Izjava

O INFORMACIONOJ SIGURNOSTI APLIKACIJA/PORTALA

BINFO.ME - BICONSULTING.ME

Očuvanje bezbijednosti BI portala podrazumijeva očuvanje povjerljivosti podataka, integriteta sistema, autentičnosti komunikacije, raspoloživosti resursa, dokazivosti istinitosti, neporecivosti tačnosti i pouzdanosti generalnih načela informacionog sistema.

U cilju definisanja rizika informacionog sistema, čije smanjivanje može imati direktnu posledicu povredivost poslovne politike i narušivanje funkcionalnosti ili bezbijednosti, u predmetnom aplikativnom softveru sa stanovišta bezbijednosti integrisani su osnovni postulati PCI DS standarda koji je prema procjeni projektantskog tima najprihvatljiviji za nivo bezbijednosti aplikacije ovog obima.

Aplikacija odgovora zahtijevima sigurnosti procesiranja zahtjeva klijenata, u djelovima životnog ciklusa zahtjeva u kojima je uključena. Od trenutka kada primi zahtjev, preko obrade, do dostavljanja rezultata procesiranja, aplikacija ispunjava sigurnosne kriterijume PCI DS standarda kao osnove arhitekture zaštite.

Kao alat zaštite u predmetnoj aplikaciji je korišćen jedinstveni softverski mehanizam zaštite (tehnička kontrola zaštite) kao kombinacija komunikacionog modula koji komunicira sa spoljnim entitetima i autentifikacionog servera, autentifikacionog protokola i same autentifikacije.

- *Komunikacioni modul predstavlja element kojim aplikacija komunicira sa spoljnim entitetima (klijentima). Uloga komunikacionog modula je dvostruka. Ovaj modul, odstranjuje elemente komunikacionog protokola iz poruke koja u aplikaciju dolazi od nekog spoljnog entiteta (klijenta). Modul izlaznim porukama iz aplikacije dodjeljuje elemente komunikacionog protokola koji su neophodni za prenos. Komunikacioni modul radi po TCP/IP protokolu. Komunikacioni modul dodjeljuje jedinstveni broj svakoj transakciji na nivou primarnog ključa, što olakšava praćenje aktivnosti na sistemu. Jedinstveni broj transakcije omogućuje lakše istraživanje u slučaju problema. Nakon dodjeljivanja jedinstvenog broja, komunikacioni modul transakcionu poruku prosljeđuje kontrolnom modulu. Komunikacioni modul koji se koristi, u suštini, predstavljaju interface aplikacije sa spoljnim svijetom. Aplikacija preko komunikacionog modula koji funkcioniše na IIS 7.5 platformi komunicira sa Database serverom.*

- *Autentifikacioni server koji se koristu za centralizaciju procesa autentifikacije u računarskoj mreži je Database server.*

- *Autentifikacioni protokol je standardno ugrađen u sam proces razmjene podataka i koriste dodatne mjere zaštite u vidu 256 bitne enkripcije u cilju šifrovanja zaštite povjerljivosti, odnosno mehanizma za zaštitu integriteta i neporecivosti za šta je odgovoran sertifikat o povjervljivosti razmjene podataka unutar aplikacije koji je izdala kompanija Godaddy na čijim je serverima instlirana i sama aplikacija. Kao dokaz tome na svakoj stranici se nalazi kontrolni modul da klijent može u svakome momentu provjeriti validnost samog sertifikata.*

- *Autentifikacija je proces sa kojim korisnik (klijent) dokazuje svoj identitet aplikaciji u vidu 256 bitnog enkripcijskog ključa.*

Verifikaciono-validacioni modul aplikacije verifikuje informacije o ispravnosti upisanog korisničkog imena i lozinke, provjerava prava pristupa korisnika aplikacije i nakon provjere proslijeđuje dalje enkriptovanu poruku.

Cjelokupan bezbijednosni proces je praćen formiranjem Log modula na nivou Database servera koji upisuje sve poruke u log file. Čuvanje poruka je definisano PCI DS standardom. Čuvanje poruka je izuzetno važno zbog istraživanja mogućih žalbi ili problema koji se mogu desiti. Kako je veza IIS 7.5 i Database servera definisana na nivou 1 server - 1 klijent to je izbjegnuta situacija neautorizovanog pristupa predmetnim podacima.

Upotrebom prethodno opisanog sigurnosnog protokola izbjegava se nedostupnost servisa i informacija, neautorizovan pristup sistemu, otkrivanje i korupcija informacija, čime se bezbjednosni rizik kao mogućnost da neke prijetnje iskoriste slabost(i) elemenata informacionog sistema svode na nulu.

Kako su prisutni i mnogobrojni novi oblici prijetnji koje se mogu grupisati u cyber terorizam, obavještajno djelovanje i informaciono ratovanje to svako dublje razmatranje predmetne problematike zalazi u domen poslovne tajne, intelektualnog vlasništva, znanja i informacija čime se potvrđuje jedinstvenost bezbijednosnog protokola koji je integrisan u portale BI Consulting-a.

Srdačno, Vaš BI Consulting Team