



HORNETSECURITY

FACT SHEET



**SCHÜTZEN SIE IHRE MARKE VOR E-MAIL-IDENTITÄTSDIEBSTAHL, PHISHING UND SPOOFING, INDEM SIE IHRE DOMAINS MIT INTUITIVEM DMARC-, DKIM- UND SPF-MANAGEMENT SICHERN.**

DomainKeys Identified Mail

Sender Policy Framework

Domain-based Message Authentication, Reporting and Conformance



DKIM



SPF



DMARC

DKIM signiert Ihre E-Mail digital, damit Empfänger wissen, dass die E-Mail wirklich von Ihnen stammt und nicht verändert wurde.

SPF stellt sicher, dass nur die von Ihrer Domain autorisierten Server E-Mails in Ihrem Namen versenden dürfen.

DMARC sorgt für einen sauberen Posteingang und definiert, wie mit verdächtigen E-Mails umgegangen wird.

Die Verwaltung der E-Mail-Authentifizierung stellt viele Unternehmen vor erhebliche Herausforderungen. Das Einrichten und Verwalten sicherer DMARC-, DKIM- und SPF-Richtlinien ist besonders für Unternehmen mit mehreren Domains komplex und zeitaufwendig. Ohne funktionierende DMARC-Einstellungen setzen Unternehmen ihren Ruf als vertrauenswürdige Absender aufs Spiel und sind anfällig für E-Mail-Identitätsdiebstahl.

Zusätzlich erschwert die Einhaltung der strengen Anforderungen von E-Mail-Anbietern die Situation. Unternehmen kämpfen oft mit mangelnder Transparenz bei E-Mail-Kampagnen und verdeckten E-Mail-Aktivitäten innerhalb ihrer Organisation. Das Ziel, dass E-Mails im Posteingang der Kunden und nicht im Spam-Ordner landen, ist ohne angemessene E-Mail-Sicherheitsmaßnahmen kaum zu erreichen.

## MEISTERN SIE SPIELEND LEICHT DMARC, DKIM UND SPF UND SCHÜTZEN SIE DEN RUF IHRER MARKE

Was ist betroffen?

Wie hilft Ihnen DMARC Manager?

Was verbessert sich?



E-Mail Kommunikation



Compliance sicherstellen

Müheleise Einrichtung und Pflege von DMARC-, DKIM- und SPF-Best-Practice-Richtlinien



Einfaches Verwalten von DNS

Fügen Sie DNS-Einträge nahtlos hinzu und ändern Sie sie innerhalb weniger Sekunden



Verhindern von Identitätsdiebstahl

Gewinnen Sie einen umfassenden Überblick über die Quellen, die E-Mails über Ihre Domains versenden



Durch die Einhaltung von Authentifizierungsstandards wird eine sichere E-Mail-Zustellung gewährleistet und zugleich die Markenreputation geschützt.



HORNETSECURITY

FACT  
SHEET

## FUNKTIONEN

**Domain-Konfigurator:** Dieses Tool bietet Ihnen eine benutzerfreundliche Oberfläche zur Einrichtung und Pflege von DMARC-, DKIM- und SPF-Best-Practice-Richtlinien sowie TLS-Einstellungen für mehrere Domains. Mit dem DMARC Manager können Sie Ihre SPF- und DMARC-Einträge mühelos verwalten und DNS-Änderungen in Sekundenschnelle umsetzen.

**Status-Dashboard:** Das Dashboard bietet Ihnen eine umfassende Übersicht mit verschiedenen Statistiken. Dazu gehören die verwalteten Domains, die Anzahl der autorisierten und nicht autorisierten Absender, das Volumen der versendeten autorisierten und nicht autorisierten E-Mails sowie die Anzahl der E-Mails, die die DMARC-Prüfung bestanden oder nicht bestanden haben.

**E-Mail-Quellenanalyse:** Diese Funktion bietet Ihnen einen umfassenden Überblick über die Quellen, die E-Mails über Ihre Domains versenden. Sie gibt Auskunft über E-Mail-Volumen, Authentifizierungsstatus (DMARC-Prüfung bestanden/nicht bestanden), Kategorisierung der Quellen (autorisiert oder nicht autorisiert), Zustellbarkeit, Absenderreputation und Bedrohungsgrad.

**BIMI E-Mail Branding:** Sobald Ihre Domain DMARC-konform ist, können Sie die BIMI-Funktion nutzen. Diese ermöglicht es Ihnen, Ihr Logo in unterstützten Posteingängen neben Ihren E-Mails anzuzeigen. Dadurch steigern Sie die Wirkung Ihrer E-Mails, erhöhen den Wiedererkennungswert Ihrer Marke und maximieren das Vertrauen Ihrer Empfänger.

**SMTP-TLS Verschlüsselung:** Stellen Sie sicher, dass ausgehende E-Mails mit SMTP-TLS-Verschlüsselung sicher übertragen werden. Sie erhalten detaillierte Berichte über E-Mails, die nicht verschlüsselt wurden und nicht zugestellt werden konnten, was eine weitere Sicherheitsstufe in Ihrer E-Mail-Kommunikation darstellt.

**Fehlerberichte und Warnungen:** Fehlerberichte liefern detaillierte Echtzeitdaten zu E-Mails, die die DMARC-Prüfungen nicht bestanden haben. So können Sie nachvollziehen, wer E-Mails im Namen Ihrer Domains versendet und warum bestimmte E-Mails nicht zugestellt werden. Richten Sie individuelle Warnungen ein und erhalten Sie Benachrichtigungen an die angegebene E-Mail-Adresse, um schneller auf Bedrohungen reagieren zu können.