DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING AND CONFORMANCE

APRIL 2021

Domain-Based Message Authentication, Reporting and Conformance (DMARC) is an email authentication policy that protects against bad actors using fake email addresses disguised to look like legitimate emails from trusted sources. DMARC makes it easier for email senders and receivers to determine whether or not an email legitimately originated from the identified sender. Further, DMARC provides the user with instructions for handling the email if it is fraudulent.

WHY SHOULD HEALTHCARE ORGANIZATIONS BE INTERESTED IN DMARC?

Phishing and Spearphishing are among the top attack vectors for healthcare organizations, which can lead to patient care impact, financial fraud, or protected health information (PHI) breaches and Health Insurance Portability and Accountability Act (HIPAA) fines. Fraudulent emails are easy to design and cheap to send, which gives threat actors incentive to use repeated email attacks. Fortunately, healthcare providers can defend their email systems so staff aren't the sole barrier between adversaries and their goal. DMARC provides an automated approach to reducing fraudulent email, before it ever reaches an employee's inbox. In addition, DMARC helps prevent adversaries sending email to your organization or others purportedly from your staff.

HOW DOES DMARC WORK?

DMARC removes guesswork from the receiver's handling of emails from non-authoritative email servers, reducing the user's exposure to potentially fraudulent and harmful messages. A DMARC policy allows a sender to indicate that their emails are protected by Sender Policy Framework (SPF) and/or Domain Keys Identified Message (DKIM), both of which are industry-recognized email authentication techniques. DMARC also provides instructions on how the receiver should handle emails that fail to pass SPF or DKIM authentication. Options include sending the email to quarantine or rejecting it entirely. Lastly, DMARC provides the receiver with an email address to provide feedback to the sender. Potential feedback can include that the sender's email was rejected/quarantined by the receiver or that a threat actor is attempting to imitate the sender's domain.

HOW CAN I ADOPT DMARC ON MY DOMAIN?

Savvy healthcare organizations that adopt DMARC do so in a staged approach, with feedback loops between IT departments and their staff. Because DMARC can block third parties delivering mail on the purported sender's behalf, some intended messages may be flagged as illegitimate in some cases. Below are a few steps organizations can take to ease into DMARC over time.

1. Deploy DKIM & SPF in reporting-only mode first, listing known authorized email servers.
2. Collect and review reports to identify unknown email servers.
3. Work with business units and IT staff to identify servers and determine their legitimacy.
4. Update DMARC policy flags to "quarantine" then to "reject" as confidence increases that most or all legitimate servers have been accounted for.

If you have questions or suggestions regarding this product, please feel free to contact CISA Central at central@cisa.dhs.gov and reference the DMARC document in the subject line.