Bachelor Degree Project

Email attacks

-Investigation about the vulnerability of the Swedish organizations against email threats

Author: Jawdat Kour
Supervisor: Ola Flygt
Semester: VT 2020
Subject: Computer Science

Abstract

Email is an essential form of communication for organizations. Nevertheless, with so much popularity came many challenges. These emails usually carry sensitive data that might cause significant harm if they get compromised. Besides, spam and phishing emails that continually reach the employees' inbox masquerading as a trusted entity due to the lack of authentication mechanisms are also considered a significant threat for organizations today. Such threats are phishing using email domain forgery attack, redirecting emails to a mail server that is under the attacker's control, and connection eavesdropping. The research aimed to investigate the vulnerability of approximately 2000 organizations within Sweden against those attacks. Toward that end, the quantity and quality of the following email security mechanisms SPF, DKIM, DMARC, STARTTLS, DNSSEC, and DANE were examined through a case study. Also, the adoption of these mechanisms was investigated, whether it varies based on different factors such as organization size, sector, and location. The research findings indicated that the average adoption rate by the tested organizations was approximately 50%. Furthermore, the result demonstrated that there were no differences in the adopted mechanisms based on the studied factors that the results were quite similar among the tested groups. It concluded that there is a lack of protection mechanisms, which made the majority of the tested organizations vulnerable to different types of email attacks.

Keywords: Email security, SPF, DKIM, DMARC, DNSSEC, STARTTLS, DANE.

Preface

We would like to thank the Internet.nl team for providing us with access to their tool's API to complete this study. We especially thank Dennis Baaten and George Thessalonikefs for their effort making that possible. We would also like to thank our supervisor Ola Flygt not only for his support and contribution in doing this research but also for his support and guidance during our entire study period at Linnaeus University.

Contents

1 Introduction

This section is an introductory explanation of the study accomplished in this research. It begins with the background section that gives an overview of the subject area, followed by information about the related researches that have been done in the same area and the results they concluded. Then, it will describe the problem and the questions that are going to be answered throughout the research in the problem formulation section, followed by the motivation, objectives, and limitations of the research. The section continues with the target group section that explains to whom this research is targeted, followed by the last section that outlines the upcoming sections of the report.

1.1 Background

In the last few years, an enormous number of email accounts have been subject to numerous types of security attacks such as ransomware, spam emails, phishing attacks, and several big-scale data breaches that have hit reputed organizations [1]. It is a proven fact that email services are completely insecure by default. The Simple Message Transfer Protocol (SMTP) does not include any mechanism for authenticating or for protecting the content of messages during transmission [2]. Despite the security vulnerabilities that threaten email services, it remains at the heart of commercial communications, and they are not expected to be dispensed soon. Moreover, the usage of email services has just increased day by day in the last few years, and it continues to grow [3]. Email is the primary means of business communications today; it is used for exchanging documents and spreadsheets. Considering that the data transmission process is susceptible, the integrity and confidentiality of this data are in question. IT managers and cybersecurity experts face difficult times securing email services. In order to respond to the security threat, several mechanisms have been developed to mitigate the risks email services might pose. The common mechanisms implemented by the organizations to secure their email services against a potential threat are SPF, DKIM, DMARC, STARTTLS, DNSSEC, and DANE [4],[5],[6],[7],[8],[9]. The quality and the quantity of the email security mechanisms might differ from one organization to another based on some factors. The organization size, sector, and location might play a role in that difference.

1.2 Related work

Due to the importance of email in the business community, a significant amount of research has been done to analyze and investigate email services with the aim to clarify a better overview of the threat these services might pose, and provide the best possible solutions that makes email services more secure. Three pieces of research that are more relevant to the study were mentioned below. These studies investigated email services globally, while our study focuses on the organizations within Sweden. In addition, the study included more mechanisms than other studies have investigated.

In 2018, a research was conducted to investigate email spoofing issues. It examined how these emails can be detected by the email provider and in which cases these emails can arrive at users' inbox. The research finding indicated that the adoption of some security extensions such as SPF, DKIM, and DMARC with a proper configuration could help to prevent or mitigate these attacks [10].

Another research was conducted in 2015 by several researchers from different organizations. The research investigates the rate of the global adoption of some of the email

security extensions. It concluded that despite the growth of the adoption of these extensions, still a lot has to be done to improve the state of mail security [11].

In 2019 a research was conducted to investigate phishing attacks. It demonstrated how the adoption of some email extensions could secure email services by authenticating all incoming mails [12].

1.3 Problem formulation

Nowadays, email is the most chosen form of electronic communication for both individuals and institutions. The total number of daily received and sent emails has exceeded 306 million [3]. Due to the increase in usage, the number of different types of email attacks has increased as well [1]. Some optional mechanisms are available to prevent or mitigate email attacks such as SPF, DKIM, DMARC, STARTTLS, DNSSEC, and DANE. These mechanisms are not a standard that every organization should comply with. Instead, they are optional extensions that can be optionally used by the organizations to enhance their email services. Although it is proven that these mechanisms can provide better security solutions for email services, they are still not adopted by a large number of organizations, which eventually makes them vulnerable to different types of email attacks such as phishing attacks using email domain forgery, redirecting email, and email connection eavesdropping attacks [11].

In this study, the vulnerability against those attacks is measured by checking the availability of email security mechanisms implemented by these organizations to secure their email services and prevent such attacks. Moreover, the status of these mechanisms is checked in case they already exist, whether they were configured correctly or not. Additionally, the project investigates if the bad practices concerning email security measurements might play a role in subjecting organizations to email attacks. The scale of the investigation includes about 2000 organizations that have ten employees or more. These organizations will be chosen from the 21 municipalities in Sweden. The project also investigates the effects of some factors, such as organization size, geographical location, and the main sector of business on the decision making related to implementing these techniques.

The study aims to answer the following research questions::

RQ_1: Which of the investigated email security standards are adopted by the tested Swedish organizations?

RQ_2: Are the adoption of email security standards techniques affected by the organization sector, size, or location?

RQ_3: How vulnerable are the tested Swedish organizations against email attacks in the light of the studied Internet Security Standards?

1.4 Motivation

Over the last few decades, email has been one of the essential forms of communication. Today, even with a large number of messenger applications and chatting services, email is still the most preferred method of communication within corporations, educational institutes, and government entities. Many services cannot be used without a valid email

account linked to them, and most correspondence one might initiate with different businesses or entities is done through email. However, with so much popularity came so many challenges, especially that email services have been proven to be completely insecure by default. Simple Message Transfer Protocol (SMTP) does not have any built-in mechanism to prevent email domain forgery or to protect the content of messages during transmission [13]. The security issues linked to email services posed different challenges for IT leaders who took it upon them to introduce new security mechanisms to email services. These different mechanisms have become a recommended standard that should be followed by every email service to make sure it is well protected against any security threats. By investigating the quantity and the quality of the adopted mechanisms by the organizations, it is possible to present potential security threats the organizations are vulnerable to as well as presenting proper solutions that these organizations can implement to mitigate the risks. Thus, the result of this study can be beneficial for the organizations involved in particular and other security-aware organizations and society in general.

1.5 Objectives

A list of objectives is presented here to identify the Swedish organisations' vulnerability against specific email threats.

O1	Define the email security standards (SPF, DKIM, DMARC, DNSSEC, STARTTLS, and DANE) that can be used to mitigate or prevent the related email threats.
O2	Identify the quality and quantity of these mechanisms used by the tested organizations to enhance their email services.
O3	Examine if the efficiency of the adopted techniques differ based on organizations size, sector or geographical location.
O4	Based on the result, identify the vulnerability of the tested organizations to email threats and attacks.

The expected results are that the majority of the organizations are exposed to email attacks due to the lack of the adoption of email security techniques that could help to prevent these attacks from occurring. It is expected that the adoption rate of these techniques is affected by the size of the organization; large organizations have higher adoption than smaller ones. Besides, it is expected that public organizations have higher adoption compared to private organizations in the investigation. Finally, when it comes to the geographical location factor, it is hard to assume whether or not there is a significant connection between an organization's location and the adoption rate of email security mechanisms, an assumption that this investigation aims to either confirm or dismiss.

1.6 Scope/Limitation

The research aimed to examine the email security mechanisms adopted by all Swedish organizations and investigate the overall status of their email services to analyze the critical challenges from a security perspective. The initial research goal was to include all the Swedish organizations in the investigation, but since gathering the required data about all the Swedish organizations was not possible. Thus, the research scope was limited only to approximately 2000 organizations.

Another limitation was that the research did not investigate all types of email attacks. Instead, it focused on email threats that are related to spam, phishing using email domain forgery, email redirection, and connection passive eavesdropping.

Additionally, the process of examining DKIM standard had a limitation, the public keys in the DKIM record could not be queried and validated, because the DKIM selector used in the query is unknown unless an email is received from the signing email address domain that needs to be checked. Therefore, only the availability of this standard is checked.

1.7 Target group

Email services are considered the most important forms of communication within and between organizations, a fact that makes email services critical for every organization. Threats such as daily phishing emails and other malware attacks on email in enterprises are a source of increasing daily inconvenience. The sophisticated email hijacking grows daily, and it cheats even the most ingenious user in the tech world. It might not come as a big surprise to company owners and IT leaders that email is a primary way for hackers to access company secret data and information. Especially considering that is about 84 percent of cyberattacks come through email [14].

The research evaluates the overall status of email services in the tested organizations, besides presenting some potential security threats that email services might pose. The research aims to target IT leaders as well as digital security providers who might use the findings to implement better and more effective email security measurements and solutions. Academics who might want to replicate the research in other countries or investigate other types of email attacks and security threats that were not included in this study are also targeted.

1.8 Outline

The remainder of the paper is organized as follows: The second section describes the method that is going to be used to fulfill the study; it also discusses the reliability and validity, as well as the ethical considerations of the research.

The third section describes in detail the recommended email security mechanisms and explains how they work to enhance the security of email services, the type of email attacks and threats these mechanisms can and cannot protect against is discussed as well.

The fourth section explains how the experiment is conducted as well as the data collection method and the tools used to conduct the experiment. The results section reports the results and findings, followed by an analysis section, in which the analysis of the obtained data is presented, including answers to the research questions.

The last sections are the discussion section that all the research findings are going to be discussed, followed by the conclusion and the future work.

2 Method

The research will conduct a case study that will involve exactly 1973 organizations in Sweden. The study will begin by collecting the required information about the involved organizations. They will be categorized by employees' number, location, and sector (whether private or public). Moreover, the email domain of each organization is also going to be listed. A sophisticated tool is going to be used in the study to identify email security mechanisms used by each of the involved organizations. A statistical study will be performed on the findings to determine whether there is a difference in the rate of adoption of email security mechanisms based on organization sector, size, and location. Also, the results will be analyzed to give an overview of the possible threats that the involved organizations might be susceptible to. The planning for the method displayed in Figure 2.1 shows how the methodology was applied. More detailed information about the source of the organizations' information and the tools used in gathering organizations' information and examining the adopted email security mechanisms will be in the Experiment chapter.

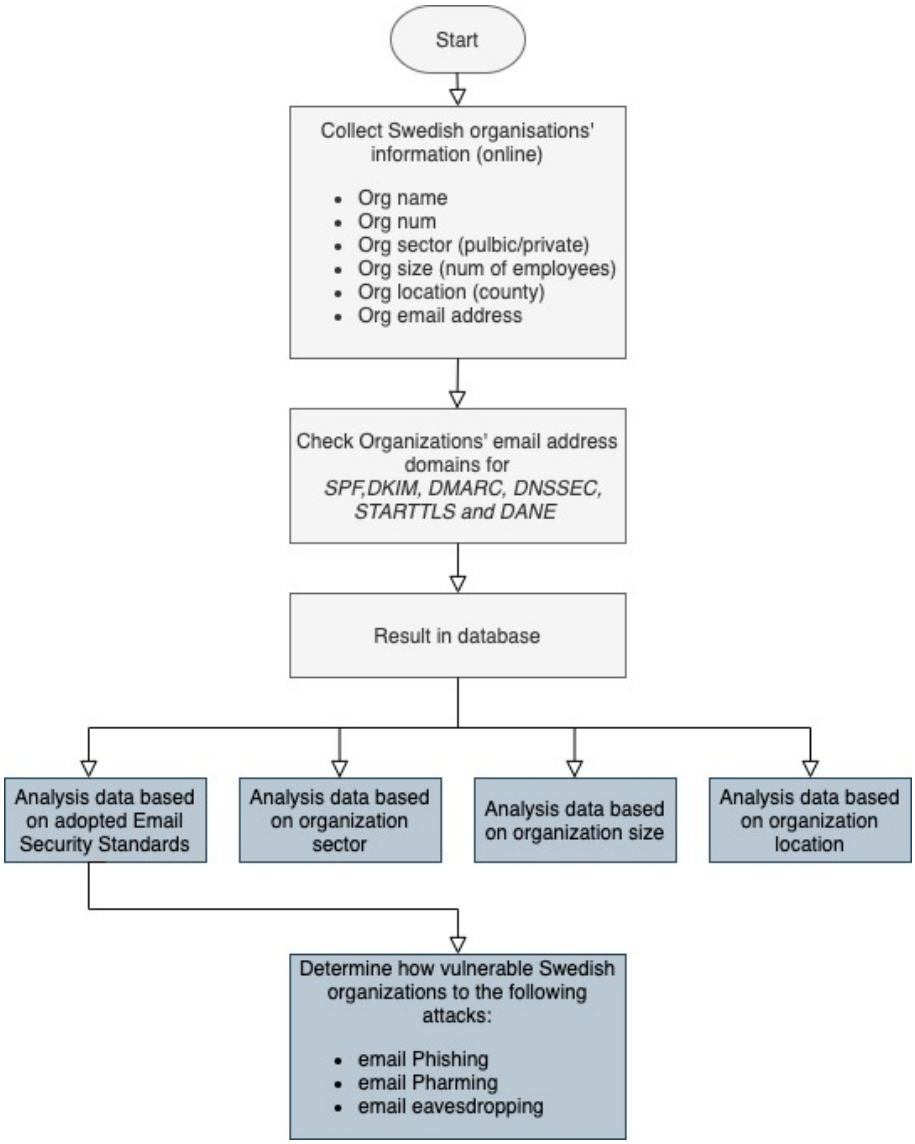


Figure 2.1: Flowchart of the method

2.1 Reliability and Validity

In this study, online service from internet.nl [15] will be used to identify the email security mechanism for the involved organizations. The platform is a result of a collaboration between the Dutch government and the internet community. This service can be considered reliable and well trusted. However, for more reliability, another tool will be implemented to validate some of the results obtained using this tool.

Additionally, the organizations' information that is going to be used in the study is reliable and valid. The required data to conduct the research is available online on Swedish Statistics Agency (SCB) [1], Allabolag [2], and LargestCompanies [3]. The same information can be found in other different, trusted online services. However, some of the required information is possible to get from the source directly, while some bulk data is only available for sale. For that reason, a web scraper tool is going to be used to scrape organizations' data from those services.

When it comes to selecting references for the theoretical part of the research, although most of the required information is available in several sources, the chosen sources are evaluated to meet specific criteria to ensure a high level of reliability for the provided information. The reliability of each source will be confirmed that the information written in that article is supported by evidence. Also, the publisher, whether they are persons or a company, will be checked that they are qualified to write on the topic. Besides checking the purpose in which this information provided alongside the relevance that the provided information should be intensely relevant to the research topic. Therefore, most of the chosen sources will be scientific research papers, journal articles, or they will be articles written by reliable IT organizations.

2.2 Ethical considerations

The obtained data of the experiment can be precious for the organizations to identify weaknesses in their email services and take action against it. However, this information can also be used for malicious purposes by unethical actors. It was taking into consideration the fundamental research ethical principle, which is avoiding harm that might intentionally or unintentionally cause negative consequences to the participant persons or entities. Every possible precaution will be taken to prevent that from occurring. Therefore, some sensitive information about the tested organizations, such as the names of the organizations that are vulnerable to certain types of email attacks, will be removed from the transcribed document [16]. Instead, a percentage result will be presented for each group of the tested organizations without including detailed information about them. Moreover, due to the variation of the research ethics from one country to another, it was checked to determine if the research complies with the Swedish ethical principles (2003:460) using Stockholm University tool, and the result was the project does not require approval, and it can proceed [17].

[1] www.scb.se. Swedish government agency responsible for producing official statistics

[2] www.allabolag.se/om. Sweden's most popular service about Swedish companies.

[3] www.largestcompanies.com. delivers quality market information of Nordic companies

3 Email security standards and the attacks they can and can not prevent

In this section, The main architecture of the Internet mail will be explained. Besides, the proposed standards by the research that will be later checked during the experiment will be explained as well, alongside the attacks, these standards can and can not protect against will be discussed.

3.1 Internet Mail Architecture

It is essential to have a basic grasp of the Internet mail architecture to understand how the involved Internet standards work. The Internet Mail Architecture is a proposed Internet Standard RFC-5598 [18].

The basic understanding of the Internet Mail Architecture is that it consists of Three components. The components are the Message User Agents (MUA) on the users' side, the Message Store (MS), and several Message Transfer Agents (MTA) model Message Handling System (MHS). The message is accepted by one of the MTA, then it is delivered to one or more MTA. The components of Internet Mail Architecture are depicted in Figure 3.2 [18].

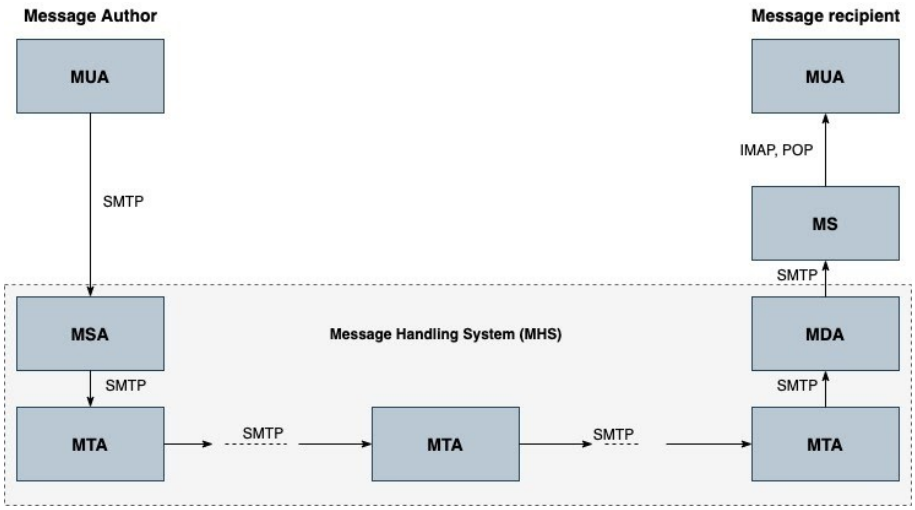


Figure 3.2: Internet Mail Architecture, retrieved from Network security essentials:Applications and Standards [19]

The first component is Message User Agent (MUA), which represents user actors and user applications within the email service. For example, the Outlook application represents MUA. The author Message Transfer Agent (MTA) creates and performs initial submission into the transfer infrastructure via a Mail Submission Agent (MSA). Moreover, It can archive creation in its Message Store (MS).

The second component is the Message Store (MS), which can be located on a remote server or at the same machine as the MUA that can employ it as a long-term message store. When a message arrives in Mail Delivery Agent (MDA), MS can gain it by local or standardized protocols such as SMTP. MUA can later access MS using POP or IMAP protocols.

The third component is the Message Handling System (MHS) - level service. which in turn consists of three parts. The first one is the Message Submission Agents (MSA), which takes responsibility for a message submitted by the author MUA and enforces the

Administrative Management Domain (ADMD) policy and the requirements of Internet standards. It rejects the message that is not conformance and performs the final message preparation for submission of responsibility to the MTA. The second part is the Message Transfer Agent (MTA) that relays mail for one hop application-level and assesses the closer path to the recipient like an IP router by adding a trace head to the message header. The message passes many MTAs using Simple Mail Transfer Protocol (SMTP) until it reaches the destination Mail Delivery Agent (MDA). It changes the data form to MIME encoding, for example, but not body content. The third part is the Mail Delivery Agent (MDA) that delivers the message from MHS to the Message Store (MS) in the Recipient's environment. It transfers the message from the MDA to MS using access protocols, such as POP or IMAP [18].

3.2 Email-related security standards

Email security standards can help to prevent dangerous actors from impersonating organizations by forging email address domain names and tricking consumers into allowing their accounts to be compromised. Furthermore, they can secure email connections between users to maintain message integrity and confidentiality. The following subsections describe each one of these standards.

3.2.1 Sender Policy Framework (SPF)

An open Internet standard is defined in RFC-7208 [4], which specifies a technical method to prevent sender address domain forgery. This technique works by adding SPF records to the Domain Name System (DNS). SPF record specifies the hosts are allowed to send an email on behalf of a given domain. The recipient MTA that implements SPF checks if the sender is authorized to send an email on behalf of a given domain by using a mechanism that queries the sender domain DNS on SPF record and matches if the sender IP is listed in SPF record. However, many other mechanisms can be used. Then the message is accepted or rejected according to the policy used in the SPF record [20]. The SPF record is determined by protocol version, mechanisms, qualifiers, and modifiers. Figure 3.3 illustrates an example of SPF records syntax.

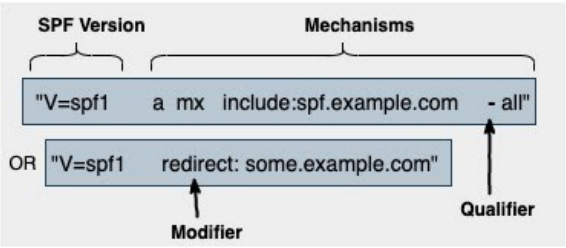


Figure 3.3: An example of SPF records syntax.

The rightmost mechanism is 'all' that denotes that the list is all-inclusive, and no other machines are allowed to send an email. The "include" mechanism makes it possible for one domain to designate multiple administratively independent domains. It is possible to redirect SPF queries into other domains to match both authorized hosts and associated policy by using a "redirect" modifier.

When a mechanism is evaluated, and it matches the prefixed qualifier value of the mechanisms, it returns as the result of that record. The qualifier specifies the action that can be taken when a sending IP matches the qualifier and it can be '+' pass, '-' hardfail, ' '

softfail and '?' neutral [4]. A sufficiently strict policy is implemented when applying 'all' mechanism with '-' (mail should be rejected) or ' ' (the message is accepted but tagged as an SPF failure) qualifiers. However, using '+' pass (even if not matched), and '?' neutral (no policy) qualifiers are not sufficient and allow sender email, which its IP address has not matched the specified IPs to be passed [21]. Figure 3.4 shows examples of typical SPF syntax and sufficient implementation of SPF policy. The parameter 'v' specifies the SPF version. 'IP4' mechanism specifies the network permitted to send messages from a given domain.

```
example.com  3600  IN TXT    "v=spf1 ip4:172.10.1.0/26  -all"
```

Figure 3.4: A typical SPF record implementing sufficient policy

The experiment will examine if the given email address domain has an SPF record in its DNS. Considering that more than one SPF record is not allowed and will lead to a test failure. Moreover, the experiment will test If that record has correct syntax and sufficient policy '-all' or ' all'. In case both 'all' mechanism and 'redirect' modifier are not presented in the SPF record, the default which is '?all' will be presented instead . Ten DNS lookups are followed in case of 'include' and 'redirect' for valid SPF records. Macros in the 'include' or 'redirect' domains are not followed as no information from an actual mail or mail server connection to expand those macros.

3.2.2 DomainKeys Identified Mail (DKIM)

A domain-level authentication method that permits a signing domain to claim some responsibility for the message in the mail stream. DKIM uses public-key cryptography to permit verification of the source and contents of messages by either the recipient MTA or the recipient MUA. Email content and some of the message headers are signed by the email provider using a private key of the administrative domain. The corresponding public key is presented in a DKIM record of the author's DNS domain. The default signing algorithm is RSA with SHA-256, but RSA with SHA-1 may also be used. The DKIM signature and all other necessary information needed by the recipient to validate the signature are inserted to the message header by the signer. When a message reaches the recipient, it queries directly the DNS of a message domain to retrieve the appropriate public key and verify the message DKIM-Signature. Thus, email that originates from out of a given domain but claims to come from a certain domain will fail the authentication test and will eventually be rejected. In other words, the protection of email identity can protect against spam and phishing. DKIM standard is defined in RFC-4871 [5],[19]. Figure 3.5 illustrates a simple example of the operation of DKIM.

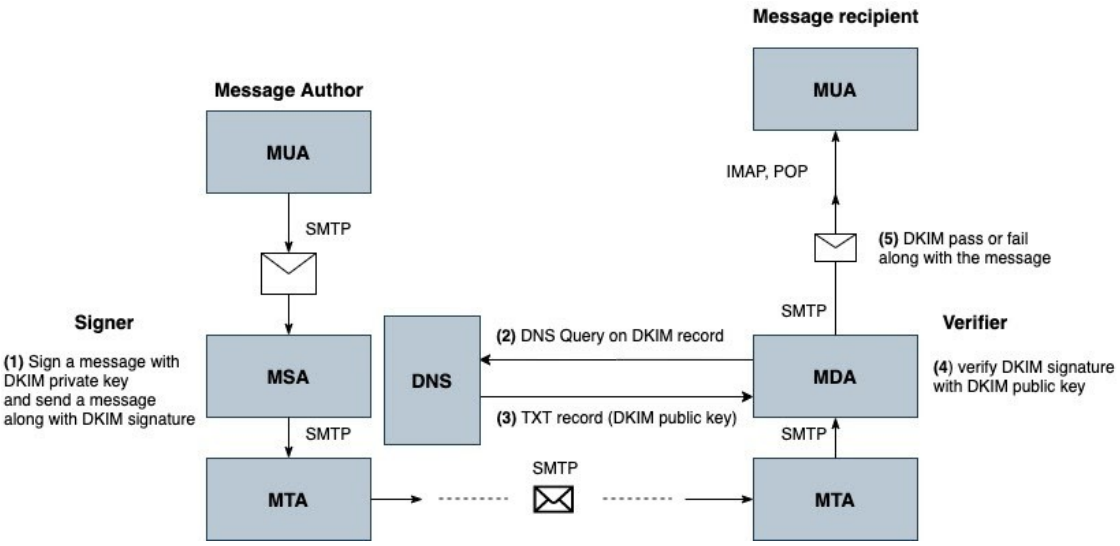


Figure 3.5: DKIM Deployment, reproduced from Network security essentials: Applications and Standards [19].

DKIM record can be queried using a selector and domain name. A selector is a name associated with a key. It is used by the verifier to retrieve the proper key during signature verification [19]. An example of a DKIM record is shown in Figure 3.6.

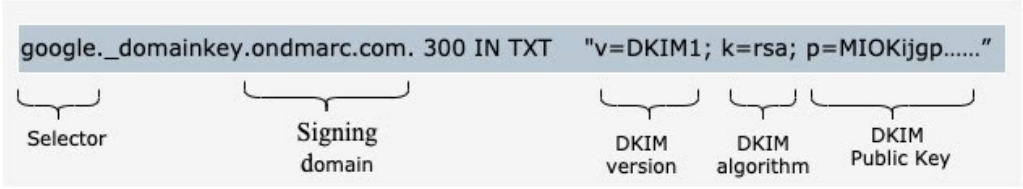


Figure 3.6: An example of a DKIM record.

The experiment will examine whether the domain supports the DKIM record or not. It's expected from the domain name server to answer with NOERROR to the query _domainkey.domain_name where the 'domain_name' is the signing domain. The test can not query and evaluate the public key in the DKIM record, because the DKIM selector is unknown unless an email is received from the tested signing domain.

3.2.3 Domain-based Message Authentication, Reporting, and Conformance (DMARC)

DMARC mechanism provides a policy that extends both the DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF), which can perfectly work together to prevent dangerous actors from sending mail that claims to come from legitimate senders. DMARC policy allows collaboration between the sender's domain and receivers' domains. In other words, the sender's domain indicates if SPF or DKIM or both are used to protect email, and what receivers have to do in case of authentication failure, ranging from no action, through altered delivery, up to message rejection. Furthermore, DMARC provides a reporting mechanism that allows the receivers' domains to report back to the sender's domain about messages that pass and/or fail the authentication. DMARC is published in the DNS as a text resource record and it is defined in RFC-7489 [6], [22], [23]. Figure 3.7 illustrates an example of a DMARC record in DNS. The example shows some important parameters for the performed experiment . As it's illustrated, 'v' tag is the protocol version, 'p' tag is the DMARC policy that should be obeyed by the receiver's

domain, ‘rua’ tag specifies the address that an aggregate report must send to, ‘ruf’ tag specifies the address that an aggregate report must send to [19].

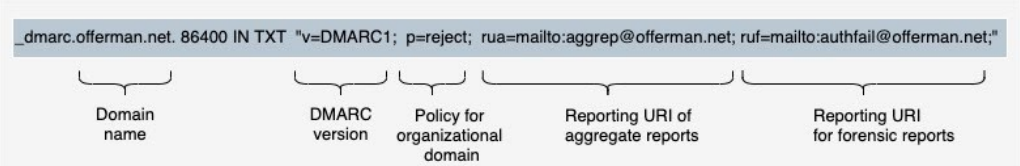


Figure 3.7: An example of a DMARC record.

The experiment will examine if the DMARC record is available in the DNS of the domain. It will be considered that more than one DMARC record is not valid and will lead to testing failure. Besides, the experiment will examine if the syntax of the DKIM record is correct and if it contains a sufficiently strict policy or not. Both values ‘p= reject’ and ‘p=quarantine’ are considered sufficiently strict policies, while ‘p=none’ is insufficient and gives a negative result. Furthermore, email addresses under ‘rua’ and ‘ruf’ are going to be checked if they are valid. If those addresses belong to other domains, the external domain is going to be checked, whether it is authorized to receive DMARC reports or not. That will be done by checking the DMARC authorization record on the external domain if it contains at least v=DMARC1.

3.2.4 Domain Name System Security Extensions (DNSSEC))

DNS Security Extensions (DNSSEC) protocol standard that has been implemented as a response by the Internet technical community to threats destined to the DNS infrastructure [24]. DNSSEC provides data integrity to existing DNS records. Moreover, it provides an authentication mechanism to DNS resolvers -through cryptographic digital signatures- to verify that a DNS response comes from an authoritative name server and ensure that a MITM attack did not alter it during transmission. However, it does not provide confidentiality [7].

In order to secure a DNS zone, a zone-signing key pair (ZSK) is created for that zone. Each Resource Recordset (RRset) of DNS is signed by the private key of ZSK, and the signature is preserved in the RRSIG record in the DNS. The corresponding public key is preserved in a DNSKEY record. The DNS security-aware resolver requests a specific record and the corresponding signature. The public key is pulled along with the record’s data from DNS to verify the response. In fact, the public key of the zone-signing key pair in the DNSKEY record must be protected to be able to trust all records in the DNS zone. For this purpose, a key-signing key pair (KSK) is created to validate the DNSKEY record that contains the public key of ZSK in the same way as ZSK secured the rest of RRsets. The public portion of KSK has also been preserved in a DNSKEY record, and the private key signs the DNSKEY set and keeps the signature in the RRSIG record. The resolver uses the KSK public key to validate the ZSK public key, then the record’s data can be verified [25]. To trust the KSK public key, “the resolver must be configured with at least a public key which authenticates one zone as a starting point” [7]. Figure 3.8 illustrates an example of the DNSSEC verification process of a DNS record’s set (AAAA RRset).

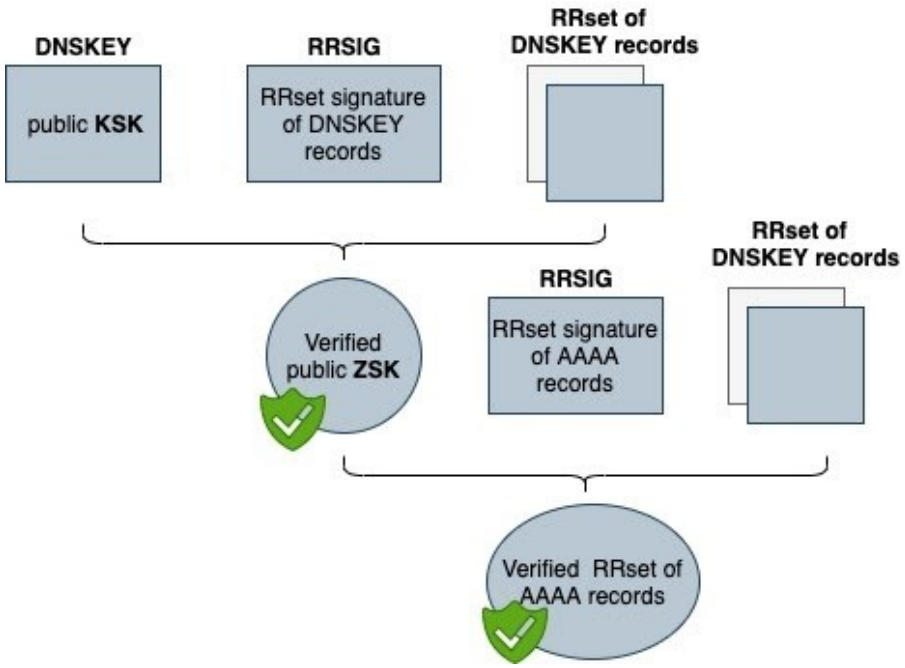


Figure 3.8: An example of the DNSSEC verification process of a DNS records' set. Reproduced from cloudfare.com [25].

Briefly, DNSSEC protects any Resource Record set (RRset) in the DNS zone by a digital signature. Resolvers who validate domain signatures can verify the authenticity of the DNS reply, including those that contain mail server domain(s) record (MX), SPF record, DKIM record, or DMARC record. This prevents dangerous actors from manipulating the DNS reply in order to redirect mails to the attacker's mail server domain.

The experiment will examine if both the email address domain and the mail server domain(s) are DNSSEC signed or not. If one of the previous domains or more redirects to another domain via CNAME record, the CNAME domain is going to be checked whether it is also signed or not. In case, the CNAME domain is not DNSSEC signed, the result of the test will be negative. Moreover, the experiment will test the validity of the DNSSEC signature of the email address domain and the mail server domain(s), making them secure. If one of the previous domains or more redirects to another domain via CNAME record, the CNAME domain signature is going to be checked if it is also valid or not. If the signature of the CNAME domain is not valid, the result of the test will be negative

3.2.5 SMTP security extension (STARTTLS)

STARTTLS refers to extensions that upgrade a plaintext connection to an 'opportunistic' encrypted connection using TLS/SSL certificates. STARTTLS command for SMTP is defined in RFC-3207 [8], and it is mainly intended to protect messages from passive eavesdroppers. A STARTTLS session starts between the client and the mail server as a typical SMTP negotiation. Then the client sends STARTTLS command to the mail server, which initiates a standard TLS connection. If an encrypted session is established, the message is sent over it on the same SMTP port. Otherwise, the client has to decide whether to send a message over a plaintext SMTP session or give up and return the message to the sender [11], [8]. The result (parameters) of the TLS negotiation must be examined by the SMTP client and mail server to check whether an acceptable degree of authentication and privacy was achieved based on local implementation-dependent decisions. For example, the server can choose to deny any more SMTP command, and the client may choose the

send QUIT command that ends the connection in case of using algorithms or key lengths that are considered not strong enough. Such TLS negotiation parameters were checked in the experiment. One consideration that should be considered that SMTP is not an end-to-end protocol. It is primarily used between the message authors and the receiving MTAs. That means the connection will not be encrypted along the way between the receiving MTAs and the message's recipients [8].

The experiment will check numerous parameters through the TLS negotiation. Specifically, the testing tool will test if the domain's mail server(s) supports:

- STARTTLS
- Secure TLS versions only (SSL3.0, 2.0, 1.0 and SSL1.0 are insecure).
- Secure ciphers only.
- Secure parameters for Diffie-Hellman key exchange (at least 224 bit-length for the use of elliptic curves in the elliptic curve Diffie-Hellman (ECDHE) key exchange, or a large key size for the use of Diffie-Hellman Ephemeral (DHE) key exchange).
- Secure hash functions to create the digital signature during the key exchange (SHA-256, SHA-384, or SHA-512 supported).
- TLS compression (the attacker can reconstruct the original data. The use of compression can give an attacker information about the secret parts of encrypted communication).
- A valid trust of the chain for their certificates (the server certificate must be published by a trusted Certificate Authority (CA), and the mail server must present all necessary intermediate certificates).

Moreover, the digital signatures of mail server certificates are going to be tested, whether they are using secure parameters or not. Also, the signed fingerprint of the mail server certificates will be checked if it was created with a secure hashing algorithm or not. Finally, the domain name of each of the receiving mail servers will be examined if it matches the domain name on the presented certificates.

3.2.6 DNS-based Authentication of Named Entities (DANE)

DANE is a protocol proposed in RFC-6698 [9], to bind digital certificates to DNS domain names based on DNSSEC without the need for certificate authority (CA). The current TLS/SSL encryption depends on a certificate from a trusted CA. But lately, some CAs have been compromised, which leads to some security breaches [26]. As a result, DANE was meant to enable domain owners to assert certificates for their domains without indicating to third-party CAs. The chain of trust in DNS (from DNSSEC) is used for authenticating certificates to provide the clients' constraints on certificates, such as the type of certificates that they should expect when they try to access the domain. For DANE to work, a DNS resource record (TLSA) signed with DNSSEC is proposed to store the certificate data and constraints in the DNS [27],[28].

SMTP over TLS (STARTTLS command for SMTP) is used to encrypt a connection between the client and the receiving mail server. However, this encryption is 'opportunistic', which means if the receiving mail server doesn't support TLS, the email automatically goes over a plaintext connection. Even if the server supports TLS, a man-in-the-middle attack can be launched by deleting the '250 STARTTLS' response from the server.

As a result, the email will also be sent over a plaintext connection by the client [8]. For solving this issue, a DANE record indicates that the sender must use TLS [29].

When a certificate is received during TLS negotiation by a client, the client looks up the TLSA record and matches the received certificate against the TLSA content to verify if the certificate is the expected one or not. TLSA record has four fields of data that determine the level of validation that the domain holder provides. The certificate usage field is used to add constraints to the certificate. While the selector field specifies which parts of the certificate should get used for matching purposes. Another field is the matching type field describing how the certificate association is presented. The certificate association data field has the actual certificate data to be matched, given the settings of the other fields. Figure 3.9 illustrates an example of a TLSA record in DNS [30], [28].

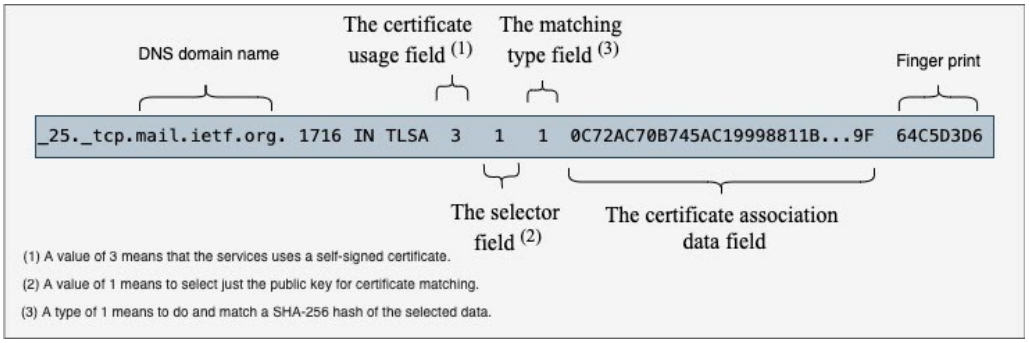


Figure 3.9: An example of a TLSA RR in a domain DNS.

In the experiment, the name servers of the receiving mail servers will be checked whether they provide a TLSA record for DANE or not. Considering that DANE is built upon the DNSSEC, the test fails in case DNSSEC is missing on the mail server domain(s) or if there is no DNSSEC proof of 'Denial of Existence' for TLSA records. Moreover, the TLSA fingerprints presented by the mail server domains will be checked if they are valid for the mail server certificates to prevent an active attacker from stripping STARTTLS encryption.

3.3 Email attacks that SPF, DKIM, DMARC, DNSSEC, STARTTLS and DANE defend against.

On the Internet, emails can be forged in several ways. Phishing attacks using email spoofing 'sender domain forgery' is one of the known forms of email attacks, that is used to trick email recipients into providing sensitive information by pretending to be legitimate business or user. For example, in case no checks are done that the sending system is authorized to send on behalf of the domain, a dangerous actor (Eve) can send Bob an email from a forged domain with a 'MAIL FROM: service@anybank.com' tag contains Bob's bank domain, asking him to fill in some sensitive information. As a result, Bob will think that the email came from his bank and will fill the required information. In another scenario, the email contains malware and Bob trusts the source, and will get malware installed when he clicks on a link.

As discussed earlier in detail, mechanisms such as SPF, DKIM, and DMARC reduce the likelihood of domain names getting fraudulently spoofed. Also, they help to prevent emails from getting flagged as spam by providing greater assurance on the identity of the email's sender. SPF specifies the hosts are allowed to send an email on behalf of a given domain. While DKIM uses public-key cryptography signatures on the mail header

to permit verification of the source by the receiver. DMARC indicates what receivers have to do in case of SPF and/or DKIM authentication failure, ranging from no action, through altered delivery, up to message rejection. Besides, it reports back the failure of the authentication to the original message's domain to give an oversight that its domain got forged [20], [5], [22]. Moreover, DKIM signs the content of the message and protects against message modification during transit by MITM attack [5].

An email pharming attack is caused when an attacker redirects traffic intended for a legitimate site to a different site by poisoning the DNS's cache of the target [30]. DNS spoofing or DNS cache poisoning is caused when an attacker tampers with the contents of DNS server records, causing the DNS server to return an incorrect result to the DNS resolver. An example of a pharming attack in the absence of DNSSEC is that the attacker Eve can provide Bob's DNS server with an unauthorized and fake response when it queries about mail servers of Bob's bank domain (anybank.com). As a result, the DNS server cashes the incorrect response in its MX records. Bob that directly queries that DNS server about the mail server of anybank.com, will get an incorrect response and his email will be redirected to a mail server under Eve's control. DNSSEC is a countermeasure against email pharming attacks using DNS cache spoofing. It uses public-key cryptography to sign the DNS server records allowing other DNS servers to validate DNS responses to ensure that they are correct and from an authoritative source, and the DNS resolver validates DNS server responses to ensure data integrity [31], [29]. In other words, DNSSEC provides data integrity to the existing DNS server records and authentication mechanisms to DNS resolvers [7].

STARTTLS provides an encryption mechanism using a public key certificate to protect users' communications mainly from passive eavesdropping attacks. However, it is primarily used between the message author and the receiving MTAs. That means the connection will not be encrypted along the way between the receiving MTAs and the message's recipients. MITM eavesdropper Eve can still see the message content of Bob's cleartext connection at that stage [8].

DANE solves security issues related to email that is delivered over TLS. STARTTLS command for SMTP provides opportunistic encryption, which means if the receiving mail server doesn't support TLS, an email goes over a plaintext connection. Even if the server supports TLS, a MITM attack can be launched by deleting the '250 STARTTLS' response from the server. As a result, the email will also be sent over a plaintext connection by the client [8]. Moreover, STARTTLS allows for MITM downgrade TLS attacks which allows the use of vulnerable SSL/TLS protocols. DANE provides opportunistic-resistant encryption by indicating that the sender must use TLS. Additionally, it protects against active attackers that manipulate the mail traffic to strip STARTTLS encryption and provides downgrade-resistant TLS support [29].

3.4 Threats that are not addressed by SPF, DKIM, DMARC, STARTTLS,DNSSEC and DANE.

SPF, DKIM, DMARC, STARTTLS, DNSSEC, and DANE do not address all security threats the email service subjected to. Therefore, there are still some threats not considered in the research. DMARC, DKIM, and SPF are email Anti-Phishing techniques. However, they do not handle all email phishing attacks, such as the use of visually similar domain names (cousin domains) or abuse of the 'From' field of the email, which is the display name of the email sender. In cousin domain attack, an attacker uses a registered domain in the email address that is deceptively similar to a target domain name that the

users are familiar with. Therefore it fools the users and imparts a degree of trust. The display name attack is based on the fact that the majority of MUAs show the display name and not the email address to the receiver. An attacker may use an arbitrary email address, while using a well-known person's name or role's name in the display name to fool the email receiver and pretend to be a legitimate actor. Cousin domain attack and Display Name Attack are out of scope for SPF, DKIM, and DMARC [6].

Since email phishing attacks are utilizing social engineering techniques to build trust, it is hard to prevent them technically, and some security awareness is required. The victim can be circumvented and deceived to click a malicious URL or malware-weaponized attachment on the email that leads to install malware. Such attacks are not addressed by the discussed Internet Standards. Brute force attack and other attacks against email password are not covered by them as well.

Email SPAM is a high volume messaging sent to a large number of recipients over email and it is especially used for advertising. Despite many tools built to filter spam, it has grown significantly over the past years and still a challenge for organizations. While spam is not always a vector of attack, it can damage those who fall for scams and other attacks [32]. Email SPAM is still problematic in the presence of the discussed Internet Standards.

4 Experiment

In this section, the process of the experiment will be described in detail. It starts by presenting the tool that is going to be used to conduct the experiments, and an explanation about the mechanisms' parameters going to be measured during the experiment. Moreover, the second tool that was implemented to validate the obtained results by the main tool will be presented as well. The section also shows how the organizations' information has been collected, followed by an explanation about how the collected data have been classified into several groups.

4.1 Experiment setup

Online service from Internet.nl was used to fulfill the entire experiment. This tool is an initiative of the Dutch Internet Standards Platform and is a collaboration between parties from the Internet community and the Dutch government [15]. The email address domains, which were part of the collected data from the organizations, were used as an input into the test tool to check if the email service offers support for the modern Internet Standards. The email Security Standards checked were: DNSSEC, DMARC, SPF, DKIM, STARTTLS, and DANE. Further information about their parameters was mentioned in detail in the Background Information section at the end of each Internet Standard subsection. Table 4.1 explores the parameters that were verified. Such parameters and test explanations can be obtained after performing a test on any email address domain using the tool.

The test tool was written in Python, and it primarily works by querying and analyzing the DNS of email domains and mail servers to examine the security mechanisms adopted by the organizations and report the result back as CSV or JSON formats.

Standard	Checked subset	Test explanation
DNSSEC	-DNSSEC signed domain -DNSSEC signature validity (domain) -DNSSEC signed MX servers domains -DNSSEC signature validity (MX)	Check whether the email address domain and mail servers domains are signed with a valid DNSSEC signature.
SPF	-SPF record existence -SPF Policy	Check if the email domain has SPF record and support sufficiently strict policy (softfail (all) or hardfail (-all))
DKIM	-DKIM record existence	Check if the email domain supports DKIM records.
DMARC	-DMARC record available -DMARC policy	Check whether the email domain has a DMARC record and support sufficiently strict policy (quarantine or reject)
STARTTLS	-STARTTLS available	Check whether mail server(s) (MX) offers STARTTLS.

	-TLS version -Ciphers selection -Key exchange parameters -Hash function for key exchange -TLS Compression -Secure negotiation	Check whether STARTTLS connection supports Only secure parameters.
	-Trust chain of certificate -Public key of certificate -Signature of certificate (Hash) -Domain name on certificate	-Check the authenticity of the TLS certificate and if secure parameters were used in the public key and signing the certificate. -Check if the domain name of mail servers (MX) matches the domain name on the presented certificates.
DANE	-TLSA record for DANE available -DANE validity	-Check whether the mail server(s) domains provide a TLSA record for DANE. -Check if the DANE fingerprints presented by the mail server domains are valid for the mail server certificates.

Table 4.1: Standards categories and subtests were checked in the experiment.

Another tool was implemented by us to validate some of the obtained results of the examined parameters by the original testing tool (Internet.nl tool). The parameters checked using the validating tool are presented in Table 4.2. The verification tool was written in bash scripting, and it also works by querying the DNS server of the email address domain and mail server(s) domain, then reporting the result back.

Standard	Checked subset	Test explanation
DNSSEC	-DNSSEC signed domain -DNSSEC signed MX servers domains	Check whether the email address domain and mail servers domains are DNSSEC signed.
SPF	-SPF record existence -SPF Policy* *If the SPF record contains 'redirect' to other domains, the tool doesn't follow them.	Check if the email domain has SPF record and support sufficiently strict policy (softfail (all) or hardfail (-all))
DKIM	-DKIM record existence	Check if the email domain supports DKIM records.
DMARC	-DMARC record available -DMARC policy	Check whether the email domain has a DMARC record and support sufficiently strict policy (quarantine or reject)

DANE	-TLSA record for DANE available	Check whether the mail server(s) domains provide a TLSA record for DANE.

Table 4.2: Standards categories and subtests were verified by the implemented tool.

4.2 Data Gathering

The required data about the Swedish organizations were collected from several reliable sources including Swedish Statistics Agency (SCB) , Allabolag, and LargestCompanies. The following fields were included for each organization: the organization name, number, size (based on the number of employees), county, sector (whether public or private), and email address domain. Collecting data about all Swedish organizations was not possible. Thus, data about 2000 organizations were collected and presented in three groups as follows:

The first group is (Group 1), which contains all Swedish organizations in the public sector. Data of this group was provided by the Swedish Statistics Agency (SCB). The data included information about all public sector organizations (349 organizations in total), including their email address domains. Upon starting the experiment, it was revealed that some of these organizations used the same domain name. As a result, the distinct domain names for those organizations became 217 domains.

The second group is (Group 2), which contains the top 1000 Swedish private organizations. Data about the top 1000 Swedish private organizations were collected based on the number of employees from a reliable online service of LargestCompanies. A web-scraper tool [4] was used to scrape the required information remove. Although some of the organizations were registered under different organization names and numbers, we found that some of the email addresses for several organizations were shared among other organizations in the group. For example, Volvo was registered under different names and numbers, but many of them use the same email domain. Therefore, the distinct email domain names of the top 1000 Swedish private organizations were only 803 domains.

The third group is (Group 3), which also contains Swedish private organizations. Data about these private organizations were collected from the online service of Allabolag. Information about 30 private organizations of each 21 counties in Sweden was scraped; 630 private organizations in total. The 30 organizations of each county were chosen based on the number of employees, which is classified into four groups according to the European Union standard [33], which are micro, small, medium-sized, and large organizations. Ten organizations of each size have been collected since the total number that will be considered for this group is 630 private organization.

Remarks about the collected data:

- Micro organizations that are an organization with less than 10 persons employed have not been collected since the majority of these organizations had no email service.

[4] www.webscraper.io. web data extractor

- The majority of the public organizations (Group 1) were registered in Stockholm county, and most of them were large organizations.
- Because Gotland county is relatively small, therefore there were only 4 large registered organizations available out of 10 that are required for the experiment. Thus, the total number of private organizations decreased by 6 organizations. (Group 3) became (630 - 6 = 624 private organizations).
- All the top 1000 Swedish private organizations (Group 2) were large organizations, and the majority were registered in Stockholm county.
- Some organizations are using email domains that differ from the domains of their websites for different reasons. However, most of the gathered information about the tested organizations initially contained the email address domains. In case of the absence of the email address domains of some organizations, the organizations' website domains were examined whether they had mail server(s) by a special script we made. The script queried the MX record in the Domain Name System (DNS) of the organization domain. If the domain had no mail server(s) available, the email address domain was manually extracted from the organization's website. As a result, only a few organizations that had no email service were excluded from the research.

4.3 Examine email security mechanisms adopted by the tested organizations

The experiment started by examining the security mechanisms for the public organizations (Group 1). The total number of email domains checked in this experiment was 217, which included all domains of the Swedish public organizations. This experiment lasted approximately 3 hours to be performed on a working day during the daytime, where the DNS service was congested on the Internet. All the 217 domain names were submitted at the same time to the tool's API to be checked.

The second experiment examined the email security standards of the top 1000 Swedish private organizations (Group 2). The total number of the tested email domains was supposed to be 1000. However, similar to the public organizations, it turns out that several organizations or the same organizations that are under different commercial names and numbers meant to use the same email domains. Therefore, the total number of the tested domains was 803 domains. This experiment lasted approximately 10 hours on a working day during the daytime, where the DNS service was congested on the Internet while it takes less time during the night. All the email address domain names of this group were submitted at the same time to the tool's API to be checked.

For the last experiment, the adopted security mechanisms by 624 private Swedish organizations (Group 3), which grouped based on registered county and size, were examined. This experiment took approximately 8 hours on a working day during the daytime, where the DNS service was congested on the Internet.All the 624 email address domain names were submitted at the same time to the tool's API.

For each of the conducted experiments on the previous organizations' groups, another test was performed to validate the obtained result. Some of the examined parameters' results were also confirmed using a tool we implemented specifically for that purpose. As an outcome, considering that both the experiment by internet.nl tool and the validation using the implemented tool were carried in the same period, the results of both tools were identical.

5 Results

In this section, the results of the experiments outlined in the experiment section are presented in detail. That includes a percentage of Internet Standards adopted by the tested organizations' groups alongside the result of the comparison among them.

5.1 The status of the adopted email security mechanisms by the Swedish public organizations (Group 1)

The obtained results of the first experiment, which was conducted on the public organizations group, showed that SPF was adopted by 89% of the Swedish public organizations. However, the results indicated that only 81% of them have sufficiently configured SPF policy.

DKIM was implemented by 46% of these organizations, DMARC got the lowest percentage among the authentication mechanisms by 29%. The results indicated that although 29% of them have implemented DMARC, only 12% of them have sufficiently configured DMARC policy.

The results showed that 29% of public organizations have DNSSEC implemented in their MX domain(s), while 53% have their email domain signed with DNSSEC. Figure 5.1 illustrates the result. Statistical information is provided in Table 1.1 in Appendix 1.

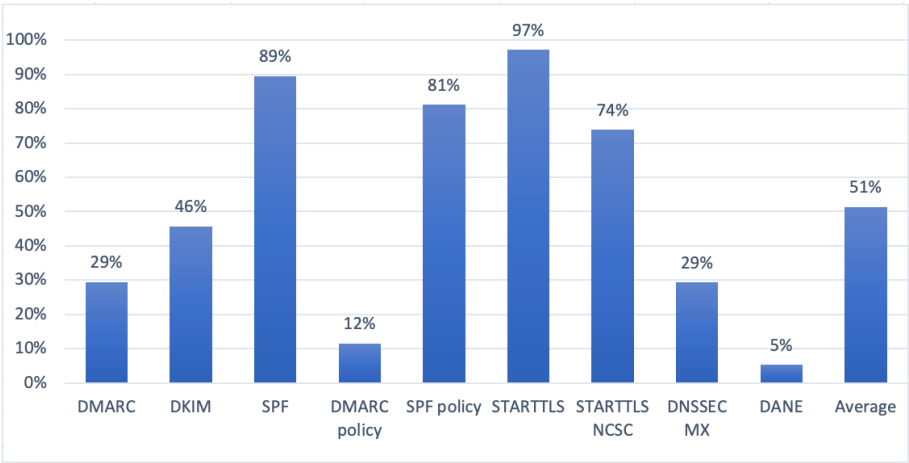


Figure 5.1: Average adoption of Standards, public Swedish organizations (Group 1)

Although the majority of these organizations (97%) support STARTTLS for secure mail transport, the results confirmed that only 5% have DANE implemented in their system as shown in Figure 5.2. More information is given in Table 1.2 in Appendix 1.

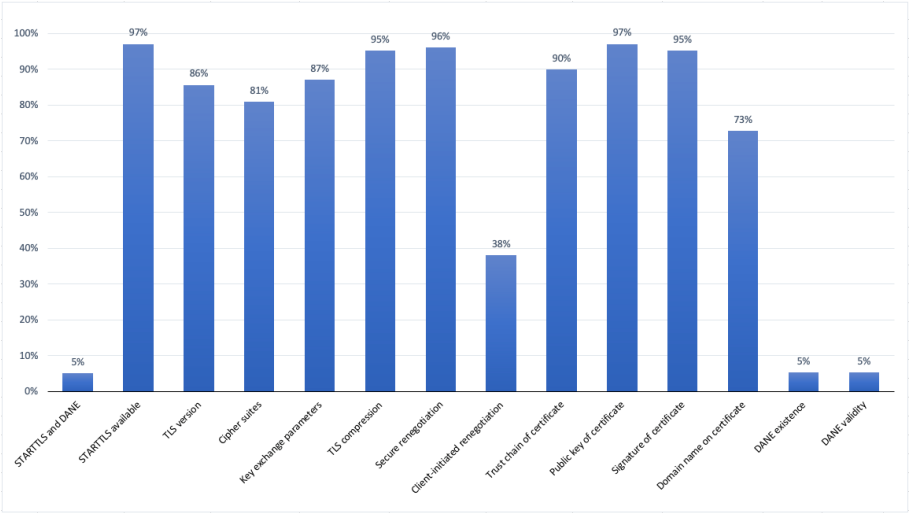


Figure 5.2: STARTTLS & DANE adoption, public Swedish organizations (Group 1)

5.2 The status of the adopted email security mechanisms by the top 1000 private Swedish organizations (Group 2)

The obtained results from the second experiment of the top 1000 Swedish organizations (Group 2) showed that DMARC was implemented by 38% of these organizations. But, only 13% of them have properly configured DMARC policy.

DKIM was implemented by 60% of this group of organizations, while SPF rate was 90% of adoption. However, the results indicate that only 81% of them have sufficiently configured SPF policy.

Besides, the results confirmed that only 5% of these organizations have implemented DNSSEC in their MX server(s), while 15% have their email domain signed with DNSSEC. Figure 5.3 below illustrates the result.

A large number of these organizations (96%) support STARTTLS for secure mail communication. As it is shown below in Figure 5.4, the majority of them have configured STARTTLS sufficiently, while only 1% of them have DANE implemented in their system.

Table 1.3 and Table 1.4 in Appendix 1 provide statistical information about the organizations and parameters that were examined.

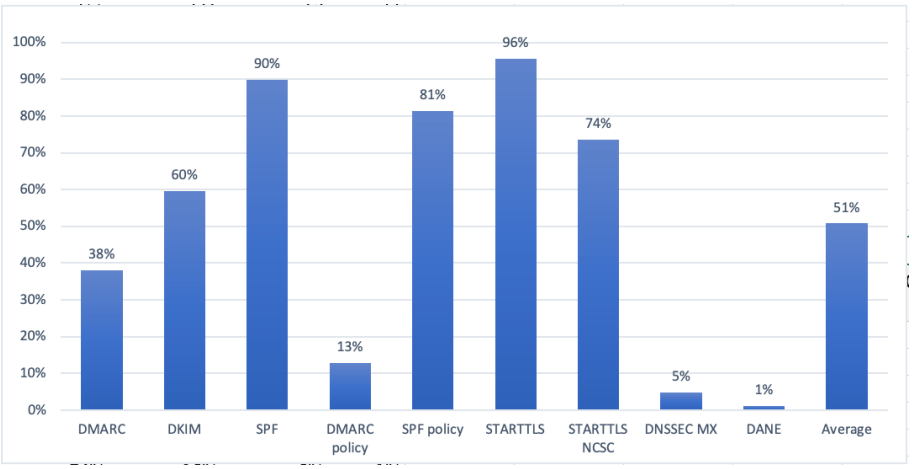


Figure 5.3: Average adoption of Standards, Top 1000 private Swedish organizations (Group 2)

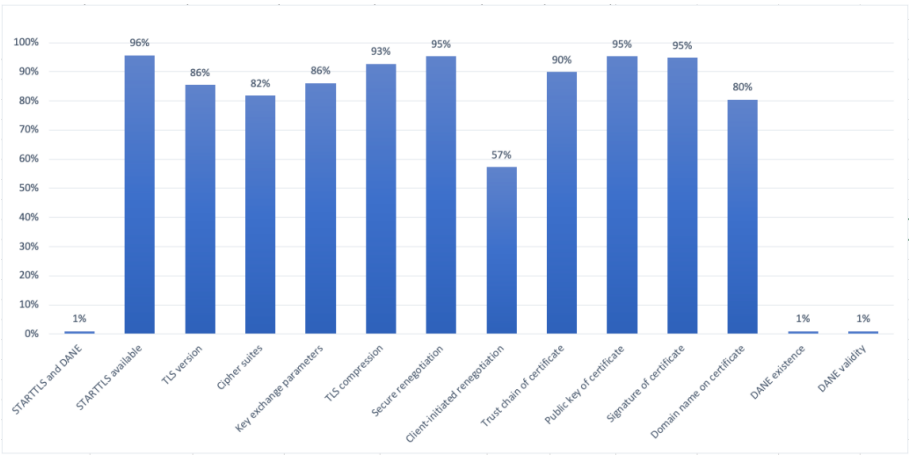


Figure 5.4: Average adoption of Standards, Top 1000 private Swedish organizations (Group 2)

5.3 The status of the adopted email security mechanisms by the private organizations (Group 3)

The third group contains different sizes of private Swedish organizations located in different counties. The experiment's results of these organizations showed that the average adoption of the specified mechanism was 47% in total. The results showed that only 5% of these organizations have DNSSEC implemented in their MX server, while 21% have their email domain signed with DNSSEC.

SPF was adopted by 83% of these organizations. However, only 75% of them have sufficiently configured SPF policy. It also showed that DKIM was implemented by 47% of them. DMARC got the lowest percentage among the authentication mechanisms by 23%. The results indicated that only 1 of 10 of these organizations have sufficiently configured DMARC policy. Figure 5.5 illustrates the result.

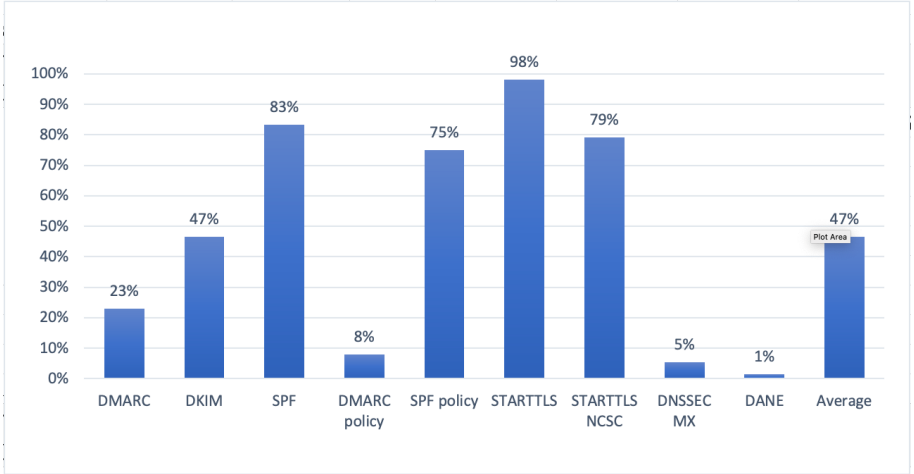


Figure 5.5: Average adoption of Standards, private Swedish organizations (Group 3)

Additionally, STARTTLS was the most implemented standard by these organizations. The results showed that 98% of these organizations have STARTTLS implemented in their mail servers. As shown in Figure 5.6, a large percentage of them have configured it sufficiently, and only 1% of them have DANE implemented in their system.

Table 1.5 and Table 1.6 in Appendix 1 provide statistical information about the organizations and parameters that were examined.

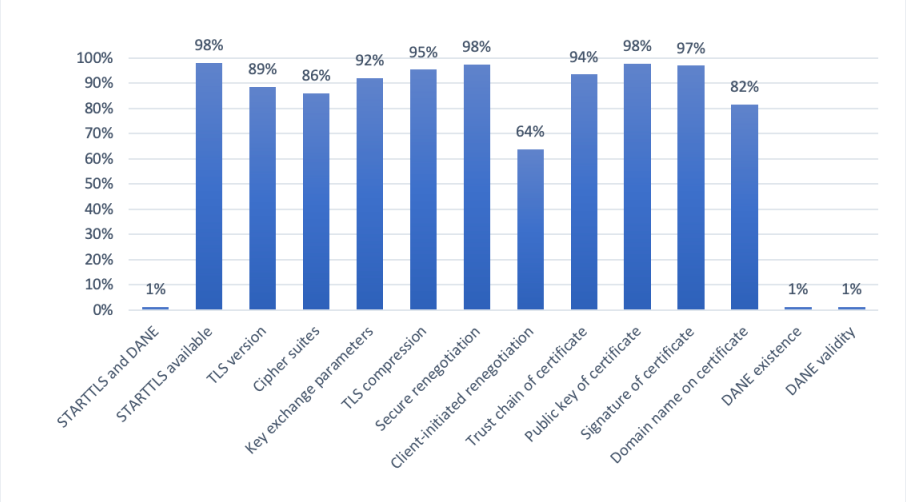


Figure 5.6: STARTTLS & DANE adoption, private Swedish organizations (Group 3)

5.3.1 Results for the large private organizations

The results of the adopted email security mechanisms by the large private organizations showed that the average of the adoption was 50%. The results confirmed that SPF was adopted by 90% of these organizations. But, only 81% of them have sufficiently configured SPF policy. In addition, DKIM was implemented by 55% of them. DMARC got the lowest percentage among the authentication mechanisms by 34%. The results indicated that only 12% of them have sufficiently configured DMARC policy.

The results showed that only 4% of these organizations had implemented DNSSEC in their MX server, while 13% have their email domain signed with DNSSEC.

Although a large number of these organizations, 96% support STARTTLS for secure mail communication, the results confirmed that only 1% of them have DANE implemented in their system. Figure 5.7 illustrates the result.

Statistical information about the organizations and parameters that were examined is given in Table 1.7 in Appendix 1.

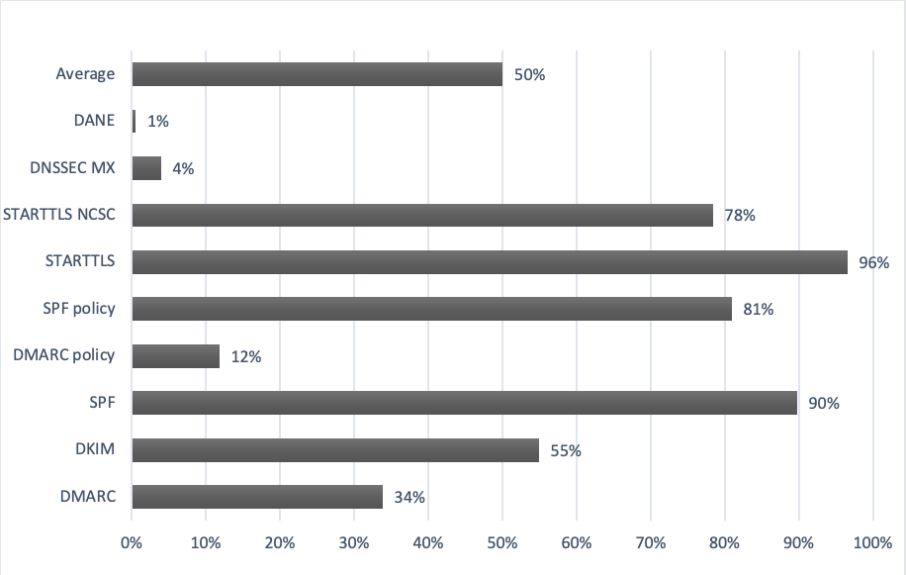


Figure 5.7: Average adoption of Standards, Large private Swedish organizations.

5.3.2 Results for the medium-sized private organizations

The results of the adopted email security mechanisms by the chosen medium-size private organizations showed that the average of the adoption was 47%. The results illustrated that SPF was adopted by 84% of these organizations and about 78% of them have sufficiently configured SPF policy. Besides, DKIM was implemented by 43% of them.

DMARC got the lowest percentage among the authentication mechanisms by 24%. The results indicated that only 10% of them have sufficiently configured DMARC policy. The results also showed that only 6% of these organizations have implemented DNSSEC in their MX server, while 21% have their email domain signed with DNSSEC.

Although the majority of these organizations (98%) support STARTTLS to secure mail communication, the results confirmed that only 2% of these organizations have DANE implemented in their system. Figure 5.8 illustrates the result.

Table 1.8 in Appendix 1 provides more detailed information about the organizations and parameters that were checked.

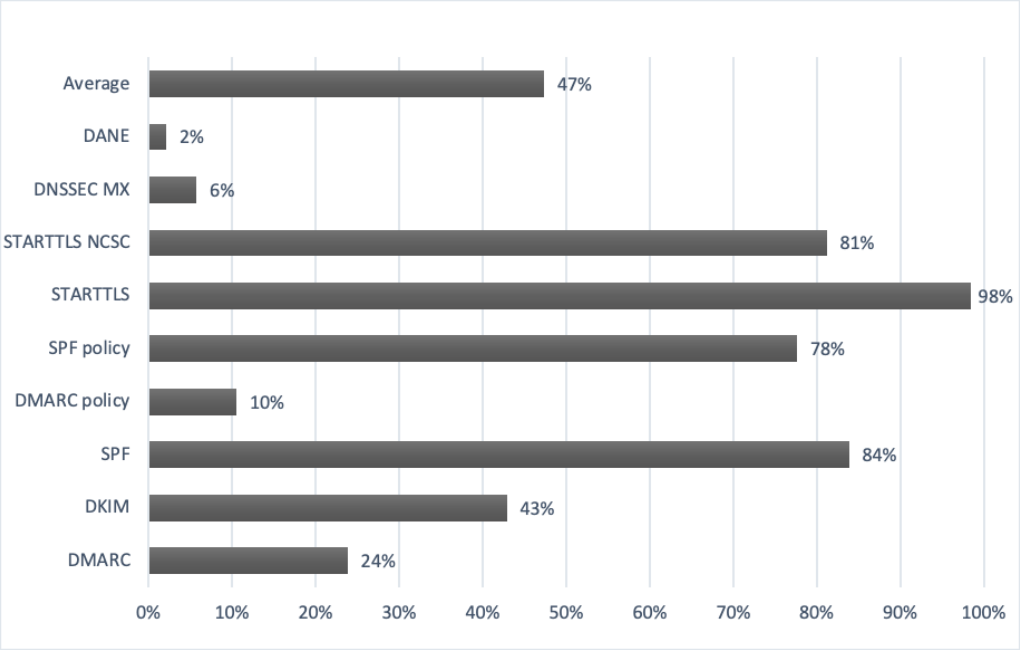


Figure 5.8: Average adoption of Standards, Medium private Swedish organizations.

5.3.3 Results for the small private organizations

The results that indicate the status of the adopted email security mechanisms by the chosen small organizations, showed that the average of the adoption was 43%. The results confirmed that SPF was adopted by 76% of these organizations. But, only 66% of them have sufficiently configured SPF policy. Moreover, DKIM was implemented by 44% of these organizations.

DMARC also got the lowest percentage among the authentication mechanisms by 13%, and it was confirmed that only 3% of them have sufficiently configured DMARC policy. The results showed that 6% of these organizations had implemented DNSSEC in their MX server, while 26% have their email domain signed with DNSSEC.

The majority of these organizations (99%) support STARTTLS for secure mail communication, but only 2% of them have DANE implemented in their system. Figure 5.9 illustrates the result.

Table 1.9 in Appendix 1 provides more detailed information about the organizations and parameters that were checked.

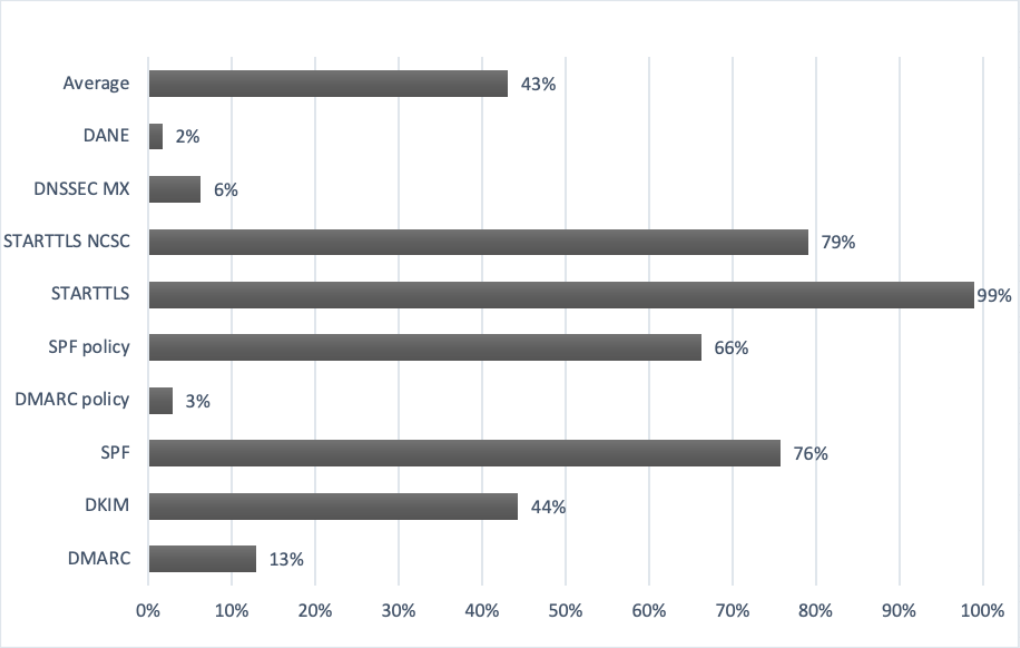


Figure 5.9: Average adoption of Standards, Medium private Swedish organizations.

5.3.4 Results for the private organizations based on their location

The average adoption of the specified email security mechanisms by the tested Swedish organizations based on their regions is between 40% and 52%. The results showed that the lowest average percentage was in Jämtland county by 40% of adoption rate while the highest was in Södermalmland county with 52%. STARTTLS was the most common standard adopted by these organizations, followed by SPF, while the less adopted standard was DNAE followed by DNSSEC. Figure 5.10 shows the results for all the checked security mechanisms for each county. Table 1.10 in Appendix 1 provides statistical information about the organizations of each county and parameters were examined.

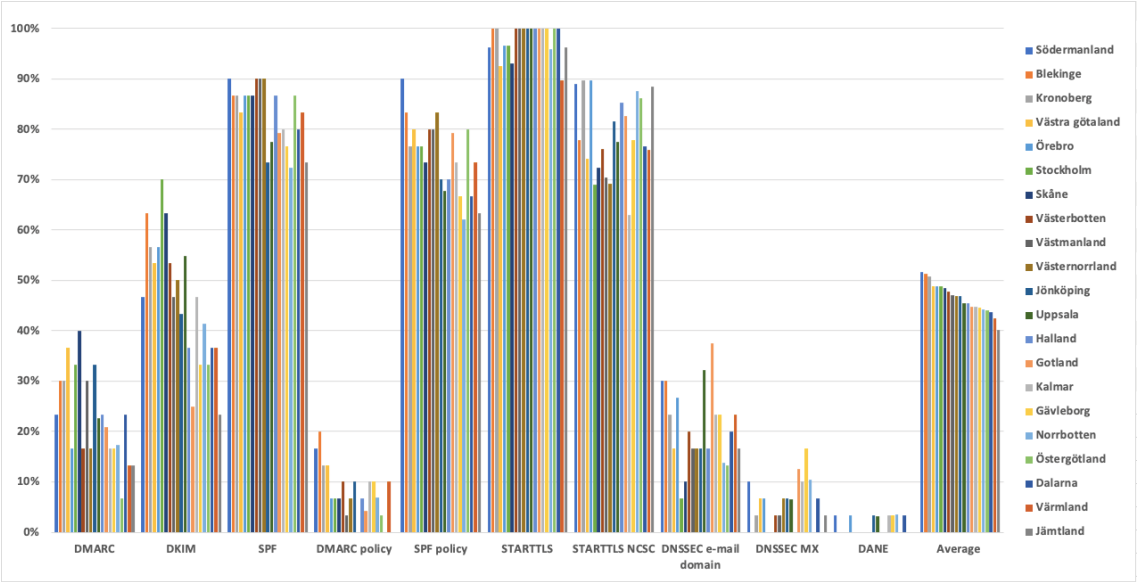


Figure 5.10: Internet Standards adoption by Swedish organizations based on the county

6 Analysis

The analysis of the data obtained from the experiment will be reviewed and discussed in detail. The research questions will be answered throughout this chapter, as well.

Question 1: Which of the investigated email security standards are adopted by the tested Swedish organizations?

The results showed that the adoption rate of the checked email security mechanisms varies from one organization to another. The average adoption rate of these standards for all the tested organizations was approximately 50%. Figure 6.1 illustrates the result.

STARTTLS and SPF are the standards that are mostly implemented by the tested organizations with over 80 percent and 90 percent of adoption, respectively. Although the number of organizations that have SPF and STARTTLS implemented in their system is quite high, about 2 of 10 of these organizations have not properly configured them.

The average rate of DKIM was 50 percent of adoption. Besides, DMARC has the lowest rate among the authentication mechanisms, with only 30 percent of adoption. However, it was remarkable that only 1 of 10 of these organizations has sufficiently configured DMARC policy.

Additionally, the result showed that DNSSEC and DANE were the lowest mechanisms adopted by the tested organizations with less than 10% for DNSSEC and less than 2% for DANE.

Table 1.11 in Appendix 1 provides detailed information about all tested organizations combined.

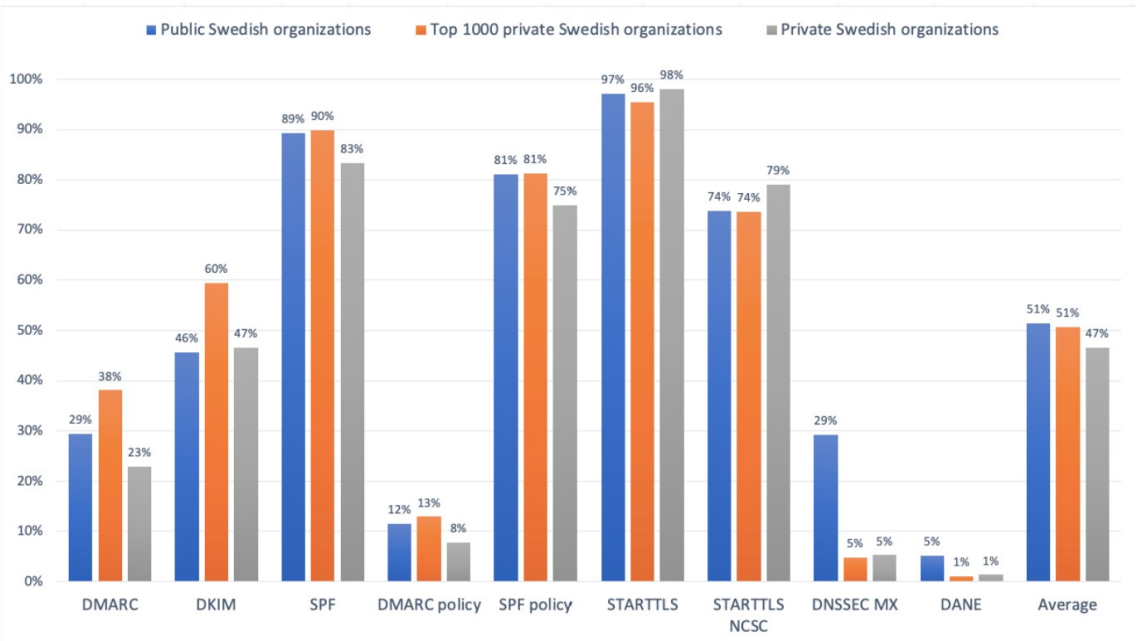
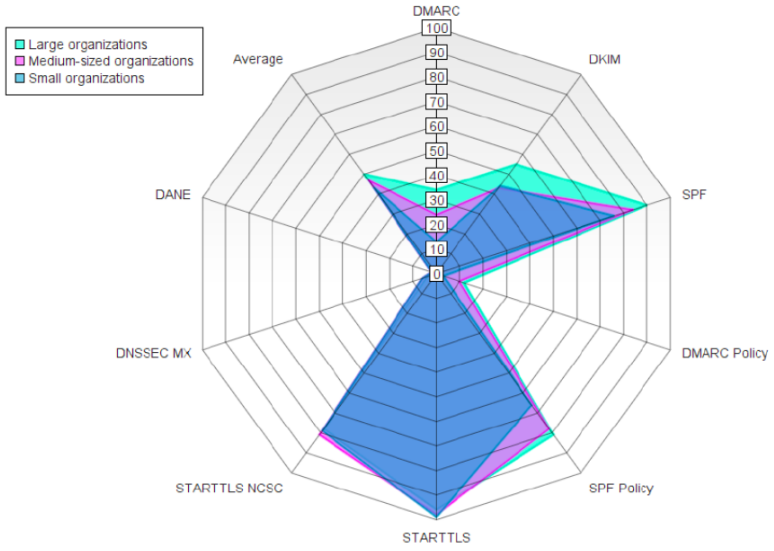


Figure 6.1: Internet Standards adoption by the tested Swedish organizations groups.

Question 2: Are the adoption of email security standards techniques affected by the organization sector, size, or location?

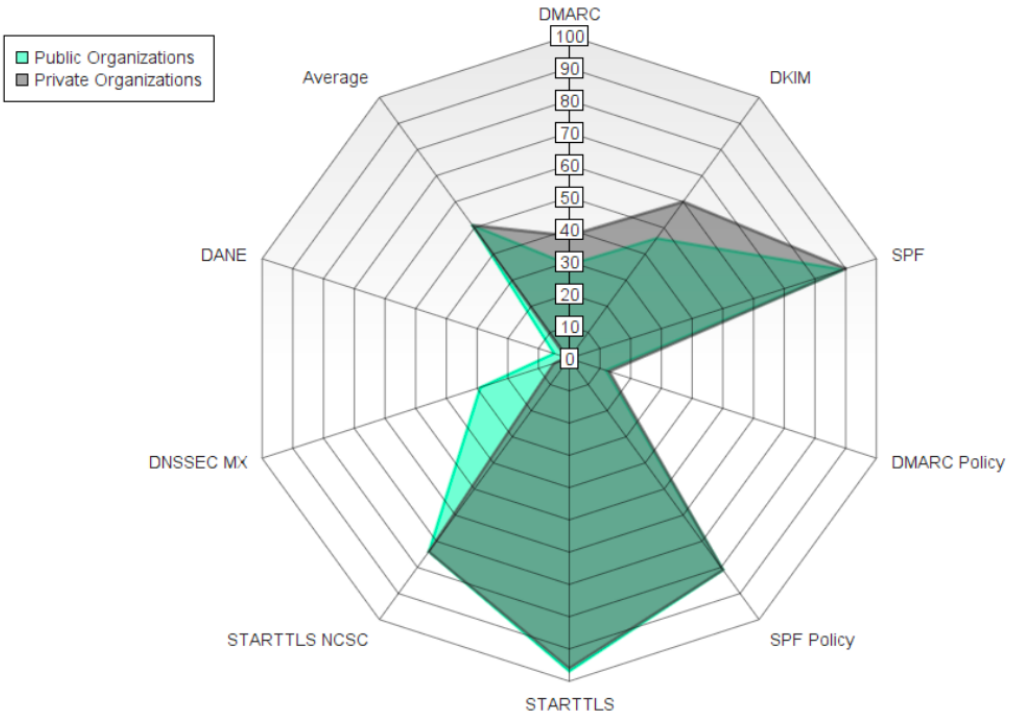
The result showed that the organization size did not affect or play a significant role in the decision making of the adoption of the email security mechanisms. The three tested organizations' groups which are large, medium-sized, and small, had almost the same rate of adoption, which is about 47 percent. However, it was noticeable that there was a small distinction between them, which is about 2% to 3% of adoption. As it is shown in Figure 6.2, large organizations were relatively better than the medium, and the same for the medium when compared to the smaller ones. However, to decide whether the displayed value can be considered a significant difference or not. An ANOVA test had been performed to confirm the result. The study concluded that the efficiency of the adopted email security mechanisms was not affected by the size of the company.



Organization Size	DMARC	DKIM	SPF	DMARC Policy	SPF Policy	STARTTLS	STARTTLS NCSC	DNSSEC MX	DANE	AVERAGE
Large	34%	55%	90%	12%	81%	96%	78%	4%	1%	50%
Medium-sized	24%	43%	84%	10%	78%	98%	91%	6%	2%	47%
Small	12%	44%	76%	3%	66%	99%	79%	6%	2%	43%

Figure 6.2: The adoption rate based on organizations' size.

To answer whether the adoption rate of standards was related to the organizations' sector or not. The results of the tested public organizations were compared to the top 1000 private organizations. The result showed that the organizations' sector did not affect the adoption of email security standards because both public and private organizations had the same adoption average, which is 51% of adoption. Figure 6.3 illustrates the results. The difference was that public organizations had a higher adoption rate of DNSSEC and DANE standards than the private ones, while the private organizations excelled at the authentication mechanisms, especially when it comes to DMARC and DKIM. Among all the tested organizations, only 9 organizations have implemented all of the investigated email security mechanisms, including sufficient policy, all of them were public organizations. However, since the average number was quite similar, the adoption of the email security mechanisms was not affected by the sector of the organizations.



Organization Sector	DMARC	DKIM	SPF	DMARC Policy	SPF Policy	STARTTLS	STARTTLS NCSC	DNSSEC MX	DANE	AVERAGE
Public	29%	46%	89%	12%	81%	97%	74%	29%	5%	51%
Private	38%	60%	90%	13%	81%	96%	74%	5%	1%	51%

Figure 6.3: Internet Standards adoption by Swedish organizations based on sector.

The result showed that organizations' location did not significantly affect the adoption of the email security mechanisms. Figure 6.4 shows the adoption rate for the tested organization for each county. There was a small distinction between them, which is about 12% in total between the highest and lowest rate. In order to decide whether the displayed value for each county can be considered a significant difference or not, the ANOVA test had been performed to confirm the result. Although there was a small difference in the adoption rate based on location, the quantity or the quality of the adopted email security mechanisms was not affected by location.

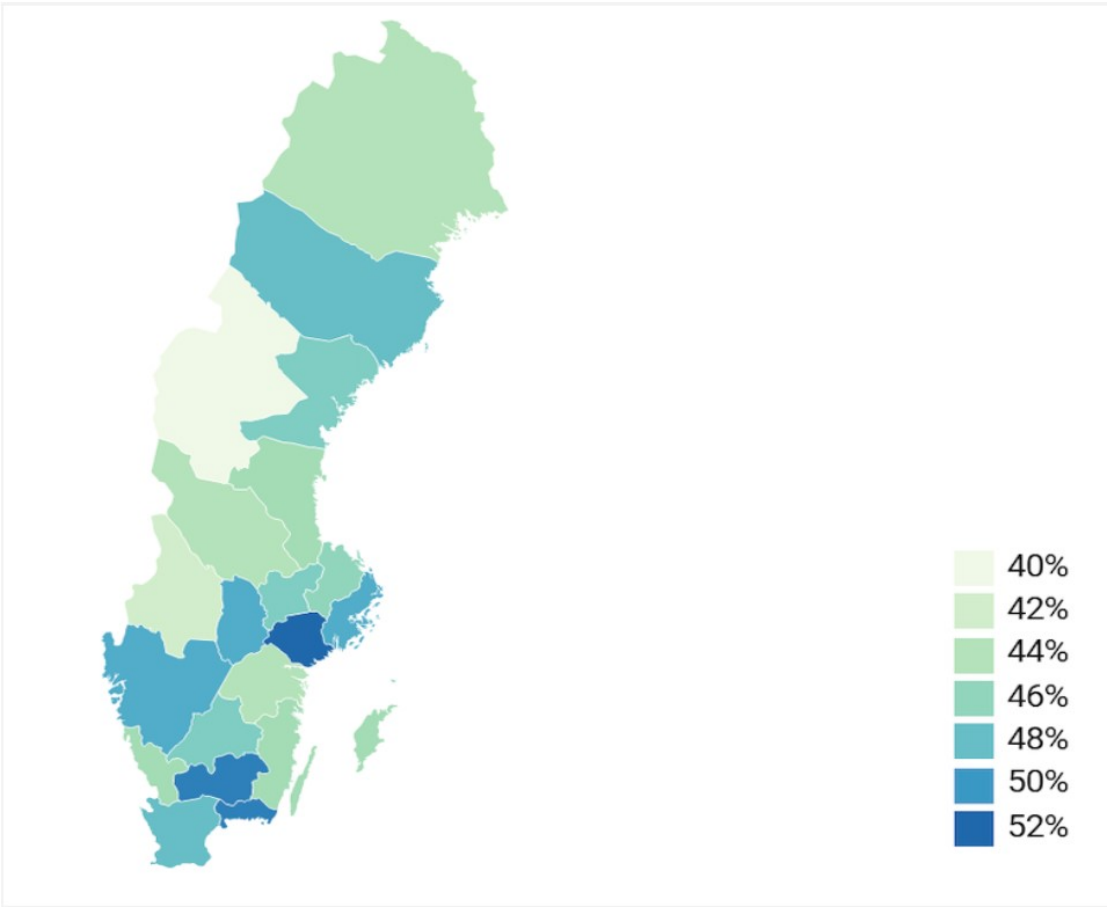


Figure 6.4: The adoption of email security extensions by the Swedish organizations based on counties.

Question 3: How vulnerable are the tested Swedish organizations against email attacks in the light of the studied Internet Security Standards?

The overall tested organizations were 1973 organizations in total that have 1514 distinct email domains. Figure 6.5 illustrates the adoption rate of each Internet Standard by the tested organizations. More statistical information is given in Table 1.11 Appendix 1.

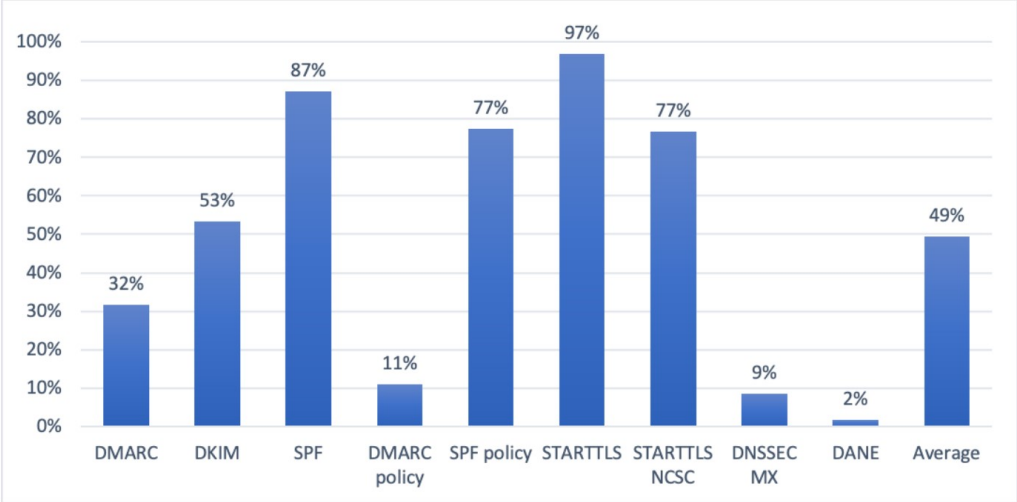


Figure 6.5: Internet Standard adoption rate by Swedish organizations.

The results showed that the average adoption of SPF, DKIM, and DMARC with sufficiently strict policies is 52%. That indicated the rest of the tested Swedish organizations (48%) were vulnerable to phishing attacks using sender domain forgery. Which means, one of two of the tested Swedish organizations were vulnerable to phishing attacks using sender domain forgery.

From a different angle, about 10% of the tested Swedish organizations that had SPF available, did not implement SPF with proper policy. And 13% of the tested Swedish organizations did not implement SPF at all. Therefore, about 23% of the tested organizations were vulnerable to phishing attacks using sender domain forgery in the case of not considering DMARC and DKIM. Furthermore, 47% of the tested organizations did not implement DKIM. That made them vulnerable to phishing attacks using sender domain forgery in the case of not considering DMARC and SPF.

About 90% of the tested organizations had no DNSSEC signed mail server domains. That made them vulnerable to active network attacks that might redirect their incoming mails into a server that is under the attacker's control. As a result, 9 of 10 of these organizations were exposed to email pharming attacks by DNS spoofing.

A large number of the tested organizations (97%) had STARTTLS implemented for secure mail communication. But, only 77% of them had secure parameters for STARTTLS. However, only 2% of them had DANE implemented. STARTTLS and DANE together can provide better protection against passive eavesdroppers. Considering that STARTTLS still allows opportunistic encryption and MITM downgrade TLS attacks, DANE plays a significant role to enhance STARTTLS security by indicating that the sender must use TLS and providing TLS downgrade-resistant. Since the majority of the tested organizations (98%) did not implement DANE, they were vulnerable to email passive eavesdropping attacks. In other words, 98 out of 100 organizations were vulnerable to email passive eavesdropping attacks. Figure 6.6 shows The possibility of the tested organizations to get attacked in light of the studied Internet Standards and relevant attacks.

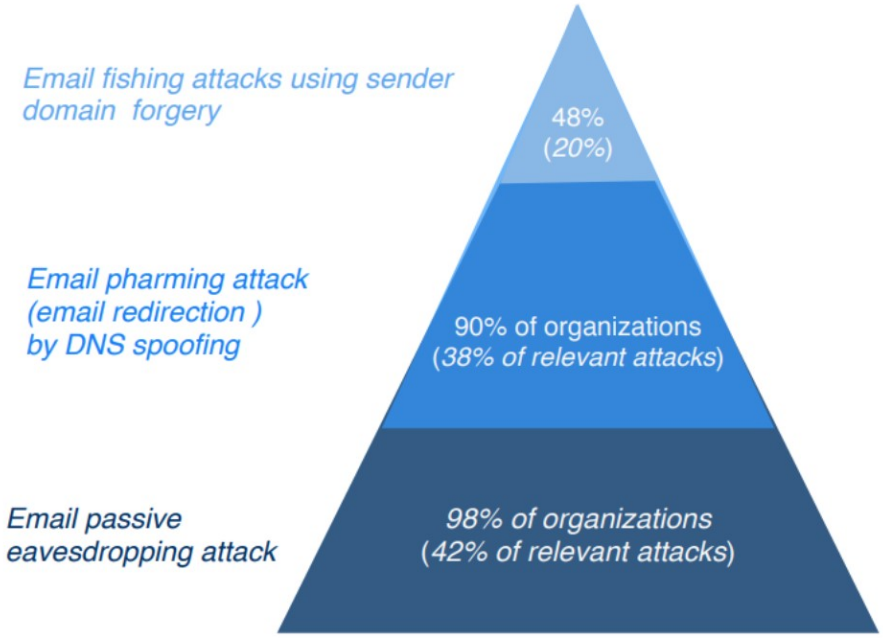


Figure 6.6: The possibility of Swedish organizations to get attacked in light of the studied Internet Standards.

7 Discussion

The adoption rate of the email security standards by the examined Swedish organizations was somewhat as expected; the average rate was about 50%. Even though the adoption rate varied from one standard to another, the result of specific mechanisms such as STARTTLS and SPF was promising, while for some other mechanisms, especially when it comes to DANE, DNSSEC was much lower than what was expected.

Since it is a proven fact that email is a major threat surface of the organizations' system, it was unexpected that a large number of the tested organizations paid no attention to these mechanisms, especially the anti-spoofing ones. But then, while doing the research, it was noticeable that the lack of the protection mechanism is not only for the organizations within Sweden but worldwide. The research finding was similar to other related research findings that indicated there is a lack of adopting protection mechanisms. That makes the majority of these organizations vulnerable against a different type of email attack unless decisive actions are taken by them to secure these services. In addition, many organizations already have some of these mechanisms implemented in their system, but they were not configured properly, which made them useless; however, that can be considered an essential step toward full adoption in a later stage.

The good news is that the adoption rate of email security mechanisms is continuously increasing. During the experiment and to get more accurate results, several tests were conducted at different times. The results indicated that the adoption rate of some standards was increased by 1 or 2 percent in a relatively short time, which means that these numbers might significantly change during the next few months. Nevertheless, there is still much to be done to make email services more secure. Governments and the IT community could positively contribute making the process of the adoption of these protection mechanisms faster. That can be done by defining guidelines or rules that force or at least strongly recommend the adoption of these techniques. Especially that it is proven that these mechanisms can play a significant role in preventing or mitigating the risk of email services.

The importance of adopting the discussed email standards can be determined by the threats that they mitigate. Email phishing is still the most frequent attack vector that faces the email service's users [34]. SPF, DKIM, DMARC are meant to be anti-phishing techniques. While SPF and DKIM can flag messages as being spoofed, DMARC that was built on them comes to add some features. Such features are the efficient policies that should be taken when spoofed addresses are detected, and reporting mechanisms which enable the domain used in the sender email to know whether it was abused. Therefore, these mechanisms should be dealt with as one anti-phishing technique. On a scale from 1 to 3, where 3 is the most important email security mechanism, this mechanisms is given a score of 3. Email pharming at DNS level (email redirecting by DNS spoofing) is the latest incarnation of phishing attacks; it is the attack of the future [35]. DNSSEC is meant to mitigate email pharming attacks. This mechanism is given a score of 2. Email eavesdropping against the cleartext email connection is a targeted email attack. TLS over SMTP can be used to encrypt the connection between mail components. Without DANE which indicates that the user MUST use STARTTLS, TLS encryption can be ignored. Since DNSSEC is a precondition for DNAE, the mechanisms (DNSSEC, STARTTLS, and DANE) can be considered one mechanism against Email eavesdropping and given a score of 1. The highest threats can be a trade-off, where the high importance mechanisms have low adoption rates. Hence, the risk of eavesdropping on the email connection that tested organizations can be exposed to is the highest, while the risk of exposure to pharming

and phishing attacks comes in second and third place, respectively. Low adoption of DNAE and DNSSEC can be returned to the fact that they are modern Internet Standards. Microsoft has recently announced that it will support DNSSEC and DANE for SMTP in its online office exchange service to provide advanced email protection to the customers [36]. The insecure connection is the highest risk because of the low adoption of the prevention mechanism such as DANE.

7.1 Recommendations

We think that it is a reasonable choice that the organizations start adopting the anti-phishing techniques (SPF, DKIM, and DMARC as one mechanism) in the first place to ensure that their domains are not abused. Secondly, considering that DNSSEC is a pre-condition for DANE, and considering that email pharming is the gate to phishing which can damage the organization when stealing sensitive information. It is recommended for organizations to implement DNSSEC as a second step. Finally, as Microsoft's approach, DANE along with DNSSEC, and STARTTLS can be applied to ensure the emails' confidentiality.

8 Conclusion

In this research, the quantity and quality of the email protection mechanisms adopted by some Swedish organizations to secure their email services are examined. The experiment includes nearly 2000 organizations located in Sweden. Furthermore, the recommended protection standards are explained in detail, and a comprehensive vision provided on how these mechanisms have a positive impact on reducing email threats.

The research shows that there is no distinction in the adopted mechanisms based on several factors such as size, sector, or location in the organizations within Sweden. The average adoption rate for the tested organization is quite similar, which is a 50% adoption rate of the tested protection mechanisms. Also, it demonstrates and discusses several types of email attacks the involved organizations might be vulnerable to due to the lack of protection.

In conclusion, the research confirms the concerns that there is a lack of protection mechanisms, and serious actions should be taken either individually by the organizations or by the IT community in general to ensure the security of email services.

8.1 Future work

The research aims to investigate the email security mechanism for all Swedish organizations. But, since getting the required data about them was beyond our ability to get, we recommend if the same test can be done, including all the Swedish organizations. Besides, the same experiment also can be done periodically to measure the increasing rate of adoption. Moreover, future work also may expand the experiment by including newer security mechanisms such as SMTP MTA-STS. Finally, A replication of the study in other countries might also give a better insight into the status of email security worldwide, and not only in Sweden.

References

[1] Osterman Research INC, "Techniques for dealing with ransomware, business email compromise and spear phishing," An Osterman Research White Paper, January, 2017. Available at https://www.forcepoint.com/sites/default/files/resources/files/whitepaper_osterman_techniques_dealing_with_ransomware_en.pdf. [Accessed: Feb 10, 2020].

[2] G. Duncan, "Here's why your email is insecure and likely to stay that way," Digital Trends, 2013. Available at https://www.digitaltrends.com/computing/can-email-ever-be-secure. [Accessed: Feb 10, 2020].

[3] THE RADICATI GROUP, "Email statistics report, 2020-2024," The Radicati Group, Inc, 2020. Available at https://https://www.radicati.com/wp/wp-content/uploads/2019/12/Email-Statistics-Report-2020-2024-Executive-Summary.pdf.

[4] S. Kitterman, "Sender policy framework (spf)," Request for Comments 7208, April 2014. Available at https://www.irt.org/rfc/rfc7208.htm.

[5] E. Allman, Sendmail, Inc, J. Callas, PGP Corporation, M. Delany, M. Libbey, Yahoo! Inc, J. Fenton, M. Thomas, Cisco Inc, "Domainkeys identified mail (dkim) signatures," Request for Comments 4871, May 2007. Available at https://tools.ietf.org/html/rfc4871.

[6] M. Kucherawy, E. Zwicky, "Domain-based message authentication, reporting, and conformance (dmarc)," Request for Comments 7489, March 2015. Available at https://tools.ietf.org/html/rfc7489.

[7] D. Eastlake, "Domain name system security extensions," Request for Comments 2535, March 1999. Available at https://tools.ietf.org/html/rfc2535.

[8] P. Hoffman, "Smtp service extension for secure smtp over transport layer security," Request for Comments 3207, February 2002. Available at https://tools.ietf.org/rfc/rfc3207.

[9] J. Schlyter and P. Hoffman, "The dns-based authentication of named entities (dane) transport layer security (tls) protocol: Tlsa," Request for Comments 6698, August 2012. Available at https://tools.ietf.org/html/rfc6698.

[10] H. Hu and G. Wang, *Revisiting Email Spoofing Attacks*. New York, United States: Department of Computer Science, Cornell University, 2018.

[11] Z. Durumeric, D. Adrian, A. Mirian, J. Kasten, E. Bursztein, N. Lidzborski, K. Thomas, V. Eranti, M. Bailey, and J. A. Halderman, "Neither snow nor rain nor mitm...: An empirical analysis of email delivery security," in *Proceedings of the 2015 Internet Measurement Conference*, ser. IMC '15. New York, NY, USA: Association for Computing Machinery, 2015, p. 27–39. [Online]. Available: https://doi-org.proxy.lnu.se/10.1145/2815675.2815695

[12] T. Nanaware, P. Mohite, and R. Patil, "Dmarcbox – corporate email security and analytics using dmarc," in *2019 IEEE 5th International Conference for Convergence in Technology (I2CT)*, 2019, pp. 1–5.

[13] J. Klensin, “Simple mail transfer protocol,” RFC 5321, October 2008. Available at https://tools.ietf.org/html/rfc5321#section-7.1.

[14] Verizon, “Data breach investigation report,” Verizon, 2019. Available at https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf.

[15] Internet.nl, “About internet.nl,” Internet.nl, 2020. Available at https://internet.nl. [Accessed April. 14, 2020].

[16] Weinbaum, Cortney, Landree, Marjory S. Blumenthal, Tepring Piquado, and Carlos Gaviria, “Ethics in scientific research: An examination of ethical principles and emerging topics,” RAND Corporation, 2019. Available at https://www.rand.org/pubs/research_reports/RR2912.html.

[17] Jonas Åkerman, “Ethical review,” Stockholm university. Available at https://www.su.se/english/research/research-ethics/ethical-review-1.332303. [Accessed May 11, 2020].

[18] D. Crocker, “Internet mail architecture,” Request for Comments 5598, July 2009. Available at https://www.rfc-editor.org/pdfrfc/rfc5598.txt.pdf.

[19] W. Stallings, "Electronic mail security", *in Network security essentials: Applications and Standards*, 4th ed. NJ ,New York, USA: Persons education, Inc, 2011, ch. 7, sec.3, pp.257–261.

[20] P. Carranza, “How to use an spf record to prevent spoofing improve e-mail reliability,” DigitalOcean, July 2013 Available at https://www.digitalocean.com/community/tutorials/how-to-use-an-spf-record-to-prevent-spoofing-improve-e-mail-reliability.[Accessed April. 22, 2020].

[21] Wikipedia, “Sender policy framework,” Wikipedia. Available at https://en.wikipedia.org/wiki/Sender_Policy_Framework.[Accessed Mar. 3, 2020].

[22] ——, “DMARC,” Wikipedia. Available at https://en.wikipedia.org/wiki/DMARC.[Accessed Mar. 5, 2020].

[23] DMARC.org, “DMARC Background,” dmarc.org Available at https://dmarc.org/overview/.[Accessed Mar. 5, 2020].

[24] A. Friedlander, A. Mankin, W. D. Maughan, and S. D. Crocker, “Dnssec: A protocol toward securing the internet infrastructure,” *Commun. ACM*, vol. 50, no. 6, p. 44–50, Jun. 2007. [Online]. Available: https://doi-org.proxy.lnu.se/10.1145/1247001.1247004

[25] Cloudflare, “How dnssec works,” Cloudflare. Available at https://www.cloudflare.com/dns/dnssec/how-dnssec-works/ [Accessed Mar. 6, 2020].

[26] P. Turner, W. Polk, E. Barker, “Preparing for and responding to certification authority compromise and fraudulent certificate issuance,” National Institute of Standards and Technology (NIST), July 2012. Available at https://csrc.nist.gov/csrc/media/publications/shared/documents/itl-bulletin/itlbul2012-07.pdf.

[27] R. Barnes, “Dane: Taking tls authentication to the next level using dnssec",” The Internet Engineering Task Force (IETF), October 2011. Available at https://www.ietfjournal.org/dane-taking-tls-authentication-to-the-next-level-using-dnssec/.

[28] C. Aishwarya, Raghuram M A, S. Hosmani, M. S. Sannidhan, B. Rajendran, K. Chandrasekaran, and B. S. Bindhumadhava, “Dane: An inbuilt security extension,” in *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, 2015, pp. 1571–1576.

[29] V. Dukhovni and W. Hardaker, “Dane for smtp,” The Internet Engineering Task Force (IETF), July 2013. Available at https://www.ietf.org/proceedings/87/slides/slides-87-dane-2.pdf.

[30] B. Aslam, L. Wu, and C. C. Zou, “Pwdip-hash: A lightweight solution to phishing and pharming attacks,” in *2010 Ninth IEEE International Symposium on Network Computing and Applications*, Cambridge, MA, 2010, pp. 198–203.

[31] Wikipedia. (2020) Dns spoofing. Available at https://en.wikipedia.org/wiki/DNS_spoofing. [Accessed: Apr. 14, 2020].

[32] W. Z. Khan, M. K. Khan, F. T. Bin Muhaya, M. Y. Aalsalem, and H. Chao, “A comprehensive study of email spam botnet detection,” *IEEE Communications Surveys Tutorials*, vol. 17, no. 4, pp. 2271–2295, 2015.

[33] The statistical office of the European Union, “Small and medium-sized enterprises (smes),” Available at https://ec.europa.eu/eurostat/web/structural-business-statistics/structural-business-statistics/sme. [Accessed: Mar. 26, 2020].

[34] B. B. Gupta, A. Tewari, A. Jain, and D. Agrawal, “Fighting against phishing attacks: state of the art and future challenges,” *Neural Computing and Applications*.

[35] R. Collette and M. Gentile, “Countering the phishing/pharming threat,” Computer Economics. Available at www.computereconomics.com/article.cfm?id=1099. [Accessed: May. 11, 2020].

[36] Microsoft, “Support of dane and dnssec in office 365 exchange online,” Available at https://techcommunity.microsoft.com/t5/exchange-team-blog/support-of-dane-and-dnssec-inoffice-365-exchange-online/ba-p/1275494#. [Accessed: May. 11, 2020].

A Appendix 1

Table 1.1: Internet Standards adoption rate by the public Swedish organizations (Group 1).

Email domain	DMARC	DKIM	SPF	DMARC policy	SPF policy	STARTTLS	STARTTLS NCSC	DNSSEC e-mail domain	DNSSEC MX	DANE
Total domains	217	217	217	217	217	217	217	217	217	217
Support	64	99	194	25	176	204	155	116	63	11
Not support	153	118	23	192	41	6	55	101	152	199
Not_applicable	0	0	0	0	0	2	2	0	2	2
Not_testable	0	0	0	0	0	5	5	0	0	5
Percentage	29%	46%	89%	12%	81%	97%	74%	53%	29%	5%

Table 1.2: The adoption rate of STARTTLS and DANE by the public organizations (Group 1).

Email domain	STARTTLS and DANE	STARTTLS available	TLS version	Cipher suites	Key exchange parameters	TLS compression	Secure renegotiation	Client-initiated renegotiation	Trust chain of certificate	Public key of certificate	Signature of certificate	Domain name on certificate	DANE existence	DANE validity
Total domains	217	217	217	217	217	217	217	217	217	217	217	217	217	217
Support	11	204	180	170	183	200	202	80	189	204	200	153	11	11
Not support	206	6	30	40	27	10	8	130	21	6	10	57	199	199
Not_applicable	0	2	2	2	2	2	2	2	2	2	2	2	2	2
Not_testable	0	5	5	5	5	5	5	5	5	5	5	5	5	5
Percentage	5%	97%	86%	81%	87%	95%	96%	38%	90%	97%	95%	73%	5%	5%

Table 1.3: Internet Standards adoption rate by the top 1000 private Swedish organizations (Group 2).

Email domain	DMARC	DKIM	SPF	DMARC policy	SPF policy	STARTTLS	STARTTLS NCSC	DNSSEC e-mail domain	DNSSEC MX	DANE
Total domains	803	803	803	803	803	803	803	803	803	803
Support	306	477	722	104	653	729	562	123	39	8
Not support	497	324	81	699	150	34	201	680	760	755
Not_applicable	0	2	0	0	0	4	4	0	4	4
Not_testable	0	0	0	0	0	36	36	0	0	36
Percentage	38%	60%	90%	13%	81%	96%	74%	15%	5%	1%

Table 1.4: The adoption rate of STARTTLS and DANE by the top 1000 private Swedish organizations (Group 2).

Email domain	STARTTLS and DANE	STARTTLS available	TLS version	Cipher suites	Key exchange parameters	TLS compression	Secure renegotiation	Client-initiated renegotiation	Trust chain of certificate	Public key of certificate	Signature of certificate	Domain name on certificate	DANE existence	DANE validity
Total domains	803	803	803	803	803	803	803	803	803	803	803	803	803	803
Support	8	730	653	624	657	708	727	437	686	727	723	614	8	8
Not support	795	33	110	139	106	55	36	326	77	36	40	149	755	754
Not_applicable	0	4	4	4	4	4	4	4	4	4	4	4	4	4
Not_testable	0	36	36	36	36	36	36	36	36	36	36	36	36	37
Percentage	1%	96%	86%	82%	86%	93%	95%	57%	90%	95%	95%	80%	1%	1%

Table 1.5: Internet Standards adoption rate by the private Swedish organizations (Group 3).

Email domain	DMARC	DKIM	SPF	DMARC policy	SPF policy	STARTTLS	STARTTLS NCSC	DNSSEC e-mail domain	DNSSEC MX	DANE
Total domains	623	623	623	623	623	623	623	623	623	623
Support	143	290	519	49	467	563	454	128	33	8
Not support	480	333	104	574	156	11	120	495	587	566
Not_applicable	0	0	0	0	0	3	3	0	3	3
Not_testable	0	0	0	0	0	46	46	0	0	46
Percentage	23%	47%	83%	8%	75%	98%	79%	21%	5%	1%

Table 1.6: The adoption rate of STARTTLS and DANE by the Private Swedish organizations (Group 3).

Email domain	STARTTLS and DANE	STARTTLS available	TLS version	Cipher suites	Key exchange parameters	TLS compression	Secure renegotiation	Client-initiated renegotiation	Trust chain of certificate	Public key of certificate	Signature of certificate	Domain name on certificate	DANE existence	DANE validity
Total domains	623	623	623	623	623	623	623	623	623	623	623	623	623	623
Support	8	563	509	494	529	548	560	367	537	562	557	469	8	8
Not support	615	11	65	80	45	26	14	207	37	12	17	105	566	566
Not_applicable	0	3	3	3	3	3	3	3	3	3	3	3	3	3
Not_testable	0	46	46	46	46	46	46	46	46	46	46	46	46	46
Percentage	1%	98%	89%	86%	92%	95%	98%	64%	94%	98%	97%	82%	1%	1%

Table 1.7: Internet Standards adoption rate by Large private Swedish organizations.

Email domain	DMARC	DKIM	SPF	DMARC policy	SPF policy	STARTTLS	STARTTLS NCSC	DNSSEC e-mail domain	DNSSEC MX	DANE
Total domains	204	204	204	204	204	204	204	204	204	204
Support	69	112	183	24	165	192	156	27	8	1
Not support	135	92	21	180	39	7	43	177	196	198
Not_applicable	0	0	0	0	0	0	0	0	0	0
Not_testable	0	0	0	0	0	5	5	0	0	5
Percentage	34%	55%	90%	12%	81%	96%	78%	13%	4%	1%

Table 1.8: Internet Standards adoption rate by medium-sized private Swedish organizations.

Email domain	DMARC	DKIM	SPF	DMARC policy	SPF policy	STARTTLS	STARTTLS NCSC	DNSSEC e-mail domain	DNSSEC MX	DANE
Total domains	210	210	210	210	210	210	210	210	210	210
Support	50	90	176	22	163	188	155	45	12	4
Not support	160	120	34	188	47	3	36	165	197	187
Not_applicable	0	0	0	0	0	1	1	0	1	1
Not_testable	0	0	0	0	0	18	18	0	0	18
Percentage	24%	43%	84%	10%	78%	98%	81%	21%	6%	2%

Table 1.9: Internet Standards adoption rate by small private Swedish organizations

Email domain	DMARC	DKIM	SPF	DMARC policy	SPF policy	STARTTLS	STARTTLS NCSC	DNSSEC e-mail domain	DNSSEC MX	DANE
Total domains	210	210	210	210	210	210	210	210	210	210
Support	27	93	159	6	139	184	147	55	13	3
Not support	183	117	51	204	71	2	39	155	195	183
Not_applicable	0	0	0	0	0	2	2	0	2	2
Not_testable	0	0	0	0	0	22	22	0	0	22
Percentage	13%	44%	76%	3%	66%	99%	79%	26%	6%	2%

Table 1.10: Internet Standards adoption rate by private Swedish organizations based on location.

County	DMARC	DKIM	SPF	DMARC policy	SPF policy	STARTTLS	STARTTLS NCSC	DNSSEC e-mail domain	DNSSEC MX	DANE	Average
Södermanland	23%	47%	90%	17%	90%	96%	89%	30%	10%	3%	52%
Blekinge	30%	63%	87%	20%	83%	100%	78%	30%	0%	0%	51%
Kronoberg	30%	57%	87%	13%	77%	100%	90%	23%	3%	0%	51%
Västra götaland	37%	53%	83%	13%	80%	93%	74%	17%	7%	0%	49%
Örebro	17%	57%	87%	7%	77%	97%	90%	27%	7%	3%	49%
Stockholm	33%	70%	87%	7%	77%	97%	69%	7%	0%	0%	49%
Skåne	40%	63%	87%	7%	73%	93%	72%	10%	0%	0%	48%
Västerbotten	17%	53%	90%	10%	80%	100%	76%	20%	3%	0%	48%
Västmanland	30%	47%	90%	3%	80%	100%	70%	17%	3%	0%	47%
Västernorrland	17%	50%	90%	7%	83%	100%	69%	17%	7%	0%	47%
Jönköping	33%	43%	73%	10%	70%	100%	81%	17%	7%	3%	47%
Uppsala	23%	55%	77%	0%	68%	100%	77%	32%	6%	3%	46%
Halland	23%	37%	87%	7%	70%	100%	85%	17%	0%	0%	45%
Gotland	21%	25%	79%	4%	79%	100%	83%	38%	13%	0%	45%
Kalmar	17%	47%	80%	10%	73%	100%	63%	23%	10%	3%	45%
Gävleborg	17%	33%	77%	10%	67%	100%	78%	23%	17%	3%	45%
Norrbotten	17%	41%	72%	7%	62%	96%	88%	14%	10%	3%	44%
Östergötland	7%	33%	87%	3%	80%	100%	86%	13%	0%	0%	44%
Dalarna	23%	37%	80%	0%	67%	100%	77%	20%	7%	3%	44%
Värmland	13%	37%	83%	10%	73%	90%	76%	23%	0%	0%	42%
Jämtland	13%	23%	73%	0%	63%	96%	88%	17%	3%	0%	40%

Table 1.11: Internet Standards adoption rate by all the tested Swedish organizations.

Email domain	DMARC	DKIM	SPF	DMARC policy	SPF policy	STARTTLS	STARTTLS NCSC	DNSSEC e-mail domain	DNSSEC MX	DANE
Total domains	1512	1512	1512	1512	1512	1512	1512	1512	1512	1512
Support	480	806	1317	166	1171	1365	1080	345	129	25
Not support	1032	704	195	1346	341	43	328	1167	1375	1383
Not_applicable	0	2	0	0	0	8	8	0	8	8
Not_testable	0	0	0	0	0	96	96	0	0	96
Percentage	32%	53%	87%	11%	77%	97%	77%	23%	9%	2%