Gaute Solbu Kleiven

A holistic approach to email security

Master’s thesis in Communication Technology
Supervisor: Karin Bernsmed, Erlend A. Gjære
June 2019

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Information Security and Communication Technology

Master’s thesis

NTNU
Norwegian University of
Science and Technology

Gaute Solbu Kleiven

A holistic approach to email security

Master's thesis in Communication Technology
Supervisor: Karin Bernsmed, Erlend A. Gjære
June 2019

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Title: A holistic approach to email security
Student: Gaute Solbu Kleiven

Problem description:

Electronic mail – email for short - is everywhere, and the same goes for threats related to it. While email was not originally designed with security in mind, a number of measures have since been developed for making it more secure to use. Unfortunately, the uptake of such measures is not nearly as high as one could expect, given that the majority of security incidents are still somehow related to email. For 2018, ENISA reported that compromised email (phishing, spam) was the dominating attack vector. More than 90% of malware infections and 72% of data breaches in organisations originate from phishing attacks.

Motivated by the key role of email in the ever-increasing threat landscape, the purpose of this thesis is to research how companies secure their use of email. The project will focus on the holistic email security of companies, taking into account both technical and organisational measures. In particular, drivers and barriers for implementing the various measures are of interest. In the first phase of the project, two methods will be used to gather relevant data. First, a literature study of related work and relevant background will be performed. Secondly, several in-depth interviews will be conducted with Norwegian companies. In the second project phase, the data collected will be analysed and used as the basis to form a generalized tool for holistic email security in companies.

Responsible professor: Karin Bernsmed, IIK
Supervisor: Erlend Andreas Gjære, Secure Practice

Abstract

Email is involved in an overwhelming share of all cyberattacks. The standards of email are old and insecure, and can easily be forged, eavesdropped or modified by a malicious entity. A large selection of security measures has been created, that can be implemented on top of the protocol standards to provide protection for email services. Despite the many options, there is no definite answer to how email security should be achieved and email remains a massive threat to companies. Email involves different components, i.e. humans, servers and clients, that each can be utilized by an attacker. A lot of research has been done on specific aspects or components of email security, but in order to obtain secure email services, every component needs to be properly secured. Rather than treating specific parts of email individually, it should be dealt with as a whole. To accommodate this, a holistic approach is proposed.

This project surveys four companies to learn about their email security contexts. By conducting interviews with informants from each company, the goal is to learn about how the companies secure their use of email, and what drivers and barriers there are for implementing email security measures. The companies present different contexts, with unique needs and objectives. In addition to the interviews, a literature study is carried out to investigate related work and state-of-the-art on email security. Based on the contexts studied in the interviews and the literature review, a prototype of a guide for holistic email security is designed. The guide is a scenario-based framework, intended to provide a clear overview of email security. The framework presents threats and threat scenarios to email security, as well as what can be done to protect against each scenario. The prototype outlines a valid approach to holistic email security, but it requires further work to be of considerable value to the user. In particular, a cost/benefit metric is a proposed extension to give the framework additional value.

Sammendrag

E-post er involvert i en overveldende andel av alle cyberangrep. E-poststandardene er gamle og usikre, og kan enkelt forfalskes, avlyttes eller modifiseres av en ondsinnet aktør. Et stort utvalg av sikkerhetstiltak har blitt laget for å styrke sikkerheten i e-post. Til tross for mange alternativer, finnes det ikke et tydelig svar på hvordan sikker e-post kan oppnås, og e-post forblir en betydelig trussel for organisasjoner. E-post involverer mange komponenter, deriblant mennesker, servere og klienter, som alle kan utnyttes av en angriper. Det har blitt gjort mye forskning på spesifikke aspekter eller komponenter av e-postsikkerhet, men for å oppnå sikre e-posttjenester må alle komponenter være tilstrekkelig sikret. I stedet for å behandle spesifikke deler av e-post individuelt, burde e-post behandles helhetlig. For å imøtekomme dette, foreslås en holistisk tilnærming.

I denne oppgaven blir e-postsikkerheten i fire organisasjoner studert. Ved å intervjue en informant fra hvert selskap, er målet å lære om hvordan de sikrer sin bruk av e-post, samt hvilke drivere og barrierer som påvirker sikringen. Selskapene presenterer forskjellige kontekster, med ulike behov og målsettinger. I tillegg til intervjuene gjennomføres et litteraturstudie for å kartlegge eksisterende arbeid og «state-of-the-art» innen e-postsikkerhet. Basert på kontekstene studert i intervjuene og litteraturstudiet, designes en prototype av en veileder for holistisk e-postsikring. Veiledningen er utformet som et scenario-basert rammeverk, som skal gi en tydelig oversikt over alle aspektene ved e-postsikkerhet. Rammeverket presenterer trusler og trusselscenarioer til e-postsikkerhet, samt hva som kan gjøres for å beskytte mot hvert enkelt scenario. Prototypen skisserer en berettiget tilnærming til holistisk e-postsikkerhet, men krever videre arbeid før den er av betydelig verdi for brukere. For eksempel, en foreslått utvidelse som kan være av stor verdi for rammeverket, er et estimat av kost/nytte for hvert sikkerhetstiltak.

Preface

This thesis was written in the spring of 2019. It concludes my five years as a Communications Technology student at the Department of Information Security and Communication Technology at Norwegian University of Technology and Science (NTNU).

Inspired by his guest lecture in TDT4237 - Software Security, I reached out to Erlend Andreas Gjære during the spring of 2018, to discuss a possible cooperation for my master thesis. Erlend works a lot with email and the threats related to it, and proposed studying email security and how implementation of it can be guided. Like many others, I was an avid user of email with a limited perception of email security before starting this project. It has been a fascinating, educational and frustrating topic to work with. Email is simple and complex at the same time. For every email security question there are many answers, yet no definite solution. Email security is a jungle of different technologies, protocols, mechanisms, programs and other security measures. I believe an essential step in improving email security is to create a comprehensive and simplified view of the tools available. That was a key motivation for writing this thesis that I hope my work can contribute to.

I would like to thank my supervisors, Karin Bernsmed an Erlend, for all their support and guidance during the project. It has been exciting and motivating to work with people so knowledgeable and enthusiastic. A big thanks also to the persons that let me interview them and contributed with valuable insight and opinions.

Gaute Solbu Kleiven
Trondheim, 6th of June 2019

Contents

Appendices

List of Figures

List of Tables

List of Acronyms

2FA Two-factor authentication.

ASVS Application Security Verification Standard.

BEC Business Email Compromise.

CISO Chief Information Security Officer.

DKIM DomainKeys Identified Mail.

DMARC Domain based Message Authentication, Reporting and Conformance.

DNS Domain Name System.

DNSBL DNS Blackhole List.

DNSSEC DNS Security Extensions.

ENISA The European Union Agency for Network and Information Security.

GDPR General Data Protection Regulation.

IMAP Internet Message Access Protocol.

MDA Mail Delivery Agent.

MTA Message Transfer Agent.

MUA Mail User Agent.

NCSC National Cyber Security Centre.

NIST National Institute of Standards and Technology.

NSM The Norwegian National Security Authority.

PGP Pretty Good Privacy.

POP3 Post Office Protocol 3.

RPZ Respone Policy Zone.

RQ Research Question.

S/MIME Secure/Multipurpose Internet Mail Extensions.

SMTP Simple Mail Transfer Protocol.

SPF Sender Policy Framework.

TCP Transmission Control Protocol.

TLD Top-level domain.

TLS Transport Layer Security.

URL Uniform Resource Locator.

VPN Virtual Private Network.

Chapter 1 Introduction

1.1 Motivation

Email is a prevalent mechanism for electronic communication. According to a survey on information and communications technology usage carried out by Statistics Norway[1] [RD18], 93% of Norwegians aged between 16 and 79 years uses the Internet to send email. The current email infrastructure has weaknesses that can be exposed. Dating back to the 1970s when today's threat landscape was non-existent, email was not created with security in mind. In general, it can easily be forged, eavesdropped or modified. Several new protocols and security mechanisms have been created to combat the weaknesses in the infrastructure. However, these extra layers of protection need to be manually implemented and are not necessarily able to provide complete security. The fact that email is insecure by default and, in theory, anyone can reach out to everyone, has made email a very popular attack vector for cybercriminals. Every year, The European Union Agency for Network and Information Security (ENISA) releases a Threat Landscape report presenting the top cyberthreats and trends in the previous year. According to the latest report [ENI19], email is the most common attack vector used in cyberattacks. Email was involved in more than 90% of cyberattacks in 2018. More than 60% of the total email traffic contained malicious content.

Email security is a crucial component for organisations and businesses that want to secure their assets. By successfully protecting their employees from malicious email and preventing illegitimate use of their domains and servers, a considerable portion of the total threats to the institution is eliminated. The direct cost associated with being the victim of a successful cyberattack should be a driver for securing email services. Business Email Compromise (BEC) is a type of email attack where C-level executives and employees in finance or human resources are targeted and tricked to make payments or disclose confidential information to the attacker. From October

[1] https://www.ssb.no/

2013 to May 2018, approximately 78.000 BEC attacks have been reported worldwide responsible for US $12,5 billion of losses [ENI19]. Cryptojacking[2] and ransomware[3] are other economically motivated cyberthreats commonly carried out by the use of email, targeting organisations. An infamous example is WannaCry, a ransomware cryptoworm targeting computers running Microsoft Windows by encrypting data and demanding ransom payments in Bitcoin currency. In May 2017, WannaCry was able to infect more than 200.000 computers and forced more than 312 ransom payments [ENI19]. Cryptojacking is a threat that has emerged in recent years. Instead of demanding a ransom from the victim, the attacker steals processing power to mine cryptocurrencies that in turn can be used to earn traditional currencies. It is estimated that more than $2.5 billion was earned through cryptojacking attacks during the first half of 2018 [ENI19].

A recently introduced legislation that highlights the importance of protecting information from an economic point of view is the General Data Protection Regulation (GDPR). In May 2018 the GDPR took effect. The regulation requires that organisations safeguard personal data and uphold the privacy rights of anyone in EU territory [Uni]. Data protection authorities in each country are allowed by GDPR to issue sanctions and fines to organisations that violate the law. The penalty can be as much as €20 million or 4% of global revenue, whichever is higher. The potential cost of non-compliance with the GDPR has been a driver for organisations to implement measures that satisfy the rules. For instance, if email containing personal data is sent within the organisation, the message needs to be encrypted to satisfy GDPR. Another example of how cyberattacks can be costly to a company is by damaging its reputation. A public data leak following a successful attack can hurt the company's trust from customers and shareholders, impacting the business and stock prices negatively. In April 2011, Sony's PlayStation Network was hacked, and 77 million user accounts were leaked. The company estimated the incident to cost them $171 million in lost revenue, compensation to customers and more [Hac11].

1.2 Research questions

Looking at the overwhelming share of cyberattacks involving email, it is clear that email pose a threat to companies. History shows that attacks carried out through email have the potential to inflict major economic damage to companies. Still, most companies continue to use email as their primary communication medium. That is one of the key motivations for this thesis; given the insecure nature of email, why is

[2] Cryptojacking is an attack where an attacker gains ownership of a device and install malicious software to start cryptocurrency mining without the computer owner noticing

[3] In a ransomware attack, the attacker gains ownership of files and/or various devices and blocks the real owner from accessing them. The attacker demands a ransom in cryptocurrency to return the ownership

it so widely used? The goal in this thesis is to find out how much of a threat email is to companies, and what is being and can be done to secure their use of email. To facilitate this goal, four Research Questions (RQs) have been defined that will be addressed:

- **RQ1:** How do companies secure their use of email?
- **RQ2:** What drivers and barriers are there for implementing email security measures?
- **RQ3:** How can a company implement holistic email security?
- **RQ4:** Based on cost/benefit analysis, how effective are the different security measures?

In the first part of the thesis, RQ1 and RQ2 will be addressed. To support the exploring of RQ1 and RQ2, a set of hypotheses has been established. H1 and H2 relate to RQ1, while the rest of the hypotheses apply to RQ2. The hypotheses will be discussed in chapter 5.

- H1: Companies have a strategy/plan on how to secure their use of email.
- H2: The companies feel like they have to accept a certain amount of insecurity.
- H3: An incident motivates securing the flaw that caused the incident.
- H4: Employees are considered the weakest link by companies.
- H5: Email security is considered time-consuming by companies.
- H6: Email security is considered expensive by companies.

In the second part of the thesis, RQ3 and RQ4 will be researched by designing a tool to guide the implementation of holistic email security. The *holistic* characteristic implies that the tool focuses on the security of email as a whole, rather than treating specific parts of email individually. The tool will be based on requirements and needs identified in part one of the thesis. The tool is designed in chapter 6, validated in chapter 7 and discussed in chapter 8.

1.3 Outline

The master thesis has the following structure:

- **Chapter 2:** Background and related work. Introduction to relevant technologies, protocols and standards, as well as related work and state-of-the-art on the topic.
- **Chapter 3:** Methods. A review of what has been done, how and why.
- **Chapter 4:** Findings. A presentation of the findings from the interviews.
- **Chapter 5:** Discussion, part 1. A discussion of the results presented in chapter 4, in light of RQ1 and RQ2.
- **Chapter 6:** Treatment design. Presentation of the proposed treatment to the problems identified in chapter 5.
- **Chapter 7:** Treatment validation. Validation of the treatment presented in chapter 6.
- **Chapter 8:** Discussion, part 2. Discussion of the treatment presented in chapter 6 and the feedback in chapter 7, in light of RQ3 and RQ4.
- **Chapter 9:** Conclusion and further work. The conclusion of the thesis and the proposed further work.

Chapter 2
Background and related work

In this chapter, the components of email will be explained. Then the shortcomings of and threats to email will be listed, followed by a presentation of the security measures that have been created to make email more secure. In the final two sections, DNS and related work is presented.

2.1 Email

Email is one of the internet's most important and utilised applications. As email is asynchronous, fast, easy to distribute and inexpensive [Kur17], it is a convenient communication medium for many situations. Simple Mail Transfer Protocol (SMTP) is the standardised protocol for transmission of email. Modern implementations of email allow features such as attachments, hyperlinks, HTML-formatted text and embedded photos.

As defined in RFC 5321 [Kle08], SMTP is used to transport mail objects. A mail object contains an envelope and content. The envelope is a series of SMTP protocol units; an originator address, one or more recipient addresses and optional protocol extension material. For the SMTP handshaking protocol, a Transmission Control Protocol (TCP) connection is established between the sending and receiving servers. The connection is then used to exchange the protocol units mentioned above between the sending and receiving servers.

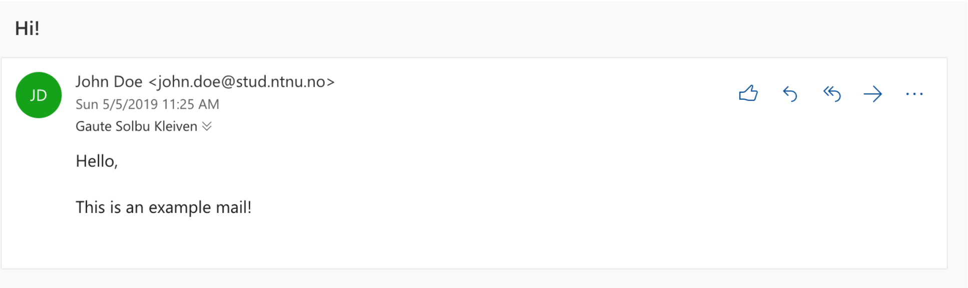
The content of the mail object can be further split into two parts: the headers and the body. RFC 5322 [Res08] defines the format of the header lines and their semantic interpretations. Each header line consists of a keyword followed by a colon and a value. Some keywords are required ('From:' and 'To:') and others are optional (e.g. 'Subject:'). Finally, also specified in RFC 5322 [Res08], the body is simply lines of ASCII characters. There are however other documents, specifically the MIME documents (RFC 2045 [FB96a], RFC 2046 [FB96b], RFC 2049 [FB96c], RFC 4288 [FK06] and RFC 4289 [FK05]) that extend and limit the body specifications, to allow for different sorts of bodies. The resulting email is a text file, where the lines and their keywords map to various parts of the message.

Listing 2.1 shows an example dialogue between a client and a mail server when sending an email. First is a series of SMTP protocol units and their corresponding responses (line 1 to 29), used to establish a Transport Layer Security (TLS) connection with the server and create the envelope of the message. Then follows the content headers (line 30-32) and content body (line 33-34), and finally closing envelope protocol units (line 35-38). The message sent by the listed code, as seen by the receiver using the Microsoft Outlook web client, is shown in figure 2.1.

```
1  S: 220 mailgw02.it.ntnu.no ESMTP Postfix (Ubuntu)
2  C: HELO 10.22.79.42
3  S: 250 mailgw02.it.ntnu.no
4  C: STARTTLS
5  S: 220 2.0.0 Ready to start TLS
6
7  C: EHLO Hey
8  S: 250-mailgw02.it.ntnu.no
9  S: 250-PIPELINING
10 S: 250-SIZE 52428800
11 S: 250-VRFY
12 S: 250-ETRN
13 S: 250-AUTH PLAIN LOGIN
14 S: 250-ENHANCEDSTATUSCODES
15 S: 250-8BITMIME
16 S: 250 DSN
17 C: AUTH LOGIN
18 S: 334 Username:
19 C: am9obi5kb2U=
20 S: 334 Password:
21 C: VGhpc0lzTm90TXlSZWFsUGFzc3dvcmQ=
22 S: 235 2.7.0 Authentication successful
23
24 C: MAIL FROM: <john.doe@stud.ntnu.no>
25 S: 250 2.1.0 Ok
26 C: RCPT TO: <gauteskl@stud.ntnu.no>
27 S: 250 2.1.5 Ok
28 C: DATA
29 S: 354 End data with <CR><LF>.<CR><LF>
30 C: Subject: Hi!
31 C: From: John Doe <john.doe@stud.ntnu.no>
```

```
C: To: Gaute Solbu Kleiven <gauteskl@stud.ntnu.no>
C: Hello,
C: This is an example mail!
C: .
S: 250 2.0.0 Ok: queued as 6011980337E
C: QUIT
S: 221 2.0.0 Bye
```

Listing 2.1: Dialogue between a SMTP client (C) and NTNU's student mail server (S), when sending an email.



Hi!

JD

John Doe <john.doe@stud.ntnu.no>

Sun 5/5/2019 11:25 AM

Gaute Solbu Kleiven

Hello,

This is an example mail!

Figure 2.1: Screenshot of the email sent by the example code in listing 2.1, as seen by the receiver using the Microsoft Outlook web client.

2.1.1 Email components

Kurose and Ross [Kur17] defines three key components of email: Mail User Agent (MUA), mail servers and protocols. Microsoft Outlook[1] and Mozilla Thunderbird[2] are common examples of MUAs. These agents allow the user to read, reply to, forward, save and compose messages. The mail servers make up the core of the email infrastructure. Examples of popularly used mail servers are Sendmail[3], Postfix[4] and Microsoft Exchange.[5] Running on each server is a Message Transfer Agent (MTA) application, responsible for sending, receiving and forwarding messages to other MTAs. SMTP is the protocol that specifies the details of transmission when MTAs send and receive email. Another agent running on the mail server is the Mail Delivery Agent (MDA).[6] When an email reaches the receiver's MTA, it is passed to the MDA, which is responsible for storing the message until the MUA fetches it. SMTP cannot

[1] https://products.office.com/outlook/

[2] https://www.thunderbird.net/

[3] http://www.sendmail.com

[4] http://www.postfix.org/

[5] https://products.office.com/exchange

[6] The MDA can be run on a separate server, but it is often bundled with the MTA on the mail server.

be used to retrieve email from the MDA. Most commonly Post Office Protocol 3 (POP3) and Internet Message Access Protocol (IMAP) are used to transfer messages to the MUA. The postal system can be used as a real-world analogy to illustrate the differences between the MTA and MDA: If the MTA is the post office, where the messages are sorted and passed on to their destinations, then the MDA is the mailbox of the recipient, where the message is stored until the receiver fetches it.

A simplified illustration of the email flow between two users is shown in figure 2.2. In the example, the sender sends an email to the receiver. The process consists of the following steps (where the steps refer to the numbers in the figure):

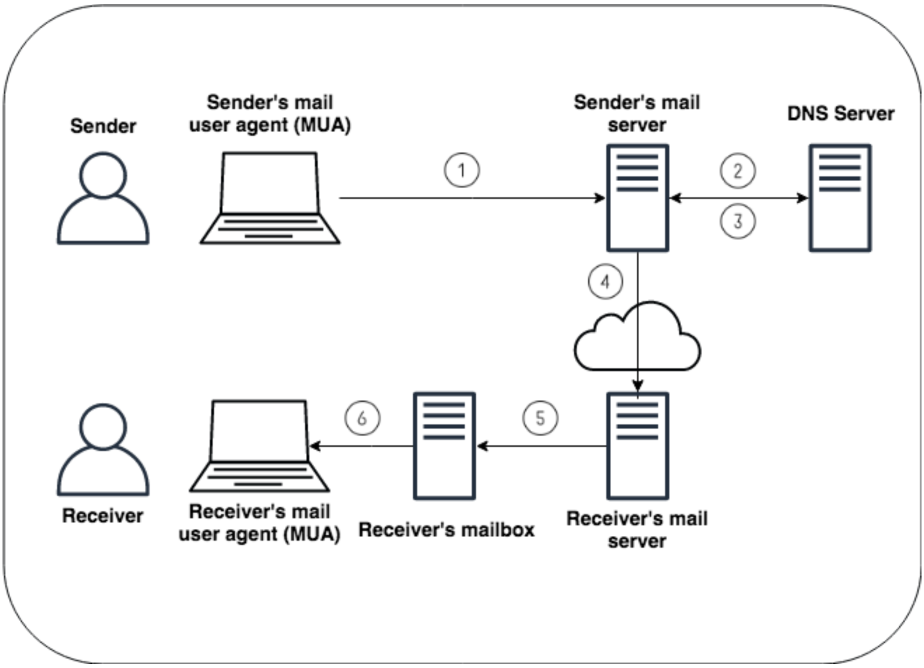


Figure 2.2: A simplified transfer of email from sender to receiver. Adapted from [Sik17].

1. The sender composes a message in his MUA. He enters the receiver's address as the receiver of the message. When he clicks 'Send', the message is transferred to his MTA using SMTP.

2. The MTA looks at the domain of the receiver's address (the text after the '@' in the address). The MTA queries a DNS for the IP address of the receiver's MTA.

3. The DNS returns the IP address of the MTA corresponding to the domain of the receiver.

4. The sender's MTA sends the email to the receiver's MTA using SMTP.

5. The receiver's MTA receives the message and hands it over to the MDA. The MDA places the message in the receiver's mailbox.

6. The receiver's MUA retrieves the message from his mailbox using POP3 or IMAP[7].

2.1.2 Email infrastructure

The mail servers form the core of the email infrastructure. To a company wanting email services, there are choices to be made as to what infrastructure they want for their mail servers. Traditionally, companies have had SMTP servers running on dedicated hardware, operated by either the company itself or a hired third party. In recent years, many businesses have made the switch to cloud-based email services, such as Microsoft Office 365[8] or Google G Suite.[9] National Institute of Standards and Technology (NIST) [MG$^+$11] defines Cloud computing as:

> *"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction."*

Instead of running the mail server on a tangible set of resources, a cloud solution allocates computing power on-demand to the company. If email is bought as a service from a third-party, the service provider is responsible for the infrastructure. As a consequence, the organisation may not have direct access to MTAs, authoritative DNS servers, or any possible special use components[10] [CGNR19]. In a cloud adoption study from 2018 carried out by security company Bitglass [Bit19], it is reported that 81.1% of the 135,000 surveyed corporate email domains use either Microsoft Office 365 (56.3%) or G Suite (24.8%) for email services.

[7] POP3 and IMAP are commonly used, however MS Exchange for instance uses MAPI/RPC [Sik17]

[8] https://products.office.com/en-ww/home

[9] https://gsuite.google.com/

[10] A special use component is, for instance, a component providing a security function such as filtering of spam or malware.

2.2 The email threat landscape

The email threat landscape is constantly changing. Accordingly, new types of malicious email and ways of deceiving and attacking the victims are developed. Although there are frequent changes to types of malicious mail attacks, most still fall within one or more of the following three basic strategies:

- **Malicious attachments.** The attacker attaches a malicious file to the email. For instance, the message contains a keylogger or ransomware that is executed when opened by the victim.
- **Links to malicious web pages.** The attacker adds a clickable link to the body or an attachment of the email. When clicked, the victim is taken to a dangerous web page. Symantec [Sym19] reports that 7.8% of Uniform Resource Locator (URL) addresses in emails were malicious in 2018. The recent reports indicate a positive trend as the number was 12.3% in 2017.
- **Social engineering.** The attacker entices the victim to send sensitive data or perform a financial transaction. For instance, the attacker pretends to be the victim's boss and requests an illegitimate money transfer.

The majority of all types of email threats use combinations of the above-listed strategies. There are many different types of threats. Four common threats related to email are presented here; malware, phishing (including spear phishing and whaling), spoofing and spam:

Malware is derived from the term 'Malicious Software'. Malware is a broad term that can refer to any piece of software that performs undesirable operations such as computer compromise or data theft. Common types of malware are trojans, viruses, worms, spyware and macros. The main distinction between the different types of malware is how they spread and infect systems. The symptoms caused by the various types may be similar [fNSa]. ENISA [ENI19] lists malware as the most frequently encountered cyberthreat. It is somehow involved in 30% of all data breach incidents reported. Malware is primarily targeted at Windows systems. 79% of the detected malware in organisations were targeting Windows, 18% Linux and 3% Mac systems. As of 2019, email is the dominant attack vector for malware [ENI19]:

> *"Again this year, it comes as no surprise that compromised email (phishing, spam and spear-phishing) is the dominating attack vector for malware infections. Email compromise was the attack vector for 92,4% of detected malware, web and browser was the attack vector for 6,3% and 1,3% have been attributed to other attack vectors."*

Phishing is a social engineering technique where a message is crafted to lure the recipient. For instance, the phisher tries to trick the recipient into opening a malicious attachment, hand over their credentials, click on an unsafe URL or wire money. Phishing is the favoured way of compromising organisations. It has been reported that 75% of the EU's Member States disclosed cases of phishing. Phishing is so heavily leveraged that over 90% of malware infections and 72% of data breaches in organisations originate from phishing attacks. [ENI19].
Spear phishing is a more advanced form of phishing, seeking unauthorised access to confidential data by targeting specific organisations or individuals. Similar to standard phishing, the attacker tries to lure the recipient by impersonating a trusted source. Moreover, the attack is typically personalised, using public information found on social networks such as Facebook or LinkedIn [fNSb].
Whaling (also known as BEC) is a type of phishing attack targeting C-level executives and employees in finance or human resources aiming to steal money from their organisations. It is a form of spear phishing, but whereas spear phishing can target any individual, whaling attacks target high ranking victims within a company. From October 2013 to May 2018, ca. 78.000 whaling attacks have been reported worldwide responsible for $12,5 billion (USD) of reported losses [ENI19]

Spoofing is when an attacker masquerades as a legitimate entity to deceive the receiver. For email, spoofing involves forging the header to make it look like it is sent from someone else than the actual source. SMTP does not prevent the sender from modifying the 'From:' field in the content header, allowing the sender to change whom the message appears to be from. A report from National Cyber Security Centre (NCSC)[11] [Cen17] discusses spoofing and how government domains are heavily leveraged by it. Attackers frequently attempt to masquerade as important institutions, such as tax authorities, to trick people into revealing confidential information.

Spam is an abusive use of email (and other messaging technologies) to flood users with unsolicited messages. Spam is an old concept, dating back to the beginning of the internet. What makes spam a threat is its low cost to send, as it is primarily distributed by large spam botnets. Despite a shrinking volume, spam is still a significant attack vector [ENI19].

2.3 Technical security measures

There are several technical security measures aimed at making email a more secure medium. For instance, there are extensions to the SMTP that can be implemented to provide authentication and confidentiality of messages in transit between mail servers. Other examples are spam filters and malware scanning tools, that can be

[11] https://www.ncsc.gov.uk/

used to filter out unwanted email. In the following subsections, various technical implementations providing security is presented.

2.3.1 Sender Policy Framework (SPF)

The SPF protocol is defined in RFC 7208 [Kit14]. What the protocol does, is allow the MTA to authorise hosts. SPF records stored in the DNS specify what hosts are allowed to send mail from a given domain. Figure 2.3 shows the flow of SPF: A domain owner publishes a SPF record to the DNS server, specifying who is allowed to send email on behalf of the domain (1). Upon receiving an email (2), the MTA can query the DNS to check if there exists a SPF record for the sender domain and if the sending MTA's address corresponds with it (3). The SPF record is used to authenticate the sender (4). If the sender is verified, the message will be delivered (5a). The SPF record specifies to which degree a message will fail, but not what the receiver should do with a failing message [Dog17]. Depending on the setup, a message failing the verification might be delivered to the mailbox (5b), either as normal or marked *quarantine*, or rejected (5c).

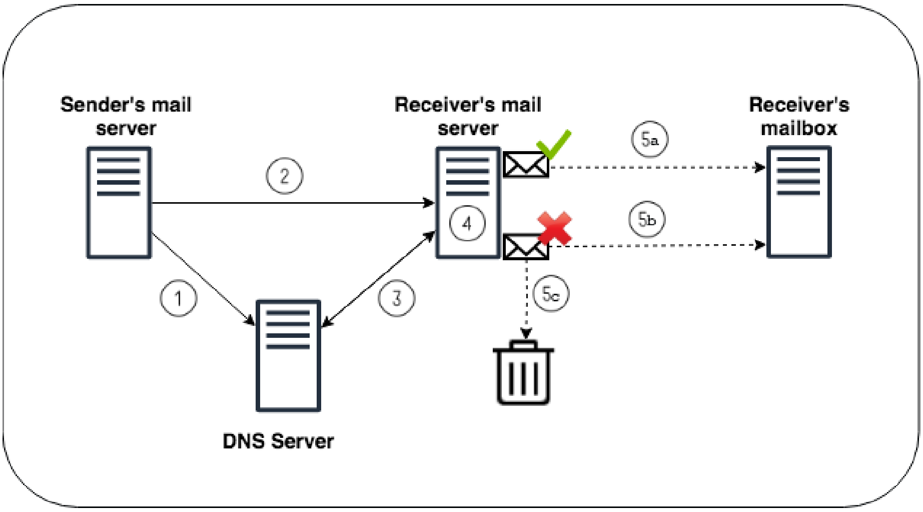


Figure 2.3: A generalised flow illustrating SPF and DKIM. Adapted from [Sik17].

2.3.2 DomainKeys Identified Mail (DKIM)

DKIM is specified in three RFCs: 5585 [HCHB09], 6376 [CHK11] and 5863 [HSHBC10]. DKIM uses asymmetric cryptography to sign messages digitally. The flow of DKIM is the same as SPF, as shown in figure 2.3. When sending an email, the sending MTA uses a private key to create a digital signature that is included in the header. The public keys of the domains are uploaded to the DNS (1). When receiving a mail (2), the MTAs queries the DNS for the key (3) that can be used to validate the signature attached to the message (4). By verifying the signature using the public key, the sender is either authenticated (5a) or not authenticated (5b or 5c). Similar to SPF, a verification failure does not force the rejection of the message. Note that DKIM does not authenticate the physical message source, it only verifies that the private key signed the message. It relies on the fact that only the entities authorised to send mail on an organisation's behalf has access to the secret key [Dog17].

2.3.3 Domain based Message Authentication, Reporting and Conformance (DMARC)

DMARC, specified in RFC7489 [KZ15], is a technology specifically developed to address the shortcomings of SPF and DKIM [Dog17]. DMARC provides three main features:

1. **Identifier alignment:** Verify that the From header matches the domain validated by SPF and the signing domain (DKIM). If any of the checks fail, the message will not pass DMARC overall.
2. **Provide policy:** Allow sending domain owner to specify a policy for how receivers must handle messages failing checks.
3. **Provide feedback:** Sending domain owners are informed of any messages failing checks, enabling easy identification of phishing campaigns or errors in SPF, DKIM or DMARC policy assignment.

Figure 2.4 shows how DMARC works when an email is received. A domain registers its DMARC policy to the DNS (1). When a mail server receives a message (2), the sending domain's DMARC policy is queried from the DNS (3). A DMARC verification is then performed on the message (4). If the message passes the verification, it is delivered as usual (5a). If DMARC authentication fails, the message is rejected (5c), placed in quarantine or delivered as usual (5b), depending on the specified policy. The receiver regularly reports back to the sending domain to inform what messages are being authenticated and not, and why (6).

2.3.4 STARTTLS

STARTTLS is an extension to SMTP, defined in RFC 3207 [Hof02]. The protocol uses TLS to provide message encryption between the sender's and receiver's mail servers. In theory, the ideal solution would be to encrypt messages end-to-end (client-to-client), but that would require an effort from the user in terms of key management and encryption. By establishing encrypted communication only between the mail servers,

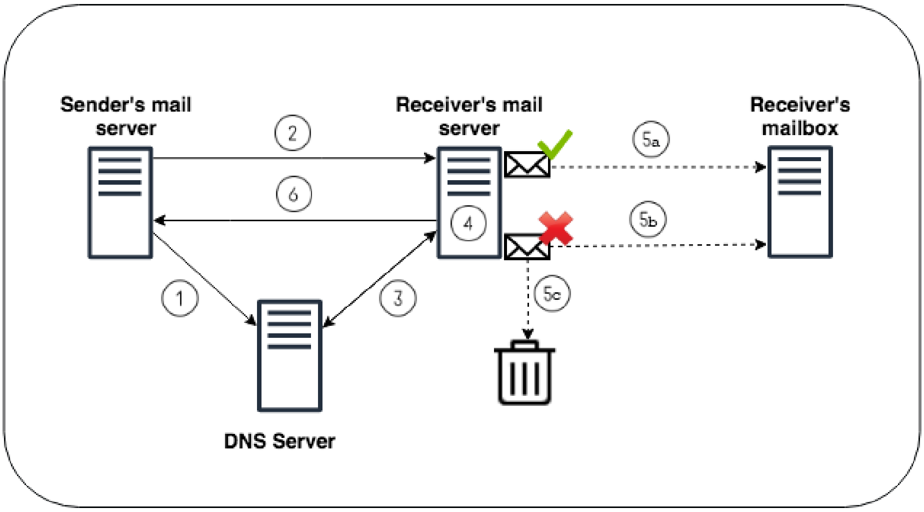
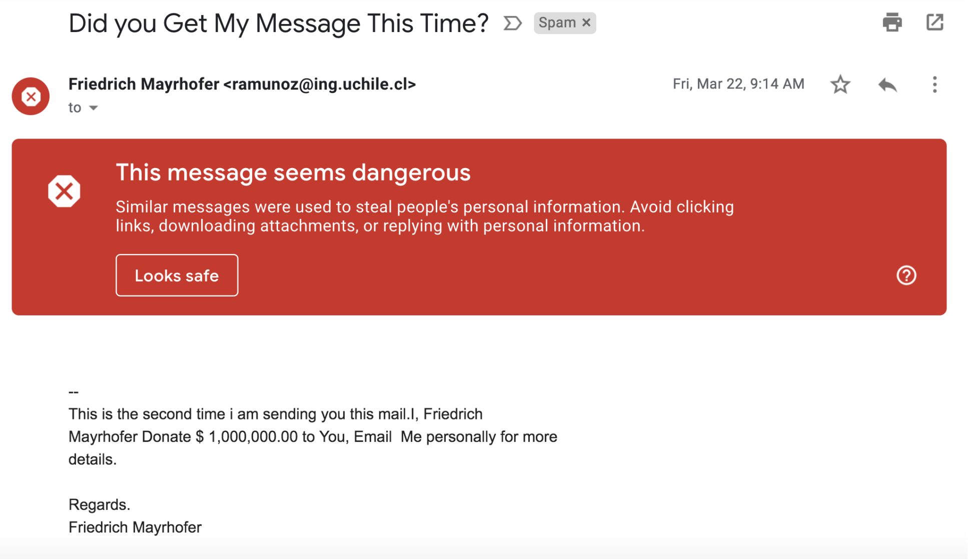


Figure 2.4: Flow of DMARC. Adapted from [Sik17].

the process is simplified for the end user while still protecting the message when it is in transit between the servers. STARTTLS will not protect the communication between a client and its server. However, this is typically secured by the company's internal network or a Virtual Private Network (VPN) [Sik17]. A drawback with STARTTLS is that it operates best-effort. By default, if one of the parties does not support STARTTLS, the session will be downgraded and established as unencrypted. A downgrade can also be forced by a man-in-the-middle attack even if both servers are properly configured to support TLS [Hof02]. To combat this, servers can be configured to force TLS, and reject the session if it cannot be established. Since this requires manual configurations, it will typically be prioritised for known destinations that are known to support STARTTLS, such as a subsidiary or a customer of the company.

2.3.5 Spam filters

A spam filter is a tool created to protect against spam messages. The generalised definition of spam filters by Cormack [C$^+$08] captures its essential nature: *"[A spam filter is] an automated technique to identify spam for the purpose of preventing its delivery"*. There are several potential, negative consequences of spam [C$^+$08]. Firstly, there are direct consequences of the message's payload. For example, the attached malware being executed, or the victim falling for the phishing attempt. Secondly, spam consumes many resources. Out of the total email traffic, more than 55% of emails received in 2018 were categorised as spam [Sym19]. By consuming massive amounts of bandwidth and storage, the spam increases legitimate messages' chance of being untimely delivered or completely lost. Spam can also have a negative impact on human resource consumption. If an employee's inbox is frequently filled with spam, it can be time-consuming and challenging to sort out legitimate messages.



Did you Get My Message This Time?

Friedrich Mayrhofer <ramunoz@ing.uchile.cl>
to

Fri, Mar 22, 9:14 AM

This message seems dangerous

Similar messages were used to steal people's personal information. Avoid clicking links, downloading attachments, or replying with personal information.

--
This is the second time i am sending you this mail.I, Friedrich Mayrhofer Donate $ 1,000,000.00 to You, Email Me personally for more details.

Regards.
Friedrich Mayrhofer

Figure 2.5: A spam mail identified automatically by Gmail. Screenshot taken in the Gmail web client.

The goal of a spam filter is to use the available information (e.g. message headers, message payload) to successfully classify what is spam and what is not. How that is accomplished varies from filter to filter. Common techniques are hand-crafted rules (e.g. blacklists, whitelists, rule-based filtering), machine learning and probabilistic classifiers, to mention a few. Typically, the filter is deployed such that it processes incoming messages. If the message is considered spam, it is put in quarantine. If not, it reaches the inbox of the recipient. There are also alternative deployment scenarios of spam filters, as presented by Cormack [C+08]. Spam filters are commonly evaluated by their false positive and false negative rates. That is, respectively: How many spam messages are classified as legitimate, and how many legitimate messages are classified as spam?

2.3.6 Malware and link protection

Anti-malware protection is aimed at preventing malicious attachments, code and viruses from reaching the user's inbox. All incoming and outgoing messages are scanned, and are not delivered to the end user if the scan concludes that they contain harmful elements. Similar to for spam filters, how messages are scanned depends on the implementation of the anti-malware protection. Typical checks include checking that the attachments comply with the allowed file extensions, or validating that the signatures of the attachments are not found in lists of known malware signatures. Signature detection works very well for identifying known malware, however, detecting unknown and new forms of malware by signatures is extremely difficult [Cis14]. Sandboxing technology is a useful security mechanism for new or polymorphic[12] malware. A sandbox is a safe, isolated environment that mimics the user's computer. By executing attachments in this environment and recording their actions, harmful behaviour such as anti-debugging techniques and keystroke logging can be revealed [Cis14]. Sandboxes are not failproof. Some newer families of malware have been designed to be aware if they are being run in a sandbox environment. This way, they can execute harmlessly in the sandbox and evade the security mechanism [LL17].

Various measures can be implemented to protect against malware on the client device. Antivirus programs are software used to prevent, detect and remove malware from a computer. There are many options to choose from, such as Symantec Norton Antivirus[13] and McAfee AntiVirus[14]. Another tool is AppLocker[15], which enables whitelisting of applications on Microsoft Windows. With AppLocker, an administrator can specify rules on what files are allowed to execute, which can be used to prevent malicious code in email attachments from executing. According to a report from Symantec [Sym19], almost half of all malicious email attachments are Microsoft Office files. Macros[16] are commonly used to attach malicious scripts to Office files. For example, the script can download a malicious payload when the attachment is opened. The first step in protecting against macro malware is to disable macros, which is done by default in recent versions of Office [LSS19]. The malicious script might still be executed if the attacker convinces the target to enable macros. By showing a fake warning, as seen in figure 2.6, the user might be tricked to activate macros. A step further is to prevent any macros from the internet from running by removing the *enable content* button for them, or to filter out all email attachments containing a macro.

Similarly to anti-malware protection, the goal of link protection is to check if the destination of a URL in an email is insecure, before the user loads the content of it. Typically, there are measures such as checking if the URL is unsafe or if it

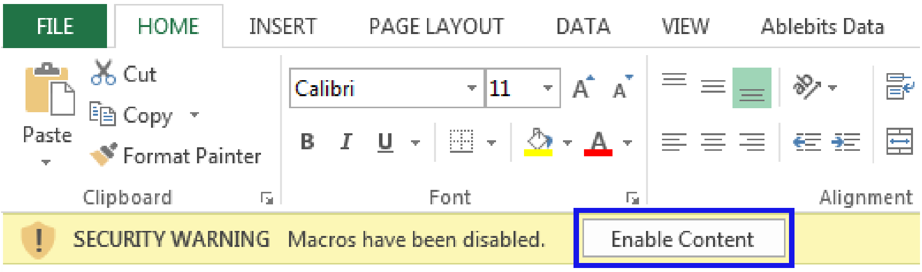
[12] Polymorphic malware changes frequently and might generate a new signature for each victim, rendering the signature checks ineffective.

[13] https://us.norton.com

[14] https://www.mcafee.com/consumer/en-ca/store/m0/index.html

[15] https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/what-is-applocker

[16] A macro is a series of commands and instructions that allows a user to automate tasks. Instead of performing several tasks manually, a macro can be configurated to execute a series of actions with one click.



SECURITY WARNING Macros have been disabled.

Figure 2.6: In a Microsoft Office program, a user can enable macros by clicking on ‘Enable Content’. The screenshot is taken from Office 365’s desktop version of Excel.

is found on a list of blocked domains. More advanced protection includes checking if it is a shortened URL[17]. If that is the case, the actual destination needs to be checked in addition to the shortened URL. Another common threat is URLs linking to downloadable files [ENI19]. In this case, the domain might be legitimate, e.g. Dropbox or Google Drive, even though the linked file is malicious. To combat this, link protection can be configured to scan linked files as if they were attached to the message [Van19].

2.3.7 End-to-end encryption

The idea of end-to-end encryption is to encrypt a message such that only the sender and receiver (the endpoints) can read it. Pretty Good Privacy (PGP) is an encryption scheme dating back to 1991, that was standardised as OpenPGP in 1997 [CDF+07]. By using symmetric and public key cryptography, a hash function and a digital signature, PGP provides confidentiality as well as integrity and authentication between sender and receiver [Kur17]. A drawback with PGP is that it is difficult to use and understand. As highlighted by Whitten [WT99] and Sheng et al. [SBKH06], the lack of feedback and the inadequate interface makes key management difficult with PGP. The fact that PGP never really caught on even though there has been much interest in achieving end-to-end email security, probably has to do with the aforementioned issues of user-friendliness. In more than 20 years, only 5.5 million PGP keys have been published to the SKS Keyserver[18] in total.

Another email standard providing encryption between endpoints is Secure/Multipurpose Internet Mail Extensions (S/MIME), as defined by several documents, most notably [Hou09], [RT10a] and [RT10b]. The main difference to PGP, is how S/MIME

[17] URL shorteners are used to generate short URL addresses. Bit.ly is a popular tool for this, where users can paste an address and get an address on the bit.ly domain pointing to the pasted address. This can be abused to hide domains. A URL that will take the user to a malicious web app when clicked, might be considered safe if the shortener domain used is trusted.

[18] SKS is the keyserver used by OpenPGP. Numbers are taken from https://sks-keyservers.net/

uses centralised authorities for key management. A trusted party is responsible for the distribution of keys and signatures, used for encryption/decryption and verification of senders, respectively. Like PGP, S/MIME has its shortcomings. Firstly, users have to assume that authorities are honest, which may not be a reasonable assumption. Secondly, there is not necessarily a natural certificate authority. S/MIME has proven well-suited for large companies or corporation with a clear certification authority, but have not been successfully adopted by the general public.

2.3.8 Two-factor authentication (2FA)

There are three common factors used for authentication: Something you know (i.e. a password), something you have (i.e. a key) and something you are (i.e. fingerprint). Many services require only that the user specifies the correct combination of username and password to gain access. Two-factor authentication (2FA) adds an extra layer of security by requiring an additional authentication factor. Commonly the extra factor is *something you have*, such as a mobile phone or a code generator. Despite the additional protection it provides, the adoption rates of 2FA remains low. At a security conference in January 2018, a Software Engineer at Google revealed that less than 10% of their active users had enabled 2FA on their Gmail accounts [Tho18]. In Febraury 2016, Dropbox revealed that less than 1% of their users have adopted 2FA [Hei16].

2.4 Human factors

In the previous section, technical measures to prevent malicious messages from reaching the end users were reviewed. There are also security measures focusing on how people using email can be trained to act securely. It is a lot less dangerous that a malicious message reaches an employee if the employee knows how to handle it securely. As reported by [Rob15], the top way threats enter the organisation is by users clicking a link or opening an attachment in an email. For this reason, in many businesses it is common to have courses, campaigns or training to promote information security awareness. By raising awareness, the intention is to allow employees to recognise IT security concerns and respond accordingly [WH03]. In *The Unrecorded Statistics Study 2018* [Sik18], data regarding the IT security situation in Norway has been collected. Phishing and social engineering are identified as the most common security incidents in the report. In response to what factors were the reasons for the incidents (*"Were any of the following factors the reason the security breach occurred?"*), human factors stand out, as shown in figure 2.7. More than half of the respondents believe a human error was a cause to the incident, and 39% attributes the breach to lack of employee security awareness. The report emphasises the importance of a digital security culture as a preventive measure. To prevent incidents and ensure that the consequences are lower when incidents do occur, it is recommended to have thorough instruction and training in digital security.

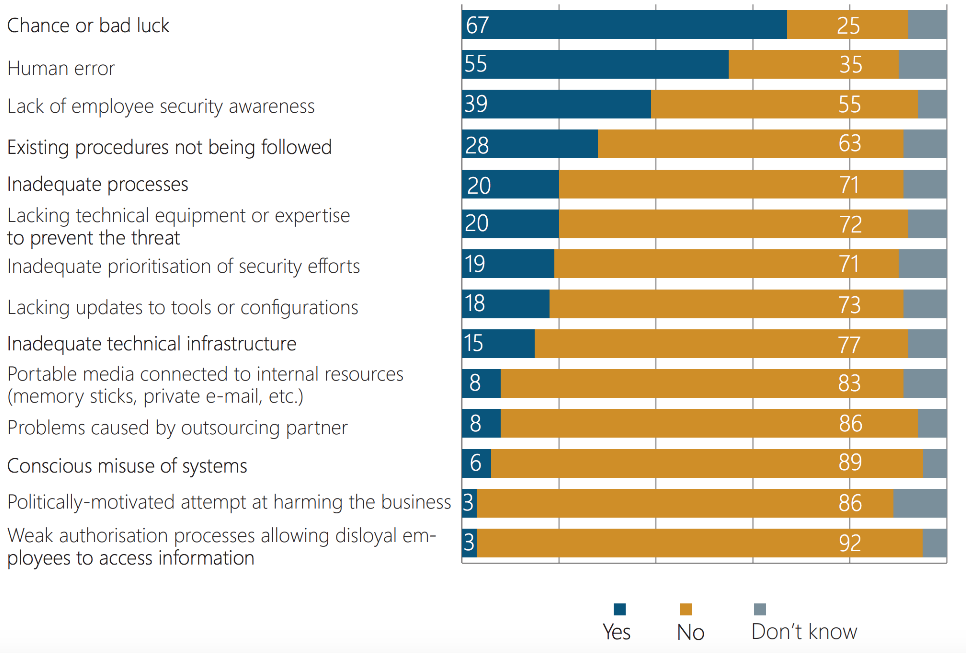


Figure 2.7: Response to the question *"Were any of the following factors the reason the security breach occured?"* in The Unrecorded Statistics Study 2018. The number of respondents were 572. Taken from [Sik18]

The report also surveyed the adoption of security awareness activities. In response to *"Has the business completed activities to improve the employees' awareness regarding security over the past year?"*, 61% of the 1500 respondents answered yes. The respondents that answered yes were further asked about what types of activities they have completed. The results are shown in figure 2.8. Internal lectures were identified as the most common activity (54%). 44% responded other activities, 31% answered that they have e-learning and 6% have completed phishing campaigns. How IT security is organised is also touched on in the report. The respondents were asked *"Does the business have a framework and/or management system for information security?"*. Out of all 1500 respondents, 61% answered "yes", 27% "no" and 12% "Don't know". There are vast differences between small and large businesses in answering this question. For businesses with more than 100 employees, 79% answer that they have a framework or management system for information security. In contrast, the share was 54% for businesses with 5-19 employees.

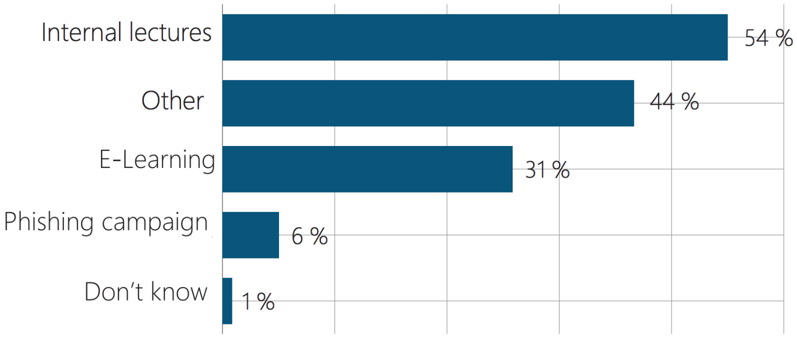


Figure 2.8: Response to the question *"Which types of activities to increase employees' awareness regarding security have been completed over the past year?"* in The Unrecorded Statistics Study 2018. The number of respondents was 913. Taken from [Sik18].

Cofense[19], an organisation working with human-focused anti-phishing, released a report in 2017 [Phi18] emphasising the ability to recognise and understand phishing emails as the best way not to be tricked. For three years they have run repeated phishing simulations in organisations. The results show a shrinking susceptibility rate every year. According to the report, the more employees report phishing, the faster the susceptibility decreases. By engaging the employees and training them routinely, anti-phishing programs become proactive and more effective. On how to identify a phishing attack, Cofense comments that rule number one is to understand that every email you receive is a potential threat [Cof]. For instance, if you are unsure about an email, you should check its validity by phoning the supposed sender or confer with the IT department.

2.5 Domain Name System (DNS)

From the previous sections, it is clear that DNS servers provide several important services for email. Not only is the DNS used to translate hostnames to IP addresses (or the other way around) such that mail servers know where to route email, it also stores the information that enables aforementioned security measures such as SPF, DKIM and DMARC. These features make the DNS a possible attack vector for malicious actors.

[19] Formerly known as PhishMe

2.5.1 How DNS works

DNS uses a large number of servers, organised hierarchically and distributed around the world [Kur17]. There are three classes of DNS servers: The root DNS servers sit on top of the hierarchy and are scattered all over the world. The root servers provide the IP addresses of the Top-level domain (TLD) servers. For each top-level domain, i.e. com, org, uk or no, there is a TLD server (or a group of servers). The TLD servers provide addresses for authoritative name servers, where the actual DNS records are stored. DNS data for a domain is referred to as a *zone*.

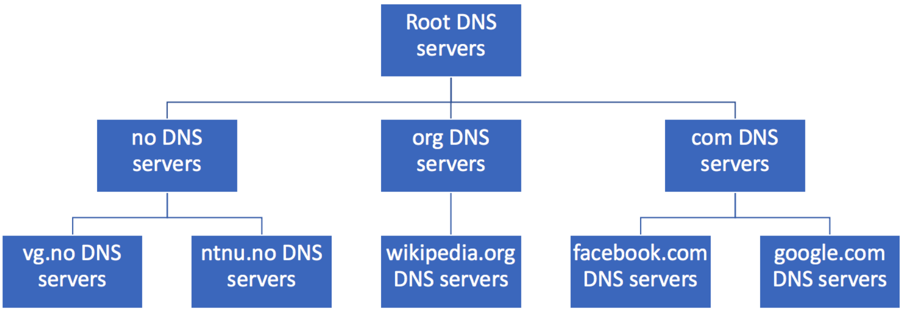


Figure 2.9: Portion of the hierarchy of DNS servers. Each box represents a zone. Adapted from [Kur17].

When sending an email, the DNS record of the recipient's domain is needed. The process starts at the sender's local DNS resolver. The local resolver relays the message to a *recursive resolver*, which is a more advanced DNS client typically run by the network operator. In turn, the recursive resolver queries authoritative name servers for the record requested by the sender. Every domain stores DNS data on an authoritative name server publicly available on the internet. DNS servers are commonly outsourced to third parties, but some organisations operate their own. DNS data is stored as resource records, which are four-tuples containing a name, a value, a type and a time-to-live[20]. There is a long list of possible record types, but only a selected few are included here:

- **A**. Standard hostname-to-IP address mapping.
- **MX**. Mail exchange record, mapping a domain name to a list of MTAs for that domain.
- **TXT.** Text record containing arbitrary text. Extensively used for SPF, DKIM, DMARC, opportunistic encryption et al.

[20] Time-to-live determines when a resource should be removed from a cache.

Similar to email, DNS was not designed with security in mind. When a recursive resolver receives a response from an authoritative name server, the resolver cannot verify the authenticity of the response. As a result, an attacker can reply with an illegitimate response to a DNS query. For instance, with email as an example, the attacker can respond with his address instead of the intended receiver's, hence misdirecting the email to himself. In a similar fashion, a malicious actor can provide falsified TXT records to pass the verification of SPF, DKIM and DMARC.

2.5.2 DNS security

DNS Security Extensions (DNSSEC), defined in RFC 4033 [Are05a], RFC 4034 [Are05b] and RFC 4035 [Are05c], is a security measure created to strengthen the authentication of DNS [fANN19]. By the use of public key cryptography, DNSSEC enables origin authentication and integrity protection for data. The former verifies that the data received came from the zone where it is believed the data originated. The latter ensures that the data has not been modified in transit. Every zone has a pair of a public and a private key that is used to sign and verify, respectively. In order to verify data using a public key, the authenticity of the key itself needs to be verified first. Each key is signed by the parent zone, creating a chain of trust. With figure 2.9 as an example, the public key of vg.no's zone is signed by the private key of *no DNS server*. In turn, the TLD is signed by the root zone. As the root zone does not have a parent, it cannot be verified and must be trusted implicitly by the resolvers. DNSSEC is not automatic, it needs to be specifically enabled by network operators and the owners of each zone. Norid[21], a subsidiary of Uninett[22], operates the Norwegian TLD name server .no. On DNSSEC, they have stated that: *"Norid considers DNSSEC an important security component of the DNS, and a technology that should be standard for all Norwegian domains"* [AS18]. They further comment that Norway is one of the world leaders of DNSSEC, with more than 58% of all active domains using it[23]. Huston [Hus19] argues that DNSSEC is not the *complete answer* to the shortcomings of DNS. He addresses several challenges to DNSSEC, such as key management, misconfiguration, increased size of DNS responses and no validation at the end host. Van Rijswijk-Deij et al. [vRDSP14] concludes that DNSSEC can be leveraged for denial of service attacks due to its DNS amplification.

DNS Blackhole List (DNSBL), also referred to as DNS Blacklists, is a security mechanism based on DNS. DNSBLs contains IP addresses of computers or networks involved in spamming activities and can be used by the mail servers to reject or flag messages from systems with a history of sending spam. The same DNSBL technology can also be used for whitelisting of well-behaving email sources, listing

[21] https://www.norid.no/no/

[22] https://www.uninett.no/

[23] As of 30-04-2019. Data were taken from https://www.norid.no/no/statistikk/dnssectall/

well/ill-behaving domain names and more. DNSBL is a medium rather than a specific list or policy, hence there are many different lists available for use. As the lists are populated based on different criteria for what a spammer is, some are stricter than others. RFC 6471 [LS12] provides guidance on DNSBL usage, highlighting the importance of transparency on listing criteria and expiration intervals on listings. Respone Policy Zone (RPZ) is a similar DNS mechanism, which is said to *"Does for DNS resolvers what DNSBL does for mail servers" [Zon].* RPZ can be used to block known bad domains and prevent users from visiting malicious websites. This can, for instance, protect a user that clicks on a malicious link in an email from reaching the destination.

2.6 Related work

A lot of research has been done on the various aspects of email security. There exist vast amounts of literature on particular topics such as filtering of spam, end-to-end security, awareness training and phishing. As for *holistic* email security, the selection is limited. A NIST publication titled *'Trustworthy Email'* [CGNR19] provides recommendations for protocols and technologies that improve the trustworthiness of email. The publication includes security measures for authentication of domains, the confidentiality of messages, reducing unsolicited bulk email and end user security. NIST concludes that email communication cannot be made trustworthy with a single package or application, it requires incremental additions of technology adapted to particular tasks. The publication provides a comprehensive view of email security, but does not include the senders and receivers as an element of email. The scope is limited to the technical aspects, listing a wide selection of security protocols and technologies, while neglecting the human factors.

Agencies similar to NIST in other countries have also published guidances and recommendations for email security, but with a much more limited view of email. In Norway, The Norwegian National Security Authority (NSM) has published an article titled *'Basic measures for securing email'* [Sik17]. Despite the title, the article is limited to transmission between MTAs, solely focusing on STARTTLS, SPF, DKIM and DMARC. There are other NSM publications that focus on different aspects of security, however not particularly for email. For instance, one article [Sik16] lists ten important measures to protect IT systems against cyberattacks. In the article, four measures are said to stop 80-90% of all internet-related attacks; upgrading software and hardware, patching of products, not assigning users with administrator privileges and blocking of unauthorised programs (whitelisting). NCSC[24], an organisation of the United Kingdom Government set up to give advice and support on how to protect against cyberattacks, have published a guide for IT managers and systems

[24] https://www.ncsc.gov.uk/

administrators on how to improve email security. In a similar fashion as NSM, NCSC limits their scope to TLS, SPF, DKIM and DMARC in the guide. In January 2018, NCSC published a paper titled *Active Cyber Defence - one year on* [Lev18], addressing the effects of DMARC to combat spoofing of government domains. The results are already showing. The number of spoofed messages from @gov.uk addresses has fallen consistently throughout 2017, suggesting the criminals are moving away from this approach as fewer messages reach the end users. Another security mechanism highlighted in the paper is protection using DNS, particularly blocking malware-related domains from the users.

In contrast to the limited selection of past work on holistic *email* security, there is a broad collection of publications on holistic *information* or *cyber* security. Atoum et al. [AOAA14] propose a framework to implement cybersecurity strategies holistically, by transforming strategy requirements into strategic moves that are, in turn, executed to achieve security objectives. Freeman [Fre07] states that a holistic approach to securing an application should be to assess vulnerabilities, threats that can exploit the vulnerabilities, and the likelihood that they will occur. This evaluation can be used by the organisation to prioritise, balance and make trade-offs to achieve a thorough information security strategy. Freeman further argues that ISO270001[25], a standard providing requirements for an information security management system, is a good method of ensuring a high level of holistic security.

[25] https://www.iso.org/isoiec-27001-information-security.html

Chapter 3 Methodology

It is important to set aside time to select a strategy and identify proper techniques and suitable methods for collecting and analysing data before carrying out the research project. General scientific methods have two shortcomings when applied in a technology context. First, while natural science is intended to gather new knowledge about the world without changing it, new technology is developed with the ambition to change the world. Second, natural science is driven by answering knowledge questions, while technology is driven by stakeholder's intention of solving or mitigating a problem. Design science, as defined by Wieringa [Wie14], is a framework intended to accommodate these shortcomings while persisting scientific reasoning. It is the design and investigation of artefacts in context. The artefacts studied are designed to interact with a problem context in order to improve something in that context. An artefact is defined as *"anything designed and created by humans, both as a real, physical object or an abstract concept"* [Wie14]. The term is broad and includes processes, techniques, methods, software and hardware, to name a few examples. For this project, the artefact is the tool that will be created to guide a holistic implementation of email security in companies. The definition of the problem context is *"anything that interacts with the artefact or that has influence on it"* [Wie14]. The context is typically a combination of several elements such as people, goals, budgets, desires and values. An artefact can have several contexts that it interacts differently with. That will be the case in this project, where each company will serve as a different context.

In design science, an iterative process with three steps is performed to design an artefact. This is called 'The design cycle' as it is performed many times in a design science research project. However, for the scope of the master thesis, the project will be limited to one single iteration. The cycle includes the following steps [Wie14]:

- **Problem investigation:** What phenomena must be improved? Why?
- **Treatment design:** Design one or more artefacts that could treat the problem.

- **Treatment validation:** Would these designs treat the problem?

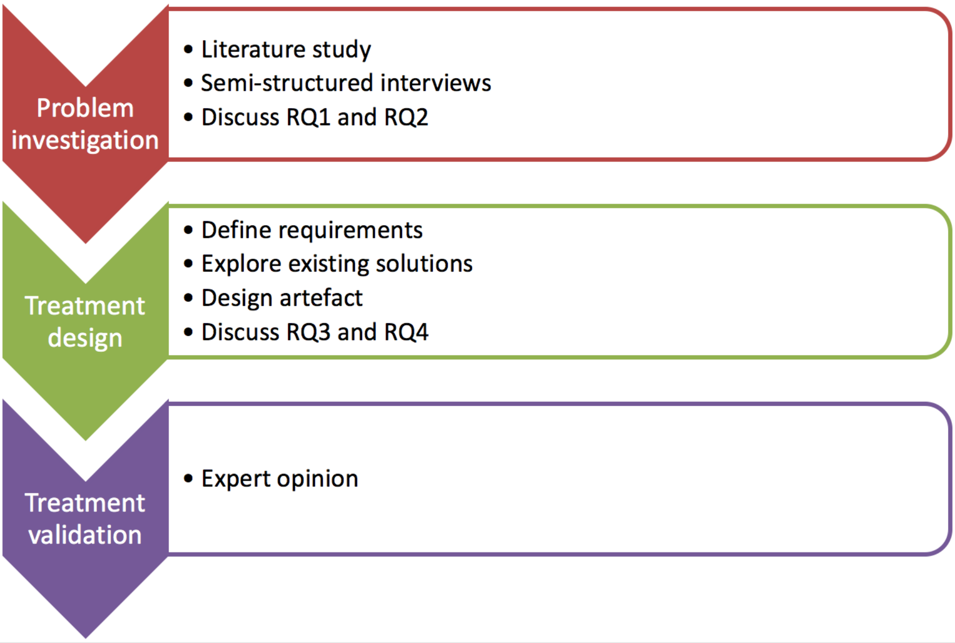


Figure 3.1: The steps in the design cycle and what was done in each step for this thesis.

3.1 Problem investigation

For the problem investigation step, the goals and desires of the stakeholders (the companies the artefact is aimed at solving a problem for) need to be identified. To get a comprehensive understanding of different stakeholders' situations and the problem we are designing a treatment for, the focus in this phase will be on qualitative insight. Two separate approaches will be taken to generate qualitative research data.

3.1.1 Semi-structured interviews

The most common way to generate data in qualitative research is to conduct interviews. Particularly, semi-structured interviews are a popular approach. In a semi-structured interview, the researcher will create a relaxed atmosphere and start a dialogue based on some topics prepared by the researcher. The goal is to make the interviewee reflect upon experiences, beliefs and opinions. The flexible structure allows the interviewer to go in-depth when the informant has a lot on his mind. This effectively allows the researcher to discover new aspects of the topic that was not initially considered, but can be relevant as the professional focuses on it. This approach was considered well-suited in understanding the stakeholders' interest, as they will be instrumental to the direction of the conversation.

Tjora [Tjo12] outlines three phases for semi-structured interviews, shown in Figure 3.2. First, there are warm-up questions, typically simple, concrete questions that do not require any reflection from the informant. Next is the core phase of the interview, consisting of reflection questions. The goal is to have the informant take us on the 'grand tour questions', by sequentially going in-depth on experiences. A question typically begins with *"Can you describe...?"*. For an hour-long interview there should be 3-6 such questions, supported by follow-up questions if necessary. Finally, there will be some questions to wrap up the interview. The intention is to normalise the situation by creating a good transition from the reflection questions. For instance, the researcher can explain what the plan is for the project going forward or what happens to the data from the interview. The researcher should also show gratitude for the informant's time and end the interview on good terms. The interview guide attached in appendix B was used in all the interviews. It was not followed sequentially but rather used as an outline indicating what should be touched on throughout the interview. The subsections of the guide labelled 2.1, 2.2 and 2.3 can be thought of as the reflection questions, whereas the questions in the respective subsection are intended as supporting questions. The interview guide was created before the first interview and was not changed between interviews.

Several factors can influence the quality of the interview, according to Tjora [Tjo12]. Firstly, body language is an important aspect of a good interview. For instance, a nod is an effective way of telling the informant to go on without interrupting him. For that reason, all the interviews were conducted face-to-face with the interviewee. Secondly, to relieve the interviewer from taking notes and allow him to focus on the conversation, the interviews were recorded digitally and subsequently transcribed. Finally, the location of the interview is influential. Being in a safe environment can make it easier for the informant to reflect on personal experiences and beliefs. To make the process as comfortable as possible to the interviewees, all the interviews were conducted at meeting rooms at their respective workplaces.

A total of six potential interview objects were selected. The candidates represented a diversified selection of companies, covering various sectors, sizes and economic situations. The titles and positions of the candidates were distinct, but common for all of them were their responsibilities for the security of the company's email services. It was expected that not all of the candidates would be available for an interview. Out of the six, four of them were interviewed. This was considered a sufficient data set, and additional candidates were not contacted.

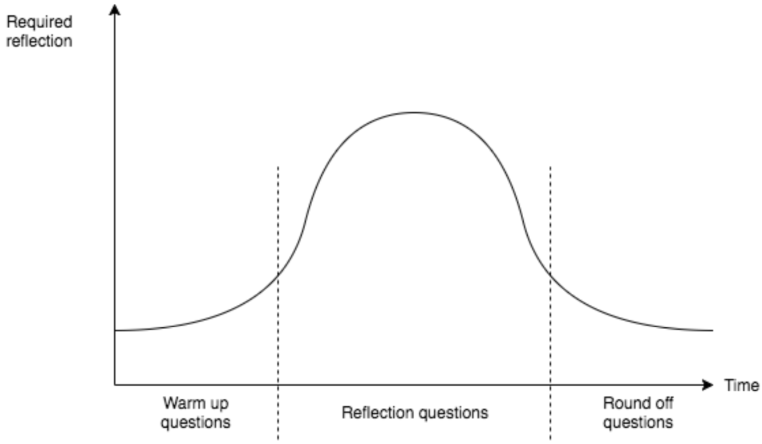


Figure 3.2: Phases of a semi-structured interview. Graphic by Tjora [Tjo12].

Following the interviews, the transcribed data had to be organised and interpreted. Malterud [Mal01] states that qualitative data represent large amounts of information, and analysis implies abstraction and some degree of generalisation. The goal is to use components from the individual informant's history to gain knowledge applicable to others. Miller and Crabtree [CM99] present three styles of analysis of qualitative data. For this thesis, the template analysis style was selected. This is a style where the text is organised according to pre-existing theoretical or logical categories, to provide new descriptions of previously known phenomena. In order to perform the template analysis, a set of categories must first be defined. Braun and Clarke [BC06] outlines a six-step guide to performing thematic analysis. The guide is written for qualitative research in psychology but is also applicable in other fields. Braun and Clarke intend to fill *"the absence of a paper which adequately outlines the theory, application, and evaluation of thematic analysis, and one which does so in a way accessible to students and those not particularly familiar with qualitative research."* [BC06]. As a novice in qualitative research, the intentions of the guide were considered fitting for this project. The first five steps of the guide were followed in order to produce a set of themes and categorise all the interview data according to them. Table 3.1 shows the steps as presented by Braun and Clarke and a short description of what was done in each of them for this thesis.

Transcription of verbal data is often considered to be an excellent starting point in familiarising with and creating meanings about data [BC06]. Having done all the work with interviews myself, the data had been familiarised consecutively during collection and processing. Moving into the second phase, the goal is to generate initial codes. A code *"identifies a feature of the data that appears interesting to the*

Phase	Description of the process	My process
1. Familiarising yourself with your data:	Transcribing data (if necessary), reading and rereading the data, noting down initial ideas.	Interviews were conducted and transcribed afterwards.
2. Generating initial codes:	Coding interesting features of the data in a systematic fashion across the entire data set, collating data relevant to each code.	All data were given initial codes using NVivo. The codes were not pre-defined and emerged during the process (10 in total). Irrelevant data were not coded and hence excluded.
3. Searching for themes:	Collating codes into potential themes, gathering all data relevant to each potential theme.	Codes were grouped and reduced to four potential themes.
4. Reviewing themes:	Checking if the themes work in relation to the coded extracts (Level 1) and the entire data set (Level 2), generating a thematic 'map' of the analysis.	The data were reviewed to see how it fits with the potential themes. Some initial codes were changed to map the data to a more fitting theme. All data were reviewed to validate that the themes embrace the data set as a whole.
5. Defining and naming themes:	Ongoing analysis to refine the specifics of each theme, and the overall story the analysis tells; generating clear definitions and names for each theme.	A definition of each theme was written. During the process, it became apparent that one name had to be changed to describe its associated data better.
6. Producing the report:	The final opportunity for analysis. Selection of vivid, compelling extract examples, final analysis of selected extracts, relating back of the analysis to the research question and literature, producing a scholarly report of the analysis.	This phase was excluded as the thematic analysis is only a part of this thesis.

Table 3.1: The phases of Thematic Analysis, as defined by Braun and Clarke [BC06].

analyst" [BC06]. NVivo[1], a program for analysis of qualitative data, was used to study the transcripts individually, highlighting interesting data and coding it based on the topic. A total of ten code labels were used, listed in table 3.2. The codes were not pre-defined but emerged during the coding. The coding process also served as a filter for the data set by excluding data that was not highlighted by any codes. Having coded and collated all the interviews, the analysis could move into phase 3. This phase involves sorting the codes into potential themes. The ten codes were reduced to four potential themes: Infrastructure, Objectives and strategy, Resources and Measures. In the fourth phase, the themes were reviewed on two levels. The first one involved going through all the coded data and reviewing how it fits with its proposed theme. During this review, it became apparent that some codes contained data that belonged under different themes. In particular, some data extracts coded as 'Drivers' and 'Evaluation' were more fitting under the 'Objectives and strategy' theme than 'Measures' and was therefore moved accordingly. In the second level of phase four, the validity of individual themes in relation to the data set as a whole was considered. One more time all of the data was read through (including the data not initially highlighted), to ascertain that the themes cover the entire data set and assure that additional data within themes has not been missed in earlier coding stages. The result of this phase was the mapping from codes to themes, as shown in table 3.2 and table 3.3. The colours indicate what codes were merged into which themes.

Finally, clear definitions of the four identified themes were created. During this process, it became apparent that 'Objectives and strategy' did not reflect the diversity of its labelled data. To include how the company is organised, their processes and opinions, in addition to objectives and strategy, the name was refined to 'Organisation and attitudes'. The resulting themes and their definitions were:

- **Infrastructure:** Structures that enables email. Including platforms, software, hardware, etc.
- **Organisation and attitudes:** How is the company organised (routines, processes, chain of command, etc.) and what are their opinions on email security (goals, threats, objectives, etc.).
- **Resources:** Assets related to email, particularly money and time.
- **Measures:** Actions taken to achieve secure email.

The interview data of interest from each interview, organised by the themes generated, are presented in chapter 4. In chapter 5, the findings are discussed to conclude

[1] https://innsida.ntnu.no/wiki/-/wiki/English/NVivo

Cloud services
Email Servers
Organisation and strategy
Threats
Economy
Time
User awareness
Technical measures
Drivers
Evaluation of measures

Table 3.2: Code labels from the second phase of the thematic analysis.

Infrastructure
Objectives and strategy
Resources
Measures

Table 3.3: Potential themes, reduced from the initial code labels. 'Objectives and strategy' was changed to 'Organisation and attitudes' for the end result of the thematic analysis.

the problem investigation. For the discussion, the data from each interview has been compared to each other, to identify similarities and differences. Two important elements of data analysis, according to Malterud [Mal01], is decontextualisation and recontextualisation. The former involves lifting out parts of the subject matter and investigating it more closely, together with other elements across the material that tells about similar issues. The latter makes sure that patterns still agree with the context from which they were collected. For the discussion of the findings, each informant's answers relating to the RQs were decontextualised, either as direct quotes or short summaries. In turn, this data was compared for each interview and used to help answering the RQs and hypotheses. Finally, the data was recontextualised to validate that the informant's statements had not been altered when extracted from its original context.

3.1.2 Literature Review

A literature review is an objective, thorough summary and critical analysis of the relevant available research and non-research literature on the topic being studied. On literature reviews, Hart [Har18] states:

> *"The review should be regarded as a process that is fundamental to any worthwhile research or development work in any subject matter in whatever discipline. The researcher have the responsibility to find out what already exists in the area they propose research, before doing the research itself."*

For the literature study conducted in this survey, a traditional review as defined by Cronin et al. [CRC08] has been used. The primary purpose of the literature review is to provide the reader with a comprehensive background for understanding current knowledge and highlighting the significance of new research. By summarising the results of a number of studies, the goal of the review is to identify any gaps in current research on the topic and summarise existing evidence. The step-by-step approach to undertaking a literature review presented by Cronin et al. was followed for the review:

Selecting a review topic was done in collaboration with the responsible professor and supervisor in the early stages of the project. It is important to specify a review topic such that the amount of information available sufficient, yet manageable. Researching 'Email' as a whole would be overwhelming for this project, hence the topic was narrowed down to 'Email security'.

Searching the literature was done using online search engines for academic literature. Initially, Google Scholar[2] and Digital Arkivering og Innlevering av Masteroppgaver (DAIM)[3] were used. Combinations of 'Email' (and 'E-mail') with various relevant terms, such as 'security', 'technical measures' and 'awareness', was used to confine the number of search results. The reference lists of relevant literature were also frequently used to find additional related literature. Relevant publications by institutions acknowledged for their work on security, such as SANS Institute[4], ENISA[5], Symantec[6] and NCSC, were retrieved directly from the respective group's websites.

Gathering, reading and analysing the literature is a comprehensive task, and the researcher should take measures to make it manageable. A good starting point is to read the summaries and abstracts, and decide whether the paper is worth further reading. At the same stage, initial classification and grouping of the articles based on types and themes were performed. Articles on general email security were grouped together, articles focusing on specific protocols were grouped together and so on. When reading the literature, personal notes and text marking was used to keep track of the information and make it easier to look it up at later stages of the project.

Writing about the most relevant findings from the literature review is found in Chapter 2. The background section is based on the literature studied and highlights relevant research and related work on the topic.

[2] Google's search engine for academical literature, https://scholar.google.no

[3] NTNU's digital archive for master theses, https://daimarkiv.idi.ntnu.no/

[4] https://www.sans.org/

[5] https://www.enisa.europa.eu/

[6] https://www.symantec.com/

References are gathered while performing the literature review and are included in the references section in this thesis.

3.2 Treatment design

In the treatment design phase, the goal is to design one or more artefacts that can treat the problem. As we are only creating one artefact, the words ‘artefact’ and ‘treatment’ are used interchangeably. The word *treatment* in design science emphasises that this is a potential solution. Whether the treatment will solve the problem or not is not known until the next stage of the cycle. The processes of the treatment design are shown in figure 3.3. First, the requirements need to be specified. By establishing requirements, we want to answer *“What are the properties desired by the stakeholders?”*, and *“What are the goals for the to-be-designed treatment?”*. The data gathered through the interviews and the literature review is used as a basis when specifying requirements. Having specified a set of requirements, the next step is to look at available treatments. It is not necessary to reinvent the wheel. Existing solutions addressing one or more of the specified requirements can be useful when designing the treatment.

Note that the format of the treatment has not initially been decided on. The treatment design is approached as a dynamic process. By identifying a set of requirements and looking at existing solutions to similar issues, ideas of how the tool can be created arise. Designing the artefact is approached as an iterative process. By creating several drafts and brainstorming various options, the treatment gradually takes shape. The design process is further described in chapter 6.

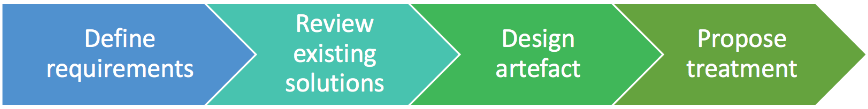


Figure 3.3: The sub-phases of the treatment design phase.

3.3 Treatment validation

In the treatment validation step, the goal is to find out if the proposed treatment is a solution to the problem or not. Wieringa [Wie14] states that since the implementation does not exist yet when performing the validation research, a validation model simulating the implementation needs to be used. An example of a validation model is a prototype of an artefact, which is the case in this thesis. The prototype treatment designed will be exposed to various scenarios presented by models of the context, to validate its applicability and usefulness in the problem context. Wieringa [Wie14] lists various methods to study validation models. A common approach is *expert* *opinion*, where the prototype is submitted to a panel of experts for feedback. The experts need to be familiar with and understand the context, such that they can make reliable predictions about the effects of the artefact in the real-world context. Expert opinion is particularly useful to eliminate bad designs ideas. As the proposed treatment is intended to be used by experts on email security, their opinions were considered fitting for validation. It is also referred to as a simple form of validation, which was appropriate given the limited time frame of the thesis. The requirements to the artefact, that were specified initially in the treatment design, also have an important role in treatment validation. In addition to the prototype, the experts will be shown the requirements as they stipulate what the artefact is supposed to do. The experts will be asked to make reliable predictions about the effects of the artefact in context. More precisely, the experts should explain their prediction in terms of what mechanisms they think will produce the effects. The treatment validation process is further described and its results are presented in chapter 7.

Chapter 4 Findings

Four interviews were conducted and subsequently analysed, as described in section 3.1.1. First in this chapter is an introduction of the industrial context, with a presentation of the four companies and their respective informants. Then follows the findings from the interviews. For each of the organisations, the findings are grouped by the four themes identified during the analysis: Infrastructure, Organisation and attitudes, Measures, and Resources.

4.1 Industrial context

Organisation A is a public institution with close to 70,000 employees and users. The person interviewed is Chief engineer of email infrastructure. Together with a small team, he is responsible for email-related operations in the company. He has more than 30 years of experience working with email in the educational sector and has been involved in implementing the company's current solutions. The company also has an operative security operations centre dedicated to detecting, analysing and handling all types of security incidents in the organisation, including email.

Organisation B is a private software company with about 150 employees across eight countries. The informant's position is Leader of Infrastructure Management, giving him the responsibility for internal as well as third-party hosted infrastructure. That includes the technical aspects of email, such as assuring the availability of the system and that it is working as intended. In addition to a couple of years at his current position, he has several years of experience from similar jobs at other, larger corporations.

Organisation C is a large, private software company with more than 8,000 employees across 15 countries. The Chief Information Security Officer (CISO) participated in the interview. He has worked at the company for 15 years, of which three has been in his current position. The organisation has an incident response team of 12 persons handling security events as well as roughly 300 employees involved in security to some extent.

Organisation D is in the public administration sector and has about 15,000 employees. The informant works as an IT security architect with broad areas of responsibility, including awareness training, configurating systems and defining policies, to mention a few. The company uses many third-party services and only has two internal employees working primarily with security activities.

4.2 Organisation A

4.2.1 Infrastructure

The informant explained that they have migrated parts of their email services to a Microsoft Office 365 cloud solution, but still maintain some internal mail servers. A move to the cloud is planned for additional services, and it is uncertain how long the internal infrastructure will persist. The informant raised concerns about the lack of control in the cloud. He characterised Office 365 as a black box where it is difficult to understand the mail flow, in contrast to the local systems where they have a complete overview. Microsoft was mentioned as a driver for migrating the rest of the organisation's systems to the cloud. The informant exemplified with how services in the cloud are being developed more than local services and how groupware functionalities are improved if the entire system resides in the cloud.

4.2.2 Organisation and attitudes

When questioned if they have a strategy or plan on how to secure their use of email, the informant responded that they do not have any documented strategy relating to email security. He added that securing email is dynamic, what needs to be done depends on what issues, threats and attacks emerge. In the company, it is primarily up to the employees working with email infrastructure to identify needs and establish security measures consecutively. Incidents were confirmed as an important factor for how the email services are secured. The informant exemplified with the distribution of large volumes of spam from compromised email accounts, which was a challenge to the company in the past. For this reason, they have introduced restrictions on mail traffic from users.

The interviewee said that what they try to communicate to their users is that email is not a secure communication medium. He added that the email protocol standards are insecure by default, and their added security measures are not enough to change that. He believed that end-to-end encryption using PGP or S/MIME is *the best we can achieve*, but it is complicated and costly. To achieve a more secure email, he continued, more work is required by the end users. As an argument to why email can never be completely secure, the informant pointed to the sender. A message sent from a trusted address might be initiated by a malicious actor who has gained unauthorised access to a legitimate account, for instance. In the informant's experience, functionality is sometimes prioritised at the expense of security in the company. Migrating to Office 365 is used as an example. He was concerned about moving to the cloud as that gives them less control of the mail flow.

Asked about what types of attacks they fear the most, the informant answered that phishing and compromised accounts have been the most significant threats in the last couple of years. He explained that the diversity in phishing mail makes them challenging to filter out. Sometimes it is a malicious URL, sometimes it is simply text requesting that the receiver sends his username and password. They have also experienced whaling, where persons in leading positions or in the economics department have been targeted.

4.2.3 Measures

Questioned about what measures the company has implemented to secure their email, the informant emphasised that his responsibility is securing email on the SMTP level, from reception of a message to delivery in the mailbox. Hence, he would not comment on measures such as unauthorised access to mailboxes or users sending messages to the wrong person. He justified their choice of measures as *industry standard* and added that they *"have a platform with server software and can pick from services and types of checks available on that platform."* When presenting the specific measures, he started with what he calls *standard protocol checks*. That includes verifying that the message complies to the SMTP protocol and that incoming messages have a real destination address, for instance. The next layer of defence, the informant said, is checking the message's signature against databases of known viruses. They use both a commercial and a free list of malicious signatures. Then follows what the informant described as a *typical content check*, such as checking the link addresses in the message against a list of untrusted domains. In addition, they have sandboxing environments for manually checking attachments, links, etc., when necessary. He explained that in general, they do not deliver messages if they suspect that it might be spam or virus. As a consequence, there is a risk that legitimate mail does not end up in the users' mailbox. They have solved this by giving their users the option to have potentially dangerous messages delivered anyway. He stressed that users who choose this option nees to understand the risk as they will receive infected email that they must handle properly.

When asked if they use SPF, he confirmed that they do have a SPF record, but that there is also produced legitimate emails from the organisation from outside of their domains. The informant told that they are cautious about rejecting messages based on SPF, as the information provided by the verification is considered limited. Similarly, with DKIM, he explained, they try to check signatures of incoming messages.

He argued that the authentication of SPF and DKIM falls short as all messages sent from large freemail providers will pass both checks, but that does not say anything about the messages' legitimacy. Further, he said that they do not DKIM sign outgoing messages and do not act on DMARC policy. Because of the diversity in their email solutions, he believed it is difficult to enforce strict rules. As an example, he pointed at legitimate email from the organisation being sent from mail servers not owned by them, as is the case with email sent from the cloud. It was also confirmed that the organisation uses opportunistic STARTTLS, meaning that if the receiver does not support TLS the message is sent unencrypted. The informant stated that they have a RPZ mechanism to block known malicious sites on a DNS level. He explained that when a user clicks on a link pointing to such a site, the user is redirected to a secure destination with information on why the user was redirected. The organisation also has reactive procedures for particular types of incidents, the informant stated. As an example, he said, that if they find out that virus has been delivered to users, email operations must be notified such that they can remove the messages containing the viruses from the users' mailboxes.

As for awareness training and organisational security measures, the informant said that it is the responsibility of the security operations centre. He remembered having small courses on phishing, spam and general security, but it was shut down. The organisation does not systematically evaluate its security measures, according to the informant. He believed they should have done more of that, to know what the effects of the measures are.

4.2.4 Resources

The informant did not consider economy a limiting factor to email security. He said that if the email infrastructure department believes something is relevant and useful, they will be allowed to purchase it. To elaborate, he listed several commercial products they are currently using. According to the informant, there have traditionally been financial arguments in favour of cloud email solutions, but in his experience, the cloud is *not necessarily cheaper as you still need an operations team.*

When talking about time spent on email security, the informant commented that distinguishing what is email security and what is email operations can be complicated. As an example, he asked if spam filtering should be considered as a security activity or operations since a substantial amount of any mail flow is spam. He emphasised that *he* considers this a security activity, but to others, the security term might be limited to more extraordinary and serious incidents. As a rough estimate, he expected that 25% of their time is spent on email security. Further on time as a resource, he believed that since email is so heavily utilised by malicious actors, there are no limitations to how much time can be spent on email security activities. In particular, reducing the number of false positives and false negatives is something he felt that he should have spent more time doing.

4.3 Organisation B

4.3.1 Infrastructure

The interviewee said that they have opted against cloud services for email. They currently have mail servers running open-source software, but are in the process of changing to Cisco IronPort[1]. The informant explained that this is a commercial solution where equipment and maintenance are bought from Cisco. Compared to the cloud, the main difference is that the email services are hosted on dedicated equipment owned by the organisation. In the interview, not knowing where the email is physically located in cloud solutions was addressed as a dealbreaker. He emphasised that even with contracts in place, you cannot be completely sure where the email is. Moreover, he added that by the contracts with their customers, they are obliged to store email internally. Other than that, the solution the company opted for has similarities with G Suite and Office 365 as it outsources liability; a third-party is hired to take responsibility for securely configuring and operating the system.

The informant believed that their choice of platforms for work is relevant. They are a Linux only production company, with minimal usage of Microsoft systems. He explained that this is relevant because almost all malware is aimed at Microsoft. Opening an attachment, he added, does not carry the same risk on a Linux operative system, as most malicious code will not be able to execute properly. In the informant's experience, all infections have been on Microsoft workstations, whereas they have never experienced any infection on their machines running Mac or Linux.

4.3.2 Organisation and attitudes

Organisation B's overarching plan is to use email less. The informant said that in time, he hopes that they can replace email with a competing tool, with better built-in support for security and cooperation. He added that email uses an old standard and is not secure by default, hence it should only be used for simple communication. He believed that to the stakeholders of the company, the most important is that the email service (alternatively the service that replaces email) *is* working, not *how* it is working. He continued that as the infrastructure and security departments are responsible for operating the service, it is primarily up to them what changes are being made. According to the informant, the organisation primarily has a reactive

[1] Cisco IronPort Email Security Appliances is a commercial email solution, including sophisticated software and hardware. https://www.cisco.com/c/en/us/services/acquisitions/ironport.html

approach; when something happens, they look into the problem and figure out what to do about it. He claimed that because their systems do not have any surveillance functionalities, they are unable to be proactive. He has not experienced any incidents causing damage during his time at the company and admitted that this might contribute to them becoming a little lazy, as the systems have been working for years.

When talking about the importance of having secure email services, the informant stated that he considers email to be one of the biggest threats to the company. He reasoned that it can be time-consuming if there are many problems related to email. As an example, he told about a very costly incident he experienced at a previous workplace, where an infected email spread to almost 80,000 work stations that all had to be shut down and reinstalled. The same incident was used as an example of why email can never be completely secure. It was a zero-day attack, which means that an unknown vulnerability was exploited. The informant explained that since the type of attack is not known yet, there is nothing you can do to protect against it. The importance of email was also touched on from a different perspective in the interview. The informant commented on how dependent employees are on information from their email to do their job, making email a crucial part of the company's operations.

Throughout the interview, it was revealed that the company is in the process of moving from an open source email solution to a commercial one. Asked about the pros of such a solution, the informant responded that it is good to be contracted to a provider with a lot of experience operating email systems for many large customers. A service level agreement with the third-party ensures that any breach of the contract is compensated economically. He added that not being responsible for configuring the solution is an advantage, and it saves them of work.

4.3.3 Measures

Questioned about what measures they have implemented, the informant made the distinction between technical and policy. As for the first, he explained that they filter and scan all incoming messages. The informant confirmed that they have SPF and DKIM, but he was not sure about DMARC. Their current solution only uses freely available blacklists. With the new system they are implementing, the hired third-party will be responsible for filtering of all messages.

On policies, he said that they have rules specifying what is okay to send by email and what is not. Another example given is that they tell the employees not to save anything locally, such that the computer can be reinstalled without losing any valuable data if it is infected. The company has internal workshops and courses a couple of times a year, where they put focus on various aspects of security. GDPR was mentioned as an external driver for email security, requiring that they do not send personal information by email. Asked about how they evaluate their measures, the informant said that they keep track of who have completed the courses and workshops. If an employee has not completed an activity, he will receive a nudge the next time the activity is taking place. He described it as a collective responsibility, where it is expected that anyone can remark if a colleague does something contrary to the policies.

4.3.4 Resources

Questioned about what role economy plays for email security, the informant responded that if they believe a measure is necessary, it is usually not a problem to fit it in the budget. He added that there are *obviously some exceptions* to this, but did not expand further on the matter. The company does not have any formalised economic model, since putting a price tag on a virus infection is difficult and very hypothetical. From the informants perspective, an incident can become very costly and time-consuming, hence he believed that it is cheaper to pay for a commercial security product. The informant described the commercial solution the organisation has opted for as *expensive*, yet he believed it is worth it as they will be relieved of much time-consuming work and the service's responsibility will be transferred to the third-party.

The informant expressed a wish for more time available for security activities. In his experience, other tasks are considered more pressing and therefore are prioritised at the expense of email security. It comes down to allocating a set of resources. He characterised email as *ad hoc.* If they need to configure a new solution, an incident occurs or a server needs to be patched, time will be set aside for that, but in general, they spend *very little* time on email security.

4.4 Organisation C

4.4.1 Infrastructure

Organisation C made the shift to Google's G Suite five years ago. The interviewed CISO complimented the change, positively highlighting features such as security as an integrated part of the service and outsourcing the responsibility of the solution's security to a third-party. The informant rationalised outsourcing to Google as a bet:

> *"Email is a service that we buy from Google. Security is a part of that delivery, hence operating and securing the email solution is Google's responsibility. (...) It is almost like a bet. Do we believe that Google can do a better job than us securing our email platform? Google has the world's largest security department, I think picking them was the right choice."*

The interviewee agreed that what security measures are implemented, depends on what is offered by the selected email solution. He added that it is very uncommon that companies give providers an ultimatum, where they demand that specific functionality is available, or else they will find another provider that offers the functionality.

4.4.2 Organisation and attitudes

When asked about their strategy or plan, the informant emphasised that they receive an out-of-the-box product from Google. For email security, their plan is essentially to outsource it to Google. He added that in recent years, there has been an increased focus on security in the company. For instance, routines and processes have been implemented to become certified and receive compliance reports. While not directly related to email systems, he believed that those measures influence email as well. The informant used the words *awareness raising* to describe the influence of incidents. Every month the company categorises all incidents that have occurred, analysing what types of threats are trending. By analysing events and being able to identify correlations, explaining peaks in graphs, etc., the informant believed they receive a certain acknowledgement that they know what they are doing.

Questioned about the threat email poses to the company, the informant focused on the consequences of email becoming unavailable or unreliable as a service, rather than the effect of a successful attack. Email is not a product of the company, hence he considered it to have a lower priority than the services being sold to the customers. At the same time, he said, if a substantial amount of email were to disappear or many attachments could not be trusted anymore, the consequences would be *quite catastrophic.* The informant proposed end-to-end encryption as the next step in email security. He stressed that the technology already exists, but current solutions such as PGP and S/MIME do not scale well, and lack proper management and availability.

Asked about their threat landscape, the informant stated that their customers (rather than the organisation itself) are often targeted by criminals motivated by profit. Attackers send phishing mail to customers where they pretend to be from the organisation. In the informant's experience, Google is so effective at filtering spam that it is not a noticeable threat. Similarly, he notices a lot less malware today compared to the past, but there are some occurrences. He explained that as a software company, they have a lot of developers that require administrator access to their computers such that they can install *anything.* This can be problematic as not everyone are able to watch their step, he added but stressed that there have not been any serious incidents related to this.

4.4.3 Measures

The product the company buys from Google comes with many technical measures, such as anti-malware and anti-spam based on machine learning. The informant pointed to these functionalities as the greatest sales argument for G Suite, and added that they have seen a major decrease in problems related to spam and malware since migrating to the cloud. He explained that as the filters are always learning, a message can initially be considered as legitimate, but if it is identified as malware or spam later, it will be removed from the inbox. He added that automated and self-learning systems are the future of security, as the time frame of traditional signature-based systems is problematic. He described setting up and configuring SPF and DKIM as an important piece of email security, which they have done thoroughly. However, as a concern with many units and several new acquisitions each year, the informant has experienced it as very difficult to keep all domains up to date. DMARC is also used, but only for reporting. The informant explained that a strict DMARC policy would have a large effect on stopping spam and phishing sent from their addresses, but it would also cause problems for their email systems used for marketing. These are external systems that would need to be added to the SPF record, but that is not possible as there is no more free space in the record. The informant described it as an issue of business versus security, that they need to figure out how to solve properly.

Questioned about what kind of user awareness training they have, the response was that they have *"some, but not much"*. He brought up a presentation he heard at a security conference, where it was made a point that even if you reduce the number of users clicking on a dangerous link from 8% to 4%, you still have 4%. Relating to awareness, he also said that they used to experience cryptolockers in their accounting department frequently. As the job of the employees in that department was to open attachments to pay invoices, the informant was not surprised that such incidents occurred more often in this department than in the rest of the company. The subject was then changed back to technical measures. He explained that they have a blacklist in DNS that is quickly updated when new threats appear. AppLocker is another mechanism praised by the informant, as it prevents malware from executing by specifying what programs are allowed to run on the machine. The informant explained that they have some policies they try to communicate to the employees. For instance, no systems should send email to customers with links. Another example was that email should not be used for personal data, to ensure privacy and GDPR compliance.

4.4.4 Resources

The informant described G Suite's economic model as simple. There are three options - G Suite standard, work or enterprise - each with a fixed price per inbox. The company have opted with the latter, including more advanced security features and accordingly being more expensive. The informant explained that the move to the cloud was not motivated by saving money. However, they are left with the impression that the cloud has been cheaper than the previous solution. This is heavily due to G Suite containing file storage and software for text editing, spreadsheets, etc. as well, allowing the company to terminate licenses to, for instance, Microsoft Office and OneDrive. A remark was made that they have opted to spend *some extra* money by selecting the enterprise product, but the informant did not further comment on whether or not email security is considered expensive.

The interviewee expressed that more time could have been spent on security. In the organisation, they have experienced a domino effect of sorts, as more advanced surveillance systems generate more events requiring investigation. In the informant's experience, the moment they start to look at all suspicious activity, the time-consumption increases. He also commented on security mechanisms' role in reducing the workload. The informant described automatic filtering as decisive in making the effort required by the security team manageable. If there were no mechanisms in place to reduce the volume of email, he believed, it would be an impossible service to use. Regarding time, the informant also commented on how some activities that are now taken care of by Google (patching, updating anti-virus, etc.) have been replaced with new needs, such as administrating G Suite users.

4.5 Organisation D

4.5.1 Infrastructure

The informant said that the organisation migrated to G Suite three years ago, primarily driven by the need to replace their outdated Exchange infrastructure. He later specified that one of the improvements when changing infrastructure, was *"access to mechanisms such as TLS for encryption, DKIM, DMARC and so on"*. In his experience, they do not have less control in the cloud compared to their previous solution. However, he stressed that their past mail servers were not internally hosted either, they were outsourced from a third-party. The informant stated that because Google is a large company and has security standards and certifications they comply to, he feels safeguarded by them. The company has third-party providers for network administration, application management and other services as well. The informant confirmed that his job is to stitch together the products from the different providers and assure comprehensive security in the organisation. He specified that for email, they are responsible for configuration and specifying policies, even though Google operates the solution.

The informant brought up a particular threat related to their choice of infrastructure, with the potential to cause a lot of harm. He explained that G Suite uses application programming interface keys for access control. If such a key is compromised, the attacker does not only get access to one user account but the entire email platform. He added that key management and access control is something they have a significant focus on, as the consequences of an incident can be large.

4.5.2 Organisation and attitudes

The informant confirmed that they have a security strategy, but it has not been updated in recent years and does not reflect the company's current focus on email security. The document contains guidelines and user policies, like what is acceptable to send by email and what is not. They experience that a lot of sensitive data is sent by email, even though there are other tools and services in place where it can - and should - be securely uploaded. On a technical level, however, the strategy is lacking. The company does not have a formalised policy on this level, but rather strive to follow best practice, as recommended by NSM and other standardisation agencies. The informant added that they depend on what is offered by their provider and that they try to utilise the security functionalities available in the solution. The informant stated that he has not experienced any incidents related to email at the company. Questioned about how that influences the situation, he answered that one might think the lack of incidents contributes to an insufficient focus on security. However, he believed there has been and still are enough incidents elsewhere to point out what needs to be done in terms of security measures.

The informant stated that email needs to be as secure as possible while persevering its availability and usability. Email must be available on the surfaces needed by the users, with security mechanisms in place making it *sufficiently secure*. He also said that *"it is clear that email should never be a super secure communication channel"*. He brought up the receiver as an example of a non-negligible source of insecurity. No matter how well you secure your end of the system, you are not in control of the receiver's email. As a consequence, he added, you can never be sure that the message is treated securely by the receiver.

When asked about the email threats to the organisation, the informant referred to what he said about sensitive data being sent by email instead of using existing, secure alternatives. He expressed that primarily, threats relate to the users and user training. For instance, there must be awareness of what is okay to send by email and what is not, and knowledge about the risk of misdirecting an email or being tricked into handing over sensitive information.

4.5.3 Measures

On technical measures, the informant confirmed that they are using Google's anti-malware and anti-spam. He added that it *"looks like it is working pretty well to handle content checking, malware and spam."* As for server protocols, he said that they have been through a process of introducing DMARC, together with DKIM and SPF. He added that currently a failed DMARC check, typically due to a failed SPF or DKIM verification, places a message in quarantine. When asked if they have experienced any problems with third-party providers not being compatible with the aforementioned server protocols, the informant responded that they have a policy requiring that all their systems have support for both SPF and DKIM. How mailboxes are protected against unauthorised users was also addressed in the interview. According to the informant, G Suite provides 2FA and a mobile device management solution that they are using. The informant explained that device management involves conforming to certain requirements, such as requiring authentication and storing data encrypted, to be able to access G Suite on the device.

On human factors, the informant stated that they try to have awareness training regularly, such as sending short learning modules on various topics by email. For example, a topic in the past has been how to recognise a phishing email, where they also performed a phishing simulation. He described the measures as a *"good procedure to generate awareness"*. When talking about the threats to email, the informant emphasised the importance of having layers of security. They depend on Google to filter out malicious code, but if it bypasses the filter and reaches the end user, they rely on the user to handle it securely.

Questioned about how they evaluate their security measures, he responded that they use the reports from DMARC to have an overview of what is being sent from their domains. The reporting from Google's filtering is limited, he added, but they receive monthly reports from their security providers with the number of incidents, the number of viruses, types of threats and similar.

4.5.4 Resources

In contrast to organisation C, this organisation have opted with *G Suite for work*. The informant explained that the additional features of the enterprise level are not considered *good enough*. For instance, he added, one feature is automatic detection of sensitive content, which cannot be effectively used in the company's context as there is a vast disparity in what is considered sensitive. The informant affirmed that while they are considering acquiring additional sandboxing functionalities, they feel like they have the measures that they want.

A need for more time to spend on security activities was considered little by the informant. Some improvements could be made with more time, but overall, he considered their current time resources as sufficient. The informant said that in periods they spend more time on email security, for example, if they make considerable changes or implement new measures. Other than that, email security activities *"is not primarily what they spend time on"*.

Chapter 5
Discussion, part 1

This chapter concludes the problem investigation phase. The interview findings presented in chapter 4, supported by the data gathered in the literature review, as described in section 3.1.2, are used as a basis to answer RQ1 and RQ2. For both questions, a set of hypotheses have been explored. The results will be discussed in line with the RQs. Finally, the problem investigation phase will be summarised.

5.1 RQ1: How companies secure email

The first RQ, *How do companies secure their use of email?*, was primarily explored by answering the hypotheses H1 and H2, as defined in chapter 1. Each of the hypotheses will be presented and discussed in the following subsections. Following the discussion in light of the hypotheses, general observations that apply to RQ1 will be discussed.

5.1.1 H1: Companies have a strategy/plan on how to secure their use of email.

In each interview, the informant was asked if they have a defined plan or strategy on how to secure their use of email. Exactly what was meant by 'plan' or 'strategy' was not further specified when the questions were asked, to leave the interviewees a certain room for interpretation. All the informants rejected that they do have a *documented* strategy or plan on email security. The informants were not explicitly asked to explain *why* they do not have a documented plan, but it was touched on as they explained how they work with email security. The terms *ad hoc* and *reactive* were used by several informants to describe their approach to email security. In the interview data, there is a trend in the companies that when something happens, what is necessary to solve it is done. Our interpretation of this is that it is a contrast to formulating a strategy or plan, which is considered a proactive and structured process. A recent survey of Norwegian organisations [Sik18] concludes that a majority of businesses have a framework and/or management system for information security.

With this in mind, the absence of a documented plan or strategy in the interviewed companies was considered surprising. Although having a framework or management system does not necessarily mean that the company has a strategy or plan, we would have expected that at least one of the companies that we interviewed have it.

While not having a *documented* plan, three of the informants expressed a plan for email security. One informant stated that their plan is to use email less as it is an insecure communication medium. Another informant explained that as a G Suite customer, their plan is essentially to outsource email security to Google, at least the mailbox security. The third informant answered that they strive to follow what is considered best practice. The plans were expressed as personal goals, rather than verifiable objectives. The plans have not been created from common ground, making them difficult to compare across companies.

5.1.2 H2: The companies feel like they have to accept a certain amount of insecurity.

Even though there are many security extensions for email available, it is a common conception that email cannot be completely secure. To facilitate the open-ended nature of the semi-structured interview, this hypothesis was not expressed directly as a yes-no-question in the interviews. Instead, it was attempted to have the informants confirm or deny the hypothesis indirectly by asking about threats in general, security measures they have and the role of email security in the company. From the interviews, there is an undeniable agreement with this hypothesis. All the four informants emphasised that email can never be completely secure, that it is insecure by default and security measures is not enough to change that, and that it is clear that email should never be considered a super secure communication channel. Examples of threats that cannot be protected against, that were brought up by the informants included unauthorised use of legitimate addresses, zero-day attacks and compromise of the receiver's mailbox. End-to-end encryption was also brought up in more than one interview as *"the best we can do"* in terms of security, implying that complete security is not possible.

Although the informants agreed that their companies have to accept a certain amount of insecurity, there is a diversity in how they felt about it. Two informants stated that functionality is prioritised at the expense of security. Of the two, one of them believed that it is a good thing to balance usability and security, whereas the other was concerned about functionality outweighing security.

5.1.3 General observations

The email platform or solution of the companies appears to be an important factor for how the companies implement technical email security. The two companies that have outsourced email to Google expressed that the product they buy includes security. Essentially, they trust Google to provide the security measures necessary to be protected against threats. Similarly, the organisation in the process of changing to IronPort will trust a third party to protect the company's email. The final organisation supported the claim, as he confirmed that they have a platform with a set of security services and checks to choose from. Moreover, one of the informants explicitly stated that in general, what security measures are implemented in companies, depends on what is offered by the selected email solution. He further added that the companies rarely demand specific functionality from the providers. Rather than selecting a platform based on the security measures available on it, security measures are selected based on what is offered by the company's platform. One informant explained that they do not work reactively with email security because their systems do not have any surveillance functionalities. In that case, the informant is limited by his platform. However, the opposite can also be the case. As one of the informants pointed out, migrating to G Suite gave them access to several useful mechanisms for email security. The phrasing gave the impression that he was referring to mechanisms that they might not otherwise have implemented. In that sense, the choice of platform or solution can have a positive impact.

Another observation from the interviews is the disparity in the companies' objectives and considerations. As the companies belong to different sectors and vary significantly in the number of employees, it is expected that they present different contexts. To one company, cloud email services was not an alternative because then they do not know where the email is physically located. That was a decisive factor because in the contracts with their customers, they oblige to store email locally. Whereas one informant complimented how the cloud relieves them of email security responsibilities, another informant criticised email in the cloud for being a black box. Personal beliefs and experiences of the informants interviewed might be a factor contributing to the differences. However, given the diversity in structures and assets of the companies, we believe they will have different needs and objectives independently of the informants' subjectivity.

5.2 RQ2: Drivers and barriers for security measures

RQ2, *What drivers and barriers are there for implementing email security measures?*, was examined by answering hypotheses H3, H4, H5 and H6, as defined in chapter 1. Each of the three hypotheses will be presented and discussed in the following subsections.

5.2.1 H3: An incident motivates securing the flaw that caused the incident.

In the interviews, the organisations were asked if they have experienced any incidents related to email in the past, and how their incident track record has impacted email security. Before this question was asked, some of the informants had already stated that what security measures are implemented depends on what issues emerge. The reactive approach to security of some of the companies implies that incidents dictate what measures are implemented. Incidents are described as an *important factor* and *awareness raising* for how the company secures email. One of the informants suggested that you do not have to be the victim of an incident for it to have an influence. He believed that incidents to other companies can be used to point out what needs to be done in terms of email security in your own company.

5.2.2 H4: Employees are considered the weakest link by companies.

There was a disparity in the informants' interest in human factors of email security. While some brought the topic up themselves and had a lot to say about internal lectures, campaigns and similar measures that raise awareness on security, others had little to say about it even when asked directly. A factor contributing to this is probably that the informants had different positions at their respective companies, with different responsibilities of the human aspect.

A recurring statement in the interviews was that the organisations have policies on what is okay to send by email and what is not. For instance, that email should not be used to send personal or confidential data. This was highlighted as the biggest threat to the company in one of the interviews. Another informant referred to GDPR as a driver for not sending sensitive data unencrypted by email. These comments portray the employees as a weak link, posing a large threat if the company's policies are not followed - intentionally or by accident. One informant said that if you reduce the number of employees clicking on dangerous links from 8% to 4%, you still have the 4%. This comment suggested that the users pose a non-negligible threat to the company, implying that employees are a constant weakness. Data from *The Unrecorded Statistics Study 2018* [Sik18] supports the idea of the employee as a weak link. More than half of the respondents to the survey believed a human error to be a cause to the incident.

5.2.3 H5: Email security is considered time-consuming by companies.

As commented on by one of the informants, distinguishing between security and operational email activities can be difficult. When the informants estimated how much time they spend on email security, it was relevant what activities they include in the estimation. However, what each considered as a security activity was not accounted for, as the focus in the interview was on the informant's experienced time-consumption rather than the actual, quantified time spent on security. Three of the informants stated that more time could have been spent on security. Based on their explanations, our interpretation is that the informants did not have a *need* for more time, but they believed that improvements could be made if they had more time. For instance, one interviewee brought up fine-tuning spam filters, and another one mentioned extending what activity is monitored, as activities they could spend more time on. The fourth informant agreed that some improvements could be made with more time, but he considered the need for it as little.

The informants did not give the impression that email security is a time-consuming activity. Two of them emphasised that they do not spend much time on such activities. One of the other expressed that automated filters are essential to reduce the workload, as the volume of email would be impossible to handle if not for these security mechanisms. We interpret this as an argument to how time needs to be spent on security activities in order to reduce the time-consumption of other email activities.

5.2.4 H6: Email security is considered expensive by companies.

The informants were asked about the role economy plays for email security. Economy was expected to be a limiting factor for how the companies implement security. Surprisingly, it was suggested that economy is not a significant consideration to the email security of any of the organisations. In the informants' experience, if they believe a measure is necessary, they will be allowed to purchase it. One of them further argued that they do not have a formalised economic model since putting a price tag on a virus infection is difficult and very hypothetical. This relates to what was discussed in subsection 5.1.1, that the organisations do not have documented plans on how to achieve secure email, but rather do what is necessary when it is necessary.

5.3 Problem investigation

To summarise the problem investigation, a set of challenges to and shortcomings of email security has been written. The list is based on the discussion above as well as the literature review in chapter 2.

- There is an absence of documented plans for email security. Most organisations work reactively and approach email security ad hoc.

- Each organisation has different assets, processes and structures, hence different needs in terms of security.
- Email security is not considered a time-consuming activity and is hence not allocated a lot of time.
- Choice of platform decides what technical security measures a company implements, not the other way around.

The list will serve as the foundation for the creation of requirements in the treatment design in chapter 6.

Chapter 6 Treatment design

In this chapter, the process of designing the artefact is presented. From the beginning, the artefact was intended to be a tool to guide holistic email security. However, the exact format of the tool was not pre-determined. Throughout the problem investigation phase, a set of shortcomings and challenges to how organisations implement email security was identified, as summarized in section 5.3. In the following sections, the specifications of the treatment are defined as a set of requirements. Then, existing solutions relevant to the treatment we are creating are presented and discussed. Finally, how the treatment was created is described, and the proposed treatment is presented.

6.1 Treatment requirements

Based on the problem investigation phase and the thesis' overall goal of creating a holistic security tool, a set of requirements for the treatment was created:

- **Comprehensive.** The treatment will include all elements involved in email.
- **Flexible**. The treatment will be applicable to different contexts, i.e. companies of different sizes, sectors, etc., and will not be platform-specific, i.e. can be used by companies using cloud email services as well as locally hosted Exchange servers.
- **Guiding.** The treatment will provide companies with a set of options for how to implement email security.
- **Identifying.** The treatment will be used to identify weaknesses in and threats to companies' email security.
- **Quantifying.** The treatment will enable comparing and/or quantifying email security between companies, by establishing a common ground.

– **Effective.** The treatment will not require a lot of time to be used.

Ideally, the requirements would be formulated such that they are measurable and easy to verify. In particular, *a lot of time* is a vague term that can be interpreted differently by individuals. However, as effectivity was a desirable feature of the treatment and the basis was considered insufficient to quantify the time requirements, the sixth requirement was kept as is.

6.2 Existing solutions

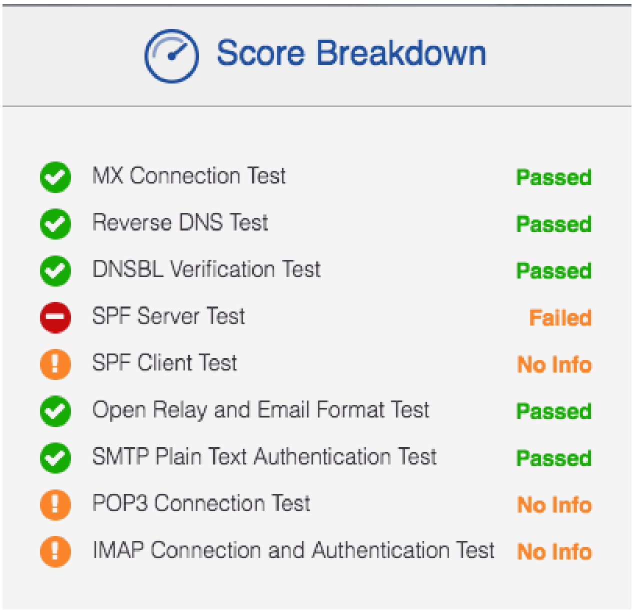
There are several tools available online where the security of email domains can be tested, i.e. Internet.nl[1] and Email Security Grader[2]. Internet.nl uses public DNS records to produce a report on how a domain complies to a set of proposed standards, including DNSSEC, DMARC, DKIM, SPF and STARTTLS. In Internet.nl's explanation of the test report, it is emphasised that this is only a compliance test, and there are more aspects which are important to email security. Email Security Grader also focuses on the mail server, assessing its DNS availability, how SPF is configured, how the servers handle invalid SMTP headers, authentication and more. An example result of a security test using Email Security Grader is shown in figure 6.1. These types of tools can effectively be used to verify certain elements of email security, but are limited to publicly available information.

Various frameworks and tools have been created to simplify security testing when developing applications or programs. For instance, a checklist of possible threats or recommended security features can be used to guide the developer. OWASP Application Security Verification Standard (ASVS)[3] is a tool created for testing of security in web applications. ASVS contains an extensive list of verifiable security requirements. It is created to help organizations develop and maintain secure applications and to help vendors and consumers to align their requirements and offerings. ASVS is suggested as a blueprint to create a security checklist specific to your application, platform or organization. The standard defines three levels of security verification. The first level contains basics security requirements to protect against common, low-cost threats. Level two is achieved by applications that are secured against most of the risks associated with software today. The third level is characterized as *high value, high assurance or high safety*, and is typically reserved for applications that require significant levels of verification. These levels of verifications allow an organisation to select requirements based on their risk profile. ASVS is not directly applicable to email, but the concept and benefits of the tool can be transferable to an email security context.

[1] https://internet.nl/

[2] https://emailsecuritygrader.com/

[3] https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project



Score Breakdown

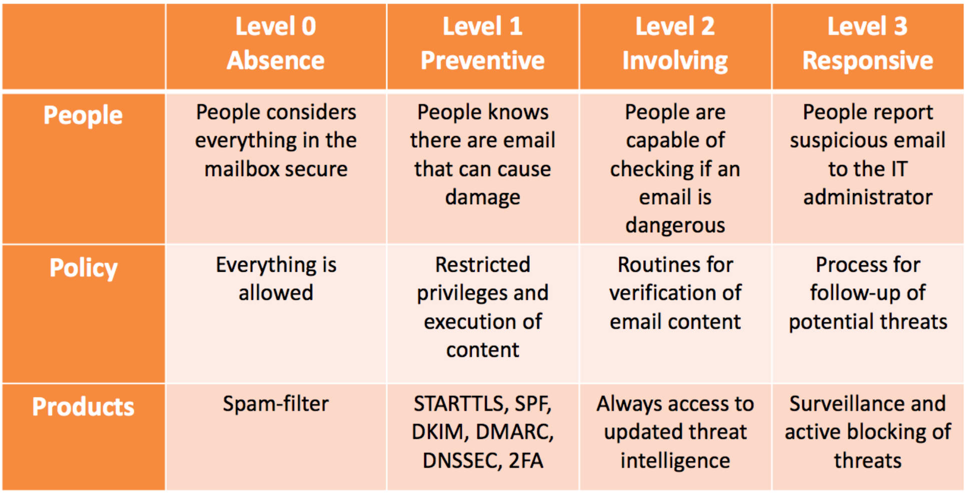
✓	MX Connection Test	Passed
✓	Reverse DNS Test	Passed
✓	DNSBL Verification Test	Passed
⊖	SPF Server Test	Failed
!	SPF Client Test	No Info
✓	Open Relay and Email Format Test	Passed
✓	SMTP Plain Text Authentication Test	Passed
!	POP3 Connection Test	No Info
!	IMAP Connection and Authentication Test	No Info

Figure 6.1: Example result from a scan with Email Security Grader. Nine security tests are performed on the domain, and graded as Passed, Failed or No info.

In a blog post by Secure Practice[4][Gja18], a Norwegian company specialized in digital security, a comprehensive approach to email security is presented. A set of security measures are listed, and grouped by a dimension - people, policy and products - and a maturity level - absent, preventive, involving, responsive. For each dimension, what is necessary to achieve a certain maturity level is listed. For instance, the table can be used to understand what is expected of the users to reach a responsive level of security. The original table is written in Norwegian, but it has been translated in figure 6.2.

From the existing solutions, certain features or concepts stood out as interesting. Grouping security measures based on dimensions provides a context for the measures and more clearly shows what the measure applies to. We believe this can simplify *'the big picture'* of email security. Another desired feature for our treatment is verifiability. If an employee is provided with a set of security requirements, the requirements should be created such that it is easy for the employee to verify whether they are achieved or not. If the conditions are open for interpretation, it is expected to be more difficult and time-consuming for the employee to go through the requirements. The option to automate tests where possible is also considered a major benefit. The time-consumption can be reduced by not having to perform a manual check, i.e.

[4] https://securepractice.no/



	Level 0 Absence	Level 1 Preventive	Level 2 Involving	Level 3 Responsive
People	People considers everything in the mailbox secure	People knows there are email that can cause damage	People are capable of checking if an email is dangerous	People report suspicious email to the IT administrator
Policy	Everything is allowed	Restricted privileges and execution of content	Routines for verification of email content	Process for follow-up of potential threats
Products	Spam-filter	STARTTLS, SPF, DKIM, DMARC, DNSSEC, 2FA	Always access to updated threat intelligence	Surveillance and active blocking of threats

Figure 6.2: A comprehensive approach to email security. Each measure is given a maturity level (column) and dimension (row). Adapted from [Gja18].

validating DNS records and handling of invalid SMTP headers.

6.3 The design process

At this point in the process, creating a scenario-based framework or checklist had emerged as the leading candidate for the treatment. The idea was to provide professionals working with email security with an overview of threat scenarios and what measures can be implemented to protect against the scenarios. The treatment design was an iterative process. First, several drafts of potential treatment structures were created. Then, the drafts were presented to and discussed with the project's supervisors. From there on, the artefact gradually took shape. In the following subsections, the design process for the different parts of the treatment is presented.

6.3.1 Defining layers of security

One of the requirements for the treatment was that it needs to include all the elements involved in email. To accommodate this, figure 2.2 from chapter 2, which shows the key components of email, was used as a basis. The key components were grouped in what we will refer to as *layers*, each representing a dimension where email security measures can be implemented. In the first iteration, shown in figure 6.3, the components were grouped in four layers. The first layer, *User*, refers to the people sending and receiving email. *MUA and Mailbox* involves the receiving and sending MUAs, as well as the receiver's mailbox. *Mail server* includes the source and destination mail servers, and *DNS* is the DNS server.

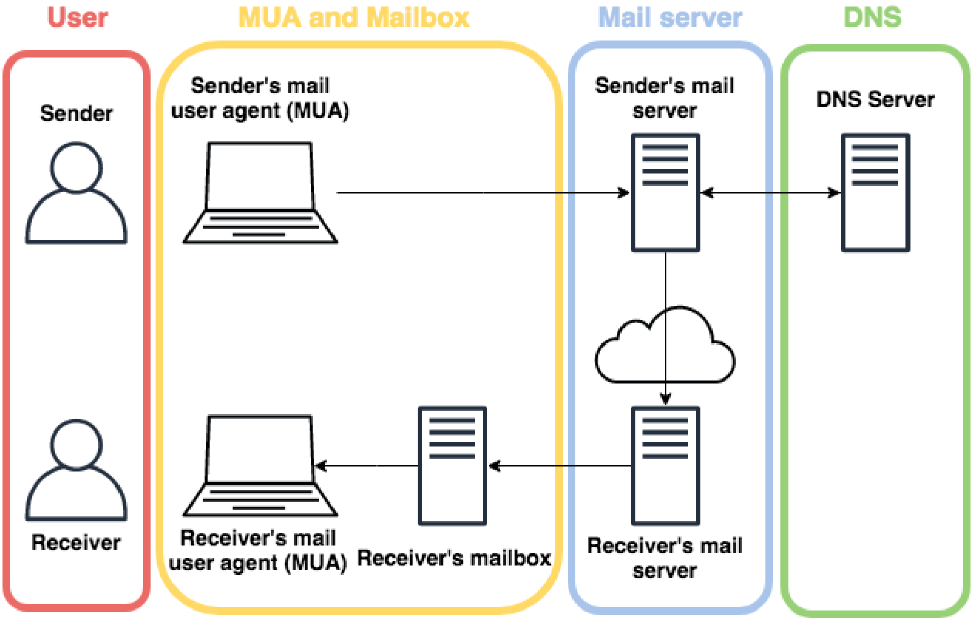


Figure 6.3: Iteration 1 of defining layers: Four layers of email security.

A few shortcomings were identified when evaluating the four layer-model. First, as the model was based on a simplified illustration of a mail flow, only the sender's mail server communicated with the DNS. Certain security measures, i.e. SPF, requires that also the receiver's mail server communicates with the DNS server. Second, there are security measures implemented on the client device. Instead of naming layer two *MUA and Mailbox*, the name was changed to *Client and Mailbox*, to include measures implemented on the client, such as anti-virus or 2FA. Third, whereas the simplified figure contains one receiving mail server, in reality, there might be several servers a message has to pass through before reaching the receiver's mailbox, i.e. spam filters, content scans and sandboxing environments. To emphasize that this layer includes all proactive security measures acting on messages entering or leaving the system, the layer is renamed to *'Mail Gateway'*. Finally, some security measures did not fit into either of the four layers. A particular scenario from one of the interviewed companies was that an attack is disclosed after the emails involved in the attack has been delivered, and the system admins need to search and destroy all the emails involved in the attack. Another example was the incident response team of one of the organisations that monitors the network and actively responds to threats. To include this family of security measures, an additional security layer titled *Surveillance and reactive handling* was added to the model. The result of the second iteration is shown in figure 6.4. Table 6.1 provides additional descriptions of the five layers.

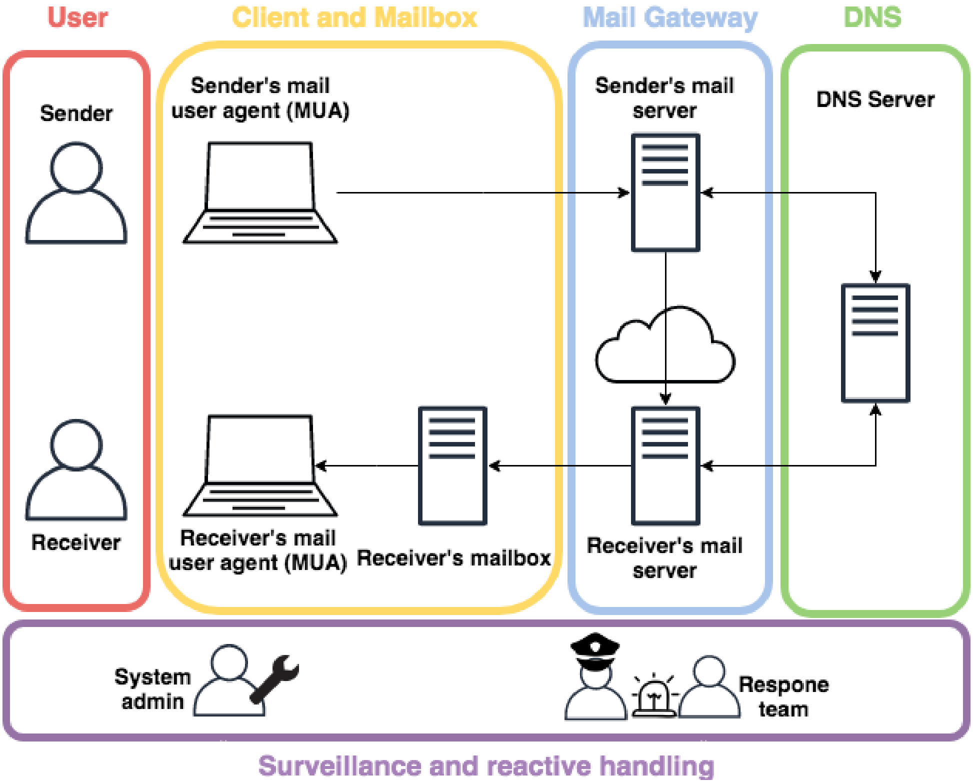


Figure 6.4: Iteration 2 of defining layers: Five layers of email security.

6.3.2 Defining threats

It was considered convenient to define a set of threats before creating the scenarios. In section 2.2, four common threats to email were listed: malware, phishing, spoofing and spam. In addition, two threats were brought up in interviews by the informants: unintentional actions by authorized users and unauthorized access. The former involves accidental acts such as sending an email to the wrong recipient, and deliberate actions that are unintentionally harmful, such as sending sensitive data in an unencrypted mail. Unauthorized access includes, amongst other things, access to read email in another users mailbox or send messages from their client. An important consideration when defining threats was to decide on an abstraction level. *Malware* can be listed as one threat, but it can also be separated into *Ransomware*, *Trojans*, *Malicious macros*, etc. It was considered most appropriate to use high-level definitions of the threats. The list of threats, shown in table 6.2, are intended to give an overview of the types of threats, whereas the scenarios and security measures will provide a greater level of detail.

#	Layer	Description
L1	User	The humans involved in sending and receiving an email.
L2	Client and Mailbox	The equipment of the end user, i.e. computer or cell phone, that enables sending and reading email, and the mailbox where the messages are stored.
L3	Mail Gateway	The entities that all incoming and outgoing emails pass through, including the mail servers running the MTAs, spam filters, content scans, etc.
L4	DNS	All the DNS servers that provides the DNS service.
L5	Surveillance and reactive handling	Surveillance systems, threat intelligence, system admins and other entities involved in monitoring and reacting to email events.

Table 6.1: The five layers of email security.

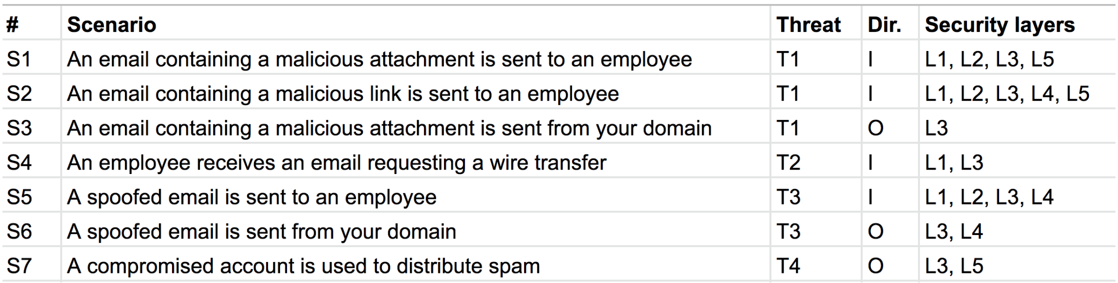
#	Threat
T1	Malware
T2	Phishing
T3	Spoofing
T4	Spam
T5	Unintentional actions by authorized users
T6	Unauthorized access

Table 6.2: List of email threats that will be used to create scenarios.

6.3.3 Presentation of scenarios

"How can the scenarios be presented in such a way that they provide an overview of what needs to be protected against, and how to protect against it?", was the question we asked ourselves going into this phase. Initially, the idea was to present specific scenarios mapping to a particular layer, such as *"The server receives an email containing a malicious attachment"* and *"The user receives an email containing a malicious attachment"*. A potential issue with this approach was that the layers become isolated from each other. Instead, a list of general email threat scenarios was created. As an example, the aforementioned layer-specific scenarios with malicious attachments were merged to one single scenario; *"An email containing a malicious attachment is sent to an employee"*. For each scenario, the layers where security measures for the scenario can be implemented were listed.

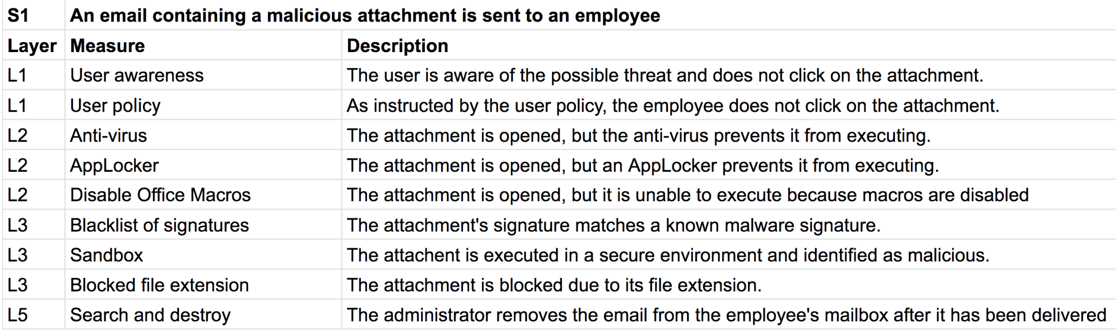
An additional concern was how to distinguish between email threats directed *at* the company and *from* the company. To use spoofing as an example: One scenario is that an employee receives a spoofed email, whereas spoofed email sent from your domain is another scenario. This was not considered a crucial feature of the treatment, but it was expected to contribute to the simplicity and understanding of the scenarios. A column titled *direction* was added to the table of scenarios, where 'O' (outbound) was used for threats directed out from the company, and 'I' (inbound) for threats directed at the company. Some threats are neither inbound or outbound, where the label is left blank. Figure 6.5 contains a portion of the list of scenarios and shows how the guide is presented to the user.



#	Scenario	Threat	Dir.	Security layers
S1	An email containing a malicious attachment is sent to an employee	T1	I	L1, L2, L3, L5
S2	An email containing a malicious link is sent to an employee	T1	I	L1, L2, L3, L4, L5
S3	An email containing a malicious attachment is sent from your domain	T1	O	L3
S4	An employee receives an email requesting a wire transfer	T2	I	L1, L3
S5	A spoofed email is sent to an employee	T3	I	L1, L2, L3, L4
S6	A spoofed email is sent from your domain	T3	O	L3, L4
S7	A compromised account is used to distribute spam	T4	O	L3, L5

Figure 6.5: A portion of the list of scenarios, as they are presented in the treatment.

The list of scenarios includes which layers security can be implemented at, but does not provide any specifics on how. The next step was to enable drilling down on scenarios. For each scenario, there is a list of security measures, including a description of what each measure protects against and what layer it is implemented on. An example is shown in figure 6.6. The intention is that a person responsible for email security in a company uses the list to get an overview of how to protect against a threat scenario. One of the reasons why the measures are presented in the context of a scenario is that it is believed to improve their verifiability. For example, during the interviews, it was clear that *"Do you use SPF?"* was a difficult question for the informants to answer strictly *"yes"* or *"no"* to, because most of them partly use SPF. If we had asked them if they use SPF in specific contexts, such as *"Do you filter incoming email based on SPF verification?"* or *"Do you have a SPF record?"*, it would have been easier for them to provide a yes-no-answer. If each measure is presented in such a way that it is easy for a security professional to answer whether they have implemented it or not, the guide can be used to effectively map how they are secured and what can be done to improve the security, against a given scenario.

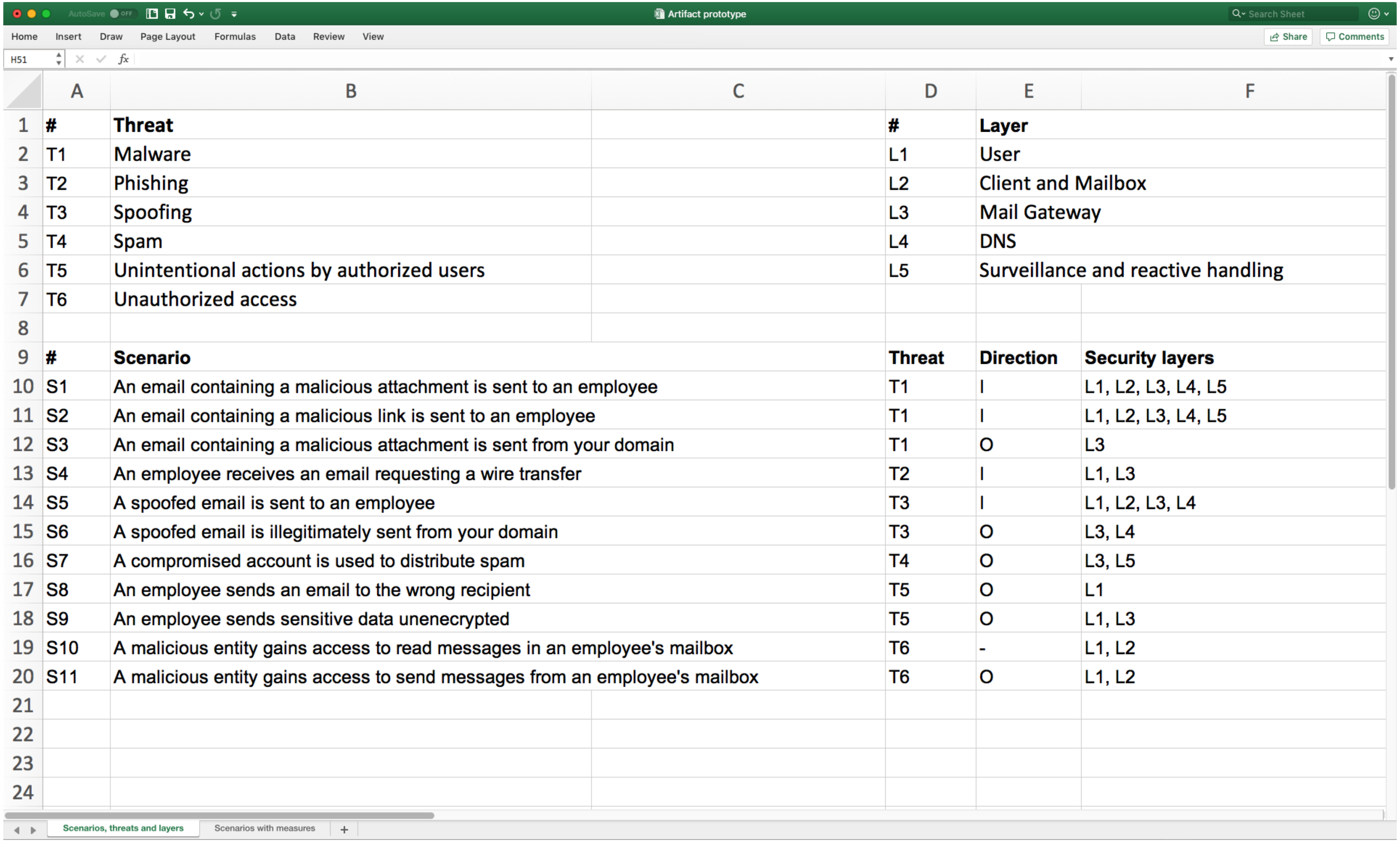


S1	**An email containing a malicious attachment is sent to an employee**	
Layer	**Measure**	**Description**
L1	User awareness	The user is aware of the possible threat and does not click on the attachment.
L1	User policy	As instructed by the user policy, the employee does not click on the attachment.
L2	Anti-virus	The attachment is opened, but the anti-virus prevents it from executing.
L2	AppLocker	The attachment is opened, but an AppLocker prevents it from executing.
L2	Disable Office Macros	The attachment is opened, but it is unable to execute because macros are disabled
L3	Blacklist of signatures	The attachment's signature matches a known malware signature.
L3	Sandbox	The attachent is executed in a secure environment and identified as malicious.
L3	Blocked file extension	The attachment is blocked due to its file extension.
L5	Search and destroy	The administrator removes the email from the employee's mailbox after it has been delivered

Figure 6.6: A portion of measures listed for scenario S1, as they are presented in the treatment.

6.4 Proposed treatment

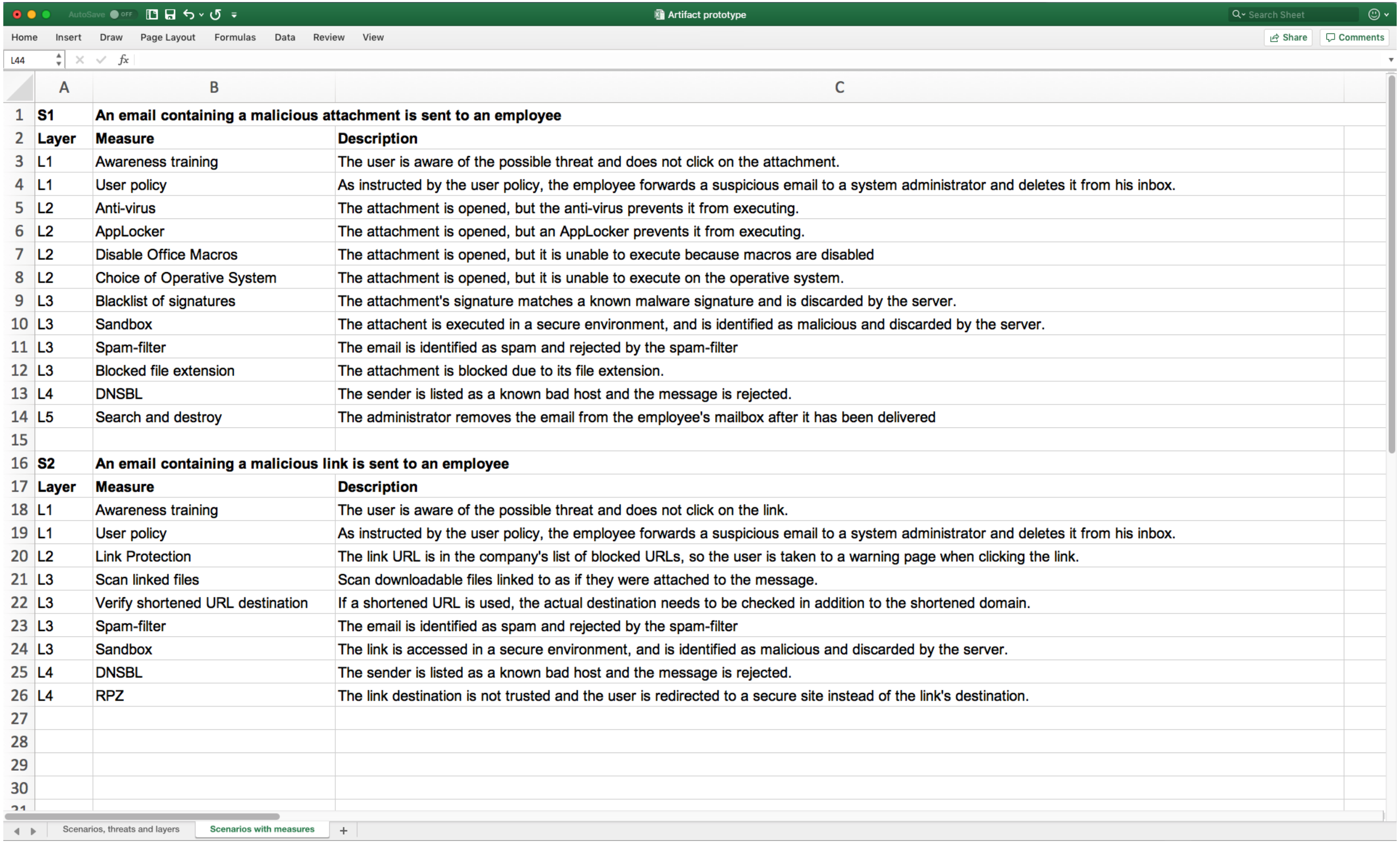
The proposed treatment is a prototype of the framework to guide holistic email security. The prototype has been created in a spreadsheet and is primarily intended to present the concept and possible design of the guiding tool. A selection of threats, scenarios and security measures has been added to the prototype, however, the lists of elements are not exhaustive. The prototype only contains security measures for two scenarios, which is considered sufficient at this point, as the objective is to propose a prototype of a potential solution. Screenshots of the artefact are shown on the following pages, in figure 6.7 and 6.8.



#	Threat	#	Layer
T1	Malware	L1	User
T2	Phishing	L2	Client and Mailbox
T3	Spoofing	L3	Mail Gateway
T4	Spam	L4	DNS
T5	Unintentional actions by authorized users	L5	Surveillance and reactive handling
T6	Unauthorized access		

#	Scenario	Threat	Direction	Security layers
S1	An email containing a malicious attachment is sent to an employee	T1	I	L1, L2, L3, L4, L5
S2	An email containing a malicious link is sent to an employee	T1	I	L1, L2, L3, L4, L5
S3	An email containing a malicious attachment is sent from your domain	T1	O	L3
S4	An employee receives an email requesting a wire transfer	T2	I	L1, L3
S5	A spoofed email is sent to an employee	T3	I	L1, L2, L3, L4
S6	A spoofed email is illegitimately sent from your domain	T3	O	L3, L4
S7	A compromised account is used to distribute spam	T4	O	L3, L5
S8	An employee sends an email to the wrong recipient	T5	O	L1
S9	An employee sends sensitive data unenecrypted	T5	O	L1, L3
S10	A malicious entity gains access to read messages in an employee's mailbox	T6	-	L1, L2
S11	A malicious entity gains access to send messages from an employee's mailbox	T6	O	L1, L2

Figure 6.7: Screenshot of the first page of the artefact prototype.



	A	B	C
1	**S1**	**An email containing a malicious attachment is sent to an employee**	
2	**Layer**	**Measure**	**Description**
3	L1	Awareness training	The user is aware of the possible threat and does not click on the attachment.
4	L1	User policy	As instructed by the user policy, the employee forwards a suspicious email to a system administrator and deletes it from his inbox.
5	L2	Anti-virus	The attachment is opened, but the anti-virus prevents it from executing.
6	L2	AppLocker	The attachment is opened, but an AppLocker prevents it from executing.
7	L2	Disable Office Macros	The attachment is opened, but it is unable to execute because macros are disabled
8	L2	Choice of Operative System	The attachment is opened, but it is unable to execute on the operative system.
9	L3	Blacklist of signatures	The attachment's signature matches a known malware signature and is discarded by the server.
10	L3	Sandbox	The attachent is executed in a secure environment, and is identified as malicious and discarded by the server.
11	L3	Spam-filter	The email is identified as spam and rejected by the spam-filter
12	L3	Blocked file extension	The attachment is blocked due to its file extension.
13	L4	DNSBL	The sender is listed as a known bad host and the message is rejected.
14	L5	Search and destroy	The administrator removes the email from the employee's mailbox after it has been delivered
15			
16	**S2**	**An email containing a malicious link is sent to an employee**	
17	**Layer**	**Measure**	**Description**
18	L1	Awareness training	The user is aware of the possible threat and does not click on the link.
19	L1	User policy	As instructed by the user policy, the employee forwards a suspicious email to a system administrator and deletes it from his inbox.
20	L2	Link Protection	The link URL is in the company's list of blocked URLs, so the user is taken to a warning page when clicking the link.
21	L3	Scan linked files	Scan downloadable files linked to as if they were attached to the message.
22	L3	Verify shortened URL destination	If a shortened URL is used, the actual destination needs to be checked in addition to the shortened domain.
23	L3	Spam-filter	The email is identified as spam and rejected by the spam-filter
24	L3	Sandbox	The link is accessed in a secure environment, and is identified as malicious and discarded by the server.
25	L4	DNSBL	The sender is listed as a known bad host and the message is rejected.
26	L4	RPZ	The link destination is not trusted and the user is redirected to a secure site instead of the link's destination.
27			
28			
29			
30			

Figure 6.8: Screenshot of the second page of the artefact prototype.

Chapter 7 Treatment validation

In this chapter, the validation of the artefact prototype is presented. As described in section 3.3, expert opinion was decided on as the approach for validating the artefact. Following is a description of the treatment validation and the results of the process. The discussion of the results of the validation is in chapter 8.

To provide the expert opinion, one or more persons with a solid understanding of the context (in this case, email security) was required. A professional with broad experience working with information security as well as having expertise on email security was contacted and asked to give feedback on the prototype. The response from the expert was positive, and a meeting was arranged. The meeting had a loose structure as it was attempted to create an informal setting with a free-spoken conversation. To facilitate for a laid-back atmosphere, the meeting took place in a cafeteria during lunchtime and was not recorded. A computer was used to take notes of the highlights of the conversation. Initially, the expert was given a short introduction of the project and what problem context the treatment is intended for. Then, he was handed a set of printed documents, including the requirements of the artefact and the prototype. The prototype consisted of four tables: layers, threats, scenarios and security measures (for two scenarios). The documents used for the treatment validation are attached in appendix C.

To give the expert a soft start, we went through the documents together while keeping an active conversation. The goal was to allow him to get an impression and basic understanding of the prototype, as well as clarifying any uncertainties before any feedback was requested. When the expert seemed to understand the structure and features of the prototype, he was asked to comment on how it conforms to each of the requirements. The feedback relating to each requirement is summarized in table 7.1. Following the review of the requirements, the direction of the conversation naturally shifted to particular features of interest to the expert. The expert was encouraged not to limit himself to the current prototype, but also comment on what features an improved prototype could include.

Requirement	**Feedback from expert**
Comprehensive	Threats, measures and scenarios do not change from one day to another, hence it is expected that an exhaustive list would be stable over time. The current lists provide a good overview but needs to be extended to be fully comprehensive. For instance, certain measures, such as endpoint and intrusion detection, are currently absent.
Flexible	The scenarios and measures are generic. Although certain measures, i.e. AppLocker, are limited to Microsoft products, one can argue that the platform is so widely deployed that Microsoft-specific measures are generic.
Guiding	The tool is guiding as it provides a knowledge base that can help the user discovering measures. To improve the value of the guidance to the user, the measures can be extended with information on benefits, to facilitate that different measures have different costs and effects. Another option is including information on the confidence of the measure's ability to stop a threat. However, that can be difficult to estimate for certain measures, such as awareness training.
Identifying	The tool can be used to identify weaknesses and threats.
Quantifying	A binary comparison of what measures two companies have implemented from the list can be done to quantify email security. However, several measures are not binary verifiable. Awareness training and user policy are subjective. For some technical measures, there are different degrees of implementation. Thus, the correct answer during verification could be *"partly yes"*. For instance, Microsoft Exchange has a default set of blocked file extensions. The set does not include all extensions that can be dangerous, to be fully protected additional extensions must be manually blocked. If a user only uses the default set provided by Exchange, the company is only partly secured against dangerous file extensions.
Effective	The requirement does not account for time being relative. A time-consuming activity can still be effective if the effects make up for the time spent.[1]

Table 7.1: Feedback provided by the expert during treatment validation, grouped by treatment requirement

[1] This feedback was directed at how the requirement was defined, rather than how the tool satisfies the requirement.

The expert asserted that the framework can be helpful to guide companies in implementing email security. He stated that the current treatment provides a useful overview, but to add more value to the tool, it should be extended with an estimate of the cost and benefit of a measure. He added that an important consideration when estimating the cost/benefit is that many measures are context specific. For instance, SPF is easy to implement for a small business, it has no direct cost and should only take an hour to configure correctly. However, for a large company with 15,000 employees and 1,000 services, no projects are small and implementing SPF would be extensive. On the other hand, the expert argued, the large company typically has more resources, hence the effort required to implement SPF might still be considered small given their size. Similarly, the expert believed that an estimation of the confidence of a measure is dependent on the context. With anti-virus as an example, its ability to protect employees will be lower in a company that is targeted by zero-day attacks, compared to a company experiencing mainstream, untargeted threats. In addition to the general feedback and suggestions, the expert commented on particular scenarios, threats and security measures that he disagreed with or experienced as unclear. He also proposed specific elements to be added to the guide, such as a scenario where the credentials of an employee's email account has been stolen, *extortion* as a threat and *"someone to ask, users are encouraged to ask for help if they are unsure about an email"* as a security measure.

Chapter 8 Discussion, part 2

In the following section, the treatment design and treatment validation are discussed. First, the treatment validation process is discussed. Then, follows a discussion in light of RQ3, *How can a company implement holistic email security?*, and RQ4, *Based on cost/benefit analysis, how effective are the different security measures?*.

8.1 Treatment Validation process

For the treatment validation, qualitative feedback was collected from a person with expertise on email security. Malterud [Mal01] argues that qualitative data can provide a degree of generalisation, as was done when analysing the interview data in chapter 5. However, in contrast to the interviews where there were four independent sources of data, there was only one informant for the treatment validation. Therefore we will be careful about generalising the data from the validation. The feedback received is subjective and will be treated as such. If the duration of the project had allowed it, the panel of experts would have been extended to strengthen the integrity of the feedback data. The goal of this phase was to find out if the proposed treatment is a solution to the problem or not. As general conclusions could not be drawn with a single source of data, we were unable to achieve the goal. All the same, the feedback contains valuable observations and opinions of the treatment's expected effects on the problem context.

8.2 RQ3: Implementing holistic email security

In an attempt to answer RQ3, *How can a company implement holistic email seurity*, a prototype of a guiding framework has been created. For the design process, the highlighted challenges and shortcomings identified during the problem investigation were used as a basis. This was done to assure that the artefact was designed in compliance with the identified contexts. The absence of documented plans for email security in the companies interviewed was identified as an element with potential for improvement. As reported by [Sik18], most Norwegian organisations have a framework or management system for information security. This was a driver for designing the artefact as a framework. To assure a holistic approach, the guidance tool needs to be fully comprehensive yet orderly structured. As was commented on during the treatment validation, the tool is currently not exhaustive. With the resources available for this project, the objective of the prototype was limited to giving a good overview. We believe that with more time and expertise available, the framework can be extended to be fully comprehensive.

Rather than answering how companies can approach email security holistically, the other observations from the problem investigation presents prerequisites for the holistic framework to be successful. One observation was that email security is not considered a time-consuming activity and is not allocated much time in the companies. Based on this, we required that the framework should not require a lot of time to be used. The validating expert remarked that a time-consuming activity can still be effective if the benefits make up for the effort. Rather than measuring the effectivity by how long something takes to use (or configure or implement), the time-consumption should be considered in light of the effects of the action. A desired feature of similar, existing solutions is an automated verification of requirements. It was evident that some of the security measures listed in the tool need to be verified manually. Still, programmatically verifying a share of the measures would contribute to the effectivity of the tool. As the prototype artefact was created in a spreadsheet, the options of automation were limited and hence not included in the design.

Another takeaway from the problem investigation was that organisations have different needs. The artefact cannot be tailored for one specific company, it needs to be applicable to various contexts. This was a driver for making the content of the framework generic. As said by the expert, even though certain security measures only apply to Microsoft products, he considers the scenarios and measures as generic. Given the prevalence of Microsoft products in enterprises, Microsoft-specific technologies cannot be excluded when we are trying to create an overview of available security measures.

A final observation from the problem investigation was that the choice of platform is decisive to what security measures a company implements. While not directly addressed by the artefact, as it is generic and does not map measures to specific providers or platforms, it was intended to present the users with a comprehensive view of the available tools and mechanisms. Difi[1] [SS15] argues that it is important to have information security expertise when ordering IT solutions. The argument applies to email security as well. By making the users aware of available security options and their effects, the users' ability to influence what they get from a provider

[1] The Agency for Public Management and eGovernment, https://www.difi.no/om-difi/about-difi

or product is expected to increase. If a company is limited to a particular set of measures, it can constrain their ability to use the artefact effectively.

The expert credited the artefact as guiding but added that the guiding value to the users should be improved. More specifically, he mentioned a valuation of the cost/benefit and estimation of the confidence level of measures as possible extensions to the tool. Successful implementation of these features would also enable quantification of email security as a whole. For instance, if each measure is assigned a score based on its benefit, the benefits of the measures a company has implemented could be summed and used to rate their level of security. The obvious challenge to this, as highlighted by the expert, is that these estimates can be context specific. It needs to be taken into consideration whether it is possible to provide general guidance on context-specific security measures. If that proves too challenging, an alternative approach is to facilitate in the artefact so the companies can conduct their own evaluation, based on their context. That would require more effort from the company, but simplifies the creation of the cost/benefit analysis model.

Verifiability of each security measure to protect against a given scenario was considered an important feature when designing the artefact. During the design, it became clear that binary verification is difficult for measures involving humans, such as user awareness and user policy. The expert also confirmed this. Another challenge to the verifiability of measures, that was revealed during the validation, was measures that are *partly* implemented. Cases of doubt were attempted avoided by presenting each measure in the context of a specific scenario. However, as highlighted by the expert, that was not sufficient to make the measures binary verifiable. An option to address this issue is to enable further drilling down on measures. To use the same example as the expert, with blocking of file extensions, the measure could be extended with a sublist of file extensions that should be protected against. On the other hand, the complexity of the framework is heavily increased if all measures are extended with submeasures. Actions such as migrating the tool from a spreadsheet to an application with collapsible lists could reduce the complexity of an extended framework to the user, but would not eliminate the challenge of balancing simplicity and comprehensivity.

We believe that the proposed artefact outlines one approach to how companies can implement holistic email security. The current prototype has several shortcomings, as was made clear during the validation. For instance, the content needs to be extended to be fully-comprehensive, more features should be added to provide additional value to the users, and the verifiability of security measures needs to be improved. Nonetheless, we consider a scenario-based framework a favourable structure of the guiding tool, as it contributes to providing a simplified and clear overview of email security.

8.3 RQ4: Effectivity of measures

RQ4, *Based on cost/benefit analysis, how effective are the different security measures?*, sought to quantify the value of the measures. During the problem investigation phase, it became clear that economy was not a major consideration to the email security professionals interviewed. Rather than sharing experience on how email security can be approached from an economic perspective, the informants confirmed that it is challenging to put a price tag on security measures. Originally, the intention was to create a model for evaluating cost/benefit of security measures during the treatment design. The cost/benefit values were to be included as a metric in the artefact. By the end of the problem investigation, we realised that we had overestimated the presence of existing economic models to base our cost/benefit analysis on. Learning about the absence of economic models for email security, we realized that the task of conducting a cost/benefit analysis was too ambitious. Given the limited time frame of the thesis, it was decided to prioritize answering the other RQs.

During the treatment validation, extending the artefact with an evaluation of security measures' cost/benefit was proposed by the expert. This further substantiates our belief that this is a desired feature of the artefact. We believe that creating an accurate model for evaluating cost/benefit of security measures is difficult. However, it is also expected to be of considerable value to the user, if added to the artefact. It would contribute to several of the requirements listed, i.e. guiding, quantifying and effective.

Chapter 9 Conclusion and further work

Email security is an extensive and constantly evolving topic. To anyone implementing email security, there are many options to choose from, ranging in price, complexity, functionality and so on. In this thesis, we have surveyed companies to understand how they work with email security. Each informant interviewed presented a distinctive context, yet certain elements or aspects were generalisable. In parallel with the interviews, a literature study was conducted, to investigate related work and the state-of-the-art on email security. Then, a prototype of a framework to guide a holistic implementation of email security was designed and validated.

RQ1: How do companies secure their use of email? The organisations that we interviewed use different platforms and solutions for email. Two of the companies have completely migrated to G Suite, whereas the other two have a local infrastructure. The companies using G Suite explained that they have outsourced email security to Google and trust them to provide the necessary protection. Choice of platform appears to be a decisive factor for what technical security measures are implemented. Rather than demanding specific functionalities from providers, the companies implement security measures based on what is available on their platform. In all the interviews it was rejected that the companies have a clear strategy or plan on email security. There is a trend of approaching email security reactively, implementing the security measures necessary to handle the situations that arise. In contrast, more than 60% of Norwegian organisations have a framework and/or management system for information security [Sik18]. There was an undeniable agreement in the interviews that the companies have to accept a certain amount of insecurity. Even with security measures in place, certain threats cannot be protected against.

RQ2: What drivers and barriers are there for implementing email security measures? Incidents were recognized as a motivating factor for how companies secure email. Given the companies' reactive approach to email security in general, it does not come as a surprise that incidents are drivers for security. In the interviews, the employees were portrayed as a weak link, posing a non-negligible threat to the companies. This was supported by literature studied, concluding that human errors are responsible for the majority of information security incidents [Sik18]. However, given the disparity in the informants' focus on human factors of email security, there is little basis for making a generalised comment on how these factors influence email security as a whole. Email security was not considered time-consuming by any of the informants. The majority said that more time could be spent on email security, but it was expressed as an option rather than a need. Overall, the informants gave the impression that they do not spend a lot of time on email security activities. Economy is not a major consideration of how the companies implement email security, and there is an absence of economic models for email security. In general, if a security measure is considered necessary or useful to the company, it will be bought.

RQ3: How can a company implement holistic email security? Based on the contexts studied, a prototype of a framework to guide holistic email security was designed. The prototype demonstrates a potential approach to helping companies assure fully-comprehensive security of their email services. The results from the validation of the prototype implied that a scenario-based framework can be useful to employees responsible for email security. The structure facilitates getting an overview of email security and understanding what threats to be protected against. The current prototype has deficiencies that need to be addressed for it to be of considerable value to the users. By extending the content to be exhaustive, adding supplementary features and enhancing the verifiability of security measures, we believe the framework can be a significant contribution to guidance of holistic email security.

RQ4: Based on cost/benefit analysis, how effective are the different security measures? This question could not be answered as we were unable to include a cost/benefit analysis in the proposed treatment. However, it is clear that a quantification of the effects of each security measure in the framework would be of great value to the users. We propose building a model for evaluating cost/benefit of a security measure as the next step in creating a holistic guiding framework. If successfully implemented, the cost/benefit model enables classifying and prioritizing various security measures, as well as quantifying the company's overall security.

Further work We propose that further research is carried out to extend the framework with additional features. In particular, a cost/benefit analysis of the security measures is expected to contribute greatly to its usefulness as a guiding tool. Other desired developments to the framework are automated verification, exhaustive content and improved verifiability of security measures. Also, we believe it is essential to validate the framework on a larger panel of experts. If feedback is collected from a representative selection, it enables a higher degree of generalisation. We also suggest performing a quantitative survey of a larger group of companies. The interview data imply, among other things, that companies work with email security in an unstructured manner. It would be interesting to explore the validity of the conclusions from the interviews against a complementary dataset.

References

[AOAA14] Issa Atoum, Ahmed Otoom, and Amer Abu Ali. A holistic cyber security implementation framework. *Information Management & Computer Security*, 22(3):251–264, 2014.

[Are05a] J et al. Arends. Rfc 4033: Dns security introduction and requirements. RFC 4033, RFC Editor, 2005.

[Are05b] J et al. Arends. Rfc 4034: Resource records for the dns security extensions. RFC 4034, RFC Editor, 2005.

[Are05c] J et al. Arends. Rfc 4035: Protocol modifications for the dns security extensions. RFC 4035, RFC Editor, 2005.

[AS18] UNINETT Norid AS. Sikrere norske domenenavn med dnssec. report, UNINETT Norid AS, 2018. https://dypdykk.norid.no/#dnssec.

[BC06] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2):77–101, 2006.

[Bit19] Bitglass. Cloud adoption 2018 war. report, Bitglass, 2019. https://pages.bitglass.com/fy18br-cloudadoption_lp.html.

[C^+08] Gordon V Cormack et al. Email spam filtering: A systematic review. *Foundations and Trends in Information Retrieval*, 1(4):335–455, 2008.

[CDF^+07] Jon Callas, Lutz Donnerhacke, Hal Finney, David Shaw, and Rodney Thayer. Rfc 4880: Openpgp message format. RFC 4880, RFC Editor, 2007.

[Cen17] National Cyber Security Centre. Guidance: Email security and anti-spoofing. Technical report, National Cyber Security Centre, 09 2017.

[CGNR19] Ramaswamy Chandramouli, Simson L Garfinkel, Stephen J Nightingale, and Scott W Rose. Trustworthy email. Technical report, NIST, 2019.

[CHK11] Dave Crocker, Tony Hansen, and Murray Kucherawy. Domainkeys identified mail (dkim) signatures. RFC 6376, RFC Editor, 2011.

[Cis14] Cisco. Building cisco advanced malware protection sandboxing capabilities. *Cisco*, pages 1–8, 2014.

[CM99] BF Crabtree and WL Miller. Clinical research-a multimethod typology and qualitative roadmap. *Doing qualitative research*, 2:3–30, 1999.

[Cof] Cofense. How to identify a phishing attack. Web page, https://cofense.com/identify-a-phishing-attack/.

[CRC08] Patricia Cronin, Frances Ryan, and Michael Coughlan. Undertaking a literature review: a step-by-step approach. *British journal of nursing*, 17(1):38–43, 2008.

[Dog17] Hrvoje Dogan. Email authentication best practices: The optimal ways to deploy spf, dkim and dmarc. Technical report, Cisco, 08 2017.

[ENI19] ENISA. Enisa threat landscape 2018. article, ENISA, 2019.

[fANN19] Internet Corporation for Assigned Names and Numbers. Dnssec - what is it and why is it important? article, Internet Corporation for Assigned Names and Numbers, 2019.

[FB96a] N Freed and N Borenstein. Rfc 2045: Multipurpose internet mail extensions (mime) part one: Format of internet message bodies. RFC 2045, RFC Editor, 1996.

[FB96b] N Freed and N Borenstein. Rfc 2046: Multipurpose internet mail extensions (mime) part two: Media types. RFC 2046, RFC Editor, 1996.

[FB96c] N Freed and N Borenstein. Rfc 2049: Multipurpose internet mail extensions (mime) part five: Conformance criteria and examples. RFC 2049, RFC Editor, 1996.

[FK05] N Freed and J Klensin. Rfc 4289: Multipurpose internet mail extensions (mime) part four: Registration procedures. RFC 4289, RFC Editor, 2005.

[FK06] N Freed and J Klensin. Rfc 4288: Media type specifications and registration procedures. RFC 4288, RFC Editor, 2006.

[fNSa] European Union Agency for Network and Information Security. What is malware? Web page, https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/malware.

[fNSb] European Union Agency for Network and Information Security. What is spear phishing? Web page, https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/phishing-spear-phishing.

[Fre07] Edward H Freeman. Holistic information security: Iso 27001 and due care. *Information Systems Security*, 16(5):291–294, 2007.

[Gja18] Erlend Andreas Gjaere. Hvordan sikre e-post paa helhetlig maate? article, 2018. https://mailrisk.no/blogg/hvordan-sikre-e-post-pa-helhetlig-mate.

[Hac11] Mark Hachman. Playstation hack to cost sony $171m; quake costs far higher. Web page, https://www.pcmag.com/news/264796/playstation-hack-to-cost-sony-171m-quake-costs-far-higher, 2011.

[Har18] Chris Hart. *Doing a literature review: Releasing the research imagination.* Sage, 2018.

[HCHB09] Tony Hansen, Dave Crocker, and Phillip Hallam-Baker. Domainkeys identified mail (dkim) service overview. RFC 5585, RFC Editor, 2009.

[Hei16] Patrick Heim. An inside look at how we keep customer data safe. Blog post, https://blog.dropbox.com/topics/product-tips/dropbox-customer-data-safety, 2016.

[Hof02] Paul Hoffman. Smtp service extension for secure smtp over transport layer security. RFC 3207, RFC Editor, 2002.

[Hou09] R Housley. Rfc 5652: Cryptographic message syntax (cms). RFC 5652, RFC Editor, 2009.

[HSHBC10] Tony Hansen, E Siegel, Phillip Hallam-Baker, and D Crocker. Domainkeys identified mail (dkim) development, deployment, and operations. RFC 5863, RFC Editor, 2010.

[Hus19] Geoff Huston. The state of dnssec validation. article, 2019. https://blog.apnic.net/2019/03/14/the-state-of-dnssec-validation/.

[Kit14] Scott Kitterman. Sender policy framework (spf) for authorizing use of domains in email, version 1. RFC 7208, RFC Editor, 2014.

[Kle08] J Klensin. Rfc 5321: Simple mail transport protocol. RFC 5321, RFC Editor, 2008.

[Kur17] James F Kurose. *Computer networking: A top-down approach.* Boston, 7th edition, global edition. edition, 2017.

[KZ15] Murray Kucherawy and Elizabeth Zwicky. Domain-based message authentication, reporting, and conformance (dmarc). RFC 7489, RFC Editor, 2015.

[Lev18] Ian Levy. Active cyber defence - one year on. Technical report, National Cyber Security Centre, 2018.

[LL17] Moony Li and Jerry Liu. How can advanced sandboxing techniques thwart elusive malware? article, Trend Micro, 2017.

[LS12] C Lewis and M Sergeant. Rfc 6471: Overview of best email dns-based list(dnsbl) operational practices. RFC 6471, RFC Editor, 2012.

[LSS19] Beth Levin, Daniel Simpson, and Nick Schonning. Macro malware. article, 2019. https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/macro-malware.

[Mal01] Kirsti Malterud. Qualitative research: standards, challenges, and guidelines. *The lancet*, 358(9280):483–488, 2001.

[MG$^+$11] Peter Mell, Tim Grance, et al. The nist definition of cloud computing. 2011.

[Phi18] PhishMe. Enterprise phishing resiliency and defense report. article, PhishMe, 2018. https://cofense.com/wp-content/uploads/2017/11/Enterprise-Phishing-Resiliency-and-Defense-Report-2017.pdf.

[RD18] Ole Røgeberg and Øystein Åmelfot Dyngen. Bruk av ikt i husholdningene. Web page, https://www.ssb.no/teknologi-og-innovasjon/statistikker/ikthus/aar, 2018.

[Res08] P Resnick. Rfc 5322: Internet message format. RFC 5322, RFC Editor, 2008.

[Rob15] Dan Robel. 2017 threat landscape survey: Users on the front line. Technical report, SANS Institute, 2015.

[RT10a] B Ramsdell and S Turner. Rfc 5750: Secure/multipurpose internet mail extensions (s/mime) version 3.2 certificate handling. RFC 5750, RFC Editor, 2010.

[RT10b] B Ramsdell and S Turner. Rfc 5751: Secure/multipurpose internet mail extensions (s/mime) version 3.2 message specification. RFC 5751, RFC Editor, 2010.

[SBKH06] Steve Sheng, Levi Broderick, Colleen Alison Koranda, and Jeremy J Hyland. Why johnny still can't encrypt: evaluating the usability of email encryption software. In *Symposium On Usable Privacy and Security*, pages 3–4, 2006.

[Sik16] Norsk Sikkerhetsmyndighet. Ti viktige tiltak mot dataangrep. Technical report, Norsk Sikkerhetsmyndighet, 03 2016.

[Sik17] Norsk Sikkerhetsmyndighet. Grunnleggende tiltak for sikring av e-post. Technical report, Norsk Sikkerhetsmyndighet, 11 2017.

[Sik18] Næringslivets Sikkerhetsråd. Mørketallsundersøkelsen 2018. *Næringslivets Sikkerhetsråd*, 2018.

[SS15] Caroline Ringstad Schultz and Haakon Styri. Vit hva du bestiller. report, Agency for Public Management and eGovernment (Difi), 2015.

[Sym19] Symantec. Internet security threat report 2019. article, Symantec, 2019. https://www.symantec.com/security-center/threat-report.

[Tho18] Iain Thomson. Who's using 2fa? Web page, https://www.theregister.co.uk/2018/01/17/no_one_uses_two_factor_authentication/, 2018.

[Tjo12] A. Tjora. *Kvalitative forskningsmetoder i praksis*. Gyldendal Akademisk, 2012.

[Uni] European Union. What is the gdpr? Web page, https://gdpr.eu/faq/.

[Van19] Denise Vangel. How atp safe links works with urls in email. article, Microsoft, 2019. https://docs.microsoft.com/nb-no/office365/SecurityCompliance/atp-safe-links.

[vRDSP14] Roland van Rijswijk-Deij, Anna Sperotto, and Aiko Pras. Dnssec and its potential for ddos attacks: a comprehensive measurement study. In *Proceedings of the 2014 Conference on Internet Measurement Conference*, pages 449–460. ACM, 2014.

[WH03] Mark Wilson and Joan Hash. Building an information technology security awareness and training program. *NIST Special publication*, 800(50):1–39, 2003.

[Wie14] Roel J Wieringa. *Design science methodology for information systems and software engineering.* Springer, 2014.

[WT99] Alma Whitten and J Doug Tygar. Why johnny can't encrypt: A usability evaluation of pgp 5.0. In *USENIX Security Symposium*, volume 348, 1999.

[Zon] Security Zones. Rpz - response policy zone. article. https://www.securityzones.net/solutions/rpz.

Appendix A
Assessment of Notification Form

Norwegian Centre for Research Data (NSD)[1] had to be notified about the collection of qualitative data in this project. A notification form was sent to NSD, asking for permission to conduct the interviews as planned. NSD's assessment is attached on the following page, confirming that the collection of data can start (as of 13th of February). The contact information (email and phone number) of the project leader and student were censored in the attached document.

[1] https://nsd.no/

NSD NORSK SENTER FOR FORSKNINGSDATA

NSD's assessment

Project title

A holistic approach to email security

Reference number

294110

Registered

11.02.2019 av Gaute Solbu Kleiven - gauteskl@stud.ntnu.no

Data controller (institution responsible for the project)

NTNU Norges teknisk-naturvitenskapelige universitet / Fakultet for informasjonsteknologi og elektroteknikk (IE) / Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Project leader (academic employee/supervisor or PhD candidate)

Karin Bernsmed, [redacted]

Type of project

Student project, Master’s thesis

Contact information, student

Gaute Solbu Kleiven, [redacted]

Project period

04.02.2019 - 01.07.2019

Status

13.02.2019 - Assessed

Assessment (1)

13.02.2019 - Assessed

Det er vår vurdering at behandlingen av personopplysninger i prosjektet vil være i samsvar med personvernlovgivningen så fremt den gjennomføres i tråd med det som er dokumentert i meldeskjemaet med vedlegg den 13.02.2019. Behandlingen kan starte.

MELD ENDRINGER
Dersom behandlingen av personopplysninger endrer seg, kan det være nødvendig å melde dette til NSD ved å oppdatere meldeskjemaet. På våre nettsider informerer vi om hvilke endringer som må meldes. Vent på svar før endringer gjennomføres.

TYPE OPPLYSNINGER OG VARIGHET
Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til 01.07.2019.

LOVLIG GRUNNLAG
Prosjektet vil innhente samtykke fra de registrerte til behandlingen av personopplysninger. Vår vurdering er at prosjektet legger opp til et samtykke i samsvar med kravene i art. 4 og 7, ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse som kan dokumenteres, og som den registrerte kan trekke tilbake. Lovlig grunnlag for behandlingen vil dermed være den registrertes samtykke, jf. personvernforordningen art. 6 nr. 1 bokstav a.

PERSONVERNPRINSIPPER
NSD vurderer at den planlagte behandlingen av personopplysninger vil følge prinsippene i personvernforordningen om:

- lovlighet, rettferdighet og åpenhet (art. 5.1 a), ved at de registrerte får tilfredsstillende informasjon om og samtykker til behandlingen
- formålsbegrensning (art. 5.1 b), ved at personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke behandles til nye, uforenlige formål
- dataminimering (art. 5.1 c), ved at det kun behandles opplysninger som er adekvate, relevante og nødvendige for formålet med prosjektet
- lagringsbegrensning (art. 5.1 e), ved at personopplysningene ikke lagres lengre enn nødvendig for å oppfylle formålet

DE REGISTRERTES RETTIGHETER
Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: åpenhet (art. 12), informasjon (art. 13), innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18), underretning (art. 19), dataportabilitet (art. 20).
NSD vurderer at informasjonen om behandlingen som de registrerte vil motta oppfyller lovens krav til form og innhold, jf. art. 12.1 og art. 13.
Vi minner om at hvis en registrert tar kontakt om sine rettigheter, har behandlingsansvarlig institusjon plikt til å svare innen en måned.

FØLG DIN INSTITUSJONS RETNINGSLINJER
NSD legger til grunn at behandlingen oppfyller kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1. f) og sikkerhet (art. 32).

Dersom du benytter en databehandler i prosjektet må behandlingen oppfylle kravene til bruk av databehandler, jf. art 28 og 29.

For å forsikre dere om at kravene oppfylles, må dere følge interne retningslinjer og/eller rådføre dere med behandlingsansvarlig institusjon.

OPPFØLGING AV PROSJEKTET
NSD vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Lykke til med prosjektet!
Tlf. Personverntjenester: 55 58 21 17 (tast 1)

Appendix B
Interview guide

The interview guide attached on the next page was translated to English before it was added to the appendix. It was originally written in Norwegian as all the interviews were conducted in that language.

Interview guide

1. Introduction/Warm-up (10-15 min)

- Introduction of interviewee (name, age, education, position)
- Introduction of organisation
    - Core business and number of employees?
    - How long have you worked here?
    - What does your day-to-day work look like?
- Who is responsible for operating email at the company?
- What technical solutions do you have for email?
- How many email addresses do you have?
- What is email used for except “regular” communication between employees?

2. Reflection questions (40-45 min)

2.1 General on email security (15-20 min)

- Do you have a strategy or plan on how to secure email?
    - If yes: Can you tell about it?
    - If no: Why not? Who decides/how is it decided what is to be done for email security?

- What measures have you implemented to secure email?
    - Example starting points if needed:
        - Server protocols (dmarc, spf, dkim)?
        - Spam filters?
        - Anti-malware?
        - Sandboxing?
        - User awareness training?
        - Reactive measures/procedures in case of an incident
    - Can you reason your selected measures?

- What threats does email pose to the company?
    - What threat actors are relevant?
    - What types of attacks do you fear the most?

2.2 Priority of email security (10-15 min)

- What role does it play to you personally that the company has secure email services?
- What role does it play to the stakeholders/decision makers of the company that the company has secure email services?
- What role does it play to the customers that the company has secure email services?

2.3 Drivers and barriers (15-20 min)

- Have you experienced any incidents related to email in the past (e.g. phishing, malware)?
    - How do you think that has impacted your email security?
    - If yes: What reactive measures has come of the incident(s)?

- What role does economy play for email security?
    - Do you have calculations comparing cost vs value for security measures?

- How much time do you spend on email security?
    - Is this sufficient in your experience?
    - Do you consider email security time-consuming?

- What drivers do you have for strengthening your email security?
    - External factors: Recommendations from agencies? Laws? Other businesses?
    - Internal factors?

- How do you evaluate the effect of various measures?
    - How do you follow-up measures?
    - Are the measures measureable?

3. Round off questions (5-10 min)

- Is there anything you want to add?
- Information on the thesis going forward:
    - How the data will be treated
    - When the thesis is due
    - Is it okay to reach out if anything from the interview needs clarification?
    - Sending a copy of the thesis when its finished
- Thank you for taking the time

Appendix C
Validation documents

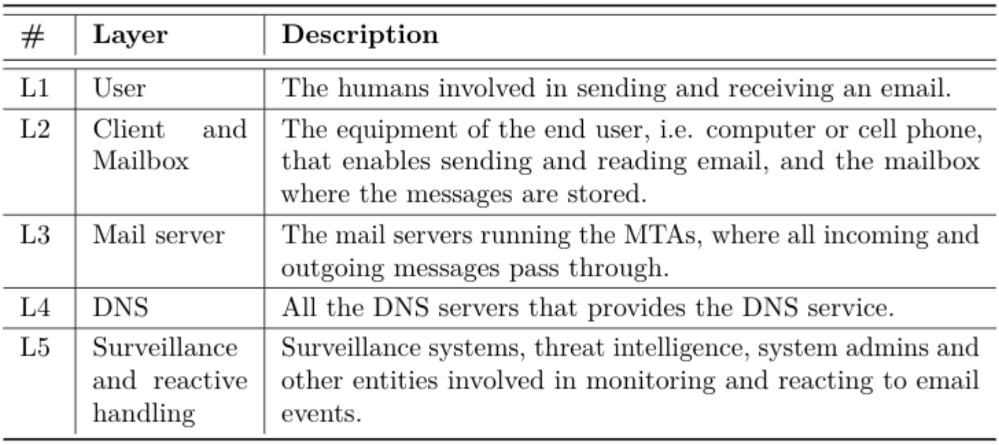
The documents attached on the following pages are the documents that were presented to the expert for the treatment validation. The expert was given the documents printed on A4 paper.

Research question: How can a company implement holistic email security?

Through a problem investigation process, consisting of interviews with companies and a literature study, a set of requirements for the artifact has been created. The requirements specify that the artifact needs to be:

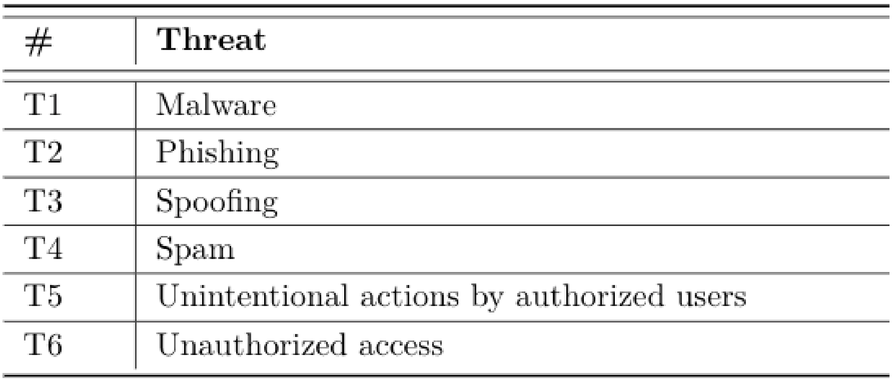
- **Comprehensive**. The treatment will include all elements involved in email.
- **Flexible**.The treatment will be applicable to different contexts, i.e. companies of different sizes, sectors, etc., and will not be platform-specific, i.e. can be used by companies using cloud email services as well as locally hosted Exchange servers.
- **Guiding**. The treatment will provide companies with a set of options for how to implement email security.
- **Identifying**. The treatment will be used to identify weaknesses in and threats to companies' email security.
- **Quantifying**. The treatment will enable comparing and/or quantifying email security between companies, by establishing a common ground.
- **Effective**. The treatment will not require a lot of time to be used.

The layers of email security:



#	Layer	Description
L1	User	The humans involved in sending and receiving an email.
L2	Client and Mailbox	The equipment of the end user, i.e. computer or cell phone, that enables sending and reading email, and the mailbox where the messages are stored.
L3	Mail server	The mail servers running the MTAs, where all incoming and outgoing messages pass through.
L4	DNS	All the DNS servers that provides the DNS service.
L5	Surveillance and reactive handling	Surveillance systems, threat intelligence, system admins and other entities involved in monitoring and reacting to email events.

Example threats of email security:



#	Threat
T1	Malware
T2	Phishing
T3	Spoofing
T4	Spam
T5	Unintentional actions by authorized users
T6	Unauthorized access

#	Scenario	Threat	Direction	Security layers
S1	An email containing a malicious attachment is sent to an employee	T1	I	L1, L2, L3, L4, L5
S2	An email containing a malicious link is sent to an employee	T1	I	L1, L2, L3, L4, L5
S3	An email containing a malicious attachment is sent from your domain	T1	O	L3
S4	An employee receives an email requesting a wire transfer	T2	I	L1, L3
S5	A spoofed email is sent to an employee	T3	I	L1, L2, L3, L4
S6	A spoofed email is illegitimately sent from your domain	T3	O	L3, L4
S7	A compromised account is used to distribute spam	T4	O	L3, L5
S8	An employee sends an email to the wrong recipient	T5	O	L1
S9	An employee sends sensitive data unenecrypted	T5	O	L1, L3
S10	A malicious entity gains access to read messages in an employee's mailbox	T6	-	L1, L2
S11	A malicious entity gains access to send messages from an employee's mailbox	T6	O	L1, L2

S1	**An email containing a malicious attachment is sent to an employee**	
Layer	**Measure**	**Description**
L1	Awareness training	The user is aware of the possible threat and does not click on the attachment.
L1	User policy	As instructed by the user policy, the employee forwards a suspicious email to a system administrator and deletes it from his inbox.
L2	Anti-virus	The attachment is opened, but the anti-virus prevents it from executing.
L2	AppLocker	The attachment is opened, but an AppLocker prevents it from executing.
L2	Disable Office Macros	The attachment is opened, but it is unable to execute because macros are disabled
L2	Choice of Operative System	The attachment is opened, but it is unable to execute on the operative system.
L3	Blacklist of signatures	The attachment's signature matches a known malware signature and is discarded by the server.
L3	Sandbox	The attachent is executed in a secure environment, and is identified as malicious and discarded by the server.
L3	Spam-filter	The email is identified as spam and rejected by the spam-filter
L3	Blocked file extension	The attachment is blocked due to its file extension.
L4	DNSBL	The sender is listed as a known bad host and the message is rejected.
L5	Search and destroy	The administrator removes the email from the employee's mailbox after it has been delivered

S2	**An email containing a malicious link is sent to an employee**	
Layer	**Measure**	**Description**
L1	Awareness training	The user is aware of the possible threat and does not click on the link.
L1	User policy	As instructed by the user policy, the employee forwards a suspicious email to a system administrator and deletes it from his inbox.
L2	Link Protection	The link URL is in the company's list of blocked URLs, so the user is taken to a warning page when clicking the link.
L3	Scan linked files	Scan downloadable files linked to as if they were attached to the message.
L3	Verify shortened URL destinat	If a shortened URL is used, the actual destination needs to be checked in addition to the shortened domain.
L3	Spam-filter	The email is identified as spam and rejected by the spam-filter
L3	Sandbox	The link is accessed in a secure environment, and is identified as malicious and discarded by the server.
L4	DNSBL	The sender is listed as a known bad host and the message is rejected.
L4	RPZ	The link destination is not trusted and the user is redirected to a secure site instead of the link's destination.

Gaute Solbu Kleiven

A holistic approach to email security

NTNU
Norwegian University of
Science and Technology