MODEL PRETNJI

Kako bi se obavio proces modelovanja pretnji sistema za plaćanje, uglavnom su se pratili sledeći koraci:

1. identifikovanje resursa od značaja i pristupnih tačaka
2. identifikovanje nivoa poverenja u sistemu
3. kreiranje dijagrama toka podataka
4. identifikovanje pretnji
5. određivanje rizika koji svaka pretnja nosi
6. identifikovanje kontramera koje se primenjuju

Identifikovanje resursa od značaja i pristupnih tačaka

U prvoj fazi identifikuju se resursi od značaja i pristupne tačke sistemu. Identifikovanje resursa se obavlja jer se oni pokušavaju dobaviti prilikom potencijalnog napada. Pristupne tačke jesu interfejsi preko kog je moguće stupiti u interakciju sa sistemom. Preko njih napadač može da naškodi internim resursima od značaja.

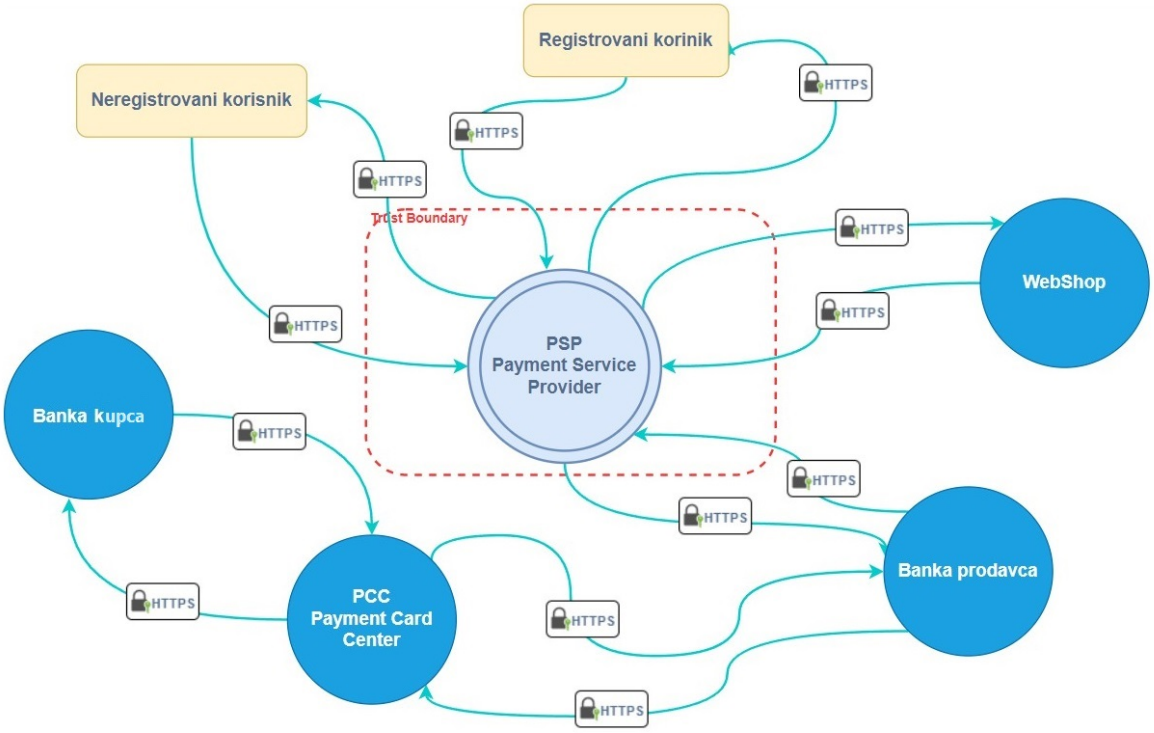
ULAZNE TAČKE			
ID	**NAZIV**	**OPIS**	**NP**
1	Stranica za prijavu i registraciju na sistem	Stranica preko koje je moguće izvršiti login i registraciju na sistem.	N, P
2	Stranice za unos podataka prilikom plaćanja	Forme u koje se unose podaci neophodni za obavljanje transakcija.	N
3	HTTP Port	Komunikacioni kanal za pristup korisnika sistemu.	N, P
4	File sistem	U File sistemu čuvaju se log fajlovi, kao i fajlovi koje servisi proizvode.	
5	Stranice za unos podataka o pretplatama	Forme sa podacima specifičnim za različite vidove plaćanja.	P

RESURSI OD ZNAČAJA		
ID	**NAZIV**	**OPIS**
1	Kredencijali korisnika	Korisničko ime i lozinka registrovanih korisnika
2	Lični podaci korisnika	Podaci o korisniku koje sistem čuva, npr. ime, adresu, broj telefona i tako dalje
3	Podaci vezani za plaćanje	Podaci specifični za različite vidove elektronskog plaćanja: PAN, Security Code, Merchant ID...
4	Baza podataka	Baza koja sadrži sve strukturirane podatke
5	Upravljanje i povezivanje s bazom podataka	Ostvarivanje konekcije i komunikacija s bazom podataka
6	Poslovna logika sistema	Osnovna funkcionalnost našeg sistema
7	Datoteke skladištene na disku	Dokumenti proizvedeni od strane različitih servisa
8	Keystore	Sadrže kriptografske ključeve i sertifikate koji su potrebni za enkripciju i digitalne potpise
9	Log fajlovi	U njima se zapisuju informacije o sistemskim i korisničkim aktivnostima
10	Konfiguracioni fajlovi	Informacije potrebne za ispravno funkcionisanje i konfiguraciju komponenti sistema.

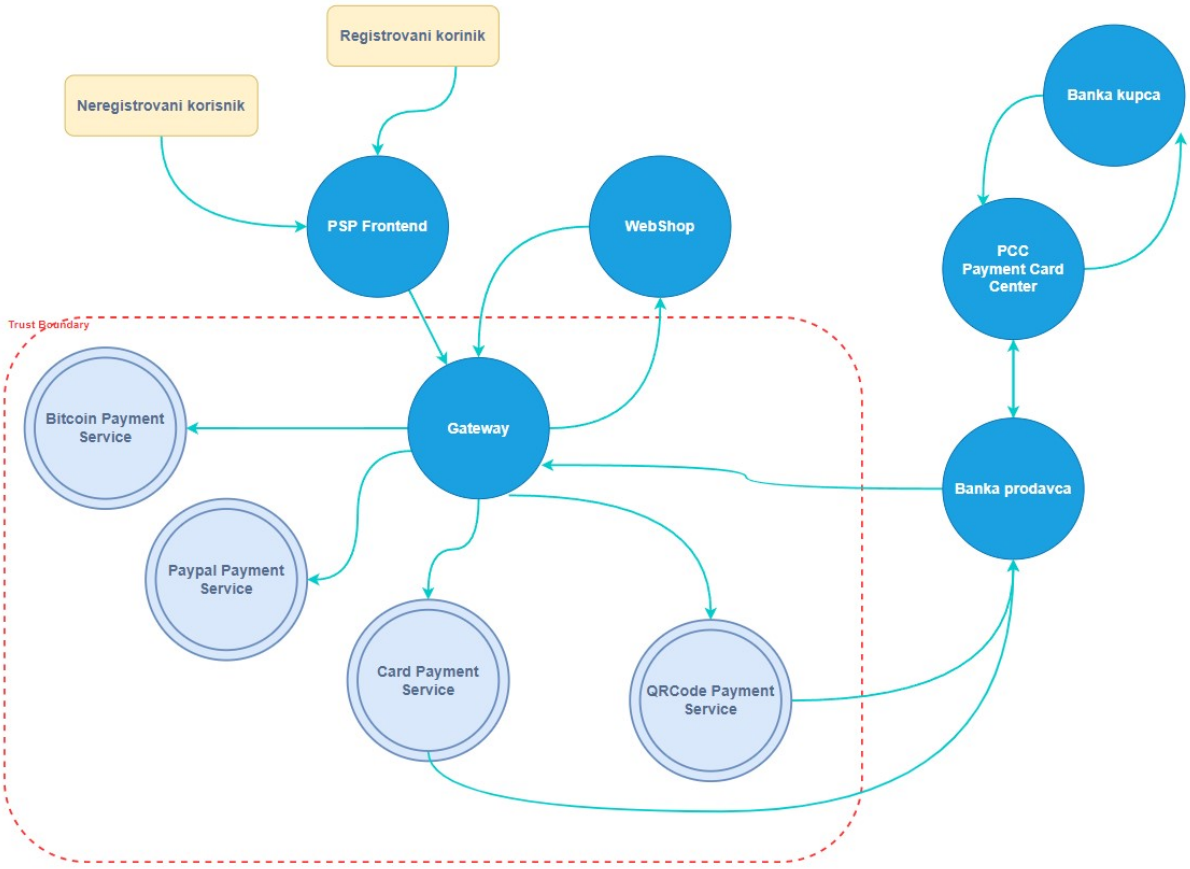
Identifikovanje nivoa poverenja u sistemu

NIVOI POVERENJA		
ID	**NAZIV**	**OPIS**
N	Neregistrovani korisnik	Korisnik koji nema mogućnost prijave na sistem, ali može izvršiti registraciju. Takođe, ima mogućnost unosa podataka za plaćanje (kupac).
P	Registrovani korisnik - prodavac	Korisnik koji je poznat sistemu i ima svoje kredencijale. Omogućava različite pretplate na načine plaćanja za svoju online prodavnicu.

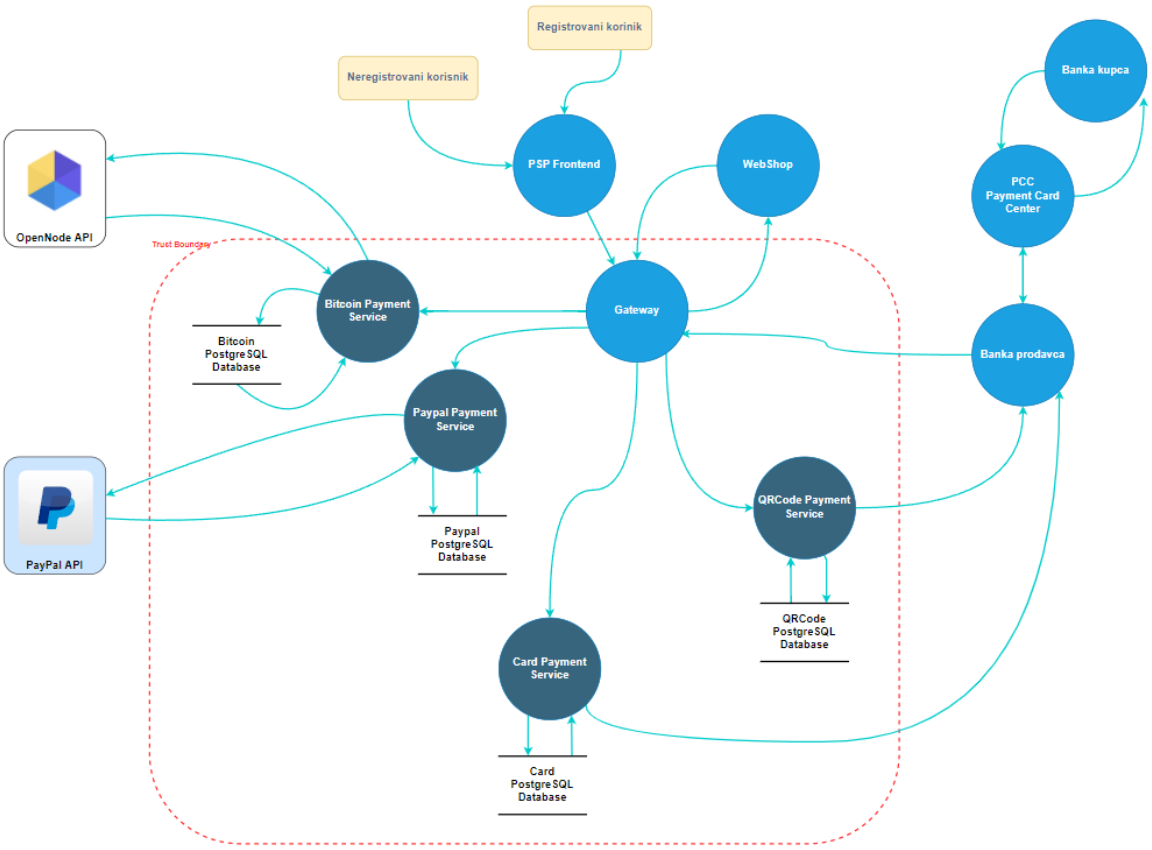
Kreiranje dijagrama toka podataka (DFD)



DFD Dijagram 1 - Konceptualni nivo



DFD Dijagram 2 – Level 1, Payment Service Provider



DFD Dijagram 3 – DFD višeg nivoa, Payment Services

Identifikovanje pretnji

U ovoj fazi identifikujemo i dokumentujemo pretnje koje bi mogle da utiču na naš sistem i kompromituju značajne resurse. Prvi korak u određivanju pretnji je usvajanje kategorizacije pretnji. Kategorizacija pretnji obezbeđuje skup kategorija sa odgovarajućim primerima tako da se pretnje mogu sistematski identifikovati u aplikaciji na struktuiran i ponovljiv način. Za klasifikaciju pretnji koristi se STRIDE metoda koja procenjuje dizajn detalja sistema. STRIDE akronim predstavlja:

1. Spoofing - napadač se predstavlja kao neko drugi
2. Tempering - napadač menja podatke na disku, mreži ili bilo kom mestu u memoriji
3. Repudiation - napadač poriče odgovornost ili samo obavljanje akcije

4. Information disclosure - napadač namerava da pročlta datoteku kojoj nema odobren pristup
5. Denial of Service - ukidanje pristupa servisu/podacima
6. Elevation of Privilege – neautorizovani pristup funkcionalnostima ili resursima sistema

PRETNJE				
ID	PRETNJA	STRIDE KATEGORIJA	UTICAJ NA SISTEM	VEROVATNOĆA
1	Kompromitovanje ličnih podataka korisnika	**SPOOFING**	High	High
2	Gubitak identiteta	**SPOOFING**	Low	Medium
3	Krađa identiteta	**SPOOFING**	High	Medium
4	Lažno predstavljanje	**SPOOFING**	High	Low
5	Kompromitovanje podataka vezanih za plaćanje	**SPOOFING**	High	Medium
6	Neautorizovani pristup mašini putem mreže	**TAMPERING**	High	Low
7	SQL Injection	**INFORMATION DISCLOSURE**	High	High
8	Replay Attack	**INFORMATION DISCLOSURE**	Medium	Medium
9	Data Flow Sniffing	**INFORMATION DISCLOSURE**	High	Medium
10	Narušavanje dostupnosti servisa (DoS napad)	**DENIAL OF SERVICE**	Medium	Low
11	Napad na neporecivost (log fajlovi)	**REPUDIATION**	Low	Low
12	Neautorizovan pristup funkcionalnostima	**ELEVATION OF PRIVILEGE**	High	Low
13	Zaobilazak kontrole pristupa Injection napadom	**ELEVATION OF PRIVILEGE**	Medium	Low
14	CSRF	**ELEVATION OF PRIVILEGE**	Medium	Low

Određivanje rizika koji svaka pretnja nosi

V \ U	LOW	MEDIUM	HIGH
LOW	LOW	LOW	MEDIUM
MEDIUM	LOW	MEDIUM	HIGH
HIGH	MEDIUM	HIGH	HIGH

Tabela za računanje rizika pretnji

Računanje rizika vrši se po tabeli iznad, odnosno množenjem uticaja na sistem i verovatnoće. U tabeli ispod prikazani su procenjeni rizici za svaku od pretnji.

RIZIK = UTICAJ NA SISTEM x VEROVATNOĆA

PRETNJE		
ID	**PRETNJA**	**PROCENJEN RIZIK**
1	Kompromitovanje ličnih podataka korisnika	High
2	Gubitak identiteta	Low
3	Krađa identiteta	High
4	Lažno predstavljanje	Medium
5	Kompromitovanje podataka vezanih za plaćanje	High
6	Neautorizovani pristup mašini putem mreže	Medium
7	SQL Injection	High
8	Replay Attack	Medium
9	Data Flow Sniffing	High
10	Narušavanje dostupnosti servisa (DoS napad)	Low
11	Napad na neporecivost (log fajlovi)	Low
12	Neautorizovan pristup funkcionalnostima	Medium
13	Zaobilazak kontrole pristupa Injection napadom	Low
14	CSRF	Low

Procenjeni rizici

Identifikovanje kontramera koje se primenjuju

1. Implementacija autorizacije i autentifikacije - Implementirana kontrola pristupa resursima i omogućeno dobijanje kredencijala za pristup sistemu, kao i ostalih osetljivih podataka potrebnih za komunikaciju.
2. Zaštita osetljivih podataka u bazi - Primenjeni algoritmi enkripcije nad osetljivim podacima.
3. Logging - Implementirano logovanje/praćenje svih aktivnosti sistema. Čuvaju se informacije o tome gde se izvršila akcija i u koje vreme.
4. Validacija podataka - Svi podaci koji se unose su validirani na serverskoj i klijentskoj strani pre unosa u bazu podataka. Takođe, koriste se parametrizovane naredbe (*Prepared Statement*) za SQL upite.
5. Bezbedna komunikacija - Servisi međusobno komuniciraju putem HTTPS protokola. Svaki od servisa ima svoj sertifikat potreban za međusobno poverenje u razmeni podataka.