Akademija tehničko-umetničkih strukovnih studija Beograd

Odsek Visoka škola za informacione i komunikacione tehnologije

**Cloud Sigurnost - AWS**

Bezbednost informacionih sistema

Natalija Vugdelija

Ilija Krstić 155/21

Đorđe Knežević 255/22

10.10.2023. Beograd

Table of Contents

[SHARED RESPONSIBILITY MODEL 3](#__RefHeading___Toc2367_1971068212)

[Opis 3](#__RefHeading___Toc2369_1971068212)

[Podela odgovornosti 3](#__RefHeading___Toc2375_1971068212)

[Primeri podele odgovornosti 4](#__RefHeading___Toc2377_1971068212)

[EC 2 (IaaS) 4](#__RefHeading___Toc2379_1971068212)

[Elastic Beanstalk (PaaS) 4](#__RefHeading___Toc136_2588892014)

[Workmail (SaaS) 4](#__RefHeading___Toc136_2588892014_Copy_1)

[AWS SECURITY BEST PRACTICES 5](#__RefHeading___Toc2367_1971068212_Copy_1)

[Opis 5](#__RefHeading___Toc2369_1971068212_Copy_1)

[Korišćenje root naloga 5](#__RefHeading___Toc2369_1971068212_Copy_2)

[Princip najmanjih privilegija 5](#__RefHeading___Toc2369_1971068212_Copy_3)

[SLIKE 6](#__RefHeading___Toc1383_2526964257)

[LITERATURA 7](#__RefHeading___Toc1385_2526964257)

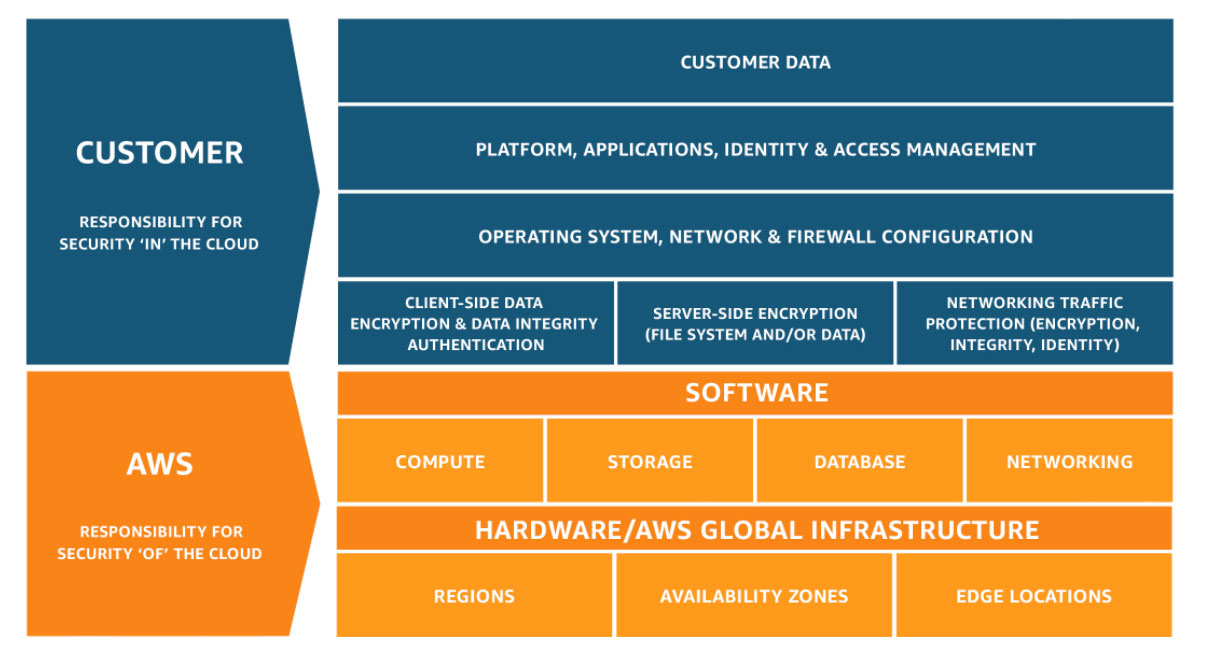
# SHARED RESPONSIBILITY MODEL

## Opis

Shared responsibility model je model po kojem se deli odgovornost za sigurnost (eng responsibility) između provajdera cloud usluga, u našem primeru amazona, i korisnika njihovih usluga i servisa.

Kako nije moguće da je više strana apsolutno odgovorna za sigurnost jedne stvari, odgovornosti se dele na manje delove, a nad delovima se stranama dodeljuje apsolutna odgovornost.

Amazon delove koji su rezultat podele grupišu kao sigurnost clouda (eng security of the cloud) i sigurnost u cloudu (eng security in the cloud) i preuzima odgovornost za prvu grupu i korisnicima predaje odgovornost za drugu[1].

Slika 1 - Opširna podela odgovornosti

## Podela odgovornosti

Podela odgovorosti često zavisi od specifičnog servisa o kome se radi, ali, najosnovije, cloud provider je odgovoran za zaštitu infrastrukture servisa koje nudi, čineći hardware, software, umrežavanje i objekte kod kojih se ovi servisi izvršavaju.

Odgovornost uveliko zavisi od vrste cloud servisa, od kojih postoje tri glavna[2].

Software as a service (SaaS) je model u kom provider pruža aplikaciju u cloudu korisniku za korišćenje, u ovakvom modelu korisnik preuzima najmanji mogući deo odgovornosti[2].

Platform as a service (PaaS) je model u kome se platforme mogu otkupiti od provajdera i koristiti za razvoj, hostovanje i upravljanje aplikacijama, u ovom modelu provider je odgovoran za hardware i software na kojem korisnici pokreću aplikacije, a korisnici su odgovorni za sigurnost aplikacija koje postavljaju na platformu[2].

Infrastructure as a service (IaaS) je model u kome provider pruža računarske kapacitete, tj komputacione resurse, korisniku, a on je odgovoran za sve što se na njima desi, samim tim, odgovoran je za operativni sistem i sve što dalje radi na njemu[2].

Minimalno, bez obzira na model, korisnik je uvek odgovoran za sigurnost podataka, kontrolu pristupa resursima i zakonitost sadržaja.

## Primeri podele odgovornosti

### EC 2 (IaaS)

Elastic Cloud Container je servis koji pruža amazon i koji prati IaaS model cloud servisa.

Amazon pruža razne vrste instanci koje predstavljaju komputacione resurse, optimizovane za različite namene, u formi virtualnih mašina.

Instance su hostovane na fizičkim mašinama, a podelu na virtualne mašine vrši hypervisor[3], sigurnost fizičkih mašina i potpuna razdvojenost između instanci su odgovornost providera.

Jedna instanca se inicijalizuje sa operativnim sistemom po izboru korisnika i od tada sve ostaje na korisniku.

### Elastic Beanstalk (PaaS)

Elastic beanstalk pruža mogućnost olakšanog pokretanja aplikacija na cloudu koji od korisnika zahteva samo otpremanje koda aplikacije koju korisnik želi da pokrene.

Amazon preuzima odgovornost za bezbednost hardware-a i software-a na kome se aplikacije pokreću, a korisnik za bezbednost aplikacija koje pokreće.

Elastic beanstalk takođe može pomoći sa dostupnošću aplikacija pokrenutih na njemu zato što nudi i automatsko skaliranje resursa aplikacija po uviđenoj potrebi, što takođe može smanjiti troškove kada potreba za resursima manja[4].

Ovaj servis takođe pri skaliranju resursa može koristiti više zona dostupnosti (eng availability zones), što osigurava dostupnost aplikacije čak i pri pretnjama koje bi mogle da onesposebe jednu[4].

### Workmail (SaaS)

Workmail nudi privatan mejl servis potpuno podešen od strane amazona.

Amazon preuzima odgovornost za bezbednost hardware-a i software-a koji omogućavaju ovaj servis, a korisniku ostaje odgovornost o podacima, kontroli pristupa, i zakonitosti sadržaja i podataka[5].

# AWS SECURITY BEST PRACTICES

## Opis

U ovom poglavlju ćemo u kratko proći nekoliko najboljih praksa (eng best practice) kada se radi o bezbednosti na AWS cloudu.

## Korišćenje root naloga

Amazon strogo preporučuje da se root nalog ne koristi za svakodnevne zadatke, već da se koristi za izvršavanje samo onih zadataka koje samo root nalog može da izvrši, a da se za sve ostale potrebe napravi i koristi administrativni korisnik[6].

Preporučen je visok nivo pažnje pri radu i zaštiti root naloga, te korišćenje unikatnih šifara i multifaktorske autentikacije[6].

## Princip najmanjih privilegija

Princip najmanjih privilegija, ili na engleskom “least privilege principle” je princip po kojem se korisnicima daju samo one privilegije bez kojih oni ne bi mogli da izvrše svoje dužnosti i ni jednu privilegiju više od tih[7].

Praćenjem ovog principa se uspešno možemo zaštititi od pristupa podacima ili sistemima od strane korisnika za kojeg ne nameravamo da njima ima pristup, smanjujemo rizik u slučaju kompromizovanja korisnika i smanjujemo mogućnost slučajnih grešaka.

Bitno je da pri praćenju ovog principa pažljivo procenimo kojem korisniku su koje privilegije potrebne kako ih ne bi sprečili u izvršavanju njihovih dužnosti, dok im istovremeno ne bi omogućili nenameren pristup.

# SLIKE

(1) Amazon, dostupno na https://aws.amazon.com/compliance/shared-responsibility-model/

# LITERATURA

[1] Amazon – Shared responsibility model.

**Dostupno** na <https://aws.amazon.com/compliance/shared-responsibility-model/>\

[2] Crowdstrike – **Shared Responsibility Model.**

**Dostupno na** https://www.crowdstrike.com/cybersecurity-101/cloud-security/shared-responsibility-model/

**[3] Amazon – What is a hypervisor?**

**Dostupno na** https://aws.amazon.com/what-is/hypervisor/

**[4] Amazon – Elastic Beanstalk features.**

**Dostupno na** https://aws.amazon.com/elasticbeanstalk/details/

**[5] Amazon – Workmail.**

**Dostupno na** https://aws.amazon.com/workmail/

**[6] Amazon -** **Root user best practices for your AWS account**

**Dostupno na https://docs.aws.amazon.com/IAM/latest/UserGuide/root-user-best-practices.html**

**[7] Wikipedia – Principle of least privilege**

**Dostupno na https://en.wikipedia.org/wiki/Principle\_of\_least\_privilege**