Upravljanje realizacijom projekta uvođenja PCI DSS standarda

Živorad Vasić, Milan Mijalković
VISER, Beograd, Republika Srbija
zvasic@viser.edu.rs, m_milan@viser.edu.rs

Minka Yordanova
Tehnički univerzitet Gabrovo, Bugarska,
mmiordanova@gmail.com

Ilja Stanišević
VIPOS, Valjevo, Republika Srbija
istanisevic@vipos.edu.rs

Dragana Sajfert
doktorant TF "Mihajlo Pupin", Zrenjanin, Republika Srbija
z.saifert@sbb.rs

Sadržaj— **U radu je predstavljen model upravljanja projektom uvođenja PCI DSS (Payment Card Industry – Data Security Standard) po fazama realizacije, uz kratak osvrt na primenu platnih kartica i nužnost uvođenja standarda, kako bi se ostvario osnovni cilj ovog projekta - prilagođavanje inforamacionog sistema zahtevima PCI DSS standarda, usklađivanje poslovanja, izrada, implementacija i verifikacija odgovarajućih procedura i polisa, urađenog posla. Projekat obuhvata poslove opisane u planu kroz 6 faza implementacije, a ne obuhvata poslove van toga, kao što su sertifikacija korišćenog softvera izrađenog od drugih proizvođača.**

Ključne reči - upravljanje projektom, zaštita podataka, platne kartice, PCI DSS.

1. UVOD

Potreba banaka za realizacijom dodatnih kanala pristupa, dovela je do široke upotrebe platnih kartica u bankarskom poslovanju. Široka rasporostranjenost bankomata i POS terminal kao i jednostavan način primene kartica, doveo je do masovne ekspanzije ovakvog načina plaćanja. Zbog osetljivosti same trasansakcije i u cilju zaštite korisničkih podataka, taj period rasta prihvata platnih kartica, pratio je i period definisanja i usaglašavanja raznih bezbednosnih standarda koji propisuju način čuvanja i zaštite podataka koji se koriste tokom realizacije plaćanja putem ovog bankarskog kanala. U poslednje vreme iskristalisao se jedan standard koji je uz podršku kartičarskih šema i kontrolu od strane Payment Security Council-a postao defacto standard za zaštitu osetljivih korisničkih podataka. Cilj ovog rada je da opiše zahteve tog standarda i predstavi projekat uvođenja PCI - DSS standarda [1], [2], [3], [4], [5], [6] uz korišćenje realnih primera iz poslovanja kompanije koja se bavi servisnim aktivnostima vezanim za terminale za prihvat platnih kartica [7].

2. PLATNE KARTICE KAO INSTRUMENT PLAĆANJA

Platne kartice su u poslednje vreme postale veoma uobičajene, kao način plaćanja roba i usluga u Srbiji [8]. U poslednjih 50 godina kreditne, debitne i razne druge vrste platnih kartica su postale pokretač u ekspanziji globalne ekonomije. Povećana mogućnost sprovođenja transakcija na svetskom nivou je donela ekonomski rast u skoro svim delovima sveta.

Izdavanje kreditnih kartica je postao veliki i unosan posao. Ove finansijske institucije generišu prihode na osnovu dogovorenih provizija. Platne kartice danas čine bitan deo naših života, što govori podatak da je u 2011 godini u Srbiji izdato preko šest miliona platnih kartica, dok je na kraju trećeg kvartala 2012 nešto manji, a i broj aktivnih kartica je opao na 44% [9].

3. PCI DSS, DEFINICIJA I ISTORIJA

PCI DSS (Payment Card Industry – Data Security Standard [1], [2], [3], [4], [5], [6]) je sveobuhvatni višestruki standard koji pokriva zahteve za upravljanje bezbednošću, polise, procedure, mrežnu arhitekturu, dizajn softvera, i druge kritične mere zaštite. Ovaj opšti standard ima namenu da pomogne organizacijama da preventivno zaštite podatke o korisnikovim računima.

Payment Card Industry security standards, odnosno bezbednosni standardi, predstavljaju tehničke i operativne propise postavljene od strane PCI Security standard Council (Savet za bezbednosne standarde) u cilju da bi se dodatno zaštitili korisnički podaci. Standardi se odnose na sve entitete koji čuvaju, procesiraju ili prenose podatke o vlasniku platne kartice - sa uputstvima za programere i proizvođače apliakcija i uređaja korišćenih u tim transakcijama. Savet je odgovoran za upravljanje bezbednosnim standardima, dok se usklađivanje sa PCI skupom standarda sprovodi putem članova osnivača ovog Saveta: American Express, Discover Financial Services, JCB International, MasterCard Worldwide i Visa Inc. Kartičarske organizacije poput VISA, MasterCard i drugih, u cilju sprečavanja prevara, (koje za sredstvo imaju podatke sa platnih kartica), kroz istoriju su uvodili i implementirali razne standarde i preporuke za poslovanje sa platnim karticama.

Osetljivi korisnički podaci su oni detalji potrebni za realizaciju kartičarske transakcije koje je potrebno prikupiti od korisnika i poslati kroz mrežu radi autorizacije te transakcije. Prikupljanje podataka može da se obavi na terminalima kao što su EFT POS, ATM, mobilni telefon, ili putem bilo kojeg internet pretraživača. Među osetljive podatke spadaju:

- Ime i prezime korisnika
- Podaci sa platne kartice:

- PVV – PIN verification Value
- CVV - Card verification Value
- Track 2 – gde se nalazi sam broj kartice

- PIN, Personal Identification Number, Lični identifikacioni broj, kojim korisnik autentifikuje transakciju.

Pored nabrojanih, postoje i drugi osetljivi podaci čijom kompromitacijom mogu biti ugrožena novčana sredstva samog vlasnika platne kartice. *PCI je standard predviđen za* zaštitu gore nabrojanih osetljivih korisničkih podataka vlasnika platne kartice - cardholder data (CDU).

Svrha ovog standarda je definisanje načina rada sa platnim karticama, a sve sa ciljem da se smanji mogućnost prevara, time da se pruži poverenje korisniku u takav kanal pristupa bankarskom poslovanju. Korisnikova privatnost mora biti na najvišem nivou, a to se može postići sprečavanjem kompromitovanja podataka. Zbog toga je neophodno dodatno obezbediti okruženje za transakcije tim načinom plaćanja. Da bi se pristupilo obezbeđivanju, primarno je identifikovati potencijalne ranjivosti sistema. Najjednostavniji način za efikasnu beznednosnu kontrolu jeste izbegavanje beleženja podataka sa platnih kartica.

Cilj PCI DSS standarda je proklamovan u sledećih par tačaka:

- Rad sa platnim karticama u cilju smanjenja prevara,
- Obezbeđivanje okruženja za platne transakcije,
- Identifikovanje potencijalnih ranjivosti,
- Pružanje poverenja korisniku,
- Poboljšavanje bezbednosti obavljanja transakcija,
- Zaštita korisnikove privatnosti,
- Sprečavanje kompromitovanja podataka,
- Izbegavanje beleženja podataka sa platnih kartica.

4. TIPOVI PREVARA SA PLATNIM KARTICAMA

Samim tim što platna kartica omogućava pristup novčanim fondovima, oduvek je bila predmet raznih prevara i krađa. Kriminalne aktivnosti su vremenom evoluirale i unapređivale se razvojem tehnologije, tako da sada imamo paralelni razvoj industrije zaštite podataka i industrije koja sa druge strane zakona pokušava neovlašćeno doći do podataka za realizaciju transakcije putem platne kartice. Uz minimalnu opremu moguće je napraviti kopiju platne kartice i sa odgovarajućim PIN-om obaviti transakciju sa tim podacima. Uvođenjem EMV (Europay-Mastercard-Visa) čip kartica te prevare su smanjene, ali pošto i dalje veliki deo kartičarskih mreža nije u potpunosti prešao na EMV, moguće je i dalje vršiti takve prevare [10], [11], [12], [13].

Najgrublje prevare su krađe same kartice i PIN koda, što je lako uočljivo jer kartica više nije u posedu njenog korisnika. Najčešći mehanizam koji se koristi u tu svrhu je lebaneese loop**,** koji se montira unutar čitača i zadržava karticu prilikom njenog ubacivanja u čitač. Kartica se potom lako izvuče, čim se njen vlasnik odmakne od bankomata.

Jedna od najčešćih prevara je nazvana skimming, a ona podrazumeva krađu podataka sa kartice ali ne i same kartice, pa je zbog toga takve prevare i teže pravovremeno uočiti.

Pomoću posebnih sofisticiranih elektronskih uređaja montiranih na čitač kartice, kopiraju se potrebni podaci prilikom ubacivanja kartice u bankomat i automatski šalju bežičnom konekcijom na obližnji laptop prestupnika. Ovakav uređaj najčešće ide u kombinbaciji sa kamerom koja slika trenutak unosa PIN koda, pa na taj način prestupnik saznaje i taj bitan element za transakciju. Ti podaci se kasnije koriste za izradu kopija kartica koje se mogu iskopirati na bilo kojem bankomatu u svetu i podići pare sa računa vlasnika skimovane kartice.

Primera ovakvih i sličnih prevara je mnogo, što samo govori u prilog potrebi da se podigne svest o bezbednosti obavljanja transakcije pomoću platnih kartica i ulaganju u dodatne mehanizme zaštite.

EMV standard predstavlja uvođenje platnih kartica sa implementiranim mikrokontrolerom odnodno chipom od strane vodećih svestskih institucija MasterCard i Visa. Prednost korišćenja kartica sa čipom je znatno povećanje bezbednosti sistema plaćanja. Za proces personalizacije čip kartica kompanija NBS/Ubiq je razvila specializovani kako hardver tako i softver. NBS/Ubiq EMV rešenje podržava i opremu za personalizaciju drugih proizvodjača, kao što su :

- DataCard,
- Mühlbauer,
- CIM,
- Eltron, i drugi.

SIP (System Inteligence, Product), zajedno sa NBS/Ubiq nudi kompletno hardversko i softversko rešenje; od proizvodnje samih čipova za kartice, kartice, opremu za testiranje kartica, opremu za personalizaciju kartica, pakerice kartica, uključujući i štampače za štampanje grafike na karticama i drugu specijalizovanu opremu.

5. SPISAK PCI DSS ZAHTEVA

Na temeljima pozitivnih iskustava zaštite podataka na inforamcionim sistemima kroz dosadašnju istoriju, Payment Security Council je definisao 6 grupa zahteva, sa detaljima opisanim u 12 stavki.

A. Izgraditi i održavati bezbednu mrežu

1: Instalirati i održavati zaštitni zid (firewall) u cilju zaštite podataka o korisnicima kartica.

Prvi od zahteva kreće od definisanja detaljnog mrežnog dijagrama svih konekcija ka osetljivim kartičarskim podacima, gde se propisuje da taj segment mreže treba da bude izolovan od ostatka mreže postavljanjem zaštitnog zida**,** koji treba da restriktivno propušta saobraćaj i to samo onaj koji je detaljno opisan. Firewall polise moraju striktno da propisuju načine propuštanja novih konekcija.

2: Ne koristiti sistemske šifre niti druge bezbednosne parametre koji su predefinisani od strane proizvođača. Drugi zahtev formalizuje način na koji se definišu i menjaju sistemske šifre, kriptuje sav nekonzolni administratovni pristup i propusuju zaštite u cilju neovlašćenog korišćenja privilegovanih naloga.

B. Zaštita podataka o korisnicima kartica

3: Zaštita podataka o korisnicima kartica kreće od toga da se minimizuje svako njihovo čuvanje, a ukoliko poslovne potrebe zahtevaju njihovo čuvanje, da se tada ti podaci maskiraju ili da se kriptuju na sistemu. Čuvanje kripto ključeva koji se koriste u tom slučaju mora da se obavlja prema strikrtnim pravilima.

4: Kriptovati podatake o korisnicima kartica prilikom prenosa preko otvorenih javnih mreža.

U slučaju prenosa kartičarskih podataka kroz komunikacionu mrežu, saobraćaj mora da bude kriptovan korišćenjem SSL/TLS ili IPSEC protokolima. Ni u jednom slučaju nije dozvoljeno elektronsko slanje.

C. Održavati program upravljanja ranjivostima

5: Koristiti i regularno ažurirati bazu antivirus softvera. Operativni sistemi na personalnim računarima moraju biti zaštićeni odgovarajućim anti-virusnim rešenjem koje obezbeđuje detekciju, ukljanjanje i zaštitu od svih poznatih tipova zlonamernog softvera.

6: Razviti i održavati bezbednosne sisteme i aplikacije. Testovi ranjivosti moraju se redovno sprovoditi na celokupnoj mreži, što ima za cilj ranu detekciju problematičnih bezbednosnih propusta i njihovo pravovremeno ukljanjanje. Razvoj softvera mora da poštuje pravila bezbednog kodiranja opisana u dokumentima poput OWASP (Open Web Application Security Project Guide). Okruženje za test i razvoj softvera mora da bude potpuno odvojemo od produkcije, a procedure moraju da propisuju način na koji se softver prebacuje u produkciono okruženje. Sve izmene na produkciji moraju da budu dokumentovane kroz odgovarajuće Change management procedure.

D. Uvesti jake mere kontrole pristupa

7: Ograničiti pristup osetljivim podacima o korisnicima kartica po principu *need-to-know.*

Ukoliko je neophodno čuvati osetljive podatke, pristup njima mora da bude striktno ograničen samo na osobe koje imaju poslovnih razloga da im pristupaju. U tom slučaju potrebno je uvesti jedinstvene identifikacije za takve pristupe i sprovesti centralizovano prijavljivanje svakog od tih pristupa, a isto tako je neophodno evidentirati i sve neuspešne i neovlašćene pristupe takvim sistemima. Polazno podešavanje sistema je eksplicitna zabrana svakog pristupa.

8: Dodeliti jedinstveni identifikator svakoj osobi sa kompjuterskim pristupom mreži.

9: Ograničiti fizički pristup podacima o korisnicima kartica.

Fizički pristup kartičarskim podacima mora biti maksimalno restriktivan. Svaki pristup mora biti autentifikovan jedinstvenim korisničkim imenom i lozinkom i mora biti zabeležen video kamerama i odgovarajućim sistemom za prijavljivanje na mrežu. Zaposleni, ali isto tako i svi posetioci moraju imati jasno istaknute identifikacije koje ih razlikuju. Svi pisani mediji koji čuvaju korisničke podatke moraju biti uništeni na odgovarajućim mašinama - schrederima.

E. Regularno nadgledati i testirati mrežu

10: Pratiti i nadgledati sav pristup mrežnim resursima i osetljivim podacima.

Svi postavljeni bezbednosni sistemi moraju da prolaze redovne kontrole. Interni i eksterni testovi ranjivosti treba da se izvode minimum jednom kvartalano i nakon svake izmene na sistemu. Rezultati testa, zajedno sa IPS/IDS testovima moraju da se čuvaju i daju na uvid oditoru.

11: Regularno testirati bezbednosne sisteme i procese. Sve kompanijske polise moraju detaljno da opišu načine poslovanja koji su usklađeni sa PCI DSS-om. Polise moraju da se redovno proveravaju i unapređuju, a dnevne procedure da ih prate. Odgovorni zaposleni moraju da budu svesni rizika sistema koji su im povereni i da predlažu rešenja. U tom cilju neophodno je sprovoditi njihovu redovnu edukaciju u skladu sa njihovim zaduženjima na sistemu. Za svaki od prepoznatih rizika poslovanja mora da postoji odgovarajući plan u slučaju incidenta i spisak aktivnosti koje se sprovode u tom slučaju.

F. Održavati mere informatičke bezbednosti

12: Održavati i unapređivati mere koje pokrivaju bezbednost podataka.

Usklađivanje sa gore navedenim zahtevima može da se svede u tri glavne celine:

- Sakupljanje i skladištenje**:** Bezbedno sakupljanje i skladištenje na siguran način, svih podataka tako da su dostupni za kasniju anlaizu.
- Izveštavanje**:** Biti u mogućnosti da potvrdite usklađenost na licu mesta ukoliko je to zahtevano tokom audita i da pružite dokaz da su sve kontrole na mestu i služe zaštiti podataka.
- Praćenje i uzbunjivanje: Obezbediti sisteme kao što su automatsko obaveštavanje, da biste pomogli administratorima da konstantno prate pristup i korišćenje podataka. Administratori mogu brzo da reaguju na problem ukoliko su momentalno i na vreme upozoreni o incidentu.

6. POSLEDICE KRŠENJA PCI STANDARDA:

- Finansijske kazne (kazne mogu da idu i do 500.000 $ po jednom prekršaju).
- Pravne posledice (Ukidanje Acquiring statusa, zabrana pristupa kartičarskim mrežama kao što su VISA, MasterCard, Amex).

7. CILJ PROJEKTA

A. Poslovni cilj

Usaglašavanje poslovanja kompanije u skladu sa propisima definisanim kroz PCI DSS. Pored usklađivanja poslovanja i marketinške vrednosti koje ta činjenica nosi, najbitnije jeste kako podizanje bezbednosti čuvanja i obrade osetljivih korisničkih podataka, tako i podizanje bezbednosti inforamcionih sistema koji su uključeni u taj proces i svesti o tome unutar cele kompanije.

B. *Projektni cilj*

Cilj ovog projekta je prilagođavanje inforamacionog sistema zahtevima PCI DSS standarda, usklađivanje poslovanja, izrada i implementacija odgovarajućih procedura i polisa, te verifikacija urađenog posla uz finalnu posetu ovlašćenog PCU oditora.

C. *Sadržaj projekta*

Projekat obuhvata poslove opisane u planu kroz 6 faza implementacije, a ne obuhvata poslove van toga, kao što su sertifikacija softvera koji koristimo izrađenog od drugih vendora.

8. FAZE PROJEKTA UVOĐENJA PCI DSS

I faza: Scoping

Najbitnija faza celog projekta, jer je već sada moguće odrediti same okvire projekta i proceniti koiji delovi sistema unutar kompanije treba da potpadnu pod rigorozna pravila koja donosi PCI DSS standard. Bitno je naglasiti da se PCI DSS bavi samo čuvanjem, prenosom i obradom osetljivih korisničkih podataka, pa je na osnovu te činjenice lako moguće iz samog opsega sertifikacije izbaciti delove poslovanja firme koji ne potpadaju pod tu kategoriju. Ova faza, dakle predstavlja procenu sistema i mreže:

1. Analiza sistema.
2. Scoping izveštaj.

II faza: Pre-compliance Audit

1. Risk Assessment baziran na ISO27001 i BS25999 standardima/metodologijama (uključujući dostavljanje pisanog dokumenta).
2. Self Assessment Questionaire – SAQ, ovo je standardni obrazac koji korisnik popunjava samostalno ili uz pomoć QSA, i koji može da ukaže na dalje smernice u kojem pravcu treba da ide sertifikacija i kojeg obima će da bude.
3. Gap Analysis izveštaj, pomaže kompaniji da uporedi stvarno stanje sa željenim. U suštini odgovara na pitanja "Gde smo sada?" i "Gde želimo da budemo?".
4. Utvrđivanje prioriteta i sastavljanje plana za remedijaciju.

III faza: Remediation, ispravljanje i usaglašavanje svih procesa rada, konfiguracije i arhitekture sistemske i komunikacione:

1. Consalting.
2. Remediation - implementacija fizičkih i logičkih sigurnosnih mera. Pre početka ovih aktivnosti neophodno je napraviti remediation plan, koji kreće od detaljne mreže sistema. Planira se odgovarajuća segmentacija infrastrukturne mreže, a kao rezultat toga je spisak neophodne oprem koju je potrebno dodatno implementirati.
3. Razvoj sigurnosne dokumentacije (polise, procedure i izveštaji po zahtevima PCI standarda). Uobičajeno je da se krene od opštih polisa nastalih kao najbolja iskustva na tom polju, a potom se svaka od njih prilagođava lokalnim okolnostima i integriše sa ostalim mrežnim bezbednosnim polisama.

IV faza: Assessment

1. Penetration test.
2. Vulnerability scanning po zahtevima PCI (ova faza se radi kvartalno u toku posmatrane poslovne godine).
3. Incident response.

V faza: Audit

Ovo je ključni deo projekta kad QSA lično dolazi i procenjuje urađeni posao:

1. Provera usklađenosti sistema sa PCI DSS standardima od strane kvalifikovanog PCI DSS revizora.
2. Izveštaj o usaglašenosti ROC Report of Compliance i AOC Atest on compliance (sertifikat).

VI faza: Kontinualno praćenje, kontrola i poboljšanje

Sam projekat usklađivanja celokupnog poslovanja kompanije prema zadatim standardima je mnogo manji posao, nego obezbeđivanje da se jednom uvedeni i dogovoreni standardi poštuju. Zbog toga je ova faza veoma bitna jer obezbeđuje da se dugoročno sprovode, ali i unapređuju već dogovoreni standardi.

9. ANALIZA I PLANIRANJE RESURSA

Sertifikaciju određenog entiteta u skladu sa PCI DSS standardom obično sprovode ovlašćene kompanije koje moraju da poseduju licencu od strane PCI DSS Councila. Te kompanije imaju zaposlenog QSA – Qualified Security Assessor (kvalifikovanog bezbednosnog procenitelja), koji je jedino ovlašćen da izda i potpiše PCI DSS sertifikat. On vodi kroz sertifikaciju i daje interpreatciju DSS pravila, daje smernice prilikom izrade polisa i radi pocenu usklađenosti sa PCI DSS. Za sada pravila dozvoljavaju da ista kompanija obavlja konsulting, audit i samu sertifikaciju, što je za očekivati da će se uskoro promeniti. Pre angažovanja važno je proveriti na PCI SSC sajtu da li odabrani QSA ima odgovarajuću validnu licencu za obavljnje procene i davanje sertifikata. Preduslov za početak projekta i sam ulazak u njega, bio je rad na edukaciji zaposlenih, prvenstveno onih koji će učestvovati u projketu. Ovaj deo je bio uglavnom obavljen kroz upoznavanje sa literatrurom na internetu i prisustvom na nekoliko tematskih prezentacija održanih u Beogradu.

Angažovanje internih resursa pretpostavlja i potrebna specifična znanja, kao što su:

- Operativni sistemi: Linux i Windows;
- Mrežne komunikacije CISCO;
- Baze: Oracle i MS SQL;
- Project management.

Projektni tim:

- Direktor projekta;
- Viši mrežni analitičar;
- Tehnički koordinator.

Administracija:

- Tehnički direktor;
- Chief security officer.

Nadgledanje, izveštavanje i kontrola:

- Upravni odbor;
- Kolegijum poslovne jedinice.

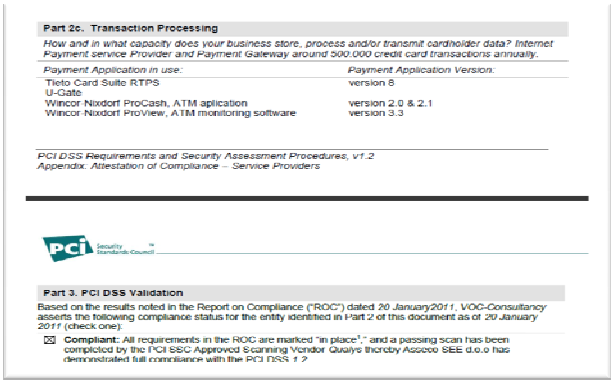
10. PROCENA TROŠKOVA

U proceni troškova neophodno je obuhvatiti sledeće stavke:

- Angažovanje internih resursa;
- Angažovanje konsalting kuće;
- Nabavka potrebne opreme:
  - Komunikaciona oprema;
  - Serveri;
  - Softver za centralizovano logovanje i alerting;
  - Softver za Vulnerability management;
  - Antivirus softver;
  - Kontrola pristupa:
    - Video kamere;
    - Alarmi.
- Angažovanje QSA-a;
- Efikasna bezbednosna kontrola.

11. FINALNI REZULTAT - ROC I AOC

Report on Compliance i Atest On Compliance, detaljno opisuju koji segmenti poslovanja su obuhvaćeni PCI DSS sertifikacijom (Sl. 1 i Sl. 2).



Part 2c. Transaction Processing

How and in what capacity does your business store, process and/or transmit cardholder data? Internet Payment Service Provider and Payment Gateway around 500.000 credit card transactions annually.

Payment Application in use:	*Payment Application Version:*
Tieto Card Suite RTPS	version 8
U-Gate	
Wincor-Nixdorf ProCash, ATM application	version 2.0 & 2.1
Wincor-Nixdorf ProView, ATM monitoring software	version 3.3

PCI DSS Requirements and Security Assessment Procedures, v1.2
Appendix: Attestation of Compliance – Service Providers

Part 3. PCI DSS Validation

Based on the results noted in the Report on Compliance ("ROC") dated *20 January2011*, *VOC-Consultancy* asserts the following compliance status for the entity identified in Part 2 of this document as of *20 January 2011* (check one):

☒ **Compliant:** All requirements in the ROC are marked "in place[1]," and a passing scan has been completed by the PCI SSC Approved Scanning Vendor *Qualys* thereby *Asseco SEE d.o.o* has demonstrated full compliance with the PCI DSS 1.2

Slika 1: Isečak iz **Report On Compliance** document Atest On Compliance je konačni dokaz da je firma sertifikovana

Slika 2: Izgled **Atest On Compliance** dokumenta

ZAKLJUČAK

Usklađivanje sa PCD DSS pavilima je kontinualni proces u kojem se uvek mogu prepoznati tri glavne faze:

- Procena.
- Remedijacija.
- Izveštavanje.

Ono što pokreće kompanije da krenu u bolan proces izmena pravila poslovanja i usaglašavanja sa rigoroznim bezbednosnim standardima jeste činjenica da bezbednost košta mnogo, ali nemati je – košta mnogo više. Bezbednost nije samo jedan program, jedan uređaj, nego je to sistem elemenata koji donose kompletno rešenje. Samim tim dolazimo do činjenice da PCI DSS projekat nije samo IT nego je više poslovno pitanje, jer pored unapređenja informacione infrastrukture, bitno utiče na način i procedure rada unutar kompanije. Tu činjenicu treba imati u vidu i kada se određuju učesnici u projektu, pa je pored kvalitetnog tehničkog kadra neophodno obezbediti podršku višeg menadžmenta, kako bi se sprovođenje standarda omogućilo na nivou celokupne firme. Sa druge strane, pored široko dostupne dokumentacije na Interentu na ovu temu, i uz sav kvalitet i znanje koje poseduju zaposleni, preporučuje se da se proces sertifikacije vrši uz obezbeđen kompetentan konsalting externe kuće iskusne na tom polju. I pored toga unapređenje znanja i njegovo međusobno deljenje unutar kompanije je najbitnija potvrda da će jednom postavljeni standardi da se održe i dalje unapređuju, što je osnova za bezbednu mrežu.

LITERATURA

[1] PCI SSC - Requirements and Security Assesment Procedures, verzija 2.0, oktobar 2010, https://www.pcisecuritystandards.org

[2] PCI Compliance for dummies, John Wiley & Sons Ltd

[3] PCI Compliance: Understand and Implement Effective PCI Data Security Standard Compliance, Dr. Anton Chuvakin, Dr. Branden R. Williams, Syncress

[4] PCI DSS A practical guide to implementing and maintaining compliance, Steve Wright, IT Governance Publishing

[5] Payment Card Industry Data Security Standard Handbook, Timothy M. Virtue, Wiley

[6] Документација са интернет странице www.pcisecuritystandards.org

[7] S. Obradović, A.Donchev, Ž. Vasić. B. Ilić, "Phases of project realization of introducing business with cards", IX Međunarodni simpozijum SYMORG 2004. Zlatibor, 2004.

[8] S. Obradović, V. Marković, S. Ilić, D. Tešić, M. Mijalković, "Payment Card Operations of Banks in the Republic of Serbia", 10th Anniversary international scientific conference UNITECH'10, Technical University of Gabrovo, Bulgaria, 19-20 november 2010, pp. III-59-III-64, ISSN 1313-230X.

[9] S. Obradović, D. Tešić, Đ. Milanović, Žorić A., Đ. Perišić, "Mreže ATM terminala u regionu srednje i istočne Evrope i Srbiji", IEEE Serbia&Montenegro COM CHAPTER and SECTION organize on the 20th, 21st, and 22nd November 2011, in the Sava Center, Belgrade, Serbia. 20th Telecommunications Forum TELFOR 2012. ISBN: 978-1-4673-2984-2, IEEE Catalog Number: CFP1298P-CDR, 1564-1567

[10] EMV Book 1 2004 *EMV Integrated Circuit Card Specification for Payment Systems*, Book 1: Application Independent ICC to Terminal Interface Requirements, Version 4.1. www.emvco.com

[11] EMV Book 2 2004 *EMV Integrated Circuit Card Specification for Payment Systems*, Book 2: Security and Key Management, Version 4.1.

[12] EMV Book 3 2004 *EMV Integrated Circuit Card Specification for Payment Systems*, Book 3: Application Specification, Version 4.1.

[13] EMV Book 4 2004 *EMV Integrated Circuit Card Specification for Payment Systems*, Book 4: Cardholder, Attendant and Acquirer Interface Requirements, Version 4.1.

ABSTRACT

The work presents a model of the PCI DSS (Payment Card Industry – Data Security Standard) introduction project management by realization stages, with a brief review of the payment card application and necessity of the standard introduction, in order to achieve the main project objective - adjusting the information system to the PCI DSS standard requirements, harmonizing operations, preparation, implementation and verification of specific procedures and policies, the work performed. The project comprises the activities described in the plan through 6 implementation stages, and it does not include other activities such as certification of the applied software produced by other vendors.

MANAGEMENT OF THE PCI DSS STANDARD INTRODUCTION PROJECT REALIZATION

Živorad Vasić, Milan Mijalković, Ilja Stanišević, Minka Yordanova, Dragana Sajfert