Standard varnosti podatkov kartičnega poslovanja/
Payment Card Industry Data Security Standard

Smernice za prodajna mesta

Smernice za prodajna mesta so povzete po spletnih straneh PCI Security Standards Council (https://www.pcisecuritystandards.org/merchants/index.php), v nadaljevanju Sveta PCI, ki določa Standard varnosti podatkov kartičnega poslovanja.

Skladnost s Standardom varnosti podatkov kartičnega poslovanja (PCI DSS) je bistvenega pomena za vsa prodajna mesta, tako za največje svetovne korporacije kakor tudi za majhne spletne trgovine, za vse, ki sprejemajo plačilne kartice, naj bo v »online ali offline« načinu, saj ni nič bolj pomembno kot varnost podatkov o plačilih in imetnikih plačilnih kartic vaših strank. Dejanske zahteve za skladnost s PCI DSS so odvisne od obsega vaših poslov. Pri tem je treba upoštevati, da zahteve za skladnost prodajnih mest določajo posamezne kartične sheme (Visa, MasterCard, American Express…), in ne Svet PCI.

Kaj je PCI DSS

Naloga in poslanstvo Sveta PCI je, da v sodelovanju z industrijo oz. deležniki kartičnega poslovanja razvija in krepi Standarde varnosti podatkov kartičnega poslovanja, zagotavlja informacije, izobraževanje in usposabljanje tako za prodajna mesta kot tudi presojevalce skladnosti, in sicer glede zaščite občutljivih podatkov pri kartičnem poslovanju v skladu z varnostnimi standardi PCI.

Varnostni standard PCI DSS je skupen nabor orodij in ukrepov za varno ravnanje z občutljivimi informacijami, ki jih vsebujejo podatki pri kartičnem poslovanju. Izvirno je PCI DSS nastal z uskladitvijo varnostnih programov kartičnih shem Vise in MasterCarda, danes pa postavlja okvir zahtev za razvoj robustnega in varnega kartičnega poslovanja ter vključuje ukrepe za preprečevanje varnostnih incidentov pri kartičnem poslovanju, njihovo odkrivanje in ustrezno odzivanje nanje.

Zakaj zagotavljati skladnost s PCI DSS

Skladnost s Standardom varnosti podatkov kartičnega poslovanja prinaša koristi prodajnim mestom vseh velikosti, medtem ko ima lahko neizpolnjevanje zahtev Standarda resne in dolgoročne negativne posledice.

Prodajna mesta, ki sprejemajo plačilne kartice, so pogosto tarča napadov in zlorab podatkov o karticah. Naloga prodajnih mest je, da zaščitijo podatke o imetnikih plačilnih kartic na prodajnih mestih.

Če so podatki o imetniku plačilne kartice ukradeni oz. odtujeni – in to po vaši krivdi, lahko plačate globo ali vas doleti druga kazen, lahko vam celo preneha pravica do poslovanja oz. sprejemanja plačilnih kartic!

Varovanje podatkov imetnikov plačilnih kartic je nujno za vaše poslovanje

Kakšne so posledice za poslovanje, če prodajno mesto ni skladno z zahtevami PCI DSS?

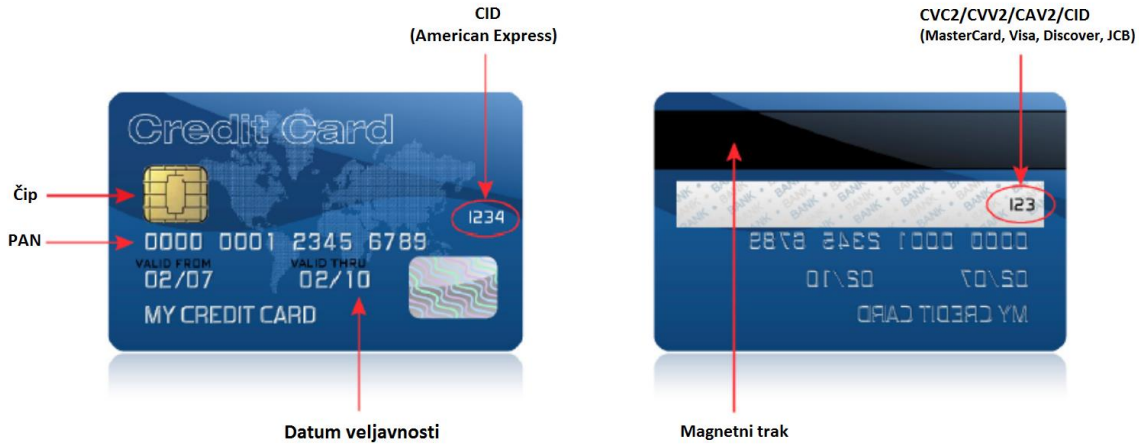
Standard varnosti podatkov kartičnega poslovanja spodbuja k skladnosti s standardom vsa prodajna mesta, na katerih se hranijo, posredujejo ali obdelujejo občutljivi podatki kartičnega poslovanja. Skladnost s PCI DSS namreč zmanjšuje finančna tveganja, ki so povezana s kartičnim poslovanjem. Svet PCI sicer te skladnosti ne preverja in tudi ukrepa ob morebitni neskladnosti. Za to skrbijo posamezne kartične sheme, ki imajo lastne programe skladnosti, vanje pa so vključeni tudi finančni in drugi ukrepi za tista prodajna mesta, ki ne zagotavljajo skladnosti s PCI DSS.

Kateri so občutljivi podatki pri kartičnem poslovanju

Vse, kar je na sliki označeno z rdečo puščico, so občutljivi podatki imetnika kartice, pri čemer se nikoli ne smejo shranjevati nobeni podatki s hrbtne strani kartice, niti identifikacijska številka kartice (CID – Card Identification Number). Vsi preostali podatki, ki jih prodajno mesto shranjuje zaradi poslovnih razlogov, pa morajo biti zaščiteni. PCI DSS pojasnjuje, kako.

Preberite več na povezavi
https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_1.pdf

Prikaz podatkov na plačilni kartici



Matrika občutljivih podatkov kartičnega poslovanja

	Podatek	Dovoljena hramba	Zahtevana zaščita	Kriptiranje podatkov
Podatki o plačilni kartici	PAN	DA	DA	DA
	Naziv imetnika plačilne kartice	DA	DA	NE
	Service Code	DA	DA	NE
	Rok veljavnosti	DA	DA	NE
Občutljivi podatki o odobritvi plačila	Podatki celotnega magnetnega zapisa	NE	N/A	N/A
	CVC2/CVV2/CID/CAV2	NE	N/A	N/A
	PIN/PIN block	NE	N/A	N/A

Zahteve za skladnost s PCI DSS

Posamezne kartične sheme same določajo zahteve za skladnost, ki jih morajo izpolnjevati prodajna mesta in preverjati banke pridobiteljice prodajnih mest. Kartične sheme tudi opredeljujejo posledice ob morebitni neskladnosti prodajnih mest s PCI DSS.

Kje začeti

Prodajna mesta, ki sprejemate plačilne kartice, morate zagotavljati skladnost s Standardom varnosti podatkov kartičnega poslovanja. O tem, katere zahteve skladnosti natančno morate zagotavljati, se lahko pozanimate pri svoji banki pridobiteljici. Preden začnete pripravljati ukrepe, je priporočljivo, da se na spletnih straneh Sveta PCI seznanite z osnovnimi informacijami in pridobite splošno razumevanje o tem, kaj morate storiti.

Kako zagotoviti skladnost s PCI DSS

PCI DSS je skupek tehničnih in operativnih zahtev za zaščito podatkov imetnika kartice, ki jih je predpisal Svet PCI. Svet PCI je odgovoren za upravljanje varnostnih standardov, medtem ko nad izvajanjem skladnosti s PCI DSS bedijo kartične sheme. Standardi se nanašajo na vsa prodajna mesta, ki hranijo, obdelujejo ali posredujejo podatke o plačilih in imetnikih plačilnih kartic. Standard vključuje tudi smernice za razvijalce programske opreme in proizvajalce aplikacij ter naprav, ki se uporabljajo pri kartičnem poslovanju.

Prodajna mesta, ki sprejemate plačilne kartice, morate zagotavljati skladnost s Standardom varnosti podatkov kartičnega poslovanja. O tem, katere zahteve skladnosti natančno morate zagotavljati, se lahko pozanimate pri svoji banki pridobiteljici.

PCI DSS v svojih zahtevah predpisuje ukrepe, ki sledijo najboljšim varnostnim praksam. Obstajajo trije koraki, po katerih pristopiti k izpolnjevanju zahtev PCI DSS. Zavedati se je treba, da je zagotavljanje skladnosti s PCI DSS stalen in neprekinjen proces.

Prvi korak je ocena. V tem koraku prodajna mesta opredelite, kje se občutljivi podatki kartičnega poslovanja za posamezno prodajno mesto hranijo, obdelujejo ali kako se posredujejo. Sledi popis sredstev in poslovnih procesov, ki se uporabljajo pri kartičnem poslovanju. Nato pripravite oceno tveganja in pregled ranljivih točk za varnost občutljivih podatkov pri kartičnem poslovanju.

Drugi korak je odprava pomanjkljivosti skupaj z odločitvijo, da ne shranjujete občutljivih podatkov kartičnega poslovanja, če jih ne potrebujete.

Tretji korak je izpolnitev poročila o skladnosti prodajnega mesta, v katerem prodajno mesto zbere in predloži opis zahtevanih ukrepov izboljšav (če je potrebno). S poročilom o skladnosti s PCI DSS je treba seznaniti banke pridobiteljice, s katerimi poslujete. Za več informacij obiščite https://www.pcisecuritystandards.org/pci_security/how in Quick Reference Guide..

Informacije o specifičnih varnostnih zahtevah, ki jih s posameznimi programi izvajajo posamezne kartične sheme, dobite na spletnih straneh kartičnih shem, in sicer:

- American Express: www.americanexpress.com/datasecurity
- Discover: https://www.discover.com/
- JCB International: http://www.global.jcb/en/
- MasterCard: http://www.mastercard.com/sdp
- Visa Inc: http://www.visa.com/cisp
- Visa Europe: http://www.visaeurope.com/ais

Za posodobljene informacije o tem, kako začeti, preglejte PCI DSS FAQs na https://www.pcisecuritystandards.org/faq/. Seznanite se z dejstvi, kako vam lahko varnostni standard PCI DSS pomaga varovati podatke kartičnega poslovanja in preprečiti krajo teh podatkov.

Klasifikacija prodajnih mest - trgovcev

Kartične sheme opredeljujejo delitev prodajnih mest na podlagi letnega obsega plačil. Na podlagi klasifikacije je določen tudi obseg ukrepov za doseganje skladnosti s PCI DSS.

Zadnje veljavne klasifikacije prodajnih mest so objavljene na spletnih straneh posameznih kartičnih shem:

- American Express: www.americanexpress.com/datasecurity
- MasterCard: http://www.mastercard.com/sdp
- Visa Europe: http://www.visaeurope.com/ais

V nadaljevanju so v preglednicah navedene zahteve posameznih kartičnih shem.

Zahteve MasterCarda

Kategorija	Kriteriji	Zahteve
Raven 1	• Vsako prodajno mesto, ki je utrpelo poskus napada ali napad na podatke kartičnega poslovanja • Vsako prodajno mesto, pri katerem se letno opravi več kot **šest milijonov plačil s karticami MasterCard in Maestro skupaj** • Vsako prodajno mesto, ki ustreza kriterijem Vise za Raven 1 • Vsako prodajno mesto, za katero MasterCard presodi, da mora izpolnjevati kriterije Ravni 1 z namenom, da prodajno mesto minimizira tveganja sistema	• Letna presoja skladnosti prodajnega mesta na lokaciji (presojo opravi kvalificirani varnostni presojevalec (Qualified Security Assessor (QSA)) • Četrtletno preverjanje varnostnih ranljivosti informacijske podpore, ki ga opravi ASV (podjetje, pooblaščeno za izvajanje zunanjih varnostnih pregledov)
Raven 2	• Vsako prodajno mesto, na katerem se letno opravi od **enega do šest milijonov plačil s karticami MasterCard in Maestro skupaj** • Vsako prodajno mesto, ki ustreza kriterijem Vise za Raven 2	• Letna samoocena (SAQ) • Presoja skladnosti prodajnega mesta na lokaciji glede na presojo prodajnega mesta • Četrtletno preverjanje varnostnih ranljivosti informacijske podpore, ki ga opravi ASV
Raven 3	• Vsako prodajno mesto, na katerem se letno opravi več kot **20.000 spletnih plačil s karticami MasterCard/Maestro in hkrati manj kot en milijon vseh plačil s karticami MasterCard/Maestro skupaj** • Vsako prodajno mesto, ki ustreza kriterijem Vise za Raven 3	• Letna samoocena (SAQ) • Četrtletno preverjanje varnostnih ranljivosti informacijske podpore, ki ga opravi ASV
Raven 4	Vsa preostala prodajna mesta	• Letna samoocena (SAQ) • Četrtletno preverjanje varnostnih ranljivosti informacijske podpore, ki ga opravi ASV

Zahteve Vise

Kategorija	Kriteriji	Zahteve
Raven 1	• Vsako prodajno mesto, na katerem se letno opravi več kot **šest milijonov plačil s karticami Visa** • Vsako prodajno mesto, ki deluje tudi v drugi državi, kjer je opredeljeno kot Raven 1	• Letna presoja skladnosti prodajnega mesta (ROC) na lokaciji (presojo opravi kvalificirani varnostni presojevalec (Qualified Security Assessor (QSA)) • Četrtletno preverjanje varnostnih ranljivosti informacijske podpore, ki ga opravi ASV (podjetje, pooblaščeno za izvajanje zunanjih varnostnih pregledov) • Posredovanje potrdila o skladnosti
Raven 2	• Vsako prodajno mesto, na katerem se letno opravi od **enega do šest milijonov plačil s karticami Visa**	• Letna samoocena (SAQ) • Četrtletno preverjanje varnostnih ranljivosti informacijske podpore, ki ga opravi ASV • Posredovanje potrdila o skladnosti
Raven 3	• Vsako prodajno mesto, na katerem se letno opravi med **20.000 in milijon spletnih plačil s karticami Visa**	• Procesiranje spletnih plačil mora potekati preko ponudnika, certificiranega za PCI DSS
Raven 4	• Spletno prodajno mesto z manj kot **20.000 spletnih plačil s karticami Visa na leto**	• Procesiranje spletnih plačil mora potekati prek ponudnika, certificiranega za PCI DSS
	• Vsi preostala prodajna mesta, ki niso spletna prodajna mesta in na katerih se letno opravi **do milijon plačil s karticami Visa**	• Letna samoocena (SAQ) • Četrtletno preverjanje varnostnih ranljivosti informacijske podpore, ki ga opravi ASV • Posredovanje potrdila o skladnosti

Zahteve American Expressa (AMEX)

Kategorija	Kriteriji	Dokumenti preverjanja	Zahteva
Raven 1	• Vsako prodajno mesto, na katerem se letno pravi **2,5 milijona ali več plačil s karticami American Express** • Vsako prodajno mesto, za katerega American Express meni, da je prodajno mesto Ravni 1	• Letna presoja skladnosti prodajnega mesta na lokaciji • Četrtletno preverjanje varnostnih ranljivosti informacijske podpore	Obvezno
Raven 2	• Vsak prodajno mesto, na katerem se letno opravi od **50.000 do 2,5 milijona plačil s karticami American Express**	• Letna samoocena • Četrtletno preverjanje varnostnih ranljivosti informacijske podpore	Obvezno
Raven 3	• Vsako prodajno mesto, na katerem se letno opravi **manj kot 50.000 plačil s karticami American Express**	• Letna samoocena • Četrtletno preverjanje varnostnih ranljivosti informacijske podpore	Priporočeno
EMV	• Vsako prodajno mesto, na katerem se letno opravi **več kot 50.000 plačil s karticami American Express**, pri čemer je **75 % plačil** opravljenih fizično s kartico na prodajnih mestih, ki so skladna s standardom **EMV** in imajo zmožnost, da plačila procesirajo stično in brezstično	• Letno potrdilo skladnosti z EMV	Obvezno

Izvajanje letne presoje skladnost s PCI DSS

Prodajna mesta, ki so zavezani k letni presoji skladnosti, morajo zagotoviti, da presojo izvede pooblaščeni presojevalec (QSA).

Pooblaščeni presojevalci varnosti (QSA) so podjetja, ki jih je kvalificiral in preveril Svet PCI. Pooblaščeni presojevalci varnosti so zaposleni v teh organizacijah, ki imajo ustrezen certifikat za presojo skladnosti prodajnega mesta - trgovca s PCI DSS na lokaciji trgovca. QSA trgovcu izda potrdilo o stanju skladnosti s PCI DSS in ga posreduje kartičnim shemam.

Seznam QSA je objavljen na naslednji povezavi:
https://www.pcisecuritystandards.org/approved_companies_providers/qsa_companies.php.

Samoocenitveni vprašalniki PCI DSS (SAQ)

PCI DSS SAQ je samoocenitveni vprašalnik za prodajna mesta in ponudnike storitev, ki niso zavezani k pregledovanju skladnosti preko pooblaščenih presojevalcev. Namen SAQ je pomagati prodajnim mestom pri samoocenjevanju skladnosti s PCI DSS, pri čemer morate s samooceno seznaniti svojo banko pridobiteljico. Posvetujte se s svojo banko pridobiteljico glede morebitnih podrobnosti zahtev PCI DSS.

Obstaja več tipov SAQ. V preglednici v nadaljevanju je predstavljena uporaba posameznih SAQ. Podrobnosti o izpolnjevanju samoocenitvenih vprašalnikov najdete na spletni strani: https://www.pcisecuritystandards.org/document_library?category=saqs#results

Vsak vprašalnik SAQ vključuje nabor vprašanj o zagotavljanju varnosti in varnostnih ukrepih, ki jih izvajate na prodajnem mestu. Na vprašanja odgovarjate z da ali ne. Izbira vrste vprašalnika SAQ je odvisna od tehnično-tehnološke rešitve, ki pri trgovcu podpira kartično poslovanje.

Tipi SAQ	**Na kakšen način izvajate plačila s plačilnimi karticami**
A	Prodajna mesta na katerih kartica ni fizično prisotna, vse funkcije, povezane s podatki imetnikov plačilnih kartic, opravljajo zunanji izvajalci
A - EP	Prodajna mesta spletne trgovine, ki delno Outsourced Using a Third-Party spletna stran za obdelavo plačil
B_IP	Prodajna mesta s samostojnimi PTS POI terminali (s točko interakcije), ki so povezani preko IP omrežja, podatki o imetnikih plačilnih kartic se ne shranjujejo elektronsko
B	Prodajna mesta le z imprinterji ali s samostojnimi klicni terminali – Podatki o imetnikih plačilnih kartic se ne shranjujejo elektronsko
C-VT	Prodajna mesta z virtualnimi plačilnimi terminali na spletu – podatki o imetnikih plačilnih kartic se ne shranjujejo elektronsko
C	Prodajna mesta s sistemi za plačilne aplikacije, ki so povezani v Internet – podatki o imetnikih plačilnih kartic se ne shranjujejo elektronsko
D	Vsa ostala prodajna mesta, ki izpolnjujejo pogoje na podlagi samoocenitvenega vprašalnika (SAQ)
P2PE	Prodajna mesta, ki uporabljajo strojne plačilne terminale samo v programski rešitvi s seznama PCI SSC-Listed P2PE – Podatki o imetnikih plačilnih kartic se ne shranjujejo elektronsko

Izpolnjevanje vprašalnika SAQ

SAQ sestavljajo: sklop vprašanj, pregled ukrepov za doseganje skladnosti in potrdilo o skladnosti. S potrdilom o skladnosti izjavljate, kakšna je raven skladnosti z zahtevami PCI DSS.

Preden si prenesete svoj vprašalnik SAQ in ga začnete izpolnjevati, preberite navodila, ki so objavljena na: https://www.pcisecuritystandards.org/document_library?category=saqs#results

Informacije o tem, kako se posamezen SAQ uvršča v Standard varnosti podatkov kartičnega poslovanja, najdete prav tako na spletni strani:
https://www.pcisecuritystandards.org/document_library?category=saqs#results

Preden začnete izpolnjevati SAQ, se seznanite z:

1. Navodili in smernicami:
   https://www.pcisecuritystandards.org/document_library?category=saqs#results

2. vpeljanimi tehničnimi rešitvami za podporo kartičnemu poslovanju.

Na podlagi navedenih informacij izberite ustrezen vprašalnik SAQ.

Pregled varnostnih ranljivosti

Izvajalci varnostnih pregledov – Approved Scanning Vendors (ASVs) so podjetja, pooblaščena za izvajanje zunanjih varnostnih pregledov. Opravljajo preverjanje varnostnih ranljivosti javno dostopnih informacijskih omrežij glede na zahteve iz PCI DSS.

Seznam ASVs pa je objavljen na tej povezavi:
https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php.

Še kratki nasveti za zagotavljanje varnosti vašega poslovanja

- Poskrbite, da se na vaših prodajnih mestih uporabljajo samo odobrene PIN naprave. Povezava na PCI-jev seznam odobrenih PIN naprav/PCI Approved PIN Transaction Security (PTS) Devices

- Za izvajanje kartičnega poslovanja prek svojih POS terminalov ali pri spletnih nakupih uporabljajte le legalno in veljavno programsko opremo. Povezava na PCI-jev seznam potrjenih aplikacij za izvajanje plačil/PCI List of Validated Payment Applications

- Ne shranjujte nobenih občutljivih podatkov kartičnega poslovanja na računalnikih ali papirju.

- Za zaščito svojega računalniškega omrežja uporabite požarni zid.

- Poskrbite, da sta vaš brezžični preusmerjevalnik oz. vaše omrežje zaščitena z geslom in da uporabljate šifriranje podatkov.

- Uporabljajte zapletena gesla. Spremenite privzeta gesla na strojni in programski opremi.

- Redno preverjajte PIN naprave in računalnike. Redno preverjajte, da na napravah niso nameščene zlonamerna programska oprema ali naprave za »skimming«.

- Seznanite svoje zaposlene s tem, kakšna je zahtevana varnost in kateri so ukrepi za zaščito podatkov kartičnega poslovanja.

- Sledite standardu PCI DSS in ga izvajajte.