Premium SSL/TLS Deep Audit Rapport

Analyse: jan-karel.nl

Opgesteld voor: **Test**

Door: **BasisHost**

Datum: **3 april 2026**

Inhoudsopgave

Management Samenvatting

Totaalscore: **83/100** (83%) — Cijfer: **B+**. Uw organisatie heeft een goed beveiligingsniveau. De meeste maatregelen zijn geïmplementeerd. Focus op de resterende aandachtspunten en continue verbetering.

Aandachtsgebieden: **Cipher Suites** (50%), **Security Headers** (85%), **Kwetsbaarheden** (86%).

Top aanbevelingen: Forward Secrecy; HSTS Preload.

Totaalscore

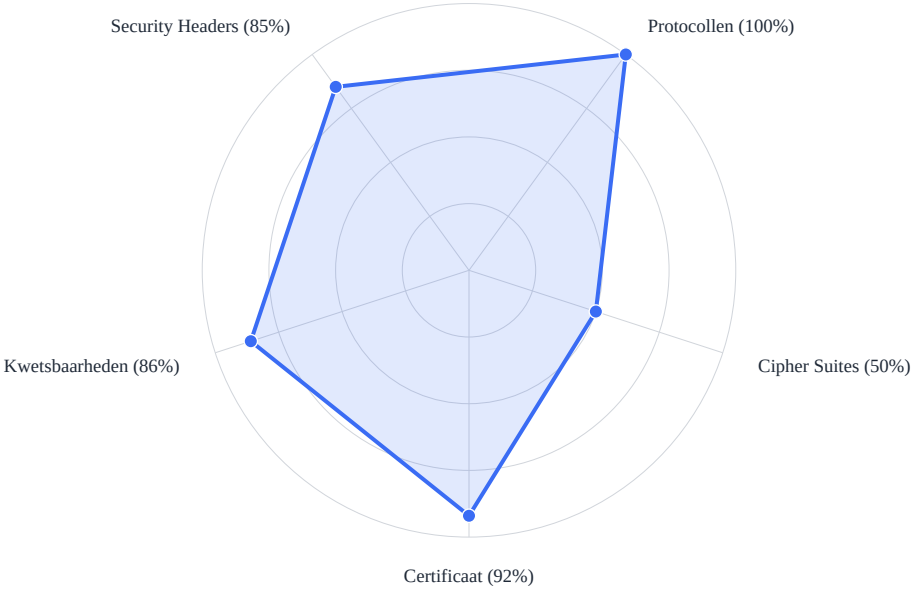
83 / 100

Cijfer: B+

Onderwerp	jan-karel.nl
Totaalscore	83/100 (83%)
Cijfer	B+
Rapportdatum	03-04-2026

Scores per Categorie

Certificaat	92%
Cipher Suites	50%
Protocollen	100%
Security Headers	85%
Kwetsbaarheden	86%


Security Headers (85%)
Protocollen (100%)
Kwetsbaarheden (86%)
Cipher Suites (50%)
Certificaat (92%)

Certificaat — 92%

Wat is dit? Het certificaat is het digitale paspoort van uw website. Het bewijst aan bezoekers dat ze echt met uw server verbonden zijn en niet met een nep-versie.

Wat betekent deze score? Uw certificaat is uitstekend ingericht. Er zijn geen dringende verbeterpunten gevonden.

Check	Status	Waarde	Advies
Geldigheid	✓ PASS	Geldig, nog 55 dagen	
Uitgever	✓ PASS	Let's Encrypt (E8)	
Subject Match	✓ PASS	jan-karel.nl	
Subject Alt Names	✓ PASS	2 SAN(s), domein gevonden	
Certificaat Type	✓ PASS	DV (Domain Validation)	Overweeg OV of EV certificaat voor meer vertrouwen.

Cipher Suites — 50%

Wat is dit? Cipher suites zijn de versleutelingsmethoden die uw server aanbiedt. Verouderde methoden kunnen door hackers worden gekraakt, waardoor data onderschept kan worden.

Wat betekent deze score? Uw cipher suites is voldoende, maar er zijn meerdere punten die verbeterd moeten worden om risico's te verkleinen.

Check	Status	Waarde	Advies
Zwakke Ciphers	✓ PASS	Geen zwakke ciphers gevonden	
Forward Secrecy	✗ FAIL	Geen Forward Secrecy ciphers	Configureer ECDHE of DHE cipher suites.

Protocollen — 100%

Wat is dit? Protocollen bepalen hoe de beveiligde verbinding tot stand komt. Oudere versies (TLS 1.0/1.1) bevatten kwetsbaarheden en moeten uitgeschakeld zijn.

Wat betekent deze score? Uw protocollen is uitstekend ingericht. Er zijn geen dringende verbeterpunten gevonden.

Check	Status	Waarde	Advies
TLS 1.3	✓ PASS	Ondersteund	
TLS 1.2	✓ PASS	Ondersteund	
TLS 1.1 Uitgeschakeld	✓ PASS	Correct uitgeschakeld	
TLS 1.0 Uitgeschakeld	✓ PASS	Correct uitgeschakeld	

Security Headers — 85%

Wat is dit? Security Headers zijn extra beveiligingsinstructies die uw server aan browsers geeft, bijvoorbeeld om altijd HTTPS te gebruiken of clickjacking te voorkomen.

Wat betekent deze score? Uw security headers is uitstekend ingericht. Er zijn geen dringende verbeterpunten gevonden.

Check	Status	Waarde	Advies
HSTS	✓ PASS	max-age=31536000; includeSubdomains	
HSTS includeSubDomains	✓ PASS	Aanwezig	
HSTS Preload	■ WARN	Ontbreekt	Overweeg HSTS preloading.
X-Content-Type-Options	✓ PASS	nosniff	
X-Frame-Options	✓ PASS	SAMEORIGIN	

Kwetsbaarheden — 86%

Wat is dit? Kwetsbaarheden controleert of uw server vatbaar is voor bekende aanvallen die de versleuteling kunnen omzeilen of data kunnen lekken.

Wat betekent deze score? Uw kwetsbaarheden is uitstekend ingericht. Er zijn geen dringende verbeterpunten gevonden.

Check	Status	Waarde	Advies
Mixed Content	✓ PASS	Geen mixed content gevonden	
Certificaatketen	✓ PASS	Volledig en geldig	
OCSP Stapling	■ WARN	Kon niet worden gecontroleerd	
CAA Record	✓ PASS	1 record(s) met issue tag	

Aanbevelingen

Geprioriteerde aanbevelingen op basis van de analyse.

Prio	Categorie	Titel	Beschrijving	Doorlooptijd
Hoog	Cipher Suites	**Forward Secrecy**	Configureer ECDHE of DHE cipher suites.	1 uur
Middel	Beveiligingsheaders	**HSTS Preload**	Overweeg HSTS preloading.	30 minuten

Bijlage: Invoergegevens

Domein	jan-karel.nl

Bijlage A: Begrippen en Afkortingen

Onderstaande lijst verklaart de belangrijkste termen en afkortingen die in dit rapport worden gebruikt.

Term	Betekenis
AVG	Algemene Verordening Gegevensbescherming — Europese privacywetgeving (ook wel GDPR).
BCP	Business Continuity Plan — plan om bedrijfsprocessen voort te zetten bij verstoringen.
BIA	Business Impact Analysis — analyse van de gevolgen van uitval van systemen of processen.
Certificaat	Digitaal paspoort van uw website dat bewijst dat bezoekers echt met uw server verbonden zijn, niet met een nep-versie.
Cipher suite	Versleutelingsmethode die uw server en de browser van uw bezoeker afspreken om het dataverkeer te beschermen.
CISO	Chief Information Security Officer — eindverantwoordelijke voor informatiebeveiliging.
CVE	Common Vulnerabilities and Exposures — gestandaardiseerd identificatiesysteem voor kwetsbaarheden.
DRP	Disaster Recovery Plan — plan voor herstel van IT-systemen na een calamiteit.
EDR	Endpoint Detection & Response — beveiligingssoftware die verdachte activiteit op werkstations en servers detecteert en blokkeert.
HSTS	HTTP Strict Transport Security — instelling die browsers dwingt altijd de beveiligde (HTTPS) versie van uw website te gebruiken.
IAM	Identity & Access Management — beheer van digitale identiteiten en toegangsrechten.
IR-plan	Incident Response Plan — vastgelegde procedures voor het afhandelen van beveiligingsincidenten.
MFA	Multi-Factor Authenticatie — inloggen met twee of meer verificatiestappen (bijv. wachtwoord + app-code).
NIS2	Network and Information Security Directive 2 — Europese richtlijn die cybersecurity-eisen stelt aan essentiële en belangrijke entiteiten.
NIST CSF	National Institute of Standards and Technology Cyber Security Framework — internationaal raamwerk voor cybersecurity.
OCSP Stapling	Techniek waarmee uw server snel kan bewijzen dat het certificaat nog geldig is, zonder dat de browser dit apart moet opvragen.
PAM	Privileged Access Management — beheer en beveiliging van accounts met verhoogde rechten.
RPO	Recovery Point Objective — maximaal acceptabel dataverlies, uitgedrukt in tijd.
RTO	Recovery Time Objective — maximaal acceptabele tijd om een systeem te herstellen na uitval.
SIEM	Security Information & Event Management — systeem dat beveiligingslogs verzamelt, correleert en alarmeert.
SOC	Security Operations Center — team dat 24/7 beveiligingsincidenten monitort en afhandelt.
TLS	Transport Layer Security — het 'slot' in de adresbalk van uw browser. Versleutelt alle data tussen bezoeker en website.
XDR	Extended Detection & Response — geïntegreerde detectie over endpoints, netwerk en cloud.

Dit rapport is opgesteld door **BasisHost**.

Rapport gegenereerd op 3 april 2026. De resultaten zijn gebaseerd op door de klant verstrekte informatie. Dit rapport vervangt geen professionele security audit of pentest. BasisHost is niet aansprakelijk voor beslissingen genomen op basis van dit rapport zonder aanvullend professioneel advies.