DMARC Bootcamp

Shehzad Mirza
Director of Operations
smirza@globalcyberalliance.org
gca-dmarc@globalcyberalliance.org
What is DMARC?

A DMARC policy allows a sender to indicate that their messages are protected, and tells a receiver what to do if one of the authentication methods passes or fails – such as send the message or junk/reject the message.
Items Needed for Implementation

• Know mail system(s)/server(s) used for org
• Admin level access to DNS for organization
• List of subdomains, if any
• SPF and DKIM (if available)
DMARC DNS TXT Record

• Basic:
  Host: _dmarc
  Value: v=DMARC1; p=none; rua=mailto:<email address>;
  ruf=mailto:<email address>;

• Complex:
  Host: _dmarc
  Value: v=DMARC1; p=none; rua=mailto:<email address>;
  ruf=mailto:<email address>; fo=1; adkim=r; aspf=r; pct=100; rf=afrf;
  ri=86400; sp=reject;
What do each of the tags mean?

**Required:**
- v=DMARC1 - version
- p= - policy level
- rua= - aggregate reports

**Recommended:**
- ruf= - forensic/failure reports

**Optional Tags:**
- fo= send message samples of emails that failed either SPF and/or DKIM.
- adkim= Alignment mode for DKIM
- aspf= Alignment mode for SPF
- pct= - % of messages impacted
- rf= - report format
- ri= - reporting intervals

Consider using
- sp= - sub-domain policy
DMARC Tag Details

p=

- Defines DMARC policy level

  "v=DMARC1; p=none;"

  "v=DMARC1; p=quarantine;"

  "v=DMARC1; p=reject;"
DMARC

What happens to the messages?

- Depends on the policy setting:
  - **None** - reports possible suspicious mail messages, but all mail is sent to inbox
  - **Quarantine** - fail SPF/DKIM and alignment, message is sent to spam/junk folder
  - **Reject** - fail SPF/DKIM and alignment, message is dropped and not delivered at all
- Best practice is to start at ‘None’ and gradually move to ‘Reject’
DMARC Tag Details continued
rua and ruf

rua – aggregate reports
ruf – forensic/failure reports

“v=DMARC1; p=none; rua=mailto:<email address>; ruf=mailto:<email address>;”

Examples:
“v=DMARC1; p=none; rua=mailto:dmarc-rua@company.com; ruf=mailto:dmarc-ruf@company.com;”

“v=DMARC1; p=none; rua=mailto:dmarc-rua@company.com, mailto:admin@company.com; ruf=mailto:dmarc-ruf@company.com;”
DMARC Tag Details continued

fo tag

Optional – used for forensic/failure reports

• send message samples of emails that failed either SPF and/or DKIM.

“v=DMARC1; p=none; rua=mailto:<email address>; ruf=mailto:<email address>; fo=<0,1d,s>”

0 - **(default)** - Generate report if all underlying authentication mechanisms fail to produce an aligned “pass” result.

1 - Generate report if any underlying authentication mechanism produced something other than an aligned “pass” result.

d - Generate a DKIM failure report if the message had a signature that failed evaluation, regardless of its alignment.

s - Generate an SPF failure report if the message failed SPF evaluation, regardless of its alignment.
DMARC Tag Details continued
adkim and aspf

Optional – define alignment mode for DKIM and SPF

“v=DMARC1; p=none; rua=mailto:<email address>; ruf=mailto:<email address>; fo=1; adkim=<s,r>; aspf=<s,r>”

s = strict alignment
r = relaxed alignment (default)
DMARC Tag Details continued

rf and ri

Optional

“v=DMARC1; p=none; rua=mailto:<email address>; ruf=mailto:<email address>; fo=1; adkim=r; aspf=r; rf=<afrf>; ri=<seconds>”

rf – report format

• afrf (default) – Abuse Report Format (RFC 5965)
  • iodef – Incident Object Description Exchange Format (RFC 5070)

ri – reporting interval in seconds.

• Default is 84600 (24 hrs)
DMARC Tag Details continued
pct tag

Optional

“v=DMARC1; p=none; rua=mailto:<email address>; ruf=mailto:<email address>; fo=1; adkim=r; aspf=r; rf=afrf; ri=84600; pct=<0-100>”

• Value = 0-100 (default is 100)
• if you use ‘p=quarantine; pct=0;’ the same as p=none
• if you use ‘p=reject; pct=0;’ the same as p=quarantine
DMARC Tag Details continued

sp tag

Optional, but must consider using

“v=DMARC1; p=none; rua=mailto:<email address>; ruf=mailto:<email address>; fo=1; adkim=r; aspf=r; rf=afrf; ri=86400; sp=<policy level>;;”

• Same policy levels as p=, but applies to all sub-domains
  • if not defined, defaults to ‘p=’ setting.

• When to use:
  • No subdomains and still at p=none. Implement sp=reject
  • Multiple subdomains and ready to move top level domain to p=reject or p=quarantine. Implement sp=none
DMARC DNS TXT Record

• Basic:
  Host: _dmarc
  Value: v=DMARC1; p=none; rua=mailto:<email address>;
  ruf=mailto:<email address>;

• Complex:
  Host: _dmarc
  Value: v=DMARC1; p=none; rua=mailto:<email address>;
  ruf=mailto:<email address>; fo=1; adkim=r; aspf=r; pct=100; rf=afrf;
  ri=86400; sp=reject;
Demonstration:
Create Records in DNS
Go ahead and implement DMARC at p=none for your organization.

Record Name: _dmarc
Value: “v=DMARC1; p=none;
rua=mailto:<email address>;
ruf=mailto:<email address>;”

Ask questions as needed (email or community forum (community.globalcyberalliance.org), or feel free to setup a conference call with us to go through the steps.
Upcoming Webinars

• If interested in BIND (May 20th) and Cloud DNS (May 21st)
• Week 4 - Ongoing Management (May 27th)
Q&A
Thank You!

Shehzad Mirza

gca-dmarc@globalcyberalliance.org

smirza@globalcyberalliance.org

Copyright @ 2020 Global Cyber Alliance