UDK 336.71:004.738.5

Kritičen pogled na standard za varovanje podatkov o plačilnih karticah

*Gorazd Žagar**

INTRODUCTION TO PAYMENT CARD INDUSTRY DATA SECURITY STANDARD
Article takes a critical standpoint towards the new standard which is believed to change the information security industry as we know it. Credit card vendors are requesting compliance with PCI-DSS standard from every merchant which processes credit card data. Information security experts believe that credit card vendors are not actually solving the core problem which is a result of an outdated system, but are rather pushing the liability and responsibility towards merchants.

JEL G21 G28 K20 K42

V svojem zadnjem prispevku sem obljubil, da si bomo podrobneje ogledali standard, namenjen trgovcem za varovanje podatkov o plačilnih karticah. Razumimo, da standard sam po sebi ne varuje, določa le normativ oz. minimalne zahteve, s katerimi se ugotavlja skladnost s kakšnim dogovorom. Zavzel bom kritično stališče in poskušal utemeljiti nasprotovanja mnogih strokovnjakov na področju informacijske varnosti, ki smatrajo standard kot orodje, ki ga izdajatelji plačilnih instrumentov uporabljajo za prenašanje odgovornosti na trgovce. V raziskovanje standarda bomo stopili laično in pobliže spoznali njegovo tehnično vsebino, nadaljevali z ugotovitvijo, komu je standard namenjen, poskušali poiskati praktične primere uporabe iz prakse in ga na koncu ovrednotili.

Zagotavljanje informacijske varnosti v informacijsko-komunikacijskem sistemu (IKS) se začne z vpeljavo varnostnih mehanizmov, ki varujejo podatke in procese. Z varnostno politiko, ki mora biti napisan dokument, si združba zada načrt, kako bo varovala poslovanje in sredstva. Standard, ki ni varnostna politika, pa je skupek minimalnih zahtev, ki so pogosto povzete po primerih dobrih praks in katerim morajo zagotoviti vsi z željo po skladnosti. Velikokrat se kot merilo za doseganje ravni kvalitete in ustreznosti uporabi za zgled kateri izmed standardov, po katerem se lahko na koncu tudi certificiramo. Če se vprašamo, zakaj želimo doseči skladnost z določenim standardom, bo mnogokrat odgovor zakonodaja, želja po boljših pogojih na razpisih, redkeje pa zgolj zaradi odločitve vodstva po varnejšem poslovanju, saj postopek standardizacije ne poteka brez stroškov.

* Gorazd Žagar, dipl. inž. rač. in inf., je samostojni, neodvisni raziskovalec informacijske varnosti, ki se tematiki ljubiteljsko posveča že 15 let. Ob prostem času ureja priljubljeni blog Infosec (http://infosec.si) in ponuja svetovanje na področju vpeljave dobrih praks varovanja informacij.
Zahvaljujem se g. Edvardu Pohlu, CME, za strokovno pomoč pri pisanju prispevka.

Odločitev za preoblikovanje poslovanja v skladu z določenim standardom (ang. compliance) naj bi bila prostovoljna odločitev, a povsod ni tako. Standard, ki se mu bomo posvetili tokrat, se močno uveljavlja in skladnost z njim je v nekaterih zveznih državah v ZDA (prva je bila Nevada[1]) že zavezujoča z veljavnim zakonom.

Čeprav je bilo že pred predstavitvijo prve različice standarda PCI-DSS na voljo nekaj sorodnih standardov, so izdajatelji plačilnih kartic - podjetja Visa, MasterCard Worldwide, American Express, Discover Financial Services in JBC International, razvijali lastne programe, namenjene vpeljavi dodatne ravni zavarovanja pri procesiranju in hranjenju podatkov o plačilnih karticah. Podjetja so leta 2006 skupaj ustanovila koncil Payment Card Industry Security Standards Council (PCI SSC) in pod njegovim okriljem še istega leta izdala prvo različico standarda PCI Data Security Standard ali krajše PCI – DSS.

PCI-DSS je namenjen organizacijam, ki posredno ali neposredno upravljajo s podatki o plačilnih karticah. Vsebuje nabor smernic ali bolje rečeno zahtev, tako tehničnih kot operativnih, za zagotavljanje varnega ravnanja z zaupnimi podatki. Trgovci, transakcijski sistemi, sistemi za zajem in hrambo podatkov, izdajatelji in ponudniki storitev so le nekatere izmed entitet, ki vstopajo dnevno v stik s tovrstnimi podatki. Vpeljava standarda v poslovanje teh entitet naj bi zagotovila bistveno višjo raven varnosti pri ravnanju s podatki o plačilnih karticah in omejila njihovo krajo, zlorabo ter druge grožnje. Ob standardu PCI-DSS poznamo še soroden standard namenjen proizvajalcem opreme PCI-PTS in standard, namenjen razvijalcem programske opreme, PA-DSS. Slednji je namenjen samo komercialni programski opremi za vodenje spletnih trgovin, ne pa tudi aplikacijam, razvitim v lastnem razvojnem okolju. Morajo pa zato lastne aplikacije ustrezati standardu PCI-DSS. PCI vzdržuje seznam odobrenih komercialnih aplikacij in je dostopen na njihovi spletni strani. V nadaljevanju se bomo osredotočili izključno na standard PCI-DSS, ki je mnogokje poimenovan preposto kar PCI.

PCI predvideva štiri nivoje skladnosti, v katere razvršča trgovce po številu letno opravljenih transakcij[2]. Ravno zadnji, četrti nivo, ki zajema trgovce z najmanjšim številom opravljenih transakcij, vključuje najbolj izpostavljene trgovce. Zaradi majhnega obsega poslovanja ti ne namenijo veliko sredstev za varovanje svojega poslovanja in so posledično bolj izpostavljeni grožnjam napadalcev, ki se želijo polastiti podatkov o plačilnih karticah. PCI lahko trgovca, ki je doživel napad in krajo podatkov, oglobi in prestavi v prvi, najstrožji nivo.

Zagotavljanje informacijske varnosti se začne z vpeljavo varnostnih mehanizmov.

Kot se bomo prepričali v nadaljevanju, je možno standard, delno ali v celoti, vpeljati tudi v IKS, ki ni nujno del plačilnega okolja. PCI vsebuje smernice, ki so rezultat dobrih praks in so priporočljive v vsakem okolju, kjer želimo povišati raven informacijske varnosti. V okviru šestih ciljev je zbranih dvanajst krovnih zahtev, vsaka pa vsebuje večje število podzahtev in nabor pripadajočih kontrol (testov), s katerimi preverimo ustreznost.

Zahteva 1: Namestite in vzdržujte protipožarne pregrade v omrežju

Obstoječo konfiguracijo moramo dokumentirati in opremiti s shemo omrežja, ki jasno prikazuje vse povezave neposredne in posredne do podatkov o plačilnih karticah. Dokumentacija mora vsebovati obrazložitev uporabe vsake storitve v omrežju (FTP, SNMP, Telnet ipd.). Vsaka naprava, priklopljena v notranje omrežje z dostopom do spleta, mora imeti nameščeno lastno protipožarno pregrado.

Zahteva 2: Ne uporabljajte privzetih gesel in drugih privzetih vrednosti ob namestitvi naprav

Pred priklopom sistema v omrežje moramo odstrani vsa privzeta gesla in skrbno pregledati vse privzete nastavitve. Pri prenosu podatkov skozi prosto berljive protokole (FTP, Telnet, NetBios in podobni) naj se uporabljajo povezave IPSec ali VPN. Vešči uporabniki znajo vsak prosto berljiv protokol preusmeriti tudi skozi tunel SSH[3].

Zahteva 3: Zaščitite skladišče podatkov o plačilnih karticah

Doba hranjenja podatkov o plačilnih karticah naj bo minimalna, njihovo uničenje pa naj bo podprto s

[1] Nevada Mandates PCI Standard , dostopno na: http://www.boazgelbord.com/2009/06/nevada-mandates-pci-standard.html

[2] PCI Compliance Levels, dostopno na: http://www.elementps.com/merchants/pci-dss/compliance-level-2/

[3] Tunneling protocol (Wikipedia), dostopno na: http://en.wikipedia.org/wiki/Tunneling protocol

preverjenimi in zanesljivimi postopki. Za trajno uničenje fizičnih medijev so na voljo storitve specializiranih podjetij, za uničenje digitalnih podatkov lahko poskrbimo tudi sami z uporabo posebnih orodij, ki večkratno prepišejo vse sektorje na enoti. Avtentikacijski podatki naj se po uspešni avtorizaciji izbrišejo. Nekateri podatki, kot so številke PIN (ang. Personal Identification Number) in CVV (ang. Card Verification Code), naj ne bodo nikoli shranjeni. Številka PAN (ang. Primary Account Number) naj ne bo nikjer izpisana v celoti, ampak zgolj njenih zadnjih nekaj številk (npr. pri izpiskih o opravljenih transakcijah in vpogledih v spletne račune).

Zahteva 4: Kodirajte prenos podatkov o plačilnih sredstvih v nezaščitenih javnih omrežjih

Zahtevana je uporaba protokolov IPSec, SSL/TLS, SSH in sorodnih pri prenosu podatkov skozi odprta, nezaščitena omrežja, med katere sodijo tudi omrežje GSM in GPRS. Uporaba algoritma WEP (Wired Equivalent Privacy) za zaščito brezžičnih omrežij WiFi je od sredine leta 2010 prepovedana.

Zahteva 5: Uporabljajte in redno nadgrajujte protivirusno in protipožarno programsko opremo

Vsi sistemi, ki so izpostavljeni grožnjam s spleta – pomeni, da imajo dostop do njega – morajo imeti nameščeno protivirusno in protipožarno programsko opremo. Zahteva cilja predvsem na osebne računalnike z nameščenim operacijskim sistemom Windows, saj se je v preteklosti izkazalo, da so bili ravno ti sistemi krivi za kompromitiranje celotne infrastrukture znotraj združbe (primer je napad na RSA[4]).

Zahteva 6: Razvijajte in vzdržujte varne IKS in aplikacije

Zagotovite, da imajo vsi sistemi nameščene zadnje varnostne popravke, identificirajte grožnje, razvijajte »varno« programsko opremo v skladu s PCI. Lastno programsko opremo mora revidirati kvalificirano osebje, to ne sme biti avtor sam, lahko pa so to zaposleni v podjetju.

Zagotoviti ustreznost vseh varnostnih zahtev je za mnoge trgovce neuresničljiv cilj.

Zahteva 7: Omejite dostop do podatkov o plačilnih sredstvih na minimum, ki je še potreben za poslovanje

Zaposleni naj imajo dostop le do podatkov, ki jih potrebujejo za neoviran delovni proces (po načelu ang. need-to-know). Vpeljan je treba imeti sistem za nadzor nad dostopi in dosledno dodeljevanje pravic uporabnikom. Dostop do podatkov naj se primarno zavrne vsem in nato omogoči samo izjemoma na zahtevo.

Zahteva 8: Zagotovite unikatno identifikacijsko številko osebi z dostopom do IKS

Omogočena mora biti sledljivost vsem uporabnikom v IKS, v vsakem trenutku. Za dostop do notranjega omrežja zunaj notranjega omrežja (LAN) naj se uporabi dvofaktorska avtentikacija in dobra politika upravljanja z gesli uporabnikov. Naj poudarim, da uporaba dveh gesel še ne specificira nujno dvofaktorskega sistema. Primer dvofaktorskega sistema je uporaba gesla v kombinaciji z generatorjem ključa, ki je generirano na ločenem sistemu. Gesla morajo biti vseskozi hranjena v neberljivi obliki (uporaba zgoščevalnih funkcij, ang. hash algorithm), kar naj bi napadalcem onemogočalo njihovo zlorabo, čeprav se z razvojem mavričnih tabel povečuje tudi zahteva po minimalni dolžini gesel in zgoščevalnem algoritmu. Leta 2012 pričakujemo nov zgoščevalni algoritem SHA-3.

Zahteva 9: Omejite fizičen dostop do IKS

Vse vstopne točke do IKS naj bodo nadzorovane, vključno z omrežnimi vtičnicami, za katere je najbolje, da so izklopljene, dokler niso v uporabi. Obiskovalci morajo biti v prostorih podjetja ustrezno vizualno označeni. Fizično je treba varovati vse medije, jih ustrezno klasificirati in za njihovo uničenje uporabiti ustrezno metodo. Premnogokrat beremo v medijih o vnovični izgubi teh in onih podatkov državljanov ali komitentov kakšne institucije zaradi malomarnosti zaposlenih.

Zahteva 10: Nadzirajte in omogočite sledenje vseh dostopov do omrežnih virov in podatkov o plačilnih sredstvih

Po incidentu mora biti omogočena rekonstrukcija dogodka na podlagi zapisov v dnevniških zapisih uporabe na sistemih. Pogoj za to je

[4] Details of the RSA Hack, dostopno na:http://www.schneier.com/blog/archives/2011/08/details of the.html

sinhroniziran čas na vseh strežnikih, ki svojo uro redno usklajujejo prek centralnega strežnika NTP (ang. network time protocol). Nenehno se mora preverjati integriteta datotek (npr. z uporabo podpisovanja z MD5 ali bolje SHA). Ne pozabimo na proaktivno pregledovanje dnevniških zapisov na strežnikih in analiziranje dogodkov (priporočam orodje Splunk).

Zahteva 11: Redno izvajajte varnostne preglede sistemov in procesov (penetracijska testiranja)

Vsaj vsako četrtletje naj se izvede notranji in zunanji varnostni pregled, vsaj enkrat letno ter po vsaki bistveni spremembi IKS pa naj se izvede tudi temeljito penetracijsko testiranje, vključno s pregledom brezžičnih točk. Penetracijsko testiranje naj izvede podjetje, ki je za to ustrezno kvalificirano in ima ustrezne reference. To, da je podjetje opravilo varnostni pregled pri nekem podjetju, še ne potrjuje njegove kompetence. Uspešnost penetracijskih testiranj je včasih težko izmeriti.

Zahteva 12: Vzpostavite varnostno politiko, ki vključuje tudi vse osebje

Verjetno najpomembnejša zahteva govori o vzpostavitvi varnostne politike, ki zajema vse zahteve PCI-DSS. Vzpostaviti je treba dnevne postopke osnovnih pregledov IKS. V politko ne smemo pozabiti vključiti osebnih naprav zaposlenih, npr. pametne telefone, ki jih ti prinašajo v podjetje in vklapljajo v notranje omrežje prek brezžičnih dostopnih točk. Aktualna naj bodo izobraževanja zaposlenih, interna in zunanja, seznanjanje z varnostno politko, preverjanje znanja in neprestano spoznavanje z novimi varnostnimi grožnjami. Ocena tveganj (ang. risk assessment) naj se izvede enkrat letno. Ocena tveganj je zelo pomembna za določitev prioritet vpeljave varnostnih kontrol pri omejenih sredstvih.

Ob vsaki zahtevi navaja standard tudi nabor testov, s katerimi si lahko pomagamo pri testiranju ustreznosti minimalnih zahtev standarda. Predvideni testi so sicer zelo skopi in odgovorijo samo na vprašanje, kaj testirati, redkeje pa tudi, kako. V preteklosti je bil PCI deležen tudi kritik,

Napredku v razvoju zlonamernih izkoriščevalskih kod podjetja le težko sledijo.

predvsem na račun zavajajočih 12 zahtev, ki dejansko zajemajo skupno 220 podzahtev. Zagotoviti ustreznost vsem zahtevam je za mnoge trgovce neuresničljiv cilj, tudi zaradi tehničnih ovir, ki bi drastično spremenile način njihovega poslovanja in bi za seboj potegnile nesprejemljive stroške. Je pa lahko standard PCI pravzaprav dober argument, ki ga vodstvu združbe predstavijo informacijski varnostni inženirji z namenom okrepitve informacijske varnosti, kjer običajne finančno zahtevne pobude ostanejo neuslišane.

Če se želimo standardizirati, lahko svojo organizacijo pripeljemo do skladnosti tudi sami, brez pomoči zunanjega izvajalca, saj je standard (v nasprotju z npr. ISO 27001:2005) prosto dostopen na spletu[5]. Združbe lahko opravijo samoocenitev skladnosti z uporabo PCI DSS Self-Assessment Questionnaire (SAQ)[6], ki vsebuje nabor vprašanj, katerim moramo zadostiti. Skladnost s standardom oz. podelitev naziva *certificirane organizacije po PCI-DSS* nam lahko zagotovi (le) podjetje, ki je za to usposobljeno in ga za to kvalificira PCI SSC. Tovrstnih podjetij ali posameznikov z nazivom ang. *Qualified Security Assessor* (QSA)[7], ki lahko podelijo oceno skladnosti, ni ravno veliko. Na seznamu[8], ki ga vzdržuje PCI, še ne najdemo nobenega slovenskega podjetja. Domača podjetja, katerih dejavnost je vpeljava informacijskih varnostnih standardov, vam lahko torej samo svetujejo pri vpeljavi, za preverjanje skladnosti pa boste primorani najeti certificiranega QSA. V šali nekateri pravijo, da vnašajo osebe QSA v združbo več strahu kot morebitni napadalci, saj z negativno oceno skladnosti združbi zadajo več stroškov kot nepridipravi. PCI SSC priporoča bankam (ang. acquirer - ni nujno banka), da zahtevajo od trgovcev standardizacijo (ang. *certified proof of PCI compliance*) v primeru, če imajo opravka z vsaj 20,000 transakcijami na letni ravni.

A vprašajmo se sedaj, nam dosledno upoštevanje zahtev standarda resnično zagotavlja neoporečno varnost in nas, kot uporabnike plačilnih sredstev, varuje pred zlorabami? Zagotovo drži, da spletni trgovec, ki dosega skladnost s standardom PCI, varuje podatke o plačilnih karticah svojih kupcev bolje kot tisti, ki ni skladen. Kot kupec bi ravno tako raje poslovali s spletnim mestom, ki posluje pod nadzorom PCI, kot z

[5] PCI Security Standards Coucil, dostopno na: https://www.pcisecuritystandards.org/security standards/documents.php

[6] PCI DSS Self-Assessment Questionnaire (SAQ), dostopno na: https://www.pcisecuritystandards.org/merchants/self assessment form.php

[7] Qualified Security Assessor Companies, dostopno na: https://www.pcisecuritystandards.org/approved companies providers/qualified security assessors.php

[8] QSA Companies, dostopno na: https://www.pcisecuritystandards.org/approved companies providers/qsa companies.php

drugimi. A vseeno prihaja zaradi napredka v razvoju zlonamernih izkoriščevalskih kod, ki mu podjetja, ki razvijajo protivirusne programe in požarne pregrade, le stežka sledijo, do vdorov v podatkovne baze. Leta 2009 se je zgodil vdor v podjetje Heartland Payment System Inc[9]., od koder so bili odtujeni podatki o 100 milijonih imetnikov kreditnih kartic. Podjetje je bilo v času vdora skladno s standardom PCI-DSS, a morda ne v celoti, saj ni uspelo zaznati zlonamerne programske opreme, ki jo je kiberkriminalcem uspelo namestiti na sisteme v podjetju.

PCI spreminja industrijo informacijske varnosti, kot jo poznamo. Če si poskušamo ustvariti širšo sliko in se opremo na debate strokovnjakov za informacijsko varnost širom sveta, se kaže PCI v ne ravno pozitivni luči. Trgovcem, bankam in skratka vsem entitetam, ki opravijo letno vsaj eno transakcijo s plačilno kartico, je postal PCI vsiljeno merilo za zagotavljanje varnosti. Pri sooblikovanju minimalnih zahtev imajo ti trgovci zanemarljivo vlogo, saj je koncil na koncu tisti, ki potrdi predlagane spremembe. PCI ni zgolj standard, ampak orodje, s katerim poskuša koncil PCI pomakniti odgovornost nivo nižje, od izdajateljev k trgovcem. Nastopi odgovornost, katere pred desetletjem med trgovci ni bilo čutiti. Ti so sedaj postali odgovorni za podatke, s katerimi ravnajo, in če z njimi ne ravnajo v skladu s pravili, bodo poslovali pod drugačnimi pogoji kot drugi. PCI je ocenil, da je bolj smiselno vpeljati varnostna merila v IKS tisočerim trgovcem, kot pa izboljšati proces avtorizacije in delovanje kartičnega poslovanja na splošno. Strokovnjaki se na raznih konferencah javno zmrdujejo ob misli, da morajo sedaj trgovci reševati problem, ki dejansko ni njihov. Problem pa bi tukaj lahko definirali kot omogočanje zlorabe plačilne kartice. PCI rešuje problem tako, da poskuša preprečiti dostop do podatkov neavtoriziranim osebam in s tem njihovo zlorabo, ne rešuje pa problema, ki bi ga po mnenju strokovnjakov moral – onemogočiti avtorizacijo osebam, ki za to nimajo pooblastila. To so izdajatelji plačilnih kartic že poskušali z vpeljavo CVV in 3Dsecure, a ne preveč uspešno. Ker je manj škodljivo izgubiti zaupanje v izpostavljeno spletno mesto kot pa v institucije, kot so Visa, Mastercard in druge, je razumevanje na dlani. PCI bi moral zaznamovati konec obdobja uporabe 16-mestnih številk in PIN-kod ter ponuditi novo rešitev, ki ne bi bremenila trgovcev.

Moje mnenje o standardu je v tej fazi kritično pozitivno. Njegovo vpeljavo bi priporočal vsaki organizacijski strukturi, četudi standarda ne vpelje v celoti in se ne certificira. Sleherni sistemski inženir ali informacijski varnostni inženir bo po bežnem pregledu zahtev v njih prepoznal dobre prakse, ki jih morda uporablja že sam pri svojem delu. V Sloveniji še ni zaslediti težnje po skladnosti trgovcev, se pa poziva k temu banke in nekatere so skladnost s PCI že dosegle.

LITERATURA IN VIRI/REFERENCES:

1. Predavanje »PCI and Compromising Controls and Compromising Security« na konferenci DEFCON 18, dostopno na: http://defcon.org/html/links/dc-archives/dc-18-archive.html

2. PCI Compliance for Dummies (brezplačna knjiga), dostopno na: http://www.qualys.com/forms/ebook/pcifordummies/

[9] Heartland data breach sparks security concerns in payment industry, dostopno na: http://www.computerworld.com/s/article/9126608/Heartland data breach sparks security concerns in payment industry

Presenetljivo majhno zanimanje za nemške obveznice

Nemčija na zadnji avkciji, na kateri je poskušala prodati desetletne obveznice, ni prejela kotacije za kar tretjino maksimalnega obsega celotne izdaje. Tako velik pomanjkanje povpraševanje je presenetljivo, če upoštevamo, da Nemčija velja za najmočnejšo evropsko ekonomijo. Tudi države z veliko večjimi težavami zaradi prevelikega javnega dolga v bližnji preteklosti niso imele težav s prodajo celotnega obsega izdaj svojih obveznic. Resda so bili zahtevani donosi obveznic držav, ki zaradi večjih primanjkljajev veljajo za bolj tvegane od nemških, višji in zadolževanje dražje, a je povpraševanje na tovrstnih avkcijah redno presegalo ponudbo.

Možno je, da za vlagatelje te obveznice zaradi relativno nizkega donosa (trenutno okoli 2 %) preprosto niso zanimive, po drugi strani pa je ta možnost zaradi relativne finančne moči in stabilnosti Nemčije malo verjetna.