DMARC BENCHMARK-BERICHT

E-Mail-Authentifizierung & Domain-Schutz Analyse

April 2026

10.833 Domains analysiert

Über 15+ Branchen in den Niederlanden, Deutschland, Belgien & Frankreich

Auftraggeber

GUARDIAN 360°

Schouwburgplein 30-34
3012 CL Rotterdam - Niederlande

ZUSAMMENFASSUNG

Dieser Bericht präsentiert die Ergebnisse einer großangelegten DMARC-Bewertung (Domain-based Message Authentication, Reporting & Conformance), die über **10.833 einzigartige Domains** durchgeführt wurde, die mit Organisationen im Guardian360-Ökosystem verbunden sind. Der Scan wurde im April 2026 von DMARC Advisor B.V. durchgeführt.

Das alarmierende Hauptergebnis lautet: **77,6 % aller analysierten Domains sind nicht vollständig vor E-Mail-Spoofing geschützt.** Dies bedeutet, dass die überwiegende Mehrheit der Organisationen Cyberkriminellen ermöglicht, E-Mails zu versenden, die von legitimen Unternehmensadressen stammen, was Phishing, Business Email Compromise (BEC) und Markenimitation im großen Maßstab ermöglicht.

Nur 22,4 % der Domains haben eine **p=reject** Richtlinie implementiert, die einzige DMARC-Richtlinienstufe, die gefälschte E-Mails aktiv daran hindert, Empfänger zu erreichen. Die verbleibenden Domains verteilen sich auf Teilschutz (p=quarantine, 22,1 %), Überwachungsmodus (p=none, 29,7 %) und keine DMARC-Konfiguration (25,8 %).

Die Analyse umfasst Organisationen über 15+ Branchen und vier Hauptmärkte: die Niederlande, Deutschland, Belgien und Frankreich. Zwischen den Sektoren wurden erhebliche Unterschiede in der DMARC-Einführung festgestellt, wobei Finanzen und Informationssicherheit führen, während Transport und Einzelhandel erheblich zurückbleiben.

WICHTIGSTE ERKENNTNISSE AUF EINEN BLICK

- **77,6%** der Domains sind nicht vollständig vor E-Mail-Spoofing geschützt
- **55,5%** haben entweder keinen DMARC-Record oder eine p=none Richtlinie (hohes bis maximales Risiko)
- **2.797 Domains** (25,8 %) haben überhaupt keinen DMARC-Record und sind maximalen Sicherheitsrisiken und E-Mail-Zustellungsproblemen ausgesetzt
- **30,5%** der Domains mit DMARC fehlt RUA-Berichterstattung, wodurch sie blind sind ohne Überwachung
- **Finanzen (35,7%)** en **Informationssicherheit (34,6%)** führen in der p=reject-Einführung
- **Transport (15,3%)** und **Recht (16,7%)** haben die niedrigsten Schutzraten

DMARC VERSTEHEN

DMARC (Domain-based Message Authentication, Reporting & Conformance) ist ein E-Mail-Authentifizierungsprotokoll, das Organisationen vor E-Mail-Spoofing und Phishing-Angriffen schützt. Es baut auf zwei bestehenden Mechanismen auf: SPF (Sender Policy Framework) und DKIM (DomainKeys Identified Mail).

Eine DMARC-Richtlinie teilt empfangenden E-Mail-Servern mit, was zu tun ist, wenn sie auf eine E-Mail stoßen, die Authentifizierungsprüfungen nicht besteht. Es gibt drei Richtlinienstufen:

Richtlinie	Sicherheitsrisiko	Was passiert	Auswirkung
p=reject	NIEDRIG	Gefälschte E-Mails werden abgelehnt (zurückgewiesen)	Vollständiger Schutz. Angreifer können keine E-Mails von Ihrer Domain versenden.
p=quarantine	MITTEL	Gefälschte E-Mails gehen in den Spam-/Junk-Ordner	Teilschutz. Empfänger können gefälschte E-Mails möglicherweise noch in der Spam-Liste finden und vertrauen.
p=none	HOCH	Gefälschte E-Mails werden normal zugestellt	Kein Schutz. Nur Überwachung. Angreifer können Ihre Domain frei spoofen.
Kein DMARC	MAXIMAL	Keine Anweisungen für empfangende Server	Null Schutz und null Sichtbarkeit. Verursacht auch E-Mail-Zustellungs-probleme bei großen Anbietern.

Wichtig: Seit 2024 haben große E-Mail-Anbieter (Google, Microsoft, Yahoo) ihre Anforderungen an die E-Mail-Zustellung verschärft. Organisationen, die mehr als 5.000 E-Mails pro Woche ohne zumindest einen grundlegenden DMARC-Record (p=none) versenden, riskieren, dass ihre legitimen E-Mails abgelehnt oder gefiltert werden, was die geschäftliche Kommunikation und die Marketingeffizienz direkt beeinträchtigt.

GESAMTERGEBNISSE

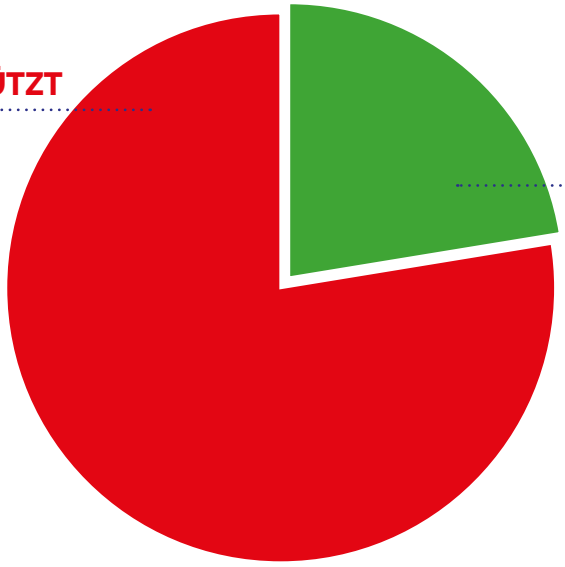
Der DMARC-Scan bewertete 10.833 einzigartige Domains. Die folgende Tabelle zeigt die Verteilung über die vier DMARC-Richtlinienkategorien:

DMARC-Richtlinie	Domains	Prozentsatz	Sicherheitsrisiko	E-Mail-Risiko
p=reject	2.432	22,4%	Niedrig	Niedrig
p=quarantine	2.391	22,1%	Mittel	Niedrig
p=none	3.213	29,7%	Hoch	Mittel
Kein DMARC record	2.797	25,8%	Maximal	Hoch
GESAMT	10.833	100%		

77,6%

NICHT VOLLSTÄNDIG GESCHÜTZT

8.401 Domains



22,4%

GESCHÜTZT

2.432 Domains

Für die 8.401 Domains ohne vollständigen Schutz sind die Folgen greifbar: Cyberkriminelle können E-Mails versenden, die angeblich von legitimen E-Mail-Adressen dieser Organisationen stammen. Für die 2.797 Domains ohne DMARC-Record ist das Risiko durch mögliche E-Mail-Zustellungsprobleme erhöht, da große Anbieter zunehmend DMARC-Compliance verlangen.

BRANCHENANALYSE

Die DMARC-Einführung unterscheidet sich erheblich zwischen Branchen. Die folgende Tabelle zeigt die DMARC-Richtlinienverteilung für jeden Sektor, sortiert nach dem Prozentsatz der Domains mit p=reject (vollständig geschützt). Die "Hohes Risiko" Spalte repräsentiert den kombinierten Prozentsatz der Domains mit entweder p=none oder keinem DMARC-Record, die anfälligsten für E-Mail-Spoofing-Angriffe sind.

Branche	n	p=reject	p=quar.	p=none	Kein DMARC	Hohes Risiko
Informationssicherheit	179	34,6%	36,3%	15,6%	13,4%	**29,1%**
Finanzen	381	35,7%	23,9%	28,6%	11,8%	**40,4%**
Behörden	401	32,4%	19,5%	6,5%	41,6%	**48,1%**
Wohnungsbau	58	27,6%	41,4%	29,3%	1,7%	**31,0%**
Wasserbehörden	8	37,5%	50,0%	12,5%	0,0%	**12,5%**
Gesundheitswesen	369	27,4%	24,1%	27,9%	20,6%	**48,5%**
Bildung	215	27,0%	25,6%	31,6%	15,8%	**47,4%**
Software & SaaS	210	25,2%	32,4%	29,5%	12,9%	**42,4%**
MSP	3,212	25,0%	24,1%	25,8%	25,1%	**50,9%**
Beratung	294	25,5%	21,8%	32,7%	20,1%	**52,7%**
Bauwesen	69	26,1%	24,6%	31,9%	17,4%	**49,3%**
Hosting	60	21,7%	28,3%	36,7%	13,3%	**50,0%**
Einzelhandel	133	23,3%	15,0%	40,6%	21,1%	**61,7%**
Transport	59	15,3%	20,3%	37,3%	27,1%	**64,4%**
Recht	24	16,7%	29,2%	33,3%	20,8%	**54,2%**

WICHTIGSTE BRANCHENBEOBACHTUNGEN

Führende

Informationssicherheit und **Finanzen** führen die DMARC-Einführung an mit den höchsten p=reject-Raten (34,6 % bzw. 35,7 %) und der niedrigsten Hochrisiko-exposition. Informationssicherheit sticht mit nur 29,1 % in der Hochrisikoklasse heraus. Diese Sektoren handhaben besonders sensible Daten, was wahrscheinlich ein stärkeres Bewusstsein für E-Mail-Sicherheit fördert. Doch auch hier bleiben die meisten Domains unzureichend geschützt.

Mittelmäßig

Behörden zeigen ein polarisiertes Bild: eine relativ hohe p=reject-Rate (32,4 %), aber auch eine sehr hohe "Kein DMARC"-Rate (41,6 %). Dies deutet darauf hin, dass viele Behörden Maßnahmen ergriffen haben, eine große Gruppe aber überhaupt nicht begonnen hat. **MSPs (Managed Service Provider)** zeigen durchschnittliche Einführung (25,0 % reject), stellen aber die größte Gruppe nach Volumen dar (3.212 Domains). Angesichts ihrer Rolle bei der Verwaltung der IT für andere Organisationen hat ihre eigene DMARC-Haltung überproportionale Bedeutung.

Nachzügler

Transport (64,4 % hohes Risiko) und **Einzelhandel (61,7 % hohes Risiko)** sind die am stärksten gefährdeten Sektoren. Diese Branchen interagieren häufig mit Verbrauchern per E-Mail (Versandbenachrichtigungen, Quittungen, Aktionen), was sie zu bevorzugten Zielen für Spoofing-Angriffe macht. Recht (54,2 % hohes Risiko) ist auch besorgniserregend angesichts der Sensibilität und des Vertrauens in rechtlichen Kommunikationen.

GEOGRAFISCHE ANALYSE

Der Scan umfasste Domains hauptsächlich aus vier Ländern: Niederlande, Deutschland, Belgien und Frankreich. Hier ist der Vergleich der DMARC-Einführung zwischen Regionen:

Land	Domains	p=reject	p=quarantine	p=none	Kein DMARC
Niederlande	4.702	25,9%	24,8%	30,3%	18,9%
Deutschland	3.003	22,7%	20,0%	27,1%	30,2%
Belgien	411	22,6%	29,4%	34,3%	13,6%
Frankreich	75	38,7%	29,3%	13,3%	18,7%

Niederlande führt in der DMARC-Einführung unter den Benelux- und DACH-Märkten (25,9 % p=reject) und hat die niedrigste Rate an Domains ohne DMARC-Record (18,9 %). Dies kann die aktive Förderung von E-Mail-Sicherheitsstandards durch die niederländische Regierung widerspiegeln.

Deutschland hat die höchste Rate an Domains ohne DMARC-Record (30,2 %), was auf breitere Bewusstseinslücken hindeutet, trotz einer starken Cybersicherheits-Regulierungsumgebung.

Belgien zeigt die höchste Quarantine-Einführung (29,4 %), was darauf hinweitet, dass viele belgische Organisationen DMARC implementiert haben, aber noch nicht zu vollständiger Durchsetzung übergegangen sind.

Frankreich zeigt die stärkste p=reject-Einführung in diesem Benchmark (38,7 %), obwohl die Stichprobengröße kleiner ist (75 Domains). Französische Organisationen haben auch die niedrigste p=none-Rate (13,3 %), was darauf hindeutet, dass französische Organisationen bei der DMARC-Implementierung tendenziell entschiedener zur Durchsetzung übergehen. Dies ist bemerkenswert im Kontext von Frankreichs starkem regulatorischem Fokus auf Cybersicherheit durch ANSSI (Agence nationale de la sécurité des systèmes d'information) und des proaktiven Standpunktes des Landes zur NIS2-Umsetzung.

DMARC-ÜBERWACHUNG & BERICHTERSTATTUNG

Ein oft übersehener Aspekt der DMARC-Implementierung ist die Konfiguration von RUA (Reporting URI for Aggregate reports). RUA ermöglicht es Organisationen, Berichte über E-Mail-Authentifizierungsergebnisse zu erhalten, was Einblick in bietet, wer E-Mails in ihrem Namen versendet und ob Spoofing-Versuche auftreten.

Metrik	Anzahl	Prozentsatz	Risiko
DMARC mit RUA (Überwachung aktiv)	5.588	69,5%	Verwaltet
DMARC ohne RUA (keine Überwachung)	2.448	30,5%	Blind

RUA-Einführung nach Richtlinienstufe:

- **p=reject:** 76,9% haben RUA konfiguriert
- **p=quarantine:** 75,2% haben RUA konfiguriert
- **p=none:** 59,7% haben RUA konfiguriert

Besonders besorgniserregend sind die **561 Domains mit p=reject aber ohne RUA und 592 Domains mit p=quarantine aber ohne RUA.** Diese Organisationen haben DMARC-Richtlinien durchgesetzt, haben aber keine Sichtbarkeit darüber, ob ihre eigenen legitimen E-Mails aufgrund von Fehlkonfigurationen blockiert werden. Ohne Überwachung riskieren sie, geschäftskritische E-Mail-Kommunikation stille zu verlieren.

GESCHÄFTLICHE AUSWIRKUNGEN & RISIKOBEWERTUNG

Sicherheitsrisiken

Für die 8.401 Domains ohne p=reject-Durchsetzung bleiben die folgenden Angriffsvektoren rentabel:

- E-Mail-Spoofing: Angreifer können E-Mails versenden, die angeblich von legitimen Unternehmensadressen stammen, und Kunden, Mitarbeiter und Partner abzielen.
- Business Email Compromise (BEC): CEO-Betrug, Rechnungsmanipulation und Zahlungsumleitungsangriffe nutzen alle gefälschte Absenderadressen aus.
- Markenimitation: Phishing-Kampagnen, die Ihre Domain missbrauchen, schädigen das Kundenvertrauen und die Markenreputation.
- Supply-Chain-Angriffe: Das Spoofen einer vertrauenswürdigen Lieferanten-Domain kann zum Eindringen in Partner-Netzwerke verwendet werden.

E-Mail-Zustellungsrisiken

Seit 2024 verlangen Google, Microsoft und Yahoo von Massensender (>5.000 E-Mails/Woche) mindestens einen DMARC-Record mit p=none. Für die 2.797 Domains ohne DMARC-Record können legitime E-Mails von diesen Anbietern abgelehnt oder gefiltert werden, was die geschäftliche Kommunikation, Marketingkampagnen und Transaktions-E-Mails (Rechnungen, Bestätigungen, Benachrichtigungen) direkt beeinträchtigt.

Warum regelmäßige DMARC-Überprüfung unverzichtbar ist

Die DMARC-Implementierung ist keine einmalige Aktivität. E-Mail-Infrastruktur ist dynamisch: Organisationen adoptieren regelmäßig neue Tools für Marketing, CRM, Kundensupport, Abrechnung und interne Kommunikation. Jedes neue Tool, das E-Mails in Ihrem Namen versendet, muss über SPF und DKIM ordnungsgemäß authentifiziert werden. Ohne regelmäßige Überprüfung führen diese Änderungen zu Konfigurationsabweichung, die sogar eine gut konfigurierte DMARC-Richtlinie untergraben kann.

Häufige Ursachen für DMARC-Konfigurationsabweichung sind:

- **Neue E-Mail-Versanddienste:** Das Hinzufügen einer Marketing-Plattform, HR-Recruiting-Tool, Abrechnungssystem oder Helpdesk, der E-Mails von Ihrer Domain versendet. Jede erfordert SPF/DKIM-Updates, die oft übersehen werden.
- **Anbieter-seitige SPF-Änderungen:** Drittanbieter können ihre eigenen SPF-Records aktualisieren oder neue DNS-Includes hinzufügen. Da SPF alle verschachtelten Lookups auswertet (mit maximal 10), können Änderungen Ihre Domain stille über das Lookup-Limit hinausschieben, was zu Authentifizierungsfehlern führt.
- **DKIM-Schlüsselrotation:** DKIM-Schlüssel sollten regelmäßig zu Sicherheitszwecken rotiert werden. Wenn DNS-Records nicht entsprechend aktualisiert werden, schlägt die DKIM-Validierung fehl.
- **Infrastruktur-Migrationen:** Der Wechsel zu einer neuen E-Mail-Plattform, einem Cloud-Anbieter oder einer IT-Umgebung führt oft zu Lücken in der Authentifizierungskonfiguration.
- **Sich entwickelnde Bedrohungslandschaft:** Angreifer passen ihre Techniken ständig an. Die Überwachung von DMARC-Berichten hilft, neue Spoofing-Versuche auf Ihre Domain zu erkennen, was eine proaktive Sicherheitshaltung ermöglicht.

Das Risiko von ***nicht*** regelmäßiger DMARC-Überprüfung ist zweifach: legitime geschäftliche E-Mails können stille abgelehnt werden (was Umsatz und Kundenkommunikation beeinträchtigt), während gleichzeitig neue Schutzlücken entstehen können, die Angreifer ausnutzen können. Kontinuierliche Überwachung durch DMARC-Aggregatberichte (RUA) ist der effektivste Weg, diese Probleme zu erkennen, bevor sie geschäftliche Auswirkungen haben.

Compliance- & Regulatorische Rahmen

E-Mail-Authentifizierung und DMARC werden zunehmend in großen regulatorischen Rahmen und Sicherheitsstandards referenziert. Organisationen, die DMARC vernachlässigen, sehen sich nicht nur direkten Sicherheits- und Zustellungsrisiken ausgesetzt, sondern stellen möglicherweise auch fest, dass sie regulatorische Erwartungen nicht erfüllen:

NIS2-Richtlinie (EU)

Die EU-Richtlinie **NIS2** (Network and Information Security Directive 2) erweitert erheblich den Umfang der Cybersicherheitsanforderungen für Organisationen in Europa.

NIS2 betont Supply-Chain-Sicherheit, Cyber-Hygiene und Risk-Management-Praktiken. Die Abwesenheit einer DMARC-Richtlinie mit Durchsetzung (p=reject) könnte die Compliance mit mehreren NIS2-Anforderungen schwächen, da E-Mail-Spoofing eines der häufigsten anfänglichen Angriffsvektoren in Supply-Chain-Kompromissen bleibt. Die meisten "wesentlichen" Entitäten haben ein Compliance-Audit-Zieldatum von **30. Juni 2026**.
Die Implementierung und Wartung von DMARC mit Überwachung ist eine konkrete, überprüfbare Maßnahme, die proaktives Risk-Management demonstriert.

ISO 27001

ISO 27001 ist der internationale Standard für Informationssicherheits-Managementsysteme (ISMS). Während ISO 27001 keine spezifischen Technologien vorschreibt, erfordert sein risikobasierter Ansatz, dass Organisationen Informationssicherheitsrisiken identifizieren und mindern. E-Mail-Spoofing und Phishing stellen erhebliche Risiken dar, die DMARC direkt adressiert. Anhang-A-Kontrollen bezüglich Kommunikationssicherheit (A.13), Systembeschaffung und -entwicklung (A.14) und Lieferantenbeziehungen (A.15) haben alle Relevanz für E-Mail-Authentifizierung. Organisationen, die ISO 27001-Zertifizierung anstreben oder halten, sollten DMARC-Durchsetzung in ihr Kontrollset als nachweisbare Maßnahme gegen E-Mail-basierte Bedrohungen einbeziehen.

NEN 7510 (Gesundheitswesen, Niederlande)

NEN 7510 ist der niederländische Standard für Informationssicherheit im Gesundheitswesen, eng verwandt mit ISO 27001, aber speziell auf den Gesundheitssektor zugeschnitten. Die niederländische Legislation verlangt von Gesundheitsanbietern, NEN 7510 einzuhalten, wenn sie Gesundheitsinformationssysteme und elektronische Austauschsysteme nutzen. Angesichts der Tatsache, dass Gesundheitsorganisationen häufig sensible Patientendaten und Terminvereinbarungen per E-Mail kommunizieren, ist DMARC-Durchsetzung eine kritische technische Maßnahme, um Spoofing von Gesundheits-Domains zu verhindern. Mit 48,5 % der Gesundheits-Domains in unserer Benchmark in der Hochrisikoklasse gibt es erhebliche Verbesserungsmöglichkeiten. Eine ordnungsgemäße DMARC-Implementierung unterstützt die NEN-7510-Compliance, indem sie die Integrität und Authentizität von E-Mail-Kommunikationen schützt.

In allen diesen Rahmen ist der gemeinsame Thread klar: E-Mail-Authentifizierung über DMARC ist nicht länger optional, sondern zunehmend erwartet als grundlegende Sicherheitsmaßnahme. Organisationen sollten DMARC-Durchsetzung nicht als Einzelprojekt, sondern als Teil ihres laufenden Informationssicherheits-Managements betrachten, mit periodischen Überprüfungen, die in ihre Compliance-Zyklen integriert sind.

EMPFEHLUNGEN

Basierend auf den Erkenntnissen in diesem Bericht empfehlen wir Organisationen, je nach ihrem aktuellen DMARC-Status die folgenden Maßnahmen zu ergreifen:

Für Domains ohne DMARC-Record (2.797 Domains)

1. **Implementieren Sie einen DMARC-Record sofort**, beginnend mit p=none, um mit dem Sammeln von Authentifizierungsdaten zu beginnen, ohne den E-Mail-Fluss zu beeinflussen.
2. **Beziehen Sie eine RUA-Adresse ein,** um Aggregat-DMARC-Berichte zu erhalten und Einblick in E-Mail-Authentifizierungsergebnisse zu gewinnen.
3. **Verifizieren Sie SPF- und DKIM-Konfigurationen**, um sicherzustellen, dass alle legitimen E-Mail-Quellen ordnungsgemäß authentifiziert sind.

Für Domains mit p=none (3.213 Domains)

1. **Analysieren Sie DMARC-Aggregatberichte**, um alle legitimen E-Mail-Quellen zu identifizieren und Authentifizierungsfehler zu adressieren.
2. **Planen Sie einen Migrationspfad zu p=quarantine und dann p=reject.** Auf p=none zu bleiben bietet auf unbestimmte Zeit keinen Schutz.
3. Erwägen Sie, einen DMARC-Management-Spezialisten einzubeziehen, um den Übergang zur Durchsetzung zu beschleunigen.

Für Domains mit p=quarantine (2.391 Domains)

1. **Wechseln Sie zu p=reject**, sobald DMARC-Berichte bestätigen, dass alle legitimen E-Mail-Quellen Authentifizierung konsistent bestehen.
2. Stellen Sie sicher, dass RUA-Berichterstattung aktiv ist (derzeit fehlt 24,8 % der Quarantine-Domains die Überwachung).

Für Domains mit p=reject (2.432 Domains)

1. **Halten Sie aktive DMARC-Überwachung**. 23,1 % der Reject-Domains fehlt RUA-Berichterstattung.
2. Überprüfen Sie regelmäßig DMARC-Berichte, um Fehlkonfigurationen frühzeitig zu erkennen, besonders wenn neue E-Mail-Versanddienste hinzugefügt oder Infrastruktur migriert werden.

Für alle Organisationen

- **Planen Sie regelmäßige DMARC-Überprüfungen** (mindestens vierteljährlich), um Konfigurationsabweichung, neue nicht autorisierte Sender und Änderungen in der Bedrohungslandschaft zu erkennen.
- **Integrieren Sie DMARC in Ihr Compliance-Programm** als nachweisbare Kontrolle für NIS2, ISO 27001 und branchenspezifische Standards wie NEN 7510.
- **Stellen Sie Lieferkettenbewusstsein sicher**: Bewerten Sie die DMARC-Haltung Ihrer Schlüsselpartner und Lieferanten als Teil Ihres Drittanbieter-Risiko-Management-Prozesses.

METHODIK

Diese Benchmark-Studie wurde mit dem folgenden Ansatz durchgeführt:

1. **Domainsammlung:** Eine deduplizierte Liste von 10.833 einzigartigen Domains wurde aus der Guardian360-Plattform zusammengestellt, die Organisationen im Guardian360-Partner- und Kundenekoystem repräsentiert.
2. **DMARC-Scanning:** Jede Domain wurde von DMARC Advisor B.V. gescannt, um ihren aktuellen DMARC-DNS-Record abzurufen, wobei die Richtlinie (p= value), Berichtsadressen (RUA/RUF) und verwandte Konfigurationen extrahiert wurden.
3. **Branchenklassifizierung:** Domains wurden mit Organisationsdatensätzen abgeglichen (85,7 % Übereinstimmungsquote), um eine Aufschlüsselung nach Branche, Organisationstyp und Geografie zu ermöglichen.
4. **Analysezeitraum:** Der Scan wurde im April 2026 durchgeführt. DMARC-Records sind dynamisch und können sich jederzeit ändern; dieser Bericht spiegelt den Zustand zum Zeitpunkt des Scans wider.

ÜBER UNS

Guardian360

Guardian360 ist ein Cybersicherheitsunternehmen mit Sitz in Rotterdam, Niederlande. Guardian360 bietet kontinuierliche Sicherheitsüberwachung, Schwachstelle-Bewertung und Compliance-Services für Organisationen in ganz Europa, sowohl direkt als auch über ein Netzwerk von Managed Service Provider (MSP)-Partnern.

DMARC Advisor

DMARC Advisor B.V., mit Sitz in Dordrecht, Niederlande, spezialisiert sich auf E-Mail-Authentifizierung und DMARC-Management. Ihre Plattform hilft Organisationen, DMARC, SPF und DKIM zu implementieren und zu warten, um Domains vor E-Mail-Spoofing zu schützen und E-Mail-Zustellbarkeit zu verbessern.

Benötigen Sie Hilfe bei der Verbesserung Ihrer DMARC-Haltung?

Guardian360 kann Sie bei der Bewertung Ihres aktuellen E-Mail-Authentifizierungsstatus, der Implementierung von DMARC mit Durchsetzung und der Einrichtung kontinuierlicher Überwachung unterstützen, um Ihre Domain vor Spoofing zu schützen und E-Mail-Zustellbarkeit sicherzustellen.

Kontaktieren Sie uns:
support@guardian360.de

GUARDIAN 360°
www.guardian360.de