

# ALI JE KAJ TRDEN VAŠ OBLAK? HOW STRONG IS YOUR CLOUD?!



GORAZD BOŽIČ,  
ARNES

I/ The title is a paraphrase of a children's game "How strong is your bridge?" where a line of children (the train) passes under the hands of two players (the bridge).

## POVZETEK

Storitve v oblaku pridobivajo na veljavi in omogočajo enostavno in cenovno ugodno implementacijo storitev za organizacijo. Izvoz podatkov in aplikacij v oblak pa ima nedvomno tudi varnostni vidik, ki ga običajno spregledamo. Smo še lastnik svojih podatkov in kaj narediti, če se oblak naenkrat razblini?

KLJUČNE BESEDE: OBLAK, VARNOST, ZANESLJIVOST, ZASEBNOST

## ABSTRACT

Cloud computing is gaining in popularity due to the ease of use, scalability and economics. Outsourcing our data and applications undoubtedly has a clear security component, which is often overlooked. Are we still true owners of our data and what can we do if the cloud suddenly dissipates?

KEY WORDS: CLOUD, SECURITY, RELIABILITY, PRIVACY

## UVOD

Enostavnost in dostopnost storitev v oblaku je dober razlog, da organizacije pričenjajo z uporabo teh storitev za različne namene. Kot ponavadi pa se kot zakasnela ali odri-njena misel pojavi vprašanje nadzora nad podatki in njihovo varnostjo. Z najemom oblaknih storitev podatke izrinemo iz našega (bolj ali manj) varnega okolja, kjer lahko z različnimi postopki in metodami poskrbimo za večnivojsko varovanje podatkov. Nujno je, da ponudnik storitev v oblaku prevzame del odgovornosti, ki se nanaša na zaščito podatkov in varen dostop do njih. Del njegove odgovornosti pa je odvisen od nivoja na oblaku, najmanj pri IaaS storitvah in največ pri SaaS.

## POMISLEKI IN MOREBITNE PASTI

Poleg tega problema, da lahko zgradimo pravo trdnjavo na svojem lokalnem omrežju, nato pa vse podatke izvozimo v oblak, se trenutno kot morda največji problem kaže preveč enostavna avtentikacija. Z ukradenim geslom (ali drugim avtentikacijskim sred-stvom) lahko napadalec naenkrat pride do širokega nabora storitev v oblaku. Oblačne storitve zaenkrat še ne ponujajo bolj strukturiranega nadzora dostopa, preko katerega bi lahko opredelili več nivojev storitev in jih zaščitili z dodatnimi mehanizmi.

Oblaki delujejo vsak zase in ne obstajajo še standardi za oblačne storitve, kar je razumljivo, saj vsak ponudnik ponuja svojo različico in tudi privablja s prednostmi svoje rešitve. Po drugi strani pa za organizacijo to pomeni "lock-in" na enega ponudnika oziroma velike probleme pri migraciji z enega ponudnika na drugega. Ta neprožnost pa je še hujša, kadar ponudnik preneha s svojo dejavnostjo. Ali so sedanji preveliki, da bi propadli? Če pa bodo, ali bo kdo drug prevzel njihovo ponudbo, ali pa se bo naš oblak razpršil?

S premikom naše storitve v oblak bomo običajno zamenjali tudi pravno jurisdikcijo, pod katero sodijo naši podatki. Tudi ponudniki se tega zavedajo in Microsoft recimo navaja situacijo, kjer je njihov podatkovni center lociran na Irskem, njegove kapacitete pa uporabljajo stranke iz Nemčije. Oboje v EU boste rekli in torej ni problema? Ne čisto: Irska ima 24-mesečni rok hrambe prometnih podatkov, Nemčija pa 6-mesečnega.

## PREDNOSTI RAČUNALNIŠTVA V OBLAKU

Oblak pa ponuja tudi nekaj prednosti, tudi varnostnih. Enotno upravljanje z nadgraj-dnjami in filtriranjem prometa in enostavno jačanje virtualnih strojev. Virtualizacija

običajno pomeni tudi možnost izdelave posnetkov stanja, kar lahko izkoristimo ob incidentih kot kopijo za forenzični pregled.

### ZAKLJUČEK

Očitno je, da oblak ponuja udoben način nudenja storitev. Nekaj varnostnih pomislekov obstaja, a si jih lahko z ustrezno opredelitvijo v pogodbi olajšamo. Direktor evropske agencije za informacijsko varnost ENISA, Udo Helmbrecht, je v priporočilih o uporabi oblachnega računalništva zato svetoval: "Javne oblachne storitve ponujajo visok nivo dostopnosti in cenovne učinkovitosti. Vendar pa bi se uporaba morala trenutno omejiti na neobčutljive in nekritične aplikacije v kontekstu dobro definirane strategije vpeljave in z jasno izhodno strategijo." Predvsem ta izhodna strategija je nekaj, kar si ne smemo odmisлити ali odriniti v nedefinirano prihodnost.

#### VIRI

1. Daniele Catteddu: Security and Resilience in Governmental Clouds, ENISA Report  
<http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/>
2. Cloud Computing Risk Assessment, ENISA Report  
<http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment>