Spruce

The Three Pillars of Email Authentication

Joseph Maltino & Mark Anthony Sanchez

Email Authentication with DMARC

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

DMARC is an email authentication protocol that helps to protect email users from phishing and spoofing attacks. It builds on the widely deployed SPF and DKIM protocols by adding linkage to the author (“From:”) domain name, published policies for recipient handling of authentication failures, and reporting from receivers to senders to improve and monitor protection of the domain from fraudulent email.

What is Email Authentication?

Verifies the true identity of the sender behind an email message, bolstering security. Three main types of email authentication exist:

Sender Policy Framework (SPF)

SPF empowers a domain owner to specify which servers are authorized to send emails on behalf of their domain.

DomainKeys Identified Mail (DKIM)

DKIM adds a digital signature to an email message.

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

DMARC gives domain owners the ability to protect their domain from unauthorized use.

Email authentication can help to prevent email spoofing, phishing, and other forms of email fraud.

Why Do We Need Email Authentication?

- **Protect** from Email Fraud
- **Boost** user confidence
- **Improve** brand reputation
- **Comply** with regulations
- **Improve** email deliverability

Sender Policy Framework

How Does SPF Work?

- SPF allows domain owners to explicitly specify the authorized servers responsible for sending emails on behalf of their domain.
- The recipient's email server can verify the sender's domain by referencing the SPF record, which determines if the sending server is authorized to send emails on behalf of that domain.
- In cases where the sending server is not authorized, the email message may be rejected.
- Implementing SPF can help to prevent email spoofing, phishing, and other forms of email fraud.

DomainKeys Identified Mail

How Does DKIM Work?

- DKIM employs a cryptographic signature to verify the sender of an email.
- The DKIM signature is generated using a private key linked to the sender's domain name.
- By utilizing the public key, the recipient's email server can validate DKIM signature, confirming that the message was indeed sent by the claimed sender.
- Implementing DKIM provides a robust defense against email spoofing, phishing, and other forms of email fraud.

Domain-based Message Authentication, Reporting & Conformance

What is DMARC

- DMARC serves as an email authentication, policy, and reporting protocol.
- Prior to implementing DMARC, it's essential that SPF and DKIM are in place.
- The DMARC policy can be configured with one of three values:
  - p=none (no action)
  - p=quarantine
  - p=reject
- The recipient's email server conducts a thorough evaluation of the sender's domain by checking the DMARC record.
- DMARC policy dictates the appropriate action for emails that do not pass DMARC.

Benefits of DMARC Implementation

Protect your brand from being impersonated in phishing attacks.

Improve email deliverability.

Reduce the risk of business email compromise (BEC) attacks.

Gain visibility into email fraud activity.

DMARC

Implementation

```
v=DMARC1; p=reject; rua=mailto:dmarc@sprucetech.com, mailto:dmarc_agg@vali.email; ruf=mailto:dmarc@sprucetech.com
```

- **Monitor your DMARC reports:**
  - v=DMARC1; p=none; rua=mailto:dmarc@yourdomain.com; ruf=mailto:dmarc@yourdomain.com
  - Run monitoring mode for around two months
    - Identify services/platforms used to send emails as your domain
      - Will need to set up SPF and DKIM for legitimate services/platforms
- **Reevaluate your DMARC policy over time:**
  - Many organizations get stuck on monitoring mode
  - Should update policy to p=quarantine
  - Final step would be p=reject

DMARC Challenges

Adoption

Since its initial publication in 2012, DMARC has gained significant traction with almost 6 million domains implementing a DMARC policy. Approximately 65% are still in monitoring mode.

DNS lookup limit

To implement DMARC, it's necessary to implement SPF records for all services/platforms. There is a limit of 10 SPF records per domain.

Compliance

While DMARC is straightforward to implement, its effective execution can lead to compliance issues.

Phishing

Although domain impersonation is blocked, successful phishing attacks can still occur.

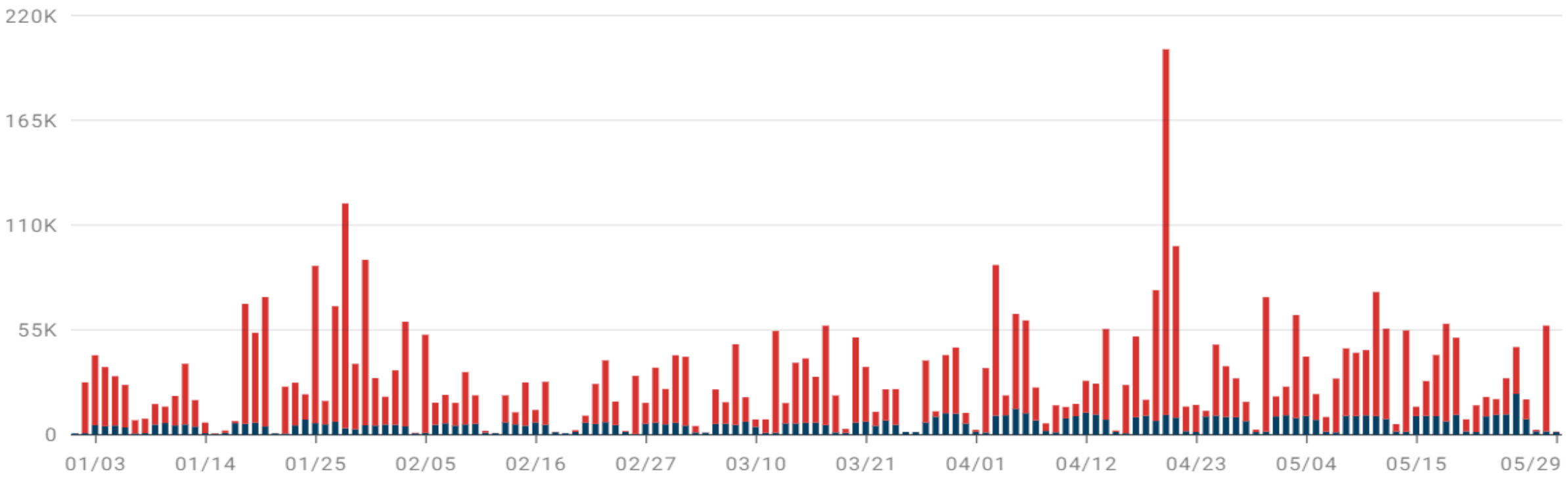
DMARC Challenges in Large Organizations

- **Resource Constraints**
- **Access to DNS Records**
- **Implementation Windows**
- **Several Departments**
  - Each might manage their own services/platforms
  - Different point of contact for every platform
- **More than 10 SPF records as there are many services**
  - Remove unused SPF records
  - Use an SPF flattening service (third-party)
  - Use a subdomain

Anonymous Case Study

PASSING DMARC
822,271

FAILING DMARC
3,686,830



Anonymous Case Study

DMARC Authentication

1,454,354 Messages

Passing 1,449,148	99.64%
with DKIM 1,445,765	99.41%
with SPF 17,554	1.21%
with DMARC override 2,811	0.19%
Failing 5,206	0.36%

Mostly Passing

4 Services

Constant Contact
Pass: 1,444,447 (99.65%)
Fail: 5,015 (0.35%)

Microsoft Office 365
Pass: 3,024 (99.70%)
Fail: 9 (0.30%)

SendGrid
Pass: 1,111 (97.03%)
Fail: 34 (2.97%)

KnowBe4
Pass: 565 (99.82%)
Fail: 1 (0.18%)

Partially Passing

0 Services

Mostly Failing

1 Service

Salesforce
Pass: 0 (0.00%)
Fail: 4 (100.00%)

Thank You!

1149 Bloomfield Ave., Ste G, Clifton NJ 07012

+1 862 225 9300

sales@sprucetech.com

Joseph Maltino
973-476-3157
Jmaltino@sprucetech.com

Mark Anthony Sanchez
862-205-5260
Msanchez@sprucetech.com