ASISA SECURE DATA EXCHANGE GUIDELINE

Effective date: 28 June 2022

Date of latest update: 28 June 2022

EMAIL ENCRYPTION

Introduction

The purpose of this Guideline is for all ASISA members to apply and enforce security capabilities on their email infrastructure in order to establish a level of trust between members. With the additional security layers, information can be shared securely negating the need to additionally password protect attachments when sharing information.

Background

Protection of confidential information in a document, happens mostly by setting a password that only the author and the recipient/s of the document would know. This practice makes it impossible for security controls to effectively scan encrypted communications to ascertain if it is malicious or not. Cyber attackers are fully aware of this, and it is common practice to encrypt malicious software deployed to unsuspecting users via email, knowing that user judgement is not always fool proof. There is therefore an additional need to encrypt the transmission channel shared by both parties. In this way it would be difficult for an unauthorised party to access the information. With POPIA and privacy legislation, this practice is becoming more prevalent.

Most companies apply a security measure to quarantine all emails that contains an encrypted attachment. Dependent on the respective internal processes, this requires a release process that does cause additional overhead and potential delays in service.

Whilst some organisations are busy migrating to other secure communication channels, the need to transmit confidential information via email will continue. There is a huge risk in in the financial services industry specifically for those that utilise brokerages that have entrenched email into their processes and are reluctant to change. Additionally, they do not always apply all the required security protocols due to cost and other factors.

If an agreed secure trust model is applied in the financial services industry, it should strongly encourage smaller entities and brokerages to begin adopting the same which would in turn improve the secure transmission and safety of millions of South African's information.

Objective of the Guideline

The objective of this guideline is to improve the security posture across a wider base of financial services entities through the reduction of risk in the following ways:

- protection of data in transit,
- reduce the operational overhead due to manual encryption methods and quarantine release processes,
- mitigate the risk of malicious software (malware, ransomware) being spread via trusted partners,
- enable trust between sharing partners, ie: ability to verify that a "sending" domain is not spoofed.

Security measures

ASISA members are encouraged to adopt and enable the following security measures for their email infrastructure. The adoption of this Guideline by members will create a "Trust Model" that ensures

communication via email between members can be accepted as being secure and trusted. There is still an element of risk and diligence must always be applied but this will holistically improve the security of participating companies.

The following aspects have been established to be adopted and enabled as a minimum standard :

a) Transport Layer Security (TLS)

Enforcing this protocol will encrypt the entire email communication channel ensuring the privacy of all data that traverses it. As a first step this should be set to enforced on incoming and outgoing emails with participating ASISA members. Thereafter it should then be extended to all 3rd parties that the member company communicates with, where applicable and able.

b) Domain verification (DMARC - SPF, DKIM)

To mitigate the risk of attackers spoofing emails and domains, both the member company and the senders must provide assurance of their "identity". This assurance can be provided by member companies through the application of Domain verification security protocols.

(Info on DMARC - SPF, DKIM- https://www.csoonline.com/article/3254234/mastering-email-security-with-dmarc-spf-and-dkim.html)

Conclusion

It is always advisable to amend processes that require the secure and confidential exchange of information via files to be done via robust secure channels other than email.

Whilst this Guideline does not address all risk areas, it will bring about a vast improvement in the industry with regards to secure communication and the protection of information.

HISTORY OF AMENDMENTS

Effective date	Amendments
28 June 2022	New Guideline

Responsible Senior Policy Advisor: Johann van Tonder