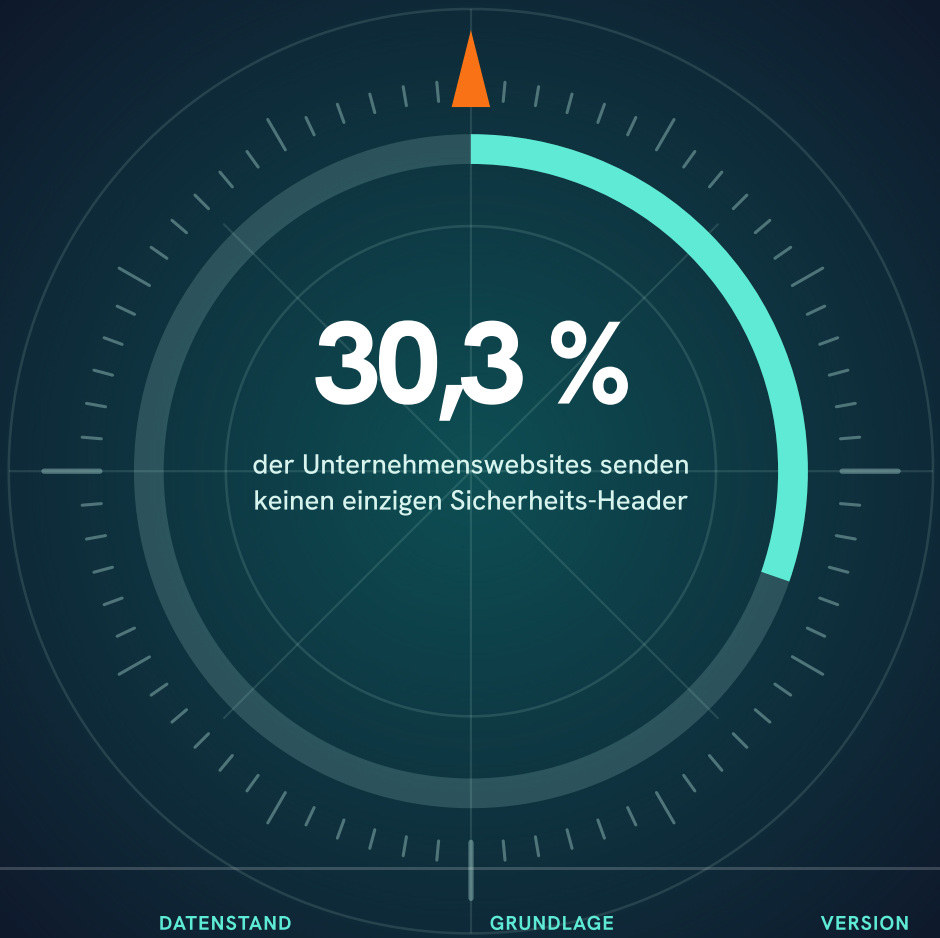
kjello.

STUDIE · NOVEMBER 2026

KJELLO-STUDIE

Website-Sicherheit 2026

Wie gut schützen Unternehmen ihre Website?



HERAUSGEBER

kjello · hagel IT-Services GmbH, Hamburg

DATENSTAND

9. Oktober 2026, Messung 08:16–11:02 Uhr MESZ

GRUNDLAGE

Messung der Startseiten von 10.107 Unternehmenswebsites in Deutschland (ohne Konzerne), 9. Oktober 2026

VERSION

1.0 · 17. November 2026
Lizenz CC BY 4.0

INHALT

Website-Sicherheit 2026

01	Management Summary	3
02	Kernaussagen	4
03	Sicherheits-Header: die Hälfte fehlt	5
04	Fast jede dritte Website ohne jeden Header	6
05	Schwache E-Mail, schwache Website	7
06	Größere Unternehmen besser aufgestellt	8
07	Einordnung: frühere Erhebungen	9
08	Methodik	10
09	Definitionen und Grenzen	11
10	Tabellen	12
11	Was Unternehmen jetzt tun können	16
12	Quellen	17
13	Zitiervorschlag, Lizenz und Impressum	18

Auf einen Blick

30,3 %
senden keinen der sechs empfohlenen Sicherheits-Header

49,9 %
verzichten auf HSTS

31,5 %
der sichtbaren PHP-Versionen ohne Sicherheitsupdates laut php.net

Steckbrief

Herausgeber	kjello – eine Marke der hagel IT-Services GmbH, Hamburg
Grundlage	Öffentliche HTTP-Antworten der Startseiten von 10.107 erreichbaren Unternehmenswebsites, Messung am 9. Oktober 2026
Datenstand	9. Oktober 2026, Messung 08:16–11:02 Uhr MESZ
Veröffentlicht	17. November 2026 · Version 1.0
Online	kjello.de/studien/website-sicherheit-2026 – mit Tabellen (CSV), Grafiken und Pressepaket
Nutzung	frei mit Quellenangabe und Link (CC BY 4.0)

MANAGEMENT SUMMARY

Website-Sicherheit 2026: Wie gut schützen Unternehmen ihre Website?

Ob eine Website den Browser ihrer Besucher anweist, nur verschlüsselt zu verbinden, fremde Skripte abzuwehren oder sich nicht in fremde Seiten einbetten zu lassen, steht in wenigen Zeilen ihrer Serverantwort – den Sicherheits-Headern. Sie kosten nichts, sind standardisiert und werden vom OWASP Secure Headers Project empfohlen.

kjello hat am 9. Oktober 2026 die Startseiten von 10.107 erreichbaren Unternehmenswebsites so abgerufen, wie es ein Browser tut – dieselben Unternehmen wie in der Studie „E-Mail-Sicherheit 2026“. Ergebnis: 30,3 % der Startseiten senden keinen einzigen der sechs empfohlenen Sicherheits-Header, 49,9 % verzichten auf HSTS, eine Content-Security-Policy haben 25,2 %.

Verschlüsselung selbst ist Standard: 93,9 % handeln TLS 1.3 aus. Lücken zeigen sich an anderer Stelle: 7,3 % sind unter der eigenen Adresse nicht fehlerfrei verschlüsselt erreichbar, und 31,5 % der sichtbaren PHP-Versionen bekommen laut php.net keine Sicherheitsupdates mehr. Unternehmen mit wirksamem E-Mail-Schutz setzen deutlich häufiger HSTS (58,3 %) als solche ganz ohne DMARC (38,7 %).

EINORDNUNG DER REDAKTION

Die Messung zeigt eine Lücke zwischen Verschlüsselung und Konfiguration. HTTPS und TLS 1.3 sind fast überall angekommen, Zertifikate werden meist automatisch erneuert (64,9 % laufen höchstens 100 Tage). Die Sicherheits-Header dagegen muss jemand bewusst setzen, und genau das fehlt bei fast jeder dritten Website ganz. Auffällig ist der Gleichlauf mit der E-Mail-Studie: Wo DMARC fehlt, fehlt auch häufiger HSTS. Website und Mail-Domain werden offenbar mit derselben Sorgfalt betreut – oder mit derselben Lücke.

KERNAUSSAGEN

Die Ergebnisse in 8 Sätzen

01

30,3 %

der Unternehmenswebsites senden keinen einzigen der sechs empfohlenen Sicherheits-Header. Alle sechs setzt nur jede zwölfte (8,3 %).

95-%-KI 29,4–31,3 % · Basis: 8.989 HTTPS-Startseiten

02

49,9 %

verzichten auf HSTS – der Browser wird nicht angewiesen, die Seite nur verschlüsselt aufzurufen. Mindestens ein Jahr lang tun das 40,1 %.

03

25,2 %

haben eine Content-Security-Policy, streng gegen eingeschleuste Skripte geregelt sind nur 2,7 %.

04

7,3 %

der Websites sind unter der eigenen Adresse nicht fehlerfrei verschlüsselt erreichbar. TLS 1.3 handeln 93,9 % aus.

Basis: 10.107 erreichbare Websites

05

31,5 %

der sichtbaren PHP-Versionen bekommen laut php.net keine Sicherheitsupdates mehr – ein Indiz, kein Befund: Distributionen können Korrekturen nachliefern.

06

58,3 %

der Unternehmen mit wirksamem E-Mail-Schutz setzen HSTS, ganz ohne DMARC sind es 38,7 %.

07

60,8 %

der Unternehmen ab 250 Beschäftigten setzen HSTS, darunter 48,2 %.

08

6,9 %

nennen per security.txt (RFC 9116) einen Ansprechpartner für Sicherheitshinweise.

Basis: 8.989 HTTPS-Startseiten mit Status 2xx, sofern nicht anders angegeben (10.107 erreichbare Websites, Unternehmen in Deutschland ohne Konzerne, Messung vom 9. Oktober 2026).

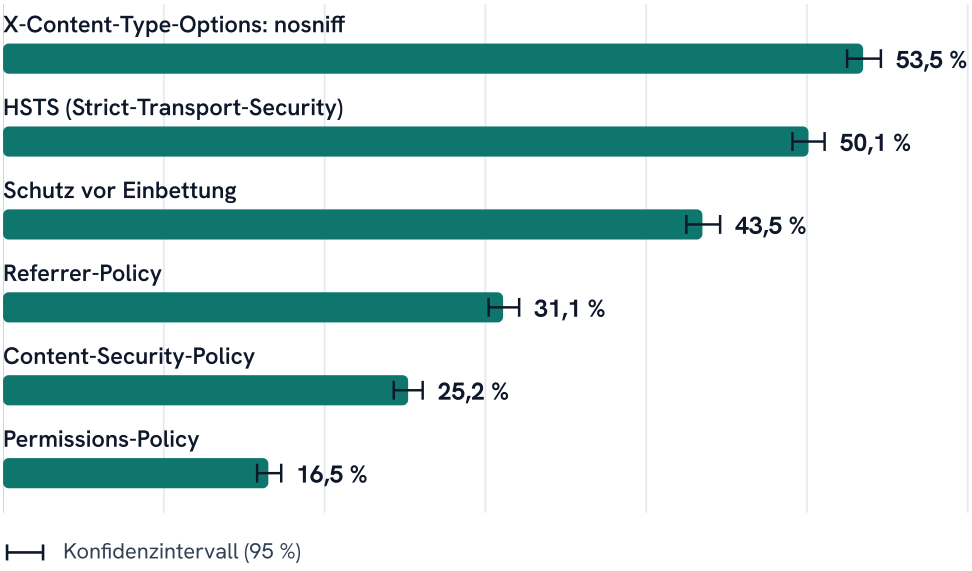
KAPITEL 1

Sicherheits-Header: die Hälfte fehlt

ABBILDUNG 1

Nur jede zweite Website setzt HSTS, nur jede vierte eine Content-Security-Policy

Anteil der HTTPS-Startseiten mit dem jeweiligen Sicherheits-Header, in % mit Konfidenzintervall (95 %), n = 8.989



Quelle: kjello-Studie Website-Sicherheit 2026, Messung vom 9. Oktober 2026 · HSTS zählt ab max-age > 0, die Content-Security-Policy nur, wenn sie durchgesetzt wird (nicht Report-Only). Schutz vor Einbettung = X-Frame-Options DENY/SAMEORIGIN oder CSP-Direktive frame-ancestors. Empfohlen werden alle sechs vom OWASP Secure Headers Project.

Am häufigsten ist X-Content-Type-Options: nosniff (53,5 %), knapp dahinter HSTS (50,1 %). HSTS weist den Browser an, die Seite für eine festgelegte Zeit nur noch über HTTPS aufzurufen (RFC 6797). Ohne HSTS kann jeder Aufruf, der unverschlüsselt beginnt – etwa durch Eintippen der Adresse ohne https:// oder einen alten Link –, in einem öffentlichen WLAN abgefangen und umgeleitet werden.

Dauerhaft, also mit mindestens einem Jahr Laufzeit, setzen 40,1 % HSTS; die Voraussetzungen für die HSTS-Preload-Liste der Browser erfüllen 11,3 % – kein Zielwert, denn die Betreiber der Liste raten inzwischen vom Preloading ab. Eine Content-Security-Policy haben 25,2 % – Skripte regeln davon nur 13,3 % aller Websites, streng ohne unsafe-inline und Platzhalter 2,7 %. Fast die Hälfte der vorhandenen Richtlinien (11,9 % aller Websites) regelt nur Nebenaspekte wie die automatische Umstellung auf HTTPS.

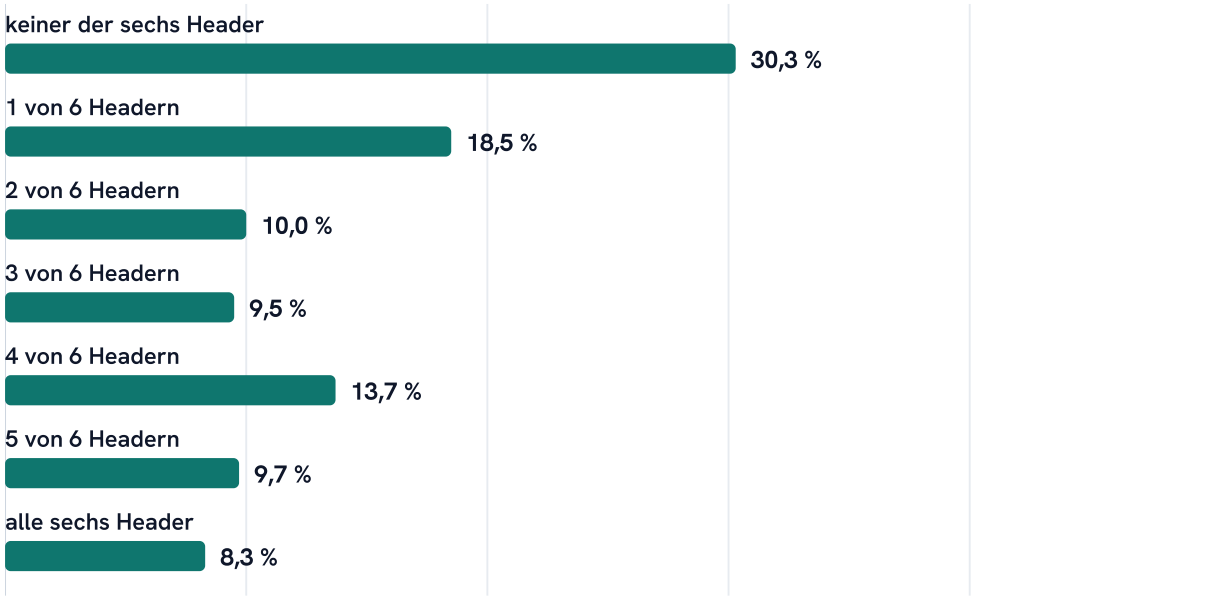
KAPITEL 2

Fast jede dritte Website ohne jeden Header

ABBILDUNG 2

Fast jede dritte Website sendet keinen einzigen Sicherheits-Header

Wie viele der sechs empfohlenen Sicherheits-Header eine Startseite sendet, Anteil in % (n = 8.989)



Quelle: kjello-Studie Website-Sicherheit 2026, Messung vom 9. Oktober 2026 · Die sechs Header: HSTS, Content-Security-Policy, Schutz vor Einbettung, X-Content-Type-Options: nosniff, Referrer-Policy, Permissions-Policy. Den Grundschutz aus HSTS, nosniff und Einbettungsschutz haben 32,3 %.

30,3 % der Startseiten senden keinen der sechs Header, alle sechs setzt nur jede zwölfte (8,3 %). Den Grundschutz aus HSTS, nosniff und Einbettungsschutz haben 32,3 %.

Verschlüsselung ist dagegen Standard, aber nicht lückenlos: 7,3 % der 10.107 erreichbaren Websites lassen sich unter der eigenen Adresse nicht fehlerfrei verschlüsselt aufrufen, bei 4,8 % zeigt der Browser beim direkten Aufruf mit https:// eine Zertifikatswarnung. 4,0 % der HTTPS-Websites liefern unter einer http://-Adresse weiter unverschlüsselt aus. Gut: 93,9 % handeln TLS 1.3 aus; Server, die nur noch veraltete TLS-Versionen beherrschen, sind praktisch verschwunden.

Jede fünfte Website verrät ihre Softwareversion (19,2 %). Von den sichtbaren PHP-Versionen bekommen 31,5 % laut php.net keine Sicherheitsupdates mehr (359 Websites, 3,7 % aller). Linux-Distributionen spielen Korrekturen teils ein, ohne die Versionsnummer zu ändern – die Zahl ist ein Indiz, kein Befund. Die OWASP empfiehlt, solche Versionsangaben ganz zu entfernen.

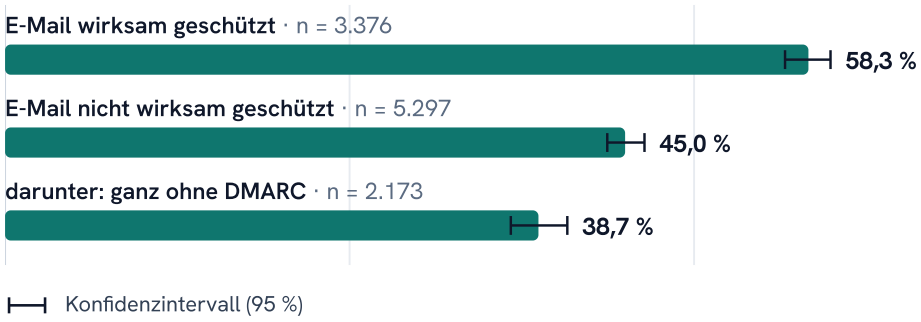
KAPITEL 3

Schwache E-Mail, schwache Website

ABBILDUNG 3

Wer seine E-Mail-Domain schützt, setzt auch häufiger HSTS

HSTS aktiv nach E-Mail-Schutz derselben Domain (Studie „E-Mail-Sicherheit 2026“), Anteil der HTTPS-Startseiten in % mit Konfidenzintervall (95 %); alle Websites: 50,1 %



Quelle: kjello-Studie Website-Sicherheit 2026, Messung vom 9. Oktober 2026 · „Wirksam geschützt“ wie in der E-Mail-Studie: DMARC quarantine oder reject für alle Mails (pct = 100) und gültiges SPF. „Ganz ohne DMARC“ ist eine Teilgruppe von „nicht wirksam geschützt“. Basis: 9.664 erreichbare Websites mit E-Mail-Empfang. Der Zusammenhang ist eine Korrelation, keine Ursache.

Die Studie misst dieselben Unternehmen wie die Studie „E-Mail-Sicherheit 2026“. Von den Unternehmen mit wirksamem Schutz gegen gefälschte Absender setzen 58,3 % HSTS, von den übrigen 45,0 % und von denen ganz ohne DMARC nur 38,7 %. Keinen einzigen Sicherheits-Header senden 23,6 % gegenüber 34,5 % bzw. 39,6 %.

Fast jedes dritte Unternehmen (31,9 %) hat weder DMARC durchgesetzt noch HSTS gesetzt; beides zusammen schaffen 22,7 %. Der Zusammenhang ist eine Korrelation, keine Ursache: Vermutlich stehen beide Werte für dieselbe Sorgfalt – oder denselben Dienstleister – hinter Domain und Website.

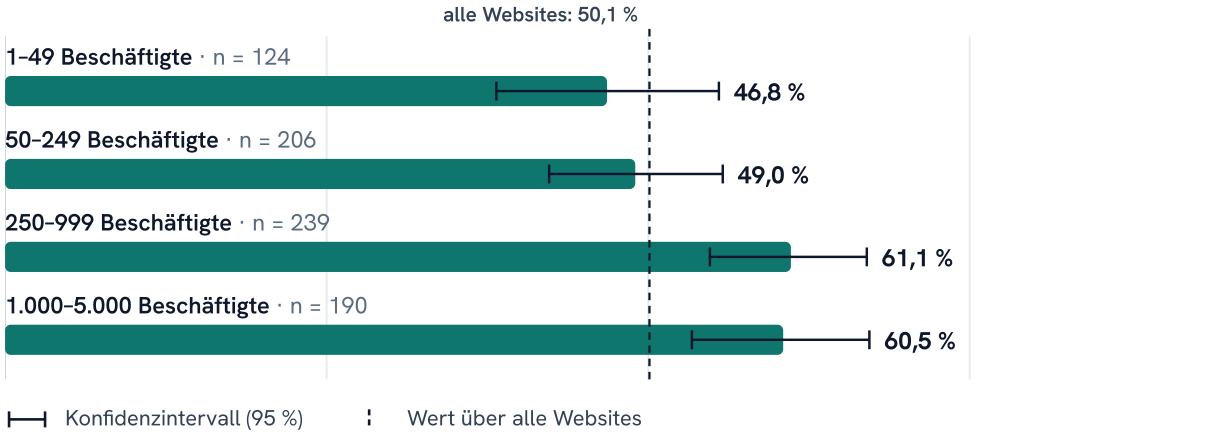
KAPITEL 4

Größere Unternehmen besser aufgestellt

ABBILDUNG 4

Ab 250 Beschäftigten setzen deutlich mehr Unternehmen HSTS

HSTS aktiv nach Beschäftigten laut Wikidata, Anteil der HTTPS-Startseiten in % mit Konfidenzintervall (95 %)



Quelle: kjello-Studie Website-Sicherheit 2026, Messung vom 9. Oktober 2026 · Die Größe ist nur für 847 der 10.107 erreichbaren Websites bekannt; die Gruppen sind klein und ihre Intervalle überlappen teils. Belastbar ist der Unterschied der zusammengefassten Gruppen: unter 250 Beschäftigte 48,2 % (42,8–53,6 %), 250 bis 5.000 Beschäftigte 60,8 % (56,1–65,3 %).

Unternehmen ab 250 Beschäftigten setzen zu 60,8 % HSTS, und nur 17,2 % senden keinen Sicherheits-Header; bei Firmen unter 250 Beschäftigten sind es 48,2 % und 31,2 %. Die 95-%-Konfidenzintervalle überschneiden sich jeweils nicht.

Sichtbares PHP ohne Sicherheitsupdates findet sich bei 7,0 % der Kleinbetriebe unter 50 Beschäftigten und bei keiner Website der Firmen mit 1.000 bis 5.000 Beschäftigten. Die Größe ist nur für 847 der 10.107 Websites bekannt; die einzelnen Klassen sind klein.

EINORDNUNG

Was frühere Erhebungen zeigen

Eine unabhängige bundesweite Messung der Sicherheits-Header von Unternehmenswebsites in Deutschland haben wir nicht gefunden. Internationale und regionale Erhebungen zeigen ein ähnliches Bild – mit anderen Stichproben und teils anderen Definitionen. Beim Vergleich wichtig: Unser „Schutz vor Einbettung“ zählt X-Frame-Options oder frame-ancestors; X-Frame-Options allein setzen 39,0 %.

HTTP ARCHIVE · JANUAR 2026 (CRAWL JULI 2025)

Web Almanac 2025, Kapitel Security

Weltweit rund 12,1 Mio. Desktop- und 15,4 Mio. Mobile-Websites aus dem Chrome-Nutzungsdatensatz (CrUX). Desktop: HSTS 37,9 %, CSP 22,3 %, X-Frame-Options 38,3 %, nosniff 51,4 %, Referrer-Policy 18,6 %, Permissions-Policy 4,0 %; security.txt 1,82 %. Die Unternehmenswebsites unserer Stichprobe liegen bei jedem Header darüber (HSTS 50,1 %, X-Frame-Options 39,0 %, Permissions-Policy 16,5 %).

https://almanac.httparchive.org/en/2025/security

SCOTT HELME · JUNI 2026

Top 1 Million Analysis – June 2026

Die eine Million beliebtesten Websites weltweit (Tranco-Liste), 819.002 antworteten am 13. Juni 2026. Das Original nennt absolute Zahlen; umgerechnet auf die antwortenden Websites: HSTS 30,9 %, CSP 20,8 %, X-Frame-Options 40,0 %, nosniff 38,1 %, Referrer-Policy 28,0 %, Permissions-Policy 12,4 %, gültige security.txt 1,2 % (9.927 Websites). Ausgewählt nach Beliebtheit, nicht nach Unternehmen.

https://scotthelme.co.uk/top-1-million-analysis-june-2026-ten-years-of-web-security/

HAGEL IT · OKTOBER 2026

Hamburger IT-Sicherheits-Index 2026

Regionale Messung von 732 erreichbaren Websites Hamburger Unternehmen (Messung 1. Oktober 2026): HSTS 44,3 %, CSP 24 %, X-Frame-Options 34,6 %, nosniff 46,2 %, Referrer-Policy 22,8 %, TLS 1.3 91,9 %. Methodisch am nächsten an dieser Studie, die Werte liegen etwas darunter. Offenlegung: Herausgeber ist hagel IT, das Systemhaus hinter kjello – keine unabhängige Quelle.

https://www.hagel-it.de/it-sicherheits-index-hamburg

BSI · AUGUST 2026

Pressemitteilung „Nur 1,8 Prozent der Webseitenbetreiber nutzen security.txt“

„Nur 1,8 Prozent der Webseitenbetreiber in Deutschland stellen bislang eine security.txt bereit“ – Messungen im Rahmen des Cyberdome-Projekts. Stichprobe, Zeitpunkt und Definition nennt das BSI nicht. In unserer Stichprobe bekannterer Unternehmen haben 6,9 % eine gültige security.txt.

https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2026/260806_security_txt.html

WAS AN DIESER MESSUNG NEU IST

- Bundesweite Messung der Sicherheits-Header von Unternehmenswebsites in Deutschland – mit offengelegter Auswahl (Wikidata, 14 Ausschlussregeln) statt Top-Listen oder Browserverkehr.
- Dazu HTTPS, Umleitung von HTTP, TLS-Version, sichtbare Softwareversionen und security.txt, jeweils mit Konfidenzintervall.
- Dieselben Unternehmen wie in der Studie „E-Mail-Sicherheit 2026“: Website- und E-Mail-Schutz lassen sich für dieselben Unternehmen vergleichen.
- Aktueller Stand vom 9. Oktober 2026, alle aggregierten Tabellen frei als CSV.

METHODIK

So wurde gemessen

Stichprobe: dieselben 10.586 Domains wie in der Studie „E-Mail-Sicherheit 2026“ – Unternehmen mit Sitz in Deutschland ohne Konzerne über 5.000 Beschäftigte, gewonnen aus Wikidata (Abruf 8. Oktober 2026, 14 Ausschlussregeln). Beide Studien lassen sich so Domain für Domain verknüpfen; veröffentlicht werden nur Summen und Anteile.

Gemessen wurde nur, was jeder Browser beim normalen Aufruf der Startseite sieht: DNS-Auflösung von Domain und www., /robots.txt (schließt sie Abrufe aus, wurde die Domain nicht gemessen – 96 Domains), die Startseite / in vier Varianten (https und http, mit und ohne www.) samt Weiterleitungen, und /.well-known/security.txt. Seiteninhalte wurden nicht gelesen; keine Portscans, keine Unterseiten, keine Schwachstellentests, keine Logins.

Abruf mit Python 3.14.5 und OpenSSL 3.6.5, Zertifikatsprüfung gegen die Mozilla-Wurzelzertifikate wie in Firefox, TLS 1.2 und 1.3 wie ein aktueller Browser. User-Agent kjello-studie/1.0 (+https://www.kjello.de/studien), höchstens 10 Domains gleichzeitig, je Domain alle Anfragen nacheinander mit 0,2 s Pause. Messzeitraum 9. Oktober 2026, 08:16–10:48 Uhr MESZ; 195 Domains ohne Antwort wurden bis 11:02 Uhr einmal nachgemessen.

Auswertungsbasis: 10.107 erreichbare Websites; die Header-Auswertung bezieht sich auf 8.989 HTTPS-Startseiten mit Status 2xx. Konfidenzintervalle: Wilson-Intervall, 95 %. Datenschutzhinweise zu dieser Messung stehen in der Datenschutzerklärung von kjello im Abschnitt „Datenstudien“: kjello.de/datenschutz#datenstudien.

DEFINITIONEN UND GRENZEN

Was die Zahlen bedeuten – und was nicht

Definitionen

Sechs Sicherheits-Header
HSTS, Content-Security-Policy, Schutz vor Einbettung (X-Frame-Options DENY/SAMEORIGIN oder CSP frame-ancestors), X-Content-Type-Options: nosniff, Referrer-Policy, Permissions-Policy. Grundschutz = HSTS + nosniff + Einbettungsschutz.

HSTS aktiv
Strict-Transport-Security mit max-age > 0; Schwellen 180 Tage (Wertung des Mozilla HTTP Observatory) und 1 Jahr (Voraussetzung der Preload-Liste).

Content-Security-Policy
nur durchgesetzte Richtlinien (nicht Report-Only). „Streng“ = script-src bzw. default-src ohne unsafe-inline (außer mit Nonce, Hash oder strict-dynamic) und ohne Platzhalter wie *, https: oder data:.

PHP ohne Sicherheitsupdates
sichtbare PHP-Version 8.1 oder älter; laut php.net (abgerufen 09.10.2026) erhalten nur 8.2 bis 8.5 Updates.

Grenzen der Studie

Nicht repräsentativ für alle Unternehmen
Wikidata verzeichnet vor allem bekanntere Firmen; Kleinstbetriebe fehlen fast ganz. Die Werte sind eher eine Obergrenze für den Schutz.

Nur die Startseite, nur Header
Unterseiten, Portale und Subdomains können anders konfiguriert sein. Fehlende Header sind fehlende Schutzschichten, keine nachgewiesenen Lücken.

Versionsnummern sind ein Indiz, kein Befund
Distributionen und manche Hoster spielen Korrekturen ein, ohne die Versionsnummer zu ändern: „PHP/7.4“ heißt ohne Support durch php.net, nicht zwingend ungepatcht.

Bot-Schutz
288 HTTPS-Startseiten antworteten auf den offen gekennzeichneten Abruf mit 401/403 und fehlen in der Header-Auswertung.

Momentaufnahme
Ein Messtag, ein Messstandort. Weiterleitungen auf andere Domains (11,9 % der Startseiten) zählen zur Ausgangsdomain.

TABELLEN

Alle Ergebnisse im Detail

Tabelle 1 – Datenfluss

SCHRITT	DOMAINS
Stichprobe (aus der Studie „E-Mail-Sicherheit 2026“)	10.586
keine DNS-Auflösung für Domain und www.	192
robots.txt schließt Abrufe aus – nicht gemessen	96
kein Webserver antwortet (auch nach einmaliger Nachmessung)	191
Auswertungsbasis: erreichbare Websites	**10.107**
davon HTTPS mit gültigem Zertifikat	9.367
davon HTTPS-Startseite mit Status 2xx (Basis der Header-Auswertung)	8.989
davon Größe laut Wikidata bekannt	847

Tabelle 2 – Verschlüsselung (Basis: 10.107 erreichbare Websites)

KENNZAHL	WEBSITES	ANTEIL	95-%-KI (%)
HTTPS mit gültigem Zertifikat unter eigener Adresse (mit oder ohne www.)	9.367	92,7 %	92,2–93,2
Zertifikatsfehler (abgelaufen, falscher Name, selbstsigniert …)	191	1,9 %	1,6–2,2
TLS-Verbindungsaufbau scheitert	124	1,2 %	1,0–1,5
kein HTTPS	89	0,9 %	0,7–1,1
eigene HTTPS-Adresse fehlerhaft, http:// leitet auf gültige HTTPS-Seite anderswo	323	3,2 %	2,9–3,6
Weiterleitungsfehler (Schleife oder mehr als 10 Weiterleitungen)	13	0,1 %	0,1–0,2
Summe: eigene HTTPS-Adresse nicht fehlerfrei nutzbar	**740**	**7,3 %**	**6,8–7,8**
Zertifikatswarnung beim direkten Aufruf von https:// (mind. eine Variante)	486	4,8 %	4,4–5,2

Tabelle 3 – Umleitung von HTTP auf HTTPS (Basis: 9.344 Websites mit gültigem HTTPS und HTTP-Antwort)

KENNZAHL	WEBSITES	ANTEIL	95-%-KI (%)
alle http://-Varianten leiten auf HTTPS um	8.644	92,5 %	92,0–93,0
mind. eine http://-Variante liefert die Seite unverschlüsselt aus	372	4,0 %	3,6–4,4
keine http://-Variante leitet auf HTTPS um	263	2,8 %	2,5–3,2

Tabelle 4 – Sicherheits-Header, TLS, security.txt, Cookies (Basis: 8.989 HTTPS-Startseiten mit Status 2xx)

KENNZAHL	STARTSEITEN	ANTEIL	95-%-KI (%)
HSTS aktiv (max-age > 0)	**4.504**	**50,1 %**	**49,1–51,1**
HSTS mit max-age ≥ 180 Tage	4.123	45,9 %	44,8–46,9
HSTS mit max-age ≥ 1 Jahr	3.607	40,1 %	39,1–41,1
HSTS mit includeSubDomains	2.515	28,0 %	27,1–28,9
HSTS preload-fähig (≥ 1 Jahr, includeSubDomains, preload)	1.017	11,3 %	10,7–12,0
Content-Security-Policy (durchgesetzt)	2.267	25,2 %	24,3–26,1
CSP regelt Skripte (script-src/default-src)	1.198	13,3 %	12,6–14,0
CSP regelt Skripte streng (ohne unsafe-inline/Platzhalter)	244	2,7 %	2,4–3,1
CSP ohne Skriptregel (z. B. nur upgrade-insecure-requests)	1.069	11,9 %	11,2–12,6
CSP nur im Beobachtungsmodus (Report-Only)	129	1,4 %	1,2–1,7
Schutz vor Einbettung (X-Frame-Options oder frame-ancestors)	3.914	43,5 %	42,5–44,6
X-Content-Type-Options: nosniff	4.811	53,5 %	52,5–54,6
Referrer-Policy gesetzt	2.799	31,1 %	30,2–32,1
Permissions-Policy gesetzt	1.487	16,5 %	15,8–17,3
alle sechs Sicherheits-Header	**745**	**8,3 %**	**7,7–8,9**
Grundschutz (HSTS + nosniff + Einbettungsschutz)	2.902	32,3 %	31,3–33,3
keiner der sechs Sicherheits-Header	**2.728**	**30,3 %**	**29,4–31,3**
TLS 1.3 ausgehandelt	8.443	93,9 %	93,4–94,4
TLS 1.2 als höchste Version	546	6,1 %	5,6–6,6
gültige security.txt (RFC 9116)	617	6,9 %	6,4–7,4
security.txt abgelaufen	36	0,4 %	0,3–0,6
setzt beim ersten Aufruf Cookies	2.953	32,9 %	31,9–33,8
mind. ein Cookie ohne Secure-Attribut (trotz HTTPS)	1.359	15,1 %	14,4–15,9

Tabelle 5 – Sichtbare Softwareversionen (Basis: 9.657 Websites mit auswertbarer Antwort)

KENNZAHL	WEBSITES	ANTEIL	95-%-KI (%)
Softwareversion im Server- oder X-Powered-By-Header sichtbar	1.858	19,2 %	18,5–20,0
X-Powered-By-Header vorhanden	1.982	20,5 %	19,7–21,3
PHP-Version sichtbar	1.140	11,8 %	11,2–12,5
PHP-Version ohne Sicherheitsupdates von php.net (8.1 oder älter)	**359**	**3,7 %**	**3,4–4,1**
irgendeine sichtbare Software ohne Herstellersupport (PHP ≤ 8.1, Apache ≤ 2.2, OpenSSL < 3.4, IIS ≤ 8.5)	390	4,0 %	3,7–4,4
… Anteil der 1.140 Websites mit sichtbarer PHP-Version	359	31,5 %	28,9–34,2

Sichtbare PHP-Versionen (n = 1.140): 8.5: 37 · 8.4: 181 · 8.3: 345 · 8.2: 218 · 8.1: 85 · 8.0: 34 · 7.4: 140 · 7.3: 25 · 7.2: 16 · 7.1: 7 · 7.0: 6 · 5.6: 24 · 5.5: 4 · 5.4: 11 · 5.3: 3 · 5.1: 2 · 4.4: 1 · 4.2: 1. Laut php.net erhalten nur 8.2 (Sicherheitsupdates bis 31.12.2026), 8.3, 8.4 und 8.5 Updates; Distributionen versorgen eigene Pakete teils länger, Debian 12 etwa sein PHP 8.2 bis 30.06.2028.

Nur 8 der 359 Versionsangaben ohne Support tragen eine Distributionskennung (z. B. -ubuntu, +deb). Distributionen und manche Hoster spielen Sicherheitskorrekturen ein, ohne die Versionsnummer zu ändern – eine sichtbare alte Version heißt „ohne Support durch php.net“, nicht zwingend „ungepatcht“.

Tabelle 6 – Nach Unternehmensgröße (Beschäftigte laut Wikidata)

KENNZAHL	1–49	50–249	250–999	1.000–5.000	UNBEKANNT	UNTER 250	250 BIS 5.000
erreichbare Websites (n)	136	228	269	214	9.260	364	483
HTTPS-Startseiten 2xx (n)	124	206	239	190	8.230	330	429
HTTPS mit gültigem Zertifikat	91,9 %	93,9 %	94,1 %	94,9 %	92,6 %	93,1 %	94,4 %
HSTS aktiv	**46,8 %**	**49,0 %**	**61,1 %**	**60,5 %**	**49,6 %**	**48,2 %**	**60,8 %**
Content-Security-Policy	24,2 %	19,9 %	33,9 %	38,9 %	24,8 %	21,5 %	36,1 %
Schutz vor Einbettung	41,9 %	40,8 %	54,4 %	57,4 %	43,0 %	41,2 %	55,7 %
nosniff	42,7 %	50,5 %	66,5 %	71,1 %	53,0 %	47,6 %	68,5 %
Grundschutz	24,2 %	30,6 %	42,7 %	41,6 %	31,9 %	28,2 %	42,2 %
alle sechs Header	8,9 %	4,9 %	13,4 %	10,5 %	8,2 %	6,4 %	12,1 %
keiner der sechs Header	34,7 %	29,1 %	17,2 %	17,4 %	31,0 %	31,2 %	17,2 %
Softwareversion sichtbar	15,6 %	20,1 %	19,7 %	8,8 %	19,5 %	18,4 %	14,9 %
PHP ohne Sicherheitsupdates sichtbar	7,0 %	3,2 %	3,1 %	0,0 %	3,8 %	4,6 %	1,7 %
gültige security.txt	4,0 %	8,7 %	8,8 %	8,4 %	6,8 %	7,0 %	8,6 %
95-%-KI „HSTS aktiv“	38,2–55,5	42,3–55,8	54,8–67,0	53,4–67,2	48,5–50,7	42,8–53,6	56,1–65,3

Basis je Zeile: HTTPS und Softwareversion = erreichbare Websites; Header und security.txt = HTTPS-Startseiten mit Status 2xx. Die Konfidenzintervalle der einzelnen Größenklassen sind breit und überlappen teils; belastbar ist der Unterschied der zusammengefassten Gruppen (letzte zwei Spalten).

Tabelle 7 – Vergleich mit der Studie „E-Mail-Sicherheit 2026“ (Basis: 9.664 erreichbare Websites mit E-Mail-Empfang)

KENNZAHL	E-MAIL WIRKSAM GESCHÜTZT	E-MAIL NICHT WIRKSAM GESCHÜTZT	DARUNTER: KEIN DMARC
erreichbare Websites (n)	3.671	5.993	2.550
HTTPS-Startseiten 2xx (n)	3.376	5.297	2.173
HTTPS mit gültigem Zertifikat	96,1 %	91,3 %	87,3 %
HSTS aktiv	**58,3 %**	**45,0 %**	**38,7 %**
Content-Security-Policy	31,8 %	20,8 %	16,0 %
Schutz vor Einbettung	51,0 %	38,7 %	33,2 %
nosniff	60,0 %	49,5 %	45,2 %
Grundschutz	39,5 %	27,6 %	22,1 %
alle sechs Header	11,0 %	6,6 %	5,2 %
keiner der sechs Header	23,6 %	34,5 %	39,6 %
TLS 1.3 ausgehandelt	93,9 %	94,0 %	92,6 %
gültige security.txt	10,3 %	4,7 %	2,8 %

„Wirksam geschützt“ wie in der E-Mail-Studie: DMARC quarantine oder reject mit pct = 100 und gültiges SPF. „Kein DMARC“ ist eine Teilgruppe von „nicht wirksam geschützt“. Nach „DMARC durchgesetzt ja/nein“ getrennt ergibt sich dasselbe Bild (HSTS 57,0 % gegenüber 45,3 %).

Auf 8.673 Websites mit beiden Messungen: wirksamer E-Mail-Schutz und HSTS 22,7 %, weder DMARC durchgesetzt noch HSTS 31,9 %. Korrelation, keine Ursache.

PRAXIS

Was Unternehmen jetzt tun können

1. HSTS setzen: Strict-Transport-Security mit einer Laufzeit von mindestens einem Jahr, includeSubDomains erst, wenn alle Subdomains HTTPS beherrschen (OWASP empfiehlt max-age=63072000; includeSubDomains).
2. Den Grundschutz ergänzen: X-Content-Type-Options: nosniff, Schutz vor Einbettung (X-Frame-Options oder CSP frame-ancestors) und eine Referrer-Policy – je eine Zeile in der Webserver-Konfiguration.
3. Eine Content-Security-Policy schrittweise einführen: zuerst als Content-Security-Policy-Report-Only beobachten, dann durchsetzen; Skripte ohne unsafe-inline regeln.
4. Versionsangaben aus Server- und X-Powered-By-Headern entfernen (OWASP) und prüfen, ob die eingesetzte PHP-Version noch Sicherheitsupdates bekommt – von php.net oder vom Distributor.
5. Zertifikate automatisch erneuern, beide Adressvarianten (mit und ohne www.) abdecken und jede http://-Adresse auf HTTPS umleiten.
6. Eine security.txt unter /.well-known/ mit Contact und Expires veröffentlichen (RFC 9116), damit Hinweise auf Schwachstellen den richtigen Empfänger erreichen.

ÜBER KJELLO UND HAGEL IT

kjello ist das Self-Service-IT-Portal von hagel IT für Unternehmen: Arbeitsplätze, Microsoft 365, Zugänge und Geräte an einem Ort – betreut von einem echten Systemhaus mit deutschem Hosting.

Die hagel IT-Services GmbH ist ein inhabergeführtes IT-Systemhaus aus Hamburg, seit 2004 am Markt, und betreut über 150 Unternehmen.

Mit eigenen Datenstudien macht kjello sichtbar, wie es um die IT in Unternehmen in Deutschland steht. Veröffentlicht werden nur Summen und Anteile – nie einzelne Unternehmen, Domains oder Rohdaten.

QUELLEN

Quellen und Einordnung

OWASP

Secure Headers Project – Best Practices, headers_add.json und headers_remove.json (Stand der Listen 04.10.2026) · owasp.github.io/www-project-secure-headers/best-practices

IETF

RFC 6797 HTTP Strict Transport Security (HSTS), November 2012 · www.rfc-editor.org/rfc/rfc6797.html

hstspreload.org

Voraussetzungen der HSTS-Preload-Liste (max-age ≥ 1 Jahr, includeSubDomains, preload); die Betreiber raten vom Preloading ab · hstspreload.org

Mozilla

HTTP Observatory – Tests & Scoring · developer.mozilla.org/en-US/observatory/docs/tests_and_scoring

BSI

TR-02102-2 „Verwendung von Transport Layer Security (TLS)“, Version 2026-01 · www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Techn...

BSI

Mindeststandard „Verwendung von Transport Layer Security (TLS)“, Version 2.4 (für die Bundesverwaltung) · www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststanda...

php.net

Supported Versions und Unsupported Branches (abgerufen 09.10.2026) · www.php.net/supported-versions.php

IETF

RFC 9116 security.txt (April 2022), RFC 9309 Robots Exclusion Protocol · www.rfc-editor.org/rfc/rfc9116.html

Wikidata

Unternehmensdaten (CC0), Abruf 8. Oktober 2026 · www.wikidata.org

HTTP Archive

Web Almanac 2025, Kapitel Security (Januar 2026) · almanac.httparchive.org/en/2025/security

Scott Helme

Top 1 Million Analysis – June 2026 · scotthelme.co.uk/top-1-million-analysis-june-2026-ten-years-of-...

hagel IT

Hamburger IT-Sicherheits-Index 2026 (Oktober 2026) · www.hagel-it.de/it-sicherheits-index-hamburg

BSI

Pressemitteilung „Nur 1,8 Prozent der Webseitenbetreiber nutzen security.txt“, 6. August 2026 · www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Press...

Alle Online-Quellen geprüft im Oktober 2026. Die Rohdaten der Messung enthalten Domainlisten und bleiben intern; alle Zahlen sind mit den Auswertungsskripten aus den Rohdaten reproduzierbar.

NUTZUNG UND IMPRESSUM

Frei verwendbar – mit Quelle

Zitiervorschlag

Quelle: kjello-Studie Website-Sicherheit 2026, kjello.de/studien/website-sicherheit-2026

Lizenz

Texte, Grafiken, Stat-Karten, dieser Report und die aggregierten Tabellen stehen unter Creative Commons Namensnennung 4.0 International (CC BY 4.0). Frei verwendbar – auch gekürzt und bearbeitet –, mit Quellenangabe und Link auf kjello.de/studien/website-sicherheit-2026. Einzelne Unternehmen, Domains oder Rohdaten veröffentlichen wir nicht.

Downloads

Tabellen (CSV), Grafiken (PNG), Stat-Karten und das Pressepaket (ZIP): www.kjello.de/studien/website-sicherheit-2026

Änderungsprotokoll

Version 1.0 vom 17. November 2026
Erstveröffentlichung. Messung der Startseiten von 10.107 erreichbaren Unternehmenswebsites am 9. Oktober 2026.

Impressum und Pressekontakt

hagel IT-Services GmbH · Spaldingstraße 64-68 · 20097 Hamburg
Geschäftsführer: Philip Kraatz · Amtsgericht Hamburg, HRB 99898 · USt-IdNr. DE252818864
kjello ist eine Marke der hagel IT-Services GmbH.
Pressekontakt: hallo@kjello.de · 040 28410268-0

kjello.