Reducing The Risk Of Email Data Breaches

by
Nick Offerman
nick.offerman@os3.nl

Assessor: Cees de Laat
Supervisor: Remco Boersma

University of Amsterdam
Ministry of Justice and Security

March 24, 2019
Abstract

Since the European Union (EU) approved the General Data Protection Regulation (GDPR) privacy law, there is an increased need to prevent data breaches. This project will investigate how the Ministry of Justice and Security (MJS) can be more compliant with the GDPR by improving the security of the email environment since many data breaches occur via inappropriate use of email by the human factor. This research will show the differences between email security protocols and commercial secure email solutions, and which technical challenges these solutions bring for the IT architecture and security architecture of the MJS. This project will investigate how the MJS can be more compliant with the GDPR by improving the security of the email environment.

Keywords: email, security, protocols, solutions, GDPR, privacy
Contents

1 Introduction 3
  1.1 Research Questions ........................................ 4

2 Related work 4

3 Method 5
  3.1 Scope .......................................................... 5
  3.2 Restrictions ..................................................... 5
  3.3 Approach ........................................................ 5

4 Results 5
  4.1 Which conventional email security protocols are available? ................. 5
    4.1.1 Spam, phishing, and spoofing protection .............................. 5
    4.1.1.1 Sender Policy Framework (SPF) .................................. 6
    4.1.1.2 DomainKeys Identified Mail (DKIM) ............................... 6
    4.1.1.3 Domain-based Message Authentication, Reporting Conformance (DMARC) .......................................................... 6
    4.1.2 Hop-by-hop email encryption ....................................... 7
    4.1.2.1 START Transport Layer Security (STARTTLS) ..................... 7
    4.1.2.2 DNS-based Authentication of Named Entities (DANE) ............... 7
    4.1.3 End-to-end email encryption ..................................... 7
    4.1.3.1 Pretty Good Privacy (PGP) ..................................... 7
    4.1.3.2 Secure Multipurpose Internet Mail Extension (S/MIME) ........... 8
  4.2 What are the characteristics of commercial secure email solutions? .......... 8
    4.2.1 Commercial secure email solutions comparison ........................ 8
    4.2.2 Sophos SPX .................................................. 9
    4.2.3 ZIVVER .................................................... 10
  4.3 Which technical challenges do commercial secure email solutions bring for the IT architecture and security architecture of the MJS? ......................... 11
    4.3.1 Cloud-related concerns ........................................... 11
    4.3.2 Malware inspection ............................................. 11
    4.3.3 Encryption .................................................. 11

5 Conclusion 12

6 Discussion and future work 12
1 Introduction

Personal data is information related to a person that can be used to identify them, e.g. location data, name, physical attributes, identification numbers, and health information [1]. The European Union (EU) approved the General Data Protection Regulation (GDPR) privacy law since 25 May 2018 [2, 3]. The GDPR is a regulation law on protecting the data privacy rights for all European citizens. As a result, EU citizens have more control about their data, and companies are more responsible for protecting the data [4]. A data breach is a security incident in which information is accessed without authorization [5]. The GDPR reserves that organizations are responsible for preventing data breaches and data breaches should be reported within 72 hours to the supervisory authority [6, 7]. Organizations who fail to meet the requirements of GDPR are fined up to €20 million, or 4 % of the annual turnover, depending on the impact, and the behavior of the organization [8, 9]. The highest fine was given to Google in 2019 of €50 million, due to the lack of transparency regarding their services, and by wrongly process data for personalized advertising [10]. Many data breaches occur by inappropriate use of email by the human factor [11, 12]. According to the Autoriteit Persoonsgegevens, the government was responsible for 20% of data breaches per sector in the Netherlands in 2018 [13]. According to the same report, 63% of the data breaches in 2018 was caused by sending email or handing over personal data to the wrong recipient.

Email is an essential factor of nowadays communication, since the existence in 1971 [14, 15]. Approximately 4.9 billion email addresses are registered [16], and there are around 7.5 billion people worldwide [17]. While both numbers continue to grow [18, 19], the number of reported data breaches also increase annually [4, 20]. According to Kroll, the number of data breaches increased 75% in 2017/2018, claiming that the following sectors are mainly responsible for the data breaches: health, business, education, and the government [21]. The human factor causes the most data breaches, and not particularly malicious acts of hackers [22, 23]. It is likely that data breaches lead to customer identity theft, and reputation damage for many organizations [24, 25]. The problem with the SMTP protocol is that it does not have any encryption mechanisms built in [26], since their existence in 1982 [27]. This means that email is sent plaintext over the network [28], so anyone who (wrongly) receives an email, is able to read it.

Figure 1: Email security threats [29].

Figure 1 shows what happens when sending an email. Administrators can control how secure the communication will be within the Local Area Network (LAN). Email has an increased risk when communicating over the internet since nation-state actors may be listening in on the internet [30]. Email is also less secure once it is received by the IT infrastructure of the company of the receiver, since the IT infrastructure may be affected by viruses, malware or hackers [31]. Moreover, email may be accessible by administrators of receiving e-mail servers.

The Ministry of Justice and Security (MJS) is responsible for public safety, imprisonment, and justice in the Netherlands [32, 33]. The MJS facilitates around 90,000 employees, of which approximately 45,000 employees are from the justice part, and about 45,000 employees are from the security part of the ministry. The MJS has to be compliant with the GDPR since it processes data from European citizens. The main focus of this research lies on ways to reduce the risk of
email data breaches because the human factor causes the most data breaches using email [13].

Sector of the MJS uses a Windows environment with Outlook for emailing to internal employees and external organizations. The MJS email with companies like Organisation of the Public Prosecution Service (Openbaar Ministerie), The Council for the Judiciary (Rechtspraak), Law enforcement in the Netherlands (Politie), and Dutch Association of Mental Health and Addiction Care (GGZ Nederland). The MJS facilitates a WiFi-environment with a direct internet connection for BYOD, which is physically separated from the internal LAN for security purposes. Email is sent plaintext to people in- and outside of the organization, but classified documents can be securely transferred via the ‘Bestandenpostbus’ which is an application for exchanging files, rather than an email solution. The SOC of the MJS scans incoming email using FireEye, which analyze the content of email messages in a sandboxing environment for malicious code like spam and malware, before being sent to the end-user.

Multiple dedicated market solutions have been developed which provide both user awareness, and email encryption. Sectors of the MJS are curious why relative new email solutions gaining much popularity over conventional security protocols like PGP, S/MIME, and STARTTLS, which exists for many years. The MJS tries to keep the multiple solutions as limited as possible without having to make links with a multitude of providers because the MJS will eventually need to support all these solutions. Supporting various dedicated market solutions is inefficient since it will increase the management burden for the company. Also, the interoperability between different solutions can be a challenge for both the administrators and end-users. The MJS expect the following of a secure email solution:

- emails are sufficiently protected against unauthorized access
- only the recipient has access to the information
- the functionality and user-friendliness is comparable with normal unsafe e-mail
- the ability to look into employees emails in case of fraud
- scanning incoming email for malware inspection
- full control over the infrastructure with the ability to troubleshoot

Via this project, the MJS want to know more about the differences between email security protocols and commercial secure email solutions, and which technical challenges these solutions bring for the IT architecture and security architecture of the MJS.

1.1 Research Questions

Based on the introduction, the main research question is defined as follows:

How to reduce the risk of email data breaches for the Ministry of Justice and Security in order to be more compliant with the General Data Protection Regulation?

To answer the main research question, the following sub-questions are defined:

1. Which conventional email security protocols are available?
2. What are the characteristics of commercial secure email solutions?
3. Which technical challenges do commercial secure email solutions bring for the IT architecture and security architecture of the MJS?

2 Related work

Kevin M. Gatzlaff et al. outlined possible risks and effects of data breaches on companies [34].
M. Tariq Banday did research on the limitations of e-mail security protocols and their effectiveness in e-mail servers. It also shows the results of their reliance on e-mail systems [35].
Ian David Foster evaluate the security provided by conventional secure email protocols and researched the effectiveness of provider-based email security [36].
The NEderlandse Norm (NEN) set up regulation (NTA 7516) on behalf of standard development for the safe exchange of healthcare data [37].

Less research was found about commercial secure email solutions and the technical challenges which may arise for companies implementing these solutions.
3 Method

This section describes the scope, restrictions, and approach of this research.

3.1 Scope

The goal of the project is to map out the possibilities to reduce the risk of email data breaches for the Ministry of Justice and Security in order to be more compliant with the GDPR privacy law.

This report will look at email security and data breaches from a broad perspective to provide the MJS with a clear understanding of the security protocols, the available commercial solutions, and the challenges of end-to-end security of emails when this is provided by external parties.

3.2 Restrictions

This research will not perform practical experiments. No structured details will be released about the infrastructure of the MJS. Selecting a supplier of secure email solutions for the MJS is out of scope of this research. This research will not look at implementing secure email solutions. Since this research is limited to email security, other solutions like securely exchanging files, and chat-apps are not included in this research.

3.3 Approach

This research will outline the differences in conventional email security protocols like PGP and S/MIME. This will be done via researching relevant documents, and interviews with members of the MJS. The conventional email security protocols will be divided into three categories. The first category looks at spam, phishing, and spoofing protection. The second category looks at hop-by-hop encryption, and the third category looks at end-to-end encryption.

To determine the characteristics of commercial secure email solutions, this research first analyses the assessments from other independent reports. The providers of commercial secure email solutions which meet the requirements from the MJS will be invited for introductory conversations. The providers will have the opportunity to introduce their product, and the author objectively writes a summarized report about the characteristics of selected commercial secure email solutions relating security, prevention of data breaches, scalability, back-up possibilities, email message flow, and user-friendliness. The user-friendliness is essential since end-users will likely fall-back to an insecure solution if the commercial secure email solution is too difficult to use. The MJS find this important since the human factor is the most significant root cause in security data breaches [13], as discussed in the introduction.

In order to see which technical challenges a commercial secure email solution bring for the IT architecture and security architecture of the MJS, this research will look at the following aspects: cloud concerns, malware inspection, and encryption algorithms. The Nationaal Bureau voor Verbindingsbeveiliging (NBV), and the Security Operations Center (SOC) of the MJS will be invited to discuss the potential challenges.

4 Results

Section 4.1 contains a categorization of different conventional email security protocols. The characteristics of commercial secure email solutions are discussed in section 4.2. Section 4.3 describes the technical challenges of commercial secure email solutions for the IT architecture of the MJS.

4.1 Which conventional email security protocols are available?

This part of the report categorizes different conventional email security protocols into three categories: spam, phishing, and spoofing protection, hop-by-hop email encryption, and end-to-end email encryption, and examine to which extent these protocols are used by the MJS.

4.1.1 Spam, phishing, and spoofing protection

Spam, phishing, and spoofing protection prevent against threats like commercial advertising, identity theft, and fraud in which companies are impersonated, or by changing the 'FROM' header from an email [38]. The SMTP protocol has no validation mechanism for the From field in the email header [39], which means that a malicious user may pretend as an employee from a company, or even from a non-existent address. The following three protocols offer protection against these threats: SPF, DKIM, and DMARC.
4.1.1.1  Sender Policy Framework (SPF)
SPF prevent spam by detecting spoofed email messages via validation of the sender’s domain [40]. Domains could be authorized via SPF validation, which shows that a sender is allowed to send email from the domain it came from. The domains which are allowed to send emails are specified in an SPF record in Domain Name System (DNS).

4.1.1.2  DomainKeys Identified Mail (DKIM)
DKIM allows a sender to sign an email message by creating a hash value using the RSA-SHA256 algorithm so that a receiver could validate whether the email was sent from a valid server from the sending domain. DKIM provides information on whether an email is from a trusted domain to spam filters of the receiving domain.

4.1.1.3  Domain-based Message Authentication, Reporting Conformance (DMARC)
DMARC has been rapidly adopted by ISPs and big companies, since their existence in 2015 [41]. The goal of DMARC is to prevent the creation of emails from unauthenticated parties from your domain, which is also known as spoofing. DMARC is used in combination with existing SPF and DKIM records in order to validate the authenticity of an email message.

Before DMARC can be implemented in the organization, an inventory must be carried out on which internal and external (e.g., surveys and newsletters) mail servers, send and receive email on behalf of the company. A receiving server could be informed whether to refuse emails from a particular sender via a DMARC policy. Depending on the policy which is being used, DMARC can make sure unauthenticated emails are blocked, so suspicious emails are not being delivered to customers. It is likely that possible phishing emails are prevented by DMARC, which may reduce the risk of reputation damage, or trust-issues from customers. If an email message does not have a valid signature, it is likely that the email message will be deleted since it is considered spoofing. Domain owners could publish the following policies for emails which are not compliant with DMARC:

- none, which only collect data and send reports.
- quarantine, which handles messages with suspicion.
- reject, which blocks messages outright.

DMARC also generates reports, which shows who is sending email to, and from the domain. Many domains within the MJS have DMARC enabled in quarantine mode so that suspicious emails would end up into receiver’s spam folder in most cases. It is recommended for every domain of the MJS to have at least quarantine mode enabled. For the sectors of the MJS that have already enabled quarantine-mode, it is essential to change the quarantine policies to reject policies, so suspicious email would be thrown away before it is being sent over the network. The problem with DMARC is that the architecture of the receiver can decide for itself whether it follows these policies or not, which provides insufficient security.

According to Google, 85.9% was authenticated by both SPF and DKIM for all non-spam email that Gmail received in 2016 [42], as can be seen in figure 2. This number is an increase of the 74.7% by both SPF and DKIM in 2013 [43]. The figure also shows that 97.4% of all emails come from authenticated users.
4.1.2 Hop-by-hop email encryption

Email encryption makes the content of an email unreadable for individuals other than the receiver. hop-by-hop encryption is achieved with protocols like STARTTLS. According to the MJS, most healthcare providers force TLS to encrypt email messages with STARTTLS, and DANE.

4.1.2.1 START Transport Layer Security (STARTTLS)

The encryption occurs after the connection has been established with STARTTLS. STARTTLS transport encryption based on certificates between mail servers. Since STARTTLS is a hop-by-hop protocol, intermediate mail relay servers see email as plaintext. This creates the possibility that email can be read by unauthorized people and therefore gives insufficient privacy guarantee. Downgrade attacks are possible via a man-in-the-middle (MITM). After the sending mail server commits the STARTTLS command, the receiving mail server can respond with: ready to start TLS, syntax error, or TLS not available due to temporary reason [44]. If a MITM answers 'TLS not available due to temporary reason', then the communication will be in plaintext. Moreover, the protocol cannot be enforced if the mail server of the receiver does not support STARTTLS. So STARTTLS improves on security, but cannot enforce, and guarantee security. This indicates conflicts with privacy, security, and sharing information. DNS-based Authentication of Named Entities (DANE) can improve on this issue, by checking the authenticity of mail servers.

4.1.2.2 DNS-based Authentication of Named Entities (DANE)

DANE gives the possibility to demonstrate the validity of mail servers via self-signed certificates via DNS. With DANE it is also possible to specify which CA can issue certificates for your domain.

4.1.3 End-to-end email encryption

End-to-end encryption is more secure than hop-by-hop encryption since it encrypts between end-users, and not only between the mail servers. There are two competing standards for end-to-end encryption: Pretty Good Privacy (PGP), and Secure Multipurpose Internet Mail Extension (S/MIME).

4.1.3.1 Pretty Good Privacy (PGP)

PGP was developed by Phil Zimmermann in 1991 and has become a de facto standard for securing email [45]. Figure 3 shows that many new PGP public keys were published after the leaking of top-secret documents of the National Security Agency (NSA), by Edward Snowden in 2013. Some of these documents show that many nation-state actors are spying, or at least try to spy on citizens [46].
Some sectors of the MJS uses PGP for validation, and not encryption since there is no Outlook plugin which meets the requirements of the MJS. The past few years, PGP tried to improve the protocol by semi-automatic key creation, distribution, email encryption, and decryption [47]. Despite the improvements PGP has made, the overall key certification architecture is still the same.

4.1.3.2 Secure Multipurpose Internet Mail Extention (S/MIME)

is also a competing standard for encrypting end-to-end email messages. S/MIME is based on Multipurpose Internet Mail Extensions (MIME), and Cryptographic Message Syntax (CMS). S/MIME is built into many email clients like Thunderbird and Outlook. S/MIME make use of X.509 certificates for public key distribution. S/MIME supports digital signing and verification of the signature to guarantee the identity of the sending and receiving mail server [48]. X.509 was designed with a top-down hierarchical Public Key Infrastructure (PKI) in mind, in which intermediate CA’s are signed by root certificate authorities [49]. After the compromise of the DigiNotar CA in 2011 [50], multiple studies gave insight into the poor state of the X.509 ecosystem in general [51].

According to the MJS, public key exchange is possible in specific customized cases, but impractical to facilitate in a secure and user-friendly way for every company and end-user they communicate.

4.2 What are the characteristics of commercial secure email solutions?

This section describes the characteristics of commercial secure email solutions, relating security, prevention of data breaches, scalability, back-ups, email message flow, and user-friendliness.

4.2.1 Commercial secure email solutions comparison

RZCC made a comparison between different providers of commercial secure email solutions [52], which can be seen in figure 4.
Figure 4: Commercial secure email solution comparison [52].

The comparison is based on the following components:

- Signaling content checks if an email is supposed to be sent/encrypted based on the content.
- Address errors check if wrong recipients can read emails which are intended for someone else, e.g. wrong CC, or BCC.
- Hack protection checks whether an attacker could bypass the encryption algorithm to read messages.
- Authentication makes sure that only access is given to users that are allowed to do so. This aspect can be improved by using Two-factor authentication (2FA), e.g. SMS.
- Recall sent email means the influence a user has after sending an email?
- Awareness helps users to be more aware of information security risks.
- Logging gives an overview in which email is sent to whom; this helps with the information gathering in the event of a data leak.

According to the MJS, the most crucial factor of the commercial secure email solution needs to be user-friendliness, since it is likely that the end-users will use an insecure solution if the commercial secure email solution is too difficult to use. The MJS find this important since the human factor is the most significant root cause in security data breaches [13].

The graph shows that there are different implementations, each with its own challenges. In order to do more research, ZIVVER and Sophos SPX were invited for a conversation with the MJS for further investigation.

4.2.2 Sophos SPX

Sophos SPX is an on-premise solution, which encrypts emails to PDF files. Since it is an on-premise solution, the MJS is responsible for the uptime, and for creating backups of the commercial secure email solution. Sophos claims that it does not keep track of user data. Sophos SPX notes that upscaling is easier when purchasing a virtual appliance, instead of running an appliance on a physical machine. Sophos offers a paid ‘sandbox’ service in the cloud, which provides an extra layer of security against ransomware and targeted attacks.

Sophos SPX focuses mainly on encryption, and less about user awareness. A Data Loss Prevention (DLP) policy can be created which enables the company to monitor and restrict the transfer of files containing sensitive data, e.g. social security number, and credit cards.

Sophos SPX has a maximum email size limit of 50 megabytes for each message, including the message content and attachments. It uses AES-128 or AES-256 symmetric encryption, and the key is created, and stored by the sender. Receivers have to get the key via another medium, like SMS. There is no master key for admins since password recovery options are not available. This is a problem since companies may need to look into the employee’s mailbox on special occasions, like fraud [53]. Sophos SPX cannot recall emails after they have been sent. Of course, there is still a reduced risk of data breaches if an email is sent encrypted.
A receiver which is outside of the domain of the company, need to create an account with three security questions before email can be read. Users who fail to remember their password, need to fill in these three security questions. Or else the user cannot retrieve mail. The receiver needs an official PDF reader, like Adobe Acrobat Reader to read an email. The receiver cannot look beforehand if an email contains an attachment, or if it contains only the header image. The receiver needs to log in before it can be checked. A receiver responds via the Sophos SPX portal over HTTPS (TLS 1.2). From here the message gets encrypted, and send back to mail server of the sender.

4.2.3 ZIVVER

ZIVVER is a cloud solution which focuses mainly on user awareness of data breaches. ZIVVER is ISO27001 and NEN7510 certified, which are international security standards that contribute to the requirements of the GDPR [54]. The platform was set up for secure communication over HTTPS, and not email in particular. Integration is possible with Windows Active Directory (AD), so employees of the MJS do not have to create a ZIVVER account. A receiver doesn’t need to create a ZIVVER account to read mail. A receiver logs into the ZIVVER platform on the cloud via SMS, email validation, or a symmetric password. ZIVVER can be accessed via the Outlook plugin, or via the ZIVVER platform over HTTPS (TLS 1.2) to set up a secure connection between the user and ZIVVER.

ZIVVER uses HTTPS instead of the SMTP protocol due to limitations with e.g., real-time content checking. The content of an email is checked real-time in the cloud via HTTPS for sensitive information to provide user awareness. ZIVVER states that real-time analytics in the cloud is negligible when looking at a performance loss. ZIVVER checks the performance of their solution via an analytic tool.

Encryption takes place on the servers of ZIVVER using hybrid RSA-2048 / AES-128 encryption. ZIVVER stores the public keys of the user accounts in the cloud. The private key is partly generated by a unique Windows AD attribute from the user, so the random value of the private key is administered by the company. ZIVVER states that the private key part will be thrown away after use in memory. Due to the encryption, the content of the sent email cannot be seen in Outlook, but only in the ZIVVER platform. Outlook just shows who is the receiver of an email message. In case of a data breach, it is also possible to withdraw an email, and ZIVVER shows if someone has opened and read your email.

ZIVVER provides scalability if more resources are needed since the product uses the Microsoft and Amazon cloud. Therefore, ZIVVER can upscale their service horizontally easily. Every mail runs via the ZIVVER platform in the cloud, and not directly via sectors of the MJS. The maximum attachment limit for emails is 5TB per file, which is possible because ZIVVER is a cloud service which doesn’t communicate via the SMTP protocol. An aspect of the cloud is that administrators give away more control, compared to an on-premise solution [55]. There is always the discussion of what happens with the company’s data if the product goes bankrupt [56]. According to Kool, the use of software in the cloud leads to dependency of welfare and financial stability of the company [57]. This is rather remarkable for ZIVVER, since Rick Goud, the owner of the Company, states that the company is not profitable yet [58]. ZIVVER claims that backups could be made and restored by the customer anytime if reorganization or bankruptcy of the company did occur. Backups can be made via File Transfer Protocol Secure (FTPS).

ZIVVER claims that it is unable to read user information since the private keys are stored by the customer. System administrators of the MJS can recover accounts or look into employees email on special occasions via a master key since all private keys are wrapped with the master key. For the MJS to be more compliant with the GDPR, the logging feature needs to be bought by the MJS which provide insight and control over audit logs and communication logs.

In order to summarize this section, the most important characteristics between ZIVVER and Sophos SPX are shown in figure 5.
<table>
<thead>
<tr>
<th>ZIVVER</th>
<th>Sophos SPX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud solution (TLS 1.2 client/server)</td>
<td>On premise: email to PDF encryption</td>
</tr>
<tr>
<td>Hybrid RSA-2048 / AES-128 encryption</td>
<td>Symmetric AES-128/256 encryption</td>
</tr>
<tr>
<td>Decrypt users private key with master key</td>
<td>No master key for administrators</td>
</tr>
<tr>
<td>Integration with AD/LDAP (objectGUID)</td>
<td>Malware inspection via sandboxing</td>
</tr>
<tr>
<td>Possible to read email without account</td>
<td>End-user need account to read mail</td>
</tr>
</tbody>
</table>

Figure 5: Important differences between ZIVVER and Sophos SPX.

4.3 Which technical challenges do commercial secure email solutions bring for the IT architecture and security architecture of the MJS?

This section describes the technical challenges of commercial secure email solutions for the IT architecture and security architecture of the MJS, regarding cloud concerns, malware inspection, and encryption algorithms.

4.3.1 Cloud-related concerns

The Chief Information Officer (CIO) of the Government of The Netherlands states that management is responsible for the data and services that companies use and store in the cloud. Companies have to make a well-considered choice if an information system can and may be used in the cloud [59]. Since a commercial secure email solution like ZIVVER provides a cloud service, more research is needed in the security risks of migrating data to the cloud. The NBV states that there is an increased risk for data that is stored virtually, or in the cloud. According to the NBV, the biggest nation threats are nation-state actors, cyber attackers, terrorists, and hackers from countries like China, Russia, Iran, and North Korea. The manifestations from threat countries are espionage, sabotage, and political influence like the Russian influence on the American election campaign via Facebook [60]. The risks of moving to the cloud are hacking, the management and use of cloud, multi-tenancy, standard outsourcing, and actors in the supply chain [61]. The NBV offers cooperation if the MJS migrates to the cloud if the company decides to migrate email related data to the cloud.

Sophos SPX does not have cloud-related problems since it is an on-premise solution which is administered by the MJS.

4.3.2 Malware inspection

The SOC of the MJS scans incoming email using FireEye because content must be viewable due to the business policies of the MJS. FireEye makes it possible to analyze the content of email messages in a sandboxing environment for malicious code like spam and malware, before being sent to the end-user [62]. There is a risk that email traffic cannot be analyzed by FireEye anymore if the MJS implement a commercial secure email solution. This is due to the change of the application protocol from SMTP to HTTPS in order to send and receive an email when using, e.g. ZIVVER. FireEye has to possibility to provide real-time detection against encrypted attachments, but it is not advertised whether real-time protection is offered against encrypted HTTPS streams [63]. Another possibility is to bring security back to the 90,000 end-users of the MJS using virus scanners and malware protection, but the SOC states that this likely costly when looking at expenses in the past. Replacements of FireEye are still not possible due to the sandbox feature, according to the SOC.

Beneficial from Sophos SPX is that it does contain a paid sandbox feature which scans for incoming email against malicious code. So increasing privacy through end-to-end encryption may limit the security measures of email inspection. Therefore, a balance between privacy interest and security interest have to be considered by the MJS.

4.3.3 Encryption

The MJS needs to make sure that the master key is securely stored since the master key can decrypt all the private keys. Moreover, ZIVVER uses the objectGUID attribute from LDAP for a specific part in the encryption process. Although this attribute is unique across the enterprise and anywhere else [64], it is also often used in other links. Therefore, the objectGUID attribute from
LDAP forms a security risk, since this value can be easily located. ZIVVER allows other input for this, so it is recommended to use a purely random attribute as a replacement of the objectGUID. An alternative is the CryptGenRandom function which fills a buffer with cryptographically random bytes, which has the following C++ syntax [65]:

```c++
BOOL CryptGenRandom(HCRYPTPROV hProv ,
DWORD dwLen ,
BYTE * pbBuffer
);
```

Sophos SPX uses AES-128 or AES-256 symmetric encryption, where the key is created by the sender, which can be forgotten. If the sender forgets the symmetric key, then the administrators from the MJS do not have the possibility to restore the encrypted email. Another problem with symmetric encryption is that the receiver has to retrieve the key before an email can be decrypted.

To conclude this section, ZIVVER is a cloud solution which introduces security risks like loss of control and the inability to troubleshoot which contradict with the business policies. Another issue is that email inspection may go from a central level (FireEye) to a user level (virus-and malware scanners). Sophos SPX uses symmetric encryption, so the sender has to find a way to hand the key to the receiver in order to decrypt an email which is not user-friendly. The biggest issue with Sophos SPX is the lack of possibility to restore or look into encrypted email under fraud suspicion which contradicts with the business policies as mentioned in the introduction.

5 Conclusion

In conclusion, an answer will be given to the main research question: How to reduce the risk of email data breaches for sectors of the MJS in order to be more compliant with the GDPR?

The MJS need the conventional email security protocols SPF, DKIM, and DMARC to protect against spam, phishing, and spoofing since commercial secure email solutions do not provide these features. Public key exchange for conventional end-to-end email encryption protocols is possible in specific customized cases, but impractical to facilitate in a secure and user-friendly way for every company and end-user they communicate. Commercial secure email solutions will likely reduce the risk of email data breaches since they focus on both user awareness and email encryption, but the implementation of these solutions create some conflicting interests for the IT architecture and security architecture of the MJS. Increasing privacy through end-to-end encryption limits the security measures of email inspection. Therefore, the MJS have to strike a balance between privacy, security, and user-friendliness in which choices must be made by the MJS.

6 Discussion and future work

For now, it is important to find a balance between privacy, security, and user-friendliness in order to give the correct clarification to secure mail. The MJS should deliberate and try to come to an agreement regarding the interfering business policies before the MJS can continue with any commercial secure email solution. If the company decides to do nothing, then emails will still be sent in plain-text. This means that the risk of data breaches is still present, which may result in penalties for violating the GDPR.

References


[58] F. M. Targets. Rick goud (zivver):.


