Varnost in računalništvo v oblaku: premik k uporabnikom

David Jelenc

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko, Laboratorij za e-medije
Večna pot 113, 1000 Ljubljana, Slovenija
E-pošta: david.jelenc@fri.uni-lj.si

Abstract

We examine security concerns in cloud computing. Cloud computing involves running application on remote hardware, storing data at distant locations and accessing it through public networks, which presents new possibilities for malicious actors. We describe the cloud shared responsibility security model, describe common risks in cloud computing, and analyze the incidence of most common ones. The analysis shows that cloud users are replacing cloud providers as the main source of risk.

1 Uvod

Računalništvo v oblaku je širok koncept. S tehničnega vidika gre za način zagotavljanja in upravljanja storitev informacijskih tehnologij, kjer različne vire združimo v homogeno celoto tj. konsolidiramo in ponudimo uporabnikom v obliki storitve na zahtevo preko samopostrežnega portala [1].

V zadnjih dveh desetletjih je v velikem porastu, saj prinaša obilne prednosti kot so poenostavljeno upravljanje z računalniško infrastrukturo, oddaljen dostop ter stroškovno učinkovitost. A vendar: pri računalništvu v oblaku uporabljamo infrastrukturo, storitve in programsko opremo, ki pogosto niso ne v naši lasti ne pod našim nadzorom. Podobna je zgodba s podatki – ti se često shranjujejo na oddaljenih lokacijah, so pod tujim skrbništvom ter v določenih primerih še tujo zakonodajo. Vse to odpira možnosti zlorab. V prispevku podamo pregled pogostih groženj in tveganj, ki se pripisujejo računalništvu v oblaku ter opišemo njihovo dinamiko, ki razkriva, da v zadnjem času uporabniki, ne ponudniki, računalništva v oblaku postajajo šibkejši varnostni člen.

Struktura prispevka je sledeča. V drugem poglavju obravnavamo za varnost relevantne vidike računalništva v oblaku, v tretjem pojasnimo idejo deljene skrbi za varnost, v četrtem podamo pregled in analiziramo pogostost glavnih tveganj ter v petem prispevek sklenemo.

2 Računalništvo v oblaku

Ker je koncept računalništva v oblaku širok, je pri varnostni obravnavi smotrna obravnava glede na model namestitve in model storitve: varnostna tveganja so različna, če s celotno infrastrukturo in podatki upravlja ponudnik v tuji državi kot pa če nastopamo v vlogi ponudnika in uporabnika sami ter imamo oblačno infrastrukturo v lastnih prostorih [2].

2.1 Namestitveni model

Model namestitve določa, kako so viri, storitve in infrastruktura strukturirani, organizirani in deljeni. Ločimo štiri glavne vrste, in sicer javne, skupnostne, zasebne in hibridne oblake.

2.1.1 Javni oblak

Pri javnem oblaku je infrastruktura v lasti zunanjega ponudnika, storitve pa so, običajno proti plačilu, dostopne vsem. Računski viri so konsolidirani in deljeni med uporabniki, od katerih lahko vsak dostopa le do svojih. Privlačnost javnega oblaka je v tem, da uporabnikom prihrani začetni strošek vzpostavitve infrastrukture in nudi predvidljive operativne stroške. Glavni varnostni pomislek pa se nanaša na to, da so računski viri in podatki pod nadzorom ponudnika. Večji ponudniki na področju javnih oblakov so Amazon, Google, Microsoft in drugi.

2.1.2 Skupnostni oblak

Pri skupnostnem oblaku skupina organizacij za lastne potrebe ustanovi skupno oblačno infrastrukturo. Takšna namestitev je pogosta za zdravstvene, znanstvene ali vladne organizacije z namenom lažjega obvladovanja stroškov. Storitve v skupnostnem oblaku so tako dostopne le uporabnikom iz omenjenih organizacij, medtem ko je delitev virov podobna delitvi v javnem oblaku, a običajno z večjo mero prilagodljivosti.

2.1.3 Zasebni oblak

O zasebnem oblaku govorimo, ko je oblačna infrastruktura v lasti organizacije in namenjena le lastnim potrebam. Računalniška oprema se običajno nahaja v prostorih organizacije, ni pa to nujno. Ta model omogoča lažji nadzor nad varnostjo, a zahteva znanje za upravljanje z oblačno infrastrukturo. (Pripomnimo, da zgolj zasebna računalniška infrastruktura še ne pomeni, da gre za zasebni oblak: računski viri morajo biti ustrezno organizirani, da podpirajo koncepte računalništva v oblaku.)

2.1.4 Hibridni oblak

Pri hibridnem oblaku gre za kombinacijo dveh ali več namestitvenih modelov. Pogosta kombinacija je javni–zasebni oblak, kjer se del računskih virov izvaja na jav-

nem oblaku, del pa na zasebnem. Razlogi za tako hibridnost so denimo varnostni pomisleki ali prevelike zakasnitve v javnem oblaku in podobno. Tak model je pogosta vmesna točka, ko organizacija seli računske vire na javno oblačno infrastrukturo. Hibridni model je privlačen, saj ponuja tako prednosti javnega kot tudi zasebnega oblaka, a je zaradi kompleksne integracije izvedbeno zahtevnejši.

2.2 Storitveni model

Model storitve določa, katere računske vire ponudnik nudi in na kakšnem nivoju abstrakcije. Čeprav je danes tovrstnih abstrakcij več, izvirna NIST klasifikacija [1] podaja tri: infrastrukturo kot storitev, platformo kot storitev in programsko opremo kot storitev.

2.2.1 Infrastruktura kot storitev

Ponudba infrastrukture kot storitve (angl. infrastructure as a service, IaaS) pomeni oskrbo računskih, podatkovnih in omrežnih kapacitet, kjer uporabnik tipično prejme navidezni stroj (angl. virtual machine) z želenimi kapacitetami in sam upravlja z operacijskim sistemom in ostalo programsko opremo. Ponudnik pa nadzira in upravlja s hipervizorjem, s strojno opremo ter z omrežno in električno infrastrukturo. Izmed vseh storitvenih modelov gre za najbolj splošnega, saj omogoča poganjanje poljubnih delovnih bremen.

2.2.2 Platforma kot storitev

Platforma kot storitev (angl. platform as a service, PaaS) pomeni, da ponudnik poleg infrastrukturnega dela še dodatno upravlja z operacijskim sistemom, izvajalnim okoljem ter različnimi aplikacijskimi storitvami. Pri tem se uporabnikova domena nadzora krči: uporabnik pri tem nadzira le še podatke, razvito aplikacijo in nekatere nastavitve izvajalnega okolja. Privlačnost platforme kot storitve je v tem, omogoča hitro namestitev in poganjanje aplikacij, ki so razvite v programskih jezikih in z orodji, ki jih ponudnik podpira. Poleg običajnih storitev ponudniki ponujajo tudi lastne specifične rešitve, ki so na voljo le na njihovi platformi. Pri tem velja omeniti, da se lahko uporabnik z uporabo takih storitev na ponudnika nehote *priklene* (angl. vendor lock-in), saj bi ob morebitni zamenjavi ponudnika tovrstne storitve izgubil.

2.2.3 Programska oprema kot storitev

Nivo programska oprema kot storitev (angl. software as a service, SaaS) pomeni, da celoten razvoj, vzdrževanje in poganjanje aplikacije preidejo v domeno ponudnika. Tako uporabnik le uporablja ponujeno aplikacijo in zanjo plačuje. Uporabnik tako priskrbi le podatke in poslovne procese, vse ostalo je v domeni ponudnika. Primeri tovrstnih storitev so Office 365, Gmail in drugi.

3 Deljena skrb za varnost

Na podlagi podane klasifikacije oblačnih storitev sledi, da so obveznosti ponudnika in uporabnika storitve odvisne od ponujenega namestitvenega in storitvenega modela. Denimo, pri predstavljenih štirih namestitvenih in treh storitvenih modelih lahko konstruiramo 12 konfiguracij: vse od infrastrukture kot storitve na javnem oblaku, do programske opreme kot storitve na zasebnem. Obveznosti ponudnika in uporabnika oblačnih storitev so pri teh kombinacijah različne.

Enako lahko trdimo za obveznosti zagotavljanja varnostnih storitev: ponudnik in uporabnik vsak zagotavljata varnostne storitve skladno z namestitvenim in storitvenim modelom, čemur pravimo **deljena skrb za varnost** (angl. shared security responsibility) [3]. Običajno omenjenih 12 kombinacij zložimo v štiri na način kot podaja Slika 1: bolj kot razmejitev med javni, zasebni, hibridni ali skupnostni oblak je pomembno ali uporabnik tudi nastopa v vlogi ponudnika storitve in ima tako tudi (lokalen) nadzor nad računskimi viri ali ne.

Le s takšnim dogovorom o deljeni skrbi za varnost je mogoče zagotavljati varnostne storitve. A podatki kažejo, da je takšna razmejitev slabo razumljena: raziskava ugotavlja, da je le 43 % anketiranih strokovnjakov, ki zasedajo vodilna mesta v službah za informatikov, v celoti pravilno podalo razmejitev deljene odgovornosti pri ponudbi infrastrukture kot storitve [4].

4 Tveganja v oblaku

V tem razdelku najprej opredelimo varnostne grožnje, zatem pojasnimo, kako se iz groženj izpeljejo tveganja, in na koncu predstavimo ter analiziramo odgovornosti pri najbolj pogostih.

4.1 Grožnje

Pod grožnjo razumemo vsakršno okoliščino, ki lahko povzroči škodo računalniškem sistemu. V splošnem to pomeni ohromitev varnostnih storitev, od katerih so najpomembnejše zaupnost, celovitost in razpoložljivost, pogosto pa med njih uvrščamo še neovrgljivost, overjanje, avtorizacijo in nadzor dostopa.

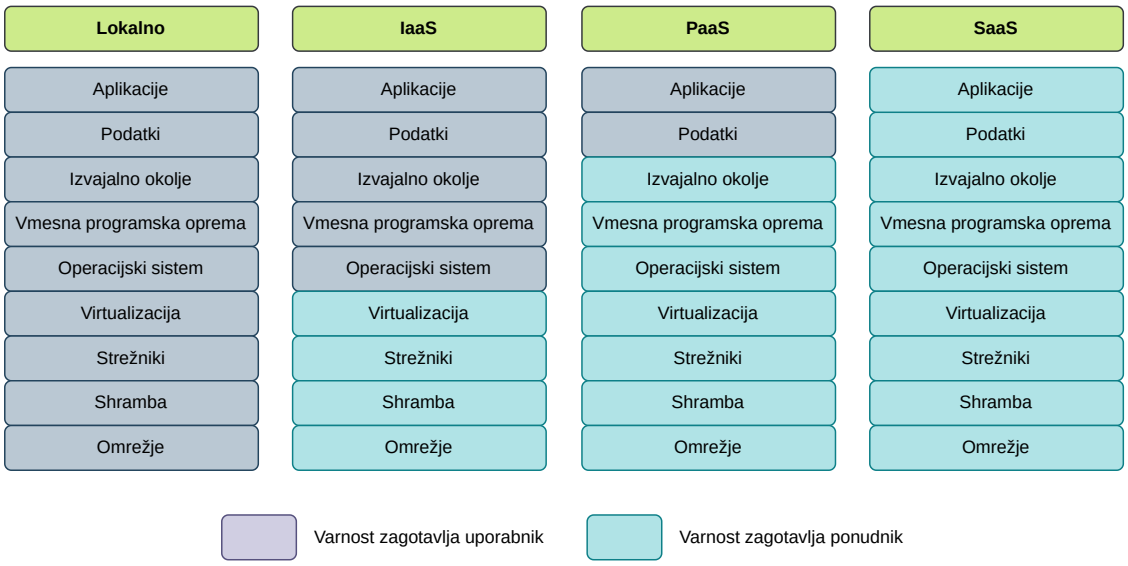
Pri varnostni obravnavi je pomembno, da so grožnje identificirane sistematično. Pogosto si pri tem pomagamo z modeli za identifikacijo groženj, kot je denimo model STRIDE [5], ali pa jih skušamo identificirati na podlagi preteklih varnostnih incidentov in izkušenj.

4.2 Tveganja

Vsaki identificirani grožnji nato pripišemo *stopnjo resnosti*, imenovano tveganje. Tveganje za posamezno grožnjo pogosto izračunano kot kombinacijo verjetnosti, da se grožnja uresniči, in negativnega učinka, ki ga tako uresničenje prinese [6]. Razmerje je podano v enačbi 1, kjer člen $P(g)$ podaja verjetnost, člen $I(g)$ pa negativni učinek.

$$R(g) = P(g) \cdot I(g) \tag{1}$$

Pri analizi tveganj je potrebno oba člena oceniti. Običajno verjetnost nastopa grožnje ocenimo na podlagi dveh komponent: **vektorja napada** ter **ranljivosti sistema**. Vektor napada podaja način, kako se napad (ali grožnja) uresniči, zato ga ocenimo kot kombinacijo zmožnosti potencialnih napadalcev in zahtevnosti izvedbe napada. Denimo, finančno dobro podprti napadalci lahko izvedejo



Slika 1: Deljena skrb za varnost podaja razmejitev odgovornosti za zagotavljanje varnostnih storitev med uporabnikom in ponudnikom storitve; povzeto po [1].

kompleksnejše napade kot nekdo, ki deluje samostojno. Ranljivost sistema pa ocenimo na podlagi pogostosti in zaznavnosti ranljivosti, ki jih mora napadalec za uspešno izvedbo napada izkoristi. Po drugi strani pa je ocena učinka napada organizacijsko pogojena. Zato pri splošni obravnavi tveganj ocenimo le tehnični učinek napada tj. kaj napadalec doseže, npr. razkrije ali uniči podatke, ne pa kakšno poslovno škodo s tem povzroči. Slednje je namreč odvisno od posamezne organizacije.

4.3 Primeri seznamov tveganj

Ko grožnjam pripišemo tveganja, jih lahko rangiramo in s tem določimo prioriteto obravnave: grožnje, ki predstavljajo večja tveganja morajo biti naslovljena prioritetno. Tako v nadaljevanju podajamo tri sezname groženj, urejene po tveganjih, med leti 2019 in 2022. Pri vsaki grožnji označimo, koga bremeni, da jo naslovi oz. po čigavi krivdi lahko nastane: P – ponudnik, U – uporabnik, O – Oba. Oznaka je podana na podlagi podrobnega opisa grožnje v primarnem viru vsakega seznama.

4.3.1 CISCO Cloud Top 10 Risks

Prvi seznam je iz leta 2019, ki ga je v svojem poročilu izdal CISCO [7] ter identificira naslednjih deset groženj kot takih z največjim tveganjem.

1. (O) Odgovornost in razpolaganje s podatki.
2. (U) Federacija uporabniških identitet.
3. (P) Pravni vidiki in regulativna skladnost.
4. (P) Skrb za neprekinjeno poslovanje in odpornost.
5. (P) Uporabniška zasebnost in sekundarna uporaba podatkov.
6. (O) Integracija storitev in podatkov.
7. (P) Večnajemniška in fizična varnost.
8. (U) Analiza incidentov in digitalna forenzika.
9. (P) Varnost infrastrukture.
10. (U) Razkritje testnih okolij.

4.3.2 OWASP Cloud-Native Application Security Top 10

Naslednji seznam je iz leta 2021 in izdan s strani organizacije Open Wordlwide Application Security Project (OWASP) [7].

1. (U) Nevarne nastavitve storitev, vsebnikov in orkestracij.
2. (O) Dovzetnost na napade z vrivanjem.
3. (U) Pomanjkljivo overjanje in avtorizacija.
4. (U) Cevovod CI/CD (angl. continuous integration/continuous deployment) in napake oskrbovalne verige programske opreme.
5. (U) Nezavarovana shramba tajnih vrednosti.
6. (O) Permisivne in nezadostne omrežne politike.
7. (O) Uporaba komponent z znanimi ranljivostmi.
8. (U) Neskrbno ravnanje z viri
9. (U) Nezadostne omejitve računskih virov.
10. (O) Neučinkovito spremljanje in beleženje.

4.3.3 CSA Top Threats to Cloud Computing

Zadnji seznam je iz leta 2022 in prihaja s strani zveze Cloud Security Alliance [8] ter podaja seznam enajstih groženj z največjim tveganjem.

1. (U) Pomanjkljivo upravljanje identitet, poverilnic, dostopa in ključev.
2. (U) Nezavarovani uporabniški in programski vmesniki API.
3. (U) Napačne nastavitve storitev in nezadosten nadzor nad spremembami.
4. (U) Odsotnost varnostne arhitekture in strategije za prehod v oblak.
5. (U) Odsotnost varnih praks pri razvoju programske opreme.
6. (O) Uporaba nevarnih knjižnic.
7. (O) Sistemske ranljivosti.
8. (O) Nenamerno razkritje podatkov v oblaku.

9. (U) Napačne nastavitve in izraba funkcij serverless in vsebniških bremen.
10. (O) Organiziran kriminal, napadalci in skupine APT (angl. advanced persistent threats).
11. (O) Kraja podatkov iz oblačne shrambe.

4.4 Diskusija

Tabela 1 povzema tveganja, ki bremenijo ponudnike in uporabnike v posameznih letih. V oklepaju sta v vsaki celici navedena še relativni delež ter mediana ranga tveganj, ki odpadejo nanju. (V primerih, ko je tveganje označeno kot dolžnost obeh, ga štejemo dvojno, zato vsota deležev v posameznem letu presega 100 %.) Denimo, leta 2019 je izmed 10 tveganj 7 takih, ki bremenijo ponudnika, kar znaša 70 %. Rangi omenjenih tveganj so 1, 3, 4, 5, 6, 7 in 9, kar nanese mediano rangov 5.

Tabela 1: Število, delež in mediana rangov tveganj s predstavljenih seznamov, ki bremenijo ponudnika in uporabnika oblačnih storitev.

Leto	Breme ponudnika	Breme uporabnika
2019	7 (70 %; 5)	5 (50 %; 6)
2021	4 (40 %; 6.5)	10 (100 %; 5.5)
2022	5 (45 %; 8)	11 (100 %; 6)

Analiza kaže, da v zadnjem času prihaja do premika. Videti je, kako čedalje bolj prednjačijo tveganja, ki bremenijo uporabnike, medtem ko se tveganja, ki bremenijo ponudnike, zmanjšujejo – tako v številnosti kot v pomembnosti. Denimo delež tveganj, ki bremenijo ponudnike, se je od leta 2019 do 2022 znižal s 70 % na 45 %, delež tveganj, ki bremenijo uporabnike, pa se je povečal s 50 % na 100 %. Podobno je tudi z resnostjo tveganj: tveganja, ki bremenijo ponudnike, so postala manj izrazita (mediana rangov se je zvišala s 5 na 8), medtem ko mediana rangov za uporabniška tveganja vztraja na 6.

Gotovih razlogov za omenjeno dinamiko ne poznamo, navajamo pa dva dejavnika, ki lahko delno pojasnita nastale razmere. Prvič, področje računalništva v oblaku je danes standardizirano [1] in v veliko vidikih tudi regulirano, npr. [9]. Posledično so ponudniki izboljšali kakovost svojih storitev, vključno z varnostnimi vidiki. Svoje je naredil še trg, kjer se ponudniki z nezadostnim nivojem varnostnih storitev niso obdržali, npr. [10]. Drugič, število uporabnikov oblačnih storitev je zadnjih nekaj let v porastu [8]. Neizogibno to vključuje tudi priliv manj veščih uporabnikov, kar veča možnost varnostnih incidentov, posebej takih, ki bremenijo uporabnike. Slednje je razumljivo, saj je uporaba oblačnih storitev pogosto drugačna od uporabe lokalne infrastrukture in zahteva dodatna znanja, ki jih marsikateri novi uporabnik nima, čeprav je morda vešč dela na lokalni infrastrukturi.

Nazadnje še omenimo, da je naša analiza omejena. Osredotočena je zgolj na največja tveganja—imamo tri sezname 10 tveganj—a vseh tveganj je več. Čeprav danes prednjačijo tveganja, ki bremenijo uporabnike, to ne pomeni, da tveganja za ponudnike ni: le manj izrazita so, zato so s tovrstnih "naj 10" seznamov tudi izpadla.

5 Zaključek

V prispevku smo povzeli za varnost relevantne vidike računalništva v oblaku, opisali koncept deljene skrbi za varnost med ponudnikom in uporabnikom ter nato analizirali pojavnost najbolj pogostih tveganj. Rezultati kažejo, da se je glavnina tveganj od leta 2019 do 2022 premaknila s strani ponudnikov na stran uporabnikov oblačnih storitev. To nakazuje potrebo po dodatnih raziskavah in, če se izkaže potreba, po razvoju novih storitev, s katerimi bi ponudniki pomagali uporabnikom omenjena tveganja nasloviti.

Literatura

[1] Peter Mell and Tim Grance. The NIST Definition of Cloud Computing. Technical Report NIST Special Publication (SP) 800-145, National Institute of Standards and Technology, September 2011.

[2] Hamed Tabrizchi and Marjan Kuchaki Rafsanjani. A survey on security challenges in cloud computing: Issues, threats, and solutions. *The Journal of Supercomputing*, 76(12):9493–9532, December 2020.

[3] Oracle and KPMG. Demystifying the cloud shared responsibility security model. Technical report, 2020.

[4] Oracle and KPMG. Cloud Threat Report 2020. Technical report, 2020.

[5] Nataliya Shevchenko, Timothy A Chick, Paige O'Riordan, Thomas Patrick Scanlon, and Carol Woody. Threat Modeling: A Summary of Available Methods. Technical report, Carnegie Mellon University Software Engineering Institute, Pittsburgh, USA, 2018.

[6] Joint Task Force Transformation Initiative. Guide for Conducting Risk Assessments. Technical Report NIST Special Publication (SP) 800-30 Rev. 1, National Institute of Standards and Technology, September 2012.

[7] Open Worldwide Application Security Project. OWASP Cloud-Native Application Security Top 10 | OWASP Foundation. https://owasp.org/www-project-cloud-native-application-security-top-10/, 2021.

[8] Cloud Security Alliance. Top Threats to Cloud Computing: Pandemic Eleven. Technical report, 2022.

[9] General Data Protection Regulation (GDPR) – Official Legal Text. https://gdpr-info.eu/.

[10] Cyber Attack On 'Code Spaces' Puts Hosting Service Out of Business. https://thehackernews.com/2014/06/cyber-attack-on-code-spaces-puts.html.