Model pretnji mikroservisnog sistema

Dat je link ka prikazu svih dijagrama sa slika (tok podataka i slike za pretnje 1, 2, 3 i 4):

https://app.diagrams.net/#G1ymY-3fPAoh_wA9MosmJXcaWwGDPa6qaj#%7B%22pageId%22%3A%22nYxKL-OTTD4OA9O75eEJ%22%7D

Tokovi podataka analiziranog modula

Analiziran modul predstavlja mikroservisnu aplikaciju za podršku rada distribuirane banke. Aplikacija pruža sledeće funkcionalnosti:

-kreiranje novih računa

-dodavanje i povlačenje sredstava sa računa

-prikazivanje podataka o računima

-kreiranje novih korisnika

-prikazivanje transakcija korisnicima na osnovu računa -prikazivanje transakcija na osnovu parametara kao što su iznos i datum

Softver se sastoji od:

-**Serverske aplikacije** izgrađene u **ASP.NET Core**-u

-**Account, Customer i Transaction mikroservisa** izgrađenih u **ASP.NET Core**-u

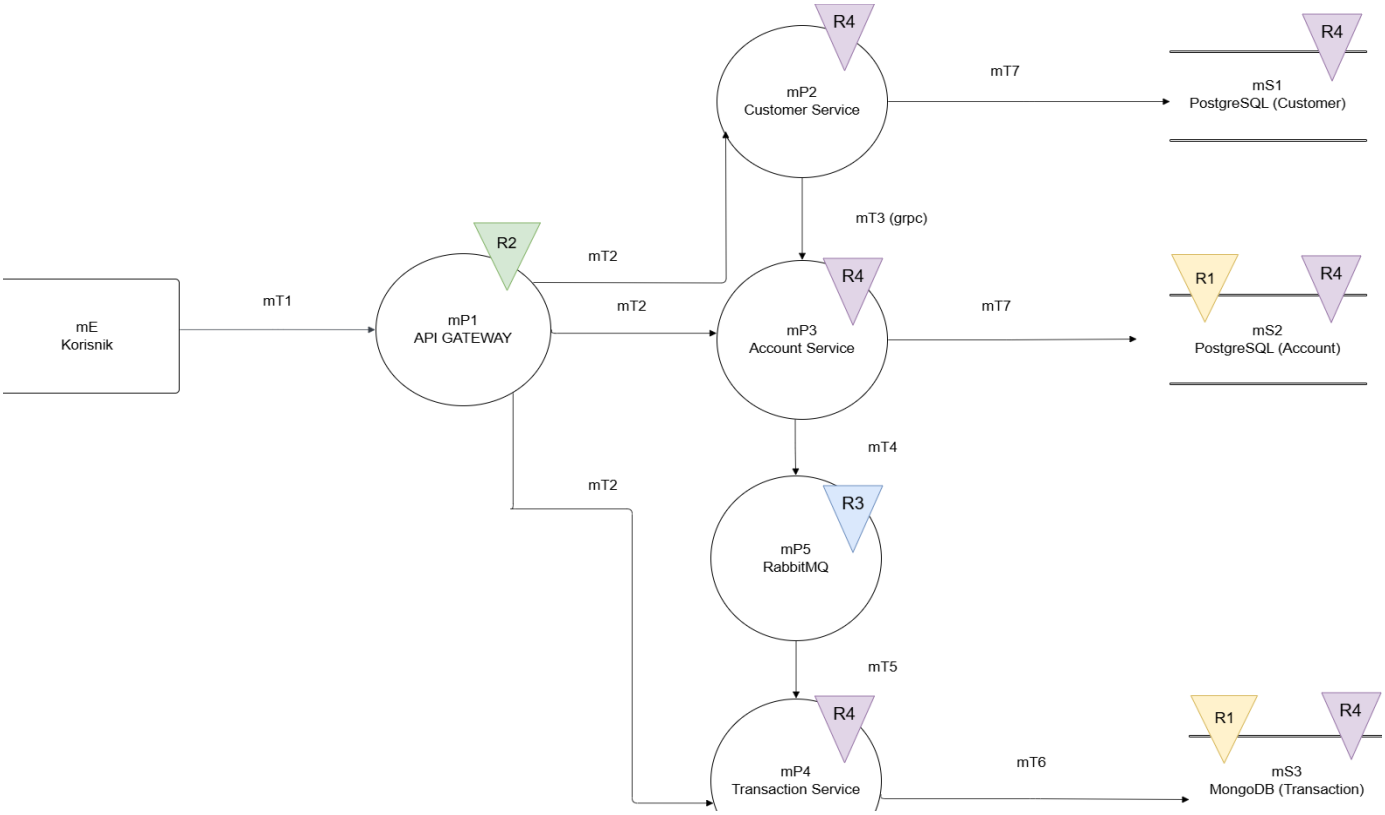
-**API Gateway**-a (Ocelot) za centralizovano rukovanje zahtevima

-**RabbitMQ** za asinhronu komunikaciju i obradu događaja između mikroservisa

-**PostgreSQL i MongoDB baze podataka:** PostgreSQL se koristi za čuvanje korisničkih podataka i računa, dok MongoDB čuva podatke o transakcijama.

-**Docker**- svi mikroservisi su pakovani u Docker kontejnerima

-**gRPC** - Koristi se za brzu i efikasnu komunikaciju između servisa



Tokovi podataka analiziranog modula

Resursi i pretnje visokog nivoa

U nastavku definišemo resurse sistema i pretnji visokog nivoa za svaki resurs.

R1. Podaci o računima	**Neovlašćeno ažuriranje , manipulacija i brisanje podataka o računima korisnika, što dovodi do finansijskih gubitaka korisnika ili banke kao i gubitka poverenja korisnika.**
R2. Konfiguracija API Gateway-a	**Neovlašćena manipulacija konfiguracijom API Gateway-a, što može dovesti do neovlašćenog pristupa, ometanja usluga ili curenja podataka.**

R3. RabbitMQ	Denial of Service (DoS) na RabbitMQ što dovodi do pada posrednika poruka (message broker-a) ili nemogućnosti odgovora
R4. Docker	Pristup host sistemu kroz docker kontejner

Analiza pretnje visokog nivoa - pretnje niskog nivoa, napadi i bezbednosne kontrole

1. Neovlašćeno ažuriranje i manipulacija podacima o računima korisnika

1. Manipulacija podacima u bazi podataka (Database Tampering)
   1.1 - SQL injection u Account mikroservisu
   1.2 - Eskalacija privilegija u bazi podataka
2. Interceptovanje i manipulacija podacima u inter-servisnoj komunikaciji
   2.1 - Uklanjanje HTTPS enkripcije između dva servisa i preusmeravanje na HTTP - SSL striping
   2.2 - Preusmeravanje saobraćaja između mikroservisa na napadačev server - DNS spoofing
3. Manipulacija porukama u sistemu za razmenu poruka
   3.1 - Neovlašćeno slanje malicioznih poruka u sistem preko RabbitMQ sistema (Unauthorized Message Publishing)
   3.2 - Presretanje i ponovno slanje poruka (Replay attack)
4. Manipulacija transakcijama u Transaction mikroservisu
   4.1 - Code injection u Transaction mikroservisu
   4.2 - Race condition u obradi transakcija

Bezbednosne kontrole za napade:

1.1 - Zaštita od SQL injekcija
  1.1.1 - Koristiti parametarske upite za sve SQL operacije
  1.1.2 - Striktna validacija i sanitizacija unosa
1.2 - Kontrola pristupa i nadzor aktivnosti u bazi podataka
  1.2.1 - Princip najmanjih privilegija (PoLP)

1.2.2 - Praćenje i revizija aktivnosti ka bazi podataka (logovanje svih upita prema bazi i redovno analiziranje zapisa)

2.1 - Ojačavanje enkripcije i autentifikacije između servisa

2.1.1 - Korišćenje mutual TLS (mTLS) za proveru identiteta obe strane

2.1.2 - HSTS (HTTP Strict Transport Security) - aktivirati HSTS zaglavlja

2.2 - Zaštita od preusmeravanja saobraćaja prema napadačevim serverima

2.2.1 - DNSSEC (DNS Security Extensions)

2.2.2 - Validacija TLS sertifikata kako bi se otkrila preusmeravanja

3.1 - Zaštita od neovlašćenog slanja poruka u sistemu za razmenu poruka

3.1.1 - API ključevi ili sertifikati za verifikaciju identiteta

3.1.2 - Ograničenje pristupa RabbitMQ-a

3.2 - Oprez kod presretanja i ponovnog slanja poruka

3.2.1 - Korišćenje jedinstvenih identifikatora poruka

3.2.2 - Korišćenje vremenskih oznaka poruka

4.1 - Zaštita od injekcija koda

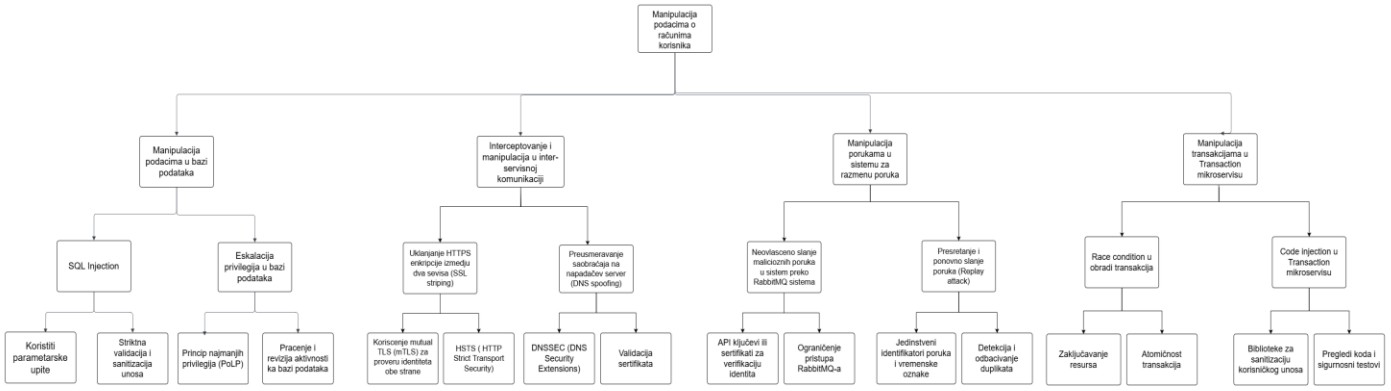
4.1.1 - Korišćenje biblioteka za sanitizaciju korisničkog unosa

4.1.2 - Redovne revizije koda i testiranje ranjivosti

4.2 - Prevencija od konkurentnog pristupa i race condition-a

4.2.1 - Zaključavanje resursa na nivou transakcije

4.2.2 - Implementacija verzionisanja podataka



Stablo za pretnju 1 koje sumira pretnje niskog nivoa, napade i bezbednosne kontrole.

2. Neovlašćena manipulacija konfiguracijom API Gateway-a

1. Neovlašćen pristup konfiguraciji Gateway-a
    1.1 - Kompromitovanje administratorskih kredencijala
    1.2 - Eksploatacija slabih autentifikacionih mehanizama
2. Manipulacija sigurnosnim pravilima
    2.1 - Onemogućavanje zahteva za autentifikaciju
    2.2 - Opuštanje parametara throttling-a ili rate-limiting-a
3. Eksploatacija ranjivosti u plugin-ovima ili ekstenzijama
    3.1 - Eksploatacija zastarelih pluginova
    3.2 - Maliciozni pluginovi koje napadač postavlja
4. Manipulacija pravilima rutiranja
    4.1 - Preusmeravanje saobraćaja na maliciozne servere
    4.2 - Onemogućavanje servisa putem pogrešnog rutiranja

Bezbednosne kontrole za napade:

1.1 - Zaštita od kompromitovanja administratorskih kredencijala
1.1.1 - Primena multifaktorske autentifikacije (MFA) za administratorski pristup
1.1.2 - Ograničiti administratorski pristup samo na poznate IP adrese korišćenjem pravila za firewall

1.2 - Zaštita autentifikacionih mehanizama
1.2.1 - Zamena podrazumevanih lozinki jakim i jedinstvenim lozinkama
1.2.2 - Pratiti administratorske prijave i aktivirati obaveštenja za neuobičajene aktivnosti

2.1 - Revizija i praćenje konfiguracije
2.1.1 - Redovno vršiti reviziju i praćenje promena u konfiguraciji Gateway-a
2.1.2 - Implementirati automatsko vraćanje u prethodne verzije u slučaju neovlašćenih izmena

2.2 - Definisanje i praćenje QoS parametara
2.2.1 - Definisati default QoS pravila i primeniti ih pri implementaciji
2.2.2 - Korišćenje alata za monitoring, kao što su Prometheus i Grafana, za detekciju neobičnih obrazaca saobraćaja

3.1 - Ažuriranje i testiranje pluginova i ekstenzija

3.1.1 - Održavati sve pluginove i ekstenzije ažuriranim sa poslednjim verzijama

3.1.2 - Koristiti sandbox okruženje za testiranje novih plugin-ova pre nego što ih implementiramo u produkciji

3.2 - Ograničavanje pristupa i verifikacija ekstenzija

3.2.1 - Ograničiti prava za instalaciju pluginova na samo pouzdane administratore

3.2.2 - Primena digitalnog potpisivanja za potvrdu autentičnosti novih ekstenzija pre instalacije

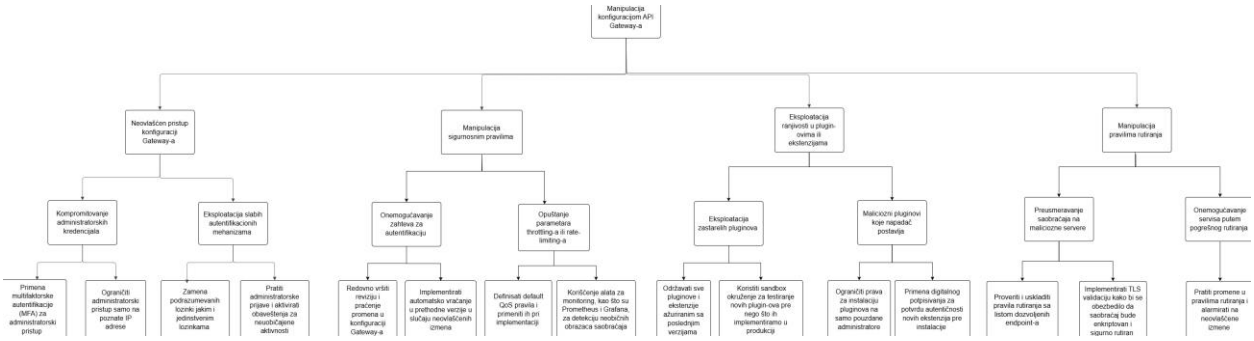
4.1 - Verifikacija pravila rutiranja i zaštita saobraćaja

4.1.1 - Proveriti i uskladiti pravila rutiranja sa listom dozvoljenih endpoint-a

4.1.2 - Implementirati TLS validaciju kako bi se obezbedilo da saobraćaj bude enkriptovan i sigurno rutiran

4.2 - Praćenje i zaštita pravila rutiranja

4.2.1 - Pratiti promene u pravilima rutiranja i alarmirati na neovlašćene izmene



Stablo za pretnju 2 koje sumira pretnje niskog nivoa, napade i bezbednosne kontrole.

3. Denial of Service (DoS) - Napad uskraćivanja usluge RabbitMQ posrednika poruka

1. Message Flooding (Preplavljivanje porukama)
    1.1. Prekomerno slanje poruka od strane proizvođača

1.2. Preopterećenje potrošača slanjem poruka koje zahtevaju kompleksnu obradu

2. Pokretanje operacija koje troše mnogo resursa
    2.1. Učestala deklaracija redova ili razmena (slanjem automatizovanih skripti)
    2.2. Velike operacije na redovima (Queue Purge)
3. Iskorišćavanje neautentifikovanih otvorenih portova
    3.1. Korišćenje skripti ili alata za slanje podataka ka RabbitMQ portovima
    3.2. Neovlašćeni pristup Management Pluginu (moguće pokretati DoS napade sa administrativnim privilegijama)

Bezbednosne kontrole za napade:

1.1.1 - Rate limiting (ograničenje brzine), autentifikacija i autorizacija

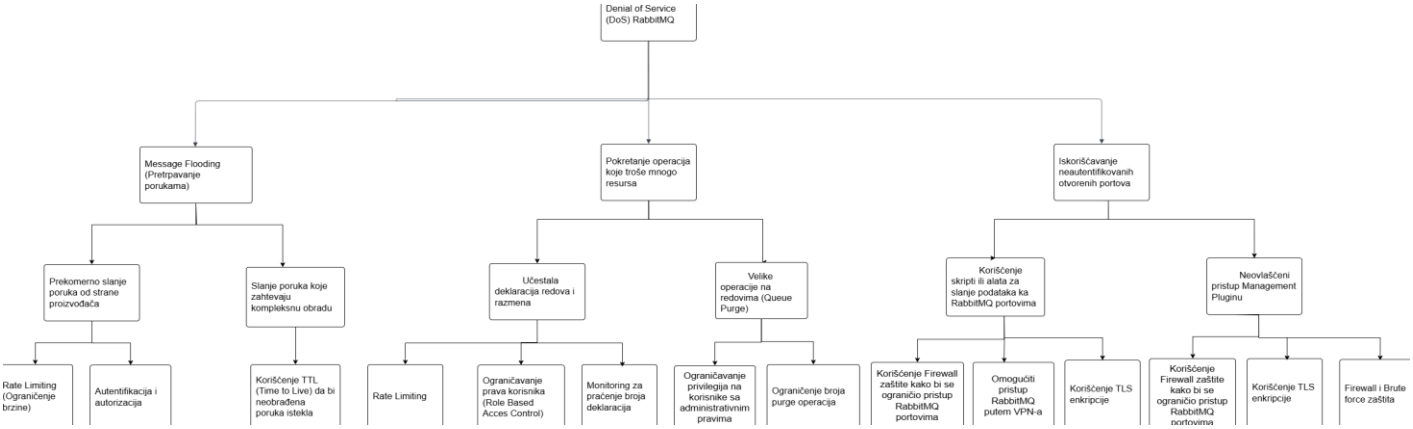
1.1.2. - Korišćenje time-to-live (TTL) da bi neobrađene poruke istekle

2.2.1 - Rate limiting, ograničavanje prava korisnika (Role-Based Access Control), monitoring za praćenje broja deklaracija

2.2.2. - Ograničavanje privilegija na korisnike sa administrativnim pravima, kao i ograničenje na broj purge operacija

3.3.1. - Korišćenje Firewall zaštite kako bi se ograničio pristup RabbitMQ portovima, omogućiti pristup RabbitMQ putem VPN-a, TLS enkripcija

3.3.2. - Korišćenje Firewall zaštite, TLS enkripcije, Rate Limiting i Brute Force zaštita



Stablo za pretnju 3 koje sumira pretnje niskog nivoa, napade i bezbednosne kontrole.

4. Pristup host sistemu kroz docker kontejner

1. Neovlašćeni pristup Docker hostu i kernelu
   1.1 - Kompromitovanje host sistema
   1.2 - Kernel eksploitacije kroz kontejner
2. Zloupotreba resursa Docker kontejnera
   2.1 - DoS napad zbog prekomernog korišćenja resursa
   2.2 - Nepravilno podešeni limiti resursa mogu dovesti do usporavanja sistema
3. Autenticnost slika kontejnera
   3.1 - Pokretanje malicioznih slika iz nepouzdanih izvora
   3.2 - Modifikacija slika tokom preuzimanja
4. Ranljivosti u slikama kontejnera
   4.1 - Postojanje nepoznatih ranjivosti u zastarelim slikama
   4.2 - Korišćenje slika koje sadrže poznate sigurnosne propuste

Bezbednosne kontrole za napade:

1.1.1 - Redovno ažuriranje host sistema i primena sigurnosnih zakrpa.

1.1.2 - Implementacija Mandatory Access Control (Seccomp, AppArmor, SELinux).

1.2.1 - Korišćenje minimalnih, kontejner-centric OS sistema kao što je CoreOS.

1.2.2 - Ograničavanje privilegija na minimum potrebnih za rad kontejnera.

2.1.1 - Konfiguracija cgroups za ograničavanje resursa.

2.1.2 - Implementacija Docker monitoringa i alertiranja.

2.2.1 - Testiranje opterećenja u pre-produkciji.

2.2.2 - Redovno praćenje i optimizacija konfiguracija za resurse.

3.1.1 - Preuzimanje slika samo sa pouzdanih izvora.

3.1.2 - Enforcing Docker Content Trust (DOCKER_CONTENT_TRUST=1).

3.2.1 - Verifikacija potpisa za sve slike pre nego što se preuzmu.

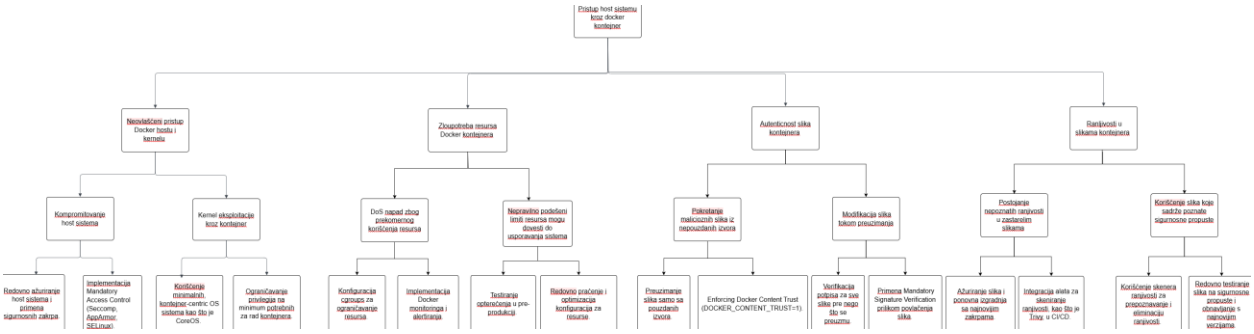
3.2.2 - Primena Mandatory Signature Verification prilikom povlačenja slika.

4.1.1 - Ažuriranje slika i ponovna izgradnja sa najnovijim zakrpama.

4.1.2 - Integracija alata za skeniranje ranjivosti, kao što je Trivy, u CI/CD.

4.2.1 - Korišćenje skenera ranjivosti za prepoznavanje i eliminaciju ranjivosti.

4.2.2 - Redovno testiranje slika na sigurnosne propuste i obnavljanje s najnovijim verzijama.



Stablo za pretnju 4 koje sumira pretnje niskog nivoa, napade i bezbednosne kontrole.