

DMARC Einführung

Einführung

- 1. MX
- 2. SPF
- 3. DKIM
- 4. DMARC

1. MX

- MX steht für den „Mail Exchanger“
Der Mailserver, der Mails für die Domäne entgegen nimmt.
- im DNS ein eigener Record für jeden Server

2.1. SPF

- Sender Policy Framework
bestimmt welche Server Mails senden dürfen
- Kein eigener Typ im DNS
es wird ein TXT Record verwendet.
- Beispiel:
„v=spf1 mx a:www.example.com -all“

2.2. SPF

- Probleme bei Mailinglisten
- Probleme bei automatischen Weiterleitungen.

3. DKIM

- DomainKeys Identified Mail
Jede Mail wird vom Server signiert
- Public Key muss im DNS eingetragen werden.
- Beispiel:
M20221114._domainkey.lug-kassel.de. TXT ("v=DKIM1;
k=rsa; "
"p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCxO
2fwXjHCVILr3HBiehdjx5TloVtUS6ksl0PcCt6HGmuDrl+izdBwb
DwZknPnBTFqb8Vvl99JPVQ0tFe9Yy2VIFGDRphaxUgCBisEC
c52H+Yqv87Cd+J963WxZfrmG0XWqWtETRcgadb6E8TBC7QI
T1JecEJWljDbILvFuwb28QIDAQAB")

4.1. DMARC

- Domain-based Message Authentication, Reporting and Conformance
- Berichte über zugestellte und abgewiesene Mails
- Kontrolle von DKIM und SPF
- Fragen zu Datenschutz

4.2. DMARC

- TXT Record im DNS
- Beispiel:
_dmarc.lug-kassel.de. TXT "v=DMARC1;
p=reject; rua=mailto:dmarc@dinoex.de;
ruf=mailto:dmarc@dinoex.de; fo=1;"

4.3. DMARC Reports

- Daten als MIME Attachment
- Formate: Textfile, XML Datei, komprimierte XML Datei, ZIP-Archiv mit XML-Datei
- Software für Auswertung erforderlich
IMAP → RIPMIME → unzip → XML Parser → CSV Datei
- Web-Interface zur Anzeige der Daten

Quellen

- github.com/dinoex/dmarc_view
- github.com/dinoex/dmarc_report
- codeberg.org/dinoex/dmarc_view
- codeberg.org/dinoex/dmarc_report