Worldline | SIX Payment Services

UPUTE ZA SUKLADNOST S PCI DSS SIGURNOSNIM STANDARDIMA ZA TRGOVCE

Svi trgovci širom svijeta koji prenose, obrađuju ili pohranjuju kartične podatke dužni su pridržavati se sigurnosnih smjernica navedenih u Standardu sigurnosti podataka u industriji platnih kartica (PCI DSS). U slučaju nepoštivanja tih smjernica, SIX Payment Services ima pravo raskinuti ugovornu obvezu s trenutnim učinkom i zatražit naknadu za nastale štete ili kazne.

Sljedeće upute, koje su u obliku tehničkih i organizacijskih smjernica, predstavljaju obvezujuće odredbe svakog ugovora s društvom SIX Payment Services.

ŠTO OBUHVAĆA PCI DSS?

PCI DSS obuhvaća 12 obveznih uvjeta kojima je svrha zaštititi kartične podatke tijekom obrade, pohrane ili prijenosa. Standard PCI DSS provodi se putem sigurnosnih programa kartičnih organizacija. To su AIS iz Vise, SDP iz MasterCarda i ekvivalentni programi iz American Expressa, Discovera (Diners Club) i JCB-a.

ZAŠTO JE PCI DSS UVEDEN?

U posljednjih nekoliko godina krađa kartičnih podataka u stalnom je porastu. Zlouporaba ukradenih kartičnih podataka uzrokovala je značajne gubitke za sve uključene strane.

KOJA JE SVRHA PCI DSS-A?

Uz PCI DSS kartične organizacije žele još više povećati sigurnost kartičnog plaćanja kako bi trgovce i nositelje kartica, kao i industriju u cjelini, učinkovitije zaštitile od krađe i zloupotrebe kartičnih podataka.

TKO MORA SLIJEDITI SMJERNICE PCI DSS?

Prema PCI DSS-u, svi trgovci koji prenose, obrađuju ili pohranjuju kartične podatke dužni su poduzeti i održavati učinkovite sigurnosne mjere.

Nadalje, trgovci su se dužni pobrinuti da se treće strane koje u njihovo ime prenose, obrađuju ili pohranjuju kartične podatke, kao što su pružatelji usluga platnog prometa (PSP) ili entiteti za pohranu podataka (DSE), također pridržavaju pravila PCI DSS.

Vidi također odjeljke u vezi s „zaštitom podataka" i „odgovornosti" općih poslovnih uvjeta koji se primjenjuju na prihvaćanje kartica.

TKO JE ODGOVORAN ZA SUKLADNOST S PRAVILIMA PCI DSS?

Sukladnost sa sigurnosnim smjernicama PCI DSS u osnovi je odgovornost svakog trgovca. Međutim, kartične organizacije od trgovaca također zahtijevaju da deklariraju (da se trgovci certificiraju) sigurnosne mjere koje provode. Opseg deklaracije (certifikacije) ovisi o broju provedenih transakcija i o tome sudjeluje li trgovac u prijenosu, obradi ili pohrani podataka.

KOJE METODE CERTIFIKACIJE POSTOJE?

PCI DSS razlikuje sljedeće tri metode certifikacije (vidite i tablicu na poleđini).

- **Upitnik za samoprocjenu (SAQ)**
  Uključuje ispunjavanje upitnika za samoprocjenu.
- **Mrežni sken**
  Akreditirana tvrtka za certifikaciju (ovlašteni dobavljač aplikacija za skeniranje) provodi prijateljski hakerski napad svaka tri mjeseca, u suradnji s trgovcem, kako bi se otkrile eventualne ranjivosti sustava.
- **Procjena na lokaciji**
  Trgovci s velikim obujmom transakcija ili oni koji su bili žrtve krađe kartičnih podataka obvezni su ispuniti izvješće o sukladnosti (ROC). Rezultate mora ispitati i potvrditi kvalificirani procjenitelj sigurnosti (QSA) ili unutarnji procjenitelj sigurnosti (ISA).

Ako trgovac ne ispuni sve kriterije za certifikaciju, bez odlaganja mora poboljšati sigurnosne mjere u relevantnim područjima.

TKO SNOSI TROŠKOVE CERTIFIKACIJE?

Troškove mjera certificiranja, kao i troškove ispravljanja nedostataka otkrivenih tijekom postupka certifikacije, u cijelosti snosi trgovac ili ovlaštena treća strana.

ŠTO SE DOGAĐA AKO TRGOVAC NE ISHODI CERTIFIKACIJU?

Ako trgovac od kojega se to traži ne ishodi certifikaciju, SIX Payment Services ima pravo raskinuti ugovornu obvezu s trenutnim učinkom i potraživati nadoknadu za novčane kazne naplaćene od strane kartičnih organizacija i nadoknadu za gubitke koje potražuje izdavatelj kartice.

TKO IMA UVID U PODATKE O CERTIFIKACIJI?

Samo trgovac i tvrtka za certifikaciju imaju pravo uvida u podatke prikupljene u opsegu postupka certifikacije. Međutim, trgovac je dužan dostaviti sažetak rezultata certifikacije društvu SIX Payment Services, koje također ima pravo uvida u upitnike za samoprocjenu. S druge strane, kartične organizacije dobivaju samo statističke procjene.

KOLIKO ČESTO TREBA OBNAVLJATI CERTIFIKACIJU?

Certifikaciju treba obnavljati periodično, kako je prikazano u tablici dolje: Promjene koje provodi trgovac kao što je instalacija novog hardvera ili softvera, nova internetska stranica ili promjena pružatelja usluga platnog prometa, trgovac je dužan odmah prijaviti društvu SIX Payment Services. U nekim slučajevima bit će potrebno provesti novi postupak certifikacije.

KOJE SU TVRTKE OVLAŠTENE ZA PROVOĐENJE MJERA CERTIFIKACIJE?

Na internetu ćete pronaći popis svih ovlaštenih tvrtki:

- za provođenje procjene na lokaciji: pcisecuritystandards.org/pdfs/pci_qsa_list.pdf
- za provođenje mrežnih skenova: pcisecuritystandards.org/pdfs/asv_report.html

GDJE MOGU SAZNATI VIŠE O STANDARDU PCI DSS?

Dodatne informacije o standardu PCI DSS možete pronaći na sljedećim stranicama

- SIX Payment Services: six-payment-services.com/pci
- PCI Vijeće za sigurnosne standarde: pcisecuritystandards.org

TKO TREBA PODUZETI KOJE MJERE CERTIFIKACIJE?

Opis	razine	Visa, Mastercard/Maestro, Diners/Discover	JCB	American Express
1	trgovci s više od 6 milijuna transakcija godišnje	• godišnja procjena na lokaciji [1] • kvartalni mrežni sken		
	trgovci nakon pretrpljenih hakerskih napada sa zloupotrijebljenim kartičnim podacima			
	trgovci s više od 2,5 milijuna transakcija godišnje			• godišnja procjena na lokaciji • kvartalni mrežni sken
	trgovci s više od 1 milijun transakcija godišnje		• godišnja procjena na lokaciji • kvartalni mrežni sken	
2	trgovci s 1–6 milijuna transakcija godišnje	• godišnji upitnik o samoprocjeni [2] • kvartalni mrežni sken		
	trgovci s 50.000–2,5 milijuna transakcija godišnje			• kvartalni mrežni sken
3	trgovci u e-trgovini s 20.000–1 milijuna transakcija godišnje	• godišnji upitnik o samoprocjeni • kvartalni mrežni sken		
	trgovci s manje od 50.000 transakcija godišnje			• kvartalni mrežni sken
4	trgovci u e-trgovini s manje od 20.000 transakcija godišnje	• godišnji upitnik o samoprocjeni • kvartalni mrežni sken	• godišnji upitnik o samoprocjeni • kvartalni mrežni sken	
	trgovci (isključujući e-trgovinu) s manje od 1 milijun transakcija godišnje			

[1] Trgovac može odlučiti želi li da se procjena na lokaciji provede uz pomoć kvalificiranog procjenitelja sigurnosti (QSA) ili unutarnjeg procjenitelja sigurnosti (ISA).
[2] Upitnik o samoprocjeni mora bit certificiran od strane unutarnjeg procjenitelja sigurnosti (ISA).

Procjene na lokaciji i/ili mrežni skenovi obvezni su samo za trgovce koji obrađuju, prenose ili pohranjuju podatke o nositeljima kartice u elektroničkom obliku. Bez obzira na to, međutim, preporučujemo da se te mjere provjere ipak provedu, pogotovo za trgovce sa složenim infrastrukturama sustava. Trgovci moraju uvijek slijediti smjernice PCI DSS, ali dokaz o sukladnosti moraju dostaviti samo na pisani zahtjev društva SIX Payments Services.

SVOJU LOKALNU OSOBU ZA KONTAKT MOŽETE PRONAĆI NA SLJEDEĆOJ POVEZNICI:
six-payment-services.com/contacts

six-payment-services.com
worldline.com

110.0110.12 INT_HR/07.2020