Digital Payments
for a Trusted World

WORLDLINE

Útmutatás szerződő partnerek részére a PCI DSS biztonsági előírások betartásáról

Világszerte az összes kártyaadatokat továbbító, feldolgozó vagy tároló szerződő partner köteles betartani a Payment Card Industry Data Security Standard (PCI DSS) szabványban lefektetett biztonsági irányelveket. Ezek figyelmen kívül hagyása esetén a Worldline jogosult a szerződéses jogviszonyt azonnali hatállyal felmondani, és az esetleges bírságok és követelések erejéig kártérítési igényt érvényesíteni.

Az alábbi útmutatások műszaki és szervezési irányelvként a Worldlinezel kötött összes szerződés kötelező érvényű elemét képezik.

MIT TARTALMAZ A PCI DSS?

A PCI DSS 12 kötelező érvényű követelményből áll, melyek a kártyaadatok védelmét biztosítják a feldolgozás, a tárolás és a továbbítás során. A PCI DSS gyakorlati megvalósítását a kártyaszervezetek biztonsági programjai – így a Visa AIS, a Mastercard SDP, valamint az American Express, a Discover (Diners Club) és a JCB megfelelő programjai – szabályozzák.

MIÉRT VEZETTÜK BE A PCI DSS SZABVÁNYT?

Az elmúlt években jelentősen megnövekedett a kártyaadatlopások száma. A lopott kártyaadatokkal történő visszaélések minden érintett számára jelentős károkat okoznak.

MI A PCI DSS CÉLJA?

A kártyaszervezetek a PCI DSS révén tovább kívánják növelni a kártyás fizetések biztonságát, és ezáltal védeni a kereskedőket, a kártyabirtokosokat és az iparág egészét a kártyaadatlopások és az adatokkal történő visszaélések által okozott károktól.

KINEK KÖTELEZŐ BETARTANIA A PCI DSS ELŐÍRÁSAIT?

A PCI DSS alapján világszerte minden olyan szerződő partner köteles hatásos biztonsági intézkedéseket foganatosítani és betartani, aki kártyaadatokat továbbít, dolgoz fel vagy tárol.

A szerződő partnerek ezenfelül felelősek azért, hogy az általuk megbízott harmadik felek, például pénzforgalmi szolgáltatók (Payment Service Provider, PSP) vagy adattárolási szolgáltatók (Data Storage Entity, DSE), akik a nevükben adatokat továbbítanak, dolgoznak fel vagy tárolnak, szintén betartsák ezeket a bizton-sági irányelveket.

Ezzel kapcsolatban tanulmányozza a kártyaelfogadásra vonatkozó általános szerződési feltételek adatvédelemre és felelősségre vonatkozó rendelkezéseit.

KI A FELELŐS A PCI DSS BETARTÁSÁÉRT?

Alapvetően minden szerződő partner saját hatáskörében felelős a biztonsági előírások betartásáért. A kártyaszervezetek azonban megkövetelik, hogy a szerződő partnerek nyilatkozzanak az általuk foganatosított biztonsági intézkedésekről (tanúsíttassák őket). A nyilatkozat (tanúsítás) hatálya függ a tranzakciók számától és attól is, hogy a szerződő partner a továbbítás, a feldolgozás vagy a tárolás során kerül-e kapcsolatba a kártyaadatokkal.

MILYEN TANÚSÍTÁSI LEHETŐSÉGEKET ALKALMAZ A SZABVÁNY?

A PCI DSS keretében háromféle tanúsítási lehetőség áll rendelkezésre (lásd a hátoldalon lévő táblázatot is):

- **Önértékelési kérdőív (Self-Assessment Questionnaire, SAQ)**
  Egy önértékelési kérdőívet kell kitölteni.
- **Hálózatvizsgálat (Network Scan)**
  Egy akkreditált ellenőrző cég (Approved Scanning Vendor) negyedévente és a szerződő partnerrel történt egyeztetés után nem ellenséges szándékú feltörési kísérleteket végez a rendszer esetleges gyenge pontjainak felkutatására.
- **Helyszíni ellenőrzés**
  A nagy mennyiségű tranzakciót lebonyolító vagy kártyalopás áldozatául esett szerződéses partnerek kötelesek megfelelőségi jelentést (Report on Compliance, ROC) készíteni. Az eredményeket minősített biztonsági szakértőnek (Qualified Security Assessor, QSA) vagy képzett belső auditornak (Internal Security Assessor, ISA) kell ellenőriznie és igazolnia.

Amennyiben egy szerződő partner nem felel meg minden feltételnek a tanúsítás során, úgy köteles a biztonsági intézkedéseit az adott területeken haladéktalanul kijavítani.

KI VISELI A TANÚSÍTÁS KÖLTSÉGEIT?

A tanúsítás költségeit a szerződő partner, illetve a megbízott harmadik fél viseli; ugyanígy az ellenőrzés során megállapított hiányosságok elhárításának költségei is őket terhelik.

MI TÖRTÉNIK, HA A SZERZŐDŐ PARTNER NEM TESZ ELEGET TANÚSÍTÁSI KÖTELEZETTSÉGÉNEK?

Amennyiben egy tanúsításra kötelezett szerződő partner nem tesz eleget kötelezettségének, úgy a Worldline jogosult a vele fennálló szerződéses jogviszonyt azonnali hatállyal felmondani, és a kártyaszervezetek bírságait, illetve a kártyakibocsátók követeléseit kártérítés jogcímén követelni.

KI TEKINTHET BE A TANÚSÍTÁSI ADATOKBA?

A tanúsítás során gyűjtött adatokba kizárólag a szerződő partner és a tanúsítással megbízott cég tekinthet be, a szerződő partner azonban köteles a tanúsítási eredmények összefoglalását a Worldline számára is megküldeni. A Worldline ezenfelül az önértékelési kérdőívekbe is betekinthet. A kártyaszervezetek azonban csak statisztikai értékelést kapnak.

MILYEN GYAKRAN KELL MEGÚJÍTANI A TANÚSÍTÁST?

A tanúsítási intézkedéseket az alábbi táblázatban megadott időközönként meg kell ismételni. Amennyiben a szerződő partnernél változások történnek, például új hardvert vagy szoftvert telepítenek, új honlapot készítenek vagy szolgáltatót váltanak, úgy ezeket haladéktalanul be kell jelenteni a Worldlinenek. Adott esetben ez új tanúsítást tehet szükségessé.

MILYEN CÉGGEL KELL VÉGEZTETNI A TANÚSÍTÁST?

Az akkreditált tanúsító cégek teljes listáját megtalálja az interneten.

- Helyszíni ellenőrzést végző cégek: pcisecuritystandards.org/pdfs/pci_qsa_list.pdf
- Hálózatvizsgálatot végző cégek: pcisecuritystandards.org/pdfs/asv_report.html

HOL TALÁLOK TOVÁBBI INFORMÁCIÓT A PCI DSS-RŐL?

A PCI DSS-ről a következő forrásokban talál további információt:

- Worldline: worldline.com/merchant-services/pci
- PCI Security Standards Council: pcisecuritystandards.org

KINEK MILYEN TANÚSÍTÁSI INTÉZKEDÉSEKRE VAN SZÜKSÉGE?

Szint	Megnevezés	Visa, Mastercard/Maestro, Diners/Discover	JCB	American Express
1	Évente 6 milliónál több tranzakciót lebonyolító kereskedők	• évente helyszíni ellenőrzés[1] • negyedévente hálózatvizsgálat		
	Kártyaadat-eltulajdonításnak áldozatul esett kereskedők			
	Évente 2,5 milliónál több tranzakciót lebonyolító kereskedők			• évente helyszíni ellenőrzés • negyedévente hálózatvizsgálat
	Évente 1 milliónál több tranzakciót lebonyolító kereskedők		• évente helyszíni ellenőrzés • negyedévente hálózatvizsgálat	
2	Évente 1–6 millió tranzakciót lebonyolító kereskedők	• évente önértékelési kérdőív[2] • negyedévente hálózatvizsgálat		
	Évente 50 000–2,5 millió tranzakciót lebonyolító kereskedők			• negyedévente hálózatvizsgálat
3	Évente 20 000–1 millió tranzakciót lebonyolító E-Commerce kereskedők	• évente önértékelési kérdőív[2] • negyedévente hálózatvizsgálat		
	Évente 50 000-nél kevesebb tranzakciót lebonyolító kereskedők			• negyedévente hálózatvizsgálat
4	Évente 20 000-nél kevesebb tranzakciót lebonyolító E-Commerce kereskedők	• évente önértékelési kérdőív[2] • negyedévente hálózatvizsgálat	• évente önértékelési kérdőív[2] • negyedévente hálózatvizsgálat	
	Évente 1 milliónál kevesebb tranzakciót lebonyolító kereskedők (kivéve E-Commerce)			

[1] A kereskedő dönthet, hogy a helyszíni ellenőrzést minősített biztonsági szakértő (Qualified Security Assessor, QSA) vagy képzett belső auditor (Internal Security Assessor, ISA) támogatásával szeretné-e végrehajtani.

[2] Az önértékelési kérdőív (Self Assessment Questionnaire, SAQ) kitöltőjének belső auditori (Internal Security Assessor, ISA) tanúsítvánnyal kell rendelkeznie.

Helyszíni ellenőrzésre és/vagy hálózatvizsgálatra csak a kártyaadatok elektronikus feldolgozását, továbbítását vagy tárolását végző szerződő partnerek kötelesek. Azonban ettől függetlenül is javasoljuk, különösen a komplex infrastruktúrával rendelkező szerződő partnereknek, hogy végeztessék el a hitelesítési intézkedéseket. A szerződő partnerek minden esetben kötelesek betartani a PCI DSS szabályait, betartásukat azonban csak a Worldline írásos felszólítása ellenében kell igazolniuk.

Helyi kapcsolattartóját megtalálja a: worldline.com/merchant-services/contacts

110.00110.61 INT_HU/11.2021