DMARC

DMARC (Domain-based Message Authentication, Reporting, and Conformance) verwendet SPF (Sender Policy Framework) und DKIM (DomainKeys Identified Mail) zum Authentifizieren von E-Mail-Absendern und um sicherzustellen, dass Ziel-E-Mail-Systeme die von Ihrer Domäne gesendeten E-Mail-Nachrichten als vertrauenswürdig einstufen. Die Implementierung von DMARC zusammen mit SPF und DKIM bietet zusätzlichen Schutz vor Spoofing- und Phishing-E-Mails.

DMARC bedient sich hierzu, wie auch SPF und DKIM, der TXT-Records des Domain Name Systems (DNS)

DMARC erstellen und prüfen

Zusätzlich zu den SPF- und DKIM-Einträgen im DNS (Domain Name System) wird ein weiterer RR-Eintrag (Resource Record) angelegt. Um einen SPF Eintrag zu erstellen, können Sie als Beispiel einen der vielen Generatoren verwenden, die Online zur Verfügung stehen. Zum Überprüfen kann man auch auf diverse Web-Tools zurückgreifen, wie beispielsweise: MX Toolbox

Info

Der DMARC-Record lässt sich, wie andere RR-Einträge auch, auf der Kommandozeile mit dem Befehl `host` oder `dig` abfragen.

Der Aufbau:

```
v=DMARC1;p=quarantine;pct=100;rua=mailto:postmaster@example.org;
ruf=mailto:forensik@example.org;adkim=s;aspf=r
```

Abkürzung	Bedeutung
v	Protokollversion
pct	Prozentualer Anteil der zu filternden Mails
ruf	Forensischer Report wird versandt an:
rua	Aggregierter Report wird versandt an:
p	Anweisung, wie mit Mails der Hauptdomäne zu verfahren ist.
sp	Anweisung, wie mit Mails der Subdomäne zu verfahren ist.
adkim	Abgleichmodus für DKIM
aspf	Abgleichmodus für SPF

Besondere Bedeutung haben die Abgleichmodi. Für SPF fordert die Spezifikation, dass erstens die Überprüfung positiv ausfällt und zweitens die From: Kopfzeile der Mail dieselbe Domäne aufweist, wie im SPF-Record hinterlegt. Für DKIM wird gefordert, dass die Signatur gültig ist und zusätzlich die dort genannte Domäne dieselbe ist, wie in der From: Kopfzeile der Mail. Als Abgleichmodi sind s='strict' bzw. r='relaxed' vorgesehen. Bei 'strict' müssen die Domänen exakt übereinstimmen, bei 'relaxed' darf die From: Kopfzeile auch eine Subdomäne enthalten. Über die Auswertung erhält der Sender einen täglichen Report an die genannte Adresse.

Die Policy (hier abgekürzt als 'p' bzw. 'sp' für Subdomains) legt schließlich fest, wie der Empfänger mit der Mail verfahren soll, wenn die Überprüfung scheitert. Vorgesehene Modi hierfür sind 'none', 'quarantine' und 'reject'. 'none' (auch als Monitormodus bezeichnet) wird in der Regel zum Testen verwendet und macht dem Empfänger keine Vorschriften über die Verfahrensweise. 'quarantine' verlangt die Kennzeichnung der Mails als Spam, 'reject' verlangt, die Mail zu verwerfen.

Die DMARC-Spezifikation entstand unter anderem auf Initiative von Google, Yahoo, Microsoft, Facebook, AOL, PayPal und LinkedIn.