MAILTOWER

Austria E-Mail Security Report™

Analyse der österreichischen E-Mail-Sicherheitslandschaft

JULI 2024

A Mailtower Austria Service Survey

Inhaltsverzeichnis

SCAN ME

Über Mailtower

Die Mailtower.app (https://mailtower.app) ist ein spezialisiertes Reportservice, ein Tool zur Verbesserung der **E-Mail-Sicherheit**, das Schwachstellen im Mailsystem aufdeckt und konkrete Optimierungsvorschläge bietet. Mit benutzerfreundlichen Konfiguratoren und Werkzeugen für SPF, DKIM und DMARC hilft die “Made in Europe”-Plattform, die E-Mail-Kommunikation sicher und zuverlässig zu gestalten. Zudem unterstützt Mailtower.app Unternehmen durch umfassende Beratung und praktische Hilfsmittel bei der Implementierung effektiver Sicherheitsmaßnahmen.

Willkommen

In einer Zeit, in der digitale Kommunikation das Rückgrat unserer Geschäftswelt bildet, ist E-Mail-Sicherheit **nicht nur ein Nice-to-have**, sondern eine absolute **Notwendigkeit**. Unser Report wirft einen detaillierten Blick auf den Status quo der **E-Mail-Sicherheit** in Österreich.

Was erwartet Sie in diesem Report?

- Eine umfassende Analyse von **87.017 aktiven österreichischen Unternehmens-Domains**, die über öffentliche Verzeichnisse sichtbar sind.
- Tiefgehende Einblicke in die **Implementierung von SPF und DMARC**
- Ein **Bundesländervergleich**, der regionale Stärken und Optimierungspotenziale aufzeigt.
- Konkrete **Handlungsempfehlungen** für die Stärkung Ihrer E-Mail-Sicherheit

Unser Ziel? Ihnen die Tools und das Wissen an die Hand zu geben, um Ihre digitale Kommunikation sicherer, effizienter und vertrauenswürdiger zu gestalten. Denn in der sich rasant entwickelnden Cyber-Landschaft ist Stillstand keine Option - vielmehr ist es entscheidend, **“proaktiv” vorzugehen.** Lassen Sie uns gemeinsam neue Wege beschreiten und kreative Räume schaffen, in denen Ihr Unternehmen florieren kann. Denn jede Herausforderung im Bereich der IT-Sicherheit ist auch eine Chance zur Innovation und Differenzierung.

Sind Sie bereit, Ihre E-Mail-Sicherheit auf ein neues Level zu heben? Dann lassen Sie uns gemeinsam in die Daten eintauchen und die Zukunft der sicheren digitalen Kommunikation in Österreich gestalten! Viel Erkenntnisgewinn bei der Lektüre wünscht

Tino, Guntram & Ronald
Ihr Mailtower.app-Team

Executive Summary

Die E-Mail-Infrastruktur österreichischer Unternehmen zeigt erhebliche Unterschiede in der Implementierung von SPF und DMARC. Angesichts der zunehmenden Anforderungen großer E-Mail-Anbieter wie Google, die in Zukunft möglicherweise keine E-Mails mehr ohne diese Sicherheitsprotokolle akzeptieren, ist es dringend notwendig, diese Verfahren umgehend umzusetzen. Dies ist nicht nur aus Datenschutzgründen wichtig, sondern auch, um die Zustellbarkeit von E-Mails sicherzustellen und das Vertrauen in die E-Mail-Kommunikation zu stärken.

Wichtigste Ergebnisse

1. **Hohe Nutzung von Basis-Schutzmaßnahmen** durch die Vergabe von Versende-Berechtigungen für definierte E-Mail-Server. (SPF: 81,2%)
2. **Bisher geringe Anwendung aktueller Schutzmaßnahmen** gegen gespoofte E-Mails (DMARC-Reject: 3,14%)
3. **Hohe unüberlegte Datenweitergabe** durch DMARC-Reporting-Dienste, die zur Veröffentlichung sensibler Unternehmens-metainformationen führen kann.

Gefahren und Herausforderungen:

- **Unzureichender Schutz vor E-Mail-Betrug** und -Missbrauch
- Risiko von Reputationsschäden und finanziellen Verlusten durch vermeidbare Cyber-Attacken.

Handlungsempfehlungen:

1. Vollständiger Einsatz von **E-Mail-Absenderüberprüfung** (SPF und DKIM-Konfiguration)
2. Einführung der sicheren **DMARC Richtlinie “Policy=Reject”**
3. Monitoring durch **passende Tools**

DKIM

Sicherer E-Mail-Versand durch digitale Signaturen
DKIM verwendet kryptografische Signaturen, um die Authentizität und Integrität von E-Mails sicherzustellen, indem es eine digitale Signatur im Kopf der E-Mail einfügt, die vom empfangenden Server mit dem DNS-Eintrag des Absenders verifiziert wird.

SPF

Verhindern Sie E-Mail-Spoofing mit SPF
SPF ermöglicht es Domain-Inhabern, die IP-Adressen festzulegen, die zum Senden von E-Mails im Namen ihrer Domain berechtigt sind, indem sie eine SPF-Eintragung im DNS veröffentlichen, die vom empfangenden Server überprüft wird.

DMARC

Kombinierte Sicherheitsmaßnahmen für einen umfassenden E-Mail-Schutz
DMARC erweitert SPF- und DKIM, indem es eine Policy-Framework bereitstellt, das angibt, wie E-Mail-Server mit nicht-authentifizierten Nachrichten umgehen sollen, und gleichzeitig Berichte über E-Mail-Aktivitäten an die Domain-Inhaber sendet. DMARC sorgt dafür, dass die Absenderadresse einer E-Mail echt ist, indem es überprüft, ob die E-Mail wirklich von der angegebenen Domain stammt.

Technical Summary

Der „E-Mail Security Report Austria„ von Mailtower.app bietet eine umfassende Analyse der E-Mail-Sicherheit in Österreich. Die wichtigsten Erkenntnisse des Reports sind:

- **SPF-Implementierung:** Österreichische Domains zeigen eine hohe Adoptionsrate von SPF (~81,2%), wobei Hardfail-Konfigurationen von rund 52% und Softfail-Konfigurationen von etwa 29,2% genutzt werden.
- **DMARC-Nutzung:** Nur 3,14% der Domains verwenden die DMARC Reject-Policy, was auf ein großes Potenzial für Verbesserungen hinweist.
- **Verbreitete Mail Provider und DMARC Services:** Die Marktführer bei den Mail Providern sind Microsoft 365 und Google Workspace, während Valimail und Proofpoint bei den Dmarc Report Servicen dominieren.
- **Regionale Unterschiede:** Es gibt signifikante regionale Unterschiede in der Implementierung und Nutzung.

Gefahren und Herausforderungen:
Der unzureichende Einsatz von E-Mail-Authentifizierungsmechanismen wie DKIM, SPF und DMARC kann zu erheblichen Sicherheitslücken führen. Risiken wie gefälschte E-Mails, können zu Phishing-Angriffen, Malware-Infektionen und Betrug führen.

Handlungsempfehlungen: Der Report empfiehlt die Optimierung der SPF-Konfiguration, die stufenweise Einführung von DMARC und die sorgfältige Auswahl geeigneter Dmarc Report Service.

Der Benchmark der E-Mail-Sicherheit

Willkommen zum „E-Mail Security Report Austria”! Als treibende Kraft und Hauptverantwortlicher hinter Mailtower.app freue ich mich, Ihnen die neuesten Technologien und Best Practices zur Sicherung Ihrer digitalen Kommunikation vorzustellen.

Tino Hager
Tino@nager.software

Datengetriebene Erkenntnisse

Hallo und herzlich willkommen! Als Business Analyst bei Mailtower.app habe ich die Daten für diesen Report sorgfältig analysiert, um Ihnen präzise und wertvolle Insights zur E-Mail-Sicherheit in Österreich zu liefern.

Guntram Bechtold
Guntram.Bechtold@StarsMedia.com

Analysen und Trends der IT-Landschaft

Herzlich willkommen zum „E-Mail Security Report Austria”. Als Forscher freue ich mich, Ihnen tiefgehende Analysen und Erkenntnisse über die aktuellen Trends und Herausforderungen in der E-Mail-Sicherheit präsentieren zu können.

Prof. Dr. Ronald Petrlic
office@datensicherheit.digital

Zielsetzung

Der „E-Mail-Security-Report Austria“ verfolgt diese zentralen Ziele:

1. **Statusaufnahme der E-Mail-Sicherheit in österreichischen Unternehmen**
2. Wir liefern einen **umfassenden Überblick** über den aktuellen Stand der Implementierung von SPF und DMARC bei über 87.017 österreichischen Unternehmensdomains. Diese Bestandsaufnahme dient als Grundlage für fundierte Entscheidungen im Bereich der E-Mail-Sicherheit.
3. **Identifikation regionaler Unterschiede**
4. Durch die **Analyse auf Bundesländerebene** decken wir geografische Disparitäten in der E-Mail-Sicherheitslandschaft auf. Dies ermöglicht gezielte Maßnahmen und Best-Practice-Sharing zwischen den regionalen Mail-Anbietern.
5. **Benchmarking und Vergleichsmöglichkeiten**
6. Unternehmen erhalten die Möglichkeit, ihre eigenen **Sicherheitsmaßnahmen** mit branchenüblichen Standards und regionalen Durchschnittswerten zu vergleichen.
7. **Sensibilisierung für E-Mail-Sicherheit**
8. Der Report zielt darauf ab, das **Bewusstsein für die Bedeutung** robuster E-Mail-Sicherheitsmechanismen zu schärfen und deren Einfluss auf die gesamte Cybersicherheit zu verdeutlichen.
9. **Handlungsempfehlungen ableiten**
10. Basierend auf den Erkenntnissen entwickeln wir **konkrete, praxisorientierte Empfehlungen** zur Optimierung der E-Mail-Sicherheit für Unternehmen verschiedener Größenordnungen.

Impulse für Innovation setzen

- Durch die **Analyse aktueller Trends** und Herausforderungen möchten wir Innovationsimpulse im Bereich der E-Mail-Sicherheit anstoßen und neue **Lösungsansätze fördern.**
- **Entscheidungsunterstützung** bieten
- Der Report soll als **solide Entscheidungsgrundlage für IT-Verantwortliche, C-Level-Executives** und **politische Entscheidungsträger** dienen, um strategische Weichenstellungen im Bereich der digitalen Sicherheit vorzunehmen.

Prüfungsaufbau & Datengrundlage

Für den „E-Mail Security Report Austria” haben wir eine umfassende und methodisch fundierte Analyse durchgeführt. Hier ein Überblick über unsere Vorgehensweise:

Datengrundlage

- Untersuchung von über 87.017 österreichischen Unternehmens-Domains
- Abdeckung aller neun Bundesländer für eine repräsentative Stichprobe
- Erhebungszeitraum: Q3 2024

Analysierte Mechanismen

1. SPF (Sender Policy Framework)
    - Erfassung von Hardfail- und Softfail-Konfigurationen
2. DMARC (Domain-based Message Authentication, Reporting & Conformance)
    - Fokus auf DMARC Reject-Policy als strikteste Sicherheitseinstellung
3. Mail Provider und Dmarc Report Service
    - Identifikation der drei meistgenutzten Anbieter pro Kategorie und Bundesland

Datenerhebung

1. Automatisierte Abfrage der DNS-Einträge für jede Domain
2. Analyse der SPF- und DMARC-Records
3. Kategorisierung der Ergebnisse nach Bundesländern

Datenanalyse

Quantitative Auswertung der SPF- und DMARC-Implementierungen
Prozentuale Berechnung der Nutzungsraten
Ranking der Mail Provider und Dmarc Report Service nach Häufigkeit

Qualitätssicherung

Mehrfache Überprüfung der Daten zur Sicherstellung der Genauigkeit
Stichprobenartige manuelle Verifizierung der automatisierten Ergebnisse

Limitationen

- Die Analyse basiert auf öffentlich zugänglichen **DNS-Einträgen**
- Die DKIM-Auswertung wurde aufgrund von Protokoll-technischer Beschränkungen nicht berücksichtigt.

Dieses Vorgehen ermöglicht es, einen detaillierten und verlässlichen Einblick in die E-Mail-Sicherheitslandschaft österreichischer Unternehmen zu geben. Es bildet die Grundlage für unsere Analysen, Vergleiche und Handlungsempfehlungen in den folgenden Kapiteln.

MAILTOWER

E-Mail Sicherheits-mechanismen

Überblick

SPF, DKIM UND DMARC

E-Mail Sicherheits-mechanismen im Überblick

DMARC (Domain-based Message Authentication, Reporting & Conformance), SPF (Sender Policy Framework) und DKIM (DomainKeys Identified Mail) sind E-Mail-Authentifizierungsprotokolle, die gemeinsam genutzt werden, um die Echtheit von E-Mails zu überprüfen und Phishing sowie Spoofing zu verhindern.

SPF

Sender Policy Framework

SPF ist ein Authentifizierungsprotokoll, das Empfänger-Mailserver dabei unterstützt, die Legitimität eingehender E-Mails zu verifizieren.

Funktionsweise:

- Der Domaininhaber definiert in einem DNS-Eintrag, welche IP-Adressen zum Mail-Versand berechtigt sind.
- Erst in Kombination mit DMARC ist die Prüfung der E-Mails sicher

Konfigurationsoptionen:
Hardfail (~49,14% im österreichischen Durchschnitt): Strikteste Einstellung, bei der nicht autorisierte E-Mails abgelehnt werden.
Softfail (~28,94% im österreichischen Durchschnitt): Verdächtige E-Mails werden markiert, aber nicht automatisch abgelehnt.
Neutral (~5% im österreichischen Durchschnitt): Keine spezifische Anweisung.
Kein SPF-Eintrag: Die verbleibenden Domains haben keinen SPF-Eintrag.

Vorteile:

- Bietet Schutz vor Spoofing-Angriffen (In Kombination mit DMARC)
- Autorisiert Mailserver bei der Versendung
- Verbessert die Zustellbarkeit legitimer E-Mails

Herausforderungen:

- Kann bei komplexen E-Mail-Setups (z.B. Weiterleitungen) Probleme verursachen
- Erfordert eine saubere IT-Landschaft.

DKIM

DomainKeys Identified Mail

DKIM ist ein kryptografisches Verfahren zur Signierung von E-Mails, das die Integrität und Authentizität der Nachricht sicherstellt.

Funktionsweise:

- Der sendende Mailserver fügt jeder E-Mail eine digitale Signatur zum E-Mail-Header hinzu.
- Der empfangende Server verifiziert diese Signatur mithilfe des öffentlichen Schlüssels, der im DNS der sendenden Domain hinterlegt ist.

Vorteile:

- Verhindert Manipulation des E-Mail-Inhalts während der Übertragung.
- Stärkt das Vertrauen in die Authentizität der E-Mail
- Funktioniert auch bei Weiterleitungen (Im Vergleich zu SPF)

Herausforderungen:

- Komplexere Einrichtung im Vergleich zu SPF
- Automatismus, um die Schlüssel regelmäßig zu erneuern.

E-Mail Sicherheits-mechanismen in Verbindung

SPF überprüft, ob eine E-Mail von einem autorisierten Server gesendet wurde, DKIM stellt sicher, dass die E-Mail während der Übertragung nicht verändert wurde, und DMARC bietet eine Richtlinie für den Umgang mit nicht authentifizierten E-Mails.

DMARC

Domain-based Message Authentication, Reporting & Conformance

DMARC baut auf SPF und DKIM auf und bietet einen umfassenden Rahmen für E-Mail-Authentifizierung und Berichterstattung.

Funktionsweise:

- Definiert eine Richtlinie für den Umgang mit E-Mails, die die SPF- oder DKIM-Prüfungen nicht bestehen
- Stellt sicher, dass die sichtbare Absender-Domain mit dem technischen Absender im SPF übereinstimmt oder dass die DKIM-Signatur von der sichtbaren Absender-Domain stammt.
- Ermöglicht Domaininhabern, detaillierte Berichte über alle E-Mail-Aktivitäten zu erhalten

Konfigurationsoptionen:

- Reject: Strikteste Policy, nicht authentifizierte E-Mails sollen abgelehnt werden (durchschnittlich bei 3.15% verwendet)
- Quarantine: Verdächtige E-Mails sollen in Quarantäne verschoben werden (durchschnittlich bei 3.87% verwendet)
- None: Keine Anweisung für den empfangenden Mailserver. (durchschnittlich bei 25.89% verwendet)
- Gesamt: 32.91% DMARC Nutzung und 67,09% ohne Konfiguration

Vorteile:

- Verbessert den Schutz vor Phishing und E-Mail-Spoofing
- Integriertes Reporting bietet einen umfassenden 360°-Blick alle E-Mail-Systeme zu sehen, die die Domain E-Mails senden können. Dies unterstützt eine vollständige Transparenz und Kontrolle über die E-Mail-Infrastruktur der Domain.
- Liefert wertvolle Einblicke über potenzielle Bedrohungen

Herausforderungen:

- Erfordert sorgfältige Implementierung und Überwachung
- Volle Effektivität erst bei breiter Adoption im E-Mail-Ökosystem

Die Kombination dieser drei Mechanismen bildet das Rückgrat moderner E-Mail-Sicherheit. Eine umfassende Implementierung aller drei Mechanismen ist der Schlüssel zu einer robusten E-Mail-Sicherheitsstrategie.

MAILTOWER

Analyse Österreich

Fokus auf Unternehmens-Infrastruktur in Österreich

Der Report im Detail: Ein umfassender Überblick

Österreich Analyse Übersichtsreport

SPF-Implementierung

1. Durchschnittliche haben 78,08% der analysierten Unternehmens-Domains SPF implement
2. Hardfail-Konfigurationen werden von durchschnittlich 49,14% der Domains genutzt.
3. Softfail-Konfigurationen finden sich bei etwa 28,94% der untersuchten Domains.

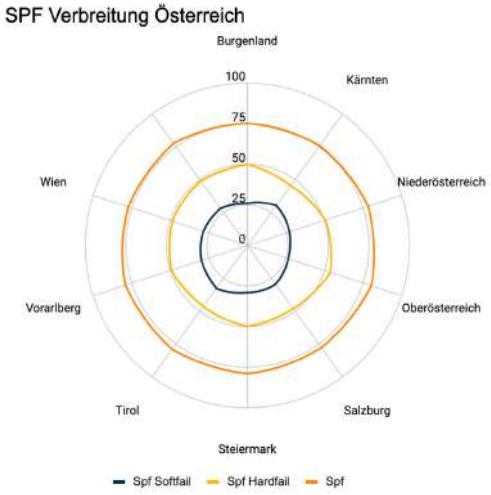
DMARC-Nutzung

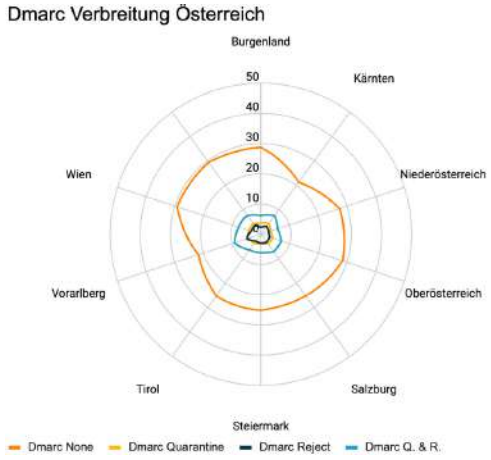
- Die empfohlene DMARC Reject-Policy wird im österreichischen Durchschnitt von 3,15% der Domains genutzt.
- Dies deutet auf ein erhebliches Verbesserungspotenzial in der Implementierung strenger DMARC-Richtlinien hin.
- Die relativ geringe Nutzung unterstreicht die Notwendigkeit verstärkter Aufklärung und Unterstützung bei der DMARC-Implementierung.

Top Mail- und DMARC-Services

- Mailprovidern dominieren Microsoft 365 und Google Workspace landesweit.
- Easyname.eu etabliert sich als starker dritter Anbieter in mehreren Bundesländern.
- Bei DMARC Reporting Services führt valimail.com, gefolgt proofpoint.com.

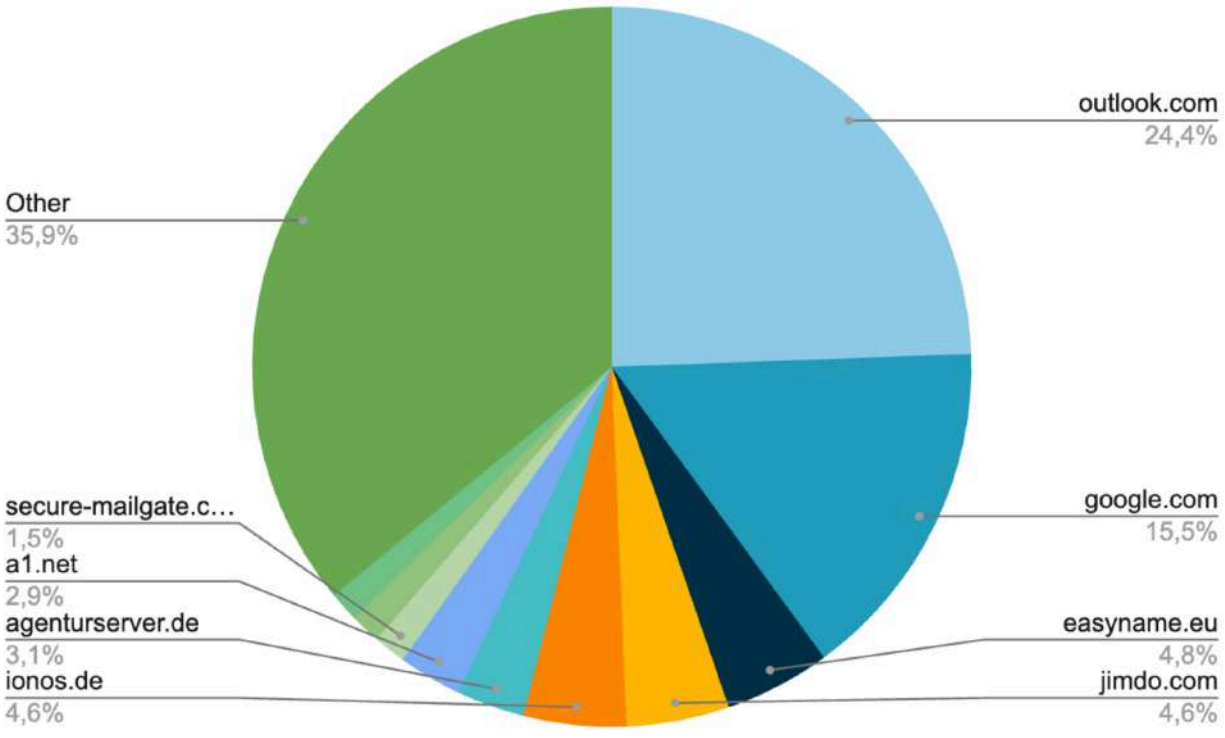
Österreich E-Mail Security Alert Map: DMARC Reject
Wien und Vorarlberger sind relativ gesehen die Nationalen Vorreiter in der E-Mail Security mit DMARC Reject Policy.
Roter: relativ wenige Schutzmaßnahmen.
Grün: relativ mehr Schutzmaßnahmen.





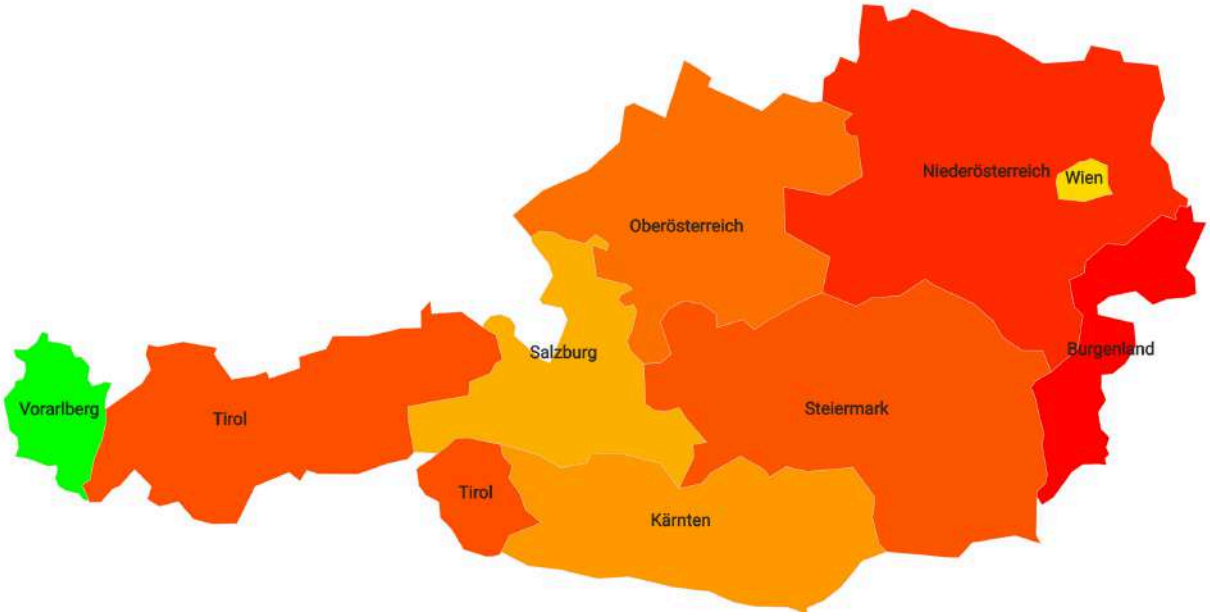
Führende Mail Provider in Österreich

	Mailprovider	Verbreitung (%)	Verbreitung Total
1	Microsoft 365	24,43	3651
2	Google Workspace	15,52	2654
3	easyname.eu	4,77	713
4	jimdo.com	4,62	691
5	ionos.de	4,61	689
6	agenturserver.de	3,05	456
7	a1.net	2,88	430
8	secure-mailgate.com	1,46	218
9	conova.com	1,37	204
10	ispgateway.de	1,35	201
11	barracudanetworks.com	1,18	177
12	one.com	1,16	174
13	rundrweb.com	0,98	146
14	mailspamprotection.com	0,94	141
15	hornetsecurity.com	0,94	141
16	bon.at	0,86	129
17	pphosted.com	0,86	128
18	mymailwall.com	0,81	121
19	mybizcloud.at	0,76	114
20	udag.de	0,69	103
21	your-server.de	0,68	102
	Other	26,08	



Führende DMARC Report-Services

- Bei den Mailprovidern dominieren Microsoft 365 und Google Workspace in Österreich.
- Easyname.eu etabliert sich als starker dritter Anbieter in mehreren Bundesländern.
- Bei DMARC-Providern führt Valimail, gefolgt von brevo.com und proofpoint.com.
- Die Präsenz spezialisierter DMARC-Provider zeigt ein wachsendes Interesse an professionellen Lösungen.



Österreich E-Mail Security Alert Map: DMARC Reject
Wien und Vorarlberger sind relativ gesehen die Nationalen Vorreiter in der E-Mail Security mit DMARC Reject Policy

Vergleichende Analyse

In diesem Abschnitt werfen wir einen detaillierten Blick auf die Implementierung von SPF und DMARC in den verschiedenen österreichischen Bundesländern.

Trotz generell hoher SPF-Raten gibt es bemerkenswerte regionale Unterschiede, während die DMARC-Nutzung insgesamt auf einem niedrigen Niveau bleibt.

Detail Analyse

SPF-Implementierung im Vergleich

- Spitzenreiter: Oberösterreich (80,37%)
- Schlusslicht: Kärnten (76,02%)
- Die Differenz von 4,35 Prozentpunkten zeigt regionale Unterschiede in der Adoptionsrate.
- Generell hohe Implementierungsraten über alle Bundesländer hinweg.

DMARC-Nutzung im Vergleich

- Spitzenreiter: Vorarlberg (4,85%)
- Schlusslicht: Burgenland (2,42%)
- Große Spannweite von 2,43 Prozentpunkten deutet auf unterschiedliche Prioritäten hin.
- Generell niedriges Niveau der DMARC Reject-Policy-Nutzung in allen Bundesländern.

Regionale Unterschiede bei Mail- und DMARC-Providern

Mailprovider:

- Microsoft 365 und Google Workspace in dominieren in fast allen Bundesländern.
- Regionale Anbieter wie easyname.eu, al.net, und mynet.at zeigen lokale Stärken.
- Wien als einziges Bundesland mit Google Workspace an erster Stelle.

DMARC-Provider:

- Valimail führt in den meisten Bundesländern.
- Brevo.com als überraschende, zweite Nennung (Siehe Anhang: Brevo).
- Regionale Unterschiede zeigen sich bei den drittplatzierten Anbietern.
- Proofpoint.com findet sich in mehreren Bundesländern unter den Top 3.

Diese Analyse zeigt sowohl landesweite Trends als auch regionale Besonderheiten in der E-Mail-Sicherheitslandschaft Österreichs. Sie bietet wertvolle Einblicke für gezielte Verbesserungsmaßnahmen und Best-Practice-Sharing zwischen den Bundesländern.

MAILTOWER

Best Practices & Hinweise

Überblick

Konkrete Tipps und Hinweise

Empfehlungen

In diesem Abschnitt zeigen wir bewährte Methoden zur Optimierung der E-Mail-Sicherheit. Insbesondere zeigen wir Ihnen, wie Sie Ihre SPF-Konfiguration verbessern können, um die Sicherheit und Zuverlässigkeit Ihrer E-Mail-Kommunikation zu maximieren.

Optimierung der SPF-Konfiguration

1. Vollständige **Erfassung aller Mailserver**:
    - Identifizieren Sie alle IP-Adressen und Domains, die E-Mails in Ihrem Namen versenden.
    - Drittanbieter wie Newsletter-Dienste oder CRM-Systeme sollten über DKIM angebunden werden.
    - Stellen Sie sicher, dass Ihr SPF-Eintrag schlank und präzise ist, um die E-Mail-Authentifizierung zu optimieren und die Sicherheit zu erhöhen. Fügen Sie nur die unbedingt notwendigen IP-Adressen und Server hinzu.
2. Wechsel zu **Hardfail**:
    - Wechseln Sie von Softfail (~all) zu Hardfail (-all), um maximalen Schutz zu gewährleisten.
3. Regelmäßige **Überprüfung und Aktualisierung**:
    - Etablieren Sie eine Sichtprüfung und ein Monitoring Ihrer SPF-Einträge.
    - Entfernen Sie veraltete oder unnötige Einträge regelmäßig.
    - Passen Sie die Konfiguration bei Änderungen in Ihrer E-Mail-Infrastruktur umgehend an.
4. **Vermeidung von vielen DNS-Lookups:**
    - Begrenzen Sie die Anzahl der DNS-Lookups auf eine geringe Zahl, um Probleme zu vermeiden. Eine tiefe Verschachtelung führt zum Versagen des SPF Mechanismus.
    - Nutzen Sie 'include:' Mechanismen effizient, um diese Grenze einzuhalten.

Monitoring und Fehleranalyse:

- Verwenden Sie DMARC-Reports, um ein Monitoring-System für SPF-Fehler zu implementieren.
- Analysieren Sie regelmäßig Fehlermeldungen, um Konfigurationsprobleme frühzeitig zu erkennen.

DMARC Implementierung

Die Implementierung von DMARC beginnt mit einer "None"-Policy (p=none) zur Beobachtung, gefolgt von einer schrittweisen Erhöhung über Quarantine bis hin zu Reject.

Für einen realistischen Zeitplan für den vollständigen Übergang zur Reject-Policy sollten 2-6 Monate eingeplant werden.

Implementierung von DMARC

Stufenweise Einführung

1. **Beginnen Sie mit einer „None"**-Policy (p=none) zur Beobachtung ohne aktive Filterung.
2. **Erhöhen Sie schrittweise** die Strenge: None → Quarantine → Reject.

Festlegung klarer Zeitpläne

1. Definieren Sie einen **realistischen Zeitplan** für die DMARC-Implementierung.
2. Planen Sie mindestens 2-6 Monate für den vollständigen Übergang zur Reject-Policy ein.

Gründliche Analyse der DMARC-Berichte

1. Richten Sie das Empfangen von **Aggregatberichten** ein.
2. Nutzen Sie **spezialisierte Tools** zur effizienten Auswertung der Berichte.

Abstimmung mit allen Stakeholdern:

1. Involvieren Sie frühzeitig **alle relevanten Abteilungen** (IT, Marketing, Kundenservice).
2. **Schulen Sie Mitarbeiter** im Umgang mit **DMARC** und möglichen Auswirkungen.

Implementierung von DKIM

1. Stellen Sie sicher, dass **DKIM parallel zu SPF** implementiert wird.
2. Konfigurieren Sie **DKIM für alle legitimen E-Mail-Quellen** Ihrer Domain.

Wählen Sie einen DMARC Reporting Service, der den österreichischen und EU-Datenschutzbestimmungen entspricht und prüfen Sie die Standorte der Rechenzentren sowie die Datenverarbeitungspraktiken.

DMARC Reporting Service wählen

Serviceangebot und Compliance

a. Stellen Sie sicher, dass der Provider den österreichischen und EU-Datenschutzbestimmungen entspricht.
b. Prüfen Sie die Standorte der Rechenzentren und die Datenverarbeitungspraktiken.

Leistungseffizienz

a. Vergleichen Sie die Preismodelle verschiedener Anbieter.
b. Berücksichtigen Sie sowohl direkte Kosten als auch potenzielle Einsparungen durch verbesserte Sicherheit.

Durch die Umsetzung dieser Best Practices und die sorgfältige Auswahl geeigneter Provider können österreichische Unternehmen ihre E-Mail-Sicherheit signifikant verbessern. Dies führt nicht nur zu einem besseren Schutz vor Cyber-Bedrohungen, sondern steigert auch die Zustellbarkeit und Vertrauenswürdigkeit ihrer E-Mail-Kommunikation.

Fortschritte und Ansätze

Trotz einer hohen SPF-Implementierungsrate bleibt die relativ geringe Nutzung der DMARC Reject-Policy ein Bereich mit erheblichem Verbesserungspotenzial, das durch gezielte Aufklärung und Unterstützung adressiert werden muss.

Ausblick und Perspektive

Der „E-Mail Security Report Austria" zeigt deutlich, dass österreichische Unternehmen bereits signifikante **Fortschritte in der Implementierung grundlegender E-Mail-Sicherheitsmechanismen** gemacht haben. Mit einer durchschnittlichen SPF-Implementierungsrate von 78,08% liegen österreichische Unternehmen im europäischen Vergleich gut positioniert.

Allerdings offenbart die relativ geringe Nutzung der **DMARC Reject-Policy** (durchschnittlich 3,15%) ein erhebliches Verbesserungspotenzial. Dies unterstreicht die Notwendigkeit weiterer Aufklärung und Unterstützung bei der Implementierung fortgeschrittener Sicherheitsmaßnahmen.

Regionale Unterschiede zwischen den Bundesländern bieten Möglichkeiten für Best-Practice-Sharing und gezielte Fördermaßnahmen. Insbesondere Vorarlberg zeigt mit der höchsten **DMARC Reject-Rate** eine relative Vorreiterrolle, von der andere Bundesländer lernen können.

Die dominante Stellung von großen internationalen Mailprovidern wie Microsoft 365 und Google Workspace neben starken lokalen Anbietern wie easyname.eu spiegelt die globalisierte Natur der E-Mail-Kommunikation wider. Gleichzeitig zeigt die Präsenz spezialisierter Dmarc Report Service ein wachsendes Bewusstsein für die Bedeutung professioneller E-Mail-Sicherheitslösungen.

Für die Zukunft ist es entscheidend, dass österreichische Unternehmen nicht nur in die Implementierung von **SPF, DKIM und DMARC** investieren, sondern auch proaktiv neue Technologien und Trends im Bereich der E-Mail-Sicherheit anwenden. Nur so kann Österreich seine Position als fortschrittlicher Standort für sichere digitale Kommunikation festigen und ausbauen.

Abschließend lässt sich sagen: Österreich ist auf einem guten Weg, steht aber vor der Herausforderung, die Lücke zwischen grundlegender und fortgeschrittener E-Mail-Sicherheit zu schließen. Mit gezielten Maßnahmen und einem starken Fokus auf kontinuierliche Verbesserung kann Österreich seine E-Mail-Sicherheitslandschaft weiter stärken und sich als Vorreiter in Europa positionieren.

Daten im Detail

Tabellarische Auflistung aller erhobenen Daten für jedes Bundesland folgen, einschließlich aller SPF- und DMARC-Statistiken sowie der vollständigen Liste der Mail- und DMARC-Provider.

E-Mail Security Übersicht

Name	Spf	Dmarc Reject	Dmarc Policy	E-Mail Provider #1	Dmarc Service #1	Domain Provider #1
Burgenland	75,51 %	2,42 %	6,04 %	Microsoft 365	Valimail	world4you.at
Kärnten	76,02 %	3,16 %	7,51 %	Microsoft 365	Valimail	a1.net
Niederösterreich	78,27 %	2,63 %	5,92 %	Microsoft 365	Valimail	world4you.at
Oberösterreich	80,37 %	2,96 %	7,02 %	Microsoft 365	Valimail	world4you.at
Salzburg	77,79 %	3,27 %	7,11 %	Microsoft 365	Valimail	world4you.at
Steiermark	78,99 %	2,83 %	6,09 %	Microsoft 365	brevo.com	a1.net
Tirol	79,11 %	2,8 %	6,54 %	Microsoft 365	Valimail	world4you.at
Vorarlberg	79,21 %	4,85 %	9,27 %	Microsoft 365	brevo.com	a1.net
Wien	77,41 %	3,46 %	7,69 %	Google Workspace	Valimail	world4you.at
Österreich	**78,08 %**	**3,15 %**	**7,02 %**	**Microsoft 365**	**Valimail**	**world4you.at**

SPF Status Übersicht

Name	Spf Softfail	Spf Hardfail	Spf
Burgenland	25,86 %	49,65 %	75,51 %
Kärnten	30,63 %	45,38 %	76,02 %
Niederösterreich	27,42 %	50,85 %	78,27 %
Oberösterreich	26,33 %	54,04 %	80,37 %
Salzburg	29,87 %	47,92 %	77,79 %
Steiermark	29,20 %	49,79 %	78,99 %
Tirol	32,62 %	46,48 %	79,11 %
Vorarlberg	29,97 %	49,25 %	79,21 %
Wien	28,54 %	48,87 %	77,41 %
Österreich	**28,94 %**	**49,14 %**	**78,08 %**

Daten im Detail

Tabellarische Auflistung aller erhobenen Daten für jedes Bundesland folgen, einschließlich aller SPF- und DMARC-Statistiken sowie der vollständigen Liste der Mail- und DMARC-Provider.

DMARC Status Übersicht

Name	Dmarc None	Dmarc Quarantine	Dmarc Reject	Dmarc Quarantine & Reject
Burgenland	28,78 %	3,62 %	2,42 %	6,04 %
Kärnten	21,35 %	4,35 %	3,16 %	7,51 %
Niederösterreich	27,49 %	3,29 %	2,63 %	5,92 %
Oberösterreich	28,51 %	4,06 %	2,96 %	7,02 %
Salzburg	25,29 %	3,85 %	3,27 %	7,11 %
Steiermark	25,25 %	3,26 %	2,83 %	6,09 %
Tirol	25,35 %	3,73 %	2,8 %	6,54 %
Vorarlberg	21,65 %	4,42 %	4,85 %	9,27 %
Wien	29,36 %	4,23 %	3,46 %	7,69 %
Österreich	**25,89 %**	**3,87 %**	**3,15 %**	**7,02 %**

E-Mail Provider Übersicht

Name	E-Mail Provider Verbreitung Platz 1	E-Mail Provider Verbreitung Platz 2	E-Mail Provider Verbreitung Platz 3
Burgenland	Microsoft 365	Google Workspace	easyname.eu
Kärnten	Microsoft 365	Google Workspace	a1.net
Niederösterreich	Microsoft 365	Google Workspace	easyname.eu
Oberösterreich	Microsoft 365	Google Workspace	easyname.eu
Salzburg	Microsoft 365	Google Workspace	ionos.de
Steiermark	Microsoft 365	Google Workspace	easyname.eu
Tirol	Microsoft 365	Google Workspace	agenturserver.de
Vorarlberg	Microsoft 365	Google Workspace	ionos.de
Wien	Google Workspace	Microsoft 365	easyname.eu
Österreich	**Microsoft 365**	**Google Workspace**	**easyname.eu**

Daten im Detail

Tabellarische Auflistung aller erhobenen Daten für jedes Bundesland folgen, einschließlich aller SPF- und DMARC-Statistiken sowie der vollständigen Liste der Mail- und DMARC-Provider.

DMARC Service Ranking

Name	Dmarc Service Verbreitung Platz 1	Dmarc Service Verbreitung Platz 2	Dmarc Service Verbreitung Platz 3
Burgenland	Valimail	brevo.com	agari.com
Kärnten	Valimail	brevo.com	proofpoint.com
Niederösterreich	Valimail	brevo.com	mailinblue.com
Oberösterreich	Valimail	brevo.com	proofpoint.com
Salzburg	Valimail	brevo.com	pinzweb.at
Steiermark	brevo.com	Valimail	proofpoint.com
Tirol	Valimail	ihc.at	proofpoint.com
Vorarlberg	brevo.com	Valimail	proofpoint.com
Wien	Valimail	brevo.com	proofpoint.com
Österreich	**Valimail**	**brevo.com**	**proofpoint.com**

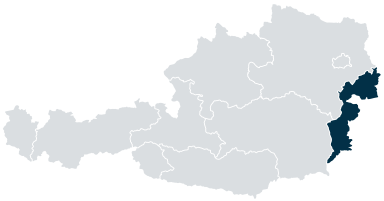
Domain Registrar Ranking

Name	Domain Provider #1	Domain Provider #2	Domain Provider #3
Burgenland	world4you.at	a1.net	easyname.eu
Kärnten	a1.net	world4you.at	domaincontrol.com
Niederösterreich	world4you.at	a1.net	easyname.eu
Oberösterreich	world4you.at	a1.net	domaintechnik.at
Salzburg	world4you.at	a1.net	domaintechnik.at
Steiermark	a1.net	world4you.at	easyname.eu
Tirol	world4you.at	a1.net	domaintechnik.at
Vorarlberg	a1.net	world4you.at	domaincontrol.com
Wien	world4you.at	easyname.eu	a1.net
Österreich	**world4you.at**	**a1.net**	**easyname.eu**

Bundesländer Analyse

Burgenland

- SPF: 79,50% (leicht unter dem Landesdurchschnitt)
- DMARC Reject: 2,12% (niedrigste Rate österreichweit)
- Top Mail Provider: Microsoft 365, Google Workspace, easyname.eu
- Top Dmarc Report Service: valimail.com, agar.com

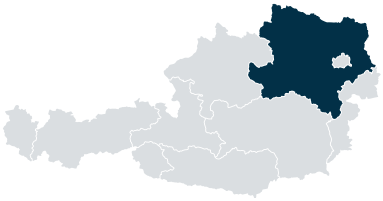


Kärnten

- SPF: 78,23% (niedrigste Rate österreichweit)
- DMARC Reject: 2,97% (im unteren Mittelfeld)
- Top Mail Provider: Microsoft 365, Google Workspace, al.net
- Top Dmarc Report Service: valimail.com, proofpoint.com

Niederösterreich

- SPF: 82,21% (über dem Landesdurchschnitt)
- DMARC Reject: 2,59% (im unteren Drittel)
- Top Mail Provider: Microsoft 365, Google Workspace, easyname.eu
- Top Dmarc Report Service: valimail.com, mailinblue.com



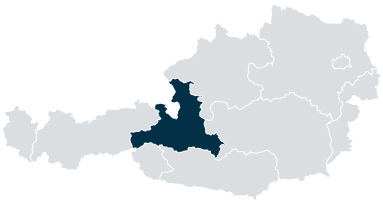
Oberösterreich

- SPF: 83,80% (höchste Rate österreichweit)
- DMARC Reject: 2,92% (im Mittelfeld)
- Top Mailprovider: Microsoft 365, Google Workspace, easyname.eu
- Top Dmarc Report Service: valimail.com, proofpoint.com

Bundesländer Analyse

Salzburg

- SPF: 81,19% (nahe am Landesdurchschnitt)
- DMARC Reject: 3,25% (im oberen Mittelfeld)
- Top Mail Provider: Microsoft 365, Google Workspace, ionos.de
- Top Dmarc Report Service: valimail.com, pinzweb.at

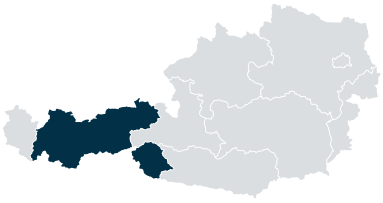


Steiermark

- SPF: 81,75% (leicht über dem Landesdurchschnitt)
- DMARC Reject: 3,73% (zweitbeste Rate österreichweit)
- Top Mail Provider: Microsoft 365, Google Workspace, easyname.eu
- Top Dmarc Report Service: valimail.com, proofpoint.com

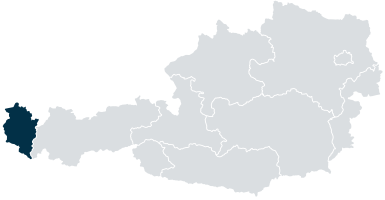
Tirol

- SPF: 82,23% (über dem Landesdurchschnitt)
- DMARC Reject: 2,70% (im unteren Mittelfeld)
- Top Mail Provider: Microsoft 365, Google Workspace, mynet.at
- Top Dmarc Report Service: valimail.com, ihc.at, proofpoint.com



Vorarlberg

- SPF: 81,81% (leicht über dem Landesdurchschnitt)
- DMARC Reject: 4,64% (höchste Rate österreichweit)
- Top Mail Provider: Microsoft 365, Google Workspace, ionos.de
- Top Dmarc Report Service: valimail.com, proofpoint.com



Bundesländer Analyse & Vergleich

Wien

- SPF: 80,22% (leicht unter dem Landesdurchschnitt)
- DMARC Reject: 3,31% (im oberen Drittel)
- Top Mail Provider: Google Workspace, Microsoft 365, easyname.eu
- Top Dmarc Report Service: valimail.com, proofpoint.com

SPF-Implementierung im Vergleich

- Spitzenreiter: Oberösterreich (83,80%)
- Schlusslicht: Kärnten (78,23%)
- Die Differenz von 5,57 Prozentpunkten zeigt regionale Unterschiede in der Adoptionsrate.
- Durchgehend hoher Implementierungsgrad in allen Bundesländern.

DMARC-Nutzung im Vergleich

- Spitzenreiter: Vorarlberg (4,64%)
- Schlusslicht: Burgenland (2,12%)
- Große Spannweite von 2,52 Prozentpunkten deutet auf unterschiedliche Prioritäten hin.
- Durchgehend niedriges Niveau der DMARC Reject-Policy-Nutzung in allen Bundesländern.

Regionale Unterschiede bei Mail Providern und DMARC Services:

Mail Provider:

- Microsoft 365 und Google Workspace dominieren in fast allen Bundesländern.
- Regionale Anbieter wie easyname.eu, al.net, und mynet.at zeigen lokale Stärken
- Wien ist das einziges Bundesland mit Google Workspace an erster Stelle.

DMARC Services

- valimail.com führt in den meisten Bundesländern.
- In der Analyse fiel auf, dass Marketing-Software-Anbieter wie „Brevo.com" vertreten ist. Dieser Anbieter stellt seinen Kunden jedoch keine Informationen aus den Berichten zur Verfügung. Möglicherweise waren den Unternehmen nicht bewusst, welche sensiblen Metadaten sie über ihren E-Mail-Verkehr an diesen Anbieter übermitteln.
- Regionale Unterschiede zeigen sich bei den drittplatzierten Anbietern.
- Proofpoint.com findet sich in mehreren Bundesländern unter den Top 3.

Diese Analyse zeigt sowohl landesweite Trends als auch regionale Besonderheiten in der E-Mail-Sicherheitslandschaft Österreichs. Sie bietet wertvolle Einblicke für gezielte Verbesserungsmaßnahmen und Best-Practice-Sharing zwischen den Bundesländern.

Fragen, Hinweise und Tipps?

Bei Fragen und für Tipps stehen wir Ihnen gerne zur Verfügung. Kontaktieren Sie uns per E-Mail unter hello@nager.software und telefonisch unter +43 677 613 855 12. Weitere Informationen finden Sie auf https://mailtower.app

Anhang

Glossar

- **SPF (Sender Policy Framework):** Protokoll zur Verifizierung der Absenderadresse einer E-Mail.
- **DKIM (DomainKeys Identified Mail):** Verfahren zur digitalen Signierung von E-Mails.
- **DMARC (Domain-based Message Authentication, Reporting & Conformance):** Rahmenwerk zur Kombination von SPF und DKIM mit Berichterstattung.
- **Softfail:** Weniger strikte SPF-Konfiguration, bei der verdächtige E-Mails markiert, aber nicht automatisch abgelehnt werden.
- **Hardfail:** Strikte SPF-Konfiguration, bei der nicht autorisierte E-Mails abgelehnt werden.
- **Phishing:** Versuch, über gefälschte E-Mails an sensible Daten zu gelangen.
- **DNS (Domain Name System):** System zur Namensauflösung im Internet.

Impressum

Mailtower.app c/o Tino Hager
Hintere Achmühlerstraße 1a
6850 Dornbirn
Austria

Unternehmensgegenstand
Softwareentwicklung und IT-Dienstleistungen

Kontakt
E-Mail: hello@nager.software
Telefon: +43 677 613 855 12
Webseite: nager.software

Umsatzsteuer-Id
UID-Nummer: ATU79348779

MAILTOWER

Austria E-Mail Security Report™

Analyse der österreichischen E-Mail-Sicherheitslandschaft

JULI 2024