DALARNA UNIVERSITY

Student Thesis

Level: Bachelor

Improving Email Security in Organizations: Solutions and Guidelines

Author: Axel Andrén, Ghaith Kashlan & Atichoke Nantarat
Supervisor: Hans Jones
Examiner: Yves Rybarczyk
Subject/main field of study: Microdata analysis
Course code: GMI2C8
Credits: 15
Date of examination: 2023-05-29

Abstract

Data breaches from email attacks have been an issue since email was first implemented. Common attack methods like phishing are still a threat to organizations to this very day. That is because it never seems to stop evolving and keeps becoming more and more convincing. Email compromises have caused billions of dollars in damage worldwide, and it shows no sign of stopping. The purpose and research questions of this thesis are formulated to find guidelines or solutions that organizations can follow to improve their overall email security and awareness. In this thesis, both a systematic literature review and interviews are methods used to conduct the research. That way, both the technical portion of the subject, as well as the human perspective are covered. We found that the most common and significant email threats to organizations are phishing, BEC, and APT attacks. This thesis provides methods to mitigate these threats. What has also become clear is that human mistakes are a large portion of the problem concerning email attacks.

Keywords: Email Security, Email Awareness, Phishing, Email Attacks, Social Engineering

Contents

1. Introduction

This chapter serves as an introduction to the research thesis. Firstly, some key concepts will be introduced. Secondly, the background of the thesis will be presented to provide contextual information for the thesis. Thirdly, the problem formulation and research aim will be introduced to highlight the research questions and objectives. Lastly, the scope and delimitations of the research will be outlined to establish the boundaries and limitations of the thesis.

1.1 Key Concepts

Confidentiality, Integrity, Availability (CIA): Confidentiality refers to protecting sensitive information from unauthorized access. Integrity refers to that the data is legitimate trustworthy and has not been modified or tampered with by an unauthorized user. And lastly, Availability refers to data that is accessible when you need it (Washington University in St. Louis, n.d.).

Data breach: Unauthorized access from an unauthorized party that gains access to sensitive or confidential data (IBM Security, n.d.).

Social Engineering: Social engineering is a broad concept of attacks consisting of getting people to provide sensitive data or take a step that might compromise an organization's security (Peltier, 2006).

Phishing: Phishing is a social engineering attack that aims to steal user data, credentials, credit card information, and/or more (Imperva, n.d.).

Spear phishing: Spear phishing is a more targeted form of phishing where the attacker sends a personalized email to a specific individual or group of individuals within an organization (Imperva, n.d.).

Bring Your Own Device (BYOD): A well-known approach implemented in most organizations, employees are allowed to bring their personal devices such as laptops, mobile devices, and other portable devices to work and use it for work-related purposes (Bann et al., 2015).

Advanced Persistent Threat (APT): A systematic and complex attack used by highly skilled perpetrators that over a prolonged time span compromises machines and networks in an

organization. APT attacks can cause a data breach, unauthorized disclosure of confidential information and or reputational damage (Bann et al., 2015).

Email security policy: Includes a set of guidelines and rules that dictate how to properly use email within a network or organization. It describes specific protocols that are required to be followed by a group of users (Odogwu, 2022).

Business Email Compromise (BEC): When phishing is conducted for information or monetary gain against a business (Microsoft, n.d.).

Malware: Harmful software that is developed to intrude and corrupt a computer, or computer network (Cisco Security, n.d.).

End-to-End System: A process that takes a complete solution that is designed to handle tasks or problems from start to finish, without the need for separate components (Sabir & Yousaf, 2018).

Anti-Spam software: A software that is used to filter emails such as spam, and phishing mail from legitimate emails. It is used to keep malicious emails out of a user's mailbox (Lowe, 2020).

Watering hole attack: Attackers infect a website's organization with malware. When a member of that organization visits the website, they expose their information (Haaster et al., 2016).

Bell La Padula model (BLP): A computer security model that focuses on access control and implements a Read Down and Write Up method. Read Down means that one with low level clearance should not have access to higher levels of security, but one with top level clearance should be able to "read down". Write Up means that a container protecting an object should not be able to have a lower clearance level than the object itself, since that would make the secret object visible (Bell & La Padula, 1976).

1.2 Background

In today's digital age, effective communication is essential to maintain efficient business operations. Email services are one of the most popular ways to communicate within organizations. Software and services such as Microsoft Outlook, Gmail, Apple Mail, and the Mail app on Windows operating systems are commonly used. These services are owned and developed by major corporations that have high-security standards (Alton, 2022).

However, according to IBM Security (2022), 83% of the organizations they contacted have experienced more than one data breach. One of the more costly attacks, business email compromises (BEC) had an average total cost of $4.89 million. Japan's IT Promotion Agency (2023) reports that financial damage caused by emails currently ranks third on the top 10 list of information security threats. These findings underline the criticality of understanding threats and vulnerabilities associated with email usage in organizations.

91% of all cyberattacks begin with an email, but the number of successful email attacks is much less than that (Ganacharya, 2020). Even though such a large majority of cyberattacks are email attacks, only 21% of successful cyberattacks are either some form of phishing or BEC (IBM Security, 2022). Email phishing is considered one of the most common threats in terms of email usage, with hundreds of millions of attempts against Gmail users daily (Bursztein & Oliveira, 2019). Since the number is so high, it is imaginable that the attackers send these phishing emails to any email address they get their hands on, but that is not the case. Several variables play a role in the likelihood of receiving an email of this nature. The variables with the most impact are age, email activity, and prior risk exposure, meaning users that somehow have data exposed by a third party. Those with prior risk exposure and active accounts are 5 times more likely to receive phishing emails (Simoiu et al., 2020). Phishing is constantly evolving, and 68% of the hundreds of millions of emails blocked by Gmail are variations that have not been seen before, and at the same time, almost half of the users do not know what phishing is (Bursztein & Oliveira, 2019).

Verizon’s 2022 data breach investigation report shows that the human element was the main weakness in 82% of breaches. A large majority of 89% of threat actors are motivated by financial gain, with the remainder driven by espionage. Phishing is the most common method of social engineering, and it remains popular because people are still consistently fooled by it. Close to 3% of employees consistently click on phishing emails. However, despite all the

negative reporting, there is still some good news: reporting of phishing incidents improves every year (Verizon, 2022).

A large majority of email attacks are considered to be social engineering attacks. The attacker uses different psychological tricks to retrieve information, to then use that information to gain access to a computer or network or for monetary gain (Peltier, 2006). This means that the attacker's goal is to trick the victim into giving them what they want. To succeed in tricking their victims, social engineers use people's human qualities to persuade them. A few examples of those qualities can be naivety, helpfulness, laziness, or the fear of getting into trouble (Peltier, 2006). The most well-known BEC scam as of yet was a variant known as vendor email compromise. A Lithuanian man set up a fake company with the same name as a real hardware supplier, "Quanta Computer", who at the time supplied Facebook and Google. He then sent invoices to the companies and it ultimately resulted in $121 million being stolen from Facebook and Google over a period of two years (Tessian, 2022).

1.3 Problem Formulation and Purpose

As previously stated, studies have shown that organizations lose large amounts of money because of BEC, phishing, and other email attacks. That means that a large portion of the problem with cyberattacks is not caused by the software but by human mistake (Verizon, 2022). There exists several security implementations to mitigate these threats, but somehow it is still a weakness that threat actors utilize and succeed in doing so.

All organizations have a need for secure email communication and therefore also mitigation against email attacks. Threat actors and their tools and tricks always improve and sometimes it is hard to separate a phishing email from an actual one. This is why most organizations need to implement email security to a greater extent, to minimize the risk of being liable or exposed. This thesis aims to investigate and explore the topic of secure email usage within organizations using both interviews and literature review. This involves conducting interviews with employees or other relevant individuals to gather empirical data and insights to answer these research questions:

- What are the most common methods used in successful email attacks against organizations?
- What are the potential solutions and guidelines for improving email security in organizations?

- What are the challenges associated with implementing email security measures in organizations?

1.4 Knowledge Contribution

The thesis aims to investigate common problems related to organizational email security to propose solutions and guidelines to improve resilience against email attacks. The information gathered will help inform organizations and facilitate the implementation of countermeasures against potential threats and vulnerabilities to email usage within organizations. Policymakers, IT managers, and many others can learn from the thesis's results about the significance of email security and the necessity for continuous development in this area.

1.5 Scope and Delimitations

The main focus of this thesis is on threats that are presented through normal email usage within organizations. This includes email usage where either the sender, receiver or both are using an organization or company-issued email address and excludes all other options. The thesis will primarily focus on post-authentication threats related to email usage, rather than threats that exist prior to the login process.

The research will be limited to current threats and vulnerabilities, and will not investigate outdated dangers or liabilities. Organizations of different sizes might face different risks associated with email usage, but the thesis will not be limited to any specific size of an organization. The thesis will not focus on a specific industry, and geographical limitations will not be necessary. That is because both threats and security implementations are most likely widely spread across different regions of the world.

2. Methodology

The Methodology chapter of this thesis outlines the steps taken to achieve the research objectives, which involves theoretical analysis of threats and vulnerabilities associated with email usage in organizations. This chapter presents the research design, data collection methods, and analysis techniques. Overall the aim of this chapter is to provide a comprehensive and transparent account of the research methods used to ensure that the findings are trustworthy, credible, and maintain academic integrity.

2.1 Internet Research

The internet has revolutionized the way researchers conduct their work, as it provides access to an enormous amount of information on almost any topic imaginable. The vast array of online resources available today means that researchers have access to a nearly limitless digital library of information (Florida Center for Instructional Technology, 2009).

Internet research is a strategy used to obtain information and data on how to secure email usage in organizations. However, as the internet is vast and can contain both poor and high-quality academic materials, checking that the author of the materials is authentic and trustworthy is a must to maintain quality for the thesis (Oates, 2006).

2.2 Data Collection

For data collection, it has been selected to perform internet research, and the digital libraries that were used are IEEE Xplore and Scopus. After searching through the digital libraries, screening was conducted by reading the abstract to select literature. Later, the whole literature was read through and those that did not give any result to the thesis were eliminated.

“AND” and “OR” were used in the search query to combine search terms quickly, to retrieve more precise results.

Our full search queries and selections are presented in Table 1 below.

Search Query	**Search Engine**	**Amount of Results**	**Selected Amount**
TITLE-ABS-KEY ("phishing" AND "security policy") AND (LIMIT-TO (OA , "all")) AND (LIMIT-TO (SUBJAREA , "ENGI") OR LIMIT-TO (SUBJAREA , "COMP") OR LIMIT-TO (SUBJAREA , "SOCI"))	Scopus	15	4
KEY (secure AND email) AND (LIMIT-TO (OA , "all")) AND (LIMIT-TO (SUBJAREA , "COMP"))	Scopus	13	1
"Document Title":Email) AND ("All Metadata":Secure Filter applied: Journals, Books, 2010-2023	IEEE Xplore	8	1

Table 1. Digital libraries and search queries.

2.2.1 Literature Review Contents

This table will present an overview of the literature review conducted and highlight the contributions made by each study. Additionally, the table includes the key findings and highlights the contribution made from our own research. To ensure clarity and conciseness, certain abbreviations will be used through the table. For better understanding a brief introduction of the abbreviations is provided below:

E2E: End-to-End email system

FI: Financial incentives

WH: Watering hole

SP: Security policy

Authors & year	**APT**	**BYOD**	**Phishing**	**E2E**	**Anti-spam**	**FI**	**WH**	**SP**
Sabir & Yousaf (2018)				✓				
Goel et al. (2021)			✓			✓		✓
Ismail et al. (2017)	✓	✓	✓				✓	✓
Silic & Back (2016)			✓					✓
Bann et al. (2015)	✓	✓	✓					✓
Lowe (2020)			✓		✓			
This Study	✓	✓	✓	✓	✓	✓		✓

Table 2. Literature review table of topics.

2.3 Literature Review

This chapter provides an overview of existing peer-reviewed articles, reports, research papers, and studies that are relevant to the scope and purpose of this report. The purpose of this literature review is to identify literature that can inform the research questions and contribute to a deeper understanding of threats and vulnerabilities that is associated with email usage within organizations.

2.3.1 Common methods used in successful email attacks

Social engineering is a broad concept, and a majority of email attacks have some form of it included. This type of attack consists of getting people to provide sensitive data or perform an action that might compromise an organization's security. This can involve strategies like Alibi, in which the attacker assumes the identity of a reliable person to win the victim's trust. Another strategy is Entice, in which the attacker presents a tempting incentive in exchange for confidential information (Peltier, 2006). Common methods for successful email attacks are phishing and spear phishing.

Phishing is a social engineering attack that aims to steal user data, credentials, credit card information, and/or more. Phishing is when an attacker poses as a trusted party and tricks the victim into opening an email or message of any kind and then clicking on a harmful link. The link can lead to downloading malware, a ransomware attack, or in any way revealing sensitive information (Imperva, n.d.). According to Silic & Back (2016, as cited in Boyed & Ellison, 2007) spear phishing is a more targeted form of phishing where the attacker sends a personalized email to a specific individual or group of individuals within an organization. The email may appear to be from a trusted source, such as a colleague or a senior executive, and may contain a request for sensitive information or a link to a malicious website (Imperva, n.d.).

Another common technique used in successful email attacks is malware attachments. Malware is software that is created to be intrusive or corruptive on a computer network. It is designed to steal data or resources for financial gain or sabotage purposes (Cisco, n.d.). The attacker sends an email with a malicious file attached which, when opened, infects the victim's computer with malware.

The last technique covered is BEC, which is used to steal critical information or money (Microsoft, n.d.). Microsoft (n.d.) states that there are five different types of BEC scams that, if successful, have the potential to be very severe and costly.

The first is Data theft, which usually targets HR departments to steal company information such as employees' schedules or personal data. The second is Chief Executive Officer (CEO) fraud, which is for example when a scammer either spoofs or hacks into a CEO's email account and then instructs employees to make money transfers. The third is Account compromise which is when scammers use phishing or malware to gain access to an employee's email account. The fourth is the False invoice scheme, which is sending companies fake invoices while posing as a legitimate vendor. Lastly, there is Lawyer impersonation, which is when scammers gain access to an email account at a law firm, and then, for example, email clients' invoices (Microsoft, n.d.).

2.3.2 Why is phishing still successful?

Phishing has been an issue for a long time and has been counteracted for just as long, but somehow it still works in deceiving victims into sending money or information. Bhardway et al. (2020) explain that a shift has recently happened, and cyber attackers have improved their methods. Instead of bulk spamming emails to any email address they get their hands on, they now try to perform targeted email phishing. These attacks now target high-level personnel such as CEOs, board members, or department heads, people that probably have access to more areas of an organization than other employees (Bhardway et al., 2020). Even though the attacks have been revamped and improved tremendously, they still use the same basic blueprint, tricking someone into clicking a link and providing information. Bhardway et al. (2020) further explain that apart from cloning websites to lure people into handing over login credentials, attackers also create fake QR codes. Those QR codes could then lead to a page that offers discounts on services or wares if you make an online payment, but in reality the payment goes to the attacker (Bhardway et al., 2020). Advertisements are often targeted nowadays and use personal offers, which makes scam emails very hard to detect.

A field experiment of employees engaged in social networking site (SNS) activities by Silic and Back (2015) revealed that employees are easy victims of SNSs that can provide psychological triggers to attackers. Organizations lack mechanisms to counteract SNSs security threats, as many companies do not have a strong information security policy that is related to SNSs. There are many security holes within SNSs, and many social engineering techniques can easily be facilitated. According to the experiment many employees lack security training related to awareness, risk, and threats of SNSs (Silic & Back, 2016).

2.3.3 Risks that come with BYOD

According to the 2014 Educare report cited in Ismail et al. (2017) paper the bring your own device trend is steadily increasing. According to Bann et al. (2015) and Ismail et al. (2017), BYOD is a rather popular trend in most organizations. However, there are drawbacks to it, and a major one is APT.

“APT is an intelligent and stealthy threat utilized by a group of highly motivated and resourceful perpetrators in order to extricate and leak important confidential data from the targeted political or business organizations" (Bann et al., 2015, p. 129).

One key feature of APT is the “Advanced”, where the APT employs different attacks and techniques via social engineering and spear phishing emails with malicious payloads to gather data (Bann et al., 2015). Ismail et al. (2017) explains that they shortened a link to a specific Google Play Store application which was a malicious application to an email, making it look genuine. The malicious application would later collect information such as username and password, and enter it into a database (Ismail et al., 2017).

2.3.4 What is APT

APT attacks have significantly increased in quantity as of late and can cause harm to an organization's system (Ismail et al., 2017). Two of the more common methods of APTs that threaten companies and other organizations are the watering hole strategy and spear phishing (Ismail et al., 2017). The watering hole strategy works by predicting or learning which websites an organization often uses and then infecting them with malware. The name APT comes from the fact that the attackers set traps that do not disappear or deteriorate, and wait until a victim falls for it.

Organizations that utilize BYOD are more likely to face APT attacks due to the general lack of understanding and awareness of users. Thus it can be hard to realize when an attack has happened (Ismail et al., 2017). BYOD is continuously gaining popularity amongst organizations. This creates a challenge to cybersecurity policy creators since the devices used in handling work information are no longer only used for work, but private matters as well (Bann et al. 2015).

2.3.5 End-to-End Web Based Trusted Email System

Sabir and Yousaf (2018) designed and implemented an end-to-end web-based trusted Email System. It provides complete end-to-end privacy, usability, portability, and trustworthiness. This system is made up of a server layer with a web server and Code Signing Module/Key Director Service CSM/KDS. It is also made up of a client layer with a plugin for a browser, a database layer for encrypted key storage, and a database layer. The emails get encrypted and decrypted and the keys can be safely stored, and finally, public key authentication is provided by CSM/KDS, which also interfaces with the server and clients. This design has been made in a complex way to ensure that the user does not need to have any technical knowledge to use it (Sabir & Yousaf, 2018).

Sabir and Yousaf (2018) also discuss the different solutions that already exist, such as Proxy-Based Designs, Identity-Based Encryption (IBE), Plugin-based approaches, and PKI-based solutions. All of these solutions contain weaknesses and have not been considered as truly end-to-end secure, therefore, the presented end-to-end design is the most secure solution (Sabir & Yousaf, 2018).

2.3.6 Anti-Spam Software

According to Lowe (2020), phishing emails are identified as spam and one way to deal with them is via Anti-spam software. The anti-spam software examines incoming mail to distinguish between spam and legitimate ones, and according to Lowe (2020), there exist 3 broad categories: on-premises, appliance, and cloud-based (hosted).

On-Premises Anti-Spam

An on-premises anti-spam program is a software application installed on a server within your network that evaluates incoming emails to identify spam and legitimate mail. It interacts directly with your email server, and legitimate emails are sent for regular processing while spam is either sent to a junk folder or stored in another location, depending on the configuration. The anti-spam software can be installed on the same server as the email server for smaller organizations or on a dedicated server for larger organizations (Lowe, 2020).

Advantages and disadvantages of using on-premises anti-spam according to Lowe (2020):
Advantages:

- High configurability and control.
- Tight integration with Microsoft Exchange and Outlook.

- User-friendly features.
- Relatively inexpensive.

Disadvantages:

- Requires maintenance and update by IT staff.
- Can experience periodic malfunctions and disrupt email flow.
- Increase workload on servers which means it will require additional resources.

Anti-Spam Appliances

An anti-spam appliance is a dedicated server that comes pre-installed with antispam software and is typically housed within a self-contained Linux-based computer. The appliance is easy to set up and use, requiring simple configuration via a web-based interface. Once connected to the network and configured, the appliance can offer many, if not all, of the features of on-premises anti-spam software (Lowe, 2020).

Advantages of using anti-spam appliances according to Lowe (2020):

Advantages:

- Simplified setup and installation process with pre-installed hardware and software.
- Self-sufficient operation with minimal maintenance required.
- Potential for additional security features, such as antivirus and firewall protection.

Disadvantages:

- Limited scalability and potential for outgrowing the appliance.
- Difficult in troubleshooting and repairing the appliance if any error would occur.

Cloud-Based Anti-Spam Services

A cloud-based anti-spam service is an online service that filters incoming emails before they reach your mail server. To use the service, you must reconfigure your public Dynamic Name System (DNS) so that your mail server points to the antispam service instead of directly to your mail server. The anti-spam service processes all incoming emails, only forwarding legitimate emails to your mail server. The service will store spam emails in the cloud for review or retrieval by users if needed (Lowe, 2020).

Advantages:

- No need to install and configure software, integrate it with Microsoft Exchange, or maintain it.
- No initial investment in software or hardware.
- Scalability and easy-to-add users.
- Reduce network and email server load.

Disadvantages:

- Less control over configuration options.
- Dependency on the service provides, including potential downtime.

May have limited options for customization.

2.4 Interviews

The interviews were conducted at an organization that will remain anonymous. The interviews were face-to-face and held in Swedish, and the transcripts were translated into English. The confidentiality of the organization and the interviewees were maintained to ensure ethical standards are upheld. The interviewees were named Employees 1 and 2, or E1 and E2 as pseudonyms when mentioned in writing to ensure their confidentiality.

Oates (2006) states that there are a few different types of interviews, and we elected to use semi-structured interviews. Semi-structured interviews allowed us to ensure the interview covered the subjects that needed to be explored, while not forcing questions that could make the interviewee uncomfortable (Oates, 2006). It also allowed the interview to cover more subjects beyond our initial approach. That is because both parties could speak more freely and go into further detail on subjects the interviewee had more knowledge of.

3. Results

This chapter will present the outcome of our data collection and interviews.

3.1 Interview Results

Both of the interviewed people stated that email is a vital part of their ability to do their job, since it is the main means of communication to both customers and co-workers. Microsoft Teams is in use within the company for internal communication, but email is still heavily relied upon, and a lot of times used instead or as a complement.

E1 prefers using the software application that Outlook provides, since it enables using more security settings. E1 also explains that they use Multi-Factor Authentication to login to their email account, which is required by their company's current security policy. On their own initiative, E1 uses another safety layer that is not required by their security policy, which is locking their Outlook phone application behind face ID. E2 on the other hand, secures their email usage by only checking the mail on their work computer or work phone. And also mentions that it is up to each and every employee to choose between using the Outlook application or the browser for email.

The awareness about phishing seemed strong amongst both of the people interviewed. Their company periodically conducts security courses and drills to make sure the people working there are always ready and aware of suspicious email activity. All employees are first asked questions about their knowledge on the subject of dangers with email. They will then be tested on their weaknesses to make everyone more well-rounded in terms of email security awareness and knowing the risks involved. The formal tests and subsequent testing is performed when they have time and is not in a classroom setting. Since they seemed so knowledgeable on the subject, this system seems to work, and they both said it has improved their awareness and was well received by other employees as well.

E1 and E2 go through a similar process when they encounter an email they suspect to be phishing. They check the sender's email address, as well as analyze the email, looking for grammar errors, misspellings or any signs of unusual activities. E1 can sometimes ask the sender about the email in person if E1 is unsure, and they both report and block phishing emails they encounter, both in private and at work.

E1 has a management position in the company, and has noticed a difference in the kind of phishing emails they receive. It is not often, but when E1 receives a phishing email to the business email address it is most of the time spear phishing. Someone pretending to be an employee of the company, asking E1 to do different things. E1 explains that their private email never receives emails that are so targeted, there it is mostly the regular kind of mass mailing. E1 reflected on email security, and said that even though you have all the knowledge in the world about phishing and other types of attacks, a mistake can happen. Maybe you are stressed or tired, and all the training in the world can not cover those moments.

3.2 Literature Review Results

This chapter will present the results from analyzing literature related to secure email usage within organizations. The aim is to provide readers with a comprehensive understanding of recommended strategies and techniques. It is important to note that while these practices are effective, they may not be universally applicable. Therefore, it is recommended to tailor them to the specific needs and context of each situation. It's also important to stay current and continuously reassess the effectiveness of existing practices as new ones may emerge due to changes in technology and societal norms.

3.2.1 BYOD

The SANS community, as cited in the study by Ismail et al. (2017), emphasizes the importance of BYOD security policies for companies that permit employees to use their devices for work purposes. SANS is an organization that provides education related to cybersecurity. They cover courses and training related to information security and cybersecurity training (SANS Institute, n.d.). The study also suggests that assigning security policies and methods to different roles with varying responsibilities can be an effective way to mitigate the risks associated with BYOD. The Bell La-Padula (BLP) model is a suitable approach for this purpose because it uses the no-write-down policy. The no-write down policy will prevent files from being uploaded into repositories or opened by lower-level users. This can help reduce the risk of data breaches and other security incidents caused by internal threats.

3.2.2 APT

Bann et al. (2015) highlight the importance of access control in mitigating APT attacks via spear phishing emails. The use of Mandatory Access Control (MAC) is the most appropriate approach for preventing unauthorized disclosure of highly sensitive data in such attacks. To

implement MAC, organizations can restrict access to data based on the sensitivity of the data and the clearance level of the user. This can help prevent unauthorized access to sensitive information and mitigate the risk of data breaches.

3.2.3 End-to-End Web Based Trusted Email System

The end-to-end solution is a high-security solution that is recommended for implementation in organizations, it provides secure and complete end-to-end privacy, usability, portability, and trustworthiness. This system is made up of a server layer with a web server and CSM/KDS. It is also made up of a client layer with a plugin for a browser, a database layer for encrypted key storage, and a database layer (Sabir & Yousaf, 2018).

In addition, implementing end-to-end web-based trusted email systems ensure the organizations their email usage from any kind of attack. Furthermore, it's important to note that implementing such a system can be expensive and time-consuming. Another important note is that the usage of HTTP requests can introduce performance considerations, depending on the volume of email traffic and the efficiency of the implementation (Sabir & Yousaf, 2018).

3.2.4 Anti-Spam Software

To ensure secure email usage within organizations, it is crucial to have effective anti-spam software in place. When selecting an anti-spam solution, organizations should follow best practices by considering their budget, required level of control and customization, and specific security needs. It is also important to evaluate the effectiveness and reliability of the considered solutions, as well as their ability to integrate with existing email systems and other security tools. According to Lowe (2020), organizations have several options for anti-spam software, including on-premises solutions, anti-spam appliances, and cloud-based services.

In addition, organizations should regularly educate their employees on safe email practices. Such education should include avoiding suspicious links and attachments, never providing personal information in response to unsolicited emails, and reporting any suspicious emails immediately. By implementing anti-spam software, organizations can help prevent phishing attacks and increase security in email usage within organizations (Lowe, 2020).

3.2.5 Minimizing spam and phishing emails

Anti-spam programs are not perfect and some amount of spam may still reach your inbox. To minimize the amount of undetected spam, the following are some guidelines that could help minimize spam emails to your main inbox (Lowe, 2020).

- Never trust emails requesting sensitive information, such as a bank sending an email notifying you about potential problems containing links to login pages. If you are in doubt, you can navigate manually with a web browser to the official legitimate bank website and check your information and status.
- Do not open attachments from unknown sources, as they may contain malware.
- Avoid replying to spam emails, as replies indicate that the email they sent an email to is in use and is a legitimate email address.
- Protect your email addresses by being careful of whom you give your email address to. Also, make sure your email address is only used on trusted websites, one should generally avoid publishing email addresses as much as possible.

3.2.6 Financial Incentives

According to Goel et al. (2021), financial incentives can be effective in promoting email security policy compliance among employees. The study divided participants into three groups: a control group, a positive group, and a negative group. The positive group received compensation for making fewer errors in complying with the security policy. The negative group received compensation for fewer errors but also faced a decrease in compensation as errors increased. And lastly the control group did not receive any compensation for compliance or non-compliance.

Goel et al. (2021) found that both the positive and negative groups made fewer errors compared to the control group, indicating that financial incentives can encourage employees to comply with email security policies. This is significant because non-compliance with email security policies can lead to security breaches, loss of sensitive information, and reputational damage for organizations.

Overall, the study suggests that financial incentives can be an effective tool in promoting email security policy compliance among employees. It can ultimately improve an organization's security posture and reduce the risk of security incidents.

4. Discussion

The main goal of this thesis was to explore strategies for securing email usage in organizations. The findings of this thesis provide valuable insights into the challenges faced by organizations in ensuring the CIA triad of email communications. In this chapter, we will discuss the key findings, their implications, and potential recommendations for improving email security practices.

4.1 What are the most common methods used in successful email attacks against organizations?

The discussion about common methods used in successful email attacks against organizations reveals the prevalent and evolving nature of these threats. Phishing, spear phishing, malware and BEC scams pose significant risk to organizational security and the confidentiality of sensitive information.

The results show effective and successful social engineering attacks. Phishing and spear phishing attacks take advantage of human weaknesses by acting like trustworthy sources and trick victims into providing sensitive information. In APT attacks, social engineering is used to gain access to sensitive information that can cause a data breach. These attacks pose significant risks to organizations, as they can result in data breaches, unauthorized disclosure of confidential information, and reputational damage.

Malware attachments are still a common way to access systems without authorization, steal data, or cause damage to the organization’s system. Attackers trick victims by sending emails with malicious attachments that, when opened, install malware on the victims computer and therefore get access to the organizations’ sensitive information.

BEC methods serve as another example of attackers' adaptability and tenacity. These types of scams use social engineering to trick victims into sending money or giving sensitive information.

4.2 What are the potential solutions and guidelines for improving email security in organizations?

By carefully analyzing the results from reviewing the existing literature, several potential solutions and guidelines have emerged to strengthen email security within organizations. Implementing these measures can significantly enhance the overall security posture and protect against various threats:

- **BYOD Security Policies**

  For organizations that allow employees to use personal devices for work purposes, implementing BYOD security policies is essential, as this will help to mitigate the risks associated with BYOD. These policies should outline guidelines for securing personal devices used for work and specify security protocols based on employees' roles and responsibilities.

- **APT mitigation**

  One way to effectively defend against APTs is with access control measures. Implementing stringent access controls, such as limiting access to sensitive data based on the user's role and clearance levels. This can significantly reduce the risk of unauthorized disclosure of confidential information. This helps prevent APT attacks that are often initiated through spear phishing emails, enhancing the overall security posture.

- **End-To-End Web based Trusted Email Systems**

  The implementation of end-to-end web-based trusted email systems can greatly enhance email security within organizations. These systems offer essential security features, including encryption and privacy. Organizations can achieve this by utilizing secure servers, browser plugins, and a database layer for encrypted key storage. Additionally, the use of a CSM/KDS can provide robust public key authentication for added security.

- **Anti-Spam Software**

  Organizations should carefully select anti-spam software that effectively minimizes the number of unwanted spam and phishing emails. By deploying reliable and up-to-date anti-spam solutions, organizations can reduce the risk of users falling victim to phishing attacks. Such software acts as a crucial line of defense in detecting and blocking malicious emails, ensuring a safer email environment for employees.

- **Employee awareness**

  To mitigate these risks, organizations must increase employees' awareness through ongoing up-to-date training, courses on email security, simulation of attacks, and what actions to take when under such attacks. This can reduce the risk of successful phishing attacks and protect sensitive information, and also strengthen employees' email usage security.

4.3 What are the challenges associated with implementing email security measures in organizations?

For many people, using email at work is a necessity since it provides a fast, easy, and reliable means of communication, and can be used on many different devices. Fast and easy communication is a staple part of many organizations across the globe, which is why you do not want to complicate it too much when it comes to securing it. If an organization's cybersecurity policy requires too many boxes that need to be checked before using your email, it could contribute to people either not following the policy or stopping using email. Instead, they might move to another method of communication, such as Microsoft Teams or cell phone messaging. Email is, and has been, very popular for a long time, but we live in an ever-changing and developing world. If the email security measures can not keep up, another method will supersede. If it is too much work to access the email account or services, employees will choose the path of least resistance and migrate to another option.

Another challenge is the one that comes with implementing an email security policy. It is difficult to make sure that everyone within an organization is compliant with the policy. Some might not use multi-factor authentication, Virtual Private Network (VPN), or other potential requirements, simply because of laziness. From our literature review, we found evidence that financial incentives can significantly improve compliance with an email security policy. The experiment showed that the best form of incentive was where participants received an award up front and would lose parts of it every time they clicked links in an email. One example of a potential implementation of a financial incentive could be as an add-on to an already existing bonus, which companies often offer. An example of how to implement it is by promising a 5-10% bonus on top of the already existing one, and if you make mistakes regarding the policy, you lose 1% each time. The specific numbers may vary depending on company budgets and other influencing factors.

The result of that study translates to, in terms of email usage, that if you have something to lose, you care more than you would if you had something to gain. But, you always have something to lose from falling victim to an email attack, whether that is directly or indirectly. It may be your login credentials that fall in the wrong hands, or your company’s reputation taking a hit. That might not be enough to consider a substantial loss, as the research shows that a small financial incentive had a meaningful impact on improving security policy compliance.

The last challenge covered is education on the subject of email security and training focused on detecting and reporting phishing emails and other forms of email attacks. Most organizations want their employees to spend their time at the workplace doing their job. But to perform well at their job, they may need workplace training, further education, or other means of improvement. That applies to cybersecurity as well. It is a broad subject, and since a large portion of work is online nowadays, proper education on how to defend yourself and the company is necessary. Email attacks are performed to a greater extent than ever before, and employees need to be able to detect when an email is a threat. It is recommended to have some kind of training courses periodically, to not only make sure that everyone has the knowledge required, but also has it on top of mind. Even though you might have all the training and experience, a mistake can still happen if you are not paying full attention.

5. Conclusion

This chapter concludes the whole thesis, the results, and other relevant parts.

Our research found that the most common security threats in email usage within organizations are phishing, APT attacks, and BEC. Guidelines for technical solutions that can secure email usage have been provided in this thesis. We highly recommend including these security measures to mitigate and defend against email attacks:

- BYOD security policies are essential when organizations allow employees to use their personal devices for work.
- Implementing robust access control measures in the organization's network is a highly effective strategy to mitigate APT attacks.
- The implementation of end-to-end web-based trusted email systems can greatly enhance email security within organizations and offer encryption and privacy.
- Implementing anti-spam software effectively reduces the influx of malicious emails, subsequently lowering the likelihood of employees falling prey to phishing attempts.
- Organizations are strongly advised to enhance employees' awareness regarding secure email practices and ensure that they consistently keep their knowledge about it up-to-date.

However, it is recommended that organizations customize their strategies based on their capabilities, including financial considerations.

If security implementations or policies make email usage too inconvenient, people will probably seek alternative methods of communication. It is important not to use a security policy that is too intricate, as it may discourage people from either using email or following the policy at all. It has also been proven that financial incentives improve policy compliance. Since email attacks constantly evolve, education and training on the subject are incredibly important. Training regularly also serves as an important reminder of email threats and what they look like. It can be difficult to detect phishing or other methods of attack, even if you are knowledgeable about the subject.

5.1 Future Research

For future research, it would be effective to experiment with a real world setting, to find trends in email security within organizations. This can provide a more detailed understanding and discover more countermeasures. In addition, integrating surveys from organizations can yield valuable insights into their current practices and the effectiveness of their email security measures.

This primary data can shed light on real-world challenges, successful strategies, and areas for improvement. It can also help identify any gaps between recommended guidelines and actual implementations in organizations.

References

Alton, L. A. (2022, June 17). Email remains the top communication tool for businesses – here's why. *The American Genius*. https://theamericangenius.com/business-news/email-remains-top-communication-tool-businesses/

Bann, L. L., Singh, M. M., & Samsudin, A. (2015). Trusted Security Policies for Tackling Advanced Persistent Threat via Spear Phishing in BYOD Environment. *Procedia Computer Science 72*, 129-136. https://doi.org/10.1016/j.procs.2015.12.113

Bell, D. E., & La Padula, L. J. (1976). *Secure Computer System: Unified Exposition and Multics Interpretation*. US Air Force. https://conferences.computer.org/sp/pdfs/early/bell76.pdf

Bhardwaj, A., Sapra, V., Kumar, A., Kumar, N., & Arthi, S. (2020). Why is phishing still successful? *Computer Fraud & Security, 2020*(9), 15-19. https://doi.org/10.1016/S1361-3723(20)30098-1

Bursztein, E., Oliveira, D. (2019, August 8). Understanding why phishing attacks are so effective and how to mitigate them [Blog post]. Retrieved from https://security.googleblog.com/2019/08/understanding-why-phishing-attacks-are.html

Cisco Security. (n.d.). *What is malware?* https://www.cisco.com/site/us/en/products/security/what-is-malware.html

Florida Center for Instructional Technology. (2009). *The Internet: Ideas, Activities, and Resources*. https://fcit.usf.edu/internet/chap5/chap5.htm

Ganacharya, T. (2020, March 20). Protecting against coronavirus themed phishing attacks [Blog post]. Retrieved from https://www.microsoft.com/en-us/security/blog/2020/03/20/protecting-against-coronavirus-themed-phishing-attacks/

Goel, S., Williams, K. J., Huang, J., & Warkentin, M. (2021). Can financial incentives help with the struggle for security policy compliance? *Information & Management, 60*(4), Article 103447. https://doi.org/10.1016/j.im.2021.103447

Haaster, J. V., Gevers, R., & Sprengers, M. (2016). *Cyber Guerilla*. Syngress.

IBM Security. (2022). *Cost of a Data Breach Report 2022*. IBM Security. https://www.ibm.com/downloads/cas/3R8N1DZJ

IBM Security. (n.d.). What is data breach? https://www.ibm.com/topics/data-breach

Imperva. (n.d.). *Phishing attacks*. https://www.imperva.com/learn/application-security/phishing-attack-scam/

Ismail, K. A., Singh, M. M., Mustaffa, N., Keikhosrokiani, P., & Zulkefli, Z. (2017). Security Strategies for Hindering Watering Hole Cyber Crime Attack. *Procedia Computer Science 124*, 656-663. https://doi.org/10.1016/j.procs.2017.12.202

Japan's IT Promotion Agency. (2023, March 29). *Top 10 Information Security Threats 2023*. https://www.ipa.go.jp/security/10threats/10threats2023.html

Lowe, D. (2020). *Networking For Dummies*. (12th ed.). For Dummies.

Microsoft. (n.d.). What is business email compromise (BEC)? https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email-compromise-bec

Oates, B. J. (2006). *Researching Information Systems and Computing* (1st ed.). Sage Publications Ltd.

Odogwu, C. (2022, January 13). What Is Email Security Policy and How Does It Work? [Blog Post]. https://www.makeuseof.com/what-is-email-security-policy/

Peltier, T. R. (2006). Social Engineering: Concepts and Solutions. *Information Systems Security, 15*(5), 13-21. https://doi.org/10.1201/1086.1065898X/46353.15.4.20060901/95427.3

Pratt, M. K. (2022, August). *Definition: cyber attack*. https://www.techtarget.com/searchsecurity/definition/cyber-attack

Sabir, M. Z., & Yousaf, M. (2018). Design and Implementation of an End-to-End Web based Trusted Email System. *Procedia Computer Science, 141,* 231-238. https://doi.org/10.1016/j.procs.2018.10.176

Silic, M., & Back, A. (2016). The dark side of social networking sites:Understanding phishing risks. *Computers in Human Behavior, 60,* 35-43. https://doi.org/10.1016/j.chb.2016.02.050

Simoiu, C., Zand, A., Thomas, K., Bursztein, E. (2020). Who is targeted by email-based phishing and malware? Measuring factors that differentiate risk. *IMC '20: Proceedings of the ACM Internet Measurement Conference,* 567-576. https://doi.org/10.1145/3419394.3423617

Sans Institute. (n.d.). *About SANS Institute.* https://www.sans.org/about/

Trend Micro. (n.d.). *Data Breach*. https://www.trendmicro.com/vinfo/us/security/definition/data-breach

Verizon. (2022). *2022 Data Breach Investigation Report*. Verizon. https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf

Washington University in St. Louis. (n.d.). *Confidentiality, Integrity, and Availability: The CIA Triad.* https://informationsecurity.wustl.edu/items/confidentiality-integrity-and-availability-the-cia-triad/

Appendices

Transcript of Interview 1

In this case the interviewee is Employee-1 (E1) that is mentioned in chapter 4.1:Interview results under chapter 4:Results

Interviewer: Our work is about how to secure email use in organizations so let me start with asking you how important email use is for you and your job?

Interviewee: But it's vital, it's the biggest part of the business because it's the main communication route. Both with customers and. But my co-workers.

Interviewer: Okay, okay. So, it's like all work is about first place email.

Interviewee: Yes, but even though we have system failures every one thing. We then have systems to keep track of customers and yes, but accounting systems for invoices. There are Teams for chatting though. Almost everything. Or all relationships with both customers and employees, there are parts that have taken place via email. It can be a victim or an agreement or as well as an agreement with 1 customer or a meeting's assignment or request. It goes by email so you would of course manage you would certainly do without as well. But at present, they rely on you to have access to email when you need to. And also to go back and look at, for example, old agreements that you have that you may not have saved elsewhere. Yes, you trust that it remains in the email.

Interviewer: Yes, I agree, emails are first contacts to create business and as you said to also communicate with employees well. We move on to the next question. Do you know what a phishing attack is?

Interviewee: Yes, if I understand correctly, for example, by pretending to be someone else, for example. For example, having with the bank is yes, but log in here to fill in your up to. Yes, it's like log in here and like this a fake page you phish for the information.

Interviewer: Yes, exactly. Yes, phishing is a huge area. There are many types of it, but how do you react when you receive an email like that?

Interviewee: Yes, it's hard to answer because you don't know if you. If you go for it, you don't know you've walked on it. But I always try. Yes, but I always check if I click on a link. Yes, what the link looks like and where it comes from. Now some kind of thing

happens or we use of course. Microsoft 365 they existed or whatever it's called? It's called Defender for 365. And it captures a lot. Both right and wrong, but I try to be restrictive and. If I'm unsure, it doesn't happen very often, but then I ask the person in question. What it is, what it will? Ok, that's really what I usually do, ask a control question, or get in touch.

Interviewer: Okay great, do you have some kind of reporting.

Interviewee: Yes, if I suspect it's phishing. Then I usually just right click in Outlook and take report junk mail and then I usually block the general sender.

Interviewer: Yes, exactly there is a feature in 365 to report phishing.
How often do you receive a phishing email, and does it end up in spam or does it go straight to the inbox?

Interviewee: We got one a week or so ago, but I think it was this Number what year it has. The security council that we use it on at the company that sends it out and it always slips through. But otherwise so. I think most of it is captured. Yes, it is extremely rare.

Interviewee: Okay, yes often I get or it happens maybe. 3-4 times a week that I get emails from some person. Where you notice that it is. Yes, but automatically translated and that they want something, that is, but you do not know if it is phishing or if it is just someone trying to market, for example that it was trained developers or that yes, but to seek contact.

Interviewer: Yes, it's a bit difficult for the present. So it is. It's the smarter and smarter way they write possible, so it's a bit of a challenge to know, but would you say that you then get as many phishing emails in your private email or in work email?

Interviewee: Privately, I have a Gmail that I have had for 15 and more than 15 years the same address. So it gets it. Yes, but. Quite a lot, but I think it's better to put it in spam.

Interviewer: It's Gmail then?

Interviewee: But that, I don't know or Outlook there, where I might not even see them, but I think I never get any. Because I have that role. So I have because I represent a company because I get it now or that there is someone who fakes being someone within the organization and wants me to do something. I never get that privately, that's where it is. There it is classic.

Interviewer: Okay, I see. What do you do if you receive an email from an address you do not recognize and you said that it either contacts the contact person or says to report it. But the question here is whether you use any type of encryption when you send mail or receive an email? Is there any encryption policy as well?

Interviewee: We have the wrong person to answer. I don't think we use them any more than that the traffic to the mail server is encrypted.

Interviewer: OK.

Interviewee: Yes, but I really don't know.

Interviewer: Because there are some tools that encrypt the whole possibility.

Interviewee: Yes yes yes no. We use that something like, well, no, we don't.

Interviewer: Okay because there are some tools that encrypt completely. Plus the traffic. In any case we move on to the next question: Do you usually use your mobile to get both jobs and. Private mail?

Interviewee: I check my phone.

Yes, I probably read and answer more on email, on mobile or on the computer actually.

Interviewer: OK. Mm, and now we will trust if your work email is linked in any social media, like Instagram, Facebook.

Interviewee: No, not at all, not.

Interviewer: Do you use software or webmail?

Interviewee: I use Outlook. Yes.

Interviewer: Okay, do you have any type of security policy installed in your phone? n.

Interviewee: Not to check the emails? I don't think so.

Interviewee: It's my old job or a previous employer had that, and it just did. People stopped using their emails on their mobile phones.

Interviewer: OK, so they couldn't access the emails?

Interviewee: Yes, but it had to check with VPN on the phone and it was buggy and reminders and stuff in the calendar. Which arrived too late or not at all. And yes. Yes, it certainly was a lot like this. It may be a safety layer, but it meant that people could not use the tool instead.

Interviewer: Okay, I see... Now we come to. Security policy, do you know if your computer or your mobile has any special security? Policy for the organization, that is.

Interviewee: The computer has it. I know what it looks like, I do not know exactly, but there we have one and we know that it is being reworked.

Interviewer: Oh well, okay.

Interviewee: Right now. The cell phone, I think, actually has none at all. I know it. Lies of course. On a separate Wi-Fi to the computer, such as the organization. Otherwise, I do not think we have it. Nor in, for example, because I think you can set a policy that you should have a certain level of security on Outlook. I do not think we have either. We have an MFA to sign in. But then that password is saved if you want and so it works until you change the password.

Interviewer: Okay, and then we'll come to another question then. Let's say someone has accidentally pressed phishing. Email, what happens then? Are there any type of restrictions too? Usage, i.e. an ordinary employee. Does it have any kind of limitations if you pressed a link?

Interviewee: I know it's us. Keep on watching now. For example, be a user or what you can do there. Own a computer for example. Partly, we have secured it, and partly you can not access the local if you do not have a VPN. Yes, so after all, you will not get local resources if you are out of the office, if you have not taken yes, if you are not inside the computer in sales. Yes, but you can't log in. On the local network, so to speak. Without having a VPN. And so it is, of course, but it still comes and then it is of course, then it has of course. MFA. To log in.

Interviewer: yes, let's say you're sitting here in the office, and you happened to open a link that has some script or something. Are there any limitations that your local computer or network will not affect the admin or others?

Interviewee: Yes, we have one like this. We have separate admin accounts because yes, I don't know what that's the right word, but before our tenant was Microsoft 365 environment with AD, we have separate admin accounts. So everyone who has administrator rights has separate accounts that you have to log in to just when you want to do something. These are not accounts that you can then sit and work in normal cases. Then there is. Resources both on the network, ie folders in the network or network drive and stuff like that. They are also very regulated. So that there are certain users who come or groups who access certain things. And it is. So then it has to find that person. Or the right person to access sensitive data or whatever we should call it. So that's right, right?

Interviewer: Isolated, you might say.

Interviewee: Yes, it is, but you can still make a mess of things because there is common information that all employees need to access so that, and you can of course do that. They will be that if you come in, but there are at least several layers of security, both in terms of. Permissions locally on the network which devices you can access. Then we have as I said before we have separate networks on. Yes, for computers and mobiles. We have yes to other connected gadgets. And certainly more too, which I don't know.

Interviewer: Do you have any kind of courses or training in security? So, the employee kind of knows how to behave when you get a phishing email like that

Interviewee: We have this one. The tool is called Number which is one. A tool to raise safety awareness. With our employees and it sends out. User specific training. That is. Yes, but depending on how you respond to the training and then it has simulated attacks and depending on how you act on them, so. Then you get. After all, tailored. Yes, new attacks and also training to make it yes, but so. Relevant as possible. Yes, that's right? What we have.

Interviewer: This is becoming more and more important and it kind of takes most of the security today, sort of.

But would you say that? The employees here are aware of how important it is not to press any link and that phishing is something that comes every constant, right?

Interviewee: But I think we've gotten better at it. I think it is, for example, obvious that we talk about it, but also that we run these trainings. Because even if you know about it, I think so. It's. Yes, it is. It's easy to make mistakes at some point. You need to be reminded even those who work with IT security can happen to make mistakes, for example, you are about to enter some important meeting and you should just yes, just want to check what it is or that you are in the kitchen at home cooking with the children and reading emails or yes, but and what others can do something for when everyone sits quietly at the computer and receives an email if you Don't be stressed about anything else. Then I think the awareness is quite high.

Interviewer: Good, good, I don't really have another question. But do you want to add anything or comment on anything?

Interviewee: So, but I thought about that thing with just this kind of security and that we kind of don't talk about, but that some know some do and. For example, I use Outlook for all mail on the phone and that's because then it can turn on face ID to open Outlook and then it's safer. Then you also get double security so if someone comes across your phone and it is unlocked, if you happen to know if someone takes it out of your pocket or not, read it or whatever it is then at least it is one more step. And you have to get past. And it's those little ones. Small things that I think can make a big difference because it is. As I am as an employer and as an organization, you want it to be as effective as possible. It should be as easy as possible for employees. At the same time, you want it to be as secure as possible and then it is, for example, face-id that. Or a pin code or whatever it is that makes it a little harder. And the same thing. I think some of that too. Examples here of the organization are good at doing small simple things like locking the computer when you walk away from it while some. They don't do it because they don't have that safety mindset and it's usually the easiest way to get around.

Interviewer: That's absolutely the most important thing and I guess it has things that come with security courses to warn that you have to lock the computer etc.

Interviewee: Yes, I know, I know what an old employer of mine had at the time. We had been to an office at. Yes, there were multi-storey buildings and so it was on us. I went out

and went for a walk around the office and that was it. There was someone who had left their computer unlocked and the window was open.

Interviewer: Yes, you have all the risks that exist in the world.

Interviewee: However, a security employee is so that you have to be security classified to even work there? Then it is a huge risk and then it does not matter which ones?

Interviewer: Yes, I agree.

Interviewee: And it's also easy to see between your fingers because it can also be like this in the office, no one wants me bad, so why would anyone do it on the computer? But you never know about anyone. It's easy. Should you then slip in?

Interviewer: Well, now we got into Social Engineering a bit.

Interviewee: Yes, yes, but. Is it?

Interviewer: Well, you should trust all but at the same time when it comes to security, you shouldn't do it even if your colleague. For now, we're talking, well, let's say we have an eye on security and IT but the finance department, they don't have as much control and that increases the risk.

Interviewee: And they can also let someone in and only I'm going to meet this person because now there is even a name on the door? And so, the guest himself is waiting here?

Interviewer: Thank you very much for the interview, it was rewarding!

Interviewee: Thank you and good luck.

Transcript of Interview 2

In this case the interviewee is Employee-2 (E2) that is mentioned in chapter 4.1:Interview results under chapter 4:Results

Interviewer: How important is email use to you and your job?

Interviewee: E-mail is very important for me and my job. This is the communication channel we use to interact with our colleagues, collaborate with teams and also communicate with our customers. It is through email that we share important information and discuss projects.

Interviewer: Understand, so would you say email plays a big role in your work?

Interviewee: Yes, absolutely. Although we have other internal tools for collaboration and project management, such as Teams, email is still a fundamental part of our work process. We use it to send formal messages, report on progress, follow up with customers, and handle important business-related cases.

Interviewer: Good. Now we move on to the next question. Can you explain what a phishing attack is?

Me: Absolutely. A phishing attack is when an unauthorized person tries to obtain sensitive information by impersonating a trusted party, such as a bank, colleague or company.

Interviewer: Thank you for your explanation. How would you react if you received a phishing email?

Interviewee: When I receive a suspicious email that may be a phishing attack, I am always cautious and take the following actions. Firstly, I carefully check the sender's email to see if it seems legitimate. I also carefully review the content of the email and look for any irregularities, such as poor grammar, spelling mistakes, or unusual behavior. If something seems suspicious or if the email asks me to click on a link or give out personal information, I never do it. Instead, I contact our IT department to report it.

Interviewer: That sounds wise and absolutely right. Do you know if you use some form of encryption when sending emails? If so, which one?

Interviewee: No, not to my knowledge anyway.

Interviewer: Do you use a work computer or personal computer to read your work emails?

Interviewee: Work on a computer only.
Interviewer: Do you use your personal or work phone at work, do you use your work phone as a private phone as well?
Interviewee: I mainly use work phones to communicate and perform tasks.

Interviewer: Do you know what webmail or email software is?

Interviewee: Yes, webmail is a service that allows users to access and manage their email through a web browser while email software on the other side is an application that is installed on a computer or device to manage emails.

Interviewer: Do you use webmail or email software to access your email?

Interviewee: We use a combination of webmail and email software to access and manage our emails. Some prefer to use web email when they are away from the office or on the move, while others use email software to organize their email and access it offline.

Interviewer: Can you name the webmail/software you use to access email?

Interviewee: We use Microsoft Outlook

Interviewer: Okay, but do you usually use VPN to read your emails?

Interviewee: No, not when I read emails, I can read it without a VPN, but if I want to access any data that is in the company, I connect via VPN.

Interviewer: I see, do you know if your organization follows any kind of security policy when it comes to email usage?

Interviewee: I dare not answer that, I know there is a policy but what does it mean, I have no idea about it.

Interviewer: I understand, but let's say someone accidentally hit a phishing link, what's going to happen do you think?

Interviewee: What I do know is that we have limitations, and the network is divided depending on the level and such, so I would probably say that it will not affect the entire organization but will of course affect some anyway.

Interviewer: Okay and the part that was affected then, how do you deal with that?

Interviewee: I guess it shuts down and scans altogether, it depends on how dangerous the link is too.

Interviewer: Yes exactly, but would you say that your colleagues have the skills to detect a phishing attack?

Interviewee: Yes, so we have a safety course that we usually get 1-2 times a month to increase awareness of how you react or what the risks are, so I would probably say that yes, most people have a background on what to do and so on.

Interviewer: Thank you very much for your time!