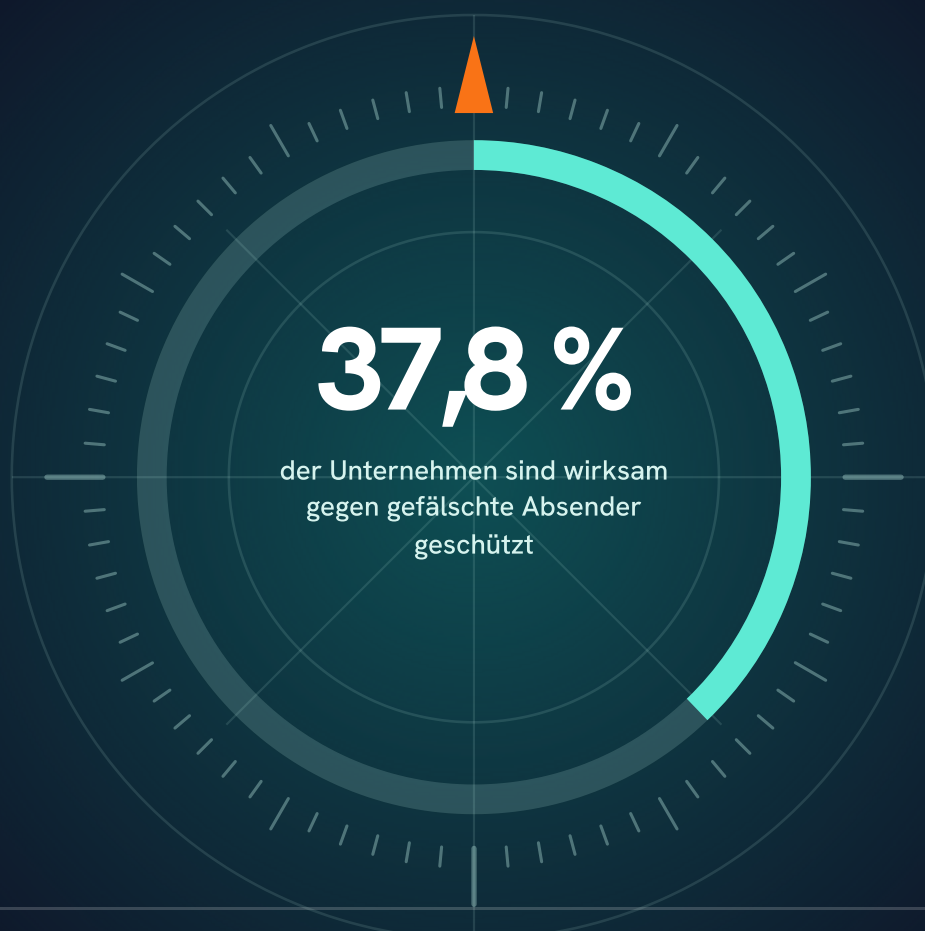


● KJELLO-STUDIE

E-Mail-Sicherheit 2026

Wer schützt seine Domain vor gefälschten Absendern?

**HERAUSGEBER**

kjello · hagel IT-Services
GmbH, Hamburg

DATENSTAND

8. Oktober 2026, Messung
13:01-13:49 Uhr MESZ

GRUNDLAGE

DNS-Messung von 9.935
Unternehmensdomains in
Deutschland (ohne
Konzerne), 8. Oktober 2026

VERSION

1.1 · 9. Oktober 2026
Lizenz CC BY 4.0

INHALT

E-Mail-Sicherheit 2026

01	Management Summary	3
02	Kernaussagen	4
03	DMARC: veröffentlicht, aber selten durchgesetzt	5
04	Kleinbetriebe am schlechtesten geschützt	6
05	Wo das Postfach liegt, macht einen großen Unterschied	7
06	Moderne Transportverfahren kaum verbreitet	8
07	Einordnung: frühere Erhebungen	9
08	Methodik	10
09	Definitionen und Grenzen	11
10	Tabellen	12
11	Was Unternehmen jetzt tun können	14
12	Quellen	15
13	Zitiervorschlag, Lizenz und Impressum	16

Auf einen Blick

37,8 %

wirksam gegen gefälschte
Absender geschützt

26,8 %

ohne jeden DMARC-Eintrag

42,8 %

der Microsoft-365-Domains
wirksam geschützt

Steckbrief

Herausgeber	kjello – eine Marke der hagel IT-Services GmbH, Hamburg
Grundlage	9.935 Unternehmensdomains mit E-Mail-Empfang – Unternehmen mit Sitz in Deutschland, ohne Konzerne mit mehr als 5.000 Beschäftigten.
Datenstand	8. Oktober 2026, Messung 13:01–13:49 Uhr MESZ
Veröffentlicht	8. Oktober 2026 · Version 1.1
Online	kjello.de/studien/email-sicherheit-2026 – mit Tabellen (CSV), Grafiken und Pressepaket
Nutzung	frei mit Quellenangabe und Link (CC BY 4.0)

MANAGEMENT SUMMARY

E-Mail-Sicherheit 2026: Wer schützt seine Domain vor gefälschten Absendern?

Jeder kann eine E-Mail mit fremder Absenderadresse verschicken – das Mailprotokoll prüft das von sich aus nicht. Ob empfangende Mailserver gefälschte Mails unter einem Firmennamen abweisen, legt das Unternehmen selbst fest: mit drei Einträgen im öffentlichen DNS seiner Domain (SPF, DKIM, DMARC).

kjello hat diese Einträge am 8. Oktober 2026 für 9.935 Unternehmensdomains gemessen – Unternehmen mit Sitz in Deutschland, ohne Konzerne mit mehr als 5.000 Beschäftigten. Ergebnis: Nur 37,8 % sind wirksam gegen gefälschte Absender geschützt. 26,8 % haben gar keinen DMARC-Eintrag, weitere 30,8 % beobachten nur (p=none).

Große Unterschiede zeigen sich je nach Mail-Anbieter und Unternehmensgröße: Bei Domains mit Postfach bei IONOS sind 6,2 % wirksam geschützt, bei Microsoft 365 42,8 %, bei Kleinbetrieben unter 50 Beschäftigten 21,3 %. Die im DNS prüfbaren Kernanforderungen der BSI-Richtlinie TR-03182 erfüllen 27,0 %.

EINORDNUNG DER REDAKTION

Die Messung zeigt weniger ein Wissens- als ein Umsetzungsproblem. Die nötigen Einträge kosten nichts und sind seit Jahren standardisiert; trotzdem steht ein großer Teil der Unternehmen bei p=none oder ganz ohne DMARC. Auffällig ist, wie stark sich die Ergebnisse je nach Mail-Anbieter unterscheiden – und wie oft Domains beim selben Anbieter wortgleiche Einträge tragen. Das spricht dafür, dass viele Unternehmen eine Vorgabe ihres Hosters übernehmen, statt den Eintrag selbst zu gestalten. Wer seine Domain schützen will, kommt um einen bewussten Schritt von p=none zu quarantine oder reject nicht herum.

KERNAUSSAGEN

Die Ergebnisse in 8 Sätzen

01

37,8 %

Nur gut jedes dritte Unternehmen ist wirksam gegen gefälschte Absender unter seinem Firmennamen geschützt.

95%-Konfidenzintervall 36,9–38,8 %

02

26,8 %

Jedes vierte Unternehmen hat gar keinen DMARC-Eintrag – nicht einmal die Mindestanforderung, die Google, Yahoo und Microsoft an Großversender stellen.

03

42 %

der vorhandenen DMARC-Einträge schützen nicht, sie beobachten nur (`p=none`). Die volle Abweisung nutzen nur 20,7 % aller Domains.

04

27,0 %

erfüllen die im DNS prüfbaren Kernanforderungen der BSI-Richtlinie TR-03182 „E-Mail-Authentifizierung“.

05

21,3 %

der Firmen mit weniger als 50 Beschäftigten sind wirksam geschützt – bei 250 bis 999 Beschäftigten sind es 48,7 %.

06

42,8 %

der Domains, deren Mails Microsoft 365 direkt annimmt, sind wirksam geschützt. Erkennbar ist Microsoft 365 auf 56,3 % der Domains.

07

6,2 %

der Domains mit Postfach bei IONOS sind wirksam geschützt.

08

3,0 %

erzwingen verschlüsselte Zustellung per MTA-STS, 5,9 % sichern ihre DNS-Einträge mit DNSSEC.

Basis: DNS-Messung von 9.935 Unternehmensdomains in Deutschland (ohne Konzerne), 8. Oktober 2026. Anteile in Prozent der Domains.

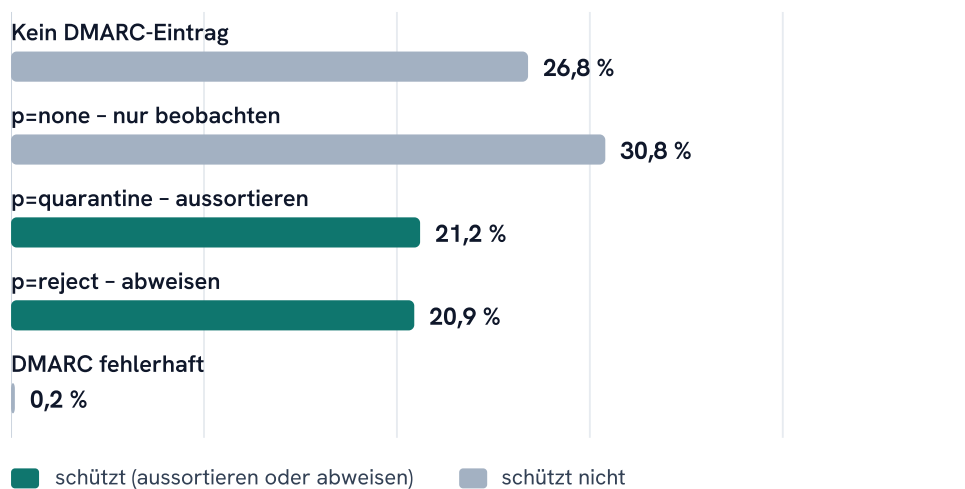
KAPITEL 1

DMARC: veröffentlicht, aber selten durchgesetzt

ABBILDUNG 1

Nur 40,7 % der Domains setzen DMARC vollständig durch

DMARC-Richtlinie der Unternehmensdomains, Anteil in % (n = 9.935)



Quelle: kjello-Studie E-Mail-Sicherheit 2026, DNS-Messung vom 8. Oktober 2026 · In p=quarantine und p=reject stecken 1,4 % der Domains mit pct < 100, die nur einen Teil der Mails erfassen. Vollständig durchgesetzt (pct = 100) sind 40,7 %, die volle Abweisung (p=reject, pct = 100) nutzen 20,7 %. Summe rundungsbedingt 99,9 %.

Wirksam gegen gefälschte Absender ist eine Domain erst, wenn DMARC eine Abwehrregel durchsetzt (`p=quarantine` oder `p=reject` für alle Mails) und der SPF-Eintrag gültig ist. Das trifft auf 37,8 % der 9.935 untersuchten Domains zu.

42 % der vorhandenen DMARC-Einträge schützen nicht – sie beobachten nur. 30,8 % aller Domains haben DMARC auf `p=none` gesetzt. Das liefert bestenfalls Berichte, hält aber keine einzige gefälschte Mail auf. Die volle Abweisung (`p=reject` für alle Mails) nutzen nur 20,7 %.

Ein Viertel der Domains (26,8 %) hat überhaupt keinen DMARC-Eintrag. Diese Domains erfüllen damit nicht einmal die Mindestanforderung, die Google und Yahoo seit Februar 2024 und Microsoft seit Mai 2025 von Großversendern verlangen (Google und Microsoft ab 5.000 Mails pro Tag, Yahoo ohne feste Schwelle). Die im DNS prüfbaren Kernanforderungen der BSI-Richtlinie TR-03182 erfüllen 27,0 %.

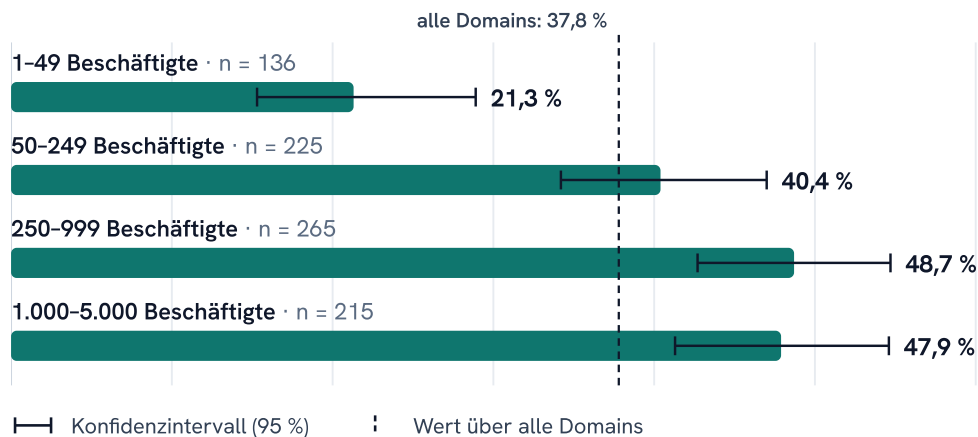
KAPITEL 2

Kleinbetriebe am schlechtesten geschützt

ABBILDUNG 2

Je kleiner das Unternehmen, desto seltener wirksam geschützt

Wirksam gegen Absenderfälschung geschützte Domains nach Beschäftigten laut Wikidata, in % mit Konfidenzintervall (95 %)



Quelle: kjello-Studie E-Mail-Sicherheit 2026, DNS-Messung vom 8. Oktober 2026 · Die Größe ist nur für 841 der 9.935 Domains bekannt; die Gruppen sind klein (136 bis 265 Domains) und haben weite Konfidenzintervalle. Domains ohne Größenangabe (n = 9.094): 37,4 %.

Bei Firmen mit weniger als 50 Beschäftigten sind nur 21,3 % wirksam geschützt, bei 250 bis 999 Beschäftigten 48,7 %. 37,5 % der Kleinbetriebe haben überhaupt kein DMARC.

Die Größe ist nur für 841 der 9.935 Domains bekannt. Die Gruppen sind klein und die Konfidenzintervalle weit – die Richtung ist aber eindeutig: Je kleiner das Unternehmen, desto seltener ist die eigene Domain gegen Fälschung abgesichert.

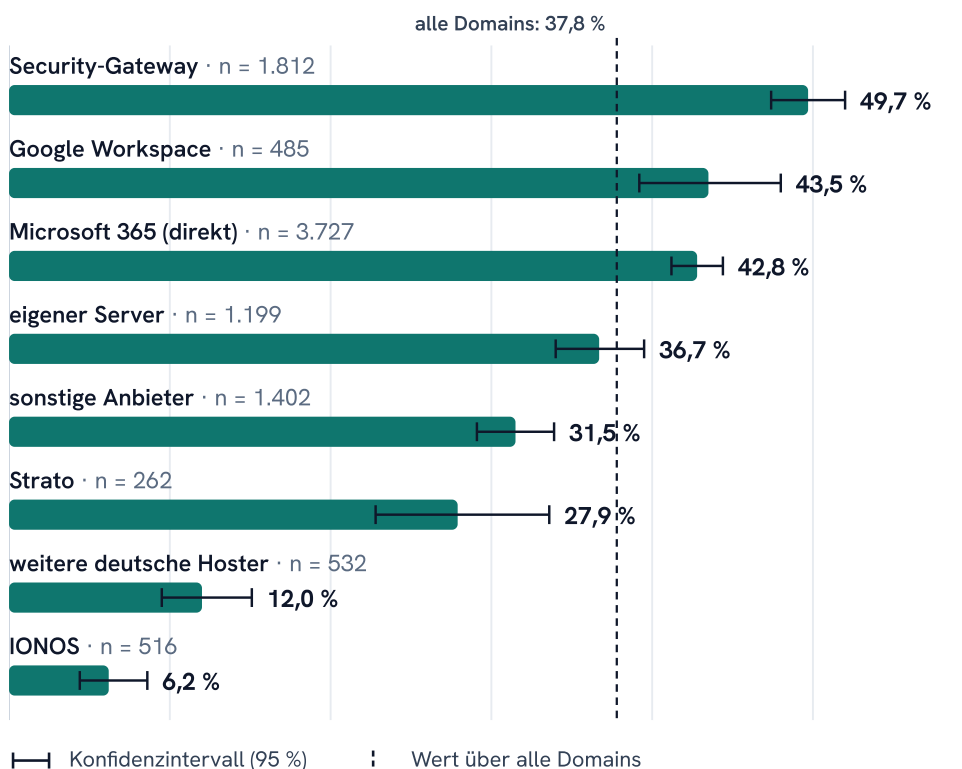
KAPITEL 3

Wo das Postfach liegt, macht einen großen Unterschied

ABBILDUNG 3

Wirksamer Schutz hängt stark vom Mail-Anbieter ab

Wirksam geschützte Domains nach Mail-Anbieter (Server mit höchster Priorität im MX-Eintrag), in % mit Konfidenzintervall (95 %)



Quelle: kjello-Studie E-Mail-Sicherheit 2026, DNS-Messung vom 8. Oktober 2026 · Wirksam geschützt = DMARC p=quarantine oder p=reject für alle Mails (pct = 100) und gültiges SPF. Bei Strato setzen 86 % DMARC durch, aber 63 % dieser Domains haben keinen SPF-Eintrag – nach dieser Definition zählen sie nicht als „wirksam“. Security-Gateway: Hornetsecurity, Proofpoint, Mimecast u. a.; hinter 1.108 dieser 1.812 Domains ist Microsoft 365 per SPF erkennbar.

Auf 56,3 % der Domains ist Microsoft 365 erkennbar (Mail-Server oder SPF-Eintrag), bei 37,5 % nimmt Microsoft die Mails direkt an. Von diesen Domains sind aber nur 42,8 % wirksam gegen Absenderfälschung geschützt, und bei einem Drittel (33,1 %) ist für die eigene Domain kein DKIM-Schlüssel nachweisbar.

Bei Domains mit Postfach bei IONOS sind nur 6,2 % wirksam geschützt – 86 % tragen DMARC im reinen Beobachtungsmodus, neun von zehn davon mit demselben Minmaleintrag `v=DMARC1 ; p=none` ;. Bei Strato setzen 86 % DMARC durch, fast immer mit demselben Eintrag `v=DMARC1 ; p=reject` ;, aber nur 37 % haben überhaupt einen SPF-Eintrag. Dass so viele Domains wortgleiche Einträge tragen, spricht dafür, dass Kunden eine Vorgabe ihres Hosters übernehmen, statt den Eintrag selbst zu gestalten.

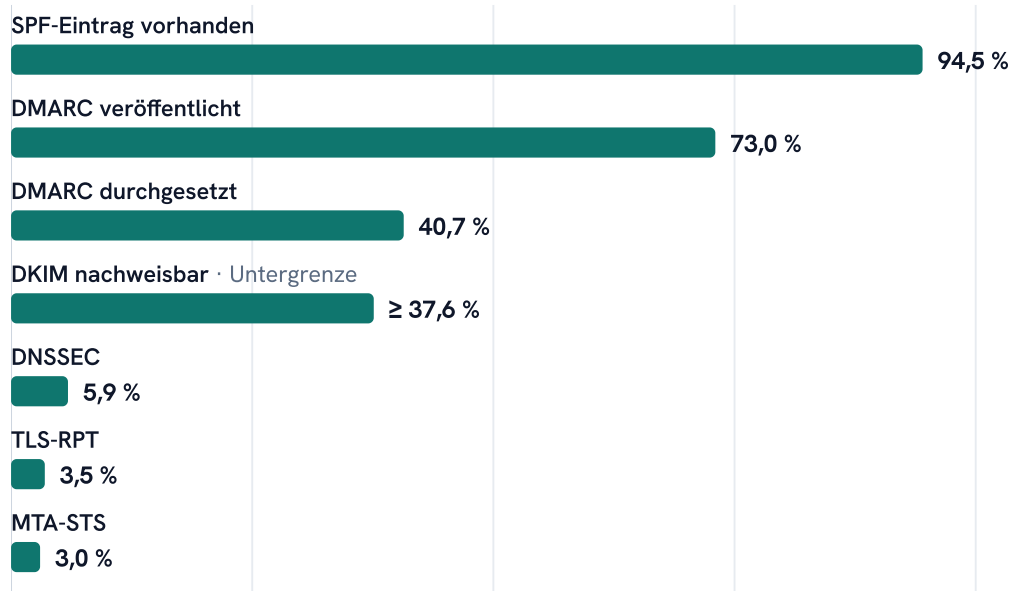
KAPITEL 4

Moderne Transportverfahren kaum verbreitet

ABBILDUNG 4

SPF ist fast überall – moderne Transportverfahren kaum

Anteil der Domains mit dem jeweiligen Verfahren, in % (n = 9.935)



Quelle: kjello-Studie E-Mail-Sicherheit 2026, DNS-Messung vom 8. Oktober 2026 · DKIM nur über zwei Standard-Selektoren geprüft (selector1 für Microsoft, google für Workspace) – der Wert ist eine Untergrenze. MTA-STS nur über den DNS-Eintrag _mta-sts erfasst.

SPF ist mit 94,5 % fast überall vorhanden. Nur 3,0 % erzwingen dagegen verschlüsselte Zustellung per MTA-STS, 3,5 % lassen sich Zustellfehler per TLS-RPT melden, und nur 5,9 % sichern ihre DNS-Einträge mit DNSSEC gegen Manipulation ab.

Nebenbefund: 548 Domains der Stichprobe nehmen keine Mails an (kein MX oder Null-MX). Die BSI TR-03182 verlangt für solche Domains Null-MX, `v=spf1 -all` und DMARC reject mit Berichtsadresse. Das erfüllen 1,6 % (9 von 548).

EINORDNUNG

Was frühere Erhebungen zeigen

Frühere Erhebungen zeigen ein ähnliches Bild – mit anderen Stichproben und meist milderer Definitionen. Unsere Kennzahl „wirksam geschützt“ verlangt zusätzlich ein gültiges SPF und ist damit strenger als reine Zählungen der DMARC-Richtlinie; ohne die SPF-Bedingung läge sie bei 40,7 %.

BSI · SEPTEMBER 2026**Das E-Mail-Sicherheitsjahr – Abschlussbericht**

„Über 30 Prozent aller Organisationen verfügen über keinen DMARC-Eintrag.“ DNSSEC erreichte unter .de-Domains vor Beginn des Sicherheitsjahrs knapp 4 %. Grundgesamtheit und Stichtag nennt der Bericht nicht. Unsere Messung liegt in derselben Größenordnung: 26,8 % ohne DMARC, 5,9 % mit DNSSEC.

<https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/EMSJ/EMSJ-Abschlussbericht-2026.pdf>

DMARCIAN · AUGUST 2026**DMARC Adoption in Germany 2026**

Die 250 umsatzstärksten deutschen Konzerne: 12 % ohne DMARC, 18 % **p=none**, 15 % **p=quarantine**, 40 % **p=reject**, 15 % mit Fehlern oder abweichend von Best Practices. Großunternehmen sind deutlich weiter als die von uns untersuchten Unternehmen ohne Konzerne (26,8 % ohne DMARC, 20,9 % **p=reject**) – das passt zu unserem Befund, dass der Schutz mit der Größe steigt.

<https://dmarcian.com/germany-dmarc-adoption/>

HIGH5MANUFAKTUR · SEPTEMBER 2026**Mail-Sicherheit im Raum Karlsruhe 2026**

Regionale Messung von 3.380 Betrieben mit Website (Karlsruhe, Rastatt, Calw, Pforzheim): SPF 77,3 %, DMARC 56,3 %, davon 58 % auf **p=none**; quarantine oder reject (ohne SPF-Bedingung) 23,9 %, MTA-STS 1,1 %. Die Stichprobe enthält viele Kleinstbetriebe und liegt deutlich unter unseren Werten – ein Hinweis darauf, dass unsere Zahlen eher eine Obergrenze sind.

<https://h5m.de/mail-sicherheit-studie>

EASYDMARC · 2026**2026 DMARC Adoption & Enforcement Report**

Weltweit, 1,8 Mio. meistbesuchte Domains: 52,1 % mit gültigem DMARC, 29,2 % **p=none**, 22,9 % **p=quarantine** oder **p=reject**. Keine eigene Auswertung für Deutschland. Zum Vergleich: In unserer Messung haben 73,0 % ein gültiges DMARC.

<https://easydmarc.com/blog/ebook/dmarc-adoption-report-2026/>

WAS AN DIESER MESSUNG NEU IST

- Bundesweite Messung von Unternehmen ohne Konzerne – mit offengelegter Auswahl (Wikidata, 14 Ausschlussregeln) statt Top-Listen oder einer einzelnen Region.
- Strengere Kernkennzahl: durchgesetztes DMARC und gültiges SPF, dazu der Abgleich mit den DNS-Kernanforderungen der BSI TR-03182.
- Aufschlüsselung nach Mail-Anbieter (Microsoft 365, Security-Gateway, Google Workspace, IONOS, Strato u. a.) und nach Unternehmensgröße, jeweils mit Konfidenzintervall.
- Aktueller Stand vom 8. Oktober 2026, alle aggregierten Tabellen frei als CSV.

METHODIK

So wurde gemessen

Quelle der Unternehmen ist Wikidata (Abruf 8. Oktober 2026). Kandidaten sind alle Einträge mit Land = Deutschland, einer offiziellen Website und einer Unternehmensklasse oder einer deutschen Rechtsform. Aus 15.047 Kandidaten und 14.961 Domains wurden nach festen Regeln Nicht-Unternehmen, Konzerne über 5.000 Beschäftigte, ausländische Gesellschaften und öffentliche Unternehmen ausgeschlossen (Stichprobe: 10.586 Domains).

Gemessen wurde ausschließlich öffentliches DNS über DNS-over-HTTPS (Cloudflare 1.1.1.1), gedrosselt auf höchstens 35 Anfragen pro Sekunde – keine Portscans, keine Verbindung zu Mail- oder Webservern. Je Domain: MX, SPF (rekursiv mit Zählung der DNS-Lookups nach RFC 7208), `_dmarc`, `_mta-sts`, `_smtp._tls` und die DKIM-Selektoren `selector1` und google; DNSSEC über das AD-Bit.

19 Domains blieben nach Nachmessung fehlerhaft, 84 existieren nicht mehr, 548 nehmen keine Mails an. Auswertungsbasis: 9.935 Domains mit E-Mail-Empfang. Konfidenzintervalle: Wilson-Intervall, 95 %.

Datenschutzhinweise zu dieser Messung (Zweck, Rechtsgrundlage, Speicherdauer, Widerspruch) stehen in der Datenschutzerklärung von kjello im Abschnitt „Datenstudien“: kjello.de/datenschutz#datenstudien.

Ausschlussregeln (jede Domain zählt bei der ersten zutreffenden Regel)

REGEL	DOMAINS
R1 aufgelöst (P576)	559
R2 Rechtsform kein Unternehmen (Verein, Stiftung, Körperschaft/Anstalt öff. Rechts, gGmbH, gUG, VVaG ...)	376
R3 Klasse kein Unternehmen / Medien / Bank / Versicherung	1.185
R6 Klasse fällt über Oberbegriffe unter Medien, öffentliche Hand, Bildung/Forschung, Finanzen, Gemeinnützige, Krankenhaus/Kultur	697
R7 nur ausländische Rechtsform (B.V., S.A., Ltd., LLC ...)	127
R8 Hauptsitz im Ausland oder Sitzländer uneindeutig	120
R13 Eigentümer ist Gebietskörperschaft/Behörde (Stadtwerke, Verkehrsbetriebe, Landesgesellschaften)	281
R14 Name weist auf Stadtwerk, Sparkasse, Volks-/Raiffeisenbank, Versicherung hin	148
R5 selbst mehr als 5.000 Beschäftigte	200
R10 Mutterorganisation (transitiv) mit mehr als 5.000 Beschäftigten	463
R12 Umsatz des Eintrags oder seiner Mutter/Großmutter über 1 Mrd. €	55
R11 Domain gehört laut Wikidata einer Organisation mit mehr als 5.000 Beschäftigten	37
R9 Länderendung eines anderen Staates (.it, .at, .ch, .nl, .co.uk ...)	127
Stichprobe	10.586 Domains

DEFINITIONEN UND GRENZEN

Was die Zahlen bedeuten – und was nicht

Definitionen

Wirksam geschützt (Kernkennzahl)

DMARC `p=quarantine` oder `p=reject` mit pct = 100 und gültiges SPF (genau ein `v=spf1`-Eintrag, höchstens 10 DNS-Lookups, alle Ziele existieren, kein +all). Ohne die SPF-Bedingung läge der Wert bei 40,7 %.

BSI TR-03182 (DNS-Kern)

wirksam geschützt und SPF endet auf -all oder ~all (TR-03182-01-M) und DMARC mit mindestens einer `rua`-Adresse (TR-03182-06-M). Die DKIM-Pflichten der TR sind per DNS nicht vollständig prüfbar.

DMARC

genau ein `v=DMARC1`-Eintrag mit gültigem p=. Mehrere Einträge oder fehlendes p= gelten als fehlerhaft. Fehlt pct, gilt 100.

Mail-Anbieter

nach dem MX-Eintrag mit der höchsten Priorität; ein vorgeschaltetes Security-Gateway zählt als Gateway.

Grenzen der Studie

Nicht repräsentativ für alle Unternehmen

Wikidata verzeichnet vor allem bekanntere Firmen. Kleinstbetriebe ohne öffentliche Spuren fehlen fast ganz – die Ergebnisse sind eher eine Obergrenze.

Größe meist unbekannt

Nur für 841 der 9.935 Domains (8,5 %) nennt Wikidata eine Mitarbeiterzahl. Eine Abgrenzung nach IfM- oder EU-Definition des Mittelstands war nicht möglich.

Konzernzugehörigkeit unvollständig

Vereinzelt bleiben Töchter großer Gruppen in der Stichprobe; umgekehrt kann eine eigenständige Firma fälschlich ausgeschlossen sein.

Domain ≠ Unternehmen

Gemessen wird die in Wikidata hinterlegte Website-Domain. Versendet eine Firma von einer anderen Domain, ist diese nicht erfasst.

Nur DNS, Momentaufnahme

Gemessen ist, was die Domain veröffentlicht – nicht, ob Empfänger es auswerten oder ob DKIM tatsächlich signiert. Eingehender Schutz (Spam- und Phishing-Filter) ist nicht Gegenstand der Studie.

DKIM und MTA-STS nur teilweise prüfbar

DKIM-Werte sind Untergrenzen; bei MTA-STS wurde nur der DNS-Eintrag erfasst, nicht die Richtliniendatei.

TABELLEN

Alle Ergebnisse im Detail

Tabelle 1 – Gesamtergebnis

KENNZAHL	DOMAINS	ANTEIL	95%-KI (%)
SPF-Eintrag vorhanden	9.386	94,5 %	94,0–94,9
SPF gültig (genau ein Eintrag, ≤ 10 DNS-Lookups, kein +all)	9.081	91,4 %	90,8–91,9
SPF endet auf -all (hart)	5.596	56,3 %	55,3–57,3
SPF endet auf ~all (weich)	3.399	34,2 %	33,3–35,2
SPF mit ?all, +all oder ohne all	176	1,8 %	1,5–2,1
SPF-Regel per redirect beim Dienstleister	193	1,9 %	1,7–2,2
Mehrere SPF-Einträge (Fehler)	22	0,2 %	0,1–0,3
SPF mit mehr als 10 DNS-Lookups (Fehler)	170	1,7 %	1,5–2,0
DMARC gültig veröffentlicht	7.254	73,0 %	72,1–73,9
Kein DMARC-Eintrag	2.666	26,8 %	26,0–27,7
DMARC fehlerhaft (mehrere Einträge / ohne p=)	15	0,2 %	0,1–0,2
DMARC p=none (nur beobachten)	3.063	30,8 %	29,9–31,7
DMARC p=quarantine	2.111	21,2 %	20,5–22,1
DMARC p=reject	2.080	20,9 %	20,1–21,7
DMARC p=reject mit pct = 100 (volle Abweisung)	2.054	20,7 %	19,9–21,5
DMARC quarantine/reject mit pct < 100	144	1,4 %	1,2–1,7
DMARC durchgesetzt (quarantine/reject, pct = 100)	4.047	40,7 %	39,8–41,7
DMARC mit Berichtsadresse (rua)	4.613	46,4 %	45,5–47,4
Wirksam gegen Absenderfälschung geschützt	3.756	37,8 %	36,9–38,8
DNS-Kernanforderungen BSI TR-03182 erfüllt	2.684	27,0 %	26,2–27,9
MTA-STX angekündigt (DNS)	302	3,0 %	2,7–3,4
TLS-RPT eingerichtet	348	3,5 %	3,2–3,9
DNSSEC validiert	586	5,9 %	5,5–6,4
DKIM nachweisbar (zwei Standard-Selektoren, Untergrenze)	3.731	37,6 %	36,6–38,5

DKIM: nur zwei Standard-Selektoren geprüft (selector1, google) – der Wert ist eine Untergrenze.

Tabelle 2 – Nach Unternehmensgröße (Beschäftigte laut Wikidata)

KENNZAHL	1–49	50–249	250–999	1.000–5.000	UNBEKANNT
Domains (n)	136	225	265	215	9.094
kein DMARC	37,5 %	22,2 %	20,0 %	18,1 %	27,2 %
DMARC p=none	36,8 %	32,4 %	26,8 %	30,2 %	30,8 %
DMARC durchgesetzt	24,3 %	43,1 %	51,3 %	50,7 %	40,4 %
wirksam geschützt	21,3 %	40,4 %	48,7 %	47,9 %	37,4 %
95-%-KI „wirksam“	15,3–28,9	34,2–47,0	42,7–54,7	41,3–54,6	36,4–38,4
BSI TR-03182 (DNS-Kern)	15,4 %	27,6 %	41,5 %	40,0 %	26,4 %
SPF hart (-all)	55,9 %	59,6 %	70,6 %	71,2 %	55,5 %
DNSSEC	1,5 %	5,8 %	8,3 %	7,9 %	5,9 %

Tabelle 3 – Nach Mail-Anbieter (Server mit höchster Priorität im MX-Eintrag)

ANBIETER	ANTEIL	N	KEIN DMARC	P=NONE	DURCHGESETZT	WIRKSAM	DKIM
Microsoft 365 (direkt)	37,5 %	3.727	25,9 %	28,1 %	44,3 %	42,8 %	66,9 % ⁴
Security-Gateway ¹	18,2 %	1.812	19,6 %	27,5 %	51,2 %	49,7 %	–
Google Workspace	4,9 %	485	16,1 %	34,4 %	46,2 %	43,5 %	71,8 % ⁴
IONOS	5,2 %	516	6,6 %	85,7 %	6,6 %	6,2 %	–
Strato ²	2,6 %	262	3,1 %	10,3 %	86,3 %	27,9 %	–
weitere deutsche Hoster ³	5,4 %	532	53,0 %	32,0 %	13,3 %	12,0 %	–
eigener Server (MX unter eigener Domain)	12,1 %	1.199	33,0 %	27,5 %	37,9 %	36,7 %	–
sonstige Anbieter	14,1 %	1.402	39,1 %	27,2 %	32,7 %	31,5 %	–

¹ Hornetsecurity, Proofpoint, Mimecast, Sophos, Cisco, NoSpamProxy, Trend Micro, Retarus, Barracuda, eXpurgate, Fortinet u. a. Hinter 1.108 dieser 1.812 Domains (61 %) ist Microsoft 365 per SPF erkennbar.

² Bei Strato setzen 86 % DMARC durch, fast immer mit demselben Eintrag v=DMARC1;p=reject; – aber 63 % dieser Domains haben keinen SPF-Eintrag und zählen nach der Definition dieser Studie nicht als „wirksam“.

³ All-Inkl, DomainFactory, Mittwald, Hetzner, united-domains, Telekom, Host Europe, mailbox.org u. a.

⁴ Nur der anbieterübliche Selektor geprüft (selector1 für Microsoft, google für Workspace) – Untergrenze.

„Wirksam geschützt“ = DMARC p=quarantine oder p=reject für alle Mails (pct = 100) und gültiges SPF.

PRAXIS

Was Unternehmen jetzt tun können

- 1 Die eigenen Einträge prüfen: SPF als TXT-Eintrag am Domainnamen, DMARC als TXT-Eintrag unter `_dmarc`. Beides ist öffentlich und kostenlos abfragbar.
- 2 Fehlt DMARC, zunächst einen Eintrag mit `p=none` und einer Berichtsadresse (`rua`) veröffentlichen. Die Berichte zeigen nach einigen Wochen, welche Dienste im Namen der Firma senden.
- 3 Alle legitimen Absender – Postfachdienst, Newsletter-Werkzeug, Rechnungsversand, Webshop – im SPF-Eintrag erfassen und für DKIM einrichten.
- 4 Die Richtlinie dann auf `p=quarantine` und später auf `p=reject` stellen. Erst dann weisen Empfänger gefälschte Mails unter dem Firmennamen ab.
- 5 Wer Microsoft 365 nutzt, prüft zusätzlich, ob DKIM für die eigene Domain eingeschaltet ist – bei einem Drittel der Microsoft-365-Domains war das in dieser Messung nicht nachweisbar.
- 6 Domains, die keine Mails versenden, absichern: Null-MX, `v=spf1 -all` und DMARC `p=reject` mit Berichtsadresse (BSI TR-03182-11-M).

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

Google

Leitfaden für E-Mail-Absender (Anforderungen ab 1. Februar 2024) · support.google.com/a/answer/81126?hl=de

Yahoo

Sender Best Practices (ab Februar 2024) · senders.yahooinc.com/best-practices

Microsoft

Strengthening Email Ecosystem: Outlook's New Requirements for High-Volume Senders, 2. April 2025 · techcommunity.microsoft.com/blog/microsoftdefenderforoffice365b...

BSI

TR-03182 „E-Mail-Authentifizierung“, Version 1.0, 24. Januar 2024 · www.bsi.bund.de/dok/TR-03182

IETF

RFC 7208 (SPF), RFC 9989 (DMARC, löst RFC 7489 ab), RFC 6376 (DKIM), RFC 8461 (MTA-STS), RFC 8460 (TLS-RPT), RFC 7505 (Null-MX) · www.rfc-editor.org

Wikidata

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

BSI

Das E-Mail-Sicherheitsjahr – Abschlussbericht, September 2026 · www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/EMSJ/...

dmarcian

DMARC Adoption in Germany 2026, August 2026 (aktualisiert 14. September 2026) · dmarcian.com/germany-dmarc-adoption

High5Manufaktur

Mail-Sicherheit im Raum Karlsruhe 2026, Messung vom 24. September 2026 · h5m.de/mail-sicherheit-studie

EasyDMARC

2026 DMARC Adoption & Enforcement Report · easydmarc.com/blog/ebook/dmarc-adoption-report-2026

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 E-Mail-Sicherheit 2026, kjello.de/studien/email-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/email-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/email-sicherheit-2026

Änderungsprotokoll

Version 1.0 vom 8. Oktober 2026

Erstveröffentlichung. DNS-Messung von 9.935 Unternehmensdomains am 8. Oktober 2026.

Version 1.1 vom 9. Oktober 2026

Formulierungen zu Mail-Anbietern präzisiert (gemessen sind wortgleiche Einträge, nicht die Vorgabe des Hosters), Schwellenwerte der Großversender-Regeln präzisiert, DMARC-Norm auf RFC 9989 aktualisiert. Alle Zahlen unverändert.

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

