PCI DSS standard

Primenjen na aplikacije PSP, First Bank, Second Bank i E-Commerce Platform

I Build and Maintain a Secure Network and Systems

I.I. Install and maintain a firewall configuration to protect cardholder data

Navedeni zahtev izlazi van opsega realizovanog projekta.

I.II. Do not use vendor-supplied defaults for system passwords and other security parameters

Navedeni zahtev izlazi van opsega realizovanog projekta.

II Protect Cardholder Data

II.I. Protect stored cardholder data

Podaci koje sistem skladišti o korisnicima predstavljaju minimum neophodan za uspešnu realizaciju plaćanja. U okviru Payment Service Provider-a, o prodavcima se ne čuvaju direktni podaci o kartici, već samo o njegovom merchant nalogu, koji su neophodni za uspostavljanje uspešne komunikacije sa njegovom bankom. O kupcima se ne prikupljaju nikakvi lični ili osetljivi podaci. Ceo PAN broj se nigde ne prikazuje. U bazi podataka osetljivi podaci (uključujući i PAN broj) su simetrično šifrovani. Ključ za šifrovanje podataka nalazi se u okviru keystore-a koji je zaštićen lozinkom, a i sam entry unutar keystore-a je takođe zaštićen lozinkom.

II.II. Encrypt transmission of cardholder data across open, public networks

Svi podaci koji se šalju preko javnih mreža su šifrovani (koristi se HTTPS (TLS v1.3) protokol). Sve komponente u komunikaciji koriste navedeni protokol. PAN broj se ne šalje ni preko jedne platforme za razmenu poruka.

III Maintain a Vulnerability Management Program

III.I. Protect all systems against malware and regularly update anti-virus software or programs

Navedeni zahtev izlazi van opsega realizovanog projekta.

III.II. Develop and maintain secure systems and applications

Zavisnosti koje postoje u sistemu su skenirane pomoću OWASP dependency-check alata i otkrivene su one koje poseduju ranjivosti. Takve zavisnosti su rangirane po nivou kritičnosti i potrebno je vršiti njihov update. Identifikovane su i ranjivosti samog sistema i njihov nivo rizika je takođe određen kako bi se one mogle rangirati i otklanjati tim redosledom. Prilikom razvoja sistema, praćene su smernice date u OWASP Top 10 listi. Razvojno okruženje odvojeno je od produkcionog tako što je izvršena eksternalizacija konfiguracije i pitanje okruženja svedeno je na prosleđivanje

odgovarajućih environemnt varijabli koje odgovaraju željenom okruženju u datom trenutku.

IV Implement Strong Access Control Measures

IV.I. Restrict access to cardholder data by business need to know

Sistem poseduje role i svaka od njih ima svoje privilegije, korišćen je RBAC. Prava pristupa kontrolišu se u okviru svake komponente i svaka uloga ima minimalan pristup funkcionalnostima, odnosno samo onima koje su mu neophodne kako bi ispunio svoje poslovne ciljeve.

IV.II. Identify and authenticate access to system components

Svaki korisnik ima svoj ID broj koji ga jedinstveno određuje. Kao mehanizam za potvrdu identiteta korisnika upotrebljen je unos korisničkog imena i lozinke. Neophodno je da lozinka zadovolji određena pravila kako bi bila prihvaćena od strane sistema. Ukoliko korisnik tri puta u roku od 10 minuta unese pogrešnu lozinku, njegov nalog biće blokiran na 24 časa. Grupne i generičke lozinke se ne koriste nigde u okviru sistema. Celokupan rad nad bazom podataka vrši se isključivo programski.

IV.III. Restrict physical access to cardholder data

Navedeni zahtev izlazi van opsega realizovanog projekta.

V Regularly Monitor and Test Networks

V.I. Track and monitor all access to network resources and cardholder data

Sistem poseduje mehanizam za logovanje. Logovi se formiraju tako da beleže sve bitne događaje u sistemu, ali je njihova količina istovremeno ograničena kako bi se na jednostavan način mogle izvući korisne informacije. Svaki log poseduje informaciju o datumu i vremenu kada je formiran, sa koje IP adrese je došao zahtev koji je inicirao akciju, koji je URL pogođen i koja je metoda poslatog zahteva. Nakon toga, svaki log sadrži informaciju o jedinstvenom identifikatoru korisnika koji je izvršio određenu akciju, koju akciju je izvršio i nad kojim resursom. Istorija logova čuva se minimum godinu dana, dok je logovima iz prethodna tri meseca moguće odmah pristupiti.

V.II. Regularly test security systems and processes

Izvršeno je white-box penetraciono testiranje sistema, kombinacijom automatskih i manuelnih testova.

VI Maintain an Information Security Policy

VI.I. Maintain a policy that addresses information security for all personnel

Navedeni zahtev izlazi van opsega realizovanog projekta.