VERSION 1.0

EMAIL ENCRYPTION AND THE FALSE SENSE OF SECURITY

Microsoft Partner

KEY TAKEAWAY

Email encryption often gives a false sense of security against intentional or accidental data loss. Most email encryption solution comes with weak sensitive data detection program and relies on the user to determine whether or not to encrypt the email. The smarter organizations often use server side robust data loss programs in conjunction with the email encryption solution.

KEY CHALLENGES

Email encryption solutions ensure secure transmissions and storage of email messages to the intended recipients. While encryption solutions strengthen certain aspects of data security, they do not protect organizations from data loss/data theft primarily for the following reasons:

Optional Encryption Feature: Most encryption solution comes with a client program with built in weak sensitive data detection programs. Depending on the content of the email and the attachment, it gives the user the option to encrypt the message. If the user fails to choose the encryption option, an email will be sent in plain-text – opening up the possibility that the email can be accessed by someone other than the intended recipient.

Limited Detection Feature: Most encryption solution can not detect sensitive information in image files and in documents with embedded images. In many cases, they do not even attempt to scan documents that are larger than a certain size. For example, Office 365 Data Loss Program can only scan first 1 MB of text.

Reliance of Regex Patterns: Most sensitive data detection software relies on the regular expression(RegEx) to detect sensitive data element ignoring emails that are sensitive (e.g. budget information, customer information, patent files, design document, drug composition datasheet) but do not have any Regex Pattern.

Lack of Real-time Reporting: If a malicious user uses encryption software to send sensitive information to a third-party recipient – there is no real-time alerting mechanism to detect and prevent the transmission automatically. For example, an employee in a payment processing company used email encryption software to transmit a bunch of documents containing sensitive information to his personal email account. This activity was undetected for a period 3 months until internal audit found this issue.

Inability to Detect Anomalous behavior: In most cases, both the email solution and the encryption solution are incapable of performing real-time analytics to detect anomalous activity either to identify a user error or malicious user activity. In our consulting engagements, we have seen a number of usage patterns that led to sensitive data loss or privacy breach:

- User sent unusual number of emails to specific email accounts in a short time frame
- User sent an attachment containing large number of sensitive information (e.g. 10000 social security numbers)
- User sent emails to large number of recipients (e.g. Lead researcher sent emails to all the trial drug participants resulting in a privacy breach)

BEST PRACTICES FOR PREVENTING DATA LOSS IN EMAILS

- **Detect Sensitive in Real-Time**: Use a server side robust sensitive data detection program to examine the content of the emails. Depending on the detection result and the output of the anomaly detection algorithm, the organization may configure its email system to perform the following:
    a) Send the email as is
    b) Encrypt the email and deliver it to its intended recipient
    c) Block the email for secondary review

- **Analyze Content in the context of Temporal and Spatial fingerprint**: Leverage advanced analytics to build a temporal and spatial fingerprint of the user email activity. Temporal fingerprint refers to the historical usage pattern. Spatial fingerprint refers to the usage pattern of enterprise data sources (e.g. sales force, MS SQL database, SharePoint). Any significant deviation from the temporal and spatial fingerprint can indicate potential data theft. Fifty-nine percent of employees steals sensitive information prior to quitting their job. An anomaly detection program will help to detect sudden spurt in data access pattern and email activity.

BOTTOM-LINE

While Email encryption solutions ensure secure delivery of emails, they do not provide a reasonable defense against intentional or accidental data loss. Enterprises consider a server-side robust data loss program with built-in real-time analytics to detect deviations.