ISSN:0975-9646
Jagjit kaur/ (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 14 (1) , 2023, 1-2

The Value of DMARC to enterprises

Jagjit kaur
Faculty in Computer Science , Suraj School , Sec-56, Gurgaon
jagjit779@gmail.com

Abstract- **(DMARC) is a free and open technological specification that is used to align SPF and DKIM techniques in order to authenticate emails. Domain owners of all sizes may combat business email compromise, phishing, and spoofing by putting DMARC in place. DMARC, co-written by the founder of dmarcian, was initially released in 2012**.

I. INTRODUCTION

For the clients in businesses, email is a key channel. Daily promotions are presented to the clients through the email channel. The client wanted to make sure that all emails reached their customers principal inboxes and that no harmful emails were sent on their behalf. In order to trick victims into thinking they are getting an email from a reliable source, such as a reputable company or a friend, phishing and spear phishing emails are both used. It is made feasible through email spoofing, a hacking technique that, when used correctly, needs little to no technical expertise but may inflict enormous damage.

II. CHALLENGES FACED BY BUSINESSES

- The average cost of a spear phishing attack on a company is $1.6 million.
- From 2013 to 2016, businesses suffered losses of over $1.6 billion.
- Phishing scams result in annual losses of $500 million.
- An organisation with 10,000 employees on average spends $3.7 million a year dealing with phishing attempts.
- The typical worker loses 4.16 hours per year to phishing schemes.
- CEO scam emails have affected 1 in 3 businesses.
- BEC scams target more than 400 firms each day.
- Dollar amounts rapidly increased by 2370% between January 2015 and December 2016 as a result of phishing assaults.
- In 2016, 6 percent of businesses reported being the target of phishing attacks.
- Malicious emails make over 70% of all emails worldwide.
- Over 400,000 phishing sites have been seen monthly on average in 2016 thus far.

III. SOLUTION

Domain-based Message Authentication, Reporting & Conformance, or **DMARC**, is a protocol that uses Sender Policy Framework, (SPF) and Domain Keys identified mail (DKIM) to determine the authenticity of an email message. It enables email senders to declare how to deal with emails that were not verified with SPF or DKIM. Senders have the option of placing those emails in the junk folder or having them completely blocked. ISPs may lessen false positives and provide better authentication reporting for more market openness by doing this. In addition, they can better identify spammers and stop dangerous email from infiltrating consumer inboxes.

DMARC is always used with these two email authentication methods or checks

1) Sender Policy Framework (SPF) - It enables the domain owner to control which IP addresses may use the domain to send email. Receiving servers can confirm that messages purporting to originate from a particular domain are indeed sent by servers that the domain owner has authorized.

2) Domain Keys Identified Mail (DKIM) - It adds a digital signature to every sent message. Receiving servers use the signature to confirm that messages are real and haven't been altered or falsified while in transit.

By implementing a policy in your DMARC record, you can utilize DMARC to communicate to the world how to address the unauthorized usage of your email domains. The three DMARC policies are:

1) p=none

Monitors your email traffic. No further actions are taken.

2) p=quarantine

Sends unauthorized emails to the spam folder.

3) p=reject

The final policy and the ultimate goal of implementing DMARC. This policy ensures that unauthorized email doesn’t get delivered at all.

IV. DMARC RECORD

An organization's DNS database contains a DMARC record**.** A DNS TXT record with the specific identifier "_dmarc.mydomain.com" is a specially formatted variant of a DMARC record. _dmarc.mydomain.com is how a DMARC record appears. "v=DMARC1; p=none; ruf=mailto:dmarc-afrf@mydomain.com;ruf=mailto:dmarc-aggregate@mydomain.com; pct=100"

- The DMARC version is specified by v=DMARC1.
- The desired treatment, or DMARC policy, is specified by p=none.
- The mailbox to which aggregate reports should be transmitted is rua=mailto:dmarc-aggregate@mydomain.com.
- The mailbox where forensic reports should be transmitted is ruf=mailto:dmarc-afrf@mydomain.com.
- The percentage of messages to which the domain owner wants to apply its policy is pct=100.

V. BENEFITS OF USING DMARC BY BUSINESSES

- Reputation: By blocking unauthorized parties from sending email from your domain, publishing a DMARC record safeguards your brand. In some circumstances, the simple act of publishing a DMARC record can lead to an improvement in reputation.
- Visibility: DMARC reports give you more insight into your email programme by revealing who is using your domain to send email.
- Security: To safeguard users from spam, fraud, and phishing, prohibit illegal usage of your email domain.
- Delivery: employ the same cutting-edge plumbing that large corporations do to send email.
- Identity: Make it simple for recipients of DMARC-capable emails to recognise your emails across their vast and expanding network.

VI. CONCLUSIONS

The greatest solution for organisations of every kind is to properly check the state of emails with the legitimacy of sources because cyber security is a critical technology today. A DMARC checker can help protect email exchanges for the trustworthiness of your domain and help avoid fraudulent actors exploiting your domain name and website by providing a report of the DMARC policy with valid DKIM signatures and SPF alignment verification. A business should frequently review its DMARC records to learn how to streamline its DMARC setup for better domain email management.

.

REFERENCES

[1] Simpson, J., 2016. Email Archiving Systems Interoperability

[2] Kontinen, V., 2020. Preventing email forgery in Finland: Research on the current SPF and DMARC implementations.

[3] Nowitz, J., 2018. A Modern Perspective on Phishing: An investigation into susceptibility to phishing attacks between mobile and desktop email clients.

[4] Eboibi, F.E., 2021. Cybercriminals and Coronavirus cybercrimes in Nigeria, the United States of America and the United Kingdom: cyber hygiene and preventive enforcement measures. Commonwealth Law Bulletin, 47(1),pp.113-142.