GUARDIAN360

in Zusammenarbeit mit DMARC Advisor

E-Mail-Security-Benchmark

DMARC-Schutz bei Managed Service Providern in der DACH-Region

Deutschland · Österreich · Schweiz | 1.311 Anbieter gescannt

NETWORKING-EVENT

„Grenzüberschreitende Cybersicherheit“ für MSPs und IT-Systemhäuser

TopGolf Oberhausen · 2. September 2026

Datenanalyse durch DMARC Advisor | Bericht von Guardian360 · Juli 2026 · Benchmark-Daten erhoben am 8. Juli 2026

Veranstaltet von der niederländischen Regierung & InnovationQuarter, mit Passguard, SecuMailer, SecureMe2, DMARC Advisor und Guardian360.

Zusammenfassung

E-Mail ist nach wie vor der wichtigste Angriffsweg auf Organisationen. DMARC (Domain-based Message Authentication, Reporting and Conformance) ist die wirksamste einzelne Maßnahme, mit der eine Organisation verhindern kann, dass Kriminelle E-Mails in ihrem Namen versenden. Dennoch ist die Verbreitung auf *durchsetzender* Ebene erschreckend gering, selbst bei den Unternehmen, die ihr Geld mit Sicherheit verdienen.

Dieser Benchmark wurde für das Netzwerk-Event „Grenzüberschreitende Cybersicherheit“ für MSPs und IT-Systemhäuser erstellt (TopGolf Oberhausen, 2. September 2026). **DMARC Advisor** hat die öffentliche DMARC-Konfiguration von **1.311 Managed Service Providern (MSPs)** in Deutschland, Österreich und der Schweiz analysiert, und **Guardian360** hat auf Basis dieser Ergebnisse diesen Bericht erstellt. Legt man einen strengen Maßstab an, bei dem nur eine Richtlinie von **p=reject** als geschützt gilt, sind die Ergebnisse ernüchternd.

74,5 %

der MSPs in DACH sind NICHT gegen E-Mail-Spoofing geschützt

Nur **25,5 %** der gescannten MSPs setzen DMARC mit p=reject durch. Die übrigen drei Viertel veröffentlichen entweder gar keinen DMARC-Eintrag oder betreiben eine Richtlinie (p=none oder p=quarantine), bei der gefälschte E-Mails den Empfänger dennoch erreichen, im Posteingang oder im Spam-Ordner, den die meisten Nutzer aktiv kontrollieren. Da MSPs E-Mail und IT für Tausende nachgelagerte Kunden verwalten, ist eine ungeschützte MSP-Domain nicht nur ein Risiko für den Anbieter selbst, sondern ein glaubwürdiger Angriffsweg in seinen gesamten Kundenstamm.

Wichtigste Ergebnisse auf einen Blick

- **Nur 1 von 4 ist geschützt.** 334 von 1.311 MSPs (25,5 %) setzen p=reject durch. Die größte Einzelgruppe, 398 Anbieter (30,4 %), verharrt bei p=quarantine, das Spoofing nicht verhindert.
- **Fast 1 von 5 hat gar keinen DMARC-Eintrag.** 257 Anbieter (19,6 %) veröffentlichen überhaupt keinen DMARC-Eintrag und lassen ihre Domain völlig offen für Identitätsmissbrauch.
- **Bemerkenswert einheitlich über Grenzen hinweg.** Der Schutz liegt bei 27,7 % in der Schweiz, 25,2 % in Deutschland und 22,4 % in Österreich. Das ist eine strukturelle, keine nationale Lücke.
- **Größe hilft kaum.** Große und Enterprise-MSPs sind nur geringfügig besser geschützt als Ein-Personen-Betriebe. Selbst im besten Größensegment ist weniger als ein Drittel geschützt.
- **Das Spezialisten-Paradox.** MSPs, die ausdrücklich Cybersecurity- oder E-Mail-Security-Dienste verkaufen (26,4 % geschützt), liegen kaum über dem Gesamtdurchschnitt und schützen ihre eigene Domain in fast drei von vier Fällen nicht.
- **Reporting ist ein blinder Fleck.** 42,0 % der MSPs haben überhaupt kein DMARC-Aggregat-Reporting (RUA) konfiguriert und haben damit keinerlei Einblick, wer in ihrem Namen E-Mails versendet.

Umfang, Methode und Definitionen

Der Benchmark basiert auf einem externen, nicht-invasiven Scan öffentlich verfügbarer DNS-Einträge. Es wurde auf keine Systeme zugegriffen und es wurden keine Daten über öffentliche DMARC- und DNS-Informationen hinaus erhoben. Der Datensatz umfasst **1.311 MSPs** für die DACH-Region: 1.006 in Deutschland, 220 in der Schweiz und 85 in Österreich. Für jede Domain wurde der veröffentlichte DMARC-Eintrag abgerufen, die durchgesetzte Richtlinie klassifiziert und das Vorhandensein eines Aggregat-Reportings (rua) geprüft.

Über diesen Bericht und das Event

Dieser Bericht erscheint im Rahmen des Netzwerk-Events **„Grenzüberschreitende Cybersicherheit“ für MSPs und IT-Systemhäuser**, das am 2. September 2026 im TopGolf Oberhausen stattfindet. Veranstaltet wird das Event von der niederländischen Regierung (ihrem diplomatischen Netzwerk in Deutschland) gemeinsam mit der regionalen Entwicklungsagentur InnovationQuarter. Es bringt deutsche MSPs mit fünf niederländischen Cybersecurity-Unternehmen zusammen: Passguard, SecuMailer, SecureMe2, DMARC Advisor und Guardian360. Die Datenanalyse hinter diesem Benchmark stammt von **DMARC Advisor**; den Bericht hat **Guardian360** erstellt. Da das Event vor allem MSPs aus Nordrhein-Westfalen zusammenbringt, sind die regionalen Ergebnisse für NRW (siehe den Fokus weiter unten) für das Publikum besonders relevant.

Wie wir Schutz klassifizieren

Gemäß der mit DMARC Advisor abgestimmten Klassifizierung wird jede Domain auf ein binäres Ergebnis reduziert: **Geschützt** oder **Nicht geschützt**. Die Logik ist bewusst streng, denn alles unterhalb der vollständigen Durchsetzung lässt eine gefälschte Nachricht weiterhin den Empfänger erreichen.

Status	Kriterium	Was das bedeutet
Geschützt	nur p=reject	Die Domain ist vollständig geschützt. Gefälschte E-Mails werden vor der Zustellung direkt abgewiesen.
Nicht geschützt	p=quarantine	Gefälschte E-Mails werden nicht blockiert, sondern in den Spam-/Junk-Ordner geleitet, wo 76-86 % der Nutzer nach „verlorenen“ E-Mails suchen.
Nicht geschützt	p=none	Nur Überwachung. Keine Durchsetzung oder Blockierung; Spoofing gelingt.
Nicht geschützt	Kein DMARC-Eintrag	Kein Eintrag veröffentlicht. Die Domain ist völlig offen für Identitätsmissbrauch.

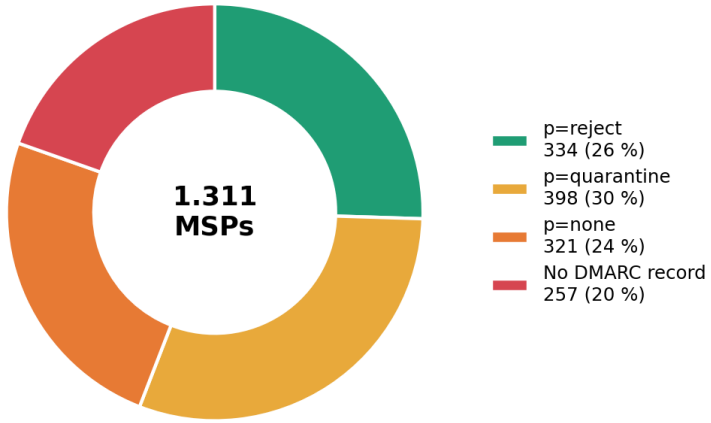
Die Begründung ist einfach: Bei „Kein DMARC“, p=none *und* p=quarantine erreicht eine gefälschte E-Mail den Empfänger dennoch. Da der durchschnittliche Nutzer seinen Spam-Ordner aktiv nach legitimer Post durchsucht, bleibt er hochgradig verwundbar. Nur p=reject entfernt die Nachricht, bevor sie Schaden anrichten kann. Deshalb zählen wir p=quarantine, die größte Einzelgruppe in diesem Datensatz, nicht als geschützt.

> *Hinweis zu p=reject: Organisationen sollten niemals direkt auf p=reject wechseln. Überwachen Sie zunächst die RUA-Berichte, stellen Sie sicher, dass sich jeder legitime Absender korrekt authentifiziert, und verschärfen Sie erst dann die Richtlinie. Eine verfrühte Durchsetzung kann legitime Geschäftspost blockieren.*

Das Gesamtbild

Über alle 1.311 MSPs hinweg verteilen sich die vier DMARC-Zustände nahezu gleichmäßig, wobei p=quarantine, eine Richtlinie, die ein trügerisches Sicherheitsgefühl vermittelt, die häufigste Konfiguration überhaupt ist.

DMARC-Richtlinienverteilung bei MSPs in der DACH-Region



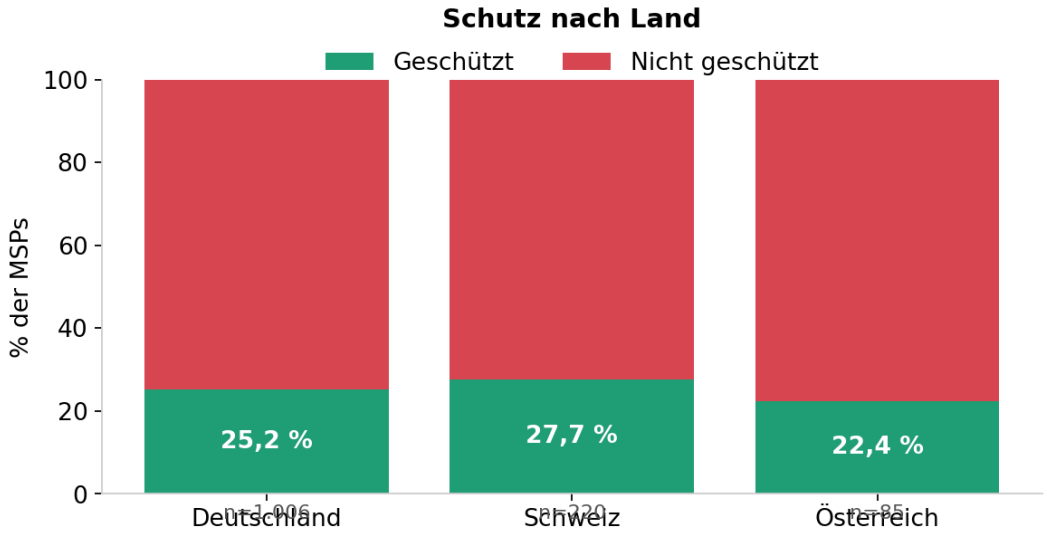
DMARC-Richtlinie	MSPs	Anteil	Geschützt?
p=reject	334	25,5 %	Geschützt
p=quarantine	398	30,4 %	Nicht geschützt
p=none	321	24,5 %	Nicht geschützt
Kein DMARC-Eintrag	257	19,6 %	Nicht geschützt
Insgesamt gescannt	1.311	100 %	-

Nur 1 von 4 MSPs in DACH ist gegen Spoofing geschützt (p=reject)

Auf die entscheidende Binärfrage reduziert, sind **977 der 1.311 gescannten Anbieter (74,5 %) nicht geschützt** dagegen, dass in ihrem Namen E-Mails versendet werden. Für eine Branche, deren gesamtes Versprechen darauf beruht, eine vertrauenswürdige, sichere Erweiterung der IT ihrer Kunden zu sein, ist das ein erhebliches Risiko.

Analyse nach Land

Man könnte deutliche Unterschiede zwischen den drei Märkten erwarten. In der Praxis ist das Bild bemerkenswert einheitlich: Der Schutz reicht nur von 22,4 % bis 27,7 %. Das Problem ist im gesamten deutschsprachigen Raum strukturell und nicht auf ein einzelnes Land beschränkt.



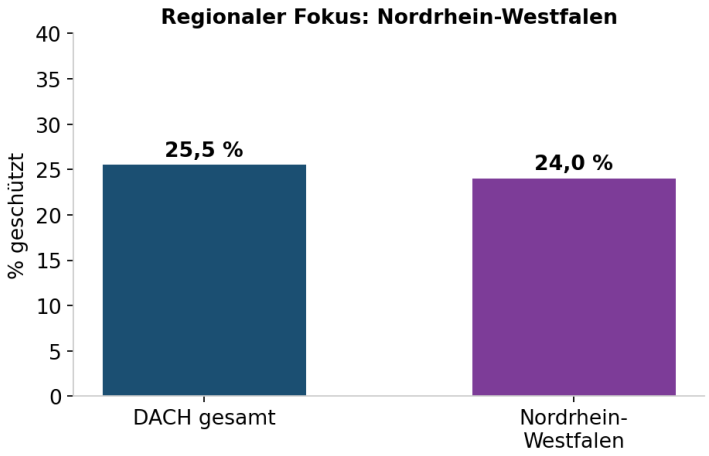
Land	MSPs	p=reject	quarantine	p=none	Kein Eintrag	% geschützt
Deutschland	1.006	254	296	243	212	25,2 %
Schweiz	220	61	74	52	33	27,7 %
Österreich	85	19	28	26	12	22,4 %

Die Schweiz führt knapp mit **27,7 %**, gefolgt von Deutschland (**25,2 %**) und Österreich (**22,4 %**). Österreich hat zudem den höchsten Anteil an Anbietern, die bei p=none (nur Überwachung) feststecken, was darauf hindeutet, dass etliche Organisationen den DMARC-Weg begonnen, aber nie abgeschlossen haben.

Regionaler Fokus: Nordrhein-Westfalen

Als bevölkerungsreichstes Bundesland und dichtester MSP-Markt Deutschlands wurde Nordrhein-Westfalen (NRW) gesondert analysiert. Mit **221 Anbietern** entspricht NRW nahezu exakt dem DACH-Durchschnitt, was bestätigt, dass die Durchsetzungslücke selbst in einem reifen, wettbewerbsintensiven regionalen Markt fortbesteht.

Diese Region ist hier besonders relevant: Das Netzwerk-Event findet in Oberhausen, im Herzen von NRW, statt, und sein Publikum besteht überwiegend aus MSPs und IT-Systemhäusern aus der Region. Die folgenden Zahlen beschreiben somit die unmittelbare Vergleichsgruppe der meisten Teilnehmenden und einen fairen Maßstab, an dem jeder die eigene Domain messen kann.



Kennzahl	Nordrhein-Westfalen	DACH gesamt
Analysierte MSPs	221	1.311
p=reject (geschützt)	53 (24,0 %)	334 (25,5 %)
p=quarantine	67	398
p=none	55	321
Kein DMARC-Eintrag	46	257
Nicht geschützt	168 (76,0 %)	977 (74,5 %)

In NRW sind 76,0 % der MSPs nicht geschützt, praktisch identisch mit den 74,5 % der Gesamtregion. Die größte Einzelgruppe ist erneut p=quarantine.

Schutz nach Bundesland

Innerhalb Deutschlands schwanken die Schutzquoten auf Länderebene stärker, wobei kleine Stichproben in den bevölkerungsärmsten Ländern zur Vorsicht mahnen. Die größeren MSP-Märkte liegen eng um den Bundesdurchschnitt.

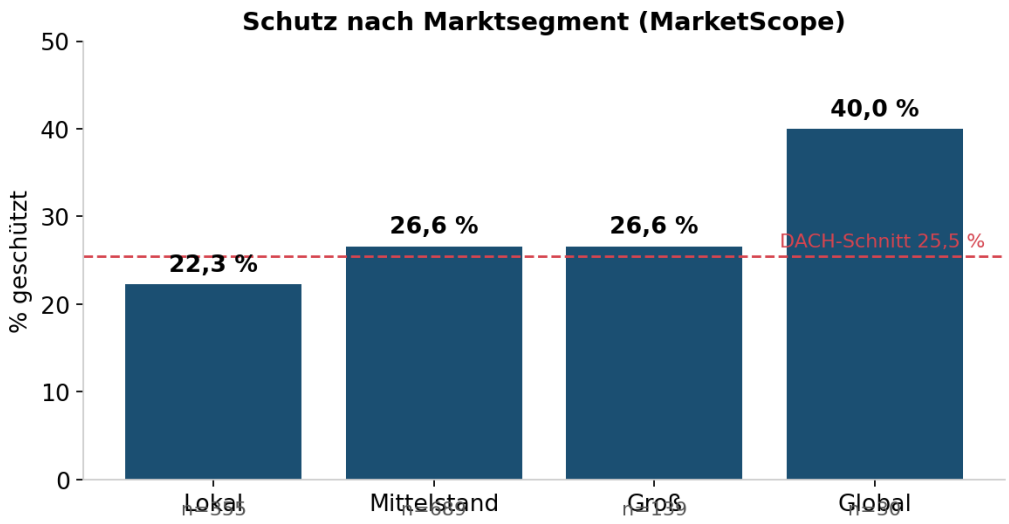
Bundesland	MSPs	Geschützt	% geschützt
Nordrhein-Westfalen	221	53	24,0 %
Bayern	194	54	27,8 %
Baden-Württemberg	141	30	21,3 %
Hessen	96	22	22,9 %
Niedersachsen	66	17	25,8 %
Berlin	57	14	24,6 %
Hamburg	53	12	22,6 %
Rheinland-Pfalz	44	13	29,5 %
Schleswig-Holstein	36	6	16,7 %

> *Bundesländer mit weniger als 30 MSPs aus statistischen Gründen ausgelassen.*

Analyse nach Unternehmenstyp und -größe

Nach Marktsegment

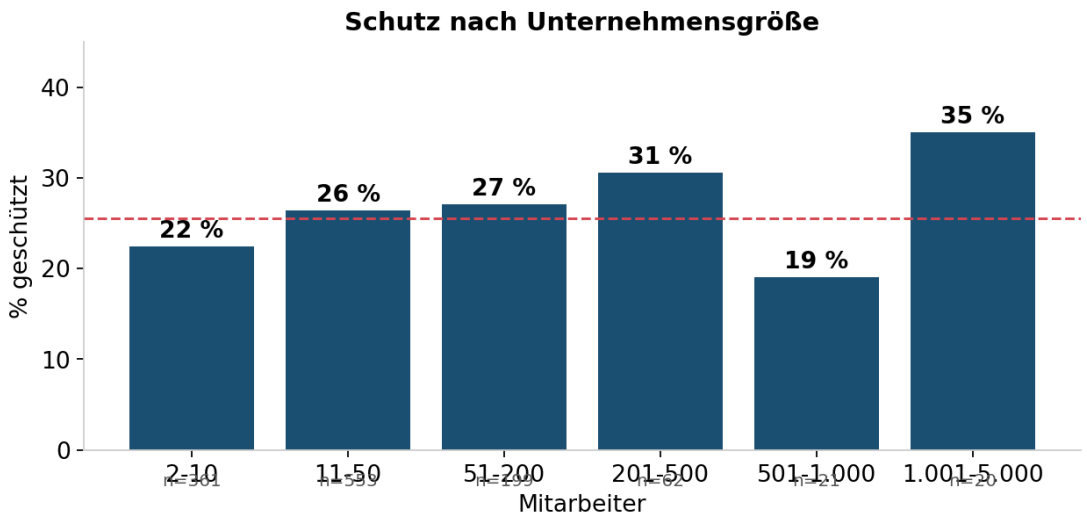
Klassifiziert man MSPs nach dem vorrangig bedienten Markt (MarketScope), zeigt sich, dass nur die kleine Gruppe global tätiger Anbieter den Durchschnitt spürbar übertrifft. Lokale Anbieter, die zahlreichste Gruppe im KMU-Segment, sind am schlechtesten geschützt.



Marktsegment	MSPs	% geschützt
Lokal	355	22,3 %
Mittelstand	689	26,6 %
Groß	139	26,6 %
Global	30	40,0 %

Nach Unternehmensgröße

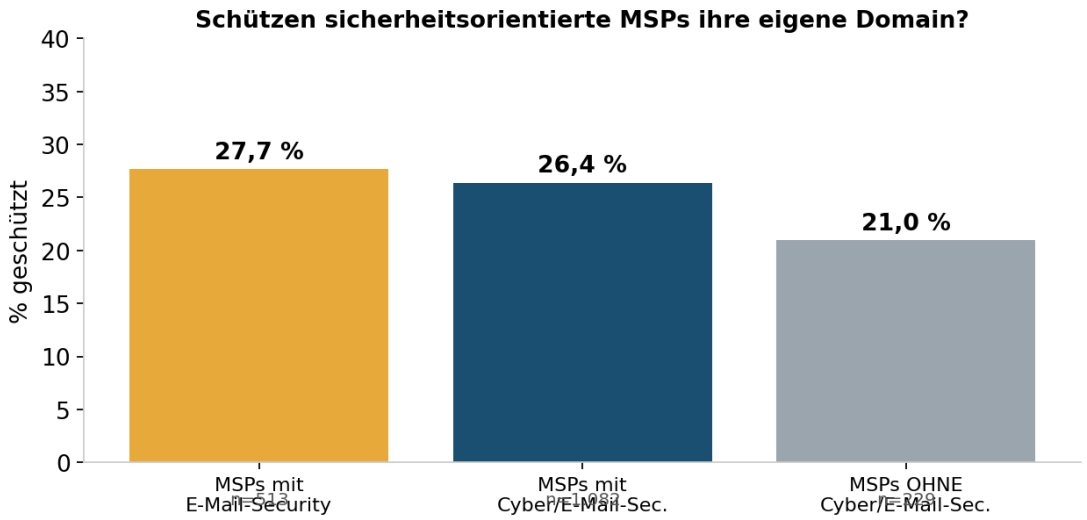
Die Annahme, dass größere, besser ausgestattete Anbieter besser geschützt sind, hält nur schwach stand. Der Schutz steigt im mittleren Bereich leicht mit der Größe, doch selbst die besten Segmente lassen rund zwei Drittel der Anbieter ungeschützt, und die größten Kategorien sind aufgrund kleiner Fallzahlen uneinheitlich.



Die Erkenntnis ist unbequem, aber eindeutig: DMARC-Durchsetzung ist in erster Linie kein Ressourcenproblem. Anbieter jeder Größe versäumen es, eine Lücke zu schließen, deren Behebung kostenlos ist und genau in ihrem eigenen Fachgebiet liegt.

Das Spezialisten-Paradox

Der vielleicht aufschlussreichste Blick auf die Daten vergleicht MSPs danach, was sie verkaufen. Wenn eine Gruppe ihre eigenen Hausaufgaben gemacht haben sollte, dann die Anbieter, die ihren Kunden ausdrücklich **Cybersecurity**- und **E-Mail-Security**-Dienste anbieten.

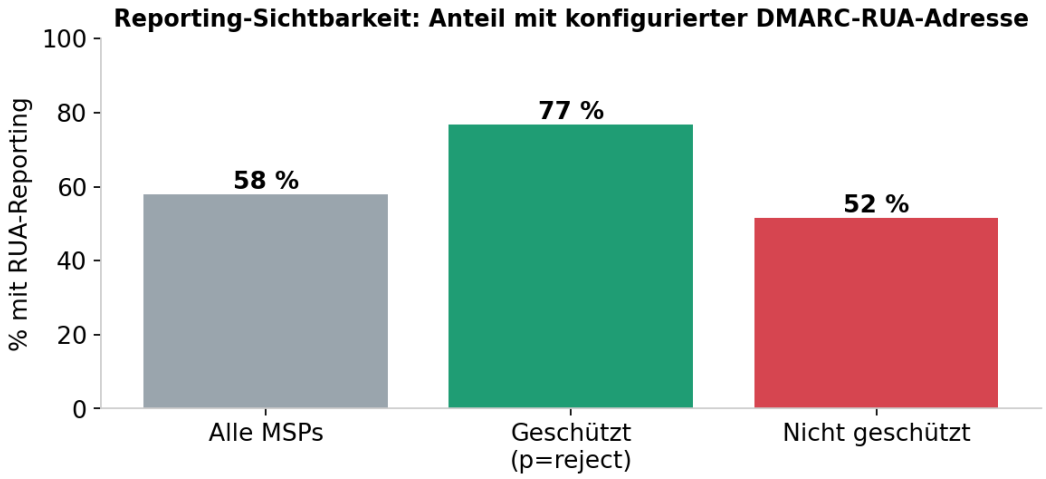


Gruppe	MSPs	% geschützt
MSPs mit E-Mail-Security	513	27,7 %
MSPs mit Cyber-/E-Mail-Security	1.082	26,4 %
MSPs ohne beides	229	21,0 %

Sicherheitsspezialisten schützen sich etwas häufiger selbst, doch der Unterschied ist gering: **26,4 % gegenüber 21 %.** Klar gesagt: Rund **drei von vier MSPs, die E-Mail-Security verkaufen, können nicht nachweisen, dass ihre eigene Domain gegen Spoofing geschützt ist.** Für potenzielle Kunden und Partner ist das eine einfache und faire Frage der Sorgfaltsprüfung.

Reporting und Sichtbarkeit (RUA)

Eine DMARC-Richtlinie ist nur die halbe Wahrheit. Die Aggregat-Reporting-Adresse (rua) verschafft einer Organisation Einblick, wer in ihrem Namen E-Mails versendet, welche legitimen Dienste authentifiziert werden müssen und woher Spoofing-Versuche stammen. Ohne sie agiert eine Organisation im Blindflug und kann nicht sicher zu p=reject fortschreiten.



Gruppe	% mit konfiguriertem RUA-Reporting
Alle MSPs	58,0 %
Geschützt (p=reject)	76,9 %
Nicht geschützt	51,5 %

42,0 % aller MSPs haben überhaupt kein Reporting konfiguriert. Reporting korreliert stark mit der Durchsetzung: 76,9 % der geschützten Anbieter erfassen RUA-Daten, gegenüber nur 51,5 % der ungeschützten, genau die Reihenfolge, der ein gesunder DMARC-Rollout folgt: Reporting einschalten, lernen, dann durchsetzen.

> *Wichtige Nuance: Ein externer Scan kann bestätigen, dass eine rua-Adresse existiert, nicht aber, ob die Berichte tatsächlich gelesen werden. Werden die Berichte an ein internes Postfach zugestellt, treffen sie als rohes XML ein, dessen Auswertung zeitaufwendig und fehleranfällig ist und häufig ungelesen archiviert wird. Eine klare Verantwortlichkeit für das DMARC-Protokoll, idealerweise mit automatisierter Berichtsverarbeitung, ist unerlässlich.*

Was das bedeutet und was zu tun ist

Die Kernbotschaft dieses Benchmarks ist nicht, dass DMARC schwierig ist. Sie lautet, dass eine Maßnahme, die kostenlos, gut dokumentiert und unmittelbar im Fachgebiet jedes MSP liegt, von drei Vierteln der Branche unvollendet bleibt. Für MSPs verschärft sich der Einsatz zusätzlich: Eine ungeschützte Anbieter-Domain ist eine perfekte Vorlage für Angreifer, um sich gegenüber den eigenen Kunden als vertrauenswürdiger Lieferant auszugeben.

Für MSPs

- **Veröffentlichen Sie noch heute einen DMARC-Eintrag, falls keiner besteht.** Beginnen Sie mit p=none und einer Reporting-Adresse, um ohne Risiko Sichtbarkeit zu gewinnen.
- **Bleiben Sie nicht bei p=quarantine stehen.** Es ist die häufigste Konfiguration in diesem Datensatz und schützt Sie nicht. Betrachten Sie es als Zwischenstation, nicht als Ziel.
- **Lesen Sie Ihre RUA-Berichte.** Nutzen Sie sie, um jeden legitimen Absender zu identifizieren und zu authentifizieren, und wechseln Sie dann gezielt zu p=reject.
- **Leben Sie vor, was Sie verkaufen.** Wenn Sie E-Mail- oder Cybersicherheit anbieten, ist eine geschützte Domain der glaubwürdige Mindestnachweis.

Für Kunden und Partner

- **Stellen Sie die Frage.** „Steht Ihre Hauptdomain auf DMARC p=reject, und überwachen Sie RUA?“ ist eine faire, aufschlussreiche Prüffrage an jeden Anbieter.
- **Prüfen Sie auch Ihre eigene Lage.** Derselbe strenge Test gilt für die Domains Ihrer eigenen Organisation.

Wie Guardian360 und DMARC Advisor helfen

Guardian360 und DMARC Advisor helfen Organisationen, sicher von keinerlei Schutz zur vollständigen Durchsetzung zu gelangen: kontinuierliches Scannen und Monitoring, automatisierte Auswertung von RUA-Berichten und fachkundige Begleitung bis p=reject, ohne legitime Post zu stören. Beide nehmen gemeinsam mit Passguard, SecuMailer und SecureMe2 am Netzwerk-Event „Grenzüberschreitende Cybersicherheit“ teil. Ziel dieses Benchmarks ist nicht, an den Pranger zu stellen, sondern ein unsichtbares Risiko sichtbar zu machen und der Branche, und den MSPs im Raum, zu helfen, eine Lücke zu schließen, für die sie bestens gerüstet sind.

Über diesen Benchmark. Datenanalyse durch DMARC Advisor; Bericht erstellt von Guardian360. Basierend auf einem externen, nicht-invasiven Scan öffentlicher DNS-/DMARC-Einträge von 1.311 DACH-MSPs, Daten erhoben am 8. Juli 2026. Erstellt für das Netzwerk-Event „Grenzüberschreitende Cybersicherheit“ für MSPs und IT-Systemhäuser (TopGolf Oberhausen, 2. September 2026), veranstaltet von der niederländischen Regierung und InnovationQuarter, mit den teilnehmenden Unternehmen Passguard, SecuMailer, SecureMe2, DMARC Advisor und Guardian360. Prozentwerte sind auf eine Nachkommastelle gerundet. Eine Domain gilt nur als geschützt, wenn ihre DMARC-Richtlinie p=reject ist.