FORTRA

GUIDE (Clearswift)

Email Encryption Best Practices

Email continues to be the lifeblood of organizations. With changes to legislation and the increased attention on data breaches now is the time to revisit email solutions and policies to improve the security of the information that flows through organizations – both inbound and outbound.

While it has been commonplace to have antivirus scanning and anti-spam on the incoming email stream for many years, organizations are now improving security around outbound email, through the increased use of encryption and deployment of data loss prevention (DLP) solutions. The reason for this is two-fold; the first is understanding the benefits and differences of the myriad of options available. The second is around the cost and ease of use for the solutions. In the past, both encryption and DLP solutions have been notoriously difficult to configure and maintain, making them only options for larger organizations with specialist IT skills.

What Is Email Encryption?

Email encryption is used to ensure that the contents of an email cannot be read or modified if it is intercepted. Email administrators know that the path of an email from sender to recipient will be processed by several different mail relays before it reaches its destination. This is why email encryption is paramount as people no control over security of these intermediate mail hops.

Encryption typically converts the information in an email from plain text to encrypted text. The text is then converted back to plain text when the recipient uses a private key to decipher the message. Each organization may have different levels of security, some may even require internal email is encrypted, but it is more common to encrypt content when it leaves an organization and sent to a third party.

The ideal place for encryption to occur is on the perimeter mail service, as the email enters or leaves the organization. Today's email gateways, which protect against inbound threats, can also provide automatic encryption of outbound email and decryption of inbound email.

So, when should an email be encrypted? The answer depends on the email, but a lack of encryption means the email content can be read by anyone. An organization needs to encrypt its sensitive information to reduce risks of data loss. Data is valuable with trade secrets, intellectual property, and sensitive data (personal identifiable information and payment card information), and some have even considered data as a new currency.

The success of an email encryption project is based on the continued adoption by both sets of stakeholders. If it too complex to send a message securely – then the project has failed. If the recipient cannot receive and open the email to use the data – then again, the project has failed.

It must work for both senders and receivers for the deployment to be success.

Types of Email Encryption

The Secure Email Gateway (SEG) encryption options allow policies to be based on sender, recipient, subject content, message body, attachment types, attachment content, message header, or document metadata. SEG can detect information that shouldn't be there. The data might be deliberately exfiltrated or someone could be sending out some content that may contain a hidden worksheet.

Securing the communications channel and securing the message itself are the essential categories of email encryption.

By providing multiple options to send data securely, organizations can choose the best method to deliver content to third parties in the most appropriate method. The following are various encryption methods used:

Transport Layer Security (TLS)
TLS is built into every email service and is the equivalent of HTTPS for browsing. The email is sent from server to server via an "encrypted tunnel." **This is the absolute minimum level of email encryption that organizations should be using today.**

This method relies on both the sending server and receiving server supporting the TLS protocol as an agreement where the sender is requesting a desired level of security. For example, if the sending server is configured to use the TLS 1.2 standard and the receiving server only supports the deprecated TLS 1.0 protocol, the sending server may not complete the connection due to a security concern.

Even though TLS usage is widespread and has been available for many years, there are renewed efforts to improve the security of TLS to avoid downgrade attacks and spoofing, including the new MTA-STS specification. This approach allows an organization to create a TLS policy which is published through DNS so that those who send to that organization are aware that they will be expected to communicate with TLS 1.2 or later and with valid TLS certificates.

Just to reiterate, this is purely covering server to server communications, and not sender to recipient communications.

Password protected files
Many people are familiar with the idea of passwords protecting files for privacy, only the people who know the password can gain access to the contents.

The downside of allowing the sender to set a password on a file and send the message through the corporate gateway is that it is likely to be blocked because the content can't be verified. If the gateway can password-protect the file after the message and its contents are verified, it fulfills the need for internal inspection and then secures the message to the recipient.

Typically, this method wraps the sender's message and attachments into a password protected Zip, Office, or PDF, using modern standards such as AES, which is then delivered to the recipient.

The sender must get the password to the recipient, typically using a different medium such SMS, or email to a secondary email account. Systems that send automatically generated passwords in the recipients email can easily be compromised and a potential data breach can occur.

Secure MIME (S/MIME)
Secure MIME is a standard for sending secure messages and widely used in Europe. This system uses public key cryptography, where users have both a private and a public key. The keys are mathematically linked so that a message encrypted with a public key can only be opened by the recipient using their corresponding private key.

Encryption is strong and hard to crack when using a public-key based system. Most mail clients, such as Microsoft Outlook, supports S/MIME as standard. This means recipients public keys are safely stored and automatically used when the sender wants to send a secure message.

Again, the same risk of a user encrypting corporate secrets and sending that through their gateway is possible, but this can be solved by requiring the sender to include a "Key Guardian" account as a "bcc" on the message. This allows the gateway to decrypt the message and determine if it is safe to send.

The whole process can also be performed on the gateway itself, which can hold recipients' public keys and perform the encryption and decryption of messages automatically — without the sender having to worry about complexities of email encryption.

Pretty Good Privacy (PGP)
Pretty Good Privacy is a similar mechanism to S/MIME where users have both private and public keys but use different sets of algorithms.

Web Pickup Over SSL (web pull)
Another popular method of delivering secure messages, especially for the B2C customers, is through an email portal. This allows senders to send messages to recipients who receive a link back to the hosted portal where the recipients can use a webmail style mail client and respond to the sender in a secure fashion.

The advantage of this method is that it allows the recipients to have a secure conversation and data sharing requiring only a browser regardless of whether they are using a Windows, Mac, Tablet, or phone.

Portal-based encryption can be done "off-premise", i.e. through a service provider, or it can be provided "on-premise," where the system can be completely under the organization's control.

Web Portal-Based Encryption (Push)
Recipients who become familiar with the service and decide they would prefer a message to be delivered with an attachment rather than just a link to a message, can elect to have the message delivered to their inbox encrypted with a password of their choice.

Best Efforts Encryption
As usage increases and organizations send to a variety of recipients that use different encryption methods, managing each one can be labor intensive. Having an approach whereby the choice of encryption options is automated, enables organizations to create a policy that might follow the following path:

1. Does the recipient have an S/MIME or PGP key? If not, move to 2.
2. Can I send the message over TLS? If not, move to 3.
3. I will send the message and use the encryption portal

Fundamentally this provides the best of all worlds.

	Encrypted Site-to-Site	Encrypted Site-to-Recipient	Encrypted Desktop-to-Desktop	Standards Based	Crypto Strength	Key Exchange or Password	Recipient Transparency
TLS	Yes	No	No	Yes	Medium	No	Yes
S/MIME, PGP	Yes	Yes	Yes	Yes	High	Yes	Site to Site - Yes Encrypted to Recipient may require key and client plugin
Password (Windows)	No	Yes	No	Yes	Medium	Yes	Yes
Password (AES)	No	Yes	No	Yes	High	Yes	Requires Zip package that supports AES256
Portal	No	Yes	No	Yes	High	No	May require plugin for "push" messages

Integrating Data Loss Prevention and Email Encryption

For some information, even email encryption is not sufficient – this information needs to be kept within the organization at all times. For this, data loss prevention technologies need to be used to watch for restricted information crossing the egress points and automatically blocking it. A DLP solution enables an organization to inspect the content of an email and its attachments looking for specific information and then carrying out an action on the email should the information be found.

One simple use-case is to block any email leaving the organization that contains top secret content — which must not be sent out — but other policies may look for sensitive information such as credit card or bank information that needs to be shared with specific third parties. For example, external payroll services have information that must be sent, but sent securely using encryption.

Protecting Web-Based Email

For many organizations, when it comes to information security, there is now a need to consider web-based email as well as corporate email. Most organizations now require that employees use their work email for work and work alone – the result is that employees often have a personal email address for use with friends and for other social reasons. However, the rise of personal email has also resulted in a rise in corporate information risk, with employees sending critical information to their home email accounts (often so they can work on the document at home). When looking at securing corporate information, this communication channel needs to be considered.

Summary

Email continues to be a critical business tool for organizations big and small. Almost all an organization's intellectual property and company confidential information will travel through email at some point in its lifecycle. This coupled with increased needs for collaboration, imposed legislation and cyberattacks on corporate information means organizations need to revisit their email security polices and solutions to protect their critical information. An increased emphasis on Information Governance, the understanding and protection of information, especially that which flows in and out of an organization, is driving all organizations regardless of size to look at technologies for securing email.

In the past secure email technology needed specialist skills to administer, but today even the smallest of organizations can readily encrypt their email and apply DLP policies without increasing management costs. The same security policies which are applied to corporate email can also be applied to web-based email by using combined web and email gateways, giving organizations the assurance, they need that their information is secured no matter which communication channel is used.

Furthermore, the increasing use of web-based collaboration tools and very large files means organizations need to look at secure file transfer technologies to enable the same policies that are applied to email to also be applied to files as they are moved between organizations or even departments.