PCI DSS standard

PCI DSS (Payment Card Industry Data Security Standard) je standard bezbednosti podataka koji se primenjuje na organizacije koje obrađuju, skladište ili prenose podatke o plaćanjima kreditnim karticama. Cilj ovog standarda je obezbediti sigurnost transakcija i zaštititi osetljive informacije o platnim karticama od neovlašćenog pristupa i zloupotrebe.

PCI DSS je razvijen od strane PCI Security Standards Council-a, koji je formiran od strane vodećih kompanija u industriji plaćanja karticama, kao što su Visa, MasterCard, American Express, Discover i JCB. Standard definiše niz zahteva i mera koje organizacije moraju primeniti kako bi osigurale sigurnost podataka o platnim karticama.

Standard definiše ukupno 12 zahteva, podeljenih u 6 grupa:

Grupa 1: Ustanoviti i održavati sigurnosnu mrežnu infrastrukturu:

1. Instalirati i održavati firewall konfiguraciju zaštite podataka
2. Ne koristiti podrazumevane vrednosti za sistemske lozinke i druge sigurnosne parametre

Grupa 2: Zaštititi podatke o karticama

3. Zaštiti podatke o karticama koji se čuvaju
4. Enkriptovati prenos podataka o karticama putem otvorenih, javnih mreža

Grupa 3: Održavati sigurnosni sistem i aplikacije

5. Koristiti i redovno ažurirati anti-virus softver ili programe za eliminaciju zlonamernih programa
6. Razvijati i održavati sigurne sisteme i aplikacije

Grupa 4: Implementirati i održavati jaku kontrolu pristupa

7. Ograničiti pristup podacima o karticama samo onima koji je neophodan za poslovne funkcije
8. Dodeliti jedinstveni identifikacioni broj (ID) svakom korisniku sa pristupom podacima o karticama

Grupa 5: Praćenje i testiranje sistema

9. Sprovesti redovno praćenje i testiranje mreže
10. Pratiti sve pristupne tačke do podataka o karticama

Grupa 6: Razvijati i održavati sigurnosne politike

11. Implementirati snažne kontrolne mere zaštite informacija
12. Održavati informacionu sigurnost kao ključni deo poslovnih procesa

Implementacija:

Tačke označene crvenom bojom nisu implementirane.

1. Instalirati i održavati firewall konfiguraciju zaštite podataka
2. Ne koristiti podrazumevane vrednosti za sistemske lozinke i druge sigurnosne parametre
3. Zaštiti podatke o karticama koji se čuvaju
   -Osetljive podatke o kartici se čuvaju šifrovano, simetričnom algoritmom (AES).
4. Enkriptovati prenos podataka o karticama putem otvorenih, javnih mreža
5. Koristiti i redovno ažurirati anti-virus softver ili programe za eliminaciju zlonamernih programa
6. Razvijati i održavati sigurne sisteme i aplikacije
   - Obzirom da je korišćen Spring Security, postignut je odredjen nivo bezbednosti upotrebom njegovih funkcionalnosti. Spring Security poseduje mehanizme zaštite od CSRF napada putem generisanja i provere anti-CSRF tokena. Ovo pomaže u sprečavanju napada gde zlonamerni korisnik pokušava da izvrši akciju na ime autorizovanog korisnika. Kroz upotrebu JPA (Java Persistence API), Spring Security može pomoći u prevenciji SQL injection napada tako što obezbeđuje bezbedno formiranje SQL upita. Spring Security pruža mehanizme zaštite od napada na sesiju, uključujući automatsko generisanje novih sesija nakon autentikacije kako bi se izbeglo korišćenje prethodne sesije. Spring Security podržava HTTPS, što pomaže u osiguravanju bezbednog prenosa podataka između klijenta i servera.
7. Ograničiti pristup podacima o karticama samo onima koji je neophodan za poslovne funkcije
8. Dodeliti jedinstveni identifikacioni broj (ID) svakom korisniku sa pristupom podacima o karticama

Svaki korisnik ima svoj jedinstveni ID. Za autentifikaciju se koristi jedinstvena kombinacija email-a i lozinke.

9. Ograničiti fizički pristup podacima o kartici

10. Pratiti sve pristupne tačke do podataka o karticama

- Praćenje je omogućeno kroz logovanje svih akcija.

11. Redovno testirati sigurnosne sisteme

12. Održavati informacionu sigurnost kao ključni deo poslovnih procesa