HORNETSECURITY

DMARC MANAGER

DIE LÖSUNG GEGEN E-MAIL-SPOOFING

Vertrauen bildet das Fundament jeder geschäftlichen E-Mail-Kommunikation. Doch Cyberkriminelle missbrauchen dieses Vertrauen, indem sie sich per E-Mail-Spoofing als bekannte Domains oder Personen ausgeben, um Betrugsversuche zu starten. Dies führt oft zu sogenannten BEC-Angriffen (Business Email Compromise), die Unternehmen teuer zu stehen kommen können.

DIE AUSWIRKUNGEN VON E-MAIL-SPOOFING:

» **Finanzieller Verlust** durch betrügerische E-Mails (z. B. gefälschte Rechnungen).
» **Rufschädigung durch Identitätsdiebstahl,** was zum Verlust des Vertrauens von Kunden und Partnern führt.
» **Erhöhtes Risiko von Phishing-Angriffen,** bei denen sensible Unternehmensdaten preisgegeben werden.

DMARC: IHRE VERTEIDIGUNG GEGEN E-MAIL-SPOOFING

DMARC (Domain-based Message Authentication, Reporting & Conformance) ist ein leistungsfähiges E-Mail-Authentifizierungsprotokoll, das Unternehmen hilft, E-Mail-Spoofing zu verhindern. Es arbeitet mit SPF und DKIM zusammen, um sicherzustellen, dass nur autorisierte E-Mails von Ihrer Domain aus gesendet werden, und schützt so Ihre Marke und Ihre Kommunikationskanäle.

WIE ES FUNKTIONIERT:

SPF prüft den SPF-Eintrag des sendenden Servers, um sicherzustellen, dass die E-Mail von einer autorisierten IP-Adresse gesendet wurde. Wenn die IP-Adresse im SPF-Datensatz aufgeführt ist, wird die Prüfung bestanden, andernfalls schlägt sie fehl.

DKIM prüft, ob die E-Mail mit dem privaten Schlüssel der sendenden Domain kryptografisch signiert ist, und gleicht sie dann mit dem entsprechenden öffentlichen Schlüssel ab. Eine positive Übereinstimmung führt zu einer bestandenen Prüfung, andernfalls schlägt sie fehl.

DMARC prüft, ob die „Absender"-Adresse in der E-Mail zur selben E-Mail-Domain gehört, die SPF und DKIM in ihren eigenen Prüfungen validiert haben.

Schließlich teilt das **Policy-Tag** ("p") ") im DMARC-Eintrag der sendenden Domain dem empfangenden Server mit, wie er die E-Mail aufgrund der Prüfergebnisse behandeln soll.

HORNETSECURITY

Das Einrichten und Verwalten von DMARC-, DKIM- und SPF-Richtlinien kann zu Konfigurationsproblemen führen, vor allem, wenn Sie diese für große und komplexe Organisationen verwalten, die viele Domains, mehrere Konfigurationen und möglicherweise unterschiedliche Anforderungen pro Domain verwalten.

Aber es gibt eine Lösung.

VERHINDERN SIE DMARC-KONFIGURATIONSPROBLEME MIT DEM **DMARC MANAGER**

MIT DEM DMARC MANAGER:

» Behalten Sie den Überblick darüber, wer E-Mails im Namen Ihrer Domain versendet, und geben Sie die Kont rolle zurück an den Domaininhaber – für eine stärkere und sicherere Markenreputation.

» Können Sie ganz einfach **DMARC-, DKIM-** und **SPF-**Best-Practice-Richtlinien für mehrere Domains einrich ten und verwalten.

» Erhalten Sie Einblicke in den E-Mail-Zustellungs- und Authentifizierungsstatus und können so legitime Kampagnen und potenzielle Spoofing-Versuche erkennen.

» Verbessern Sie Ihre E-Mail-Marketingstrategien, indem Sie sicherstellen, dass Massen-E-Mails zugestellt werden, indem Sie die von großen E-Mail-Anbietern wie Yahoo und Gmail geforderten Authentifizierungs standards einhalten.

» Stärken Sie Ihre Compliance mit branchenweiten/globalen Vorschriften wie DSGVO, PCI-DSS, NIST, HIPPA und anderen.

MEHR ERFAHREN

EMAIL: info@hornetsecurity.com | www.hornetsecurity.com