zivver

Digital communications essentials

The why, what and how of email and file transfer security

Knowledge Article

Table of Contents

01

Why, what and how of email and file transfer security

- Why email is and will remain important
- Email and file transfer security, explained
- What are the risks of data leaks?
- The advantages of enhanced email and file transfer security
- Five ways email security can boost business value

02

The key to data leak prevention: Identifying errors before they occur

- Outbound email security prevents data leaks
- Most data leaks happen before sending

03

Ensuring compliance by protecting messages from unauthorized access

- Compliancy comes with serious challenges when using outbound email

04

Data leak identification, message retraction and behavioural insights

- Financial benefits of preventing human error

05

Control and continual improvements

- The importance of having visibility over business email usage
- Measures required to be in control

06

What sets Zivver apart

- A user-friendly compliance solution with advanced encryption and two-factor authentication
- Take the next step in safe email communication

Why, what and how of email and file transfer security

Practically every organization requires a secure method of sending emails and transferring files to customers or other contacts. There is often, however, a lack of awareness in how best to safeguard that data within the organization, let alone how to exchange information while complying with GDPR and similar regulations.

In this whitepaper, we will delve into the fundamentals of email and file transfer security, while exploring:

- The increased need for more robust and modern email security solutions
- A modern and user-friendly solution
- What securing outbound email and file transfers actually entails
- How securing outbound emails can help address operational challenges;
- And the true value of email security.

The needs for strengthening email security can vary significantly within organizations. While some will champion adopting stringent email security practices, others may require more convincing. Many people are simply unaware of the positive impact that enhanced email security measures can bring across an entire organization.

Why email is and will remain important

On average, employees spend over two hours per day, dealing with 130 business emails. Research of the Radicati Institute[1] shows that over 300 billion emails are sent per day.

Why email is popular and widespread

Standardization: Email is built on top of various official, public standards or so-called RFCs, like SMTP, IMAP and many more. Standardizations enable vendors who develop tools with unique features to align to the needs of users without impacting how the recipient receives the communication. This is similar to telephone communication; due to industry standards, consumers can select a provider that suits their needs, without consideration of the underlying technology.

Simplicity: Today, the number of email users has already surpassed 4 billion. As the email ecosystem has matured, improving usability has become the central tenet.

Habit: Until the emergence of WhatsApp, email was the only digital communication solution available to a mass global audience. Due to its simplicity, it was widely adopted by users and businesses as their primary method of digital communication. Although the limitations of email are well-known, the push to change the status quo is hindered by the fact that habits are hard to change. In the case of email, both the behaviour of users and recipients need to adapt to ensure better security. When you need to influence changes in habit outside your own environment, it becomes exponentially more challenging to implement.

Approx.

130

emails are handled every day by workers

Approx. over

300 billion

emails are sent worldwide, every day

The number of emails sent annually is increasing at a rate of

4%

Approx.

8%

of all emails are sent unencrypted

Email and file transfer security explained

According to Gartner[2], "Email security refers collectively to the prediction, prevention, detection and response framework used to provide attack and access protection for email". Or, put simply, anything to prevent data leaks related to the use of email. IT-minded people tend to interpret email as the technology behind it, like SMTP. Preventing data leaks stemming from emails, however, requires looking at email as a 'use case'; how do various people use it and for what purpose(s)? Of course technology is important, but exists only to support the use case.

"Secure email" vs "Securing a way of working"

When organizations need 'secure email' they express an intention to 'secure' (in their view) their way of working. This may include the use of current communication tools for email, such as Outlook, without any consideration of the underlying technology. Sharing files, and thus file transfer security, is increasingly becoming an essential component of the email use case.

Many email vendors have traditionally restricted attachment sizes to 10 MB per email. This meant that sharing large files necessitated using other platforms. **With increasing file size limits, including up to 5 TB with Zivver, users no longer need to switch platforms if they want to send a file that would normally exceed the email server limit.**

Email was not initially built with security or user privacy in mind

While this may come as a surprise to some, email communication was not developed with security concerns in mind. The first versions of email originated during the 60s, a time when security and privacy protection concerns were effectively nonexistent.

Subsequent attempts have been made to enhance the security of email, with transport encryption (STARTTLS), mail server authentication (DANE), and spoofing and spam protection (DMARC, SPF, and DKIM) becoming global standards. Most of these features, however, are optional. They are not widely adopted and fail to address challenges like phishing or lack of user authentication. What's more, these technical standards were not designed to mitigate the single biggest cause of data leaks, human error.

What are the risks of data leaks?

Since the introduction of GDPR, every EU country must report all privacy sensitive data leaks to their respective industry watchdogs.

Analyzing the causes of data leaks from different reports, they reveal that the vast majority of data leaks are not cyber-related. In the UK, reports from the ICO routinely show that over 80% of data leaks were non cyber-related. Meanwhile other countries such as the Netherlands tell a similar story, with upwards of 90% of data leaks stemming from human error, and largely preventable.

The top reasons for inadvertent mistakes when using email include:

- Sending the information to the wrong recipient;
- Adding the wrong attachment;
- Exposing recipient information via the To or CC fields, when BCC should have been used;
- Unauthorized access to data, usually due to weak passwords and lack of two-factor authentication.

The advantages of enhanced email and file transfer security

Email security is primarily about preventing data leaks. It is important for an organization to first determine if the security measures they introduce will serve a specific purpose, or whether they will be implemented solely for compliance reasons. If data leak prevention and/ or compliancy is the core objective, they will need to determine if an email security solution can effectively address the following:

- Increase employee awareness: Cited as one of the most important measures in GDPR and similar legislation, awareness is the key to targeting the primary source of most data leaks, unintended mistakes by human error.
- Prevent misaddressed emails: The number one cause of data leaks.
- Prevent unintended sharing of sensitive data: This umbrella category accounts for 95% of all data leaks.
- Ensure BCC is used properly: In the UK, ICO data breach trend reports even lists this data leak cause separately, given its frequent occurrence and potential impact.
- Protect from unauthorized access: The ultimate goal of all legislation related to privacy protection.
- Apply data retention policies: A specific measure that is a key component in legislation such as GDPR.
- Guaranteed message encryption: Email encryption is opportunistic, meaning it tries to deliver an email encrypted, and if that is not possible, it will deliver the message unencrypted. Having guaranteed encryption is important for compliance to GDPR, HIPAA, etc.
- Limit the impact of data leaks: GDPR-like legislation requires organizations to have measures in place to safeguard against data leaks and have a capacity to mitigate when they do occur.
- Identify risks: This is the ability to have insight on how to improve security, which is essential for enhancing security standards and compliance.
- Measure the effects of measures: Improving security is about applying measures and assessing their effectiveness, always with an eye on how things could be better.

Five ways outbound email security can boost business value

While many people think of email security as defending an organization against phishing, malware and hacking attempts, these no longer pose the biggest threat. Interestingly, the use of email encryption could not have prevented any of the reported data leaks according to public records. Consequently, focusing primarily on email encryption is ultimately for compliance reasons only.

Preventing data leaks from occurring requires organizations to increase their efforts on outbound email security and defend against unauthorized access with two-factor authentication. If done in a way that is user-friendly while being simple to implement and maintain, organizations can unlock business value in areas such as:

- Increased productivity
- Cost savings
- Reduced need for costly and ineffective customer portals
- Brand enhancement

The key to data leak prevention: identifying errors before they occur

Preventing data leaks should be a top priority in any organization. This helps to ensure compliance with the GDPR or similar legislation, protect the company reputation, plus prevent fines and save on other costs associated with having a data leak.

Outbound email security prevents data leaks

On average, employees spend over two hours per day, dealing with 130 business emails. As data leak statistics show that most data leaks happen in the process of sharing information, outbound email security is a must have for every organization. Outbound email security should help organizations to prevent data leaks before, during and after sending.

Most data leaks happen before sending

Most people believe that hacking and phishing are the main causes of data leaks. Reports on data leaks, however, show that the vast majority of data leaks derive inadvertently from mistakes internally, rather than malicious external behaviour.

Internal mistakes are mostly caused by:

- Auto completion functionalities of email
- Attaching a file that contains sensitive information the sender is unaware of
- Exposing recipients contact details by failing to use BCC
- Unawaredly sharing information in the body of emails which is sensitive

Security solutions designed to raise employee awareness should cover the entire spectrum of the communication journey. Below is an example of how this works in practice with Zivver:

- Real-time classification: While the email is being composed, the system will classify the type of information users intend to share. This applies to both the email text plus any attachments. The out-of-the-box AI and dictionary-based classifiers are used to detect medical, legal, financial or personal information, as well as social security or credit card numbers, for example.
- Raising user awareness: Based on the assessment, the user is notified about any anomalies before the email is sent. This notification method is either fully integrated in the email client while composing, or by actionable notifications via email. Email client integration is currently available with Outlook Desktop, Outlook Online (Office 365) and Gmail. Other email clients are supported on the server side.
- Seamless contextualization: The recipients addressed in the To, CC and BCC fields are analyzed and scanned to assess if the message or attachments pertain to specific people or organizations.
- Communication evaluation: Based on the analysis, each email is evaluated for:
- Unintended content (‘Attachment A contains social security numbers, is that intended?’)
- Unusual recipients (‘You have never shared medical information with John Doe before; are you sure?’)
- Non-compliant security measures (‘You are about to share sensitive financial information; follow recommendations to protect your email?’).

Ensuring compliance while protecting messages from unauthorized access

Compliancy comes with serious challenges when using outbound email In article 32 of the GDPR, it states that organizations are responsible to prevent “unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed”. Similar responsibilities are also described in ISO27001, HIPAA, PCI-DSS. Compliance requires three types of security measures, each with their own challenges:

- Secure transport of messages: Secure email transport via STARTTLS is considered a very basic security measure. Nonetheless, 8% of emails are sent unencrypted[3]. Although this seems easy to solve, email security has two weak spots:
  - Email transport security is opportunistic: STARTTLS is an opportunistic protocol. It tries to deliver an email encrypted. However, if that is not possible it will deliver it unencrypted.
  - Email server identity spoofing: The DNS-lookup is intercepted and gives a faulty response back through an IP-address of another email server than that of ‘organization.com’. The email will be delivered to an unintended recipient.
- Secure storage of messages: On-premise email servers require installing additional tools and plugins to encrypt email. Email cloud providers usually support encryption of data out-of-the-box. However, most cloud providers still have access to private keys. It’s important to note that GDPR and HIPAA put the onus on the actual sender to properly protect data.
- Authenticated access to messages: Authentication is, by nature, distinct from email. Unlike many other email service providers, Zivver provides two-factor authentication (2FA). This is a helpful step-up for standard email security, as 86% of all passwords used[4] are still easy to hack.

Data leak identification, message retraction and behavioural insights

There has been a data leak – now what?

Mistakes will understandably happen occasionally, but there are solutions available to help organizations mitigate the risks of a data leak. Having the right tools in place can drastically reduce the risk, support employees in achieving effortless data security, and help mitigate the impact when a potential data leak occurs.

Time is of the essence and the ability to mitigate data leaks is vital

To mitigate the risk of data leaks and ensure compliance, email security solutions need to include the following options:

- Real-time behavior and communication logging: Any solution should provide real-time logs of the communication activity of its users and make that available to admins. This includes ignored business rules, communication partners, attachment types etc. With these logs, organizations can identify near real-time risks via the solution or integration of these logs with Security Incident and Event Management (SIEM) systems.
- Retracting messages: Users should have the ability to retract messages, including any attachments. This useful feature helps to contain potential data leaks.
- Insight into information access: For every message, both senders and their organizations should have insight into who accessed or retrieved the message and its attachments. This gives stakeholders a clear insight into whether the risk was mitigated in time or what the potential impact of a data leak could be.

The following additional functionalities are essential to comprehensive outbound email security:

- Identification of a potential data breach: Organizations must take action to prevent data breaches. This not only includes preventative measures, but also the system capacity to identify potential data leaks. Proper and swift identification of leaks can mitigate their impact while containing it to prevent further escalation and damage.
- Mitigate adverse effects: Once a data leak has been identified, organizations should be able to take immediate action to mitigate any adverse effects. This is also an explicit GDPR requirement.
- Insights on impact: When a data leak occurs, understanding its impact is crucial; this will help determine how best to contain it. The organization must also inform internal and external stakeholders, including pertinent authorities, and the data subject, as stipulated under the GDPR.

Financial benefits of preventing human error

IBM research shows[5] that data leaks on average cost more than $3.9 million (USD. Three grounds for fines under the GDPR and similar legislation include:

- Failure to report data breaches in a timely manner
- Failure to inform appropriate stakeholders on the impact of the data breach, or
- Failing to demonstrate the capacity to effectively mitigate the adverse effects of the breach.

Average cost of a data leak caused by human error is $3.9m (USD)

Control and continual improvements

Legislators recognize that while it is impossible to completely eliminate all data leaks, significantly improving security measures should remain a priority for organizations. That is why GDPR-like legislation puts a lot of emphasis on the checks and balances organizations must have in place to detect data leaks, identify risks and be able to measure the effect of any steps taken to improve security.

The importance of having visibility over business email usage

Increasingly organizations have implemented systems to monitor inbound emails and any corresponding threats. While most people consider hacking and phishing to be the main causes of data leaks, the vast majority of data leaks are a result of internal instead of external threats.

In the UK, 79% of all data leaks are caused by employees making mistakes[6], while over 40% of the reported data leaks were caused by sending information to the wrong recipient. In the Netherlands, misaddressed information accounts for 63% of data leaks[7].

All privacy-related legislation cite that timely identification of data leaks, including errors made by employees, must be reported swiftly to national authorities. With the GDPR this must be done within 72 hours. Aside from reporting capabilities, organizations must also demonstrate that they are able to routinely identify risks, create and implement plans to mitigate those risks, plus have the ability to measure the impact. As one can imagine, many organizations find adhering to these requirements challenging from both an organizational as well as technical perspective.

Measures required to be in control

There are various measures organizations need to be in control of in order to comply with legislations:

- Accurate logging: Having detailed insights with the ability to investigate the logging data forms the basis of control. Naturally the items in the logs should be both valuable (logging only relevant data) and timely (the closer to real-time the better).
- Anomaly detection: With an ever-increasing number of applications and items logged, it can be hard to gauge what is and isn't relevant. Being able to effectively detect anomalies is crucial for timely risk and data leak identification.
- Alerting: No one wants to be looking at data logs all day. That is why it's important to be alerted when anomalies or events that are considered to be of interest actually occur.
- Analytics: Having logging is great, but ultimately it is about what the logs mean or what you can derive from them. Having analytics that provide effective insight is essential to identify risks and foster a learning organization.
- Actionability: Ultimately improving security and limiting the impact of data leaks is about taking actions. Tools which suggest and monitor actions are valuable for any organization.

Empowering organizations and people with effective tools

Organizations can be well equipped to secure their outbound email with tools to identify security risks, privacy risks, non-compliance as well as best practices. These tools include (exportable) logs and statistics.

With Zivver, customers have full visibility of the following:

- Communication patterns: Organizations and users have insight into communication behavior, including what type of information is shared with who, how the information was secured and whether it was in accordance with organizational policies.
- Read status: Both senders of messages, as well as the organization (admin), have insight into whether messages and attachments have been accessed by recipients. This insight can help to determine the impact of a (potential) data leak.
- User logins: Users and admins can see login behavior of users including information on type of device, IP address and type of authentication.
- Admin actions: See which settings were changed or what information was accessed by admins.

Take the next step

Zivver makes achieving digital communications security effortless. No complicated processes, no extra steps; Zivver fits seamlessly with existing workflows, making security best-practice second nature.

Powered by machine learning technology and advanced encryption, Zivver protects emails and attachments before, during and after hitting 'send'. Flawless integration with Gmail and Outlook enables users to share confidential information without leaving the comfort of their familiar email client.

Designed to deliver an effortless user-friendly experience for both the sender and recipient, Zivver empowers users to secure their organization's most valuable digital assets.

Sources:

1: https://www.radicati.com/wp/wp-content/uploads/2018/12/Email-Statistics-Report-2019-2023-Executive-Summary.pdf

2: https://www.gartner.com/en/documents/3938516/market-guide-for-email-security

3: https://transparencyreport.google.com/safer-email/overview

4: https://www.troyhunt.com/86-of-passwords-are-terrible-and-other-statistics/

5: https://transparencyreport.google.com/safer-email/overview

6: https://ico.org.uk/action-weve-taken/data-security-incident-trends/

7: https://ekker.legal/wp-content/uploads/2019/10/meldplicht_datalekken_feiten_en_cijfers_1e_helft_2019.pdf

Zivver

+44 (0) 203 285 6300
contact@zivver.com

www.zivver.com