



Whitepaper

Data Leakage Prevention

- Protection of Outbound Email Communication -

Expertise matters

Contents

1	The Underestimated Danger	2
2	Measures for Secure Outgoing Communication	2
2.1	Checking Outgoing Attachments	3
2.1.1	Example: Protection of Engineering Drawings	3
2.1.2	Example: Sending Electronic Invoices	3
2.2	Checking Outgoing Message Contents	4
2.2.1	Analyzing Legally Binding Declarations of Intent	4
3	Further Protective Mechanisms.....	6
3.1	Analyzing the Email Traffic	6
3.2	Encryption of Outgoing Communication	7
4	Conclusion.....	8

1 The Underestimated Danger

Speaking of email security, one often only thinks of protection against viruses and spam. Typically, while many companies focus on the incoming communication, few are those who think about the risks involved in uncontrolled communication to the outside world.

But practice shows that problems are increasingly caused by the loss of sensitive information, the careless disclosure of personal data and non-compliance with legal provisions such as the protection of customer data. In this context, data leakage prevention (DLP) has become a major concern and key priority for many companies and organizations essentially concerned with data protection issues and protecting their know-how.

Regarding email communication, this means looking at the email traffic from a process point of view. The issue is to identify hazards in time to respond in a proactive and efficient way.

2 Measures for Secure Outgoing Communication

iQ.Suite is a solution that effectively protects the entire email traffic – be it incoming or outgoing – in many ways. It does this with all operational and legal aspects taken into account and implemented in an overall business process. This integrated approach avoids disrupting the email communication and actually is the essential starting point for defining and applying a targeted DLP strategy.

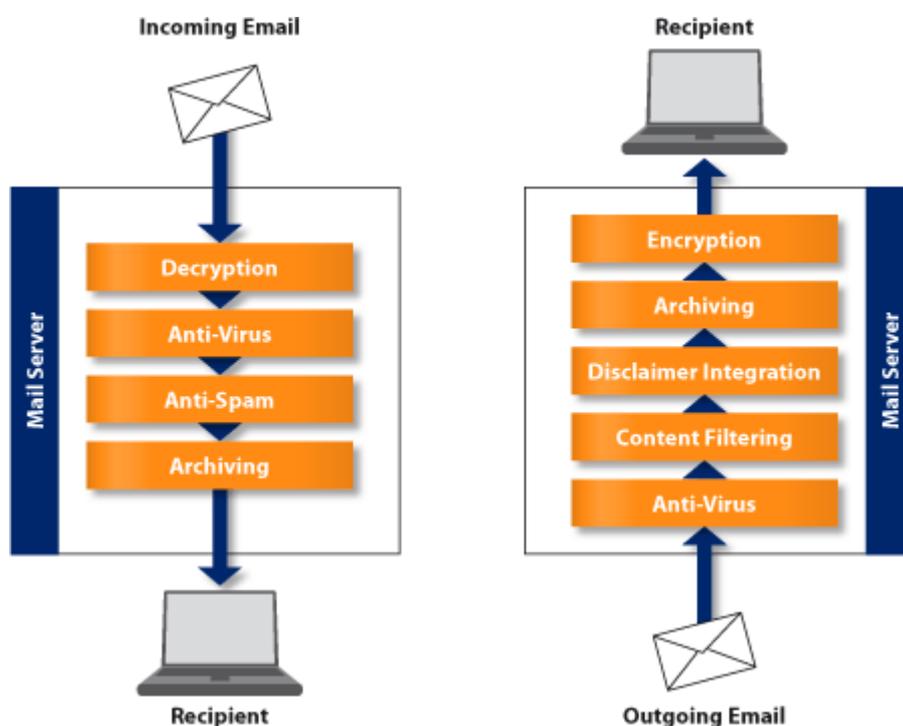


Illustration 1: Incoming and outgoing email communication

2.1 Checking Outgoing Attachments

Email attachments quite often contain sensitive information and corporate knowledge, be it in the form of quotations, contracts or specifications. And usually sending this sort of data in an uncontrolled manner is not consciously intended.

This is where iQ.Suite comes in with an electronic fingerprint-based technology, which reliably identifies file formats regardless of the file extension. Currently, the software provides out-of-the-box capability to analyze over 300 formats, with further file formats added as required. Thus, this technology represents an important solution component for the protection of confidential data.

2.1.1 Example: Protection of Engineering Drawings

Engineering drawings often include important technical innovations or patent-relevant information, which plays a critical role in high-tech industries such as aerospace and automotive. iQ.Suite recognizes the underlying file formats (e.g. from AutoCAD, CATIA, Pro/Engineer etc.) and processes them according to applicable organizational policies. The software provides a number of processing methods that can be individually adjusted to the company's specific needs.

Possible actions include:

- Block specific file formats for all outgoing emails
- Define exceptions for dedicated communication channels
- Statistics on the frequency of detected restrictions
- Detected restrictions report to third parties (e.g. security officer)
- Automatic email encryption
- Email notification to all senders involved
- Make the sending of critical information subject to four-eye principle

2.1.2 Example: Sending Electronic Invoices

For cost and convenience purposes, many companies have implemented electronic invoicing methods, as email has proven to be a reliable and quick carrier for exchanging data, including invoices. In this context, it may be necessary to implement intelligent mechanisms to control the sending of such invoices, which are often attached to the email as PDF file.

iQ.Suite is able to recognize file types such as Invoice.pdf and process them according to specific rules. In case emails come automatically from an ERP system, it is possible to have them processed by iQ.Suite through the mail server or an SMTP gateway.

Various actions can be taken when one of these file formats is found, including:

- Block these file formats for all outgoing emails
- Block entire emails that include these file formats
- Define exceptions for dedicated communication channels
- Statistics on the frequency of detected restrictions
- Detected restrictions report to third parties (e.g. security officer)
- Automatic email signing
- Email notification to all senders involved
- Make the sending of such information subject to four-eye principle

2.2 Checking Outgoing Message Contents

Every day, countless orders, invoices, delivery terms and order confirmations are being sent by email. These documents normally have a legally binding character, which means they involve the liability of the company or the sender.

In addition, industry-specific requirements make increasing demands on the protection of sensitive contents. For instance, a major issue in the health care sector is to guarantee the protection of patient records against unauthorized access, while the financial sector is primarily concerned with the protection of balance sheets and financial data.

Whenever they entrust data to a third party, customers and partners will rely on their data being protected. Therefore, it should go without saying that this protection also extends to email communication.

With iQ.Suite, you can check emails for specific words, strings and text modules in over 300 file formats, thus effectively providing a comprehensive, permanent and reliable recognition of message contents.

2.2.1 Analyzing Legally Binding Declarations of Intent

Each sector has its typical specific keywords used to define and describe daily processes. Due to its high level of flexibility, iQ.Suite is able to take into account these specific features and analyze emails accordingly with the help of weighted word lists or dictionaries.

These dictionaries can be compiled by sector, company or even department. This ensures, for instance, that technical terms are taken into account in the proper way and that email communication is implemented and performed in accordance with corporate policies.

Various actions are available, including:

- Block entire emails that contain specific words/phrases
- Define exceptions for dedicated communication channels
- Statistics on the frequency of detected restrictions
- Detected restrictions report to third parties (e.g. security officer)
- Automatic email encryption
- Email notification to all senders involved
- Make the sending of such information subject to four-eye principle

3 Further Protective Mechanisms

Besides the scenarios mentioned above, a number of other aspects also play a decisive role in the protection of the email communication. For instance, collecting and analyzing information on communication streams is a crucial point, as it provides insight into the communication behavior and facilitates the detection of anomalies.

Any comprehensive security strategy will also include the automatic encryption of sensitive information, in particular taking into account the needs of communications partners in the fields of B2B and B2C. Again, iQ.Suite provides the means to reliably implement such a strategy.

3.1 Analyzing the Email Traffic

To implement a consistent email process, you definitely need to know which data periodically arrives in and leaves the company. In addition, it is crucial to fully control aspects such as the protection of data and the efficiency of email communication. Also indispensable is a precise knowledge of your own email infrastructure.

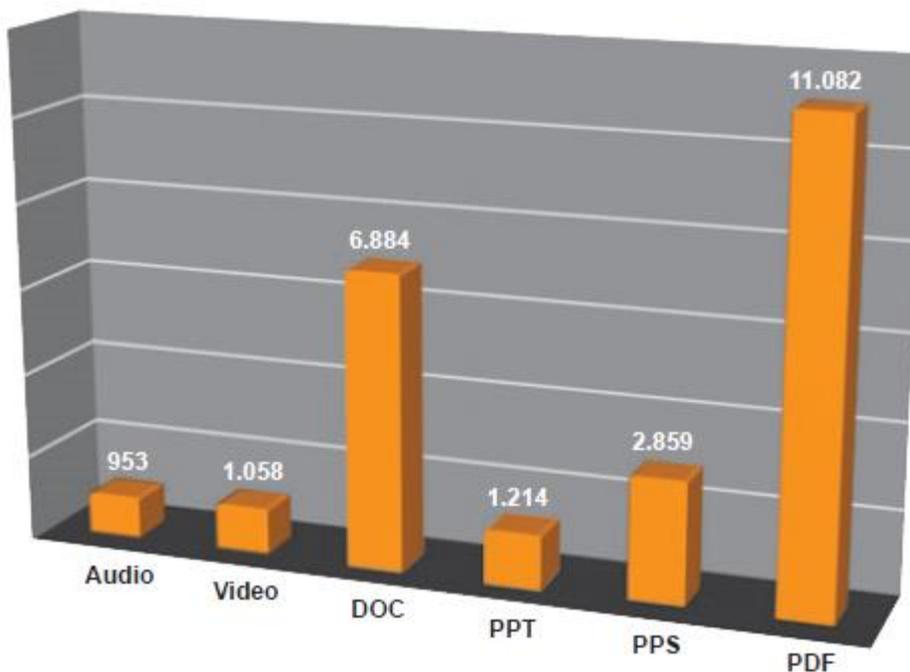


Illustration 2: Number of Outgoing Attachments

With iQ.Suite, GROUP Business Software provides this kind of comprehensive overview. The solution allows analysis of the entire email traffic and records a multitude of parameters needed to evaluate the use of email, such as for instance the type and size of attachments.

The results obtained can be used in a multitude of ways:

- Comprehensive analysis of the actual email communication
- Detection of violations of email policies
- Evaluation of the email traffic, e.g. as regards file types sent
- Systematic security checks and risk reduction
- Increased efficiency and optimized email processes
- Increased productivity and reduced cost of ownership

3.2 Encryption of Outgoing Communication

Everybody knows the analogy: Sending an email is similar to sending a postcard – unsecured, readable and accessible by anyone. Obviously, this cannot be in the interest of companies. What they need is a set of mechanisms that protect the company’s know-how and customer data.

Email encryption offers this kind of security by effectively protecting the email against unauthorized access on its way to the recipient. While this is undisputed, the necessary use of a multitude of keys and certificates has made this approach a rather challenging undertaking in the past.

With iQ.Suite, GROUP Business Software has eliminated the complexity of email encryption. As a matter of fact, the key to higher efficiency and ease of use was to abandon a client-based procedure, as server-based methods are the only way to relieve the workload of employees while providing the required level of security.

iQ.Suite offers two options for email encryption:

1. In the field of B2B communication, iQ.Suite Crypt Pro allows to secure email communication through a set of rules and a server-based email encryption method. Whether PGP or S/Mime – iQ.Suite Crypt Pro supports both key-based technologies and certificates. The emails are consistently encrypted according to predefined rules – without any interaction required from the end users. To enable a highly flexible control of encrypted communication, the software can be configured to dedicated rule for each recipient.
2. In the field of B2C communication it is not always possible to implement specific methods, as recipients usually do not have their own encryption solution. To ensure the necessary confidentiality when sending sensitive data in this kind of environment, GROUP Business Software offers another encryption solution – iQ.Suite WebCrypt Pro – that does not require any keys or certificates. And best of all: All the recipient needs to display encrypted messages is a web browser. This allows companies to send encrypted emails to any customers or partners.



4 Conclusion

In today's world, data leakage prevention should be on the agenda of any IT officer and business manager, as a reliable protection of corporate know-how, customer data and competition-relevant information can only be ensured through elaborate DLP strategies. For email communication, this means implementing a consistent email process that takes into account all aspects of electronic communication – including both incoming and outgoing emails.

The decisive issue is to comply with operational and legal requirements, some of which may be further detailed by industry-specific regulations. It is only when all of these aspects are integrated into the email process that emails and their contents are effectively and reliably protected.

About GBS

GROUP Business Software is a leading vendor of solutions and services in the fields of messaging security and workflow for the IBM and Microsoft collaboration platforms. Over 5,000 customers and more than 4 million users worldwide trust in GBS expertise. The company operates in Europe, North America and Asia.

Further information at www.gbs.com

© 2016 GROUP Business Software Europa GmbH, All rights reserved.

Our product descriptions are of a general and descriptive nature only. They do not stipulate any specific features nor do they represent any form of warranty or guarantee. We reserve the right to change the specifications and design of our products without notice at any time, in particular in order to keep abreast of technical developments. The information contained in this document presents the topics from the viewpoint of GBS at the time of publishing. Since GBS needs to be able to react to changing market requirements, this is not an obligation for GBS and GBS cannot guarantee that the information presented in it is accurate after the publication date. This document is intended for information purposes only. GBS does not extend warranty for this document, in either explicit or implied form. This also applies to quality, execution, standard commercial practice or suitability for a particular purpose. All the product and company names that appear in this document may be trademarks of their respective owners.