Whitepaper PCI DSS

Hoe gaat u veilig en verantwoord om met de betaalkaartgegevens van uw klanten?

PaySquare

Inhoud

Inleiding

Vertrouwen winnen

U geeft uw klanten graag de gelegenheid om met een creditcard of internationale debetpas te betalen. Dankzij het betaalgemak en de veiligheid van betaalkaarten verlaagt u de koopdrempel voor uw klanten. Met andere woorden: creditcards en debetpassen accepteren levert u meer omzet op. Maar voor u als ondernemer houdt dat ook een verantwoordelijkheid in.

De kaarthouder gaat ervan uit dat zijn of haar kaartgegevens bij u in goede handen zijn. Als ontvanger van de betaling bent u mede verantwoordelijk voor de beveiliging van die gegevens. Om het u gemakkelijk te maken, hebben de grote betaalkaartmaatschappijen, onder wie Visa en MasterCard, een beveiligingsstandaard ontwikkeld: de Payment Card Industry Data Security Standard (PCI DSS). Als ondernemer kunt u alleen kaartbetalingen accepteren als u voldoet aan de eisen van PCI DSS. Ook uw leveranciers, zoals Payment Service Providers (PSP's) en betaalautomaatleveranciers, moeten zich houden aan de PCI DSS-voorschriften. Zo leveren we met elkaar een belangrijke bijdrage aan het veiliger maken van uw betalingsverkeer. Uiteraard brengt PCI DSS voor u een aantal verplichtingen met zich mee, maar daar staat een voordeel tegenover dat uiteindelijk veel waardevoller is: een klant die vol vertrouwen bij u koopt. En u beschermt uw onderneming tegen de kosten en boetes die kunnen ontstaan door diefstal en misbruik van kaartgegevens.

Deze PaySquare whitepaper geeft u inzicht in de achtergronden van PCI DSS. U leest erin hoe u het vertrouwen van uw klanten kunt vergroten en u krijgt een overzicht van de stappen die u moet zetten om te voldoen aan de beveiligingsstandaard. Daarnaast vindt u informatie over waar u als ondernemer wel en niet verantwoordelijk voor bent.

Definitie

Wat is PCI DSS?

Om een duidelijk kader te creëren voor de beveiliging van betaalkaartgegevens, hebben de grote betaalkaartmaatschappijen een aantal richtlijnen opgesteld voor alle partijen die deel uitmaken van het betalingsverkeer met betaalkaarten. Die richtlijnen vormen samen de Payment Card Industry Data Security Standard (PCI DSS).

Primary Account Numbers

- PCI DSS heeft uitsluitend betrekking op situaties waarin Primary Account Numbers (PANs), oftewel volledige kaartnummers, worden opgeslagen, verwerkt, verstuurd of ontvangen. Voor andere kaartgegevens (zoals de naam van de kaarthouder en de vervaldatum) hoeft u alleen beschermende maatregelen te treffen als u ze samen met de gerelateerde kaartnummers verwerkt of opslaat. Authenticatiegegevens als de CVC (Card Validation Code) dan wel CVV (Card Verification Value) (die op de achterkant van elke creditcard staan) en de pincode mag u in geen enkel geval opslaan.

  In het algemeen geldt: sla zo min mogelijk kaartgegevens op. De figuur hieronder laat duidelijk zien welke kaartgegevens u wel en niet mag opslaan. Het voorbeeld laat een MasterCard zien, maar het geldt voor alle betaalkaarten.

Kaartgegevens die beschermd moeten worden:

Gevoelige Authenticatie Data: mogen onder geen omstandigheid worden opgeslagen:

- Card track gegevens (= volledige kaartinformatie zoals opgeslagen in bijvoorbeeld de magneetstrip 1 en/of chip 2)
- Card Verification Code (3-cijferige code (CVC2, CVV2) op de achterkant in de handtekeningstrip 3
- Pincode

Kaarthoudergegevens die mogen worden opgeslagen (mits conform de PCI DSS voorschriften) indien dit nodig is voor de bedrijfsvoering:

- PAN (Primary Account Number = Volledige kaartnummer 4)
- Naam van de kaarthouder 5
- Vervaldatum 6

De volgende gegevens mogen onversleuteld worden opgeslagen, mits losgekoppeld van overige kaarthoudergegevens:

- Transactiebedrag, transactiedatum, transactie autorisatiecode

De basisstandaard

PCI DSS is inmiddels uitgegroeid tot de basisstandaard voor het beschermen van kaarthoudergegevens. De standaard is bedoeld om ondernemers te helpen bij het opstellen en uitvoeren van een doeltreffend beveiligingsbeleid Om betaalkaarten te kunnen accepteren, moet u dan ook voldoen aan de PCI DSS-eisen. Voldoet u aan PCI DSS, dan beschermt u uw klanten en verstevigt u het fundament onder uw onderneming.

Aansprakelijkheid

Als u in gebreke blijft bij het beveiligen van de kaartgegevens van uw klanten, kunt u daarmee de deur openzetten voor kwaadwillenden. Als gevolg daarvan kan de schade hoog oplopen. U bent aansprakelijk voor de directe verliezen die voortkomen uit het gebruik van vervalste betaalkaarten en/of het gebruik van gestolen kaartgegevens. Maar bijvoorbeeld ook voor de juridische kosten, de kosten voor het vervangen van betaalkaarten, voor het onderzoek en imagoschade. Daarnaast bestaat de mogelijkheid dat de kaartorganisatie u een boete oplegt en u uitsluit van het accepteren van betaalkaarten. Ook als het gaat om aansprakelijkheid is er dus alle reden om te voldoen aan de richtlijnen van PCI DSS.

Doelstellingen

Wat is het doel van PCI DSS?

Met PCI DSS hebben de betaalkaartmaatschappijen u niet op goed geluk een aantal voorschriften opgelegd. Integendeel. De beveiligingsstandaard is gebaseerd op een aantal heldere doelstellingen voor úw onderneming. Door die doelstellingen te realiseren, kan uw klant in uw winkel of op uw website snel, makkelijk en veilig betalen met een internationale betaalkaart.

De PCI DSS-doelstellingen:

1. Een betaalnetwerk tot stand brengen dat veilig is en veilig blijft.
2. De gegevens van de kaarthouder (uw klant) beschermen.
3. Een programma opzetten en onderhouden waarmee u kwetsbaarheden in het betaalsysteem kunt beheersen.
4. De toegang tot kaartgegevens van uw klanten tot een minimum beperken.
5. Een betrouwbare IT-infrastructuur opzetten en onderhouden.
6. Een praktisch en doelmatig informatiebeveiligingsbeleid voeren.

PCI DSS eisen

Hoe realiseert u de PCI DSS-doelstellingen?

Bij iedere eis die deel uitmaakt van PCI DSS horen praktische maatregelen om de doelstellingen te realiseren. Afhankelijk van de wijze waarop u betalingen accepteert zijn meer of minder van deze maatregelen van toepassing voor u. Daar waar nodig kunt u voor de uitvoering van de verschillende maatregelen veelal terecht bij uw leveranciers (zoals uw PSP, betaalautomaatleverancier, software-leveranciers etc).

De PCI DSS-eisen:

Een veilig betaalnetwerk

- Maatregel 1: U installeert en onderhoudt een firewall.
- Maatregel 2: U gebruikt géén standaard-wachtwoorden van uw systeemleverancier.

Kaartgegevens beschermen

- Maatregel 1: Sla betaalkaartgegevens alléén op als dat echt nodig is. Als opslag onvermijdelijk is voor uw bedrijfsvoering, zorg dan voor goede beveiliging van die gegevens.
- Maatregel 2: Verstuurt u de kaartgegevens van uw klanten via openbare netwerken, zorg dan voor een goede encryptie.

Kwetsbaarheden beheersen

- Maatregel 1: Gebruik anti-virussoftware en zorg voor regelmatige updates.
- Maatregel 2: Beveilig uw systemen en applicaties en onderhoud de beveiliging regelmatig.

Toegangsbeperking

- Maatregel 1: Geef medewerkers toegang tot kaartgegevens op een need-to-know basis.
- Maatregel 2: Geef iedere medewerker die toegang heeft een unieke gebruikersnaam en wachtwoord.
- Maatregel 3: Beperk de fysieke toegang tot kaartgegevens.

Monitoring van uw IT-infrastructuur

- Maatregel 1: Bewaak de toegang tot alle relevante IT-componenten en kaarthoudergegevens – en controleer de bewaking regelmatig.
- Maatregel 2: Test alle beveiligingscomponenten en -processen regelmatig.

Informatiebeveiligingsbeleid

- Maatregel 1: Stel een beleid op dat informatiebeveiliging als uitgangspunt heeft – en toets de praktijk regelmatig aan dat beleid.

Vier categorieën

Wat voor ondernemer bent u?

Ondernemers zijn er in veel soorten en maten. De betaalkaartmaatschappijen hebben daar rekening mee gehouden bij het opstellen van de PCI DSS-eisen. Voor PCI DSS zijn vier bedrijfscategorieën vastgesteld. Op basis van het aantal kaartbetalingen dat u ontvangt en de manier waarop u de betalingen accepteert, kunt u vaststellen in welke categorie uw onderneming valt. Voldoet u aan de eisen die gelden voor uw categorie, dan mag u zichzelf 'PCI DSS compliant' noemen.

Categorie	Kenmerken	Verplichte PCI DSS-handeling
Level 1 Fysieke winkels en kopen op afstand (e-commerce, MO/TO)	Alle betaalkaart accepterende bedrijven met meer dan 6 mln Visa transacties, of Alle betaalkaart accepterende bedrijven met meer dan 6 mln MasterCard én Maestro transacties bij elkaar, of Alle betaalkaart accepterende bedrijven waar een data compromittatie heeft plaatsgevonden	Jaarlijkse PCI DSS evaluatie op locatie door PCI SSC (Security Standards Council) geaccrediteerd intern personeel of door PCI SSC erkende (externe) Qualified Security Assessor (QSA) Ieder kwartaal een netwerk-scan door een Approved Scanning Vendor (ASV)
Level 2 Fysieke winkels en kopen op afstand (e-commerce, MO/TO)	Alle betaalkaart accepterende bedrijven met meer dan 1 mln maar minder dan 6 mln Visa transacties, of Alle betaalkaart accepterende bedrijven met meer dan 1 mln maar minder dan 6 mln MasterCard én Maestro transacties bij elkaar	Jaarlijks een zelfbeoordeling (Self Assessment) door PCI-SSC (Security Standards Council) geaccrediteerd intern personeel of door PCI SSC erkende (externe) Qualified Security Assessor (QSA) + ieder kwartaal een netwerk-scan door een ASV
Level 3 (alleen e-commerce)	Betaalkaart accepterende bedrijven met meer dan 20.000 maar minder dan 1 mln Visa e-commerce transacties of Betaalkaart accepterende bedrijven met meer dan 20.000 maar minder dan 1 mln MasterCard én Maestro e-commerce transacties bij elkaar	Jaarlijks een Self Assessment Questionnaire (SAQ) + ieder kwartaal een netwerk-scan door een ASV
Level 4	Alle overige betaalkaart accepterende bedrijven	(Beleid kan per Acquirer verschillen) Jaarlijks een Self Assessment Questionnaire (SAQ) + ieder kwartaal een netwerk-scan door een ASV

Praktijk (1)

Hoe voldoet u aan de PCI DSS-eisen?

Als u aan de slag gaat met PCI DSS is uw gezond verstand het belangrijkste instrument. Voordat u zich in de exacte voorschriften verdiept, is het goed om na te gaan wat de algemene bedoelingen van de beveiligingsstandaard zijn. In veel gevallen legt u daarmee al een stevige basis onder uw PCI DSS-project.

Van start met de SAQ

De Self Assessment Questionnaire (SAQ) is een prima beginpunt als u voor het eerst een PCI DSS-traject gaat doorlopen. Er zijn 5 verschillende vragenlijsten. Welke lijst voor u van toepassing is hangt af van de manier waarop uw onderneming kaartbetalingen accepteert. Neemt u de vragen door, dan krijgt u een goed beeld van uw vorderingen op weg naar een veilig betalingsverkeer. Voldoet u nu al aan de eisen, dan kunt u de SAQ volledig invullen en indienen bij uw acquirer .

Wilt u al aan de slag met PCI DSS en bent u klant bij PaySquare, dan kunt u bij de afdeling Merchant Services direct een wachtwoord opvragen voor de PCI DSS-pagina van PaySquare.
Via https://pci.paysquare.nl/Default.aspx vindt u de vragenlijst die past bij uw onderneming.

In de meeste gevallen zal uw onderneming niet direct voldoen aan alle PCI DSS-eisen. In dat geval kunt u binnen uw bedrijf een begin maken met het nemen van maatregelen of het PCI DSS-project uitbesteden aan een externe onderneming. Op de website van de PCI Security Standards Council (SSC) vindt u onder https://www.pcisecuritystandards.org/approved_companies_providers/index.php alle ondernemingen en betaalsoftware die door de SSC gecertificeerd zijn om u te ondersteunen bij PCI-DSS projecten.

Praktische tips voor een succesvol PCI DSS-traject

- **Ga vandaag nog van start**
  Als u vroeg begint, bespaart u kosten en neemt u een voorsprong op uw concurrenten.
- **Sla gegevens niet onnodig op**
  PCI DSS is de beveiligingsstandaard voor het opslaan, verwerken en verzenden van kaartgegevens. Maar in veel gevallen is het opslaan van kaartgegevens helemaal niet nodig. Inventariseer welke gegevens u wilt en/of moet opslaan en of dat misschien gebeurt zonder dat u het weet. In het algemeen geldt: If you don't need it, don't store it!
- **Maak beleid**
  Een helder beleid op het gebied van betaalkaartgegevens is een basis om op terug te vallen. Stel procedures op voor het opslaan, verwerken en versturen van kaartgegevens.
- **Vergelijk voorschriften**
  Het is mogelijk dat u zich bij het opslaan van betaalkaartgegevens nu al moet houden aan bepaalde (wettelijke) voorschriften, zoals die voortkomen uit de Wet Bescherming Persoonsgegevens. Al in een vroeg stadium kunt u nagaan of die voorschriften wel in lijn liggen met de PCI DSS-eisen.

- **Maak een gap analysis**
  Voor PCI DSS heeft u gespecialiseerde kennis nodig. Bekijk voor ieder afzonderlijk voorschrift of de benodigde kennis aanwezig is in uw bedrijf. Is dat niet het geval, schakel dan externe deskundigen in.
- **Overleg met uw leveranciers en leg afspraken vast**
  Als u wilt voldoen aan de PCI DSS-eisen, moeten ook leveranciers van hardware en software die betaalkaartgegevens namens u verwerken of verzenden voldoen aan PCI DSS-regels. Gaat u er nooit zomaar van uit dat uw leveranciers (ook) voldoen aan PCI DSS , maar maak daar concrete afspraken over. Vraag om bewijs en leg de afspraken contractueel vast. Op de website van de PCI Security Standards Council (PCI SSC) kunt u onder https://www.pcisecuritystandards.org/approved_companies_providers/index.php tevens controleren of uw leverancier en/of de door hem bij u geïnstalleerde hard-/en software door de SSC zijn goedgekeurd.
- **Neem contact op met uw leveranciers**
  Track data (de volledige kaartinformatie in de magneetstrip of chip van een betaalkaart) mag u in geen enkel geval opslaan. Met die informatie is het betrekkelijk eenvoudig om illegale kaartkopieën te maken. Ook autorisatie- en authenticatie-gegevens mag u nooit opslaan. Sommige apparatuur slaat deze informatie onbedoeld toch op. Vraag bij uw hardware- en betaalsoftware leverancier(s) na of dat ook bij uw betaalautomaat of betaalinfrastructuur het geval kan zijn.
- **Ontdek de data**
  Ga op zoek naar alle gegevens die voor PCI DSS relevant zijn. Identificeer alle betaalkanalen en datastromen en maak een overzicht van alle locaties waar kaartgegevens terecht (kunnen) komen.
- **Maak van encryptie een gewoonte**
  Als u kaartgegevens verstuurt, moet dat altijd versleuteld gebeuren.
- **Gebruik alleen beveiligde WiFi-netwerken**
  Een onbeveiligd draadloos netwerk is niet geschikt om kaartgegevens te versturen.
- **Train uw mensen**
  Niet iedere medewerker hoeft een PCI Qualified Security Assessor (QSA) te zijn, maar het is wél belangrijk dat iedere medewerker weet wat er nodig is om aan de PCI DSS-eisen te voldoen.
- **Let op uw POS-systemen**
  Point-of-salesystemen (bijvoorbeeld de koppeling van uw kassa met een betaalautomaat en uw administratieve software) vormen vaak een kwetsbare plek als het gaat om de beveiliging van kaartgegevens. Zorg ervoor dat uw POS-systeem geen volledige kaartgegevens opslaat en zeker geen Card Verification Value/Code. Het is ook niet toegestaan om het volledige 16-cijferige creditcardnummer op een bon te tonen.
- **Beveilig de systemen ook fysiek**
  Zorg ervoor dat alleen uw eigen, bevoegde medewerkers aan uw betaalsystemen kunnen komen.
- **Registreer het proces**
  Houd in een ‘logboek’ bij welke stappen u neemt om te voldoen aan de PCI DSS-voorschriften.

Praktijk (2)

Hoe blijft u voldoen aan de PCI DSS-eisen?

Als uw betalingsverkeer voldoet aan de PCI DSS-voorschriften, heeft u uzelf én uw klanten verzekerd van een veilig en verantwoord betalingsverkeer. Vervolgens is het aan u om ervoor te zorgen dat de manier waarop u omgaat met betaalkaartgegevens ook in de toekomst in overeenstemming is met de standaardeisen.

Praktische tips om PCI DSS compliant te blijven

- **Blijf herhalen**
  Breng het onderwerp PCI DSS regelmatig (opnieuw) onder de aandacht van uw medewerkers. Stel duidelijke en eenvoudige richtlijnen op.
- **Beperk de toegang**
  Blijf de toegang tot kaartgegevens beperken. Alleen medewerkers van wie u zeker weet dat zij echt met de gegevens moeten werken, krijgen een gebruikersnaam-wachtwoordcombinatie.
- **Wis regelmatig**
  Controleer op vaste tijden welke gegevens van klanten u niet (meer) nodig heeft en wis die data direct.
- **Stel een worst case scenario op**
  Zorg ervoor dat er niets mis kan gaan met de kaartgegevens van uw klanten. En wees erop voorbereid dat het tóch gebeurt. Bedenk wat u en uw medewerkers in zo'n situatie te doen staat. Stel noodscenario's op.
- **Blijf controleren**
  Loop regelmatig de systeembeveiliging en de controlejournaals na.

Samen fraude bestrijden (2)

Waar begint en eindigt uw verantwoordelijkheid?

Betalen met een betaalkaart is makkelijk, veilig en efficiënt. Uw klanten vertrouwen erop, dat u voor het inrichten van uw betalingsverkeer werkt met veilige technische voorzieningen en met betrouwbare partners en leveranciers.

Met PCI DSS ondersteunen de betaalkaartmaatschappijen uw inspanningen om de kaartgegevens van uw klanten optimaal te beschermen. Uw verantwoordelijkheid voor de beveiliging van die gegevens heeft betrekking op de volgende aspecten van het betalingsverkeer:

- De apparatuur die u gebruikt om creditcards en andere betaalkaarten van uw klanten te lezen.
- De betaalautomaten die u in uw winkel(s) gebruikt (POS-systemen).
- De netwerken en hardware die een rol spelen in uw betalingsverkeer (servers, draadloze routers, modems etc.).
- De opslag, verwerking en verzending van betaalkaartgegevens.
- De beveiliging van hardware en software van alle partijen die u bij uw betalingsverkeer betrekt.
- Fysieke toegang tot belangrijke IT-componenten en kaarthoudergegevens.

Uw leveranciers hebben hun eigen beveiligingsstandaarden

Uiteraard bent u als ondernemer niet de enige die verantwoordelijk is voor een veilig betalingsverkeer. Ook andere betrokken partijen hebben een rol en moeten PCI DSS compliant zijn. Zo heeft u bijvoorbeeld een betaalautomaat of internetkassa nodig en betalingssoftware. Voor de fabrikanten en leveranciers van betaalautomaten en voor betaalsoftwareleveranciers zijn afzonderlijke beveiligingsstandaarden ontwikkeld. Volgens de PCI DSS-eisen moet u altijd gebruik maken van een betaalautomaat/-applicatie en werken met een softwareleverancier die aan deze standaarden voldoen. Op https://www.pcisecuritystandards.org/approved_companies_providers/index.php vindt u een lijst met aanbieders van gecertificeerde betaalapplicaties en leveranciers.

PCI DSS – en verder?

Als u voldoet aan de PCI DSS-eisen, levert u een prima bijdrage aan de bescherming van gegevens die voor uw klanten van groot belang zijn. Maar uiteraard maakt de beveiligingsstandaard van de betaalkaartmaatschappijen andere (wettelijke) voorschriften niet overbodig. Zo bent u bij het opslaan, verwerken en versturen van kaartgegevens van uw klanten ook gehouden aan de Wet Bescherming Persoonsgegevens. Hierover is meer te lezen op www.rijksoverheid.nl/persoonsgegevens. Die wet verplicht u zorgvuldig en veilig om te gaan met de gegevens van uw klanten, maar stelt bijvoorbeeld ook beperkingen aan de manieren waarop u de gegevens van uw klanten mag gebruiken voor commerciële activiteiten.

Risico's

Met welke vormen van fraude moet u rekening houden?

Fraude komt in diverse vormen voor. Iedere manier van acceptie van betaalkaarten brengt specifieke risico's met zich mee. En specifieke maatregelen om die risico's te verkleinen. In de PaySquare white-paper over fraude met creditcards en internationale betaalpassen vindt u meer informatie over hoe u fraude herkent en wat u ertegen kan doen. In het kader van PCI DSS lichten we hieronder enkele specifieke gevallen toe van mogelijke fraude.

Een stand-alonebetaalautomaat in de winkel

Zelfs als uw kassa en de betaalautomaat in uw winkel niet met elkaar verbonden zijn, bestaat weliswaar nog steeds het risico dat de betaalautomaat zelf of de dataverbinding wordt gemanipuleerd. Criminelen kunnen hierdoor de kaart- en/of transactiegegevens van uw klanten onderscheppen.

- **Wat kunt u doen?**
  Controleer uw betaalautomaat en de communicatieverbinding regelmatig op tekenen van manipulatie (liefst elke ochtend). Als u het vermoeden heeft dat onbevoegden uw betaalautomaat en/of aansluitingen en/of kabels hebben gemanipuleerd, kan uw leverancier u helpen.

Een betaalautomaat in de winkel die verbonden is met de kassa

Zijn uw kassa en uw betaalautomaat wel met elkaar verbonden, dan kan de communicatielijn en/of de betaalsoftware worden gehackt en daardoor kaartgegevens worden bemachtigd uit uw systeem. In het systeem kan dan schadelijke software ofwel malware worden geplaatst.

- **Wat kunt u doen?**
  Zorg voor voldoende beveiliging en gebruik bij de overdracht van gegevens een goede encryptie (versleuteling).

Een geïntegreerde betaalautomaat in de winkel

Ook als u gebruik maakt van een betaalautomaat en kassa in één, kan de communicatielijn worden gehackt. Omdat deze apparatuur vooral voorkomt bij ondernemers met meerdere vestigingen, is ook een hack in de verbindingen tussen filialen onderling en met het hoofdkantoor mogelijk.

- **Wat kunt u doen?**
  Maak goede afspraken met uw IT-leverancier. En controleer vooral of de producten van uw leverancier voldoen aan de door de PCI SSC gestelde voorschriften.

Een webwinkel die gebruik maakt van de betaalpagina van een PSP

Veel e-commerce-ondernemers maken voor kaartbetalingen gebruik van de betaalpagina van een PSP. Ook PSP's moeten hun werkwijze regelmatig laten toetsen aan de PCI DSS-eisen. Toch moet u er zélf op letten dat de PSP waarmee u werkt, de PCI DSS-voorschriften daadwerkelijk naleeft. Als de betaalpagina van uw PSP onzorgvuldig geconfigureerd is en toch kaartgegevens opslaat, kan dat gevolgen hebben voor úw klanten.

- **Wat kunt u doen?**
  Leg in het contract met uw PSP vast dat de betaalpagina altijd moet voldoen aan de PCI DSS-voorschriften. Zorg ook zelf voor goede beveiligingsmaatregelen zoals anti-virus software en firewalls, want anders blijft uw webwinkel kwetsbaar voor hackers.

Een webwinkel met een eigen betaalpagina

E-commerce-ondernemers met een eigen betaalpagina lopen (te) veel risico.

- **Wat kunt u doen?**
  Door veel acquirers worden e-commerce-ondernemers met een eigen betaalpagina (dus niet van een PSP) niet toegelaten. Maak gebruik van een betaalpagina van een PSP die voldoet aan PCI DSS om fraude- en beveiligingsrisico's tot een minimum te beperken.

Creditcardacceptatie voor MO/TO

Als u gebruik maakt van postorder of telefonische verkoop (MO/TO), kunt u via een door PaySquare geselecteerde PSP onder strikte voorwaarden creditcardgegevens handmatig invoeren. Daarbij creëert u risico's als u kaartgegevens opslaat of per e-mail (of via een website) met uw klanten communiceert.

- **Wat kunt u doen?**
  Sla geen creditcardgegevens van uw klanten op. En zorg bij communicatie rondom de bestelling voor een goede encryptie van de verstuurde informatie.

Opheldering

Misverstanden over PCI DSS

Er bestaan nogal wat misverstanden over de beveiliging van kaartgegevens. En over PCI DSS. We nemen er graag een aantal weg.

Misverstand 1
PCI DSS is een aanbeveling en geen voorschrift.
Betaalkaartmaatschappijen hebben het recht om te bepalen hoe u als ondernemer moet omgaan met kaartgegevens. U moet dus voldoen aan de PCI DSS-eisen om betalingen met betaalkaarten te kunnen accepteren.

Misverstand 2
Een scan door een ASV is alles wat ik nodig heb om PCI DSS compliant te zijn.
De security scan, uitgevoerd door een Approved Scanning Vendor, is maar een onderdeel van de PCI DSS-procedure. Als ondernemer moet u in de meeste gevallen ook jaarlijks een Self Assessment Questionnaire invullen. Zie op https://pci.paysquare.nl welke voorwaarden PaySquare stelt voor de bij haar aangesloten klanten.

Misverstand 3
Ik accepteer zo weinig kaartbetalingen dat ik niet aan de PCI DSS-eisen hoef te voldoen.
Zelfs voor het accepteren van slechts één kaartbetaling moet uw onderneming al voldoen aan de PCI DSS-voorschriften.

Misverstand 4
Ik bewaar geen kaartgegevens, dus PCI DSS geldt niet voor mij.
PCI DSS is de beveiligingsstandaard voor het opslaan, verwerken én versturen van kaartgegevens. U moet daarom wél voldoen aan de meeste PCI DSS-voorschriften. Overigens: weet u héél zeker dat u geen kaartgegevens bewaart?

Misverstand 5 (zie tabel p.8)
Een kleine onderneming krijgt nooit een boete van een betaalkaartmaatschappij.
Als in uw bedrijf kaartgegevens worden gestolen, moet u kunnen aantonen dat u op het moment van de diefstal heeft voldaan aan de PCI DSS-eisen. Kunt u dat niet, dan wordt de schade op u verhaald, ongeacht de omvang van uw onderneming. Daarnaast kunt u onder meer worden uitgesloten van het accepteren van kaartbetalingen en in een hogere Merchant Level-categorie (zie tabel p.9) terecht komen, met scherpere verplichtingen en hogere auditkosten.

Misverstand 6.

PCI DSS is alleen van toepassing op e-commerce.

Elke ondernemer die kaartgegevens opslaat, verwerkt en/of verzendt, moet voldoen aan de PCI DSS-eisen. Dus ook fysieke winkels (points-of-sale) en ondernemers die gebruikmaken van postorder en telefonische verkoop (MO/TO).

Misverstand 7.

Met het indienen van een ingevulde Self Assessment Questionnaire is het PCI DSS-traject voltooid.

Het invullen van de SAQ is een momentopname. Als ondernemer moet u ook daarna voortdurend voldoen aan de PCI DSS-eisen. Gaat er bij u iets mis met betaalkaartgegevens, dan moet u kunnen aantonen dat u op dat moment PCI DSS-compliant was.

Misverstand 8.

PCI DSS laat te veel ruimte voor interpretatie.

De PCI DSS is de meest specifieke opsomming van beveiligingseisen die in de branche tot nu toe is opgesteld. In tegenstelling tot andere standaards op het gebied van beveiliging (SOX, ISO, ISO 27002) biedt PCI DSS méér dan een kader. De standaard beschrijft de eisen en procedures in detail.

Misverstand 9.

Met een PA DSS-gecertificeerde applicatie voldoe ik aan de PCI DSS-eisen.

Het gebruik van een PA DSS-gecertificeerde applicatie is één stap. Vervolgens moet u alle eisen en controles implementeren die ervoor zorgen dat al uw netwerken en servers voldoen aan de PCI DSS-eisen. Heeft u het systeembeheer uitbesteed, dan moet de beheerder aan de eisen voldoen.

Terminologie

Het PCI DSS-woordenboek

Acquirer
Een acquirer verzorgt de afwikkeling van kaartbetalingen voor de ondernemer. De acquirer sluit daarvoor een licentieovereenkomst met een (internationale) kaartorganisatie.

Attestation of Compliance (AoC)
Verklaring van naleving, waarin je bevestigt dat je de SAQ naar waarheid hebt ingevuld.

Approved Scanning Vendor (ASV)
Een ASV voert scans uit bij bedrijven om IT-systemen en –netwerken van kaartaccepterende bedrijven te testen. Een ASV moet gecertificeerd zijn door de PCI Security Standards Council. Een lijst met gecertificeerde ondernemingen is te vinden op de website van de de PCI Security Council: www.pcisecuritystandards.org. De meeste IT-systemen en –netwerken moeten iedere drie maanden worden gescand. In de meeste gevallen kan dat op afstand gebeuren. Die procedure is vergelijkbaar met een virusscanner op uw PC.

Certificatie
Bij een certificatie onderzoekt een certificerende instantie of een ondernemer op het moment van certificering voldoet aan bepaalde regels en eisen.

Compliance
Het naleven van en/of voldoen aan bepaalde wetten en/of regels.

Compromittatie
Manipulatie, diefstal of verlies van data en/of systemen of de controle daarover, ten behoeve van misbruik.

Payment Service Provider (PSP)
Een PSP verzorgt de technische verbinding van een ondernemer met de acquirer en verwerkt kaarttransacties. Daarnaast levert een PSP andere producten en diensten voor de afwikkeling van de meest uiteenlopende soorten (elektronische) betalingen.

PCI DSS
Een geheel van voorschriften, opgesteld door de grote betaalkaartmaatschappijen (waaronder Visa en MasterCard) en bedoeld om betaalkaarten te beschermen tegen misbruik. Alle deelnemers in de keten van het betalingsverkeer met betaalkaarten (zoals ondernemers, acquirers, PSP's en IT-leveranciers) moeten aan de PCI-eisen voldoen.

Qualified Security Assessor (QSA)
Een IT beveiligings specialist, die door de PCI-SSC is geaccrediteerd om veiligheidscontroles (OnSite Assessments) uit te voeren bij kaartaccepterende en verwerkende bedrijven.

Safe-harbour-oplossing
Als een winkelier PCI DSS compliant is en toch slachtoffer wordt van een datacompromittatie, kan de betaalkaartmaatschappij onder bepaalde omstandigheden de opgelegde boetes verlagen of kwijtschelden.

Security Audit
Een fysieke veiligheidscontrole op de locatie van de ondernemer. Hierbij worden ook de serverruimtes geïnspecteerd en vinden er interviews plaats met medewerkers.

Security scan
Onderzoek om eventuele zwakke plekken in de IT-infrastructuur of de configuratie van systemen te ontdekken. Een security scan vindt in de meeste gevallen online plaats.

Self Assessment Questionnaire (SAQ)
Een SAQ is een vragenlijst waarmee een ondernemer informatie verstrekt aan zijn Acquirer met betrekking tot de implementatie van de PCI DSS-voorschriften in zijn bedrijf. De diverse bedrijfscategorieën hebben verschillende vragenlijsten. De vragenlijsten gaan in op de manier waarop de ondernemer kaartbetalingen accepteert en verwerkt en behandelen ook algemene bedrijfsinformatie, (contractuele) verbindingen met andere ondernemingen en technische details. Afhankelijk van de merchantcategorie (zie tabel pagina 9) moet de SAQ over het algemeen eens per jaar door de merchant worden ingevuld en bij de acquirer worden opgeleverd.

Meer informatie

Meer informatie
Meer informatie kunt u vinden op:
www.paysquare.nl
www.visa.com
www.mastercard.com
www.pcisecuritystandards.org

Aan de inhoud van deze whitepaper kunnen geen rechten worden ontleend. Deze informatie is verkregen uit algemeen toegankelijke bronnen. Druk- en zetfouten voorbehouden.

Als professioneel partner in het betalingsverkeer informeren wij u graag pro-actief en op objectieve wijze over het betalingsverkeer door middel van onze whitepapers. Hierin bieden wij oplossingen aan met betrekking tot zeer uiteenlopende onderwerpen, gerelateerd aan concrete behoeften in de markt. Naast 'PCI DSS' zijn inmiddels de whitepapers 'Chargebacks', 'Dynamic Currency Conversion voor fysieke winkels en webwinkels', 'De kassa van uw webwinkel', 'Fraude met creditcards en betaalpassen' en 'Interchange fee en commissie' verschenen. Alle whitepapers kunt u downloaden via http://www.paysquare.eu/nl/nl/ondernemers/meerinformatie/whitepapers/index.jsp.

PaySquare brengt regelmatig nieuwe whitepapers uit over uiteenlopende onderwerpen.
Via www.paysquare.nl/whitepaper blijft u op de hoogte van de nieuwste whitepapers.

10.01 NN 02.14

PaySquare SE
Eendrachtlaan 315
3526 LB Utrecht
Postbus 30600
3503 AJ Utrecht

T +31 (0)88 385 73 33
E service@paysquare.nl
W www.paysquare.nl
K.v.K. 30196418

PaySquare