ASISA SECURE DATA EXCHANGE GUIDELINE

Date of first publication: 28 June 2022

Date of last update: 18 July 2024

EMAIL ENCRYPTION

1. INTRODUCTION

1.1. The purpose of this Secure Data Exchange Guideline ("**Guideline**") is to guide ASISA members in applying 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.

1.2. This Guideline is being shared with ASISA members and the public at large for their consideration and voluntary implementation and is non-binding on ASISA members.

2. BACKGROUND

2.1. Protection of confidential information in a document occurs 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.

2.2. Most members 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.

2.3. 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.

2.4. 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.

3. OBJECTIVE OF THE GUIDELINE

3.1. 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:

3.1.1. protection of data in transit;

3.1.2. reduction in the operational overhead due to manual encryption methods and quarantine release processes;

3.1.3. mitigating the risk of malicious software (malware, ransomware) being spread via trusted partners;

3.1.4. enabling trust between sharing partners, i.e. ability to verify that a "sending" domain is not spoofed.

4. SECURITY MEASURES

It is recommended as follows:

4.1. 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 should always be applied, but this will holistically improve the security of participating members.

4.2. The following should be adopted and enabled as a minimum standard:

4.2.1. **Transport Layer Security (TLS)**

4.2.1.1. 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 communicates with, where applicable and reasonable practicable.

4.2.2. **Domain verification (DMARC - SPF, DKIM)**

4.2.2.1. To mitigate the risk of attackers spoofing emails and domains, both the member and the senders should provide assurance of their "identity". This assurance can be provided by members through the application of domain verification security protocols.

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

5. CONCLUSION

5.1. 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 aims to bring about a vast improvement in the industry with regards to secure communication and the protection of information.

DOCUMENT HISTORY

Date	Publication/amendment
28 June 2022	First published
28 June 2022	Updated
18 July 2024	Competition law review

RESPONSIBLE SPA AND COMMITTEES

Responsible Board Committee	Technical and Operations Board Committee
Responsible Standing Committee	ASISA/SAIA CSIRT Standing Committee
Responsible Senior Policy Advisor	ASISA Point Person to the Technical and Operations Board Committee