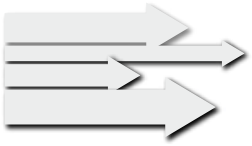
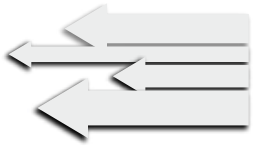
Sichere E-Mail

Was Sie über DMARC wissen sollten

eco Guide zu Domain-based Message Authenticatioon, Reporting and Conformance



DMARC



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

ist ein Internetstandard zur E-Mail-Authentifizierung, welcher

- legitime E-Mail einer Senderdomain mit Hilfe der Internetstandards SPF und / oder DKIM authentifiziert
- einer empfangenden Mailplattform mitteilt, wie mit Nachrichten verfahren werden soll, welche nicht authentifiziert werden konnten
- der empfangenden Mailplattform Ziele nennt an welche diese Reporte über erfolgreiche wie nicht erfolgreiche Authentifizierungen senden kann, damit die Besitzer der Senderdomain erfahren können ob möglichweise nicht autorisierte System versuchen, im Namen der Senderdomain Nachrichten in dem Umlauf zu bringen.

DMARC wurde erstmalig im März 2015 in RFC 7489 spezifiziert.

Wie funktioniert DMARC?

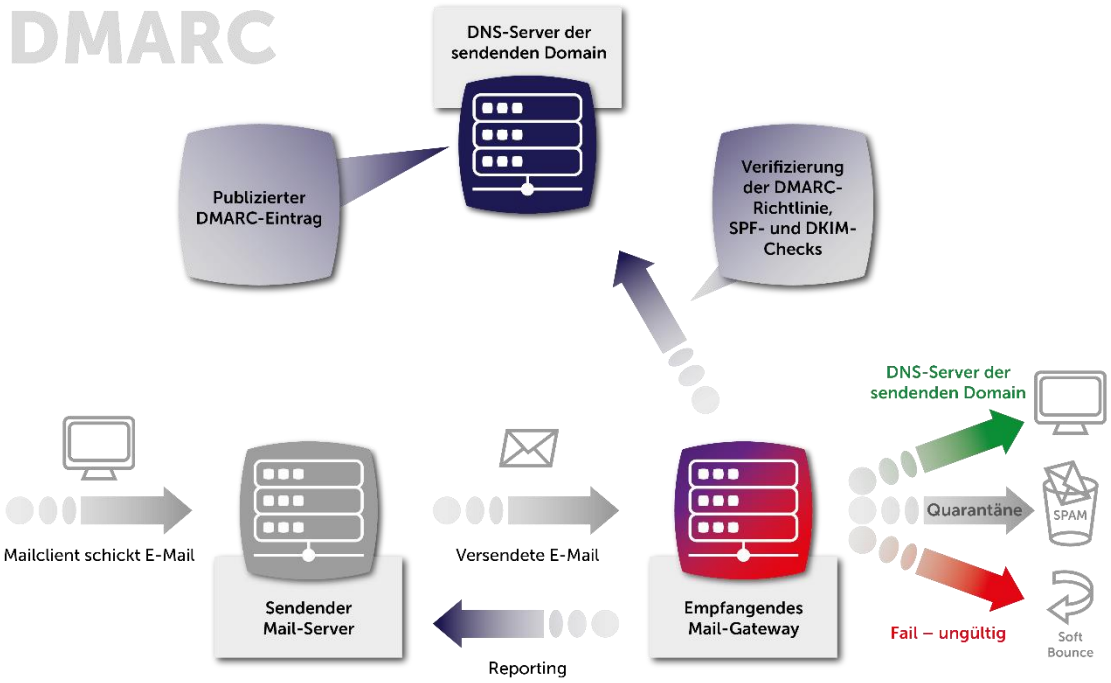
DMARC ist ein Verfahren, welches eine DMARC-Richtlinie (engl. Policy) als TXT-Record in der DNS-Zone einer Senderdomain im Internet veröffentlicht. Diese Richtlinie kann von empfangenden Mailplattformen abgerufen, ausgewertet und auf Nachrichten, welche gerade von einem sendenden Mailsystem an die empfangende Mailplattform herangetragen werden, angewendet werden.

Eine DMARC-Policy gibt einem empfangendem Mailsystem im Wesentlichen Antwort auf folgende drei Fragen:

- Kann die Nachricht, unter Einsatz der Technologien SPF und / oder DKIM, der Senderdomain zugeordnet werden?
- Was soll geschehen, wenn eine Zuordnung nicht möglich ist?
- Wer soll Berichte bei Erfolg und / oder Scheitern eine Zuordnung erhalten?

Darüber hinaus kann eine DMARC-Richtlinie noch weitere Angaben enthalten, welche bestimmte Aspekt der Policy noch detaillierter regeln.

DMARC



DMARC einrichten

Eine DMARC-Policy muss in einer bereits für E-Mail genutzten Domain im Rahmen eines sogenannten Staging stufenweise eingeführt werden, bis sie letztendlich ihre volle Schutzfunktion entfalten kann. Wird die volle Schutzfunktion sofort aktiviert, besteht die Gefahr legitime Nachrichten zu verlieren, weil diese möglicherweise von legitimen, aber noch nicht legitimierten Systemen versendet werden soll, aber aufgrund noch nicht erfolgter Legitimierung zurückgewiesen wird.

DMARC-Staging

Aufgabe des Staging ist, noch nicht legitimierte Systeme durch Sichtung von DMARC-Reports zu identifizieren und diese mit Hilfe von SPF und / oder DKIM zu legitimieren, so dass am Ende des Staging nur noch Systeme als illegitim in Berichten auftauchen, welche die Senderdomain missbräuchlich nutzen. Im Rahmen eines DMARC-Staging wird die sogenannte DMARC-Policy von anfänglich none stufenweise über quarantine auf bis zu reject angehoben. Ist das reject-Level erreicht, bietet DMARC die gewünschte Schutzfunktion (siehe auch:).

DMARC-Eintrag veröffentlichen

Ein DMARC-Eintrag ist ein DNS TXT-Record, welcher in der DNS-Zone einer Senderdomain veröffentlicht wird. Der Eintrag besitzt ein vorgegebenes DNS-Label, d. h. er muss in der DNS-Zone unter dem Namen _dmarc abgelegt werden. In der Domain example.com muss der DMARC-Record also als TXT-Record _dmarc.example.com veröffentlicht werden.

Für die Subdomain invoice der Domain example.com muss der TXT-Record als _dmarc.invoice.example.com veröffentlicht werden, wenn er von der Policy in der übergeordneten Zone example.com abweichen soll. Veröffentlicht invoice.example.com keine eigene DMARC-Policy wird ein empfangendes System selbstständig nach einer DMARC-Policy in der übergeordneten DNS-Zone suchen und diese anwenden.

Policy-Level

DMARC sieht drei unterschiedliche, sich wechselseitig ausschließende Policy-Level vor, mit denen eine Senderdomain einem empfangendem Mailsystem mitteilen kann wie es mit Nachrichten umgehen soll, welche weder durch SPF legitimiert noch durch DKIM verifiziert werden konnten.

- **None**
  Das empfangende System soll nichts unternehmen. Dieses Level schützt nicht, aber versetzt die Betreiber einer Senderdomain in die Lage, DMARC-Berichte zu erhalten und diese auszuwerten, ohne dass dabei legitime E-Mails abgelehnt werden.
- **quarantine**
  Das empfangende Mailsystem soll E-Mails, welche die Authentifizierung nicht bestehen, annehmen, aber nicht in die INBOX zustellen, sondern z. B. in den Spam-Ordner.
- **reject**
  Das empfangende Mailsystem soll E-Mails, welche die Authentifizierung nicht bestehen, nicht annehmen, sondern den Empfang ablehnen.

Aufbau eines DMARC-Eintrags

Ein TXT-Record mit einer DMARC-Richtlinie muss mindestens die folgenden Kriterien erfüllen:

- in der DNS-Zone darf nur eine einzige DMARC-Richtlinie vorhanden sein. Sind mehrere TXT-Records mit DMARC-Angaben vorhanden werden alle ignoriert, weil nicht ersichtlich ist, welche der Angaben befolgt werden soll
- der TXT-Record muss mit der Angabe v=DMARC1; beginnen oder er wird ignoriert
- der TXT-Record muss ein Policy-Level – none, quarantine oder reject – nennen

Ein TXT-Record mit einer DMARC-Richtlinie sollte zusätzlich die folgende Angabe führen:

Eine rua-Report-Adresse an welche empfangende Systeme DMARC-Reports senden können, welche ausgewertet und auf möglichen Missbrauch der Senderdomain überprüft werden können. Veröffentlichen Sie als Erstes einen Text (TXT)-Eintrag in Ihrem DNS wie beispielsweise diesen:

```
”v=DMARC1; p=none; rua=dmarc-reports@example.com;”
```

Wenn sie sich. z. B. im Rahmen eines DMARC-Stagings, sicher sind, keine legitime Mail zu verlieren, erhöhen sie das Schutzlevel zunächst auf quarantine und später dann auf reject, indem sie den bestehenden TXT-Record aktualisieren:

```
"v=DMARC1; p=quarantine; rua=dmarc-reports@example.com;"
```

Achtung! Fügen sie ihrer DMARC-Policy keine ruf-Angaben hinzu, denn dann erhalten sie sogenannte forensische DMARC-Reports. Diese sind im Inhalt wesentlich umfangreicher als solche, welche mit einer rua-Adresse angefordert werden. Sie enthalten dann personenbezogene Angaben, welche mit der DSGVO nicht vereinbar sind (siehe auch: eco-Gutachten zur Vereinbarkeit von DMARC mit der DSGVO und anderen Rechtsvorschriften).

Weitere Informationen bezüglich des Zusammenspiels von DMARC, DKIM und SPF finden Sie in den Dokumenten der Kompetenzgruppe-E-Mail in unserem Downloadbereich auf https://www.eco.de

Kontakt:
Michael Weirich
Projekt Manager IT-Sicherheit
eco – Verband der Internetwirtschaft e. V.

Mobil: +49(0)171 – 554 0303
E-Mail: michael.weirich@eco.de
Web: https://www.eco.de/