Re-assessing the effectiveness perimeter security & exploring attack surfaces at the Port of Rotterdam

University of Twente

Capstone Project ATLAS

Author

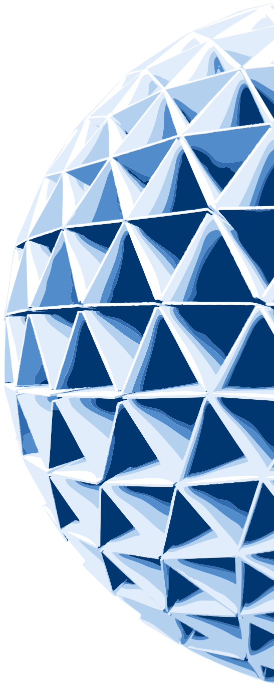
Jitka Bojorge-Alvarez

Supervisors

Daily supervisor: Elmar Lecher

ATLAS supervisor: Martin Streng

UT supervisor: Erik Tews



12-08-2022

ACKNOWLEDGEMENTS

With the completion of my capstone project, I will have obtained my bachelor's degree at ATLAS. I am very grateful for ATLAS for allowing me to explore all the different fields and domains that I wanted to be able to find my passion.

I would now like to thank all my supervisors individually:

Thank you Elmar Lecher for increasing my passion for information security even more and giving me the opportunity to do an internship at the Port of Rotterdam. This internship has taught me what it means to be a security officer. Thank you for always helping me out and being enthusiastic about my thesis topic.

Next, I want to thank Martin Streng for guiding me when I got stuck and helping me into the right direction. Your patience and positive attitude are very much appreciated.

Lastly, I want to thank Erik Tews for helping me out with the academic parts of writing my thesis, and also being patient with me when it was unclear on how to proceed and giving me the confidence to just start the writing process.

`

ABSTRACT

State-of-the-art literature suggests that traditional perimeter security is not applicable to the current network infrastructure. Reasons include the migration of data to cloud service providers and employees increasingly working from home, making it difficult to place a perimeter. The goal of this thesis is to get a practical understanding of lesser-known attack surfaces and to measure the compliancy level of employees on the current perimeter security guidelines at the Port of Rotterdam, scoped down to the IT department. This was done in the form of a questionnaire and interviews. Results from the questionnaire show that a significant number of employees avoid using the company laptop or using a VPN when at work, both of which are common policies. The main reasons for doing so are to improve their ability to work, not knowing these policies, and forgetting such policies. The interviews show that there is a need for improved communication and a wish for active involvement of security officers within their teams. Additionally, not all data from every team interviewed goes through the broker network. In conclusion, this study took a critical look at the current security policies and proposes among other best practices the adaptation of a zero-trust network.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

Hackers are constantly looking for new ways to exploit vulnerabilities of organisations and companies. Cyber-attacks can do serious damage to companies and the risk is getting higher; the number of cyber-attacks have increased by 15.1% in 2021 compared to 2020 (Brooks, 2021). Furthermore, it is estimated that in 2014 cybercrime did between 345 and 445 billion dollars in damages around the world (Lewis, 2018). In 2018 this estimate rose to 445 to 600 billion. It is likely that this number has increased in 2022. To mitigate this, organisations are constantly creating new best practises, methods, and concepts to protect their companies from these exploitations. However, technology is developing fast, which can make it difficult to keep track of what is still usable and what is outdated. This necessity for constant revision makes it important to keep being critical on the current best practises in the field of information security.

1.1 Problem Statement

The concept of perimeter security has been around for twenty years now with books and academic papers dating back to the 2000's, such as 'Network Perimeter Security' by Riggs (2003). However, technology is advancing rapidly and has become more essential to us now than twenty years ago. Nowadays, most companies are completely dependent on their digital infrastructure to be able to do their work. But not only do they have to be dependent on their own infrastructure: since the internet has become so interconnected they are also dependent on other companies as they often outsource services such as using Microsoft Teams for intercommunication.

The traditional perimeter security concept is often still implemented to protect companies against cyber threats: closely monitor what goes in- and outside of your organization's network by using firewalls and logging suspicious data traffic based on this. Perimeter security supports the idea that everything physically (such as computers) on your company's premises is safe (assuming that the laptop has not been compromised), and queries from somewhere outside the company's ground are not. This thus results in a virtual barrier in the form of a firewall along the companies ground to protect it from attacks.

However, since the time perimeter security came into existence, it is not so clear anymore what lies inside and outside your network. Due to the pandemic people have been forced to work from home using VPNs to connect to their company's network, and companies are no longer storing data on their companies ground as cloud service providers are often cheaper. Whereas the attack surface twenty years ago seemed quite straightforward, it has now become blurrier. Where should one place the digital perimeter if there still is one?

The number of cyber-attacks have also increased, with larger companies potentially facing monetary, data, and image losses if an attack succeeds. It is therefore important for companies to keep improving and challenging their security practices, and possibly switching to other ways to secure themselves. For this capstone project we will take a critical look at perimeter security and the current attack surface of the Port of Rotterdam as it can shed more insight on the effectiveness of perimeter security and help make companies more aware of potential weaknesses in their security practices.

1.2 Research gap

Research has been done on perimeter security, but this research has been limited to a more theoretical basis. No research studies so far have been found on using perimeter security at a company and its effectiveness in practice. Lately, more academic research is questioning the approach of perimeter security and even suggesting other frameworks. For instance, instead of trusting everyone that passes the firewall, no one is trusted. This is the main idea of the zero trust model, which comes from another security approach called Software-Defined Perimeter which argues that one should limit the perimeter down to the server (Kumar et al., 2017).

A similar thing can be said about attack surface monitoring: research has been done on a theoretical level, but this attack surface primarily focuses on the software aspect. However, one effort has been made to connect this attack surface on a network level (Zhang et al., 2018). As for perimeter security, an attack surface is probably more difficult to map when considering all the services that a company might use. Are third parties (e.g. external brokers) to be included? Again, it would be useful to explore such a possible gap in the knowledge on attack surfaces at the Port of Rotterdam.

1.3 Research objective

The objective of this thesis is to research the effectiveness of perimeter security at the Port of Rotterdam and whether it is becoming outdated or if it is still a valid security best practise. By also looking into the awareness of the security team on the attack surface of teams inside the Port of Rotterdam and external companies, we can also draw a conclusion on how/if perimeter security still fits in this attack surface in a business environment. Lastly, this thesis will aid in improving the gap between theory and practice regarding network security at the Port of Rotterdam and can reshape security best practises within organizations in general.

1.4 Research scope

This thesis has been written whilst being was an intern at the Port of Rotterdam in the IT department in the security team. ~~S~~ince it is not within the scope of this capstone project to consider the entire company, the focus will be on the IT department.

1.5 Research questions

The following questions and sub questions were defined based on the research objective:

RQ 1: What is the effectiveness of perimeter security at the IT department of the Port of Rotterdam?

RQ 2: What are theoretical unknown attack surfaces at the Port of Rotterdam, and do they fall within their already set perimeter/firewall?

> RQ 2.1: If these attack surfaces are not covered by the firewall, how else should you monitor all the traffic (what are best practices for cyber security monitoring)?

1.6 Research approach

This capstone project starts with a literature review to investigate the current state-of-the-art regarding perimeter security and attack surface monitoring. The goal of this literary analysis is to get an understanding on how perimeter security is defined, the current discourse, and possible other types of security. An analysis on attack surface monitoring is done to find a clear definition to guide the interviews, to understand what an attack surface entails, and where the concept came from.

After this literary analysis, expert interviews are performed. Two of these interviews contain an extra part which contain questions about perimeter security and in what possible ways it could disrupt their work. This is done to help define hypotheses that could be an answer the RQ 1 and will be able to help structure the questionnaire.

To be able to find possible attack surfaces or ways to get a better understanding of the attack surface at the Port of Rotterdam interviews are performed. By doing this, RQ2 can be answered, and opinions on best practises from the interviews with experts in different fields (e.g. broker system engineer, data engineer, information security officer, infrastructure engineer) can answer RQ 2.1.

In addition to the interviews, a questionnaire will be distributed within the IT department about their experience regarding the current broker system (perimeter security). By understanding how the broker system plays a role in their way of working it is possible to get an answer to the RQ 1 on the effectiveness of perimeter security.

1.7 Structure of thesis

SECTION 2: **LITERATURE RESEARCH**	Literary analysis on the state-of the-art on attack surface monitoring and perimeter security
SECTION 3: **METHODOLOGY**	Method section explains the reasoning behind the usage of qualitative and quantitative research of this capstone
SECTION 4: RESULTS	Results of the interviews & questionnaire
SECTION 5: DISCUSSION	Discussion/Reflection on the findings and implications
SECTION 6: CONCLUSION	A conclusion will be given with an additional future outlook on possible future research

Table 1: structure of thesis

2 LITERATURE REVIEW

In this second chapter the concepts of perimeter security and attack surface monitoring are defined to create to align views of what both concepts mean. Defining what traditional perimeter security was meant to do twenty years ago and comparing this to more state-of-the-art papers will help get an insight in answering RQ 1. In literature, attack surface monitoring seems to have different definitions. Therefore, papers will be compared to find a suitable definition on what an attack surface is. This will help guide the interviewees in answering the interview questions.

2.1 Perimeter security

2.1.1 Background

Security has not been a priority in network design when first developed (Daya, 2013). If a company wants to secure their entire network, this does not only entail computers at the end-points but it also includes data in transmission (Daya, 2013). This data in transmission can be seen as the integrity of data, which is part of the security CIA triad. This CIA triad has three components which have to be considered: Confidentiality, Integrity, and Availability (CIA). The purpose of this CIA triad is to guide companies improve security. When implementing security policies, these three pillars have to be protected. Additionally, when wanting to make sure right people have access to data the concept AAA security (Authentication, Authorization, and Auditing) is also used. Understanding these pillars are useful for determining what secure means and by which concepts to measure it. However, when wanting to secure data and monitor who gets access to it, it quickly becomes more complicated.

Concept	Meaning
Confidentiality	Making sure only the right people have access to the data and no one else
Integrity	Making sure that the data has not been changed/altered in any way when arriving at the receiver
Availability	Ensuring that the data and functionality is available to the user
Authentication	Identifying the user and making sure they are who they claim (Mylonas, 2018)

Concept	Meaning
Authorization	Used to make sure access to data, resources, and systems is according to your rights
Auditing/Accounting	Can be seen as logging data and user information such as consumed resources by the user (Mylonas, 2018)

Table 2: basic security principles

2.1.2 Firewalls

Before moving on to any further analysis of perimeter security, it is essential to understand what a firewall is. This is because a firewall acts as a perimeter for an internal network (Rusere & Ngassam, 2020), so the concepts are closely linked together. A firewall can be defined as a digital barrier to prevent unauthorized people from gaining access to the private network (Göksel, 2019). This is done by blocking untrusted external traffic. If an incoming data packet does not match the rules, it is dropped (Kumar et al., 2017). With the increasing complexity of networks and enterprises which are continuously growing, firewalls have developed more complex rules. Additionally, there can be multiple layers of firewall functionalities on different layers of the OSI network (for example the network level based, protocol level based, application level based). In this case, there could be a trusted zone, semi-trusted zone, and untrusted zone. Before moving onto a zone that needs a higher amount of trust, a firewall needs to be passed. This firewall among other systems seen in figure 1 acts as the network perimeter.

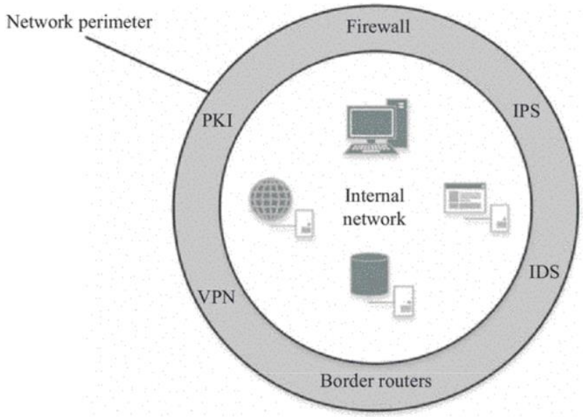


Figure 1: simplified conceptual perimeter structure (Kumar et al., 2017, p.153)

2.1.3 Other parts that can make up perimeter

As seen from figure 1, the perimeter may further consist of other components. One of these is a virtual private network (VPN). A VPN enables a secure connection between two systems. To be more specific, a VPN can protect data in transit between two endpoints (Kumar et al., 2017). In companies, VPNs are used by employees working remotely to be able to connect to the company's network with a secure connection. However, if an attacker is able to compromise the system (see Table 2) of an employee using a VPN at one of the end-points, the VPN will grant the attacker access to the network of the company (Kumar et al., 2017). Public Key Infrastructure (PKI) enable the verification of encryption keys that allow users to communicate using encryption keys (Kumar et al., 2017). Additionally, intrusion detection systems (IDS) and intrusion prevention systems (IDS) may be used. These systems try to monitor behaviour across a network to find unusual patterns that could signify malicious intent (Ledesma, 2022).

2.1.4 Recent developments

In the early stages of perimeter security in the 2000s, companies still stored all data inside their network. Additionally, employees could access the organizations' network only when at work. This made it straightforward to employ a firewall, as the (digital) border was on the company's ground itself. Now twenty years later, the internet has evolved and has become more interconnected and organizations often outsources services/tasks to other companies. Since the start of the pandemic, employees found them working from home using a VPN to enter their companies' network. Another new trend in the last few years has been the usage of cloud services. Large companies are moving their data to the cloud, meaning that it is no longer stored on the company's premises. This results in a separation between the owners of the data (the organization) and their data (Kumar et al., 2017). Since data is now stored at the cloud service provider, the definition of perimeter security is no longer applicable. However, data can still be behind the perimeter of the cloud service provider, so data is not automatically unprotected. Reasons for choosing cloud service providers include an increase in speed of projects and software development, a reduction in maintenance costs and because it is easier in terms of complexity and up/downscaling (Kumar et al., 2017). Due to this 'blurring' effect on the edges of the perimeter, researchers are starting to question the effectiveness of perimeter security and relying mostly on (Kumar et al., 2019; Mukherjee, 2020; Ullrich et al., 2016). Moving data to the cloud can add extra vulnerabilities and a lack of access management (Rusere et al., 2020).

Perimeter security relies on the fact that everyone inside the network has no bad intentions. However, there only has to be one weakness in the firewall for a threat actor to gain access. Additionally, a little over 50%

of cyber attacks come from insiders (Leong, 2017). This suggests that you should not trust insiders in your network.

2.1.5 Useful analogies

Some useful analogies are given by DelBene et al. (2019) which illustrate some of the current issues with perimeter security. The first analogy they give is that perimeter security can quickly turn into a game of ‘whack-a-mole’: since networks are continuously expanding, firewalls must constantly be adjusted to be able to effectively filter network traffic. The second analogy given by DelBene et al. (2019) compares a network to a house. In a house, you do not lock every door because you probably know everyone that enters the house. In an apartment complex however, every apartment has its own lock, and you would not leave all doors unlocked except the entrance building. Whereas a network some 20 years ago may have look like a house, nowadays it looks more like an apartment complex. Here, different locks must be implemented for each apartment.

2.1.6 Zero Trust

In the last few years, some researchers have created a new approach to solve this issue: zero trust architecture. Zero trust comes from another security approach called ‘Software Defined Perimeter’ (SDP) (Kumar et al. 2017). The basic idea of a SDP is to narrow the perimeter down to the server. They argue that with the development of BYOD (Bring your own device, which is similar to the ‘working from home’), virtualization technology and cloud computing, traditional perimeter security is not sufficient as there are ‘too many moving devices inside the perimeter and applications and data migrating outside the perimeter for a traditional fixed perimeter to be successful’ (Kumar et al., 2017, p.156). Based on this idea, the zero trust model came to be, which could be seen as the opposite of perimeter security: trust is no longer based on the location inside a company's perimeter but instead there should be no trust at all (Mukherjee, 2020). As a result, the confidentiality, authentication, and authorization improve (see Table 2). Rusere and Ngassam (2020) also mention the usage of zero trust as a way to increase security within an organization. Based on the house and apartment analogy from the previous paragraph, different locks can be translated into a segmentation of the network. By doing this, emphasis is no longer of the perimeter, but on the ‘discrete applications and services within a network’ allowing specific access controls (DelBene et al., 2019). This way of building security around services as opposed to the entire network can be defined as ‘microsegmentation’ (DelBene et al., 2019). By doing this, authorization improves since microsegmentation makes it easier to decide what rights should be given to the user. Zero trust Architecture has now also been adapted by the National Institute of Standards and Technology. In a paper written by this institute by Rose et al. (2020), basic zero trust architecture should rely on the principles in table 3. These principles cover the security principles defined in Table 2.

Nr. of principle	Principle
1	“All data sources and computing services are considered resources”
2	“All communication is secured regardless of network location”
3	“Access to individual enterprise resources is granted on a per-session basis”
4	“Access to resources is determined by dynamic policy” Additionally, least privilege principle enforced.
5	“The enterprise monitors and measures the integrity and security posture of all owned and associated assets”
6	“All resource authentication and authorization are dynamic and strictly enforced before access is allowed”
7	“The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture”

Table 3: zero trust architecture principles based on NIST guidelines by Rose et al. (2020), p. 6-7

A simplified three step plan to incorporate zero trust is given by DelBene et al. (2019). These are to first verify the user, then verify the device, and lastly verify access privileges. Steps one and two are part of the authentication process, while the last step requires authorization (see Table 2).

Although zero trust seems to be favoured in literature, perimeter security can still serve a purpose as a first line of defence (DelBene et al., 2019). However, companies should no longer be reliant on it. Meyer (2019) adds that perhaps perimeter security is not becoming obsolete, but that instead our idea of what perimeter security is has to change.

2.2 Attack surface

As explained in the previous part, the network perimeter is getting more complex. The seventh zero trust principle in Table 3 states that a company should collect as much information about their assets, infrastructure, and communications as possible. One way of getting a better understanding on these assets is by means of attack surface monitoring.

Some of the same reasons that make the concept of the perimeter blurrier also make the attack surface blurrier. Companies are increasingly outsourcing services to other companies, making an attack surface more fluid. To determine which parts fall under the attack surface of a company, a clear definition must be formulated.

2.2.1 defining attack surface

The concept of attack surfaces is used in many slightly different ways. Originally, attack surface monitoring came into existence as a way to measure a software's degree of security from the perspective of entry and exit points, channels, and untrusted data items (Zhang et al. 2018). In order to create a more general definition, a systematic literature review was performed by Theisen et al. (2018). After looking at 644 scientific papers, they defined six themes among which the term 'attack surface' was used. Applicable to this thesis is the term 'Adversaries', which defines an attack surface by '*the union of all possible ways an attacker could cause damage to a system'* (Theisen et al., 2018, p. 99). The most common definition was 'The attack surface is the methods of implementation, data channels, and data present in the system, with no specific attack features mentioned' (Theisen et al., 2019, p. 99), however, this is mostly a programming-centric definition, and in the case of this thesis we are also looking at the attack surface on a network level as well as from the point of view of an attacker and not from a neutral standpoint. Creating an overview of your attack surface will satisfy the seventh zero trust principle (Table 3) and improve the auditing AAA principle (Table 2), which is why attack surface should be monitored and mapped. As unknown vulnerabilities are difficult to predict, researching the 'unknown unknowns' can turn into an ambitious project, the concept of the attack surface could pose as a solution. This is because mapping an attack surface is done by looking at intrinsic properties, independently from external factors such as disclosure of vulnerabilities (Manadhata et al., 2010).

2.2.2 Mapping/monitoring attack surface

A first step to mapping an attack surface is to use port scanning (Everson & Cheng, 2020) as open ports mean that the network is accepting connections, which could be used as a way in by attackers. By doing this you can only get so far but unfortunately there is a lack of automated and mature tools for mapping attack surfaces (Zhang et al., 2018). The Open Web Application Security Project (OWASP) organization provides a general list of what an attack surface contains, which includes among other things: login/authentication entry points, admin interfaces, inquiries and search functions, business workflows, and APIs. Mistry (2022) adds more items to this list including laptops and PCs, IoT endpoints, websites, services, cloud services, and supply chain infrastructure and services. In a report from TrendMicro in 2022 among 6000 IT security decision makers, they estimate that they have insight in around 62% of their attack surface. With 40% still possibly unknown, it becomes clear that research done in this area is beneficial to improve security.

3 METHODS

This section is dedicated to explaining the chosen research methods and the reason behind them. The sections will be divided by participants, methods, design, and procedure.

3.1 Participants

All participants in the questionnaire are employees at the IT department of the Port of Rotterdam. These employees can either work as an intern or extern as long as they are working within one of the teams in IT. In total, the IT department contains 122 people, out of which 61 filled in the survey. This gives a response rate of fifty percent. In Table 5 the ratio of respondents and their job type is given. Twelve people filled in the 'other' option: 1 Business consultant/project manager, another project manager, 2 development professionals, 4 product owners/leads, 1 service & contract manager, 1 software engineer, and 2 advisors. The project managers and the service & contract manager were all added to the manager job type. For ease of data analysis, the software engineer was added to the data engineer count.

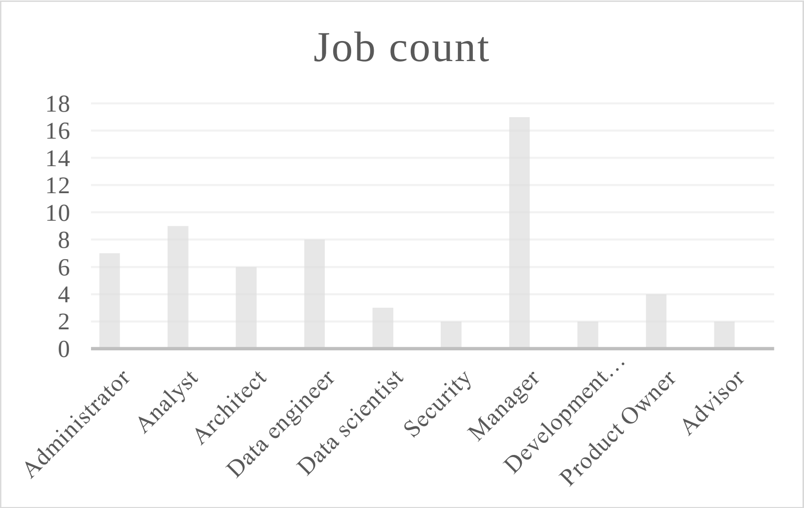


Figure 2: job ratio among respondents

Participants in the interviews are also employees at the IT department. In addition to these interviewees, employees from external companies who deliver security services to the Port of Rotterdam are interviewed as well. Participants in the interviews are chosen based on creating a diverse set of teams interviewed and relevance of service. This is done to get a wider range of answers in the questionnaire. Interviewees are furthermore chosen on perceived knowledge on security related subjects by the security team. In total, twelve participants were contacted for this interview, but in the end only ten responded. For a complete overview of the different experts of the teams interviewed, see the table section in the Appendix.

3.2 Materials

The questionnaire was made in Microsoft Forms as it is the preferred way of the Port of Rotterdam of handling surveys. This questionnaire contains nine questions. The questionnaire is designed to measure the attitude of employees on perimeter security and to measure the compliancy level of employees on following the broker system guidelines and policies. See the Appendix for the complete list of questionnaire items.

The online interviews were performed in Microsoft Teams as that is the main way of communication within the Port of Rotterdam. On site interviews were held at the office of the Port of Rotterdam for convenience of the interviewees. These interviews were recorded using a phone. Two of the interviews contain an extra part about the broker firewall which is designed to qualitatively measure the opinion on perimeter security and to get an understanding on what policies are not followed and why. These results are then incorporated into the questionnaire. The rest of the interviews are designed to explore possible unknown attack surfaces and security best practises.

3.3 Design

3.3.1 Questionnaire

An overview of the entire survey in Microsoft Forms is given in the Appendix.

The survey starts off with a general introduction to the topic and an introduction of the researcher. It is made clear that participation is voluntary, results are processed anonymously, and that data will be deleted after completion of the thesis. After actively clicking ‘I consent’, the survey continues to the next question. Otherwise, the participant will go directly to the end of the questionnaire and is thanked for their participation. Q2 is a multiple-choice question to ask about the best fitting job description. Sliding scales are used for Q3 to Q5 to get a generalizable view of how well they think participants know the security guidelines, how much they feel these security guidelines enable them to do their work, and how much they feel like these guidelines restrict their work. Q6 is a ‘yes’ or ‘no’ question. The term ‘in the last twelve months’ is added to make sure that data obtained is still up to date with current guidelines and policies. Q7 and Q8 are both multiple choice questions where multiple answer may apply. Q9 is a multiple-choice question. Lastly, Q10 was an open-ended question which allowed the participant to add any remarks about the survey.

Q2, Q7 and Q8 all contain an ‘other’ option to explore other possibilities. Furthermore, in case of multiple-choice Q7 and Q8 the order of options is randomized to avoid bias.

All questions are mandatory, except for Q7 and Q8, which only have to be answered in the answer to the previous question is ‘yes’ and Q10 on if there are any final remarks on the survey.

3.3.2 Variables

A dependent variable in this study is the job description. The technical skill level needed for the job might influence the attitudes on the security guidelines and policies, which is an independent variable.

The job description might also influence the other independent variables which are the compliancy level of employees and the reasons for this compliancy level.

3.3.3 Interviews

All interviews are designed with the same structure. A distinction is made between internal employees, external employees from other companies and employees from the security team, as some questions are not applicable to each group. Two of the interviews contain some extra exploratory questions. See the Appendix for all interview questions.

All interviews contain around ten open ended questions. To avoid misconceptions, a baseline among all interviewees is established by them to give their definition of an attack surface. The *adversaries* definition from Theisen et al. (2018) found in the literature research is used for this.

3.4 Procedure

Before sending out the questionnaire, the two interviews containing an extra part were performed. Answers to this extra part were then incorporated into the survey. The questionnaire was emailed to the collective IT email address to reach everyone in the department. A few days later, a manager sent a reminder to this same collective IT email address to increase the response rate.

Interviewees were contacted through email and Microsoft Teams. Before the start of the interview, interviewees were asked for consent of recording the interview. After the interview, participants were asked if they had any further remarks and told they could contact me if they had any additions. Lastly they were thanked for their time and participation. In the end all interviews were recorded except for one participant.

Data collection of the survey lasted two weeks, and interviews were also done within a time frame of two weeks. The questionnaire took roughly five minutes to complete on average and interviews lasted around twenty minutes on average.

3.5 Data analysis

For questions two to five that have an interval scale, the median and mean are analysed. Data from the questionnaire is analysed in excel. Cross tabulations will be used on the quantitative results to distinguish results from different job subgroups. Open answers in the ‘other’ multiple choice section will be compared to account for possible similarities. Additionally, results will be put into different charts to make interpretation of the data easier.

Interviews are recorded. All interview questions are asked in English but respondents could answer either in English or Dutch. In total, eight interviews were recorded in Dutch and the remaining two in English. After each interview notes are made and common themes are identified for later analysis. After completion of all interviews, the interviews will be rewatched. The interviews are not fully transcribed due to time limitations. During this rewatching of the interviews, notes will be taken and different themes are written down and compared to the common themes in the other interviews to look for similarities and differences.

Hypotheses

Hypotheses are derived from two interviews of experts in data engineering, from personal impressions from working in the IT department for three months, and talking to a security officer in the security team.

Perimeter security

H1: Employees working in the field of data science/engineering are most likely to not follow the rules

H2: Data scientists/engineers will also be most likely to actively find ways to work around the broker system as they have the most computer knowledge

H3: The most common ways people are avoiding rules are by using a private laptop instead of the company laptop, and not always using a VPN

Attack surface

H4: Attack surfaces outside of the company can have a significant impact on the Port of Rotterdam

H5: Interviewees wish to be more aware of attack surface mapping, but do not know their entire attack surface

H6: Communication between Port of Rotterdam and other companies on possible attack surfaces and their impact could be improved

H7: Port of Rotterdam has more understanding of attack surfaces within the Port of Rotterdam than outside the Port of Rotterdam

4 RESULTS

General

Out of these sixty-one respondents who filled in the survey, one participant did not consent, hence sixty responses have been processed in this analysis. For tables with the results from question three to five, see the Appendix. In total, ten interviews have been conducted, out of which nine gave permission for recording of the data. For the other participant notes were taken during the interview.

Data from the subgroup data engineers/scientists will often be compared to the total data of all respondents. This subgroup contains the seven data engineers, three data scientists, and one software engineer. Every time the subgroup data engineers/scientists is mentioned, this specific group is meant unless specified otherwise.

RQ1: What is the effectiveness of perimeter security?

The first research question can be answered using the results from the questionnaire.

To start, the distribution of the different jobs can be found in the method section in the participant paragraph.

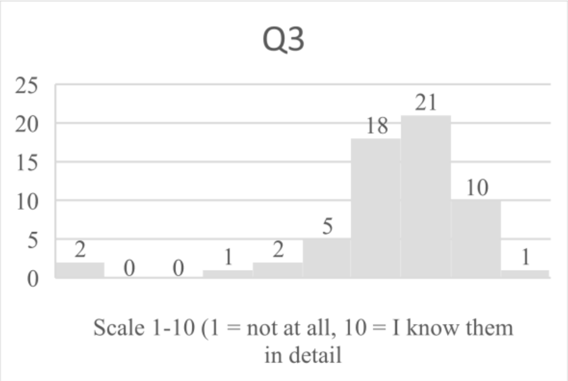


Figure 3: mean Q3

As can be seen from Figure 3, the rules are quite well known by all respondents. Among all respondents, the mean ends up at a 7.3 on a scale of one to ten. This is useful information as it means that they will better be able to answer the following questions in the questionnaire.

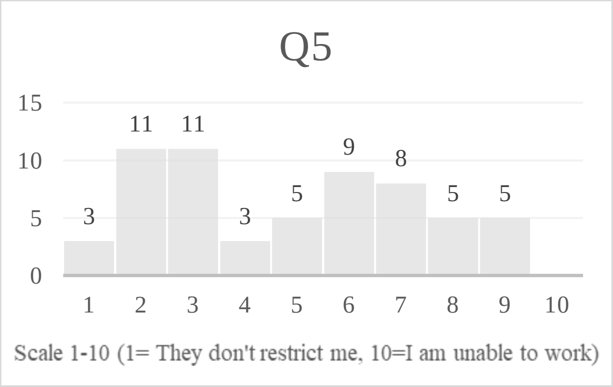


Figure 4: mean Q5

An interesting distribution here is the one from Q5. As you can see, opinions are varied across the scale. Almost half of the respondents (count = 27) give a score of six or higher, meaning that half of the respondents think that the rules are on the restrictive side.

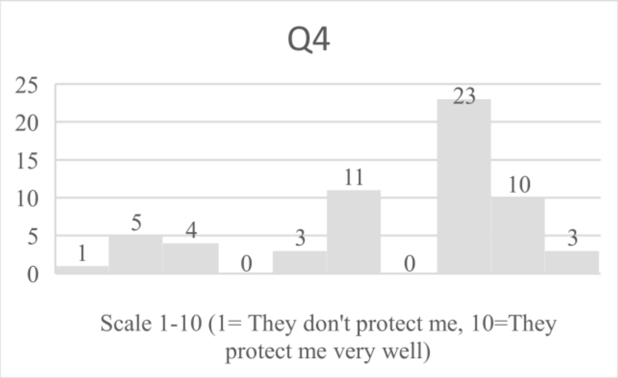


Figure 5: mean Q4

When calculating the averages, Q4 gives a mean of 7.4. However, this mean is more than two whole points higher than the mean of the data engineers/scientists, which ends up at a 5.1. This means that data engineers/scientists tend to believe that the current guidelines and policies do not make their work more secure. In addition, the mean to Q5 ends up at a 4.8, while the subgroup data engineers/scientists had an average mean of 5.4. Interestingly, analysts had a mean of 6.4, and the subgroup containing *only* the seven data engineers gave a score of 6.4. One would think that with tighter rules, employees would think that they become more secured. This does not seem to be the case for data engineers.

For Q6, one third (35%, count = 21) of respondents say there have been security guidelines that they did not follow in the last twelve months. This ratio becomes higher when only considering the subgroup data engineers/scientists. Of this dataset, 82% answered yes to this question.

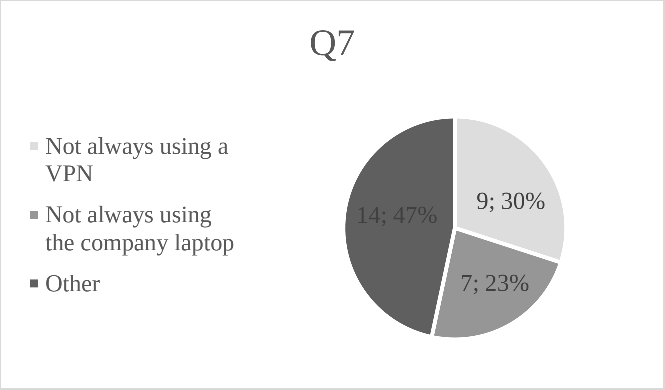


Figure 6: ratio Q7

Twenty-four participants filled in Q7. This is interesting, as three participants apparently answered ‘no’ to Q6 but still gave an answer to Q7. This means that the percentage of Q6 could be even higher. For clarity, this is not taken into account for further data analysis for Q6.

Participants could select multiple options; hence thirty responses have been collected and analysed. Although ‘other’ was chosen fourteen times, no overarching themes could be identified. Some of these other reasons included: ‘not locking laptop when going to get tea’, ‘not sharing personal data via mail’, ‘retrieving passwords in a non-compliant way’, ‘forwarding emails with attachments because unable to download them in webclient’, and ‘bypassing route tables on Azure to avoid broker network’. So the most common rule is still not following a VPN, followed by not using the company laptop.

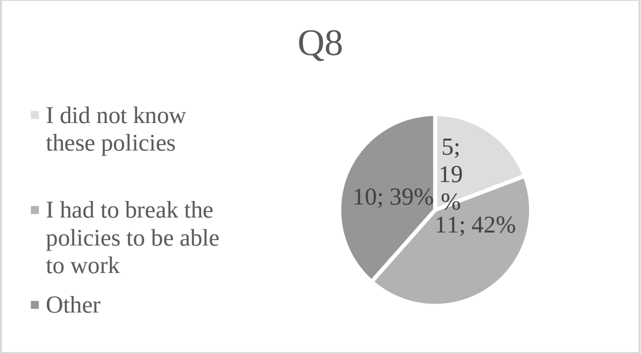


Figure 7: ratio Q8

Twenty-three participants filled in Q8. Again, multiple answers could be selected, hence 26 answers have been analysed which can be seen in figure 7. Interestingly, almost half of the participants state that they had to break the policies in order to be able to work. It should be kept in mind that there is still a percentage of people that did not break any rules. Another interesting finding is that out of these twenty-three participants, nine of them belonged to the data engineers/data scientists subgroup. Four of those data engineers/scientists gave the answer 'I had to break the policies in order to work' while the rest came from other subgroups. This signals that it is not only data engineers/scientists who think this way. When looking at the job descriptions of these other people, we see one administrator, two managers, two architects, and two product owners. This means that the distribution of job types is quite distributed among other groups. Based on the results of Q8, it is likely that the guidelines and policies are not that effective. Almost one out of four participants (thirteen out of sixty) gave a score of 5 or lower on Q4 on whether they feel like the security policies make their work more secure. These results together give an indicator that the guidelines are not that convincing, and that employees have to avoid some guidelines due to an otherwise inability to work.
Participants often chose not using a private laptop in addition to not using a VPN (Q7). Out of these nine people that at least answered not using a VPN, six of them answered that they had to break the policies in order to work. This could also be in combination with other reasons such as not knowing the policies. Still, it is an interesting finding as it shows that not using a VPN is likely not due to laziness but instead done purposefully.

For Q9, twenty-three percent stated having succeeded at circumventing policies. Another eight percent tried to, but did not succeed, and the majority with sixty-eight percent of respondents stated that they had not tried this. This shows again that almost one out of four participants fall outside of the perimeter, and another eight percent tried to do so. Out of the nineteen participants that tried to circumvent rules, four belonged to the group data scientists/engineers. Other common job types were: four managers, three analysts, and three administrators. This shows that it is not mostly data engineers/scientists that tried to circumvent rules

RQ 2: What are the attack surfaces of a company, and do they fall within their already set perimeter/firewall?

Originally interviews with four external companies were scheduled. However, only two responded. Due to time limitations, it was decided to only interview people from these two companies. The paragraphs are structured by main themes that together will be able to answer RQ2 and RQ2.1.

Attack surfaces outside of the Port of Rotterdam

On interview question 3 (‘In what way could a cyber attack on your company have an impact on the Port of Rotterdam?’), one interviewee answered that ‘such an attack would probably not be directed at the Port of Rotterdam, and more likely affect all clients. In case such a thing would happen, multiple processes that contain data stored at our company would be unavailable.’ The other external interviewee answered that they could only answer it from a red teaming perspective but that it could have a large impact. ‘There would be no longer support in executing security tests. Furthermore, a data breach could happen as for example data on red teaming events is stored for three months (depending on the contract).’

On the question on what a possible attack surface could be (question 5), both parties say that they would not know how attackers could gain access to the system. To conclude, it remains difficult to say to what extent it is likely that the possible threat from question 3 may become reality and what attack surfaces could be used by a possible attacker.

Communication wise, both parties agree that the attack surface is pretty well known by the security team at the Port of Rotterdam. They think that communication is good as it is. For example, one of the external interviewees answers question 7 with: ‘Yes, very well. They are very aware on a continuous level.’

On the answer to question 5 (What could be an attack surface of your company that the Port of Rotterdam may need to know about?) one interviewee answers that if there was something they would be fixing it already. At question 7 (Do you think the Port of Rotterdam is aware of their attack surface?), this interviewee answers with ‘Yes I think so, since the Ukraine situation actions have been started with among others our company to see what attack surfaces there are at our company and other suppliers of the Port of Rotterdam have taken a good look at risks and mitigations.’ This shows that communication levels between external companies and the security team are good as it is according to this interviewee. This could be the different expectation on the level of awareness the Port of Security should have or simply that they are indeed aware on the external attack surfaces already.

Attack surface inside of the Port of Rotterdam

On average, most participants in the interviews are content on how they perceive the amount of knowledge the security team has on the attack surface of their team. Only two interviewees think that more involvement is necessary for the security team to be able to get a better picture. Here, one interviewee says that communication is ‘very limited, there is no security officer in the team. Since last month there is a security officer working [in our team] (…) but before that little time has been put in. Not because of the security team but because there is too little manpower.’. He says that he thinks he is able to communicate issues to the security team, but that this is now dependent on the amount of spare time he has left on top of his other work. This shows that although communication could be improved, this is partly due to outside factors. The other critical interviewee says ‘I don’t think they know it [the attack surface of their team] very well, but that is an assumption.’ ‘There is not always a clear division of responsibilities (..)’. The interviewee ends by saying that it is getting better, but that improvement is still possible. Therefore, the addition of more security officers could increase awareness of the security team.

A third interviewee says that there are always the small details that are unknown. Other interviewees stress the self-sufficiency of the team with involvement on the side lines being sufficient. Whereas both external companies think that communication is good as it is, there is some disagreement within the internal teams. An interesting finding is that not all data of the internal teams go through the internal broker system: one interviewee explained that question 7 (‘How confident are you in the broker firewall at the Port of Rotterdam?’) only applies to them in case of VPN’s and user aware firewalling. At question 8 the interviewee explains that the internet connection (internetkoppeling) of their team does not go through the Port of Rotterdam broker system, but instead has a direct connection to an external company. Another interviewee also says that everything that can get on the internet from their team does not go through the broker network. Other teams do go through the current broker system, but due to difficulty of working, workarounds may be constructed for short time frames. This shows that not all data goes through the internal network broker due to a different infrastructure of the team, or due to issues that cannot be solved otherwise. It remained difficult for participants internally and externally to mention specific attack surfaces, but by gauging their opinion on the awareness of the security team, we can see if the security team is currently up to date with possible threats that the internal teams may have identified already.

Best practises

Although not all of these points are directly related to attack surfaces not covered by the firewall, they are improvements that help minimize attack surfaces. Zero trust network was mentioned by the internal interviewee. Three of the interviews mention that there needs to be more alignment between the teams. An improvement in this could then lead to an increased understanding of the attack surface of the different internal teams by the security teams. One interviewee wishes better guidelines, which is also what another interviewee mentioned is a good security practise in general. Three interviewees mention that more input from a security officer would be beneficial to improve their security. Two mention that the broker system might create a false sense of security. To illustrate, one of these interviewees says that people could end up thinking ‘It is in the broker system so it is secure’. The other interviewee says that because ‘everything is inside the broker you don’t really think about security, so you let loose a little.’ ‘Although it did help when we forgot authentication: because there was a broker system, only people inside the broker could exploit it.’

One of the external interviewees mentions having no unnecessary public facing systems, but two internal teams mention issues needing public endpoints but not being able to due to the broker system. However, this was not possible because the endpoint would no longer be behind the broker network. The only way to fix this was by adding the client to their route table, giving their external client some unnecessary privileges along with this. This is not ideal, as you do not want clients to have more privileges than necessary. This difference in experience between the external interviewee and internal teams is interesting since it depicts a clash of interest. No exposed endpoints are the most secure, but if it is necessary it might force ~~t~~eams to use workarounds that are not the most secure option due to the current broker system. A zero trust architecture could perhaps pose as a solution in this case.

5 DISCUSSION

The results of this study highlight that employees might be less compliant than one might think or hope. As a result, this might create an attack surface (PCs and laptops) that could be exploited. Implementation of a zero trust infrastructure could help out in this case. To illustrate, if you cannot trust that your own employees are following security policies, a zero trust architecture could fix this as the default is simply 'trust no one'. On the other hand, one could also think that one should improve the awareness on following the rules or create a stricter environment in which workaround are not tolerated. Employees with a more technical job (data engineers/scientists) are likely to disobey policies and guidelines. This could be due to them having to work with more types of software and more technical knowledge. It could also be due to a different type of attitude among engineers/scientists. However, quite some engineers mentioned 'not being able to do their job' as a possible reason, making the former more likely. Answering H1: data engineers/scientists indeed make up a significant amount of the people that have not followed some of the security guidelines, but they are not the only ones, making this not only a problem for them but also for other employees in the IT department. This becomes clear when looking at the data and one out of three participants in questionnaire said there have been security guidelines they did not follow in the last twelve months. This hypothesis is therefore partly confirmed. Answering H2: although some data engineers/scientists indeed try to circumvent guidelines, it is not mostly them who actively try to circumvent rules but instead these people come from multiple subgroups. This hypothesis is therefore partly confirmed. The results from H1 and H2 are interesting as it was expected that mostly data engineers/scientists were not following guidelines. Although it is true that a significant amount of this group is not following all guidelines, other groups are also likely to not follow guidelines. Therefore, it seems that this issue is not specific to one subgroup but instead a more widespread issue. Based on the data H3 is confirmed with not using a VPN mentioned the most. It is interesting that more participants answered not using a VPN than not using the company laptop: it means that some participants still use their company laptop but then disable the VPN.

The answers from the interviews show that it is difficult to approach the question on what possible attack surfaces are from an interview perspective. It did better in giving insight in possible attack surfaces that the security team could look into, or how knowledgeable the security team is perceived to be in the different teams. Not enough external companies were interviewed to give a conclusive answer to H4. One of the external interviewees did mention that an attack on their company could have a significant impact on the Port of Rotterdam but that this is very unlikely. More companies would need to be interviewed for a better view. H5 is partly confirmed for the internal teams. This is shown by a need for more participation by the security team which means that there might be knowledge on their attack surfaces missing. The external companies seem to be more confident in knowing their attack surfaces. This contrast could be due to a difference in trust levels as interviews done internally could feel more trustworthy for the interviewees than someone outside of your company wanting an interview on a sensitive topic. H6 is confirmed as multiple internal teams mention either appreciating active involvement/communication of the security team or wanting improved communication. If the security team were to put more focus on the teams that reported wanting more support, this could lead to improved security and possibly discoveries of attack surfaces by the security team themselves. Lastly, H7 surprisingly seems to be the opposite. Internal teams tended to have more points of improvement. This could be due to higher standards of the internal teams or because the security team is closer to them than the security team is for external companies. To draw more conclusive results, more external companies would have to get interviewed to get a more even ratio of internal and external interviews.

5.1 Contextual exploration

Findings of this research are beneficial for the computer science domain and more specifically in the area of information security. However, the questionnaire also looked into behavioral aspects of employees which can also benefit researchers in the social sciences. When all guidelines and policies are up to date, it is likely that a certain percentage of employees will still ignore these rules. In this research, some people chose to not follow the guidelines to be able to do their work, however, sometimes these guidelines are forgotten, or people are too lazy. How do we motivate these people to follow the rules? Is it only a matter of increasing awareness or should we approach it from a more behavioral standpoint? Securing a company through implementation of a zero trust architecture is one way to secure a company's data, but one of the most common ways attackers gain information is by phishing. In this case, it is not the technology that is lacking, it is people themselves who are the weakest link. To a certain extent, these issues can be mitigated by adding a warning to every file that comes in through email, or by using filters to try and remove suspicious emails from employee's mailboxes. However, employees might feel restricted by these rules. One of the responses in the questionnaire said that they forward emails to their personal inbox because the security rules make it unable to download *any* file normally. This poses a dilemma: on the one hand you want to create tighter rules to avoid employees accidentally downloading malware, but on the other hand it makes it harder for employees to perform certain tasks. And then you run the risk of employees looking for ways to avoid these rules. Research on finding this balance between workability and security from a behavioral approach could yield useful results that could lead to improved security. Furthermore, research into the most common barriers employees face when asked to adopt new behaviours to improve security can in turn positively influence the security of companies.

To look at it from a broader perspective, eliciting change in companies in general is also something that should be researched. One of the security officers at the Port of Rotterdam has tried to implement a zero-trust infrastructure for a while now, but it only seems to be heading into that direction slowly. So, how does one change things in larger corporations and not just on an individual level? It is not only perimeter security that can be outdated. Management styles, outdated software/hardware, or even creating sustainable long-term solutions, these can be hard to change or implement. In larger companies, change usually takes even longer. How does one speed up this process? Hackers do not wait until security officers have improved their security strategies, and climate change does also not wait on companies actually implementing sustainable options. Research into the area of facilitating change in large companies could have an impact on the speed of which solutions are implemented that could help prevent global warming, improve well-being of employees, and in light of this thesis, improve security.

5.2 Limitations

At first the list of ‘job types’ was closed. However, multiple comments were made in the remarks session on their job type not being available. As can be seen from Figure 2, there is a high number of managers who filled in the questionnaire. It is unclear whether these were actually all managers or that this option was chosen in case no better description was fitted. As a result, the list of job types was changed to include an ‘other’ option. However, this might have skewed the proportion of managers or other job types a bit. Two data engineers were interviewed on the broker network to ask what type of workarounds they use with VPNs and private laptops. Interviewing employees in other teams might have shed more insight in completely other ways workarounds are used specific to their job type. Lastly, although fifty percent of the IT department responded to the survey, it is still possible that a subgroup of employees is not represented enough. For example, the software engineer was added to the data engineers since there was only one response. Underrepresentation could result in a distorted ratio on whether participants have been following the security guidelines or not. Another limitation to this study is that the questionnaire did not ask if this rule breaking was done repeatedly. It could be the case that a group of the people answered yes only sporadically disobey guidelines. A question on whether this is done repeatedly could show to what extent this issue is systemic.

6 CONCLUSION

The goal of this research was to get a better understanding of the effectiveness of perimeter security and to improve the gap in knowledge between the theoretical concept of perimeter security and in a business environment. Additionally, we looked into attack surfaces and whether they fall within this already set perimeter. Lastly, we looked into best practises that might move beyond the concept of perimeter security. We did this by means of a questionnaire and interviews. Based on these results we were able to answer the research questions and hypotheses of this thesis.

Based on the literature review, a zero trust network seems to be preferred above the traditional perimeter security framework. Implementation of a zero trust infrastructure is specifically mentioned by one of the participants interviewed as a best practise. Additionally, the security guidelines, placed upon employees due to the implementation of the classical perimeter security, drive a significant number of employees to avoid them. This is due to them not being able to do their work, not knowing the policies, or simply forgetting rules. As a result, they might become a weak link that attackers can use to gain access to the network. Implementation of a zero trust infrastructure might lessen the rights of the attackers with such a compromised account, as ‘no one is trusted’ in any case. RQ1 can therefore be answered with ‘not so effective’, but as mentioned in the literary analysis, perhaps our way of thinking what perimeter security does has to change. This research shows that perimeter security might not only be outdated on theoretically, but also in practise.

It remains difficult to find unknown attack surfaces. Due to the limited number of external companies interviewed, it is difficult to make a generalization. Most of the internal interviewees think that the security team is decently up to date, but that better communication can improve this, and can help their team become more secure in general. Not all data from the internal teams go through the broker network. This holds true for data from two teams. These attack surfaces could better be looked into by the security team. The most often mentioned best practise was communication. Improvement in this area might lead to better insight of unknown attack surfaces. Lastly, there was also a need and appreciation for active involvement in the internal teams from a security officer. Answering RQ 2: no specific list of attack surfaces can be given, but by looking into the teams that want/need more input, attack surfaces could be discovered in this way as it is likely that some security issues are unclear at this time and teams might still lack the maturity to find these weak points themselves. Regarding RQ 2.1, the most common best practises include: increased communication, implementation of a zero-trust network, and clear guidelines. Lastly, based on the literary analysis, implementing the NIST zero trust principles from Table 3 can also improve the awareness of possible attack surfaces.

6.1 Future research

Although this research suggests that employees do not always follow the security guidelines, it is not possible to generalise this statement for other companies or the entirety of the Port of Rotterdam. Therefore, it can be beneficial to replicate this study on a greater scale within this company or across different businesses. It can be interesting to see if the ratio of reasons why people choose to not follow the rules are different. Another research that can be done in the future is interviewing more employees from external companies that work for the Port of Rotterdam. This way more conclusive results can be obtained regarding possible unknown attack surfaces or best practises. If a zero trust architecture becomes implemented, it would be interesting to redo this study and compare the results. Did the guidelines change? Are more people following rules and could this be due to more attainable guidelines? Perhaps the distributions of Q3-5 of the questionnaire will look different.

REFERENCES

Brooks, C. (2022). *Alarming cyber statistics for mid-year 2022 that you need to know*. Retrieved from https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/

DelBene, K., Medin, M., & Murray, R. (2019). *The Road to Zero Trust (Security)*. Defense Innovation Board Report.

Everson, D., & Cheng, L. (2020). *Network attack surface simplification for red and blue teams*. In 2020 IEEE Secure Development (SecDev) (pp. 74-80). IEEE. DOI:10.1109/SecDev45635.2020.00027

Göksel, U. Ç. T. U., ALKAN, M., Doğru, İ. A., & Dörterler, M. (2019, October). *Perimeter network security solutions: a survey*. In 2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT) (pp. 1-6). IEEE. DOI:10.1109/ISMSIT.2019.8932821

James, L. (2018). *Economic Impact of Cybercrime - No Slowing Down*. Retrieved from: https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf.

Kon Leong. (2017). *Which of Your Employees Are Most Likely to Expose Your Company to a Cyberattack?* Harvard Business Review Digital Articles, 2–5. Retrieved from: https://hbr.org/2017/12/which-of-your-employees-are-most-likely-to-expose-your-company-to-a-cyberattack

Kumar, V., Chaisiri, S., & Ko, R. (2017). *Data Security in Cloud Computing*. DOI:10.1049/PBSE007E

Ledesma, J. (2022). *IDS vs IPS: what organisations need to know*. Retrieved from: https://www.varonis.com/blog/ids-vs-ips

Meyer, D. (2019). *The death of the network perimeter and the firewall? Not so fast.* Retrieved from: https://blogs.cisco.com/security/the-death-of-the-network-perimeter-and-the-firewall-not-so-fast

Mistry, B. (2022). *Why it's time to map the digital attack surface.* Retrieved from: https://www.trendmicro.com/en_us/research/22/f/reduce-attack-surface-digital-mapping.html.

Mukherjee, A. (2020). *Network Security Strategies: Protect your network and enterprise against advanced cybersecurity attacks and threats*. Packt Publishing Ltd.

Mylonas, L. (2018). *What is AAA security? An introduction to authentication, authorization and accounting.* Retrieved from https://codebots.com/application-security/aaa-security-an-introduction-to-authentication-authorisation-accounting.

OWASP. *Attack Surface Analysis Cheat Sheet.* Retrieved from: https://cheatsheetseries.owasp.org/cheatsheets/Attack_Surface_Analysis_Cheat_Sheet.html

P. Manadhata and J. Wing (2010). *An attack surface metric*. IEEE Trans. Softw. Eng., vol. 37, no. 3, pp. 371–386. DOI:10.1109/TSE.2010.60

Riggs, C. (2003). *Network perimeter security: building defense in-depth*. Auerbach Publications. DOI:10.1201/9780203508046

Rose, S., Borchert, O., Mitchell, Stu., Connelly, S. (2020). *Zero trust architecture*. NIST Special Publication, 800, 207. DOI:10.6028/NIST.SP.800-207

Rusere, K., & Ngassam, E. K. (2020, May*). Emerging Network Security Issues in Modern Tertiary Institutions*. In 2020 IST-Africa Conference (IST-Africa) (pp. 1-9). IEEE.

Theisen, C., Munaiah, N., Al-Zyoud, M., Carver, J. C., Meneely, A., & Williams, L. (2018). *Attack surface definitions: A systematic literature review.* Information and Software Technology, *104*, 94-103. DOI:10.1016/j.insfof.2018.07.008

TrendMicro (2022). *A global study: mapping the digital attack surface. Why global organisations are struggling to manage cyber risk.* Retrieved from: https://www.trendmicro.com/explore/trend_global_risk_research_2/the-challenge-of-man.

Ullrich, J., Cropper, J., Frühwirt, P., & Weippl, E. (2016). *The role and security of firewalls in cyber-physical cloud computing.* EURASIP Journal on Information Security, 2016(1), 1-20. DOI:10.1186/s13635-016-0042-3

Zhang, M., Wang, L., Jajodia, S., & Singhal, A. (2018). *Network attack surface: Lifting the concept of attack surface to the network level for evaluating networks' resilience against zero-day attacks.* IEEE Transactions on Dependable and Secure Computing, *18*(1), 310-324. DOI:10.1109/TDSC.2018.2889086

APPENDIX

Interview questions

Questions for external companies

1. What is your area of expertise?
2. In what way is your company affiliated with the Port of Rotterdam/what service does your company deliver to the Port of Rotterdam?
3. Are you familiar with the concept of attack surface mapping/monitoring?
4. In what way could a cyber attack on your company have an impact on the Port of Rotterdam?
5. What could be an attack surface of your company that the Port of Rotterdam may need to know about?
6. How well do you think the attack surface of your company in general is known to the Port of Rotterdam?
7. Do you think the Port of Rotterdam is aware of their attack surface?
8. What do you think the Port of Rotterdam has to do to map, mitigate and/or reduce their attack surface?
9. Do you think the current security measures taken by the Port of Rotterdam are up to date?
10. Could you think of security measures to improve the security at Port of Rotterdam?
11. Is the Port of Rotterdam security team aware of concerns that you and your company have regarding the security of Port of Rotterdam?

Questions for teams within Port of Rotterdam

1. What does your team deliver for the Port of Rotterdam?
2. Are you familiar with the concept of attack surface mapping/monitoring?
3. In what way could a cyber attack in your team have an impact on the Port of Rotterdam?
4. What could be an often overlooked/lesser known attack surface in your team? (That the security team might not take into consideration as much)
5. What could be an attack surface in your team that the security team may need to know about?
6. How well do you think the attack surface of your team is known to the Port of Rotterdam (Security)?
7. How confident are you in the broker firewall at the Port of Rotterdam?
8. Could you think of areas where the Broker Firewall reduces the security of the Port of Rotterdam?
9. Do you think the current security measures taken by the Port of Rotterdam are up to date?
10. Could you think of security measures to improve the security at Port of Rotterdam?

11. Is the Port of Rotterdam security team aware of concerns that you and your team have regarding the security of Port of Rotterdam?

Questions software teams to map possible reasons attack surface and a second part for non-compliance perimeter security

1. What does your team deliver for the Port of Rotterdam?
2. Are you familiar with the concept of attack surface mapping/monitoring?
3. In what way could a cyber attack in your team have an impact on the Port of Rotterdam?
4. What could be an often overlooked/lesser known attack surface in your company? (That the security team might not take into consideration as much)
5. How well do you think the attack surface of your team is known to the Port of Rotterdam?
6. Do you think the current security measures taken by the Port of Rotterdam are up to date?
7. Could you think of security measures to improve the security at Port of Rotterdam?

P.2 interview compliance perimeter security

8. Are you familiar with the broker system?
9. How confident are you in the broker firewall at the Port of Rotterdam?
10. Could you think of areas where the Broker Firewall reduces the security of the Port of Rotterdam?
11. Does it ever prevent you from doing work (efficiently)?
12. If yes, in what ways does it prevent you from working?
13. Do you accept it, or do you try to find ways to mitigate it (by avoiding rules)?
14. If you try to find ways to mitigate it, what did you do and was it successful?
15. Do you think the broker system is doing a good job at protecting you?

Questions security team

1. Are you familiar with the concept of attack surface mapping/monitoring?

2. Do you think you have a good overview of all the attack surfaces of the Port of Rotterdam?

3. What about attack surfaces outside of the Port of Rotterdam?

4. In what ways yes, in what ways no?

5. Where do you see potential gaps in knowledge?

6. How confident are you in the broker firewall at the Port of Rotterdam?

7. Could you think of areas where the Broker Firewall reduces the security of the Port of Rotterdam?

8. Do you think the current security measures taken by the Port of Rotterdam are up to date?

9. Could you think of security measures to improve the security at Port of Rotterdam?

Tables

Question number	Question
1	'I consent to participating in this survey as described above'
2	'Which of the following best describes your job?
3	'How well do you think you know the security guidelines and policies at the Port of Rotterdam?
4	How much do you feel these security guidelines and policies enable you to do your work in a secure manner?
5	How much do you feel like these security guidelines and policies restrict your work?
6	Are there any security guidelines or policies you did not follow during work in the last 12 months?
7	If you chose yes, which policies did you not follow?
8	If you chose yes, what is your reason for not following these policies?
9	If you actively tried circumventing policies, did you succeed?
10	Do you have any other remarks about this survey?

Table 4: list of survey questions

Job type	Count
Administrator	7
Analyst	9

Job type	Count
Architect	6
Data engineer	8
Data scientist	3
Security	2
Manager	17
Development professional	2
Product owner	4
Advisors	2

Table 5: ratio respondents

Job type	Mean 'How well do you think you know the security guidelines and policies at the Port of Rotterdam?'
Administrator	8.2
Analyst	7.3
Architect	7.3
Data engineer	5.4
Data scientist	7.3
Security	9.5
Manager	7.6
Development professional	7.5
Product owner	7.2
Advisors	7.5
All	7.3

Table 6: mean Q3

Job type	Mean 'How much do you feel like these security guidelines and policies enable you to do your work in a secure manner?'
Administrator	6.5
Analyst	8.3
Architect	6.5
Data engineer	4.8
Data scientist	6
Security	7
Manager	8.1
Development professional	8
Product owner	8.6
Advisors	8.5
All	7.4

Table 7: mean Q4

Job type	Mean 'How much do you feel like these security guidelines and policies restrict your work?'
Administrator	3.6
Analyst	3.9
Architect	6.5
Data engineer	5.9 (Data engineer 6.4, Software Engineer 2)
Data scientist	4
Security	5

Job type	Mean ‘How much do you feel like these security guidelines and policies restrict your work?’
Manager	4.8 (Service & Project manager 8)
Development professional	7
Product owner	4
Advisors	4
All	4.8

Table 8: mean Q5

Interviewee number	Best practises mentioned during interview
1	Separation/fragmentation, ‘more alignment in views security team so our team is not the middle-man’, ‘Having a security officer help out’ ‘Authentication also on test environments’
2	Constantly improving monitoring, more scanning tools, new policies, different approach to handling general infrastructure
3	Get rid of ‘feel good’ security measures
4	Get a security officer that looks over project in general
5	Edge firewalling, make responsibility clear (is it the team or the security team?), ‘create clear guidelines on responsibilities, now it is up to me what I tell security team’
6	‘More communication security team and our team’ ‘Have someone know the total picture of the network broker landscape’
7	‘Zero trust landscape’, ‘more decision made based on technical input and not functionality' ‘more input security team on certain Palo Alto options’ ‘Don’t trust anyone in your network’ ‘Current network exists on subnets, so ports are open that should be closed. Use specific IP’s on the server. So only specific route is possible, an closed when not used.’ ‘Software defined access, software defined wan (white area network)’
8	‘More active participation security team’, ‘vulnerability analysis’ ‘rethink what are actual vulnerabilities (per team): software updating for vulnerabilities in an environment that is not internet facing not practical’ ‘Pentesting’

Interviewee number	Best practises mentioned during interview
9	‘Not really, but stick to certain documentation to guarantee continuity, let architecture designs get approved’ ‘make sure that when people stop working people still know the whole picture’
10	‘Make sure no unnecessary internet facing systems’ ‘continuously improving monitoring’

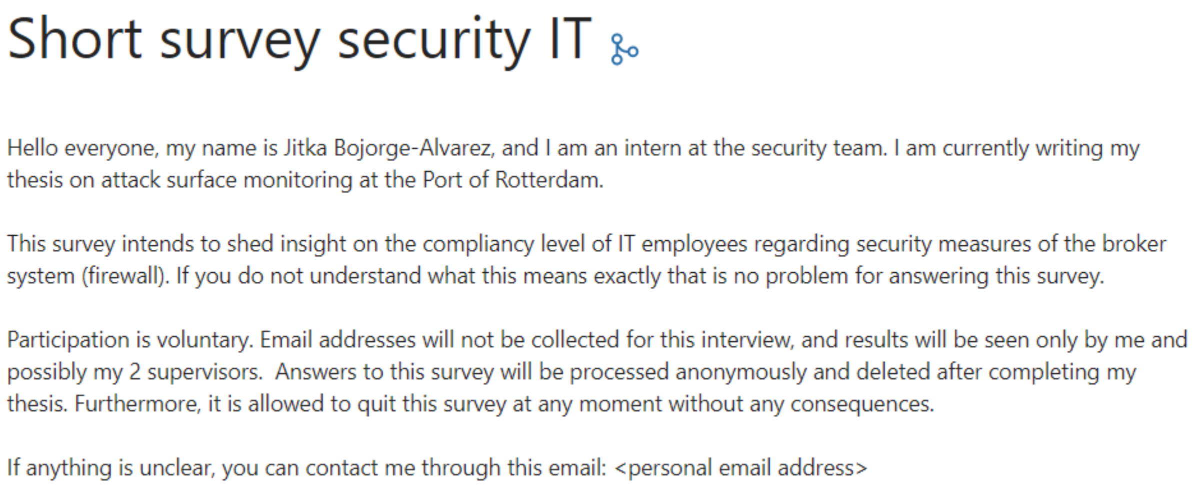
Table 9: Best practices

Interviewee number	How well do you think the attack surface of your team is known to the Port of Rotterdam/Security team?
1	‘Difficult to evaluate, on average good enough, except perhaps details on repository level, but that is the responsibility of our team’ ‘Perhaps a 6-7/10, but difficult to judge’
2	Depends. Attack surface changes over time and it depends on how you measure it. No systematic approach yet, with which you could approach unknown unknowns.’ ‘6-7/10’
3	‘Pretty well but could be better’ ‘5-6/10’
4	‘Don’t know. Depends on security team. Probably an 8/10, there is always something that is missing.’
5	‘Very limited, there is no security officer in the team’ ‘Since last month there is a new security officer working [in our team], but before that little time has been put in. Not because of the security team but because there is too little manpower.’
6	‘I don’t actually know.’ ‘I don’t think they know it very well but that is an assumption. It is not always a clear division of responsibilities, but it is now become more clear but there is still improvement possible’
7	Every three weeks there is a meeting with a security officer to go through the risk log. We should be on the same page’

Interviewee number	How well do you think the attack surface of your team is known to the Port of Rotterdam/Security team?
8	‘Difficult. They are pretty knowledgeable. There is no active involvement, but more like standing on the side lines. That does not mean they do not know what is going on, they are just aware.’

Table 10: perceived knowledge security team on attack surface

Questionnaire questions



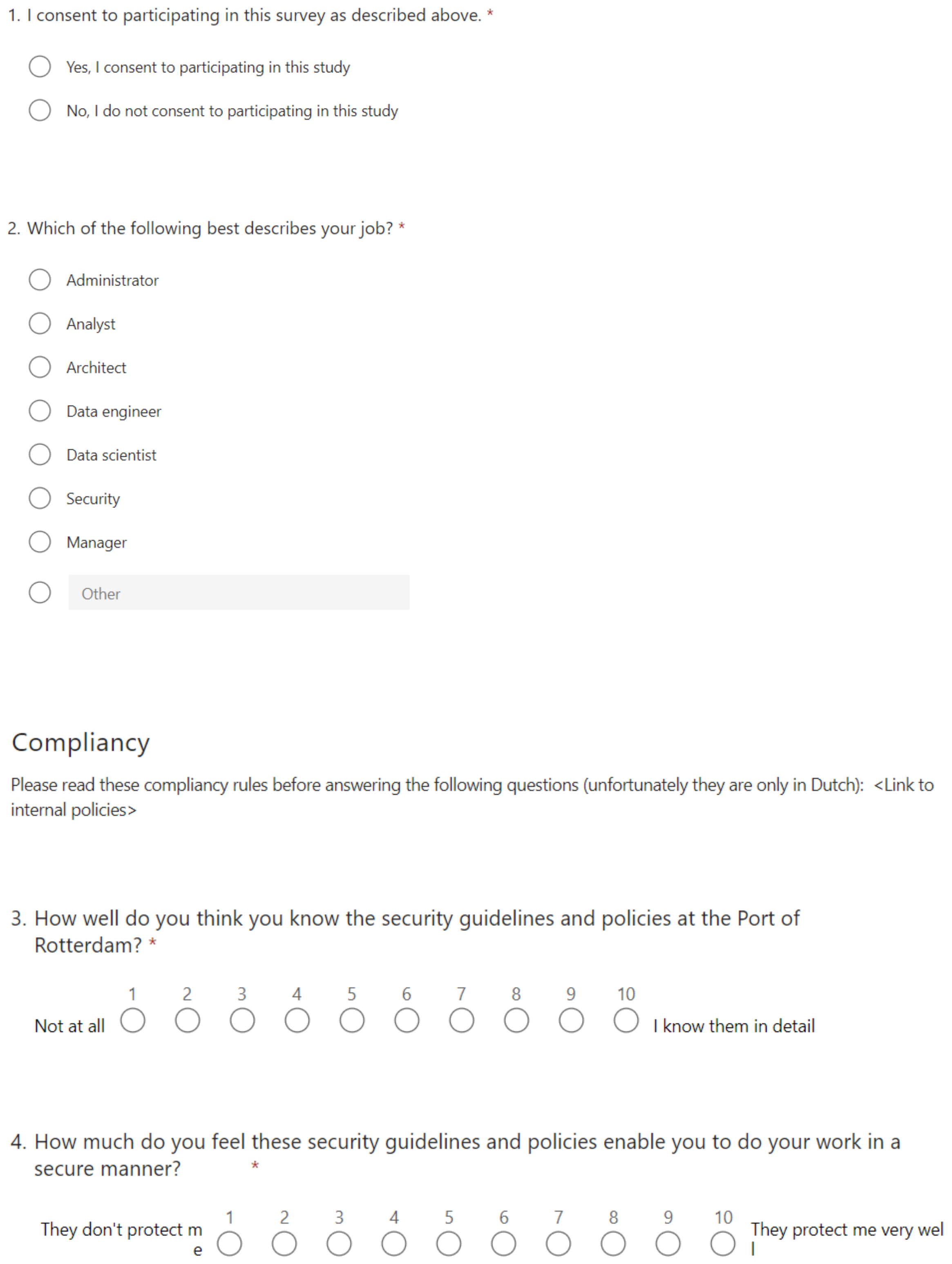
Short survey security IT

Hello everyone, my name is Jitka Bojorge-Alvarez, and I am an intern at the security team. I am currently writing my thesis on attack surface monitoring at the Port of Rotterdam.

This survey intends to shed insight on the compliancy level of IT employees regarding security measures of the broker system (firewall). If you do not understand what this means exactly that is no problem for answering this survey.

Participation is voluntary. Email addresses will not be collected for this interview, and results will be seen only by me and possibly my 2 supervisors. Answers to this survey will be processed anonymously and deleted after completing my thesis. Furthermore, it is allowed to quit this survey at any moment without any consequences.

If anything is unclear, you can contact me through this email: <personal email address>



1. I consent to participating in this survey as described above. *

○ Yes, I consent to participating in this study

○ No, I do not consent to participating in this study

2. Which of the following best describes your job? *

○ Administrator

○ Analyst

○ Architect

○ Data engineer

○ Data scientist

○ Security

○ Manager

○ Other

Compliancy

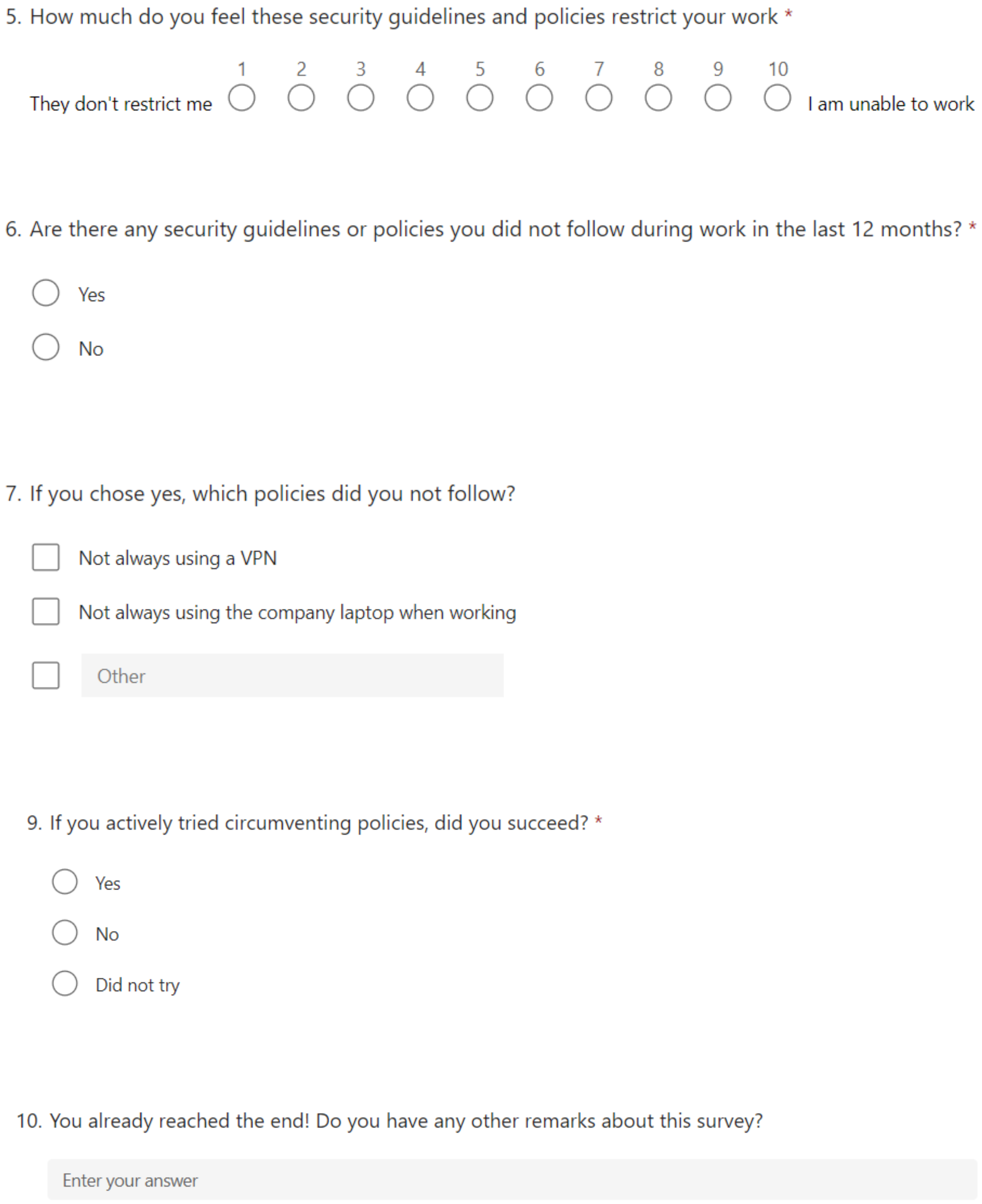
Please read these compliancy rules before answering the following questions (unfortunately they are only in Dutch): <Link to internal policies>

3. How well do you think you know the security guidelines and policies at the Port of Rotterdam? *

	1	2	3	4	5	6	7	8	9	10	
Not at all	○	○	○	○	○	○	○	○	○	○	I know them in detail

4. How much do you feel these security guidelines and policies enable you to do your work in a secure manner? *

	1	2	3	4	5	6	7	8	9	10	
They don't protect m e	○	○	○	○	○	○	○	○	○	○	They protect me very wel l



5. How much do you feel these security guidelines and policies restrict your work *

	1	2	3	4	5	6	7	8	9	10	
They don't restrict me	○	○	○	○	○	○	○	○	○	○	I am unable to work

6. Are there any security guidelines or policies you did not follow during work in the last 12 months? *

○ Yes

○ No

7. If you chose yes, which policies did you not follow?

□ Not always using a VPN

□ Not always using the company laptop when working

□ Other

9. If you actively tried circumventing policies, did you succeed? *

○ Yes

○ No

○ Did not try

10. You already reached the end! Do you have any other remarks about this survey?

Enter your answer

Figure 8: layout questionnaire