Issue # 11 Volume #16 November 2015

Solutions are our Business

AaSys Offers New DMARC Implementation Service

AaSys continues to remain at the cutting edge of technology. We recognize this industry is filled will constantly moving pieces. We want to make it easy for our customers to navigate through the sometimes complicated yet necessary changes, and because of that, we are now offering new DMARC Implementation Services.

History

The origin of email can be traced back to the early 1970s. But it wasn't until the early 1980s, when a new protocol was introduced called SMTP (Simple Mail Transfer Protocol), that email started to gain momentum. When SMTP was designed, it did not include a way to guarantee the sender of an email was actually the sender. In the early days, users of email were a very small group of government agencies, universities and some corporations, and thus, you could safely assume the sender was indeed the sender of the email. Years later, the Internet would explode in popularity and email would be used by everyone. The protocol to deliver email today is still SMTP and although there have been changes over the years, many of its pitfalls and shortcomings remain. One of them is the ability to spoof the FROM address of an email header. Spoofed emails have become a daily occurrence for everyone using email and it has become a billion dollar industry for spammers and hackers.

Over the years, a few measures have been put in place to fight email spoofing. The two most popular solutions are called SPF (Sender Policy Framework) and DKIM (Domain Keys Identified Mail). SPF checks the source IP address of the sending email server and verifies that the server is allowed to send email for a given domain. DKIM uses a public/private key to ensure that email coming from a domain is allowed and contents of the email are not altered once the email is sent. Usage of SPF and DKIM has steadily increased over the years and most of the large email providers such as Yahoo!, Gmail, and Microsoft are using these in some capacity. But adoption of these two standards throughout the world has been sporadic. Starting in 2010, a group of leading organizations (JP Morgan, Bank of America, Google, and Microsoft) came together to develop a new standard for using both SPF and DKIM. The result was the release of DMARC (Domain-based Message Authentication, Reporting & Conformance) in 2012.

What is DMARC?

DMARC is a standard that allows participants to ensure that emails being received are not spoofed and legitimately originate from the sender. Not only can DMARC prevent spoofed email from entering your organization, but it can prevent others from spoofing your domain. It can also provide reporting on who is attempting to spoof your domain and the frequency of these spoofing attempts.

Continued on Page 2

Are there subjects that you would like to have covered in future newsletters? We are always looking for topics of interest and we welcome all suggestions! To submit a topic, subscribe, or unsubscribe to our distribution list, please send an email to newsletter@aasysgroup.com

11301 N. US Highway 301
Suite 106
Thonotosassa, FL 33592
(800) 799-8699
www.aasysgroup.com

AaSys will be closed on Thursday, November 26, 2015 for Thanksgiving Day. The Helpdesk will be closing at 4PM on Friday, November 27, 2015.

Other Important Dates: AaSys will be closed on Friday December 25, 2015 for Christmas and Friday January 1, 2016 for New Years Day. The Helpdesk will be closing at 3PM on Thursday December 24, 2015 and Thursday December 31, 2015.

Inside this issue:

FREQUENTLY ASKED QUESTIONS

Why should I Implement DMARC?
How many of your customers are receiving spoofed emails appearing to come from your organization? Would you like to stop this? Would you like to see how many spoofed emails are happening daily and where they are coming from? DMARC implementation provides the answer to these questions. The more participants in DMARC, the more effective it becomes. Most all major email providers are now using it.

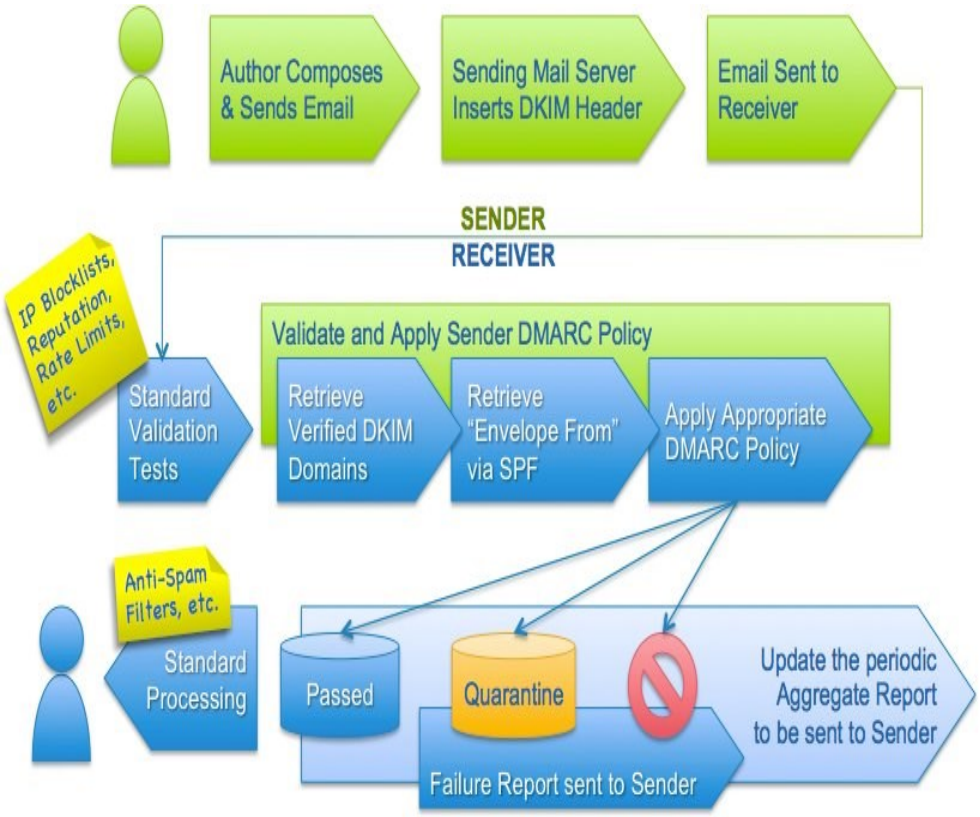
How do I implement DMARC?
Implementing DMARC is a *process* and not something that is just turned on. The first step is to set a DMARC policy and set it to "monitor" only. Next, implement SPF and DKIM on your domain. During this time you will receive reports on where your email is coming from and to who (only those email servers participating in DMARC send these reports). If legitimate emails are being sent from other vendors using your domain, that vendor will need to participate in the DMARC process. Once you are confident that all email coming from your domain is included in the DMARC process, you can set the DMARC record to reject. This will tell other mail servers that email can only originate from you and your vendors, and if an email does not originate from these sources, the email will be rejected, thus preventing it from being spoofed.

How much does DMARC cost?
There are no hardware or software costs with DMARC other than the time to initially set it up. Once DMARC has been setup completely there is not much time needed to maintain and monitor it. The setup process largely revolves around reviewing reports identifying email activity within your organization (or allegedly within your organization). Working with vendors who may have legitimate reasons to use your email address and confirming their acceptance of DMARC technology is the biggest time commitment. The involvement of vendors who send out statements on behalf of the institution, for instance, is critical.

How long does the process take?
Implementation time frames may vary, depending on the availability and cooperation of partner vendors. On average, this process will take between 4-6 weeks.

What are the implementation fees?
Please reach out to your account manager for pricing details.

*****If you recently purchased a .BANK domain and plan to use it for email, you must implement DMARC.*****



Come Join Us at Our Next ISO Peer Group Meeting In FL, TN & WV!

AaSys Group is once again holding another Information Security Officer Peer Group Meeting in Florida, Tennessee and West Virginia. For those responsible for the ever-increasing demands of Information Security, the Peer Group provides a great resource to share issues, concerns & compare best-practices to improve the overall security structure of their financial institution. We look forward to seeing you there!

Riverview, FL

Topic: Proactive Use of the FFIEC Cyber Security Tool, FS ISAC Presentation, What is Hardening of Your Network, Cyber Security Threat Intelligence and much more!

Date: Friday, November 20, 2015
Time: 9:30 AM– 3:00 PM, lunch included
Location: Hilton Garden Inn
4328 Garden Vista Drive
Riverview, FL 33578

Knoxville, TN

Topic: Cybersecurity Framework (Note: For those of you who attended the March Roundtable about the NIST Cybersecurity Framework, this discussion is about new and different information.)

Date: Wednesday, December 2, 2015
Time: 10:00 AM – 2:00/2:30 PM, lunch included
Location: Hampton Inn Knoxville West Cedar Bluff
9128 Executive Park Drive
Knoxville, TN 37923

Clarksburg, WV

Topic: Cybersecurity Framework

Date: Thursday, December 3, 2015
Time: 10:00 AM– 2:00/2:30 PM, lunch included
Location: West Union Bank
320 Emily Drive
Clarksburg, WV 26301

AaSys
Solutions are our Business