Data leak prevention is essential for securing email communications

By Simeon Tassev

28 Jul 2015

The business world has become increasingly digital, and email is the most prevalent means of communication in many organisations. While email offers many benefits, such as improved efficiency and overall productivity, it can also prove to be the single biggest point of risk when it comes to information security.

Simeon Tassev

Not only can email open organisations up to vulnerabilities such as theft of Intellectual Property (IP) and other confidential or sensitive information, email security is now part and parcel of compliance to regulations such as the Protection of Personal Information (PoPI) Act. Data leak prevention technology is therefore essential for securing email communication.

An unseen challenge for organisations

While email has provided many benefits in the form of convenience and improved productivity, it is also often an unseen challenge for organisations. Users have become increasingly comfortable with email as a means of communication that they may unintentionally engage in risky data practices. Take for example credit card information. This should never be emailed, because email is not a secure communication method and can be hacked, leading to theft of this confidential data that could otherwise be prevented. Often, information of significant value, including personal details, is sent via email, which can have serious repercussions for organisations if this data is breached.

Data leak prevention is therefore an essential component of email security, including rules and policies as well as supporting technology. Data leak prevention technology for email helps organisations to control what data goes out of the organisation. It works by flagging emails that are potentially in breach of policy to stop this information from leaving the organisation or falling into the wrong hands, either intentionally or unintentionally. However, in order to create these flags, the technology first needs to be able to identify emails that are potentially risky.

David Castillo Dominici via freedigitalphotos.net

Email security top of mind

Comprehensive policies must be developed to guide the technology, as part of an overall data protection strategy. This in turn requires that organisations firstly understand their data, what data they are trying to protect, and the ways in which it might find its way out of the organisation. While email is the most common culprit, there are other methods of data leakage, from sophisticated hacks to simple methods such as copying information onto a memory stick and walking out of the office with it. Data protection strategies need to classify and define data leakage risks specific to an organisation, with email security top of mind.

With effective policies and rules in place, data leak prevention technology can scan all incoming and outgoing information for a number of pre-identified triggers. This may include keywords, phrases or other references, which need to be built into the definitions for data leak prevention. These definitions are then applied to users, and provide instructions for the system as to what actions to take should the email be flagged. This could include capturing the mail to prevent its release, notifying the individual or a manager for a decision on release, or, if the information contained is highly confidential, the email can be deleted or redirected as required.

Rules and policies also need to be constantly adapted and refined, in order to ensure they remain relevant and continue to fit the business and its requirements. The aim of data leak prevention is not to generate masses of false positives, but to narrow in as closely as possible on only those emails that are in breach of policy.

Creating a chain of custody

When looking for a data leak prevention solution for email, organisations should first and foremost identify a solution that will enable them to create a complete chain of custody or audit trail of the email information. This requires a solution that consolidates all of the necessary channels into a single, integrated platform.

The complete audit trail will show exactly what actions were taken by data leak prevention, where email was sent from and to, and more. In addition, organisations should look for flexibility and the ability to define custom policies as required by their individual business. Further features to look for include the ability to encrypt sensitive documents on the fly, preventing data leakage without blocking the email, but by putting additional controls in place.

Ultimately, email is an essential business tool that is in widespread use for corporate communication both internally and externally. While people are often to blame for data leakage, it is impossible to entirely control on a human level. Thus, data leak prevention technology is critical to help businesses control the flow of confidential information and prevent sensitive data from falling into the wrong hands, either accidentally or intentionally.

ABOUT THE AUTHOR

Simeon Tassev, director of Galix, reseller of Mimecast Solutions in South Africa