Centar Informacijske Sigurnosti

Standard PCI DSS

prosinac 2011.

CIS-DOC-2011-12-033

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

1. Uvod

Kreditne kartice su u širokoj uporabi, a njihovo korištenje za plaćanja preko Interneta raste velikom brzinom. Prošle godine zabilježeno je preko 3 milijarde vlasnika kreditnih kartica. Prodaja putem Interneta u posljednjem je kvartalu 2006. godine iznosila 33,9 milijarde dolara, što predstavlja povećanje od 25% u odnosu na isti kvartal 2005. godine.

No, uz ovaj veliki porast prodaje preko Interneta pojavio se i problem prijevare i krađe. Prijevare putem kreditnih kartica (tj. krađa putem neovlaštenog korištenja tuđih kreditnih kartica) u 2005. godini bile su najčešći oblik krađe identiteta s udjelom od 26% u ukupnom broju slučajeva. Imajući na umu kako su financijske institucije globalno pretrpile gubitak veći od 48 milijardi dolara zbog krađe identiteta te iste godine, te gubitak od 5 milijardi dolara koji su pretrpile privatne osobe, može se slobodno reći da je prijevara putem kreditnih kartica duboko posegla u svačiji džep.

Tvrtka TJX Companies Inc. je 17. siječnja 2007. godine javno objavila kako je pretrpjela neovlašteni upad u sustav za obrađivanje plaćanja kreditnim i debitnim karticama. Brojevi kreditnih i debitnih kartica 45,700,000 korisnika kao i oko 455,000 bilješki o povratu robe (koje sadrže imena korisnika te brojeve njihovih vozačkih dozvola) ukradeni su iz tvrtkinog IT sustava. Ovaj incident smatra se najvećom krađom kartičnih podataka do danas.

Zbog takvih sve učestalijih slučajeva računalnog kriminala i sve većeg broja kartičnih prijevara najveće kartične kuće udružile su se kako bi zajednički odgovorile na izazove kriminalaca novog doba. Zajedničkim snagama, unaprjeđenjem i usuglašavanjem pojedinačnih propisa nastao je novi sigurnosni standard u kartičnoj industriji – Standard sigurnosti podataka industrije platnih kartica (eng. *The Payment Card Industry Data Security Standard, PCI DSS*).

Standard PCI DSS vrlo je važan faktor u dnevnom poslovanju pružatelja usluga plaćanja karticama pošto oni obrađuju velike količine kartičnih podataka svojih klijenata. Sve organizacije koje spremaju, obrađuju ili prenose podatke o kartičnom plaćanju moraju biti usklađene sa standardom PCI DSS.

2. Standard PCI DSS

Standard sigurnosti podataka industrije platnih kartica široko je prihvaćen skup pravila i procedura namijenjenih za optimizaciju sigurnosti kreditnih, debitnih i novčanih kartičnih transakcija koji štiti vlasnike kartica protiv zlouporabe njihovih osobnih podataka. Standard PCI DSS izrađen je 2004. godine, a u njegovoj izradi sudjelovale su četiri glavne tvrtke na području kartičnog poslovanja: Visa, MasterCard, Discover i American Express. Navedene tvrtke zajedno s tvrtkom JCB čine PCI Odbor za sigurnosne standarde (slika 1), koji propisuje i upravlja PCI DSS standardom.

Odbor je osnovan kako bi pomogao organizacijama koje obrađuju kartična plaćanja. Cilj Odbora je spriječiti prijevare putem kreditnih kartica povećanjem provjere podataka i smanjiti njihovu izloženost kompromitiranju. Standard se odnosi na sve organizacije koje spremaju, obrađuju ili prosljeđuju informacije korisnika kartica koju su brendirane s logotipom jednog od kartičnih brendova.

Slika 1. Logo PCI Odbora za sigurnosne standarde
Izvor: Google

Vrednovanje sukladnosti obavlja jednom godišnje vanjski kvalificirani procjenitelj sigurnosti (eng. *Qualified Security Assessor, QSA*) za organizacije koje upravljaju velikim količinama transakcija. Tvrtke koje upravljaju manjim količinama transakcija koriste upitnik samoprocjene (eng. *Self-Assessment Questionnaire, SAQ*).

Vanjsko skeniranje mreže mora provesti ovlašteni prodavač aplikacija za skeniranje. Ovlašteni prodavači aplikacija za skeniranje (eng. *Approved Scanning Vendors, ASV*) konzultanti su informacijske sigurnosti koji pružaju rješenja za skeniranje tvrtkama kako bi otkrile jesu li u skladu s PCI DSS zahtjevom za vanjsko skeniranje ranjivosti. Svi ASV-ovi moraju proći ASV test svake godine da bi ih PCI Odbora za sigurnosne standarde certificirao. Nakon certificiranja mogu obavljati skeniranje raznih mreža i sustava što rezultira usklađivanjem sa standardom PCI DSS.

Kvalificirani procjenitelji sigurnosti konzultanti su za informacijsku sigurnost koje je osposobio i certificirao PCI Odbor za sigurnosne standarde. Oni provode provjere na lokaciji klijenta kako bi provjerili njihovu usklađenost s PCI DSS standardom sigurnosti te kvartalno skeniranje ranjivosti od strane ovlaštenog prodavača aplikacija za skeniranje.

Potpuni popis ASV-ova možete pronaći na sljedećoj web adresi:

https://www.pcisecuritystandards.org/PDF/pci_qsa_list.pdf

Dio standarda su i sigurnosni zahtjevi za PIN transakcije (eng. *Point-to-point credit card encryption, PTS).* To je skup sigurnosnih zahtjeva koje moraju poštivati proizvođači uređaja koji se koriste za obradu PIN-ova korisnika kartica kao i druge kartične aktivnosti. Zahtjevi daju proizvođačima

smjernice o tome kako uređaji moraju biti projektirani, proizvedeni i transportirani organizacijama koje ih koriste.

PTP šifriranje, također poznato kao šifriranje s kraja na kraj (eng. *end-to-end*) osigurava zaštićenost kartičnih podataka i pri slučajevima krađe kartica ili pri ulasku u sustav plaćanja i dok su podaci u prijenosu prema kartičnom procesoru. Najnoviji moderni uređaji obavljaju šifriranje podataka vlasnika kartica prije obavljanja transakcije, tako da trgovci ne dolaze u dodir s nezaštićenim informacijama. Ovi sofisticirani uređaji koriste Triple DES[1] kriptiranje i DUKPT[2] ključeve za zaštitu i prijenos podataka vlasnika kartica preko bilo koje mreže.

Drugi način zaštite je korištenje tokena (eng. *tokenization*). Tokene se može oblikovati na različite načine. Neki izdavatelji tokena ili aplikacija koje ih generiraju oblikuju te vrijednosti tako da odgovaraju obliku izvornih osjetljivih podataka. U slučaju plaćanja karticama, znak može biti iste duljine kao i broj kartice (eng. *Primary Account Number, PAN*) ili može sadržavati elemente izvornih podataka, kao što su posljednje četiri znamenke broja kartice. Kada se pojavi zahtjev za autorizacijom kako bi se provjerila legitimnost transakcije, vrijednost tokena može se vratiti trgovcima umjesto broja kartice, zajedno s autorizacijskim kodom za transakciju. Token je pohranjen u zaštićenom sustavu za pohranu podataka gdje su pohranjeni i stvarni podaci o vlasniku kartice. Pohrana tokena i plaćanje karticama podataka mora biti u skladu s važećim PCI standardima.

Upotreba tokenizacije otežava zlonamjernim napadačima pristup podacima kartice izvan token sustava za pohranu. Provedba tokenizacije može pojednostaviti zahtjeve PCI DSS standarda, kako bi sustavi koji više ne pohranjuju ili obrađuju osjetljive podataka bili uklonjeni iz djelokruga PCI DSS revizija.

Standard sigurnosti aplikacija industrije platnih kartica (eng. Payment *Application Data Security Standard, PA-DSS*) vrijedi za bilo koju organizaciju koja je razvila programsko rješenje ili se bavi integriracijom kartičnih aplikacija. Takva programska rješenja se koriste u svrhu skladištenja, obrade ili prijenosa podataka korisnika kartica kao dio autorizacije kada su ti programi prodani, distribuirani ili licencirani trećim stranama. Potpuni popis certificiranih aplikacija može se pronaći na sljedećoj poveznici:

www.pcisecuritystandards.org/security_standards/pa_dss.shtml

2.1. Razvitak standarda PCI DSS

Standard PCI DSS izvorno je započeo kao pet različitih programa:

- program za sigurnost kartičnih informacija tvrtke Visa (eng. *Visa Card Information Security Program*),
- program za zaštitu podataka tvrtke MasterCard (eng. *MasterCard Site Data Protection*),
- smjernice za upravljanje sigurnosnim informacijama tvrtke American Express (eng. *American Express Data Security Operating Policy*),
- program tvrtke Discover za sigurnost informacija i sukladnost (eng. *Discover Information and Compliance*),
- program tvrtke JCB za sigurnost podataka (eng. *JCB Data Security Program*).

Namjere svake tvrtke (slika 2) bile su slične: stvoriti dodatnu razinu zaštite izdavateljima kartica osiguravajući da tvrtke zadovoljavaju minimalnu razinu sigurnosti kada obavljaju spremanje, obradu i prijenos podataka s kartice. PCI Odbor za sigurnosne standarde (eng. *The Payment Card Industry Security Standards Council, PCI SSC*) osnovan je 15. prosinca 2004. godine kada su ove tvrtke uskladile svoje pojedinačne politike i objavile *Standard sigurnosti podataka industrije platnih kartica (PCI DSS).*

[1]Triple DES kriptiranje se koristi za rješavanje slabosti algoritma DES koji koristi 56-bitne ključeve. Podaci se propuštaju kroz algoritam tri puta, uz korištenje dva ključa čime se provodi efektivna snaga ključa od 112 bita. Predstavlja tri faze rada algoritma DES.

[2] DUKPT (eng. *Derived Unique Key Per Transaction*) je način upravljanja ključevima gdje se za svaku transakciju koristi jedinstveni ključ koji je izveden iz fiksnog ključa.

Slika 2. Glavni osnivači PCI DSS standarda
Izvor: Google

U rujnu 2006. godine standard PCI nadograđen je na inačicu 1.1 te nudi manje izmjene i objašnjenja s obzirom na stariju inačicu 1.0.

Inačica 1.2 objavljena je 1. listopada 2008. godine, a inačica 1.1 prestala je biti važeća na dan 31. prosinca 2008. godine. U inačici 1.2 nisu se promijenili zahtjevi, već je poboljšana prilagodljivost i više je pažnje posvećeno novim razvijenim rizicima i opasnostima. U kolovozu 2009. godine PCI SSC najavio je skok s inačice 1.2 na inačicu 1.2.1 u svrhu izrade manjih ispravaka dizajniranih za unaprjeđenje jasnoće i dosljednosti između standarda i popratne dokumentacije.

Trenutna inačica standarda je inačica2.0, objavljena 26. listopada 2010. godine. PCI DSS inačica 2.0 moraju usvojiti sve kartične tvrtke do 1. siječnja 2011.godine, a od 1. siječnja 2012. godine sukladnost će se ocjenjivati prema inačici 2.0 standarda. PCI DSS inačica 2.0 donosi dva nova zahtjeva, a u međuvremenu se razvijaju 132 promjene na ostalim zahtjevima. Preostale izmjene i poboljšanja spadaju u kategorije pojašnjenja ili dodatnih smjernica.

2.2. Zahtjevi standarda PCI DSS

U nastavku dokumenta su sažeto navedene glavne točke standarda inačice 1.2 od 1. listopada 2008. godine koje određuju 12 zahtjeva (slika 3) za usklađenost organiziranih u šest logičkih povezanih skupina koje se zovu kontrolnim ciljevima. Standard PCI DSS sastoji se ovih 6 poglavlja i 12 točaka, od kojih svaka točka ima svoje specifične zahtjeve. Da bi bili usklađeni prema standardu PCI DSS, moraju se zadovoljiti sve točke koje se odnose na poslovanje tvrtke.

Slika 3. Zahtjevi PCI DSS standarda
Izvor: Mphasis

2.2.1. Izgradnja i održavanje sigurne mrežne infrastrukture

Ovi zahtjevi podrazumijevaju sigurnu mrežnu infrastrukturu koja se mora održavati i u kojoj se transakcije mogu obavljati.

- Zahtjev 1: Ugraditi i održavati vatrozid podešen tako da zaštiti kartične podatke.
- Zahtjev 2: Ne koristiti lozinke i druge sigurnosne parametre dobivene od prodavača sklopovlja i programa.

Podrazumijeva se korištenje vatrozida (eng. *firewall*) koji su dovoljno robusni da budu učinkoviti bez izazivanja neugodnosti i kašnjenja nepotrebnog za poslovanje karticama. Specijalizirani vatrozidi dostupni su i za bežične lokalne mreže (eng. *Wireless local area network*, LAN), koji su vrlo osjetljivi na prisluškivanje i napade zlonamjernih napadača. Osim toga, podatke za autorizaciju, kao što su osobni identifikacijski broj (PIN) i lozinke, ne smije se uključivati u podatke koje isporučuju dobavljači. Kupci bi trebali biti u mogućnosti jednostavno i često mijenjati te podatke.

2.2.2. Zaštita kartičnih (korisničkih) podataka

Podaci o vlasniku kartice moraju biti zaštićeni gdje god su pohranjeni.

- Zahtjev 1: Zaštiti spremljene kartične podatke.
- Zahtjev 2: Šifrirati kartične podatke za vrijeme prijenosa po otvorenim, javnim mrežama.

Repozitoriji s vitalnim podacima, kao što su datumi rođenja, djevojačko prezime majke, JMBG (Jedinstveni matični broj građana), OIB (Osobni identifikacijski broj), broj osobne iskaznice, brojevi telefona i adrese elektroničke pošte, trebali bi biti sigurni od neovlaštenih korisnika. Kada se podaci s kartice prenose putem javne mreže moraju biti kodirani na učinkovit način. Digitalno šifriranje važno je u svim oblicima kartičnih transakcija, a posebice u e-trgovini putem interneta.

2.2.3. Održavanje programa za upravljanje ranjivostima

Sustavi trebaju biti zaštićeni od djelovanja zlonamjernih napadača pomoću svakodnevno ažuriranih antivirusnih programskih rješenja, *anti-spyware* programa i drugih *anti-malware* rješenja.

- Zahtjev 1: Koristiti i redovito ažurirati anti-virusne programske pakete.
- Zahtjev 2: Razvijati i održavati sigurne sustave i aplikacije.

Sve prijave trebaju biti bez pogrešaka (eng. *bug*) i ranjivosti koje bi mogle otvoriti vrata za eksploataciju osjetljivih podataka pri čemu bi moglo doći do krađe i mijenjanja osjetljivih podataka. Potrebno je redovito provjeravati i nadograđivati antivirusni programski paket i operacijski sustav nadogradnjom koje nude proizvođači kako bi se osigurala najviša moguća razina sigurnosti.

2.2.4. Implementacija jakih provjera pristupa

Pristup podacima i operacijama sustava mora se ograničiti i provjeravati kako bi se smanjila mogućnost zlouporabe.

- Zahtjev 1: Ograničiti pristup kartičnim podacima modeliranjem poslovnog procesa.
- Zahtjev 2: Dodijeliti jedinstveni ID svakoj osobi koja pristupa računalu.
- Zahtjev 3: Ograničiti fizički pristup kartičnim podacima.

Vlasnici kartica ne bi trebali davati informacije o kartici tvrtkama s kojima obavljaju nekakvu transakciju, osim ako one moraju znati te podatke kako bi zaštitile sebe i učinkovito obavile transakciju. Svaka osoba koja koristi računalo u sustavu kartičnog poslovanja mora imati dodijeljen jedinstveni identifikacijski i povjerljiv broj ili ime. Podaci o vlasniku kartice moraju biti zaštićeni fizički, kao i elektronički. Primjeri fizičke zaštite uključuju korištenje aparata za uništavanje dokumenata, izbjegavanje nepotrebnog kopiranja papirnatih dokumenata te korištenje brava i lanaca na kantama za smeće kako bi se obeshrabrilo kriminalce koji bi inače prekopavali po smeću.

2.2.5. Redoviti nadzor i ispitivanje mrežne infrastrukture

Mreže preko kojih se odvija kartično poslovanje moraju se stalno pratiti i redovito ispitivati.

- Zahtjev 1: Pratiti i provjeravati svaki pristup mrežnim resursima i kartičnim podacima.
- Zahtjev 2: Redovito provjeravati sigurnost sustava i procesa.

Održavanje mreža je važno kako bi se osiguralo ispravno provođenje i obavljanje funkcija za sve procedure i mjere sigurnosti. Na primjer, anti-virusne i *anti-spyware* programe treba redovito nadograđivati s najnovijim definicijama i obrascima. Ti programi trebali bi često pretraživati sve podatke koji se razmjenjuju, aplikacije, memoriju s izravnim pristupom (engl. *random-access memory, RAM*) i sve medije za pohranu podataka.

2.2.6. Održavanje sigurnosne politike

Sve službene informacije koje se odnose na sigurnosnu politiku moraju se definirati u pravilnicima te održavati i pratiti.

- Zahtjev 1: Održavati pravilnik koji se odnosi na informacijsku sigurnost.

Također su potrebne mjere za nepoštivanje pravilnika i neizvršavanje svih mjera, kao što su revizije i kazne.

2.3. Usklađivanje sa standardom PCI DSS

Najveće kartične kompanije Visa, MasterCard, American Express, Discover i JCB propisuju svim organizacijama koje spremaju, obrađuju ili prenose kartične podatke da postignu usklađenost sa standardom PCI DSS (slika 4). To uključuje banke, pružatelje usluga plaćanja karticama, Internet trgovce te trgovce s fizičkim prodajnim mjestima.

Iako PCI DSS zahtjeve moraju provoditi sve strane u tom procesu, formalna verifikacija usklađenosti nije obvezna za sve subjekte. Trenutno i Visa i Mastercard zahtijevaju PCI DSS provjeru od strane trgovaca i pružatelja usluga. Banke zaprimatelji koje izdaju kartice ne moraju proći kroz PCI DSS provjere, ali u slučaju proboja sigurnosti, bilo koji subjekt koji nije bio usklađen sa standardom PCI DSS u vrijeme sigurnosnih problema bit će podložan dodatnim kaznama, kao što su novčane.

Slika 4. Proces usklađivanja sa zahtjevima
Izvor: Qualys

Usklađivanje nije jednokratni zahtjev. Trgovci su dužni jednom godišnje obaviti provjeru usklađenosti te se od njih očekuje da zadrže usklađenost u svakom trenutku. Usklađenost određuju različite kartične kuće, a ne PCI Odbor za sigurnosne standarde.

Ovisno o veličini i vrsti organizacije, treba provesti bilo potpuni PCI DSS upitnik za samoprocjenu (eng. *Self-Assessment Questionnaire, SAQ*) ili formalnu procjenu na lokaciji klijenta. Provjeru obično provodi kvalificirani procjenitelj sigurnosti. Ako elektroničkim putem prenosite podatke korisnika kartica, također je potrebno kvartalno skeniranje ranjivosti (koje izvodi ovlašteni prodavač aplikacija za skeniranje), a potrebno je i poslati godišnje četiri čista izvješća skeniranja banci prihvatitelju.

Svi trgovci i druge organizacije moraju poslati potvrdu o usklađenosti (eng. *Attestation of Compliance, AOC*) svojim bankama prihvatiteljima kao pokazatelj usklađenost sa standardom PCI DSS. Trgovac ili druge organizacije ponekad trebaju dostaviti i dodatne podatke kao što su SAQ, kvartalna slanje izvještaja o obavljenom skeniranju mreže ovisno o zahtjevima kartičnih kuća ili godišnje potvrde o usklađenosti za procjene na lokaciji klijenta.

Kvartalno skeniranje mreže provodi se svaka tri mjeseca i odnosi se na tvrtke koje pružaju uslugu smještaja stranica za plaćanje, spremaju elektroničke podatke o kreditnoj kartici (čak i ako je to samo trenutno) ili prenose podatke platne kartice putem aplikacija.

Sigurnosna mrežna skeniranja nenametljivi su pregledi kojima se procjenjuju mrežni opsezi organizacije na informacijske sigurnosne propuste. Mora se obaviti čisto skeniranje vanjske mreže čiji se rezultati u obliku izvješća trebaju prikazati odgovarajućoj banci prihvatitelju prije postizanja PCI DSS usklađenosti.

Usklađenost sa standardom PCI DSS mora se održavati svakodnevno i certificirati na godišnjoj razini zato što trgovci mogu promijeniti svoju infrastrukturu zbog razvoja poslovanja, nadogradnji, akvizicija i sl. Napretkom industrije vjerojatno je da će se standard mijenjati kako bi se prilagodio novim sigurnosnim prijetnjama ili potrebama tržišta. Subjekti će usklađenost sa standardom PCI DSS lakše postignuti nego u prijašnjim godinama, a vrijeme koje će biti potrebno za provođenje procesa usklađenosti značajno će se smanjiti.

Trenutno godišnju provjeru moraju provesti trgovci koji imaju više od 6 milijuna transakcija godišnje te pružatelji usluga plaćanja karticama i većina banaka. MasterCard su propisali mandatom da trgovci razine 2 (bilo koji trgovac s više od milijun ukupnih MasterCard i Maestro transakcija godišnje) moraju provesti godišnju provjeru na lokaciji klijenta vođenu od strane kvalificiranog procjenitelja sigurnosti (QSA).

Manji trgovci i pružatelji usluga koriste upitnik za samoprocjenu, alat za vrednovanje kako bi pokazali da rade na postizanju PCI DSS usklađenosti. PCI Odbor omogućuje ovim vrstama organizacija korištenje ovog upitnika umjesto da prolaze procjenu PCI DSS usklađenosti na njihovoj lokaciji.

Najčešći razlog zbog kojeg poslovne organizacije ne prolaze provjeru usklađenosti sa standardom PCI DSS jesu neadekvatne sigurnosne procedure. Nerijetko se događa da se podaci kao što su CVV2/CVC2 ili PIN čuvaju i nakon autorizacije što PCI DSS izričito zabranjuje ili se, na primjer, brojevi platnih kartica čuvaju uz nedovoljne mjere zaštite. Treba imati na umu kako je krajnji cilj standarda PCI DSS povećanje sigurnosti platne transakcije, odnosno smanjenje rizika od zloupotrebe, što je moguće postići i bez intenzivnih ulaganja u opremu, alata za nadzor ili uvođenja složenih sigurnosnih procedura.

2.4. Prednosti usklađivanja sa standardom PCI DSS

Iako se na prvi pogled, pogotovo manjim trgovcima i organizacijama usklađivanje sa standardom PCI DSS čini nepotrebnim i zbunjujućim, ono na kraju može donijeti jako puno koristi pogotovo ako razmišljate o proširivanju i unaprjeđenju svojeg poslovanja.

Usklađenost sa standardima o sigurnosti podataka može donijeti velike koristi za tvrtke svih veličina, a nepoštivanje može imati ozbiljne i dugoročne negativne posljedice.

Usklađenost sa standardom PCI DSS znači da su sustavi sigurni, a korisnici mogu imati povjerenja pri obavljanju transakcija sa svojim karticama i osjetljivim informacijama:

- važno je steći povjerenje kupaca u poslovanju,
- ukoliko se kupci uvjere u sigurnost transakcije vrlo je vjerojatno da će se vratiti te tvrtku koja im je omogućila sigurno poslovanje preporučiti drugima.

Usklađenost organizacija poboljšava i širi pozitivan ugled tvrtke koji prepoznaju banke i pružatelji usluga plaćanja karticom te ostali partneri kako bi mogli proširiti poslovanje.

Usklađivanje sa standardom PCI DSS je proces u kojem se tvrtka neprestano razvija. Pomaže u sprečavanju narušavanja sigurnosti i integriteta kao i krađu informacija o kartičnim transakcijama, ne samo danas, već i u budućnosti:

- Kako postupci zlonamjernih napadača koji napadaju kartične sustave i sustave s osjetljivim podacima postaju sve sofisticiraniji, pojedinim trgovcima postaje sve teže preduhitriti napade i moguće prijetnje.
- PCI DSS Odbor za sigurnosne standarde stalno prati prijetnje i nove tehnologije te radi na načinu kako poboljšati odgovor industrije na njih, kroz poboljšanja za PCI DSS sigurnosne standarde i obuku sigurnosnih profesionalaca.
- Kada je tvrtka usklađena sa standardima dio je rješenja globalne sigurnosti kartičnog poslovanja – i s ostalim tvrtkama dio globalnog odgovora na prijetnje i nesigurnosti kartičnog poslovanja.

Usklađenost sa standardima ima i neizravne koristi:

- Kroz svoje napore kako bi se uskladile sa sigurnosnim standardima PCI, tvrtke će vjerojatno biti bolje pripremljene za usklađivanje s drugim propisima koji dolaze zajedno, kao što su HIPAA, SOX, itd.
- Postojat će osnove za korporativne sigurnosne strategije.
- Vjerojatnost pronalaska novih načina za poboljšanje učinkovitosti IT infrastrukture.

Ukoliko tvrtka nije usklađena sa sigurnosnim standardima, ishod može biti vrlo loš za njezino poslovanje:

- kompromitirani podaci negativno utječu na potrošače, trgovce i financijske institucije,
- samo jedan incident teško može oštetiti ugled tvrtke i sposobnost za vođenje poslovanja na učinkovit način, čak i daleko u budućnost,
- neovlašteni pristup osjetljivim podacima o transakcijama može dovesti do katastrofalnog gubitka prodaje, ugleda i odnosa sa zajednicom te pad cijena dionica.

Moguće negativne posljedice uključuju:

- tužbe,
- potraživanja osiguranja,
- otkazivanje računa,
- kazne izdavatelja kartica,
- državne kazne.

Svaka bi tvrtka trebala provesti politiku usklađivanja sa sigurnosnim standardima kako bi osigurala osjetljive podatke klijenata koji se služe kartičnim plaćanjem te stekla ugled i povjerenje kod sadašnjih, ali i budućih klijenata.

3. Podjela subjekata prema standardu PCI DSS

3.1. Podjela prema razinama

VISA, MasterCard i ostali kartičarski brandovi dijele poslovne subjekte u nekoliko razina. Razine podjele određene su prema ukupnom godišnjem broju transakcija, ali i prema funkciji poslovnog subjekta u procesu transakcije.

1. Banka zaprimatelj (eng. *Acquirer bank*)

Banka zaprimatelj nalazi se na vrhu piramide odgovornosti i ona je odgovorna prema VISA-i i MasterCard-u za sigurnost poslovanja svojih trgovaca.

2. Trgovac (eng. *Merchant*)

Trgovac je ugovorno vezan za banku zaprimatelja i on je početna točka u lancu puta kartičnih podataka. Od prodajnog mjesta trgovca kartični podaci putuju kroz mrežu prema banci zaprimatelju.

3. Treće strane (eng. *Third Parties*)

U treće strane ubrajamo sve druge tvrtke koje su povezane s bankom i trgovcem te imaju u nekom dijelu uvid u kartične podatke. U ovu skupinu ubrajamo sve sustave za Internet naplatu (eng. *Internet Payment Gateway sustav, IPG*), sustave za usluge kartičnog plaćanja, tvrtke koje pružaju usluge poslužitelja internetskih stranica, telekom operatere, proizvođače sklopovlja, proizvođače programa, ponuđače usluga pohrane kartičnih podataka, servisere opreme i dr. Također u ovu skupinu spadaju i podizvođači usluga, npr. dostavne službe, ugovorno vezane tvrtke koje održavaju računalne sustave ili proizvode programe za naručitelja.

Važno je napomenuti da se standard PCI DSS u nekoj mjeri odnosi na sve gore spomenute subjekte i izravno utječe na njihovo poslovanje.

3.2. Podjela pružatelja usluga

Započevši s inačicom standarda 1.2 pružatelji usluga (eng. *Service Providers*) koji u nekoj mjeri sudjeluju u obradi kartičnih podataka, bilo da izravno obrađuju, prenose ili pohranjuju kartične podatke, kao i svi oni koji su indirektno povezani s pružateljem usluge, bilo da održavaju vatrozide, usmjeritelje, poslužitelje ili drugu mrežnu opremu, ali i svi oni koji održavaju programe i aplikacije koji su u opsegu PCI DSS-a.

1. **Razina 1**

U razinu 1 ubrajamo sve banke zaprimatelje, procesore za plaćanja (eng. *payment processors*), sustave za Internet naplatu (eng. *Internet Payment Gateway*) i one trgovce koji imaju više od 600,000 transakcija VISA kartica godišnje. Ova skupina dužna je jednom godišnje obaviti PCI DSS provjeru ovlaštenog revizora, kojeg odobrava PCI konzorcij. Također, potrebno je svaka tri mjeseca obaviti redovno skeniranje mreže, a jednom godišnje penetracijski test.

2. **Razina 2**

U razinu 2 ubrajamo sve subjekte koji ne spadaju u prvi, a pohranjuju, obrađuju ili prenose kartične podatke, te imaju od 120,000 do 600,000 kartičnih transakcija godišnje. Svi subjekti iz skupine druge razine dužni su jednom godišnje ispuniti atest koji predaju banci s kojom imaju ugovor. Također imaju obvezu obaviti mrežno skeniranje svaka 3 mjeseca.

3. **Razina 3**

U razinu 3 ubrajamo sve subjekte koji pohranjuju, obrađuju ili prenose kartične podatke, ali imaju manje od 120,000 transakcija kartica godišnje. Svi subjekti iz skupine treće razine dužni su jednom godišnje ispuniti atest koji predaju banci s kojom imaju ugovor.

4. Primjena standarda PCI DSS

4.1. Primjena standarda PCI DSS kod subjekata

4.1.1. Banke prihvatitelji

PCI DSS predstavlja složeni skup zahtjeva te izazova s kojima se suočavaju organizacije te način primjene i usklađuvanje standarda ovisi o vrsti poslovanja subjekta. PCI DSS može biti osobito težak za implementaciju kod složenih infrastruktura kao što su banke prihvatitelji.

Zajednički problemi s kojima se banke prihvatitelji susreću, a koji mogu utjecati na njihovo postizanje usklađenosti odnose se na sljedeće točke primjera:

- razumijevanje, definiranje i smanjenje opsega procjene,
- rješavanje neusklađenosti s obzirom na naslijeđene sustave,
- učinkovitost kompenzacijskih provjera,
- upravljanje višestrukim timovima u dislociranim odjelima i lokacijama.
- suradnja s trećim stranama kao što su dobavljači, u koje spadaju IT tvrtke koje pružaju podršku bankama prihvatiteljima, vlasnici sustava za Internet naplatu ili pružatelji usluge plaćanja karticama, koji nisu certificirani kao usklađeni.

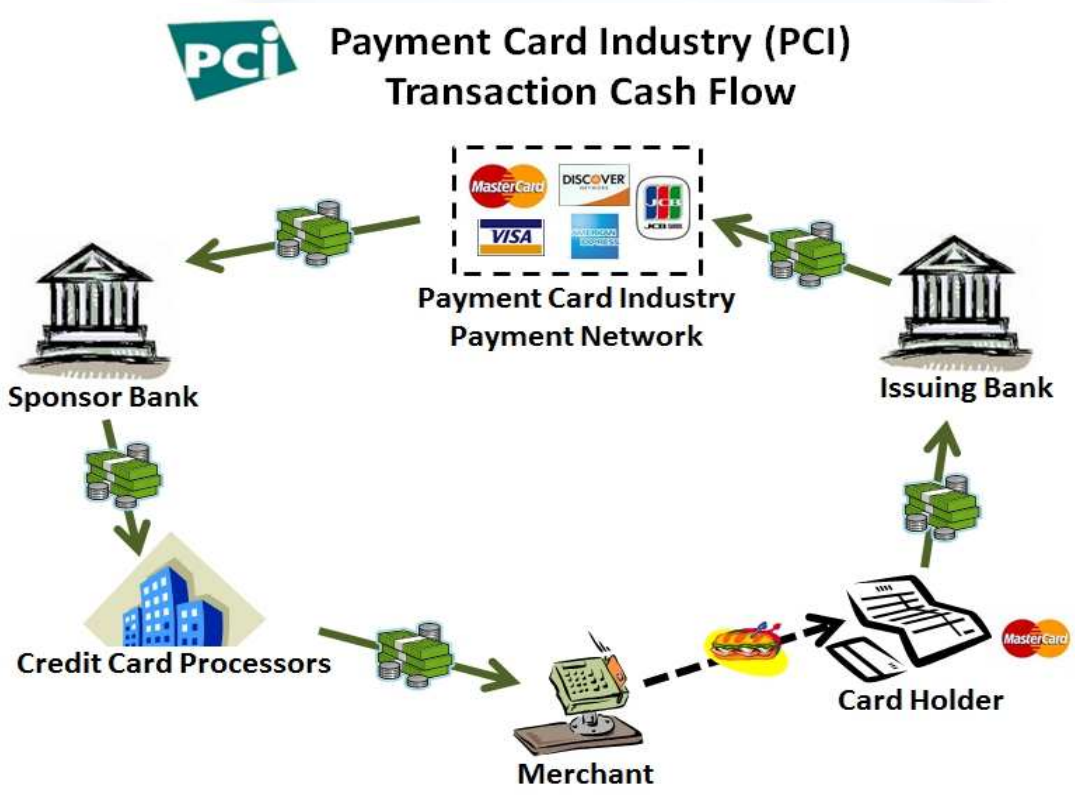
Važno je standard PCI DSS integrirati u složene poslovne procese, infrastrukturu, sustave i tehnologije koje postoje u velikim financijskim institucijama.

4.1.2. Banke

Banke imaju veliki opseg područja svojeg djelovanja koji mora zadovoljiti PCI DSS zahtjeve. Banke često imaju više odjela na više lokacija koji dijele jednu mrežu. To povećava opseg područja koje mora zadovoljiti PCI DSS zahtjeve i naglašava probleme kao što je odijeljivanje mreže. Još jedan jedinstveni PCI DSS problem, koji banke često ističu, prevladavanje je problema naslijeđenih bankarskih sustava. Banke koje imaju probleme s naslijeđenim sustavima najčešće doživljavaju PCI proces usklađivanja kao vrlo skup proces.

Također i poslovanje s trećim stranama kao što su IT tvrtke i pružatelji platnih usluga (slika 5) koji nisu certificirani kao usklađeni sa standardom PCI DSS stvaraju neugodnosti i probleme bankama te se one drže provjerenih subjekata.

S obzirom na mnoge i složene PCI DSS probleme s kojima se suočavaju banke, važno je usklađivanje i provođenje sigurnosnih mjera kako bi se olakšalo poslovanje. Velika pažnja pridaje se čestom skeniranju sigurnosti koje obavljaju kvalificirani procjenitelji sigurnosti (QSA), konzultanti koji posjeduju veliko znanje o različitim sustavima i tehnologijama koje banke koriste svakodnevno. Osim toga, za banke koje imaju složene infrastrukture bitno je dobro sastaviti i razumjeti QSA izvješća.



Slika 5. Proces transakcije novca
Izvor: Google

4.1.3. Trgovci

PCI DSS je prilično zahtjevan za trgovca sa samo jednim prodajnim mjestom, dok za one s više prodajnih mjesta ili s više kanala plaćanja često dodatno komplicira situaciju.

Kartične kuće zahtijevaju izradu PCI upitnika za samoprocjenu (SAQ) za svako prodajno mjesto zasebno jer je izvješće koje banka prihvatitelj dostavlja kartičnim kućama tako

raščlanjeno. Neke banke prihvatitelji ipak dopuštaju trgovcima izdavanje jednog SAQ upitnika. Zajednički problem s kojim se suočavaju trgovci s više prodajnih mjesta je osigurati da se PCI DSS zahtjevi i politike razumiju kroz cijelu mrežu prodajnih mjesta. To je posebno važno za dogovorene prodajne franšize gdje sigurnosni incident na jednom prodajnom mjestu može imati negativni utjecaj na cijelu mrežu.

Mnogi trgovci koriste IP (eng. *Internet Protocol*) terminale i zbog toga je unutarnje skeniranje pojedinačnih terminala osnovni faktor njihovog programa usklađenosti.

Dobro je provesti trening zaposlenika koji se bave sigurnošću kako bi razumjeli važnost uglađivanja s PCI DSS normom te njihove specifične odgovornosti vezane uz zaštitu kartičnih podataka korisnika kartica na razini prodajnog mjesta. Svaka kartičarska kuća ima svoju podjelu trgovaca na više razina.

4.1.4. Pružatelji usluga plaćanja karticama

PCI DSS je vrlo važan faktor u dnevnom poslovanju pružatelja usluga plaćanja karticama (eng. *Payment Service Provider, PSP*) jer oni obrađuju velike količine kartičnih podataka svojih klijenata. Pružatelji usluga plaćanja karticama dostavljaju vodeća poslovna rješenja za svjetsku kartičnu industriju, pri tome pomažući svojim trgovcima u obrađivanju velikog broja kreditnih kartica. S obzirom na velik broj kartičnih informacija koje prolaze kroz PSP sustave, ne iznenađuje činjenica da su česta meta zlonamjernih napadača. Zbog toga se pružatelji usluga plaćanja karticama moraju zaštititi od napada i provoditi intenzivna ispitivanja i revizije.

Osim redovitog ispitivanja važno je održavati certifikate i biti prisutan na listama PCI DSS usklađenih tvrtki koje se nalaze na internetskim stranicama raznih kartičnih kuća. Odlazak s ovih lista ili neaktivnost može imati negativne posljedice za postojeće i nove PSP-ove klijente.

4.1.5. Prodavači kartičnih aplikacija

S obzirom na velik broj kartičnih informacija koje prolaze kroz aplikacije pružatelja usluga plaćanja karticama nužno je održavati visoku razinu informacijske sigurnosti. Kako PCI DSS postaje sve važniji za trgovce na svjetskom tržištu, tvrtke koje se bave kartičnim poslovanjem moraju pružiti rješenja koja su usklađena s normom. Pružatelji usluga plaćanja karticama moraju osigurati da njihovi proizvodi zadovoljavaju promjenjive potrebe klijenata. Iz tog razloga, vrlo je važno da njihove kartične aplikacija prođu proces certifikacije kako bi se pokazale da su sukladne standardu PCI DSS. Kartičnim aplikacijama bave se prodavači kartičnih aplikacija koji moraju biti certificirani prema standardu PCI DSS.

Na Visa internetskim stranicama vidljivo je koje su kartične aplikacije sigurne i u tijeku s najnovijim zahtjevima kartične industrije te usklađene sa standardom PCI DSS.

4.1.6. Pružatelji usluga smještaja i održavanja Internet stranica

Pružatelji smještanja i održavanja Internet stranica mogu se susresti s raznim izazovima ovisno o tome jesu li upravljani ili neupravljani. Upravljan pružatelj navedenih usluga mora zadovoljavati sve aspekte PCI DSS-a, dok su neupravljanim postavljeni ograničeni zahtjevi za postizanje usklađenosti.

Nepridržavanje odrednica PCI DSS standarda može dovesti do gubitka posla za pružatelja usluga smještanja i održavanja Internet stranica jer trgovci mogu odlučiti kako ne žele koristiti njihove usluge za svoju infrastrukturu jer su necertificirani. Umjesto toga, trgovci mogu odlučiti odabrati drugog pružatelja usluga smještanja i održavanja Internet stranica koji je usklađen s ovim standardom.

Pružatelj navedenih usluga može se suočiti s daljnjim izazovima u nastojanju da su cijela infrastruktura, fizička sigurnost, operacijski procesi/procedure kao i logička sigurnost

usklađeni sa standardom PCI DSS. Pružatelji usluga smještanja i održavanja Internet stranica moraju imati certifikat koji će potvrditi njihovu usklađenost sa standardom PCI DSS. Ukoliko pružaju uslugu trgovcu, svi dijelovi usluge kao što su anti-virusni programi, usluga otkrivanja proboja poslužitelja ili mreže te upravljanje vatrozidom moraju biti certificirani

4.2. Status primjene u Hrvatskoj

U Hrvatskoj se koristi gotovo osam milijuna različitih platnih kartica. Unatoč tome što banke u Hrvatskoj u tehnologiju godišnje ulože u prosjeku 900 milijuna kuna, slučajeva kriminalaca koji misle da mogu prevariti banke te potkradati putem Interneta i te kako ima. Banke u Hrvatskoj rade na uvođenju novog standarda u kartičnom poslovanju, koji će pospješiti zaštitu od zloupotreba osjetljivih korisničkih podataka. Na uvođenje novih tehnologija vodeće svjetske kartičarske kuće natjerao je rastući trend krađe podataka korisnika kartica, posebno u SAD-u, zbog čega trgovci i financijske institucije trpe velike gubitke, a korisnici kartica su uznemireni. Ovaj problem proširio se i u Hrvatsku na korisnike kartica koji žele znati da su njihovi podaci zaštićeni, a njihov novac siguran. U posljednje vrijeme veliki se napori kartične industrije ulažu na uvođenje niz novih standarda u načine plaćanja i obradu transakcija koje danas koriste ne samo banke već i trgovci te svi posrednici u lancu. Ovdje je prisutna praksa da trgovci i procesori podataka pohranjuju interne podatke bez ikakve provjere, pa i one podatke koji im nisu potrebni, što može biti predmet zloupotreba. Standardom PCI DSS trgovci su podijeljeni na četiri razine zavisno od broja transakcija, a većina trgovaca u Hrvatskoj podliježe četvrtoj razini s obzirom na to da imaju do milijun transakcija godišnje.

Implementacijom standarda poboljšala bi se zaštita od zloupotrebe osjetljivih kartičnih podataka, i u segmentu izdavanja kartica i u području rada s trgovcima. Na taj način bile bi zaštićene i banke i trgovci jer bi se osigurala zaštita povjerljivih podataka.

Banke u Hrvatskoj trebale bi upoznati trgovce s kojima imaju ugovor o značaju uvođenja standarda PCI DSS, te da se na razini radne skupine koju bi činili predstavnici banka, razmijene iskustva o tome, kako bi se što prije stvorili uvjeti za jedinstvenu i sveobuhvatnu primjenu tog standarda.

Također je bitno unaprijediti suradnju s MUP-om Hrvatske u informiranju o računalnom kriminalu na području kartičnog poslovanja, novim tehnologijama koje se javljaju i standardima koje bi trebalo voditi i poštivati. Učinkovitost u tom području treba unaprijediti kroz veću suradnju s bankama, uvođenjem zakonske regulative koja će uvažiti nove tehnologije i stalnom edukacijom kadra, te nabavkom novih materijalno-tehničkih sredstava.

Zagrebačka banka prva je banka u Hrvatskoj i prva u cijeloj UniCredit grupi koja je stekla certifikat PCI DSS (slika 6), čime je u potpunosti potvrđena usklađenost njenog poslovanja s visokim međunarodnim sigurnosnim standardom platnih sustava. Cjelokupno usklađivanje sa standardom PCI DSS provela je do 15.1.2009.

Zagrebačka banka, kao licencirani izdavatelj, izdaje kartice dviju kartičarskih kuća – MasterCard Worldwide i Visa International. Klijenti Zagrebačke banke koriste više od oko 2,6 milijuna kartica – kreditnih kartica ima oko 460 tisuća, a debitnih oko 2,2 milijuna. Kao prvi vlasnik certifikata PCI DSS u Hrvatskoj, Zagrebačka banka predvodi u razini obrade i obrađivanja podataka pri kartičnim transakcijama u okviru svog sustava, a u cilju maksimalne zaštite svojih klijenata.

Splitska banka druga je banka u Hrvatskoj s certifikatom usklađenosti s PCI DSS. Za sve klijente Splitske banke – preko 500.000 fizičkih i preko 24.000 pravnih osoba to znači da su podaci s njihovih kartica, kao i sve kartične transakcije zaštićene najvišim mogućim važećim sigurnosnim mjerama. Cjelokupno usklađivanje sa standardom PCI DSS banka je provela do 21.5.2010. godine.

Zagrebačka banka i Splitska banka certifikat PCI DSS stekle su proceduralnom provjerom, provedenom od kvalificiranog i certificiranog procjenitelja, kojom se uspoređivala usklađenost kartičnog sustava banke sa svim zahtjevima za dobivanje navedenog certifikata.

PBZ Card je već 2003., prvi na hrvatskome tržištu, uveo sustav za Internet naplatu (eng. *Internet Payment Gateway sustav, IPG*), sofisticirani informatički sustav koji udovoljava najsuvremenijim sigurnosnim uvjetima *online* kupnje, jamči sigurnu i brzu transakciju, zaštitu podataka prodajnog

mjesta, korisnika kartice i PBZ Carda. IPG sustav, koji je sada u domeni Intesa Sanpaolo Card-a, također je certificiran prema PCI DSS zahtjevima.

RBA također posjeduje sustav za Internet naplatu usklađen sa standardom PCI DSS, dok je PBZ Card u posljednjoj fazi priprema za usklađivanje prema standardu PCI DSS.

U cilju dodatnog podizanja razine sigurnosti podataka u budućnosti će u Hrvatskoj i u drugim zemljama Europe provjeru sustava zaštite prema zahtjevima standarda PCI DSS, osim banaka i kartičnih kuća, morati obaviti i svi trgovci koji prihvaćaju kartice na svojim prodajnim mjestima te njihovi davatelji usluga obrađivanja transakcija u procesu plaćanja karticama.

U Hrvatskoj se stanje, što se tiče PCI DSS-a polako pomiče, no procesori koji su certificirani još se uvijek mogu nabrojati na prste. Što se tiče sustava za Internet naplatu, neminovno je da će morati biti certificirani po standardu PCI DSS.


Trustwave®

Date of Compliance:
18 August 2009

Payment Card Industry Data Security Standard
(PCI DSS)
Certificate of Compliance

Awarded to
MBU Ltd.
Level 1 Service Provider

This is to certify that MBU Ltd. has successfully completed an assessment by Trustwave against the Payment Card Industry Data Security Standard v1.2 (PCI DSS).

Conditions of Issuing:
1. Trustwave has issued this certificate to indicate that the aforementioned company's card holder environment has been validated against the Payment Card Industry Data Security Standard v1.2 (PCI DSS) as of the Date of Compliance as stated above. Trustwave makes no warranties or representations regarding the security or vulnerability of company's systems or payment applications.
2. This certificate is subject to validation conditions as laid out within the PCI DSS audit and assessment procedures. Any queries please contact Trustwave at Compliance-QA@trustwave.com. This certificate covers a one year period beginning from the Date of Compliance.
3. This certificate shall not warrant or guarantee to any third party that MBU's card holder environment is invulnerable to attack or compromise. Accordingly, in no event shall Trustwave be liable to any third party in the event of loss or damage caused by any failure or breach of MBU's systems or payment applications.

David Froud, Vice President of PSO, EMEA — 02 September 2009

Slika 6. Certifikat usklađenosti sa standardom PCI DSS
Izvor: mbu

U banci Erste su uveli standard PCI DSS jer su prepoznali kako u cjelokupnom procesu rada s kartičnim transakcijama postoje područja koja je potrebno unaprijediti te standardizirati. Također je njihov sustav za Internet naplatu, MBU certificiran sa standardom PCI DSS, čime postaje prvi PCI DSS sukladan kartični procesor u regiji. MBU je u kolovozu 2009. godine na Visa i MasterCard službenim Internet stranicama certificiranih kartičnih procesora potvrđen kao procesor usklađen s visokim međunarodnim sigurnosnim standardom platnih sustava. Nakon što je VISA ovlaštena revizorska kuća Trustwave završila revizijsku procjenu, MBU se uključio u međunarodni projekt dodatnog podizanja razine sigurnosti s ciljem što bolje zaštite svojih klijenata. U sustavu MBNET-a je bilo više od 25 banaka, 1.192,365, kartica te 62.899,219 obrađenih transakcija u 2008. godini. Ostvarenjem sukladnosti sa standardom PCI DSS MBU je na službenim listama Vise i MasterCarda naveden kao PCI DSS sukladan davatelj vrlo širokog opsega usluga:

- autorizacije plaćanja platnim karticama,
- provjera i namirenje potraživanja,
- sigurnosni protokol 3-D Secure,
- pružatelj usluga plaćanja karticama (eng. *Internet Payment Service Provider*) ,
- obradba transakcija,

- obradba transakcija kartica s magnetskom trakom.

Ukoliko sustavi za Internet naplatu (eng. *payment gateway*) ne certificiraju svoje poslovanje u skladu sa standardom PCI DSS, banke će prekinuti suradnju s njima

5. Budućnost standarda PCI DSS

Sredinom kolovoza 2010. godine, PCI Odbor za sigurnosne standarde službeno je objavio vijest o puštanju novih inačica PCI DSS i PA DSS standarda na tržište. Promjene u standardima relativno su male, odnosno radi se o evoluciji standarda, a ne njegovoj temeljitoj preradi. Namjera je nove inačice dokumenta jasniji pregled zahtjeva koje postavlja PCI DSS, povećanje prilagodljivosti, učinkovitijeg upravljanja rizicima, te usklađivanje standarda s industrijskom praksom.

Potpuno uvođenje standarda PCI DSS inačice 2.0 tvrtke moraju obaviti do kraja 2011. godine pri čemu će kartično poslovanje postati još sigurnije.

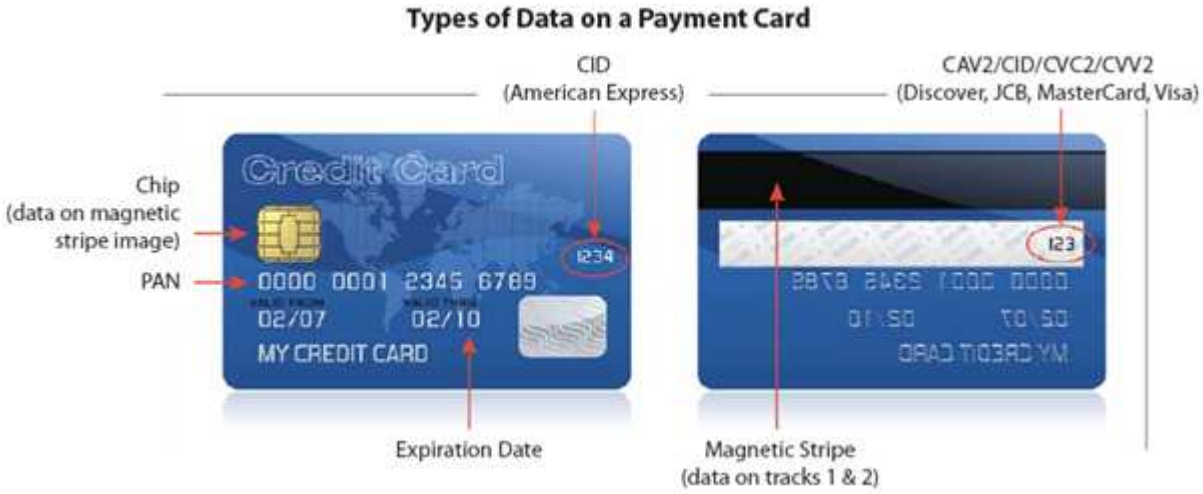
Neka od novih poboljšanja koja nas čekaju početkom 2012. godine su:

- maskiranje broja kartice (eng. *Permanent Account Number, PAN*),
- sve lokacije za pohranu podataka, kao i svi tokovi povjerljivih korisničkih podataka moraju biti identificirani i dokumentirani,
- jasnije su definirane granice i načini odvajanja segmenta Interneta od segmenta u kojem se nalaze povjerljivi korisnički podaci,
- standard uzima u obzir promjene koje se odnose na virtualizacijske tehnologije, pri čemu na jednom poslužitelju može biti implementirana samo jedna primarna funkcija,
- izdavateljima kartica dozvoljava se čuvanje osjetljivih autentikacijskih podataka (npr. PIN/PIN blok i slično), pohrana ovih podataka za sve druge subjekte izričito je zabranjena (slika 7),
- proces upravljanja ključevima, odnosno postupci prijenosa, pohrane i ažuriranja ključeva, dodatno su pojašnjeni,
- uvodi pojam rangiranja uočenih ranjivosti pa se prioritet u otklanjanju ovih ranjivosti daje upravo onima koje imaju najveću važnost. Rangiranje rizika treba se zasnivati na najboljoj industrijskoj praksi. Organizacije koje nemaju dobro definiranu i dokumentiranu politiku implementacije sigurnosnih zakrpa (eng. *patch*) mogu imati problema s ovim zahtjevom.
- proširuju se zahtjevi koji se odnose na sigurno kodiranje korisničkih aplikacija, a ne samo web aplikacija kao do sada. Pored OWASP[3] standarda, u okviru standarda navedeni su standardi CWE[4] i CERT[5] za sigurno kodiranje čime je uklonjena ovisnost o standardu OWASP.
- dozvoljen je autorizirani daljinski pristup i lokalna pohrana podataka, ali isključivo kada je tako nešto opravdano konkretnom poslovnom potrebom i kada se lokalno pohranjeni podaci štite u skladu s PCI DSS odredbama.

[3] OWASP (eng. *Open Web Application Security Project*) je standard za izvršavanje sigurnosnih verifikacija na razini aplikacija.

[4] CWE (eng. *Common Weakness Enumeration*) je formalni popis vrsta slabosti programskih paketa

[5] CERT standard razvija se kao dio CERT programa na Carnegie Mellon sveučilištu. Usredostočen je na sigurnost u internetu.



Slika 7. Važni podaci na platnim karticama
Izvor: Google

Jedna od glavnih teškoća implementacije standarda PCI DSS i dalje će se kriti u činjenici da veliki broj organizacija PCI certifikaciju razumijeva kao jednokratni projekt i napor, a ne kao trajni zadatak i obavezu kompanije. Najbolji dokaz gornje tvrdnje jesu provale napadača u sustave velikih kartičnih procesora koji su u trenutku provale bili, barem formalno, PCI DSS certificirani.

U budućnosti će nad standardom PCI DSS biti potrebno provesti mnoge revizije zbog unaprjeđenja poslovanja, ali i tehnologija koje se koriste. Samim time će se metode ispitivanja ovlaštenih revizora morati poboljšati te će se povećati nadzor nad subjektima kako bi se ažurnije i učinkovitije provodila usklađenost. Unatoč takvim povećanjem nadzora, malo je vjerojatno da će ljudski element u industriji sigurnosti podataka nestati. On će i dalje biti bitan faktor u očuvanju integriteta i povjerljivosti cijelog sustava.

Trenutno, mnogim korisnicima sigurnost podataka nije poznato područje te im ne pridaju mnogo pažnje. Međutim, ukoliko bi korisnici bolje razumjeli količinu i ozbiljnost prijetnji zlonamjernih napadača, uveli bi strože mjere zaštite računalne sigurnosti u svoje poslovanje zbog pojačanih potreba za internim kontrolama i održavanjem povjerljivosti podataka.

Budućnost plaćanja i sigurnost podataka industrije može uključivati niz inovativnih rješenja, od računalne sigurnosti zasnovane na biometrijskim podacima čovjeka do poboljšanja sigurnosti pomoću SMS poruka. Bez obzira na što budućnost donosi važno je u sadašnjosti primjenjivati postojeće standarde zaštite podataka i provoditi usklađivanje pomoću dostupnih alata, zajedno s kombinacijom stroge interne provjere.

6. Zaključak

Prodaja bilo kakvih roba ili usluga danas je nezamisliva bez kvalitetne podrške sigurnosti kartičnog poslovanja. Debitne i kreditne kartice danas se koriste na bankomatima, na POS uređajima, za internetsko i telefonsko plaćanje i dr., a njihovim podacima raspolažu banke, trgovci te davatelji usluga na području kartičnog poslovanja. Zbog toga se sve više pažnje pridaje sigurnosti kartičnih podataka korisnika, pri čemu računalna sigurnost i sigurnost procedura koje se koriste u kartičnom poslovanju postaje od ključne važnosti.

Zbog toge je PCI Odbor za sigurnosne standarde, nezavisno tijelo osnovano od strane kartičnih kuća, razvilo standard PCI DSS, normu za zaštitu kartičnih podataka i podizanje razine sigurnosti kartičnog poslovanja.

Svi subjekti u kartičnom poslovanju (banke, trgovci, davatelji usluga) koji prenose, pohranjuju ili obrađuju kartične podatke obvezni su uskladiti se sa zahtjevima standarda PCI DSS.

Prema nedavnom istraživanju (2011 PCI DSS Compliance Trends Study) na uzorku od 670 IT stručnjaka uključenih u implementaciju standarda PCI koje je u svojim kompanijama provela ugledna analitička kuća Ponemon Institute, PCI DSS i dalje je jedan od najvažnijih regulatornih dokumenata za sve one organizacije koje čuvaju, obrađuju ili razmjenjuju osjetljive podatke o vlasnicima kreditnih kartica.

Jedan od ključnih nalaza spomenute studije je onaj o dramatičnoj razlici u broju incidenata (proboja u IT sustave) koje su pretrpjele organizacije za koje se u trenutku incidenta smatralo da su usklađene s PCI odredbama i onima koji to nisu bile. Prema nalazima analize, 99 posto organizacija koje su svoje poslovanje uskladile sa standardom PCI DSS prijavile su jedan ili ni jedan upad u sustav povezan s kompromitacijom kartičnih podataka. Istovremeno, jednak broj proboja u sustav kod organizacije koje nisu prošle PCI vrednovanje prijavilo je njih 85 posto.

Ovi podaci govore o važnosti standarda PCI DSS i potrebe da se svi subjekti koji su dio industrije platnih katica, od banaka koje ih izdaju do trgovaca, moraju uskladiti i provesti reformu svojeg poslovanja kako bi unaprijedili razinu sveopće računalne sigurnosti, kao i povjerenja klijenata i vlasnika kartica. Napretkom tehnologije načini napada i pokušaja krađe osjetljivih podataka postaju sve sofisticiraniji te se i u budućnosti očekuje razvoj novih tehnologija zaštite podataka, a samim time i razvitak i revizija postojećeg standarda PCI DSS.

7. Leksikon pojmova

PCI DSS (eng. The Payment Card Industry Data Security Standard)

Standard sigurnosti podataka industrije platnih kartica je široko prihvaćen skup pravila i procedura namijenjenih za optimizaciju sigurnosti kreditnih, debitnih i novčanih kartičnih transakcija.

http://en.wikipedia.org/wiki/PCI_DSS

PCI Odbor za sigurnosne standarde (eng. The Payment Card Industry Security Standards Council, PCI SSC)

Odbor je osnovan kako bi pomogao organizacijama koje obrađuju kartična plaćanja spriječiti prijevare putem kreditnih kartica povećanjem provjere podataka i smanjiti njihovu izloženost kompromitiranju.

http://en.wikipedia.org/wiki/PCI_DSS

Kvalificirani procjenitelj sigurnosti (eng. Qualified Security Assessor, QSA)

Kvalificirani procjenitelji sigurnosti su konzultanti za informacijsku sigurnost koji su osposobljeni i certificirani od strane PCI Odbora za sigurnosne standarde.

http://en.wikipedia.org/wiki/Qualified_Security_Assessor

Upitnik samoprocjene (eng. Self-Assessment Questionnaire, SAQ)

Koriste ga tvrtke koje upravljaju manjim količinama transakcija.

https://www.pcisecuritystandards.org/merchants/self_assessment_form.php

Ovlašteni prodavači aplikacija za skeniranje (eng. Approved Scanning Vendors, ASV)

Konzultanti informacijske sigurnosti koji pružaju rješenja za skeniranje tvrtkama kako bi otkrile jesu li su u skladu s PCI DSS zahtjevom za vanjsko skeniranje ranjivosti.

http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

Sigurnosni zahtjevi za PIN transakcije (eng. Point-to-point credit card encryption, PTP)

Skup sigurnosnih zahtjeva koje moraju poštivati proizvođači uređaja koji se koriste za obradu PIN-ova korisnika kartica kao i druge kartičnih aktivnosti.

https://www.pcisecuritystandards.org/documents/pci_ptp_encryption.pdf

Tokenizacija (eng. tokenization)

Korištenje tokena u kartičnoj sigurnosti. Token je pohranjen u zaštićenom sustavu za pohranu podataka gdje su pohranjeni i stvarni podaci o vlasniku kartice.

http://en.wikipedia.org/wiki/Tokenization

Standard sigurnosti aplikacija industrije platnih kartica (eng. Payment Application Data Security Standard, PA-DSS)

Standard koji vrijedi za bilo koju organizaciju koja je razvila programsko rješenje ili se bavi integriracijom kartičnih aplikacija u svrhu skladištenja, obrade ili prijenosa podataka korisnika kartica.

http://en.wikipedia.org/wiki/PA-DSS

Potvrda o usklađenosti (eng. Attestation of Compliance, AOC)

Pokazatelj usklađenosti trgovaca sa PCI DSS standardom.

http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

CVV2/CVC2

Sigurnosni kodovi kartica.

http://en.wikipedia.org/wiki/Card_security_code

PAN (eng. Permanent Account Number)

Broj platne kartice.

http://en.wikipedia.org/wiki/Permanent_account_number

PIN (eng. Personal Indetification Number)

Osobni indentifikacijski broj. Brojčana tajna lozinka koja se dijeli između korisnika i sustava i koristi se za provjeru autentičnosti korisnika.

http://en.wikipedia.org/wiki/Pincode

8. Reference

[1] Elementps: http://www.elementps.com/merchants/pci-dss-compliance/, prosinac 2011.

[2] Kartice: http://kartice.ba/banke.php?type=tema_mart2011_1&page=1&rel=yes, prosinac 2011.

[3] MBU: http://www.mbu.hr/Default.aspx?sid=1199, prosinac 2011.

[4] PCI Security Standards Council: https://www.pcisecuritystandards.org/, prosinac 2011.

[5] Poslovni dnevnik: http://www.poslovni.hr/vijesti/banke-i-karticari-uveli-standard-za-jos-sigurniju-ekupnju-166255.aspx, prosinac 2011.

[6] REP: http://www.rep.hr/vijesti/financije/hoce-li-neki-hrvatski-payment-gatewayi-ostati-bez-posla/2457/, prosinac 2011.

[7] Search Financial Security: http://searchfinancialsecurity.techtarget.com/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard, prosinac 2011.

[8] Splitska banka: http://www.splitskabanka.hr/Opcenito/Press/articleType/ArticleView/articleId/1311/Splitska-banka-posjeduje-certifikat-usklaenosti-s-PCI-DSS-koji-jamci-klijentima-najvisu-zastitu-karticnih-podataka, prosinac 2011.

[9] Sysnet global solutions: http://www.sysnetglobalsolutions.com/hr/PCI_DSS.aspx, prosinac 2011.

[10] Webteh: http://www.webteh.hr/, prosinac 2011.

[11] Wikipedia: http://en.wikipedia.org/wiki/PCI_DSS, prosinac 2011.

[12] Wikipedia: http://en.wikipedia.org/wiki/Tokenization_%28data_security%29, prosinac 2011.