CENTRE FOR CYBERSECURITY BELGIUM

dnsbelgium

DMARC INTEGRATION & IMPLEMENTATION

Content

DOCUMENT CONTROL AND REVIEW

Document Control	
Author	
Owner	
Date created	
Last revised by	
Last revision date	

.

VERSION CONTROL

Version	Date of approval	Approved by	Description of change
1.0			

Introduction: why implement DMARC?

In today's digital world, e-mail is an essential means of communication, both within organisations and with customers and partners. At the same time, e-mail is one of the most abused attack vectors for cybercriminals, who use techniques such as phishing, spoofing and fraud to steal confidential data or cause damage to organisations.

To effectively address these risks, implementing **DMARC** is a crucial step. DMARC is an e-mail authentication protocol that enables organisations to protect the sender identity of their e-mails, prevent domain misuse and provide transparency in e-mail traffic through reporting. It builds on existing protocols such as SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) and adds an extra layer of control and management.

Here are the main reasons why DMARC is an essential part of a robust email security policy:

1. Protection against email spoofing

DMARC provides a powerful defence against email spoofing, a technique in which attackers send emails that appear to come from a legitimate sender. By requiring emails to validate both SPF and DKIM and enforcing rejection policies (such as quarantine or blocking), DMARC prevents fraudulent emails from being delivered to recipients.

2. Improving email reputation

When a domain is misused for phishing or spamming activities, this can lead to reputation damage and an increased likelihood of legitimate emails being marked as spam. DMARC helps organisations protect their email reputation by preventing unauthorised parties from abusing their domain.

3. Strengthening customer confidence

Email fraud can lead to loss of trust among customers and partners, especially if they are affected by spoofing attacks that misuse the company's name. By implementing DMARC, an organisation demonstrates that it is taking proactive measures to protect its customers and partners from cyber threats.

4. Understanding e-mail traffic and threats

One of the unique advantages of DMARC is its reporting mechanism. By enabling DMARC reporting, organisations gain insight into:

- Which servers send emails on behalf of their domain.
- How often SPF and DKIM verifications succeed or fail.
- Attempts to misuse the domain by unauthorised parties.

This provides valuable information to detect security incidents and optimise e-mail infrastructure.

5. Meeting legal and industry requirements

In certain industries, such as the financial and healthcare sectors, there are stringent data security and privacy requirements. DMARC can help comply with regulations such as GDPR, PCI DSS, and NIS2, by ensuring more secure email communications.

6. Improving email deliverability

By implementing DMARC, organisations can increase the chances of legitimate emails being delivered correctly. When recipients trust the authenticity of emails from a domain, they reduce the chances of emails being marked as spam.

7. Cost savings

The consequences of a phishing attack or e-mail fraud can be huge, both financially and operationally. This includes incident response costs, reputational damage recovery, legal fines and loss of customer trust. DMARC helps mitigate these risks and provides a cost-effective way to take proactive security measures.

8. Protection of trademarks and intellectual property

One of the biggest threats to companies is the misuse of their brand name in phishing and fraudulent emails. This can lead to loss of customer trust and damage to intellectual property. DMARC protects brands by preventing third parties from unlawfully using a company's domain.

9. Synergy with other protocols

DMARC works together with other e-mail security protocols such as SPF and DKIM. While SPF and DKIM provide technical authentication of e-mails, DMARC adds a policy and reporting layer. This combination provides comprehensive security against the most common e-mail threats. In turn, the implementation of DNSSEC ensures the integrity of the DMARC record.

10. Easy implementation with step-by-step approach

Although DMARC may seem complex at first, it can be implemented incrementally. Organisations can start with a "none" policy (perform no actions) to gain insight into their e-mail flows and later move to more stringent policies such as "quarantine" or "reject". This makes implementation manageable and flexible.

11. Conclusion

DMARC is an essential part of a robust e-mail security policy and provides protection against a wide range of threats arising from the misuse of e-mail domains. Besides preventing spoofing, it strengthens e-mail reputation, increases customer trust, provides insight into e-mail traffic and contributes to regulatory compliance.

With DMARC, an organisation can not only improve its own security, but also contribute to a more secure internet ecosystem as a whole.

12. How does DMARC work?

DMARC adds an extra layer on top of SPF and DKIM by providing three main functions:

12.1 AUTHENTICATION CHECK

Upon receiving an e-mail, the receiving mail server checks whether the e-mail:

1. **SPF-compliant**: The sending IP address must be in the domain's SPF record.
2. **DKIM** compliant: The digital signature in the e-mail must be valid.
3. **Alignment** has: SPF and/or DKIM values must match the **"From" domain** seen by the user.

12.2 POLICY ENFORCEMENT

DMARC allows domain owners to define policies that specify how the receiving server should handle e-mails that do not comply with authentication rules:

- none: No action, report only (often used in testing).
- Quarantine: Mark inauthentic e-mails as suspicious or place them in the spam folder.
- reject: Reject inauthentic emails completely.

12.3 REPORTING

DMARC offers two types of reports:

1. **Aggregate Reports**: An overview of all e-mails sent on behalf of a domain, including results of SPF/DKIM checks.
2. **Failure Reports** (optional): Detailed reports on failed authentication attempts.

These reports are sent to the e-mail address specified in the DMARC record.

13. Building DMARC records

DMARC is configured as a **TXT record** in DNS and has the following syntax:

v=DMARC1; p=<policy>; rua=mailto:<report-email>; ruf=mailto:<error-report-email>; fo=<options>; sp=<subdomain-policy>; pct=<percentage>

Key tags:

- **v=DMARC1**: Indicates that this is a DMARC record (mandatory).
- **p**: Policy rule (none, quarantine, reject) (mandatory).
- **rua**: E-mail address for aggregate reports (optional).
- **ruf**: E-mail address for failure reports (optional).
- **fo**: Failure options, e.g. 1 (issue a report for one failure) or d (issue a report for DKIM errors only).
- **sp**: Policy for subdomains (optional).
- **pct**: Percentage of emails to which the policy is applied (default: 100).

Example of a DMARC record:

v=DMARC1; p=reject; rua=mailto:dmarc-reports@voorbeeld.nl; ruf=mailto:dmarc-errors@voorbeeld.nl; fo=1; sp=reject; pct=100

- p=reject: Reject e-mails that fail SPF/DKIM.

- rua: Aggregate reports are sent to dmarc-reports@voorbeeld.nl.
- ruf: Failure reports are sent to dmarc-errors@voorbeeld.nl.
- fo=1: Send a report in case of a single error.
- sp=reject: Same policy applies to subdomains.
- pct=100: Apply policy to 100% of incoming emails.

14. Step-by-step implementation of DMARC

14.1 ANALYSE EXISTING EMAIL INFRASTRUCTURE

- Identify all systems and services that send emails on behalf of your domain (e.g. mail servers, marketing tools, CRM systems).
- Make sure SPF and DKIM are set correctly.

14.2 START WITH A "NONE" POLICY

Start by implementing a DMARC record with the p=none policy. This collects data on emails without actually taking action. Use a record such as:

v=DMARC1; p=none; rua=mailto:dmarc-reports@voorbeeld.nl

14.3 ANALYSE DMARC REPORTS

- Use tools such as DMARC analysers (e.g. DMARCian or Valimail) to understand sending sources and abuse attempts.
- Identify invalid sources and adjust SPF/DKIM to authorise them, if legitimate.

14.4 SWITCH TO A 'QUARANTINE' POLICY

If you trust the configuration, change the policy to p=quarantine. This will place suspicious emails in the spam folder:

v=DMARC1; p=quarantine; rua=mailto:dmarc-reports@voorbeeld.nl

14.5 INCREASE SEVERITY TO "REJECT"

Once you are sure that all legitimate sources are set correctly, change the policy to p=reject to block fraudulent emails completely:

v=DMARC1; p=reject; rua=mailto:dmarc-reports@voorbeeld.nl

15. Monitor and optimise continuously

- Keep analysing DMARC reports to check for new threats.
- Add new authorised e-mail sources to SPF/DKIM configurations if needed.

16. Technical advantages of DMARC

- **End-to-end security**: DMARC ensures that only authorised sources are allowed to send e-mails on behalf of the domain.
- **Transparency**: The reporting mechanism provides real-time insight into e-mail traffic.
- **Protection against impersonation**: Prevents attackers from successfully carrying out phishing campaigns using a spoofed domain.
- **Control over subdomains**: Specific policies can be applied to subdomains with the sp tag.

17. Common challenges and solutions

Challenge	Solution
Correctly configuring SPF/DKIM	Check records with tools such as MXToolbox or SPF/DKIM validator.
Wrong policy leads to blocked emails	Always start with a "none" policy and analyse reports before moving to stricter policies.
Complexity with multiple email sources	Keep a detailed list of authorised sources and use the include mechanisms in SPF.

18. Synergy with other protocols

DMARC works in harmony with:

- **SPF**: Validates whether the sending IP address is authorised.
- **DKIM**: Checks that the content of the e-mail has not been modified during transmission.
- **BIMI** (Brand Indicators for Message Identification): Combine DMARC with BIMI to display brand logos in compatible email clients.
- **DNSSEC:** ensures the integrity of the DMARC record.

Disclaimer