DMARC Analyzer

CASE STUDY DMARC ANALYZER

Customers are protected against phishing and spoofing

This case study is based on a collaboration with a leading Dutch eCommerce company.

Challenge
Multiple domains being spoofed on a regular basis.

Solution
After aligning SPF and DKIM the DMARC policy was enforced.

Results
Customers are protected against phishing and spoofing attacks.

Email is an important channel for this client. Email Marketing is their primary channel to reach out to customers. On a daily basis the email channel is used to present daily deals to their customers. The client wanted to ensure that all email gets delivered in the primary inbox of their customers and make sure their customers do not receive malicious emails on their behalf.

> "Our company has a database of 850.000 email addresses. We're sending out millions of emails on a monthly basis. Before deploying DMARC our domains were spoofed. The DMARC deployment specialists really helped us during the Managed Services project. After validating the sources with the DMARC Analyzer team we were able to protect all of our domains from being spoofed by deploying a DMARC policy. Within a year all of our domains were protected."
>
> **General Manager - eCommerce company**

Challenges

The challenges that ensured DMARC Analyzer was needed as an executive party:

- Limited insight in email channels
- Legitimate email was marked as spam
- Client was placed on black lists by several ISPs
- No setup for DKIM signature
- Ongoing spoofing attacks on brand

Company details

Company
eCommerce company

Country
The Netherlands

Company Size
SMB

Industry
eCommerce

Project goals

The main project goals of this DMARC deployment project:
- Get insight in all email channels
- Authenticate emails with a DKIM signature
- Improve email deliverability and the performance of email marketing channels
- Mitigate the effect of phishing, spoofing and other attacks. This includes inbound attacks as well as attacks aimed at clients and partners

Project approach

DMARC Analyzer started collecting the DMARC reports for this client after they published the custom monitoring-only DMARC record into their DNS. These DMARC reports provided full visibility into all their email channels. To resolve the challenges, our DMARC deployment specialists had to investigate each single sending source and eventually had to make sure that each single (legitimate) sending source would become DMARC compliant. In order to make these legitimate sending sources DMARC compliant one of the email authentication techniques, SPF or DKIM had to be aligned.

In collaboration with the client, DMARC Analyzer was able to align all SPF and or DKIM for their known legitimate sending sources. As a result of this, the client was nearly able to achieve a full DMARC compliance rate. Unfortunately, a full compliance rate could not be achieved. Knowing this, our DMARC deployment specialists did deeper analysis and determined that one specific source had forwarding issues. Both SPF and DKIM broke when this specific source was forwarding emails. This did not occur on other forwarding sources.

In collaboration with the customer DMARC Analyzer decided to not implement the reject policy, since this would result in the loss of many forwarded legitimate emails. Instead of the reject policy, DMARC Analyzer decided to implement the quarantine policy with a percentage tag of 100%. This way these emails, that first were not delivered at all, will be delivered in the spam folder of the receiver.

DMARC Analyzer and the client are now in consultation to create a subdomain for this specific source. That way a reject policy can be applied on the domains of the client and a quarantine policy can be placed on the specific subdomain.

Achievements

Achievements realized for the client as a result of the DMARC Analyzer deployment:

- Gained full insight into the email channel
- Authenticated all email with a DKIM signature
- All domains are protected with a DMARC enforcement policy
- Email deliverability improved
- Customers are protected against phishing and spoofing attacks