DMARC

PATRICK BEN KOETTER <P@SYS4.DE>

2022-08-30

What is DMARC?

- Abbreviation for Domain-based Message Authentication, Reporting, and Conformance
- IETF Standard RFC 7489
- A DNS-based mechanism to filter and report by senderdomain
- A sender-side email policy mechanism

How does DMARC work?

- Senderdomain uses DNS to publish a DMARC policy
- Receiving platform checks for DMARC policy
  - Checks in (Sub)domain
  - Checks in organizational domain

- Receiving platform checks for SPF
- Receiving platform checks for DKIM
- Receiving platform checks for local override
- Receiving platform acts out DMARC policy
- Receiving platform sends DMARC report

What problems does DMARC create?

- DMARC solved the problems of those who invented it
- DMARC solves works for main email use cases, but not for all
- It has become industry standard
- It has a long history of trying to make it an IETF standard
- DMARC breaks forwarding

Writing DMARC-Policies

switch.ch DMARC policy

```
$ dig +short TXT _dmarc.switch.ch
"v=DMARC1; p=none; rua=mailto:dmarc-rua@switch.ch;
ruf=mailto:dmarc-ruf@switch.ch; fo=1; adkim=r; aspf=r"
```

DMARC-Vocabulary

- `v`
- `p`
- `rua`, `ruf`
- `adkim`, `aspf`
- alignment

Version

- A valid DMARC record MUST contain a version statement
- The version statement MUST be the first entry in the TXT record
- The only valid version statement today is `v=DMARC1`

Policy

- DMARC knows three policies:
  - `none`
  - `quarantine`
  - `reject`
- Only `quarantine` or `reject` protect receivers!

Reports

DMARC knows two report types:

`rua`
: general data, aggregated, daily

`ruf`
: all data incl. message, per incident, continuously

- Only `mailto` will survive as report channel

Identifier Alignment mode

DMARC allows to specify how strict or relaxed alignment must be treated:

`adkim` (default: relaxed)
: Indicates whether strict or relaxed DKIM Identifier Alignment mode is required by the Domain Owner.

`aspf` (default: relaxed)
: Indicates whether strict or relaxed SPF Identifier Alignment mode is required by the Domain Owner.

Identifier Alignment

- This is the DMARC key feature!
- envelope-sender and RFC2821-From:-Header are in no logical relationship
- DMARC relates them and expects alignment (DMARC Alignment)

DMARC-Design

Staging!

1. Publish an `~all` SPF-Policy
2. Start to DKIM-sign outbound messages
3. Publish a policy `none` DMARC-Policy **and** request reports using `rua`
4. Monitor reports
5. Send reports (Email Authentication für Empfänger)
6. Fix your own problems
7. Upgrade DMARC-Policy to `quarantine` or `reject`

When to use rua- / ruf-reports?

- Gutachten zur Vereinbarkeit von DMARC mit der EU-DSGVO
- Use `rua` for daily reports and only add `ruf` temporarily when threatened

TTL - Prepare to fail!

- DMARC is a hard policy – you pass or you fail
- What if you fail and it is your problem?
- Use short `TTL` in for SPF, DKIM and DMARC in DNS!
- A `TTL` of `300` will not kill your DNS servers.

(continued...)

```
_dmarc.dmarcian.com.    300    IN    TXT    "v=DMARC1;
p=reject; rua=mailto:dmcn-corp-ag-in@corp-ag-in.dmarcian.com;
ruf=mailto:wbxefl4v@fr.dmarcian.com;"

_dmarc.bund.de.         600    IN    TXT    "v=DMARC1; p=none;
rua=mailto:bund.de@dmarc.reports.bund.de;"
```

Sub- and organizational domain policies

If there's no DMARC policy in the subdomain the verifier will look for one in the organizational domain.

- What will happen when you ask for reports at org-level?
- What will happen if you `reject` at org-level and neither have SPF nor DKIM in your subdomains?

Sub- and organizational domain staging

1. Start adding a DMARC policy for every subdomain with `p=none` and **don't** request reports
2. Add a DMARC policy at the APEX of the organizational domain with `p=none` and **don't** request reports
3. Now begin to DMARC stage each each subdomain
4. Optional: Upgrade to `p=reject` and request reports at APEX of the organizational domain when all subdomains are compliant and at same level

Questions?