PCI DSS - Beveiliging van kaartbetalingen

PCI DSS (Payment Card Industry Data Security Standard) is een set van veiligheidsregels voor het veilig verwerken van kaartbetalingen. Alle partijen die betrokken zijn bij kaartbetalingen (bv. handelaars, PSP's) moeten aan deze regels voldoen zodra ze kaartgegevens verwerken, doorsturen of opslaan.

De 12 basisvereisten van PCI DSS

Nr.	Vereiste	Doel
1	Installeer en onderhoud een **firewall-configuratie** om kaarthoudersgegevens te beschermen.	Beveilig de kaartgegevens tegen ongeoorloofde toegang.
2	Gebruik **geen standaardwachtwoorden** of beveiligingsinstellingen van leveranciers.	Voorkom kwetsbaarheden door zwakke standaardinstellingen.
3	Bescherm **opgeslagen kaarthoudersgegevens**.	Versleutel of maskeer gevoelige gegevens (bv. PAN, CVV).
4	Versleutel **transmissie van kaarthoudersgegevens** over openbare netwerken (bv. internet).	Voorkom onderschepping van gegevens tijdens verzending (bv. via TLS 1.2+).
5	Gebruik en update **regelmatig antivirussoftware**.	Bescherm tegen malware en kwaadaardige aanvallen.
6	Ontwikkel en onderhoud **veilige systemen en applicaties**.	Patch kwetsbaarheden (bv. via regelmatige updates).
7	Beperk **toegang tot kaarthoudersgegevens** tot "need-to-know"-basis.	Minimaliseer risico's door strenge toegangcontroles.
8	Ken een **unieke ID toe** aan elke persoon met computertoegang.	Zorg voor traceerbaarheid van acties (bv. via tweefactorauthenticatie).
9	Beperk **fysieke toegang** tot kaarthoudersgegevens.	Beveilig datacenters, servers en werkstations.
10	**Monitor en log** alle toegang tot netwerkbronnen en kaarthoudersgegevens.	Detecteer en onderzoek verdachte activiteiten.
11	**Test regelmatig** beveiligingssystemen en -processen.	Identificeer kwetsbaarheden via penetratietests en scans.
12	Onderhoud een **beleid voor informatiebeveiliging** voor medewerkers en aannemers.	Zorg voor bewustzijn en naleving binnen de organisatie.

Volledige PCI DSS-regels: PCI Security Standards Council

PCI DSS-certificering: Hoe wordt naleving gecontroleerd?

Naleving wordt **jaarlijks gecontroleerd** via:

1. **Zelfbeoordelingsvragenlijsten (SAQ – Self-Assessment Questionnaire)**
    - Afhankelijk van hoe u kaartgegevens verwerkt, vult u een specifieke SAQ in:
        - SAQ A (minimaal risico, bv. bij gebruik van een gehoste betaalpagina).
        - SAQ A-EP (e-commerce met gedeelde hosting).
        - SAQ D (meest uitgebreid, voor handelaars die kaartgegevens opslaan of verwerken).
    - *Voorbeeld:* Als u de gehoste betaalpagina of het formulier voor kaartbetalingen van Axepta BNP Paribas gebruikt, volstaat vaak SAQ A.
2. **Persoonlijke PCI DSS-audit**
    - Voor grote organisaties of complexe omgevingen kan een onafhankelijke audit vereist zijn.

Het platform van Axepta BNP Paribas wordt jaarlijks geaudit en gecertificeerd volgens PCI DSS Level 1 – het meest strikte niveau binnen de PCI DSS-normen.

Vereenvoudigde PCI DSS-compliance voor handelaars

Axepta BNP Paribas verlicht uw compliance-verplichtingen door het direct verwerken van kaartgegevens over te nemen, mits u gebruikmaakt van onze:

- Gehoste betaalpagina, of
- Formulier voor kaartbetalingen