Primena PCI-DSS-a

Requirement 1.1 - 1.2

Ustanoviti i implementirati Firewall i konfiguracije rutera tako da ograniči pristup komponentama sistema u čijem okruženju se nalaze osetljivi podaci. Dozvoliti samo autorizovani saobraćaj između komponenti sistema. Nadgledati sva podešavanja svakih 6 meseci.

Requirement 1.3

Zabraniti direktan pristup putem interneta komponentama sistema sa osteljivim podacima. Ne odavati privatne IP adrese i informacije o rutiranju neautorizovanim učesicima.

Requirement 1.4

Instalirati firewall software na svim kompjuterskim uređajima.

Requirement 1.5

Dokumentovati sve sigurnosne polise u vezi firewall-a i obavestiti sve učesnike o njima.

Requirement 2.1

Ne koristiti default password i sigurnosne parametre za thrid party software i obrisati sve default naloge.

Requirement 3.1

Poštovati polise za skladištenje, zadržavanje i brisanje podataka. Jedini podaci o platnoj kartici koji se smeju čuvati su: PAN (sa nemogućnošću čitanja njegovog originala), datum isticanja, ime vlasnika kartice, servis kod. Ako ti ne treba, ne čuvaj ga!

Requirement 3.2

Ne čuvati osetljive autentifikacione podatke, čak i ako su enkriptovani. Ne čuvati ceo sadržaj magnetne trake ili čipa sa kartice. Ne čuvati PIN i CVV(CVC).

Requirement 3.3

Kada se prikazuje PAN pikazati najviše prvih 6 i poslednje 4 cifre.

Requirement 3.4

Čuvati PAN tako da se ne može original direktno iščitati. Koristiti strategije: isecanje cifara, one-way hashes, indextokens, strong cryptography.

Requirement 3.5 - 3.6

Dokumentovati i implementirati procedure za zaštitu ključeva koji se koriste za obezbeđivanje skladištanja podataka. Strong cryptography se mora koristiti. Kriptografski ključevi moraju biti dobro zaštićeni(npr. čuvani u HSM-ovima, koristimo keystore koji bi mogao biti korišćen uz HSM). Key encrypring ključevi moraju biti iste jačine kao i data encrypting ključevi na isti način obezbeđeni. Menjate ključeve nakon isteka njigovog perioda važenja. Dokumentovati bezbednosne polise i operacione procedure vezane za skladištenje podataka o platnim karticama i obavestiti sve učesnike o istim.

Requirement 4.1

Koristiti strong cryptography i sigurnosne protokole za prenošenje podataka preko otvorenih javnih mreža - ovo ćemo implementirati korišćenjem HTTPS-a i sertifikata. Trebalo bi koristiti sertifikate koji su proverni od strane autorizacionih tela.

Requirement 4.2

Nikad ne slati nezaštićen PAN krajnjim korisnicima, preko mail-a ili SMS-a.

Requirement 4.3

Obavestiti sve učesnike da čuvamo njihove osteljive podatke.

Requirement 5

Koristiti antivirusne software na svim sistemima i pobrinuti se da oni rade i da ne može svako da ih isključi.

Requirement 6.1

Ustanoviti procese za otkrivanje ranjivosti sistema koristeći respektabilne spoljašnje izvore i rangirati ranjivosti sistema prema stepenu opasnosti po sistem.

Requirement 6.2

Zaštititi sve sistemske komponente i software od opšte poznatih napada.

Requirement 6.3

Omogućiti bezbednu autentifikaciju i prijavu na sistem. Pre puštanja aplikacije u produkciju ukloniti sve naloge koji su korišteni prilikom razvoja i testiranja software-a.

Requirement 6.4

Razgraničiti okruženje i dužnosti za razvoj i produkciju.

Requirement 6.5 - 6.6

Ukazati programerima da treba da se zaštite od opšte poznatih rizika - injection napadi, npr SQL injection, buffer overflows, nesigurna kriptografska skladišta, nesigurna komunikacije između komponenti sistema, loše rukovođenje greškama, XSS, loša kontrola pristupa, CSRF, loše uprvaljanje autentifikacijom i sesijama.

Requirement 7

Dozvoliti pristup podacima samo onim učesnicima kojima su ti podaci neophodni.

Requirement 8.1

Definisati i implementirati polise i procedure za sigurno upravljanje identifikacijom korisnika. Kontrolisati dodavanje, izmenu i brisanje identifikacionih podataka o korisniku. Onemogućiti pristup korisnicima koji su izbačeni iz sistema.

- Ukoliniti ili onemogućiti pristup korisnicima koji su neaktivni više od 90 dana.
- Zaključati korisnčki nalog nakon 6 neuspešnih pokušaja pristupa na bar 30 minuta ili dok administrator sistema ne odključa zaključalog korisnika.
- Ukoliko je korisnik neaktivan više od 15 minuta tražiti da se ponovo autentifikuje (implementirati korišćenjem token expiration time = 15)

Requirement 8.2

Omogućiti sigurnu autentifikaciju korisnicima pomoću lozinke (password-a). Koristiti strong cryptography za kredencijale korisnika prilikom njihovog prenosa i skladištenja.

- Proveriti korisnikov identitet prilikom promene kredencijala - prilikom promene lozinke prvo zatražiti njegovu staru lozinku.
- Lozinka mora imati minimalno 7 karaktera i mora imati i numeričke i alfabetske karaktere.
- Tražiti korisniku promenu lozinke na svakih 90 dana i nova lozinka ne sme da bude ista kao prethodne 4.
- Prilikom prve prijave na sistem tražiti promenu lozinke.

Requirement 8.3

Osigurati remote pristup korišćenjem multi-factor autentifikacije. Za pristup sistemu je potrebno više načina autentifikacije, uz lozinku npr poslati email sa kodom koji korisnik unosi prilikom prijave na sistem.

Requirement 8.4

Dokumentovati o obavestiti sve korisnike o tome kako bi trebalo da izgleda jaka lozinka, kako da što bolje zaštite svoje kredencijale, da ne smeju da koriste lozinke koje su prethodno koristili na sistemu i instrukcije kako da izmene lozinku.

Requirement 8.5

Ne koristiti grupne ID-eve, lozinke i autentifikacione podatke.

Requirement 8.7

Pristup bazamo koje sadrže osteljive podatke je strogo ograničen. Direktan pristup bazama je dostupan samo administratorima baza. Ostali korisnici ne mogu direktno da pristupe podacima (samo putem aplikacija koje koriste).

Requirement 8.8

Definisati i implementirati polise i procedure za sigurno upravljanje identifikacijom korisnika. Kontrolisati dodavanje, izmenu i brisanje identifikacionih podataka o korisniku. Onemogućiti pristup korisnicima koji su izbačeni iz sistema.

Requirement 10.1

Implementirati pregled korisničkih pristupa sistemu - logging.

Requirement 10.2

Pratiti pristup korisnika privatnim podacima. Beležiti sve akcije administratora. Beležiti pristup logovima. Beležiti neuspešne pristupe sistemu. Beležiti brisanje i kreiranje sistemskih objekata (npr. tabele u bazi)

Requirement 10.3

Beležiti minimalno sledeće logove za sve sistemske komponente i svaki događaj:

- identifikacija korisnika
- tipa događaja
- datum i vreme
- uspešno ili neuspešno
- poreklo događaja
- identitet date komponente

Requirement 10.4

Sinhronizovati vreme na svim komponentama.

Requirement 10.5

Obezbediti logove da ne mogu biti direktno izmenjeni. Omogućiti uvid u logove samo onima kojima je to neophodno. Zaštiti logove od neautorizovanih izmena. Backup log fajlova.

Requirement 12.5.4

Administratorsko upravljanje koriničkih naloga, uključujući dodavanje brisanje i modifikaciju - administratorska aplikacija.