

ONDERZOEKSRAPPORT 2026

CSS Industry Security Report

De Staat van Webbeveiliging in de Europese
Comparison Shopping Service Industrie

143 CSS partners onderzocht | 13 landen | Mei 2026

Gepubliceerd door ShoppingPartnerLab.com | Gemeten via Snyk Security Headers

AANLEIDING

Dit rapport is tot stand gekomen naar aanleiding van het grootschalige datalek bij Odido in 2026, waarbij persoonsgegevens van miljoenen Nederlandse klanten werden gelekt. Dit incident stelde ons voor een fundamentele vraag: als een van de grootste telecomproviders van Nederland de basisbeveiliging niet op orde heeft, hoe staat de CSS partner industrie er dan voor — een sector die dagelijks toegang heeft tot Google Ads accounts en betalingsdata van duizenden webshops?

Executive Summary

Dit rapport presenteert de resultaten van het eerste grootschalige onafhankelijke beveiligingsonderzoek naar de Europese CSS (Comparison Shopping Service) partner industrie. In mei 2026 werden **143 CSS partners uit 13 landen** beoordeeld op hun implementatie van kritieke HTTP security headers, gemeten via het Snyk Security Headers platform (securityheaders.com).



Belangrijkste bevindingen:

- 65% van alle CSS partners scoort onvoldoende (D, E of F) — ruim twee derde van de industrie voldoet niet aan minimale beveiligingseisen
- Slechts 4% haalt een A+ score, en geen enkele CSS partner heeft alle 9 beveiligingslagen volledig correct geïmplementeerd
- De A-score is misleidend: partners met een A missen structureel kritieke headers zoals COEP, COOP en CORP
- 40% scoort F — het laagst mogelijke cijfer, waarbij basale bescherming volledig ontbreekt
- Eén partner draait in 2026 nog op HTTP zonder HTTPS-encryptie
- Budget en bedrijfsgrootte correleren niet met beveiligingskwaliteit
- Duitsland en Nederland laten de meeste F-scores zien

Onderzoeksmethode

Wat zijn security headers?

Security headers zijn instructies die een webserver meestuurt bij elke pagina die bezoekers opvragen. Ze vertellen de browser hoe hij de pagina veilig moet weergeven en beschermen gebruikers tegen een breed scala aan cyberaanvallen. Het ontbreken van deze headers is een van de meest voorkomende en makkelijkst te misbruiken kwetsbaarheden in de moderne webinfrastructuur.

De 9 gemeten headers:

Header	Beschermt tegen
Strict-Transport-Security (HSTS)	Dwingt HTTPS af — voorkomt man-in-the-middle aanvallen
Content-Security-Policy (CSP)	Blokkeert XSS aanvallen — voorkomt injectie van kwaadaardige scripts
X-Frame-Options	Voorkomt clickjacking — blokkeert het laden in een onzichtbaar frame
X-Content-Type-Options	Voorkomt MIME-sniffing — dwingt correcte bestandsinterpretatie af
Referrer-Policy	Controleert welke data wordt gedeeld bij navigatie naar externe sites
Permissions-Policy	Blokkeert ongewenste toegang tot camera, microfoon en locatie
Cross-Origin-Embedder-Policy (COEP)	Voorkomt laden van externe resources zonder expliciete toestemming
Cross-Origin-Opener-Policy (COOP)	Isoleert browsing context — beschermt tegen cross-origin aanvallen
Cross-Origin-Resource-Policy (CORP)	Controleert wie externe resources mag laden

Meetinstrument en methodologie

Alle metingen zijn uitgevoerd via Snyk Security Headers (securityheaders.com). Van de 143 gescande CSS partners konden 138 worden beoordeeld. Vijf partners (3%) konden niet worden gemeten door technische blokkades of timeouts en zijn buiten de statistische berekeningen gelaten.

Resultaten

Totaaloverzicht

Score	Aantal	Percentage	Beoordeling
A+	6	4%	Uitstekend — alle headers correct geïmplementeerd
A	14	10%	Goed — vrijwel compleet, kleine hiaten
B	15	10%	Redelijk — meerdere headers ontbreken
C	13	9%	Matig — meerdere beveiligingsrisico's aanwezig
D	32	22%	Onvoldoende — significante kwetsbaarheid
E	1	1%	Kritisch — geen HTTPS-encryptie
F	57	40%	Gevaarlijk — directe actie vereist
N/A	5	3%	Niet meetbaar (geblokkeerd / timeout)

Schokkende conclusie

Slechts 35 van de 138 meetbare CSS partners (25%) halen een voldoende score (A+, A of B). De overgrote meerderheid — 90 van de 138 partners (65%) — scoort D, E of F.

Verdeling per land

Land	A+	A	B	C	D	E/F	Totaal
Duitsland (DE)	—	2	2	2	4	15	25
Nederland (NL)	1	1	4	—	1	5	12
Tsjechië (CZ)	2	2	1	3	6	2	16
Polen (PL)	—	1	2	3	4	5	15
VK (UK)	—	2	—	1	3	4	10
EU (overig)	—	4	2	1	6	13	26
Frankrijk (FR)	—	1	—	—	2	4	7
Zweden (SE)	—	—	1	2	—	2	5
Denemarken (DK)	—	—	—	—	2	2	5
USA (US)	2	—	—	—	—	2	4
Griekenland (GR)	1	—	1	—	1	—	3
Overig	—	1	—	—	1	3	5

De A-Score Paradox: Goed is Niet Goed Genoeg

Een van de meest verrassende bevindingen is de kloof tussen de officiële score en de werkelijke beveiligingsstatus. Meerdere CSS partners scoren een A maar missen bij nadere analyse alsnog kritieke beveiligingslagen.

Kernbevinding

Geen enkele van de 143 onderzochte CSS partners heeft alle 9 security headers volledig en correct geïmplementeerd. Zelfs de zes A+-scorers missen structureel de Cross-Origin headers (COEP, COOP, CORP).

Header-aanwezigheid per scoreniveau

✓ = aanwezig en correct | ~ = aanwezig maar zwak | ✗ = volledig afwezig

Header	A+	A	B	C	D	F
HSTS	✓	✓	✓	✓	✓	✓
X-Content-Type-Options	✓	✓	✓	✓	✓	✓
X-Frame-Options	✓	~	✓	✓	✓	✓
Referrer-Policy	~	~	✓	✓	✓	✓
Permissions-Policy	~	~	~	✓	✓	✓
Content-Security-Policy	~	~	~	~	✓	✓
COEP	✗	✗	✗	✗	✗	~
COOP	✗	✗	✗	✗	✗	✓
CORP	✗	✗	✗	✗	✗	✓

De Gevaren: Concrete Aanvalsscenario's

Ontbrekende security headers zijn niet slechts technische onvolkomenheden — ze vertegenwoordigen concrete, uitbuitbare kwetsbaarheden. Voor CSS partners die toegang beheren tot Google Merchant Center en Google Ads budgetten zijn de gevolgen bijzonder ernstig.

1. XSS credential-diefstal

Zonder een correcte Content-Security-Policy kan een aanvaller kwaadaardige JavaScript injecteren op de website van een CSS partner. Iedere webshop-eigenaar die vervolgens inlogt levert zijn Google Ads credentials direct af aan de aanvaller.

Impact: Volledige overname van Google Ads accounts, frauduleuze advertentie-uitgaven, verlies van campagnedata.

2. Clickjacking via iframe-injectie

Zonder X-Frame-Options kan een aanvaller de inlogpagina van een CSS partner onzichtbaar laden in een eigen nepwebsite. Gebruikers interacteren met de echte CSS partner terwijl wachtwoorden worden onderschept.

Impact: Accountovername, sessie-kaping, ongeautoriseerde wijzigingen in advertentiecampagnes.

3. Supply chain aanval

CSS partners zijn een klassiek supply chain target: één succesvolle aanval treft niet één webshop, maar potentieel honderden aangesloten webshops tegelijk.

Impact: Massale datadiefstal, gecompromitteerde advertentieaccounts van honderden webshops.

4. Man-in-the-Middle via ontbrekend HSTS

Partners die HTTPS niet correct afdwingen stellen gebruikers bloot aan af luistering op openbare WiFi-netwerken. Login-gegevens en sessie-cookies kunnen worden onderschept.

Impact: Credential-diefstal, sessie-kaping, ongeautoriseerde datatoegang.

5. GDPR/AVG aansprakelijkheid

De AVG vereist passende technische maatregelen. Ontbrekende security headers worden door toezichthouders beschouwd als het nalaten van deze verplichting.

Impact: Boetes tot 4% van de wereldwijde jaaromzet, verplichte melding aan toezichthouder.

Beveiliging in het AI-Tijdperk: SEO, Adverteren en Google

De gevolgen van slechte webbeveiliging reiken verder dan directe cyberaanvallen. Technische beveiliging heeft directe impact op vindbaarheid, advertentie-effectiviteit en de relatie met Google.

Impact op Google rankings en SEO

- Core Web Vitals en technische gezondheid: Ontbrekende security headers signaleren technische verwaarlozing, wat negatief doorwerkt in de overall technische score.
- Vertrouwenssignalen: Sites die bezoekers niet adequaat beschermen genereren hogere bounce rates bij beveiligingswaarschuwingen — een negatief signaal voor rankings.
- Indexering en crawl budget: Sites met beveiligingsproblemen kunnen worden vertraagd in indexering.

Google Ads sancties en accountrisico's

Google's beveiligingsvereisten

Google vereist dat CSS partners voldoen aan minimale beveiligings- en betrouwbaarheidsnormen. Een CSS partner wiens infrastructuur wordt gecompromitteerd riskeert schorsing van het Google Partner programma.

- Accountsuspensie: Google kan CSS partner accounts schorsen bij beveiligingsincidenten, waardoor alle gekoppelde webshop-accounts ook worden geraakt.
- Verlies van CSS-status: CSS partners die de Google CSS partner status verliezen, kunnen niet langer kortingen bieden op Google Shopping kosten.
- Fraudedetectie: Gecompromitteerde accounts die worden gebruikt voor klikfraude kunnen leiden tot permanente accountuitsluiting.

Impact op AI-vindbaarheid en LLM-zoekmachines

- Technische autoriteit als rankingfactor: LLM-gebaseerde zoekmachines beoordelen ook de technische betrouwbaarheid van bronnen. Sites met sterke beveiliging worden als betrouwbaarder beschouwd.
- Crawlbaarheid voor AI: AI-zoekmachines crawlen het web actief. Sites met beveiligingsproblemen worden mogelijk minder frequent gecrawld.
- E-E-A-T signalen: Google's Experience, Expertise, Authoritativeness en Trustworthiness framework wordt negatief beïnvloed door beveiligingstekortkomingen.
- Reputatie in AI-antwoorden: Een CSS partner betrokken bij een datalek riskeert dat dit in AI-gegenereerde antwoorden verschijnt, met permanente reputatieschade.

Aanbevelingen

Voor webshops die een CSS partner selecteren

- Controleer de security score: Scan de website van uw CSS partner via securityheaders.com.
- Vraag naar GDPR-compliance beleid: Welke technische maatregelen neemt de CSS partner?
- Beoordeel technische professionaliteit: Een CSS partner die de eigen website niet beveiligt, beveiligt waarschijnlijk ook de data van klanten niet adequaat.
- Controleer uw eigen webshop via shoppingpartnerlab.com.

Voor CSS partners zelf

- Implementeer onmiddellijk: HSTS, X-Content-Type-Options en X-Frame-Options — de basishygiëne die geen enkel professioneel platform mag missen.
- Configureer CSP correct: Een CSP met alleen 'unsafe-inline' of 'upgrade-insecure-requests' is onvoldoende.
- Voeg Cross-Origin headers toe: COEP, COOP en CORP ontbreken bij vrijwel de gehele industrie.
- Implementeer automatische monitoring via securityheaders.com.
- Voer regelmatig penetratietests uit.

Conclusie

De Europese CSS partner industrie heeft een structureel beveiligingsprobleem. 65% van alle partners voldoet niet aan minimale beveiligingseisen, en geen enkele partner heeft alle 9 kritieke headers volledig correct geïmplementeerd. In een tijdperk waarin datalekken steeds vaker voorkomen, AI-zoekmachines technische betrouwbaarheid steeds zwaarder meewegen, en Google steeds strengere eisen stelt aan partners, is dit een serieus risico — niet alleen voor de CSS partners zelf, maar voor alle webshops die zij vertegenwoordigen.

Het goede nieuws: de oplossing is technisch eenvoudig. De vraag is niet of het kan, maar of de industrie de prioriteit stelt.

Onderzoek uitgevoerd door **ShoppingPartnerLab.com** — Europe's only independent CSS partner comparison platform.

Gemeten via Snyk Security Headers (securityheaders.com). Mei 2026.

Voor vragen of een gratis security scan: shoppingpartnerlab.com