UDC: 004.738:336.7 INFO M: str. 19-24

PROCES PRIMENE PCI STANDARDA
THE PROCESS OF APPLYING PCI STANDARDS

Dejan Simić

REZIME: Rad opisuje PCI standarde: PCI PED, PCI PA-DSS i PCI DSS. Osnovna namena ovih standarda je da zaštiti korisnike kartica od neautorizovanog pristupa podacima. Kako se zloupotrebe u sistemima platnih kartica povećavaju, tako i primena PCI standarda postaje obavezna za trgovce, banke i provajdere servisa. Primena PCI standarda doprinosi ostvarenju visokog nivoa zaštite podataka korisnika kartica. Način za implementaciju PCI DSS standarda nije jedinstven. U ovom radu je prikazan pristup zasnovan na prioritetima koji za neke organizacije može imati prednosti u odnosu na druge pristupe.
KLJUČNE REČI: PCI PED, PCI PA-DSS, PCI DSS, pristup zasnovan na prioritetima, zaštita podataka
ABSTRACT: The paper describes PCI standards: PCI PED, PCI PA-DSS, and PCI DSS. The main purpose of these new standards is to protect cardholders against unauthorized data access. As fraud in payment card systems increases, PCI standards compliance becomes mandatory for merchants, banks, and service providers. Applying the PCI standards contributes to achievement of high level of cardholder data security. The way to become PCI DSS compliant is not unique. In this paper prioritized approach is presented, which may have advantages for some organizations.
KEY WORDS: PCI PED, PCI PA-DSS, PCI DSS, prioritized approach, data security

1. UVOD

Pored svih dobrih karakteristika koje sistemi za rad sa platnim karticama imaju osnovni problem je povećani fraud [13, 1]. Kao odgovor na povećani fraud u sistemima koji rade sa platnim karticama nastao je skup PCI (Payment Card Industry) standarda za zaštitu podataka u ovim sistemima. PCI standarde čine: PCI PED (Payment Card Industry PIN Entry Device), PCI PA-DSS (Payment Card Industry Payment Application Data Security Standard) i PCI DSS (Payment Card Industry Data Security Standard). U stvaranju standarda učestvovali su brendovi: Visa International, MasterCard Worldwide, American Express, Discover Financial Services i JCB [10, 11].

Pre nastanka PCI (Payment Card Industry) standarda zaštite svaki brend platnih kartica je imao svoj standard za zaštitu podataka, kao što su na primer: Visa CISP (Cardholder Information Security Program), MasterCard SDP (Site Data Protection Program), American Express DSS (Data Security Standard) i Discover DISC (Discover Information Security Compliance Program).

PCI PED se prvenstveno odnosi na proizvođače hardvera. PCI PA-DSS se odnosi na proizvođače softvera, odnosno softverske proizvode. PCI DSS je obavezujući za sve organizacije koje direktno učestvuju u sistemima za rad sa platnim karticama, tj. organizacije koje procesiraju plaćanja platnim karticama, razvijaju softverske sisteme za rad sa transakcijama koje su generisane platnim karticama, prenose i/ili skladište podatke koji se odnose na podatke sa platnih kartica. Specifikacija PCI DSS standarda obuhvata zahteve za upravljanje zaštitom, procedure, politike zaštite, arhitekturu mreže, dizajn softvera i druge kritične mere zaštite. Ključni aspekt PCI DSS standarda je fokusiranje na zaštitu kartičnih podataka, tako da se oni učine "nečitljivim" primenom mehanizama kriptografije kao što su šifrovanje i heširanje.

2. OPIS PROBLEMA

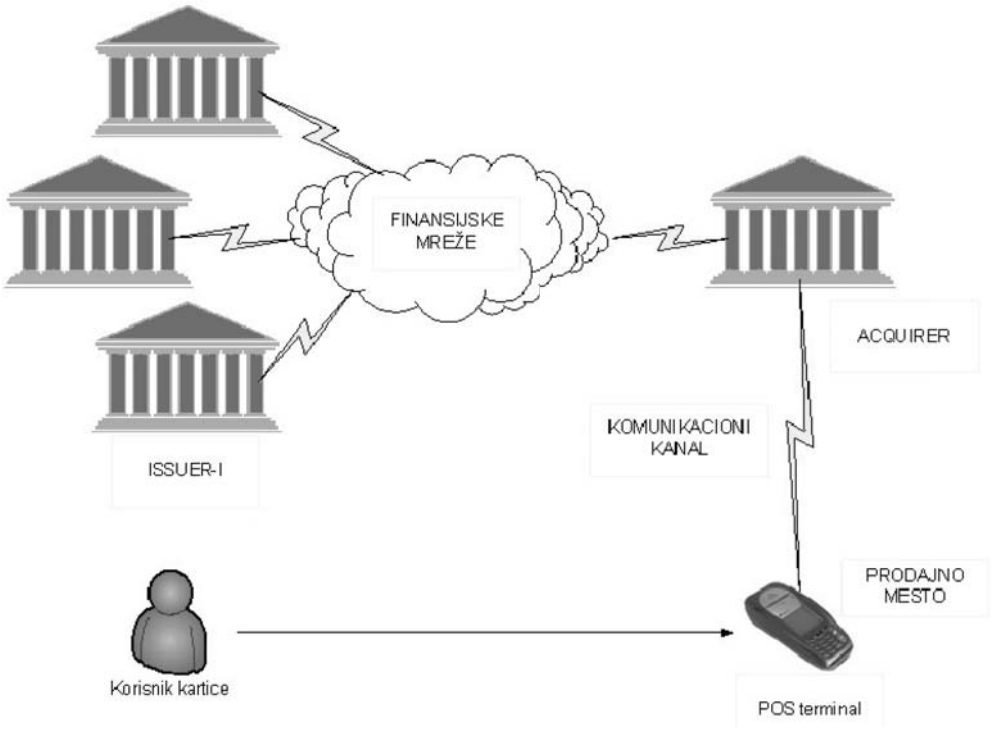
Primeri zloupotreba kod elektronskih sistema plaćanja se mogu klasifikovati u nekoliko sledećih grupa:

- zloupotrebe usled falsifikovanja kartica,
- zloupotrebe na mestu trgovca,
- zloupotrebe u sistemima bez fizičkog prisustva platne kartice,
- zloupotrebe na ATM uređajima,
- zloupotrebe na POS uređajima,
- zloupotrebe na KIOSK uređajima,
- zloupotrebe na sistemima koji rade preko Interneta,
- zloupotrebe prouzrokovane ukradenim i izgubljenim karticama,
- zloupotrebe prouzrokovane krađom identiteta,
- MOTO ("Mail Order Telephone Order") zloupotrebe,
- zloupotrebe u sistemima plaćanja gde se koriste mobilni telefoni itd.

Moguće štete usled nedovoljne zaštite u sistemima platnih kartica su gubitak ugleda, gubitak korisnika kartica i na kraju gubitak profita. Cena zloupotrebe kreditnih platnih kartica dostiže milijardu dolara godišnje. Na primer, u Velikoj Britaniji u 2008. godini finansijska šteta prouzrokovana zloupotrebama platnih kartica iznosila je 609.9 miliona funti [1]. Od toga, 379.7 miliona funti štete je napravljeno u Velikoj Britaniji, a 230.1 miliona funti izvan Velike Britanije.

Povećanje korišćenja platnih kartica na Internetu i neodgovarajuća zaštita podataka može dovesti do kompromitovanja podataka o milionima kartica, što je potvrđeno i u praksi kompromitovanjem podataka o 94 miliona kartica [6].

Povećanje zloupotreba transakcija generisanih platnim karticama je evidentirano i u Australiji. Najčešći tip zloupotreba su 'card not present' transakcije, koje čine 48% ukupne vrednosti zloupotreba napravljenih kreditnim i *charge* karticama [2].



Slika 1. – *Primer arhitekture sistema na koji se odnosi primena PCI standarda*

Rezultati eksperimenata dostupni iz literature [7], pokazuju da je u elektronskim sistemima plaćanja rizik kompromitovanja PIN-a visok čak i kada su u pitanju transakcije napravljene čip karticama.

U Evropi finansijska šteta prouzrokovana zloupotrebama na bankomatima u 2007. godini je povećana sa 306.48 miliona € koliko je iznosila u 2006. god. na 439.01 miliona € [3]. Povećanje je 43%. Najveći deo štete je prouzrokovan skimovanjem kartica na bankomatima.

3. PCI STANDARDI ZAŠTITE

PCI standarde zaštite čine 3 standarda: PCI PED, PCI PA-DSS i PCI DSS. U nastavku teksta dat je sažet opis navedenih standarda. Ispunjenje zahteva PCI standarda se odnosi na sve učesnike u elektronskim sistemima plaćanja kod kojih postoji skladištenje, procesiranje ili prenos podataka o korisnicima platnih kartica. Na primer, PCI standardima su obuhvaćeni sistemi e-trgovine, sistemi za rad sa POS (Point Of Sale) terminalima, sistemi koji koriste MOTO (Mail Order, Telephone Order) transakcije itd. Standardi se odnose na sve komponente sistema, tj. na sve mrežne komponente (firewall-ove, rutere, switch-eve, sisteme za detekciju i prevenciju napada, pristupne tačke za bežični prenos i druge mrežne uređaje), servere i aplikacije. Primer arhitekture sistema na koji se odnosi primena PCI standarda zaštite je dat na slici 1.

3.1 *PCI PED*

PCI PED standard je namenjen proizvođačima uređaja za unos PIN-a [9]. PIN je broj koji ima više cifara i koristi se za proveru autentičnosti korisnika date platne kartice. Ovaj broj ne sme da se zapisuje ni na papiru ni na bilo kom računaru, ni na bilo kom drugom mestu.

PCI PED sadrži zahteve koji se odnose na karakteristike uređaja i na upravljanje uređajima. Postoje logičke i fizičke karakteristike uređaja koje odgovaraju logičkim i fizičkim napadima usmerenim ka dobijanju vrednosti PIN-a. Upravljanje uređajem obuhvata sve faze životnog ciklusa uređaja, kao što su: proizvodnja, kontrola ispravnosti uređaja, skladištenje, transport uređaja, inicijalno punjenje ključa/ključeva, način korišćenja uređaja. Ukoliko se datim uređajem ne upravlja na propisani način, neautorizovane modifikacije mogu dovesti do promena fizičkih i logičkih karakteristika uređaja.

Pored tradicionalnih uređaja kao što su POS terminali, PCI PED obuhvata i uređaje za plaćanje kod kojih nije prisutan trgovac, kao na primer, kioske, mašine za prodaju raznih karata i uređaje za plaćanje na benzinskim pumpama. Takođe, PCI PED obuhvata i HSM (Host Security Modules) uređaje koji se koriste u elektronskoj trgovini, za personalizaciju magnetnih i chip kartica, zaštitu podataka i PIN translaciju.

3.2 *PCI PA-DSS*

PCI PA-DSS je standard namenjen proizvođačima softvera za rad sa platnim karticama, tj. svima koji razvijaju softver za rad u sistemima sa platnim karticama. Ovaj standard je zasnovan na najboljoj praksi aplikacija za rad sa VISA karticama.

PCA PA-DSS sadrži sledećih 14 zahteva:

1. Ne memorisati kompletne podatke sa magnetne staze, kao ni kontrolnu vrednost za validaciju kartice (CVV2, CVC2, CID, CAV2), niti PIN blok podatke.

2. Omogućiti bezbedne lozinke [15].
3. Zaštititi memorisane podatke o korisnicima kartica.
4. Log-irati sve aktivnosti aplikacije (obavezan je žurnal).
5. Razviti zaštićene aplikacije.
6. Zaštititi bežični prenos podataka.
7. Testirati aplikacije radi pronalaženja ranjivosti [8, 18].
8. Omogućiti bezbednu mrežnu implementaciju.
9. Podaci o korisniku kartice ne smeju da se skladište na serveru koji ima pristup Internetu.
10. Omogućiti bezbedno daljinsko ažuriranje softvera.
11. Omogućiti bezbedan daljinski pristup aplikaciji.
12. Kriptovati osetljiv saobraćaj preko javnih mreža.
13. Kriptovati svaki administrativni pristup koji nije preko konzole.
14. Održavati dokumentaciju i programe obuke za korisnike, prodavce i sistem integratore.

3.3 *PCI DSS*

PCI DSS je namenjen trgovcima, bankama i procesorima platnih transakcija [4]. Cilj ovog standarda je da pomogne organizacijama da proaktivno zaštite podatke o plaćanjima svojih korisnika [14].

PCI DSS ima 12 osnovnih zahteva prikazanih u 6 logički povezanih grupa:

GRUPA 1: Instalacija i održavanje bezbedne računarske mreže

Zahtev 1: Instalirati i održavati konfiguraciju firewall-a radi zaštite podataka.

Zahtev 2: Ne koristiti za sistemske lozinke i druge parametre zaštite default, tj. predefinisane vrednosti postavljene od strane proizvođača softvera, odnosno hardvera.

GRUPA 2: Zaštita kartičnih podataka

Zahtev 3: Zaštititi podatke koji se skladište.

Zahtev 4: Kriptovati podatke sa kartice i druge osetljive podatke koji se prenose preko javnih mreža.

GRUPA 3: Održavanje i razvoj programa za upravljanje ranjivostima sistema

Zahtev 5: Koristiti i redovno ažurirati antivirusni softver.

Zahtev 6: Razviti i održavati zaštićene sisteme i aplikacije [8, 16].

GRUPA 4: Implementiranje mera jake kontrole pristupa

Zahtev 7: Ograničiti pristup podacima primenom poslovnog pravila "need-to-know".

Zahtev 8: Dodeliti jedinstveni ID svakoj osobi koja ima pristup računaru.

Zahtev 9: Ograničiti fizički pristup podacima sa kartica.

GRUPA 5: Konstantni nadzor i testiranje mreža

Zahtev 10: Nadgledati i evidentirati sve pristupe mrežnim resursima i podacima sa kartice.

Zahtev 11: Redovno testirati sisteme i procese zaštite.

GRUPA 6: Održavanje i razvijanje politike zaštite informacija

Zahtev 12: Održavati politiku koja adresira zaštitu informacija.

U oktobru 2008. godine je objavljena trenutno važeća verzija 1.2 PCI DSS standarda. Ciljevi ove nove verzije su da se poveća jasnost tehničkih zahteva, da se omogući poboljšana fleksibilnost i da se adresiraju rizici i pretnje, kako novi, tako i oni koji evoluiraju. Bitne razlike u odnosu na prethodnu verziju 1.1 su sledeće:

I) WEP više nije dozvoljen. Bežične mreže koje prenose podatke o korisnicima platnih kartica moraju biti zaštićene korišćenjem enkripcije. WEP protokol se mora zameniti sa Wi-Fi zaštićenim pristupom – WPA (Wi-Fi Protected Access). Počev od 31. marta 2009. godine WEP protokol se ne sme koristiti u novim instalacijama.

II) Svi sistemi za koje postoje *malware* programi, moraju da koriste anti-*malware* softver. Pored korišćenja anti-virusnog softvera obavezno je korišćenje i anti-*spyware* softvera na svim sistemima. Maliciozni softver je definisan tako da uključuje viruse, crve, Trojanske konje i *rootkit*-ove.

III) Za Web aplikacije su obavezni aplikativni *firewall*-ovi [5]. Na taj način se sprečava postojanje *back door* pristupa.

IV) Logovi moraju da se čuvaju bar godinu dana. Zahtev 10.7 propisuje obavezu čuvanja logova na serverima i drugim uređajima bar godinu dana, a za logove do 3 meseca neophodna je trenutna raspoloživost. U verziji 1.1 PCI DSS standarda nije bilo specificirano koliko dugo je obavezno čuvanje logova.

V) Lozinke novih korisnika moraju da se promene na početku rada tih korisnika. Sve pre-instalirane lozinke na ruterima, serverima i ostalim računarima na kojima se koriste podaci o korisnicima platnih kartica moraju se promeniti. Takođe, na osnovu zahteva 8.5 lozinke moraju da sadrže i slova i cifre.

Trenutno ažurna lista servis provajdera za rad sa VISA karticama koji ispunjavaju zahteve PCI DSS standarda je prikazana u [17].

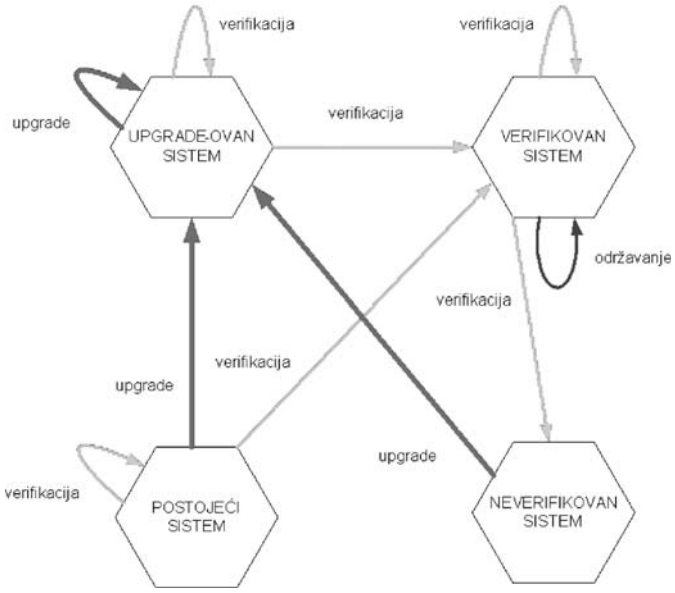
4. ŽIVOTNI CIKLUS PRIMENE PCI STANDARDA

Primena PCI standarda zaštite je kontinuirani iterativni proces. Jedan od načina za ispunjenje zahteva PCI standarda zaštite jeste korišćenje sopstvenih resursa unutar date organizacije, odnosno kompanije, ukoliko je to moguće. Prvi korak je upoznavanje sa sadržajem zahteva PCI standarda zaštite, zatim je potrebno uraditi analizu odstupanja postojećeg načina rada u datoj organizaciji od propisanih zahteva standarda. To su *Pre-Assessment* i *Assessment* aktivnosti. Nakon toga je potrebno napraviti plan aktivnosti za razrešenje identifikovanih odstupanja. Sledeći korak je implementacija na osnovu plana aktivnosti i praćenje realizacije do ispunjenja svih zahteva. Poslednji korak je verifikacija ispunjenosti zahteva PCI standarda pozivanjem spoljašnjih eksperata radi potvrde ispunjenosti svih postavljenih zahteva.

Postoje 3 kategorije usklađenosti:

a) upgrade sistema plaćanja i sistema zaštite prema važećem standardu,
b) verifikacija usklađenosti sistema prema važećem standardu i
c) održavanje sistema prema novim verzijama standarda.

Cena neusklađenosti datog sistema prema važećem standardu lako može biti 20 puta veća od cene uspostavljanja usklađenosti. Na slici 2 su prikazana moguća stanja datog sistema u toku životnog ciklusa primene PCI standarda, tj. u toku procesa uspostavljanja usklađenosti sa zahtevima PCI standarda.



Slika 2. – *Stanja sistema u toku procesa uspostavljanja usklađenosti sa PCI standardima zaštite*

Početno stanje je označeno sa POSTOJEĆI SISTEM. Iz ovog stanja procesom verifikacije može se preći u stanje VERIFIKOVAN SISTEM ukoliko su ispunjeni svi zahtevi PCI standarda, ili ostati u istom stanju ukoliko neki zahtev nije ispunjen. Ukoliko verifikacija nije bila uspešna, procesom upgrade se može preći u stanje sistema koje je označeno UPGRADE-OVAN SISTEM. Proces upgrade obuhvata planiranje, analizu odstupanja produkcionog sistema od standarda, korekciju, testiranje i isporuku korigovanog softvera. Iz stanja UPGRADE-OVAN SISTEM procesom verifikacije se može preći u stanje VERIFIKOVAN SISTEM ukoliko su ispunjeni svi zahtevi PCI standarda, ili ostati u istom stanju ukoliko neki zahtev nije ispunjen. U ovom stanju sistem ostaje sve dok se ne ispune svi zahtevi PCI standarda. U stanju VERIFIKOVAN SISTEM kontinuirano se primenjuje proces održavanja. Nakon isteka važnosti sertifikata koji se dobija ispunjenjem svih zahteva PCI standarda, potrebno je ponoviti proces verifikacije. Uspešnom verifikacijom dati sistem ostaje u stanju VERIFIKOVAN SISTEM, a u suprotnom prelazi u stanje NEVERIFIKOVAN SISTEM.

Vodeće softverske kompanije, kao što je na primer, IBM kreiraju proizvode koji se mogu primeniti u svim fazama životnog ciklusa primene PCI standarda.

U oktobru 2007. godine Visa International je objavila Payment Application Security Mandates – skup obaveznih zahteva, koji su projektovani da pomognu kompanijama u ispunjenju PCI standarda [19]. Navedeni zahtevi se moraju ispuniti do sredine 2010. godine.

Za samostalnu procenu ispunjenosti zahteva PCI standarda postoje formulari SAQ (Self-Assessment Questionaire) v1.2 koji su objavljeni u oktobru 2008. godine i koji su trenutno važeći [12]. Prethodna verzija SAQ formulara v. 1.1 je prestala da važi 31. decembra 2008. godine. SAQ formulari predstavljaju validacioni alat za sve trgovce i provajdere servisa kod kojih nije obavezna procena zaštite podataka (PCI DSS Security Assessment Procedures) na njihovoj lokaciji. Postoje 4 tipa formulara: A, B, C i D. Tip A je namenjen trgovcima koji koriste 'card not present' transakcije (e-trgovina i MOTO transakcije). Tip B je namenjen trgovcima koji koriste imprinter ili dial-up terminale i kod kojih nema skladištenja podataka u elektronskom obliku o korisnicima kartica. Tip C je namenjen trgovcima koji koriste IP terminale ili POS sisteme, koji su povezani na Internet i kod kojih nema mrežnih uređaja i nema skladištenja podataka u elektronskom obliku o korisnicima kartica. Tip D je namenjen svim ostalim trgovcima i provajderima servis usluga. Pored samostalne procene ispunjenosti zahteva PCI standarda za sve trgovce koji su povezani sa Internetom je obavezno kvartalno skeniranje ranjivosti sistema.

4.1 *Izazovi u toku primene PCI standarda*

U toku primene PCI standarda postoji više izazova, kao što su:

– nedostatak zaposlenih za zaštitu sistema,
– poznavanje toka podataka,
– testiranje i održavanje produkcionih sistema,
– zaštita aplikacija,
– cena,
– opseg primene (ograničiti primenu standarda gde je to neophodno)
– firewall-ovi i antivirusni softver,
– minimiziranje skladištenja podataka,
– primena zahteva 5 i 6 PCI DSS standarda na POS sisteme:

Zahtev 5: Koristiti i redovno ažurirati antivirusni softver,

Zahtev 6: Razviti i održavati zaštićene sisteme i aplikacije.

– implementacija,
– kriptovanje uskladištenih podataka,
– log-ovanje i zaštita podataka i
– menjanje i upravljanje ključevima koji se koriste za kriptovanje podataka.

Takođe, u opštem slučaju svaka organizacija ima različitu informaciono-komunikacionu infrastrukturu i različite poslovne procese i na osnovu toga ima i različite izazove u primeni PCI DSS standarda.

4.2 *Moguća rešenja*

Moguća rešenja za primenu PCI standarda, imajući u vidu prethodno navedene izazove koji postoje kod primene PCI standarda, su:

– koristiti sertifikovane aplikacije i hardver,
– angažovati kompaniju koja ima potrebna znanja za stručnu pomoć i verifikaciju ispunjenosti zahteva PCI standarda,
– pratiti promene PCI standarda i produkcione sisteme brzo dovoditi do stanja da budu usaglašeni sa tim promenama,
– izabrati najbolji pristup za primenu PCI standarda,
– pripremiti plan aktivnosti za bilo koji slučaj incidenta na produkcionom sistemu i
– ograničiti opseg primene tamo gde su podaci, gde se podaci skladište, gde se vrši kriptovanje, arhiviranje itd.

5. PRISTUP ZASNOVAN NA PRIORITETIMA

Pristup zasnovan na prioritetima kod primene PCI DSS standarda omogućava sledeće prednosti:

– Rizici se mogu adresirati po redosledu prioriteta,
– Primenjuje se pragmatičan pristup koji omogućava brzu implementaciju,
– Omogućena je podrška finansijskom i operacionom planiranju,
– Omogućeno je praćenje napredovanja implementacije uvođenjem merljivih indikatora,
– Promoviše se konzistentnost između različitih kvalifikovanih osoba koje rade procenu ispunjenosti PCI DSS-a (QSA – Qualified Security Assessors).

Za dobijanje PCI DSS sertifikata svi zahtevi PCI DSS-a moraju biti ispunjeni bez obzira na redosled primene. Pristup zasnovan na prioritetima ne mora biti najbolje i obavezno rešenje za sve organizacije kod kojih je neophodna primena i uvođenje PCI DSS-a. Međutim, pristup zasnovan na prioritetima može imati prednosti kod nekih organizacija. Pristup zasnovan na prioritetima je na primer, podesan za trgovce koji izaberu procenu ispunjenosti zahteva PCI DSS-a na svojoj lokaciji ili koriste SAQ D. Ovaj pristup je takođe podesan i za sve manje organizacije kod kojih postoji nedostatak ili nedovoljan broj zaposlenih za zaštitu sistema.

Tabela 1 – *Opis prioriteta i pridruženih ciljeva kod primene PCI DSS-a*

Prioritet	Ciljevi
1	Ne memorisati osetljive podatke za proveru autentičnosti i limitirati podatke koji se memorišu. Ukoliko se osetljivi podaci za proveru autentičnosti i drugi podaci o korisnicima kartica ne skladište, tada se efekti mogućih zloupotreba značajno redukuju. Prema tome, ukoliko navedeni podaci nisu neophodni ne treba ih skladištiti.
2	Zaštititi granicu mreže, internu mrežu i bežične mreže. Ovaj cilj se odnosi na kontrolu tačaka pristupa kod većine kompromitovanja podataka – tj. odnosi se na mrežu ili tačku pristupa bežičnoj mreži.
3	Zaštititi aplikacije koje rade sa platnim karticama. Ovaj cilj se odnosi na aplikacije, aplikativne procese i aplikativne servere.
4	Nadgledati i kontrolisati pristup internim sistemima. Ovaj cilj se odnosi na dobijanje pitanja ko, šta, kada i kako u kontekstu pristupa mreži i podacima koji se odnose na korisnike platnih kartica.
5	Zaštititi uskladištene podatke o korisnicima platnih kartica. Ovaj cilj se prvenstveno odnosi na organizacije koje zbog svojih poslovnih procesa moraju da skladište podatke o brojevima platnih kartica. Cilj se ostvaruje primenom ključnih mehanizama zaštite uskladištenih podataka.
6	Završiti sve ostale delove standarda i obezbediti da je zaštita primenjena svuda gde je to potrebno. Namena ovog cilja je kompletiranje svih preostalih PCI DSS zahteva i završavanje svih preostalih politika, procedura i procesa potrebnih za zaštitu podataka koji se odnose na korisnike platnih kartica.

Najviši prioritet – prioritet 1 imaju sledeći zahtevi PCI DSS standarda:

1.1.2 Obezbediti dijagrame postojeće mreže sa svim vezama prema podacima korisnika platnih kartica, uključujući bežične mreže.

3.1 Skladištenje podataka o korisnicima platnih kartica svesti na minimum. Razviti politiku zadržavanja i uklanjanja podataka. Ograničiti skladištenje podataka i vreme zadržavanja podataka prema poslovnim pravilima, pravnoj i zakonskoj regulativi, kao što je dokumentovano u politici zadržavanja podataka.

3.2 Ne skladištiti osetljive podatke potrebne za proveru autentičnosti nakon autorizacije (čak ni enkriptovane). Osetljivi podaci potrebni za proveru autentičnosti su dati u zahtevima 3.2.1, 3.2.2 i 3.2.3.

3.2.1 Ne skladištiti kompletne podatke sa bilo koje staze magnetne trake kartice (koja se nalazi na poleđini kartice, unutar čipa ili bilo gde drugde). Ovi podaci se alternativno zovu *full track, track, track 1, track 2* i podaci sa magnetne trake.

3.2.2 Ne skladištiti CVC ili CVV vrednost.

3.2.3 Ne skladištiti PIN vrednosti ili enkriptovan PIN blok.

9.10 Uništiti medijume koji sadrže podatke o korisnicima platnih kartica kada nisu više potrebni za poslovne procese ili pravnu regulativu.

9.10.1 Nakon isteka perioda važnosti štampani materijal iseckati, spaliti ili učini takvim da nije moguće rekonstruisati podatke o korisnicima platnih kartica.

9.10.2 Obezbediti da se podaci o korisnicima platnih kartica na elektronskim medijumima ne mogu oporaviti, odnosno rekonstruisati nakon isteka perioda važnosti.

12.1.1 Adresirati sve PCI DSS zahteve.

Nakon ispunjenja svih ciljeva najvišeg prioriteta, otklonjeni su najveći rizici i tada se prelazi na ispunjenje ciljeva drugog prioriteta. Ovaj postupak se nastavlja sve do ispunjenja svih ciljeva u okviru prioriteta 6. Progres aktivnosti se može vrlo lako pratiti. Prioritet ciljeva je definisan na osnovu dosadašnje prakse u radu elektronskih sistema plaćanja, povratne

sprege od kvalifikovanih QSA-a i forenzičkih istražitelja, kao i na osnovu informacija od savetodavnog tela za PCI standade (PCI SSC Board of Advisors).

6. ZAKLJUČAK

Podaci dostupni iz literature ukazuju na porast zloupotreba platnih transakcija u elektronskim sistemima plaćanja u svim regionima sveta. Kao rezultat nepostojanja opšte prihvaćenog standarda za zaštitu podataka u elektronskim sistemima plaćanja, brendovi platnih kartica American Express, Discover Financial Services, JCB International, MasterCard Worldwide i Visa, Inc. su kreirali PCI (Payment Card Industry) standarde zaštite: PCI PED, PCI PA-DSS i PCI DSS.

Za organizacije koje prenose, skladište ili procesiraju podatke koji se odnose na korisnike platnih kartica trenutno je važeći standard PCI DSS ver. 1.2.

Praksa je pokazala da je na sistemima kod kojih je bilo većih zloupotreba (po broju transakcija i po ukupnoj vrednosti), više od polovine zahteva PCI DSS standarda nije bilo ispunjeno. Na osnovu toga ispunjenje PCI DSS zahteva dobija najviši prioritet.

Postoji više načina za ispunjenje zahteva PCI standarda zaštite. Zajednička karakteristika svih tih načina jeste da su vremenski zahtevni procesi i da se moraju pažljivo planirati, implementirati i kontinuirano održavati. U ovom radu je ukratko prikazan pristup implementacije PCI DSS standarda zasnovan na prioritetima koji može imati prednosti za neke organizacije, kao što su npr. trgovci.

Pored svih dobrih karakteristika koje PCI DSS standard ima u pogledu sveobuhvatnosti i proaktivnog pristupa zaštite sistema, potrebno je naglasiti da on ne obuhvata krajnje korisnike, tako da oni postaju najslabija karika u sistemu zaštite.

LITERATURA

[1] APACS, »Fraud: The Facts 2009", http://www.apacs.org.uk/resources_publications/documents/FraudtheFacts2009.pdf

[2] APCA, "Payment Fraud in Australia", http://www.apca.com.au/Public/apca01_live.nsf/ResourceLookup/Press_Release_Payments_Fraud_Statistics_5.pdf/$File/Press_Release_Payments_Fraud_Statistics_5.pdf, December 2008.

[3] ATMmarketplace, "European ATM skimming jumps 43%", http://www.atmmarketplace.com/article.php?id=9916&na=1, 08 maj 2008.

[4] Bradley Tony (Technical Editor), Burton Jr. James D., Dr. Chuvakin Anton, Elberg Anatoly, Freedman Brian, King David, Paladino Scott, Schooping Paul,"PCI Compliance – Implementing Effective PCI Data Security Standards", *Syngress Publishing, Inc.*, 2007.

[5] Cobb Michael, "PCI compliance and Web applications: Code review or firewalls?", http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1311874,00.html, 08. maj 2008.

[6] Lemos Robert, "Court filings double estimate of TJX breach", *Security Focus*, http://www.securityfocus.com/news/11493, October 2007.

[7] Matyaš Vaclav, Krhovjak Jan, Kumpost Marek, Cvrcek Dan, "Authorizing Card Payments with PINs", *IEEE Computer*, Vol. 41, No. 2, pg. 64-68., February 2008.

[8] Open Web Application Security Project (OWASP), http://www.owasp.org, septembar 2009.

[9] PCI, "PIN Entry Devices", https://www.pcisecuritystandards.org/security_standards/ped/index.shtml, septembar 2009.

[10] PCI DSS, https://www.pcisecuritystandards.org/, septembar 2009.

[11] PCI DSS,Wikipedia, http://en.wikipedia.org/wiki/PCI_DSS, septembar 2009.

[12] PCI Security Standard Council, "Self-Assessment Questionaires", https://www.pcisecuritystandards.org/saq/instructions_dss.shtml, septembar 2009.

[13] Simić Dejan, "Reducing Fraud in Electronic Payment Systems", *Proceedings of the 7th Balkan Conference on Operational Research*, Constanta, Romania, May 2005.

[14] Simić Dejan, "PCI DSS – standard za zaštitu sistema za rad sa platnim karticama«, Predavanje po pozivu, XXIII Naučno-stručni skup, InfoTech 2008, Vrnjačka Banja, 02. - 05. juna 2008.

[15] Stallings William, Brown Lawrie,«Computer Security: Principles and Practice«, *Pearson Education, Inc.*, 2008.

[16] Stanković Srđan, Simić Dejan, "Defense Strategies Against Modern Botnets", IJCSIS (International Journal of Computer Science and Information Security), Vol. 2, No. 1, June 2009.

[17] "VISA List of PCI DSS Compliant Service Providers", http://usa.visa.com/download/merchants/cisp-list-of-pcidss-compliant-service-providers.pdf, septembar 2009.

[18] Van der Linden Maura A.,"Testing Code Security", *Auerbach Publications*, 2007.

[19] Vijayan Jaikumar,"FAQ: What Visa's payment application security mandates mean", *Computer World*, 2007.

Dr Dejan Simić, vanr. profesor FON-a
e-mail: dsimic@fon.bg.ac.rs
Oblasti interesovanja: elektronski sistemi plaćanja, zaštita informacionih sistema