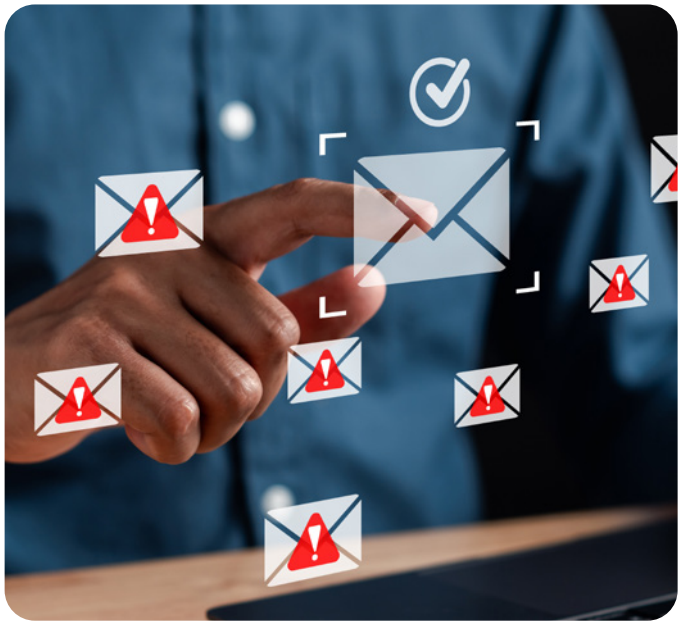
# Mails sicher zustellen

## plus Markenschutz und Vertrauenssicherung

CAIRO

secure • digital • IT-infrastructures

In einer zunehmend digitalen und vernetzten Welt ist es wichtiger denn je, E-Mails sicher und zuverlässig zu versenden und zu empfangen. Die E-Mail-Kommunikation, einst als einfach angesehen, stellt heute eine echte Herausforderung dar, besonders im professionellen Umfeld mit vielen verschiedenen Domänen, Diensten und leider auch einem Missbrauch der Mail-Domänen.



Um sicherzustellen, dass E-Mails nur durch die Originalfirma versendet werden und korrekt zugestellt & nicht fälschlicherweise durch Mail-Server abgelehnt oder als Spam markiert werden, ist es wichtig, alle neuen Praktiken und Sicherheitsstandards wie SPF, DKIM, DMARC und BIMI zu befolgen. Erfolgt dies nicht, kann es sogar zu Umsatzverlusten im B2C/B2B-Bereich führen, wenn Marketing-E-Mails nicht den gewünschten Empfänger erreichen. Im B2B-Bereich ist es zudem entscheidend, den Mail-Missbrauch mit großem Schaden für die Marke zu vermeiden und solche Mails und Mail-Wege von den legitimen E-Mails aus der eigenen Organisation zu unterscheiden.

Ohne den Einsatz von professionellen Werkzeugen ist die Organisation „blind“ hinsichtlich der Nutzung und des Versandes von Emails.

Einen neuen Fokus bekommt das Thema auch durch die Einführung der e-Rechnung, in der die Rechnung in Form von digitalen Inhalten per Mail versendet wird.

## Die vier Säulen des sicheren und verlässlichen E-Mail-Verkehrs

Hier kommen die vier grundlegenden Technologien ins Spiel, die den Schutz und die Verlässlichkeit Ihrer E-Mail-Kommunikation gewährleisten: **SPF, DKIM, DMARC** und **BIMI**.
Darüber hinaus sorgen MTA-STS und andere Sicherheitsprotokolle für zusätzlichen Schutz. Gemeinsam bieten diese Technologien eine robuste Lösung für Ihre E-Mail-Authentifizierung und verhindern, dass Ihre Domäne missbraucht wird, E-Mails in die falschen Hände geraten oder den Empfänger nicht erreichen.

### 1) SPF (Sender Policy Framework)

SPF stellt sicher, dass nur **autorisierte Server E-Mails** im Namen Ihrer Domain senden dürfen. Dies schützt vor Missbrauch und stellt sicher, dass E-Mails nur von vertrauenswürdigen Quellen kommen. Wenn eine E-Mail von einem unberechtigten Server gesendet wird, wird sie abgelehnt – eine erste Verteidigungslinie gegen Phishing und Spam, die für eine zuverlässige Zustellung sorgt. Eine einmalige Einstellung der SPF-Settings ist aber nicht ausreichend - vielmehr muss diese ständig kontrolliert werden.

### 2) DKIM (DomainKeys Identified Mail)

DKIM fügt jeder E-Mail **eine digitale Signatur** hinzu, die vom Empfänger überprüft werden kann, um sicherzustellen, dass der Inhalt der Nachricht unverändert ist und wirklich vom angegebenen Absender stammt. Dies sorgt nicht nur für zusätzliche Sicherheit, sondern gewährleistet auch, dass die E-Mail wie beabsichtigt beim Empfänger ankommt.

### 3) DMARC (Domain-based Message Authentication, Reporting and Conformance)

DMARC geht noch einen Schritt weiter, indem es eine klare Richtlinie für den **Umgang** mit E-Mails vorgibt, die entweder die SPF- oder die DKIM-Prüfung nicht bestehen. Der Absender kann festlegen, wie der Empfänger mit nicht authentifizierten E-Mails verfahren soll: Soll die E-Mail abgelehnt, in Quarantäne gestellt oder einfach akzeptiert werden? DMARC sorgt so für eine konsequente und zuverlässige E-Mail-Zustellung.

### 4) BIMI (Brand Indicator for Message Identification)

Mit BIMI können Sie Ihr Firmenlogo in E-Mails sichtbar machen, sodass Ihre Marke nicht nur durch die E-Mail-Adresse, sondern auch durch das visuelle Branding sofort erkennbar ist. Dies stärkt das Vertrauen der Empfänger und sorgt für eine verbesserte Markenpräsenz in der digitalen Kommunikation.

## Zusätzlicher Schutz durch MTA-STS

MTA-STS stellt sicher, dass E-Mails über sichere Verbindungen gesendet werden. Es erzwingt die Verwendung von TLS (Transport Layer Security), um die Daten vor unbefugtem Zugriff während des Transports zu schützen. Dies sorgt dafür, dass Ihre Kommunikation nicht nur authentifiziert und sicher, sondern auch zuverlässig bleibt.

## CAIRO & Sendmarc

Eine umfassende und einmalige Konfiguration des eigenen Mail-Server hinsichtlich aller Parameter ist notwendig, aber nicht hinreichend. Vielmehr entstehen oft neue Domänen und neue Adressaten mit neuen Mail-Servern. Daher ist eine 7x24 Dauermonitoring-Lösung wie Sendmarc inkl. DMARC Reporting, Blacklist Monitoring, Changelog für Parameter uvm. entscheidend, um Missbrauch und erfolgreiche Zustellung zu kontrollieren.

Ob Sie wissen möchten, wer im Namen Ihrer Domain E-Mails versendet (Programme, Geräte, Fremde Firmen), Ihre IT-Sicherheit durch gezielte Optimierung gegen Phishing verbessern oder sicherstellen wollen, dass alle transaktionalen E-Mails im B2C/B2B immer zugestellt werden – CAIRO hilft Ihnen weiter.

Wir bieten Beratung, & Implementierung von Sendmarc als professionelles Mail-Monitoring Produkt und damit eine datenschutzkonforme & günstige Lösung, die in Europa betrieben und von uns verwaltet wird. Bei Missbrauch liegen genug Informationen vor, um auch mit den Behörden die entsprechenden Maßnahmen zu starten.

**Kontaktieren Sie uns, um mehr zu erfahren!**

**Unser Beratungsportfolio deckt alle Aspekte moderner IT-Infrastrukturen ab, von Mail-Systemen über Security- und Compliance-Prüfungen bis hin zu Schwachstellenmanagement, Security Awareness Trainings und dem sicheren IT-Betrieb.**

**CAIRO ist nach VdS 10000 zertifiziert und bietet ein Informationssicherheits-Management-System (ISMS) auf höchstem Niveau.**

CAIRO
secure · digital · IT-infrastructures

Tel.: +49 (0)621 86 75 10 Mail: info@cairo.ag Web: www.cairo.ag