Benefits of DMARC

Last Modified on 15/08/2024 1:40 pm BST

The Issue

Email security international standards use a variety of mechanisms to look for signs of phishing or spoofing emails. These attacks can use an impersonation of the domain and are usually sent in huge numbers to try and get as many users as possible. Spammers and phishers have a tremendous financial incentive to compromise user accounts, enabling theft of passwords, bank accounts, credit cards, and more. Email is easy to spoof and criminals have found spoofing to be a proven way to exploit user trust of well-known brands. Simply inserting the logo of a well known brand into an email gives it instant legitimacy with many users.

When a company sends a high volume of emails, it can trigger other email service anti-spam systems into thinking these emails are spam and/or phishing attempts, even if sent from a legitimate source using a legitimate domain.

When this happens email filtering will not allow emails to reach the main inbox of their intended recipient,

The Solution

DMARC stands for Domain-based Message Authentication, Reporting & Conformance and is an email authentication protocol. It builds on the existing SPF and DKIM anti-spoofing protocols and adds reporting and enforcement functions that allows senders to block fraudulent email that uses their domain and increase deliverability.

Why is DMARC important?

Receiving users can't tell a real message from a fake one, and large mailbox providers have to make very difficult (and frequently incorrect) choices about which messages to deliver and which ones might harm users. Senders remain largely unaware of problems with their authentication practices because there's no scalable way for them to indicate they want feedback and where it should be sent. Those attempting standard anti-spoofing checks (SPF and DKIM) deployment proceed very slowly and cautiously because the lack of feedback also means they have no good way to monitor progress and debug problems.

DMARC is a way to make it easier for email senders and receivers to determine whether or not a given message is legitimately from the sender (you), and what to do if it isn't. This makes it easier to identify spam and phishing messages, keeping illegitimate emails out of peoples' inboxes and increasing the likelihood your genuine emails stay in, thus protecting your brand from impersonation.

How it works

A DMARC policy allows a sender to indicate that their messages are protected by the anti-spoofing checks, SPF and/or DKIM, and tells a receiver what to do if neither of those authentication methods passes – such as junk or reject the message. DMARC removes guesswork from the receiver's handling of these failed messages, limiting or eliminating the receiving user's exposure to potentially fraudulent & harmful messages. DMARC also provides a way for the email receiver to report back to the sender about messages that pass and/or fail DMARC evaluation.

DMARC has 3 possible policy states:

p=none - This is a policy that requires no DMARC compliance. You are only receiving reports and no DMARC policy is being applied to emails that fail DMARC compliance.

p=quarantine - This policy requires DMARC compliance and means that emails which fail DMARC will more than likely be moved to a receiving user spam folder.

p=reject - This policy that also requires DMARC compliance and is the optimal state organizations would like to get to where any email which fails DMARC compliance is rejected from the receiving mail server.

By having your security profile recognized by email systems as secure, email deliverability rates will increase.

How it is implemented

Shackleton Technologies uses a solution called OnDMARC by RedSift to configure and implement DMARC. We chose this solution as the best in class business offering for us to be able to help our clients implement this complex system after many hours of research in to solutions available on the market. OnDMARC is a cloud product that helps organizations of all sizes implement their email security profile using DMARC, effectively blocking cyberattacks that start with phishing and email impersonation.

- OnDMARC analyzes email reports from the configured domains in order to quickly and easily identify authorized and unauthorized traffic
- OnDMARC gives us specific actions to configure your email services. It gets your domain ready for full DMARC protection in the fastest time possible (typically 4 to 8 weeks)
- Once your domain is protected, OnDMARC helps us continue to monitor and report any security or configuration issues to you
- Activity logs allow us to see who has made an “Addition”, “Modification” or “Deletion” as well as the time and date of that event. This is really important for us complying with security standards like ISO27001 by ensuring you and us both have a clear way to manage systems access
- Forensics allows us to search through emails that failed DMARC for individual forensics. Don’t worry though, the DMARC protocol redacts all sensitive information, such as the body of the email, and OnDMARC further redacts it to ensure compliance with GDPR
- Comprehensive reporting provides clear visual graphs on DMARC validation for all emails sent from your domain. This includes compliance, senders, receivers and locations. Additionally, we include ARC (Authenticated Received Chain) to help resolve issues that may arise with indirect mail flow
- Threat Intelligence checks new IP addresses against SPAM blacklists and exploits, allowing you to quickly identify senders with a low reputation and blocking these potential threats automatically.
- OnDMARC has a secure single sign-on (SSO). with M365 using SAML (Security Assertion Markup Language)