E-Mail-Authentifizierung

Schutzschild für Ihre Domain – Türöffner zum Posteingang

Herausgeber:

DDV Deutscher Dialogmarketing Verband e. V.
eco – Verband der Internetwirtschaft e. V.

CSA
Certified Senders Alliance

Inhaltsverzeichnis

1. Executive Summary

Wussten Sie schon?

- **Gmail und Yahoo** verlangen seit Februar 2024 von allen Versendern ab 5.000 E-Mails pro Tag den Einsatz von SPF, DKIM und DMARC sowie eine leicht nutzbare Abmeldemöglichkeit.
- **Microsoft** zog in 2025 mit vergleichbaren Vorgaben für Outlook-Consumer-Domains nach.
- **Ziel dieser Maßnahmen:** weniger Angriffsflächen für Betrüger und eine bessere Qualität der E-Mails im Posteingang.

Faktenlage

Die Bedrohungslage ist dramatisch. Hornetsecurity untersuchte 45 Milliarden E-Mails aus dem Jahr 2023. Ergebnis: 36,4 Prozent waren unerwünscht, 3,6 Prozent eindeutig bösartig – das entspricht über 589 Millionen gefährlichen Nachrichten in nur einem Jahr. Phishing machte 43,3 Prozent aller Angriffe aus, die höchste je gemessene Quote (Quelle: Hornetsecurity).

Kaspersky registrierte 2024 weltweit mehr als 893 Millionen blockierte Phishing-Versuche – ein Anstieg um 26 Prozent gegenüber dem Vorjahr (Kaspersky 2025). Betroffen waren nahezu alle Branchen, besonders Web-Services, Internetportale und Banken, aber auch Handel, Lieferdienste und soziale Netzwerke.

Die wirtschaftlichen Folgen sind gravierend. Laut Bitkom beliefen sich die Schäden durch Cyberangriffe in Deutschland 2024 auf 267 Milliarden Euro. Sie umfassen direkte Umsatzeinbußen, Störungen von IT-Systemen, Rechtskosten und langfristigen Reputationsverlust (Quelle: Bitkom 2024).

Konsequenz

E-Mail-Authentifizierung ist keine technische Option mehr. Sie ist heute die Eintrittskarte in den Posteingang. Unternehmen, die SPF, DKIM und DMARC nicht korrekt implementieren, riskieren Blockaden, Reputationsschäden und finanziellen Verlust.

Empfehlung

Dieses Whitepaper erläutert, wie Unternehmen mit SPF, DKIM und DMARC die Basis für sichere Kommunikation schaffen, welche organisatorischen und technischen Hürden zu meistern sind und warum Monitoring zum strategischen Frühwarnsystem wird. Es macht deutlich, dass E-Mail-Authentifizierung Pflicht ist und dass Partner wie die Certified Senders Alliance (CSA) über Transparenz den Schlüssel zu langfristigem Vertrauen und stabiler Zustellbarkeit liefern.

2. Einleitung

> **Executive Insight:** E-Mail-Authentifizierung ist Pflicht. Ohne sie drohen Spam, Blockaden und Missbrauch.

E-Mail ist das Rückgrat moderner Unternehmenskommunikation. Sie ist schnell, kostengünstig und universell einsetzbar. Gleichzeitig ist sie eines der größten Einfallstore für Cyberangriffe. Ohne Authentifizierung laufen E-Mails Gefahr, im Spam-Ordner zu landen oder vom empfangenden Server abgewiesen zu werden.

Noch gravierender ist die Bedrohung durch Missbrauch der eigenen Marke. Angreifer versenden täuschend echte Phishing-Mails im Namen von Unternehmen, um Empfänger zur Preisgabe sensibler Daten zu bewegen. Die Folgen sind Imageschäden, rechtliche Risiken und ein Vertrauensverlust, der nur schwer wiederherzustellen ist.

In diesem Whitepaper, das in Kooperation der Certified Senders Alliance (CSA) mit dem Deutschen Dialogmarketing Verband e. V. (DDV) entstanden ist, erfahren Sie:

- warum Authentifizierung im E-Mail-Versand unverzichtbar ist,
- welche Risiken bei fehlender Umsetzung bestehen,
- wie SPF, DKIM und DMARC funktionieren und zusammenspielen,
- welche typischen Stolpersteine zu beachten sind,
- und wie Monitoring sowie Partner wie die CSA Unternehmen nachhaltig unterstützen.

Ziel ist es, Fach- und Führungskräften in IT, Marketing und Geschäftsführung eine klare Grundlage für Entscheidungen zu geben. Das Whitepaper verbindet technische Erläuterungen mit praktischen Empfehlungen und zeigt, dass E-Mail-Authentifizierung nicht nur ein IT-Thema ist, sondern ein geschäftskritischer Erfolgsfaktor.

3. E-Mail im Spannungsfeld zwischen Kommunikation und Bedrohung

> **Executive Insight:** E-Mail ist unverzichtbar – und zugleich der am meisten genutzte Angriffsvektor.

E-Mail ist für Unternehmen so wichtig wie kein anderes Kommunikationsmittel. Sie transportiert Informationen, Markenbotschaften und Transaktionsdaten. Genau das macht sie zum bevorzugten Ziel von Angreifern.

Die großen Postfachanbieter haben reagiert. Seit Februar 2024 verlangen Gmail und Yahoo bei hohem Versandvolumen eine konsequente Authentifizierung und klare Abmeldemechanismen

(Google, Yahoo 2024). Microsoft kündigte im April 2025 vergleichbare Vorgaben für Outlook-Consumer-Domains an (Quelle: Proofpoint 2025).

Die Bedrohungslage ist messbar: Hornetsecurity analysierte 45 Milliarden E-Mails aus dem Jahr 2023. 36,4 Prozent waren unerwünscht, 3,6 Prozent bösartig. Phishing war mit 43,3 Prozent die häufigste Angriffsform (Quelle: s.o.).

Auch global steigt die Gefahr. Kaspersky registrierte 2024 mehr als 893 Millionen blockierte Phishing-Versuche – ein Zuwachs von 26 Prozent gegenüber dem Vorjahr. Betroffen waren alle Branchen, besonders Web-Services, Internetportale und Banken, aber auch Handel und soziale Netzwerke (Quelle: Kaspersky 2025).

Die wirtschaftlichen Schäden sind enorm. In Deutschland lagen die Verluste durch Cyberangriffe 2024 bei 267 Milliarden Euro. Diese Zahl umfasst direkte finanzielle Schäden ebenso wie Imageschäden und Rechtskosten (Quelle: s.o.).

Interpretation: Unternehmen, die auf Authentifizierung verzichten, riskieren nicht nur Spamfilter-Probleme, sondern ihre Reputation, ihren Umsatz und die Sicherheit ihrer Kunden.

4. Was bedeutet E-Mail-Authentifizierung?

> **Executive Insight:** Authentifizierung ist der Identitätsnachweis im E-Mail-Verkehr. Sie bestätigt Absender und schützt Empfänger vor Manipulation.

E-Mail-Authentifizierung hilft dem empfangenden Server zu prüfen, ob eine Nachricht tatsächlich vom angegebenen Absender stammt und auf dem Weg nicht verändert wurde. Drei Standards sind dabei zentral: **SPF**, **DKIM** und **DMARC**.

- **SPF** legt fest, welche Server im Namen einer Domain E-Mails versenden dürfen.
- **DKIM** signiert jede E-Mail digital und stellt sicher, dass der Inhalt unverändert bleibt.
- **DMARC** verbindet beide Methoden, legt Regeln fest, wie Empfänger mit fehlerhaften Nachrichten umgehen sollen, und liefert Berichte über Auffälligkeiten.

Auch wenn Authentifizierung allein nicht alle Angriffe verhindert, ist sie das Fundament für sichere Kommunikation. Unternehmen, die SPF, DKIM und DMARC korrekt einsetzen, werden von Postfachanbietern als vertrauenswürdig eingestuft und verbessern damit ihre Chancen auf Zustellung im Posteingang.

Interpretation: Authentifizierung ist für die E-Mail, was ein Reisepass für Menschen ist – ein Nachweis von Identität und Integrität. Ohne diesen Nachweis bleibt der Zugang verwehrt.

5. Die Folgen mangelhafter oder fehlender Authentifizierung

> **Executive Insight:** Fehlende Authentifizierung führt zu Missbrauch, Zustellproblemen und finanziellen Schäden.

Die Risiken sind konkret und vielfältig:

Markenmissbrauch und Phishing

Wenn eine Domain nicht geschützt ist, können Angreifer täuschend echte E-Mails im Namen des Unternehmens versenden. Kunden werden so verleitet, sensible Daten preiszugeben. Die Marke wird direkt mit Betrug in Verbindung gebracht.

Vertrauensverlust

Phishing-Vorfälle im Namen eines Unternehmens hinterlassen Spuren – in sozialen Netzwerken, in der Presse, bei Kunden und Partnern. Vertrauen zurückzugewinnen ist kostspielig und langwierig.

Zustellprobleme

Fehlende oder fehlerhafte Authentifizierung führt dazu, dass E-Mails blockiert oder im Spam-Ordner abgelegt werden. Nachrichten, die nicht gelesen werden, sind wirkungslos.

Geschäftseinbußen

Wichtige Transaktionsmails – wie Rechnungen oder Passwort-Resets – erreichen den Kunden nicht. Das führt zu Kaufabbrüchen, Umsatzeinbußen und vermehrten Serviceanfragen.

Rechtliche Konsequenzen

Phishing und Datenschutzverletzungen können Bußgelder, Schadenersatzforderungen und Rechtskosten nach sich ziehen.

Interpretation: Ohne Authentifizierung verlieren Unternehmen nicht nur E-Mails, sondern Reputation, Umsatz und Rechtssicherheit.

6. Die drei Grundpfeiler der E-Mail-Authentifizierung

> **Executive Insight:** SPF, DKIM und DMARC bilden gemeinsam das Fundament einer sicheren E-Mail-Infrastruktur.

SPF – die Gästeliste für Mailserver

Ein SPF-Eintrag im DNS legt fest, welche Server E-Mails im Namen einer Domain versenden dürfen. Der empfangende Server prüft, ob die Nachricht von einer autorisierten Quelle stammt.
Risiko: Veraltete oder zu breite Einträge öffnen Angriffsflächen.

DKIM – das digitale Siegel

DKIM versieht jede E-Mail mit einer digitalen Signatur. Wie ein Siegel auf einem Briefumschlag zeigt sie, ob die Nachricht unverändert ist. Der öffentliche Schlüssel liegt im DNS, der private bleibt beim Absender.
Risiko: Unzureichende Schlüssellänge oder fehlende Rotation schwächen die Sicherheit.

DMARC – der Türsteher mit Regelbuch

DMARC kombiniert SPF und DKIM und gibt vor, wie Empfänger mit Mails umgehen, die die Prüfung nicht bestehen. Drei Modi stehen zur Verfügung:

- none: Beobachten ohne Eingriff,
- quarantine: verdächtige Nachrichten landen im Spam,
- reject: nicht authentifizierte Mails werden konsequent abgewiesen.

Zusätzlich liefert DMARC Berichte, die zeigen, welche Server im Namen einer Domain Mails versenden – ob autorisiert oder nicht.

Interpretation: Erst das Zusammenspiel der drei Standards schafft einen wirksamen Schutz. SPF prüft die Quelle, DKIM die Unversehrtheit, DMARC entscheidet über das Vorgehen. Gemeinsam bilden sie das Schutzschild gegen Missbrauch.

7. Typische Stolpersteine und wie Sie sie vermeiden

> **Executive Insight:** Die größten Hürden sind nicht technischer Natur, sondern organisatorisch: fehlendes Wissen, unklare Zuständigkeiten, gewachsene Systeme.

Viele Unternehmen scheitern bei der Einführung von SPF, DKIM und DMARC nicht an der Technik, sondern an Strukturen und Abläufen. Fünf Stolpersteine treten besonders häufig auf:

Mangelndes Bewusstsein

Die Relevanz von E-Mail-Authentifizierung wird unterschätzt. Risiken wie Phishing oder Zustellprobleme werden erst dann ernst genommen, wenn es zu spät ist.

Empfehlung: Schaffen Sie internes Bewusstsein. Schulen Sie Mitarbeitende in IT, Marketing und Compliance.

Technische Komplexität

SPF, DKIM und DMARC erfordern DNS-Kenntnisse und ein präzises Verständnis der Versandinfrastruktur. Schon kleine Konfigurationsfehler können legitime Mails blockieren.

Empfehlung: Ziehen Sie bei Bedarf externe Expertise hinzu.

Veraltete Systeme

In historisch gewachsenen IT-Landschaften ist oft unklar, welche Systeme überhaupt noch Mails verschicken. Nach Fusionen oder Tool-Wechseln bleiben alte Versandpfade ungesichert.

Empfehlung: Beginnen Sie mit einer Bestandsaufnahme. Priorisieren Sie zentrale Versandquellen.

Falsches Sicherheitsverständnis

Firewalls oder Verschlüsselung werden fälschlich als Ersatz für Authentifizierung gesehen. Doch sie schützen nicht vor dem Missbrauch einer Domain.

Empfehlung: Verankern Sie Authentifizierung als eigenständigen Teil Ihrer Sicherheitsstrategie.

Fehlende Abstimmung

Häufig fehlt die Koordination zwischen IT, Marketing, Kundenservice und Compliance. Die Folge sind Lücken in der Authentifizierung oder blockierte legitime E-Mails.

Empfehlung: Etablieren Sie feste Prozesse für den Austausch zwischen allen Beteiligten.

Interpretation: Authentifizierung ist kein IT-Projekt, sondern ein organisationsübergreifender Prozess. Nur wenn Verantwortlichkeiten geklärt sind, gelingt eine nachhaltige Umsetzung.

8. Grundlagen zur Umsetzung: So gehen Sie es richtig an

> **Executive Insight:** Drei Schritte sichern eine wirksame Authentifizierung: Analyse, Einrichtung und Monitoring.

Schritt 1: Systemanalyse

Zu Beginn steht die Bestandsaufnahme. Welche Systeme versenden im Namen Ihrer Domain? Dazu zählen klassische Mailserver, Marketing-Plattformen, CRM-Systeme oder externe Dienstleister. Auch scheinbar stillgelegte Domains müssen berücksichtigt werden – sonst werden sie zum leichten Angriffsziel.

Fragen, die Sie stellen sollten:

- Welche Systeme verschicken Mails im Namen unserer Domain?
- Nutzen externe Anbieter unsere Absenderadressen?
- Gibt es Domains, die aktuell nicht aktiv genutzt werden?

Schritt 2: SPF – die Gästeliste für Mailserver

SPF legt fest, welche Server autorisiert sind, E-Mails für Ihre Domain zu verschicken. Ein SPF-Eintrag im DNS funktioniert wie eine Gästeliste: Nur wer eingetragen ist, wird akzeptiert.

Ein Beispiel:
v=spf1 ip4:192.0.2.0/24 include:_spf.google.com -all

Typische Fehler:

- veraltete Einträge, die neue Server nicht abbilden,
- zu breite Definitionen ganzer Netzbereiche,
- Überschreiten des Limits von zehn DNS-Abfragen.

Schritt 3: DKIM – das digitale Siegel

DKIM versieht jede E-Mail mit einer digitalen Signatur. Wie das Siegel auf einem Briefumschlag zeigt es, ob die Nachricht unterwegs verändert wurde.

Wichtige Empfehlungen:

- mindestens 2048-Bit-Schlüssellänge,
- regelmäßige Schlüsselrotation,
- Signatur über alle relevanten Header,
- Verzicht auf den Parameter „l=“, da er Manipulation ermöglicht.

Schritt 4: DMARC – der Türsteher am Eingang

DMARC kombiniert SPF und DKIM und legt fest, wie E-Mail-Server mit Nachrichten umgehen, die die Prüfungen nicht bestehen.

Drei Richtlinien stehen zur Verfügung:

- none: Beobachtung ohne Eingriff,
- quarantine: Nachrichten landen im Spam-Ordner,
- reject: nicht authentifizierte Nachrichten werden blockiert.

Ein Beispiel:
v=DMARC1; p=quarantine; rua=mailto:reports@domain.de

Praxisempfehlung:

- starten Sie mit „none“, um erste Daten zu sammeln,
- wechseln Sie schrittweise zu „quarantine“ und „reject“, sobald alle Versandquellen bekannt sind,
- aktivieren Sie Berichtsfunktionen, um Missbrauch zu erkennen.

Interpretation: Die Einrichtung von SPF, DKIM und DMARC ist kein einmaliges Projekt, sondern ein Prozess. Wer regelmäßig prüft, überwacht und nachjustiert, schafft nachhaltige Sicherheit.

9. Realdaten und Monitoring – Schlüssel zu effektivem und sicherem E-Mail-Versand

> **Executive Insight:** Monitoring ist das Frühwarnsystem für Sicherheit und Zustellbarkeit. Ohne Daten bleibt Missbrauch unsichtbar.

Warum Monitoring entscheidend ist

E-Mail-Sicherheit endet nicht mit der Einrichtung von SPF, DKIM und DMARC. Entscheidend ist, was danach geschieht. Monitoring macht sichtbar, welche Systeme im Namen einer Domain tatsächlich versenden – ob gewollt oder nicht.

DMARC-Berichte als Kontrollinstrument

Postfachanbieter liefern sogenannte Aggregate Reports. Diese zeigen:

- von welchen IP-Adressen E-Mails im Namen Ihrer Domain versendet wurden,
- ob SPF und DKIM die Prüfung bestanden haben,
- wo Fehler oder Auffälligkeiten auftreten.

Diese Berichte sind maschinenlesbar und für Menschen schwer verständlich. Deshalb lohnt sich der Einsatz spezialisierter Tools, die Daten analysieren und aufbereiten.

Performance und Reputation

Monitoring ist nicht nur ein Sicherheitsinstrument, sondern auch ein Werkzeug für bessere Zustellung. Wichtige Kennzahlen sind:

- Spam-Beschwerderaten,
- Zustellraten,
- Treffer in Spam-Traps.

Eine schlechte Reputation führt dazu, dass Postfachanbieter Nachrichten blockieren. Eine gute Reputation erhöht die Chance, zuverlässig im Posteingang zu landen.

Handlungsempfehlungen

- Aktivieren Sie DMARC-Berichte für alle Domains.
- Nutzen Sie Monitoring-Tools, die Reports verständlich aufbereiten.
- Reagieren Sie sofort auf Auffälligkeiten in den Kennzahlen.

Interpretation: Monitoring ist kein Luxus. Es ist das Nervensystem der E-Mail-Sicherheit. Wer Daten kontinuierlich beobachtet, erkennt Angriffe, sichert Zustellbarkeit und schützt langfristig die Reputation seiner Marke.

10. Warum sich ein Partner lohnt: Die Certified Senders Alliance (CSA)

> **Executive Insight:** Die CSA ist seit 20 Jahren die neutrale Instanz für sicheren E-Mail-Versand – mit Praxisdaten, Expertise und einem starken Netzwerk.

Die Certified Senders Alliance (CSA) ist ein Gemeinschaftsprojekt von **eco – Verband der Internetwirtschaft** und dem **Deutschen Dialogmarketing Verband (DDV)**. Sie entstand aus der Einsicht, dass E-Mail-Kommunikation nur dann zuverlässig bleibt, wenn Versender und Postfachanbieter auf einheitliche Standards vertrauen können.

Der CSA-Certification Monitor

Das Herzstück der CSA ist der Certification Monitor. Er liefert Realdaten direkt von Postfach- und Sicherheitsanbietern – keine Schätzungen, keine Drittanalysen. Unternehmen sehen damit, wie ihre E-Mails tatsächlich bewertet werden.

Zentrale Kennzahlen sind:

- Spam-Beschwerderaten,
- Spam-Trap-Treffer,
- Authentifizierungsfehler wie ungültige DKIM-Signaturen oder fehlendes Alignment.

Diese Daten sind für Versender ein Frühwarnsystem. Auffälligkeiten können erkannt und behoben werden, bevor es zu systematischen Blockaden kommt.

Mehrwert für zertifizierte Versender

Zertifizierte Unternehmen profitieren von:

- individuellem Feedback durch CSA-Expertinnen und -Experten für Technik und Recht,
- Hinweisen auf Beschwerden oder Auffälligkeiten im Versandverhalten,
- Unterstützung bei technischen und rechtlichen Fragen,
- Zugang zu einer Community aus Versendern, Anbietern und Spezialisten,
- dem CSA-Zertifikat als anerkanntem Qualitätsmerkmal im Markt.

Vorteil für DDV-Mitglieder

Mitglieder des DDV profitieren zusätzlich von Sonderkonditionen bei der CSA-Zertifizierung.

Interpretation: Die CSA ist mehr als ein Prüfzeichen. Sie ist Schnittstelle, Datenlieferant und Partner. Unternehmen, die CSA nutzen, erhöhen ihre Zustellraten, senken Risiken und gewinnen Vertrauen bei Kunden wie auch bei Postfachanbietern.

11. E-Mail-Authentifizierung ist Pflicht – auch für Sie

> **Executive Insight:** Authentifizierung ist heute nicht Kür, sondern Pflicht. Ohne sie verlieren Sie den Zugang zum Posteingang.

Ob Startup, Mittelstand oder Großkonzern – jedes Unternehmen, das E-Mails verschickt, ist betroffen. Die großen Postfachanbieter haben Authentifizierung verbindlich gemacht. Wer SPF, DKIM und DMARC nicht korrekt implementiert, läuft Gefahr, dass seine Nachrichten nicht mehr zugestellt werden.

Die Konsequenzen sind eindeutig:

- **Verzicht ist keine Option.** Ohne Authentifizierung werden E-Mails blockiert oder aussortiert.
- **Halbe Lösungen reichen nicht.** SPF allein schützt nicht. Nur das Zusammenspiel mit DKIM und DMARC schafft Sicherheit.
- **Der Zeitrahmen ist abgelaufen.** Gmail und Yahoo haben 2024 Fakten geschaffen. Microsoft folgte in 2025.

Interpretation: Authentifizierung ist heute so selbstverständlich wie SSL-Verschlüsselung bei Webseiten. Sie ist die Eintrittskarte in den Posteingang und die Voraussetzung für Vertrauen. Unternehmen, die jetzt nicht handeln, riskieren den Ausschluss aus dem wichtigsten Kommunikationskanal der digitalen Wirtschaft.

12. Glossar wichtiger Begriffe

Aggregate Reports
Standardisierte DMARC-Berichte im XML-Format, die gesammelt (z. B. für 24 Stunden) Informationen über Versandquellen, SPF-/DKIM-Ergebnisse und Fehlversuche enthalten. Für Menschen schwer lesbar, daher sind Auswertungstools empfehlenswert.

Alignment
Übereinstimmung zwischen der sichtbaren Absenderadresse („From“) und der Domain, die über SPF und/oder DKIM validiert wurde. Ohne Alignment schlägt DMARC fehl, auch wenn SPF oder DKIM für sich genommen korrekt sind.

Allowlisting
Das Gegenteil von Blocklisting: Eine Domain oder IP wird als vertrauenswürdig eingestuft, sodass E-Mails mit höherer Wahrscheinlichkeit zugestellt werden.

BIMI (Brand Indicators for Message Identification)
Ein Standard, der es Unternehmen ermöglicht, ihr Markenlogo im Posteingang neben authentifizierten E-Mails anzeigen zu lassen. Voraussetzung ist eine konsequente Umsetzung von DMARC mit *p=quarantine* oder *p=reject*.

Blocklisting
Aufnahme einer Domain oder IP-Adresse in eine Sperrliste von Spam-Blockierdiensten oder Postfachanbietern. Führt in der Regel dazu, dass E-Mails blockiert oder im Spam landen.

Bounce
Rückmeldung des empfangenden Servers, dass eine E-Mail nicht zugestellt werden konnte. Unterschieden wird zwischen *Hard Bounce* (dauerhaft, z. B. ungültige Adresse) und *Soft Bounce* (temporär, z. B. volles Postfach).

DKIM (DomainKeys Identified Mail)
Ein Verfahren, bei dem jede ausgehende E-Mail mit einer digitalen Signatur versehen wird. Der private Schlüssel signiert die Mail, der öffentliche Schlüssel liegt im DNS-Eintrag. Der empfangende Server prüft, ob die Signatur passt und die Mail unterwegs nicht verändert wurde.

DMARC (Domain-based Message Authentication, Reporting and Conformance)
Eine Erweiterung von SPF und DKIM, die Regeln vorgibt, wie empfangende Mailserver mit nicht oder fehlerhaft authentifizierten Mails umgehen sollen. Zusätzlich liefert DMARC Berichte über die Authentifizierungsergebnisse. Es gibt drei Richtlinien: *none*, *quarantine*, *reject*.

Forensikberichte (Forensic Reports)
Detailberichte, die im Falle einer fehlgeschlagenen DMARC-Prüfung einzelne Nachrichtenfragmente enthalten können. Werden häufig aus Datenschutzgründen nicht aktiviert.

MTA-STS (Mail Transfer Agent Strict Transport Security)
Ein relativ neuer Standard, der erzwingt, dass E-Mails nur über TLS-verschlüsselte Verbindungen übertragen werden. Erhöht die Sicherheit zusätzlich zur Authentifizierung.

Phishing
Versuch, Empfänger durch gefälschte E-Mails zur Preisgabe vertraulicher Informationen (Passwörter, Zahlungsdaten etc.) zu bewegen. Erfolgt oft durch Täuschung des Absendernamens (Domain-Spoofing).

RUA / RUF (Reporting Adresses for DMARC)

- **RUA (Aggregate Reports):** Tägliche, maschinenlesbare Berichte, die zeigen, welche Server im Namen einer Domain E-Mails versenden und ob diese korrekt authentifiziert wurden.
- **RUF (Forensic Reports):** Detaillierte Einzelberichte über fehlgeschlagene Authentifizierungen. Werden seltener genutzt, da sie potenziell sensible Daten enthalten.

Sender Reputation
Der „Ruf" einer Absenderdomain oder IP-Adresse bei Postfachanbietern. Sie basiert u. a. auf Spam-Beschwerden, Zustellraten, Bounce-Raten und Authentifizierungsstatus. Eine schlechte Reputation kann zur Blockade führen.

Spam-Trap
Eine „Falle" von Postfachanbietern oder Anti-Spam-Diensten: E-Mail-Adressen, die niemals aktiv genutzt wurden oder nicht mehr existieren. Werden sie angeschrieben, gilt das als Zeichen schlechter Listenqualität.

SPF (Sender Policy Framework)
Ein DNS-Text-Eintrag, der festlegt, welche Mailserver im Namen einer Domain E-Mails versenden dürfen. Der empfangende Server prüft, ob die eingehende Mail von einem autorisierten Server kommt. Schützt vor Spoofing, ist aber allein nicht ausreichend.

Spoofing
Fälschung der Absenderadresse in einer E-Mail, sodass sie scheinbar von einer vertrauenswürdigen Domain stammt. Ohne SPF, DKIM und DMARC kaum erkennbar.

TLS (Transport Layer Security)
Verschlüsselung für die Übertragung von E-Mails zwischen Mailservern. Stellt sicher, dass

Nachrichten während des Transports nicht im Klartext mitgelesen werden können. Ergänzt, aber ersetzt nicht SPF/DKIM/DMARC.

Über die Certified Senders Alliance

Die Certified Senders Alliance (CSA) ist ein Service des eco – Verband der Internetwirtschaft e.V. und ist in Kooperation mit dem Deutschen Dialogmarketing Verband (DDV) im Jahr 2004 entstanden. Die CSA bildet eine neutrale Schnittstelle zwischen Mailboxprovidern und Versendern kommerzieller E-Mails. Ziel der CSA ist es, die Qualität kommerzieller E-Mails (z.B. Newsletter, Rechnungen, Auftragsbestätigungen etc.) zu erhöhen. Um dieses Ziel zu erreichen, erstellt sie rechtliche und technische Qualitätsstandards. Die Qualitätsstandards ergeben sich aus geltendem Recht und technischen Anforderungen der Mailboxprovider. Sie werden entsprechend den aktuellen Gesetzgrundlagen und Marktanforderungen regelmäßig aktualisiert.

Autoren

Sandra Schubert
Customer Success Managerin
Certified Senders Alliance
eco – Verband der Internetwirtschaft e.V

Franz Peter Altemeier
Geschäftsführer
DDV Deutscher Dialogmarketing Verband e. V.

Julia Janßen-Holldiek
Director
Certified Senders Alliance
eco – Verband der Internetwirtschaft e.V

Impressum

DDV Deutscher Dialogmarketing Verband e.V.

Hahnstraße 70
60528 Frankfurt

Tel: +49 69 401 276 500
E-Mail: info@ddv.de

Vereinsregister Frankfurt am Main, VR 15630
Umsatzsteueridentifikationsnummer: DE 113821908

Vorstand:
Martin Nitsche (Präsident), Patrick Tapp (Präsident), Ulf Uebel (Vizepräsident Finanzen)

Geschäftsführer: Franz Peter Altemeier

eco – Verband der Internetwirtschaft e.V.

Certified Senders Alliance
Lichtstrasse 43h
50825 Köln

Tel: +49 221 70 00 48-0
E-Mail: info@certified-senders.org
https://certified-senders.org/

Vereinsregister Köln, VR 14478
Umsatzsteueridentifikationsnummer: DE 182676944

Vorstand:
Oliver Süme (Vorsitzender), Klaus Landefeld (stv. Vorsitzender), Silke Kanes, Felix Höger, Prof. Dr. Norbert Pohlmann

Geschäftsführer:
Alexander Rabe, Andreas Weiss