacija kakva je prije postojala između sigurnosnih zona prestaje postojati, postoji samo logička separacija.

Složeniji sigurnosni zahtjevi, kao što su npr. aplikacijski firewall, kriptografija ili definicija prava pristupa putem tokena, nisu podržani u javnim cloud uslugama.

Korisnici očekuju da pojačana sigurnost podataka služi kao kompenzacijska kontrola za moguću oslabljenu infrastrukturnu sigurnost jer se dio korisnikove infrastrukturne sigurnosti izmaknuo njegovoj kontroli, a infrastrukturna sigurnost davatelja cloud usluge može biti manje robustna nego što se očekuje.

Iako je prijenos podataka prema cloudu kriptiran (i treba biti kriptiran), bilo kakvo korištenje podataka u cloudu –

osim jednostavnoga spremanja – zahtijeva da podatci budu dekriptirani (zbog pretraživanja i indeksiranja). Također ne treba podrazumijevati da davatelj usluge ima pričuvne preslike podataka pohranjenih u cloudu.

Samoposluživanje može biti problem u slučaju zlopotrebe administrativnih ovlasti. Ako se aktiviraju neželjene usluge, nepotrebno se povećava trošak cloud computing usluge. Još je gora situacija ako netko otkáže uslugu. Što će se dogoditi s podacima korisnika? Hoće li im moći ponovo pristupiti nakon otkrivanja problema ili će ih davatelj usluge trajno izbrisati?

Pun potencijal cloud computinga ovisi o raspoloživosti brzoga pristupa Internetom za sve. To ne mora uvijek biti slučaj; brzina je pristupa manja u ruralnim krajevima, otocima, kod mobilnoga pristupa. Također je moguće da davatelj internetske usluge obavlja filtriranje prometa ili ograničavanje brzine ovisno o vrsti prometa (da bi promovirao svoju cloud uslugu ili ograničio pristup uslugama koje generiraju velik promet od kojega davatelj internetske usluge ne zarađuje). Pouzdanost usluge ovisi o pouzdanosti samoga davatelja cloud computing usluge,

kao i o pouzdanosti svih internetskih veza između krajnjega korisnika i davatelja cloud usluge.

Problem je i s migracijom aplikacije u i iz clouda. Trenutačno ne postoji standard za programsko sučelje u cloudu, ap-

likacije nisu prenosive. Interoperabilnost je bitna da možemo prebaciti podatke na drugu platformu. Npr. možda ćemo ERP aplikaciju ostaviti u tvrtki, a u cloud prebaciti CRM aplikaciju.

Korisnik bi trebao biti zainteresiran da zna koje informacije davatelj usluge cloud computinga prikuplja i kako ih štiti. Koje meta-podatke prikuplja o vašim podacima, kako su zaštićeni i koji pristup vi, kao korisnik, imate do tih meta-podataka.

Davatelj usluge također prikuplja i trebao bi zaštititi veliku količinu podataka vezanih uz sigurnost. Primjerice, na mrežnoj bi razini davatelj usluge trebao prikupljati, nadgledati i zaštititi podatke iz firewalla,

●●● Pun potencijal cloud computinga ovisi o raspoloživosti brzoga pristupa Internetom za sve

IDS/IPS, SIEM uređaja i flow podatke iz routera. Na razini bi poslužitelja davatelj usluge trebao prikupljati sistemske logove, a davatelj bi cloud usluge aplikacijske razine trebao prikupljati i logove aplikacije, uključujući i podatke o autentifikaciji i autorizaciji.

Dodatna kontrola sigurnosti od strane korisnika katkad nije dopuštena. Neki od davatelja usluge po pravilima korištenja ne dopuštaju skeniranje portova i to je kršenje ugovora. Kako onda ispitati sigurnost svoje vlastite platforme pohranjene u cloudu?

U slučajevima kada je potrebno imati visoki stupanj kontrole i transparentnosti, korisnicima obično grade privatni cloud jer je tako lakše biti usklađen s postojećim korporativnim standardima sigurnosti, politikama i zahtjevima regulatora. Lokalna zakonska regulativa može zahtijevati promjene u cloud aplikaciji za koje je pitanje kojom brzinom ih davatelj cloud usluge može provesti (i želi li ih uopće provesti).

Jedina je mogućnost koja danas postoji da bilo koji podatak koji su osjetljivi ili je njihova upotreba zakonski regulirana ne smiju biti smješteni u javnome cloudu (ili da korisnik sam kriptira podatke koji se samo pohranjuju u javnome cloudu).

U javnome cloudu da bi se nadoknadio gubitak kontrole na mrežnoj razini, organizacije će biti prisiljene oslanjati se na programske kontrole kao što su sigurnost aplikacija i kontrola korisničkoga pristupa. Te se kontrole manifestiraju kao: snažna autentifikacija korisnika, autorizacija korisnika zasnovana na ulozi u organizaciji, federacija identiteta, jednostruka prijava (SSO), analiza i praćenje rada korisnika.

Kako tvrtke u cloud computingu gube kontrolu nad zaštitom podataka, sve će više biti prijava (SSO), analiza i praćenje rada korisnika usmjerena na kontrolu pristupa i upotrebi podataka. Od zanimljivih tehnologija tu treba istaknuti otkrivanje prijevara (fraud detection) i zaštitu od nekontroliranoga curenja podataka (data leaking protection).

Nevenko Bartolinčić
www.recro-net.hr

Tvrtka RECRO-NET odlučila je tržištu ponuditi novu metodu sprječavanja i otkrivanja nezakonitih radnji. Još jedan novi naziv u našem rječniku: Proactive Fraud Management.

Spriječimo prijevaru

Sigurnost IT sustava najčešće povežemo s internetskim prijetnjama u obliku hakerskih napada, virusa, crva ili stotinu drugih aplikacijskih i korisničkih aktivnosti. Naravno, svjesni smo da nije samo to u pitanju. Vrlo često sve prijetnje koje nam dolaze gledamo isključivo kroz moguća zatajanja vlastitoga informatičkoga sustava ili poslovnih procesa te koja je financijska šteta ako posao stane. No, što je s prijevarama ili „curenjem“ vrijednih informacija?



U našem su se rječniku smjestile dvije strane riječi koje danas svi prepoznaju, a to su **Data Leakage i Fraud**. Ti nazivi (kao ni njihovo otkrivanje) nisu ni prije bili nepoznati, no tada nisu bili vezani uz informatiku, nego uz silno pregledavanje tona i tona papira, vizualno praćenje procesa i aktivnosti. Danas, gotovo sve takve prijetnje dolaze i prolaze kroz IT sustave. Da li se upravo zbog toga, sprječavanje i otkrivanje trebaju gledati kroz informatiku? I da, i ne. Silne informatičke metode, kao što su prikupljanje logova, enkripcije,

identifikacije, malware detektori, vatrozidi,... nisu uspjele riješiti problem.

Tko se god susreo s takvim problemima, vrlo je vjerojatno krivnju svalio na internu informatiku ili izvanjskoga partnera koji se brine za informatičku/informacijsku sigurnost. Na žalost, problem je širi i, ako se pogleda iz većega kuta, vjerojatno će se otkriti da je pravi problem u tome da nisu potpuno definirane sigurnosne procedure same tvrtke. Mnogobrojni su se za pomoć obratili različitim savjetnicima koji su, nakon snimke stanja, jednostavno rekli „uzmite rješenja za logove, vanjsku zaštitu, video nadzor, enkripciju, identity management,...“ Na kraju smo dobili nekoliko rješenja za svaki segment sigurnosti individualno. Individualne analize rezultata dobivenih korištenjem tih sustava, iznimno troše ljudske resurse, vrijeme i novac ili, jednostavnije rečeno, čekaju da ih netko obradi. To se čekanje najčešće svede na mjesec dana, pola godine, godinu.... ili nikad. Kad se šteta pojavi, već je kasno.

Da bi se željena svrha postigla, a bez velikoga financijskoga i vremenskoga ulaganja, zagrebačka je tvrtka RECRO-NET odlučila tržištu ponuditi novu metodu sprječavanja i otkrivanja nezakonitih radnji. Od sada je u našem rječniku još jedan novi naziv: Proactive Fraud Management. Rješenje se zasniva u prvome redu na pripremljenim sigurnosnim procedurama, definiranju uobičajenih obrazaca ponašanja

Kako se
zaštititi
od curenja
podataka?



pomoć snažnoga analitičkoga alata koji u realnome vremenu simultano prati različite izvore informacija, analizira i vrjednuje svaki korak izvan okvira uobičajenih obrazaca ponašanja, za rezultat dobivamo ALARM U STVARNOM VREMENU.

Zamislimo situaciju...

Agent call centar službe unutar kartičarske kuće, banke ili druge ustanove zanimaju podatci neke slavne osobe. Vrlo jednostavno pristupi podacima i pogleda podatke, zapiše adresu, stanje na računu ili nešto treće. Razloga može biti stotine: znatiželja, koristoljublje, osveta... Koja god bila opravdanja, takva radnja bez valjana razloga nije dopuštena! Agent ima pravo pristupa tim podacima, ali samo ako je to zbog pružanja informacije klijentu, dakle opravdano pregledavanje tih podataka. Svi ćemo sad pomisliti: pa šteta i nije toliko velika... nije nam sustav stao, posao ide dalje, a taj agent više ne radi. Krivo! Jesmo li ikada pomislili na milijunski iznos možebitne naknade štete klijentu, te gubitak ugleda pouzdane tvrtke?

Taj primjer ne ulazi nužno u Fraud područje, ali je definitivno opasno „curenje“ informacija koje se treba spriječiti prije nego dođe do ozbiljnije štete. Ali analiza

neobičajenih radnji agenata ili, još bolje, njihova spoznaja da se aktivnosti analiziraju, dovest će gotovo do 100%-tna sprječavanja tih radnji.

Pa gdje još postoje mogućnosti takvih neovlaštenih korištenja informacija? Svugdje!

Sjetimo se malo i razmislimo o nekim primjerima koje smo već vidjeli na televiziji, Internetu ili u novinama: snimke jurnjava automobilima kroz tunele, ispisi telefonskih poziva, fotografije ili snimke prometnih prekršaja, tajni dokumenti, pa čak i zapisi smiješnih razgovora call centar agenata sa svojim klijentima... od kuda dolaze te informacije??? To je curenje podataka - Data Leakage.

Aprijevare-Fraud? Čega se možemo sjetiti?

- Pružanje i prodaja informacija o telefonskim pozivima poznatih osoba
- Pružanje i prodaja informacija o financijskome statusu klijenata
- Pružanje i prodaja informacija o zdravstvenome statusu klijenata
- Pružanje i prodaja informacijama o

navikama klijenata

- Pružanje i prodaja poslovnih tajni
- Pružanje informacija o prometnim kaznama te retroaktivne izmjene podataka
- Pružanje informacija o policama osiguranja te retroaktivne izmjene podataka
- Pružanje informacija o kreditima, kamatama, uvjetima te opet retroaktivne izmjene podataka
- Pružanje informacija o nadnevcima transakcija i izmjene

To su samo neke od informacija koje svaka tvrtka čuva i jamči za njih, a opet katkad završe u krivim rukama zbog individualnoga interesa, a na golemu štetu i tvrtke i uprave. Kad se to dogodi, već je prekasno. Sad ćemo nakon svega reći da smo i do sad imali alate za sprječavanje... logovi za aktivnosti, identity management za identifikaciju, document management za praćenje „života“ dokumenta, video i snapshot snimače, keystroke snimače, itd. No, do sada nismo imali jedan sustav koji sve te funkcionalnosti ili rezultate ujedini u jedan inteligentan analitički alat koji već na osnovu otkrivanja netipičnih radnji u zadanoj okolini upozorava, odnosno sprječava prijevaru ili neovlašteno prosljeđivanje informacija.

Najljepše od svega je to što implementacija takva sustava ne zahtijeva goleme informatičke i ljudske resurse, nego se zasniva na primjeni pravila koja je gotovo svaka tvrtka uz pomoć onih savjetnika s početka članka raspisala, ali ih ne primjenjuje u potpunosti ili uopće. A ako i nismo pripremili pravila, sam sustav prema vrsti poslovanja ili industriji ima stotine predefiniраниh obrazaca koje možemo primijeniti i postupno prilagoditi.

Na kraju se umjesto nekoga velikoga zaključka možemo zapitati još jednu stvar – što sve možemo izgubiti ako dopustimo ili ne spriječimo „curenje“ samo jedne riječi koja je zaštićena zakonom, poslovnom etikom ili već samo povjerenjem? Zaslužuje li to naš klijent i zaslužujemo li mi da nam se takvo nešto dogodi?