TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Juhan Kaalep 153276IVCM

THE STATUS, REASONS AND PERSPECTIVE OF CYBER SECURITY OF ESTONIAN SME-S IN THE CONTEXT OF THE CYBER ESSENTIALS SCHEME

Master's thesis

Supervisor: Andro Kull
PhD

Tallinn 2017

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Juhan Kaalep 153276IVCM

EESTI VÄIKEETTEVÕTETE KÜBERTURVALISUSE OLUKORD, PÕHJUSED JA PERSPEKTIIV CYBER ESSENTIALSI RAAMISTIKU KONTEKSTIS

Magistritöö

Juhendaja: Andro Kull
PhD

Tallinn 2017

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Juhan Kaalep

02.01.2018

Abstract

The aim of the study is to assess the current cyber security situation within Estonian SME-s, and more specifically within micro-businesses, from the perspective of Cyber Essentials – government backed cyber security scheme that is mandatory for SME-s to follow in the UK. It is assumed that most companies assessed within the study would fail to produce satisfactory results. The study would further look into the main reasons of microbusinesses not investing more into cyber security, and offer solutions to the lack of security, as follows:

1) Making CE mandatory in some way would reduce the cyber security risks in a similar fashion to Pareto's 20/80 rule in economics;

2) The Estonian ID-card and X-road architecture take care of the worst-case scenarios and further investment into secure authentication may prove inefficient;

3) The cost-benefit ratio of improving cyber security is either unfeasible or feasible, and would therefore make a suggestion to take either direction.

This thesis is written in English and is 89 pages long, including 3 chapters, 17 figures and 5 tables.

Annotatsioon

Eesti väikeettevõtete küberturvalisuse olukord, põhjused ja perspektiiv Cyber Essentialsi raamistiku kontekstis

Uurimuse eesmärk on hinnata Eesti väike- ja suurettevõtete küberturvalisuse olukorda, täpsemalt mikroettevõtteid. Uurimuse lähtepunktiks on võetud Cyber Essentials'i raamistik – riiklikult toetatud küberkaitse raamistik, mis on Suurbritannias väikestele ja keskmise suurusega ettevõtetele kohustuslik. Uurimuse teostamisel eeldatakase, et valdav enamus vastanuist ei saavuta uurimuses rahuldavaid tulemusi. Seejärel keskendub uurimus põhjustele, miks mikroettevõtted ei panusta küberturvalisusele rohkem ning üritab leida lahendusi alljärgnevalt:

1) Cyber Essentials'i kohustuslikuks muutmine aitaks tõsta analoogselt Pareto 20/80 printsiibile majanduses ka küberkaitses ettevõtete olukorda;

2) Eesti ID-kaardi ja X-tee lahendused pakuvad piisavalt kõrget kaitset kõige halvemate stsenaariumite eest, mistõttu täiendav investeering autentimise taseme tõstmiseks võib osutuda tarbetuks

3) Tasuvusanalüüs võib näidata, et küberkaitse taseme tõstmine on mõistlik, kuid võib näidata ka vastupidist, kuid uurimuse autor üritab anda soovituse seniste tulemuste põhjal.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 89 leheküljel, 3 peatükki, 17 joonist, 5 tabelit.

List of abbreviations and terms

CE	Cyber Essentials
IT	Information Technology
RIA	Riigi Infosüsteemide Amet, (In English: Estonian Information System Authority)
SME	Small- and Medium-Sized Enterprise

Table of contents

List of figures

List of tables

1 Introduction

Cyber security is undoubtedly an increasingly important part in every company's every day dealings. Whether companies want to admit it or not, their business data and processes are in jeopardy by an increasing number of actors. It is unclear, however, for most companies, what to do exactly to protect themselves against cyber threats and how much emphasis it should require. Moreover, on a national scale, such information can become critical for lawmakers, in order to protect their country's businesses. It is less clear what is currently being done in most of Estonian businesses in order to protect against cyber threats and what are their experiences with cyber threats so far, aside from incident reports from the Estonian Information Systems Authority. Furthermore, based on the experiences so far, what should be done to improve the situation and is there really any need for it, is another question.

1.1 Research problem

In the context of Estonia, general practices towards implementing a standardized cyber security framework in businesses relies largely on ISKE and ISO. These frameworks are large and often-times overwhelming for small and medium-sized companies (SME-s). The official framework supported and enforced by the Estonian Information System Authority (RIA), is ISKE, with a dedicated web portal for easier use made available to the general public (Estonian Information System Authority (RIA), 2017). The Cyber Essentials framework, which originates from and is implemented in the UK carries a much smaller weight compared to ISO and ISKE, and can mitigate many of the more common and trivial cyber security risks due to its relatively common-sense set of controls and easy adaptation. The question is, whether it would be applicable for Estonian SME-s and how much would it help reduce risks. Another problem is that the current decision-making is based largely on estimates by various state authorities, such as RIA, and a relevant study that would map the existing cyber security practices and experiences remains to be found. The data used by policymakers is therefore reactive, rather than predictive.

The thesis hopes to shed light on current security practices by Estonian microbusinesses, define the weakest points and suggest on first points to improve, taking into account the estimated cost of a one-time project to harden a company's IT infrastructure.

1.2 Goals of the study

The goal of the study would be to demonstrate that implementing an already existing light cyber security framework, in the example of Cyber Essentials, would help reduce the risks of an average Estonian SME by 80%.

1.3 Importance of the study

The aim of the study is to demonstrate that most of the wide-spread cyber threats can be reduced by implementing common security practices. Naturally, targeted attacks by skilled attackers would be able to penetrate the defences put up using the Cyber Essentials framework, these remain beyond the scope of this study.

In case the study accomplishes to demonstrate an effective reduction in risk by implementing Cyber Essentials, it would provide a baseline for other companies to implement it. Further, larger companies may also benefit from the study as it would draw attention to the actual reasons of implementing a cyber security framework, rather than implementing a ubiquitous policy.

1.4 Limitations and key assumptions

The key limitations included statistics being available for attack vectors on Estonian SME-s, finding companies that would be willing to share their past experiences regarding cyber threats, and finally, that companies have not implemented many of the hardening methods described in Cyber Essentials. In the course of the study, all of these limitations proved to be correct.

1.5 Literature review

There seems to be no documented attempt to implement the Cyber Essentials scheme in not only Estonian SME-s, but elsewhere in the world. In fact, no studies could be found

that would investigate the impact of implementing the Cyber Essentials scheme. It is therefore reasonable to assume that this is the first attempt at a study of its kind.

Similarly to the UK, where according to Chris Rhodes (Rhodes, 2017, p. 3), 96% of businesses are micro-businesses with fewer than ten employees in the UK, 91% of Estonian companies also employee less than 10 people (Statistics Estonia, 2017). Considering the simplicity and low cost of establishing a new company in Estonia, which increases the number of inactive companies, these differences are perhaps bigger. Nevertheless, micro-businesses make up most of the total number of companies in Estonia, and thus need to be addressed accordingly.

The importance of investing time and effort into handling private and non-profit organisations in Estonia from the cyber security improvement aspect is also stressed in the "Annual Cyber Security Assessment 2017" by Estonian Information System Authority.

Security awareness in the private sector is inconsistent and investments into security are insufficient[.] As expected, the majority of cyber incidents last year [2016] affected the private sector, which is where the greatest number of users is found. It includes companies large and small, NGOs and individual computer users whose levels of digital dependence and cyber security awareness vary widely. It is also true that the importance of functioning of digital solutions tends to be underestimated and that instead of preventing risks, attention is devoted to security only after an incident occurs. (Estonian Information System Authority (RIA), 2017, p. 23)

The Estonian Information System Authority further lists the main threats for Estonian microbusinesses as "out of date web pages where vulnerabilities are exploited for data theft" and "security flaws and administration errors in their information systems" (Estonian Information System Authority (RIA), 2017, p. 23). Finally, the report concludes: "The private sector's awareness of cyber risks is spotty, both on the individual employee and corporate level. Small companies and NGOs in particular don't think "it could happen to them" and don't invest into security." (Estonian Information System Authority (RIA), 2017, p. 24).

Legislation to improve the situation among more critical sectors of the private industry is under development in Estonia at the time of writing of this thesis. The Ministry for

Economic Affairs has drafted the Cybersecurity Act, which is scheduled to take effect on 10.05.2018. (Ministry of Economic Affairs - Republic of Estonia, 2017, p. 12). According to the legislation draft, it will mostly regulate critical infrastructure companies, as well as companies operating with client data, providing cloud services or providing an e-commerce service. While it is most certainly an improvement, it does not seem to cover all companies in the country.

1.6 Methodology

The study can be separated into smaller pieces. First, to understand if the final solution would be applicable to the majority of Estonian SME-s, a small statistical analysis was done to define the average Estonian company based on number of employees, which would in turn help determine the rough estimate of the level of complexity to harden the average company's IT infrastructure. Data from the Estonian Business Register was used to find the specific companies to study. Second, a survey was carried out to collect self-assessments by Estonian SME-s based on CREST's Cyber Essentials questionnaire 3.1, in combination with additional questions that would help find more vulnerable target groups within the overall selection. The study was carried out in both Estonian and English, albeit only 1 response was submitted in English. Third, a scoring system was developed to study the level of vulnerability among the respondents. Fourth, reasons for the perceived lack of security would be studied. Fifth and the last chapter would focus on possible solutions to the situation.

The questionnaire was modified to include additional descriptive data regarding the respondents' general information. The questionnaire was subsequently translated into Estonian, while the English version was also kept. Both versions were published on Google Forms to be redistributed later. Respondents were cordially invited to fill the questionnaire with a promise to see other respondents' results averages.

During the scoring phase, since the CREST public version of Cyber Essentials questionnaire is not equipped with a grading mechanism by itself, one needed to be created. In order to standardize the questions and the 5 different sections of the questionnaire, each possible response was assigned a grade ranging from 0 to 10, with increments of 2.5 to the score in most cases. The most common set of possible answers to a question and their scores can be seen on the following table. Increments of 2.5 were

chosen, as in most cases, 4 positive choices were possible for the questions, while some questions also included more options and others less. In order to accommodate all the possibilities, a scale of 0 – 10 was chosen.

Table 1. An example of assigned scores to the possible answers to a single question in the questionnaire.

Yes always	10
In most cases	7,5
Sometimes	5
Rarely	2,5
Never	0

Next, each subsection – Firewalls, Secure Configuration, Access Control, Malware Protection and Patch Management – was graded separately. The purpose of this was to standardize each section and rule out over-estimating the importance of one section over another due to the number of questions in the section. Each section was assigned a maximum value of 10 and scores recalculated to match that. This was done by dividing the sum of answers in a given section by the number of questions within that section. This means that questions in different subsections essentially carry different weights. To rule out any negative impact this may have had, the total scores were also calculated without using sub-totals of sections and results compared. While there were minor differences in the overall ranking, they were in a reasonable range. Since the ranking of the companies is of little importance compared to the overall scores, which were largely unaffected by this aspect, the difference is ignored.

1.7 What is Cyber Essentials

Cyber Essentials (CE) is a government backed cyber security scheme used in the United Kingdom. CREST is one of the accredited certification bodies for the scheme and their latest version, 3.1 to be exact, was used for the study. Cyber Essentials can by and large be separated into 2 versions – Cyber Essentials and Cyber Essentials Plus. The current research will focus on the first and more basic version. It is a verified self-assessment meaning companies map out their own infrastructure and assess the hardening of the systems themselves. A certification body, such as CREST or many of the other certified bodies verifies the questionnaire and performs an external vulnerability scan. A Cyber Essentials Plus certificate would also include internal vulnerability scans and assessments

by the accredited certification body. This study focuses on the self-assessment to determine whether a further action would even be carried out.

The Cyber Essentials scheme focuses on 5 distinct security areas: 1) Boundary firewalls and internet gateways, 2) Secure configuration, 3) User access control, 4) Malware protection and 5) Patch management. In order to score the responses, a scoring index was developed. No existing scoring scheme was readily available for the self-assessment from CREST, although a far more thorough version of self-assessment than the CE scheme, was made available that did include automatic self-scoring.

1.8 Why Cyber Essentials

Several comprehensive frameworks already exist for cyber security compliance, for example ISO/IEC 27001/2, IASME, (ISKE based on BSI manual). However, Cyber Essentials provides a more robust and easily adaptable approach compared to the previously mentioned frameworks. Rather than introduce methods to analyse risk and make financial decisions based on the level and likelihood of any given risk, Cyber Essentials provides the most basic list of controls to harden a network and the nodes belonging to it. As stated in the Cyber Essentials requirements documentation, it only "[…] presents requirements for mitigating the most common Internet based threats to cyber security." (CE Requirements, 3). "What Cyber Essentials does, is define a focused set of controls which will provide cost-effective, basic cyber security for organisations of all sizes." (CE Assurance framework, 3).

The main target of the study is to assess the feasibility of implementing Cyber Essentials in Estonia from the viewpoint of how much there is to gain, at what cost and what would be the overall impact.

2 Survey setup and results

The study's focus lies with measuring the efficiency of the Cyber Essentials framework on Estonian companies. In order to find the number of possible target companies in Estonia, data from Statistics Estonia was used, specifically number of employees in full-time equivalent units. As seen on Table 1, the two groups employing the largest number of employees in Estonia are the smallest and largest companies, employing either a relatively small number of employees of 1-9 people, or over 250 respectively.

Table 2. FS025: ENTERPRISES' EMPLOYMENT AND HOURS WORKED by Year, Economic activity (EMTAK 2008), Number of persons employed and Indicator. Statistics Estonia. (11.04.2017)

	Number of enterprises	**Number of persons employed**	**Number of employees**	**..number of part-time employees**	**Number of employees in full-time equivalent units***
Total	78624	454965	434198	37948	416044
1-9	71282	143893	123917	15656	119437
10-19	3776	50006	49793	3789	47296
20-49	2231	63208	63050	4117	60580
50-99	768	49814	49722	3486	47621
100-249	390	55299	55266	3418	53133
250 and more	177	92745	92451	7483	87977

The arithmetic average number of employees in Estonian companies can be deduced by Table 1 to be five. Since the complexity of a computer network should not increase significantly with less than 10 workstations, though, the target group will include companies with up to 10 employees.

Amadeus database was used to find suitable respondents to the survey, with 3 criteria set, each one narrowing down the number of suitable results out of the overall data. The first and default criteria was to find all active companies and companies with unknown situation from the database. The second criteria established the country of the company as Estonia. This already narrowed down the number of prospects from 3,376,177 to 9,951.

The third and last criteria set the number of employees employed in each company as between 1 and 10. The final number of suitable results was therefore narrowed down to 2,826. A manual filtering was then performed on the remaining company names and contact data, filtering out multiple entries and removing excess email addresses from companies with more than one address.

The survey questionnaire was sent out in two larger batches of emails, each further reduced to batches of less than 500 e-mails per 24 hours in order to remain below blacklist levels. It did not help, unfortunately. The first larger batch included all the remaining contacts and took about a week to distribute. The second larger batch of emails was sent to contacts who seemed not to have opened the first email, either due to being on vacation, out of office, or lack of interest. The second batch consisted of roughly 1900 contact addresses and was distributed in the same pace as the first batch.

Initially, a response rate of 5-10% was expected to the survey, with 5% being the realistic and 10% optimistic expectation. The response rate to the survey was, in fact, closer to 1%, which created a large divide between expected number of responses and final number of respondents.

The Cyber Essentials questionnaire itself was translated into Estonian, while the original questions in English were also made available to respondents. Additionally, general data was also gathered to be able to generalize on the overall results. A total of 8 questions were added to the original questionnaire, under a general information section to better distinguish them. The additional information requested included company's main field of activity, county of activity in Estonia, number of employees, authentication methods used, experience of suffering from cyber-attacks or cybercrime and the size of the losses from them, in case there had been any.

Google Forms was used to make versions in both languages available to respondents. Follow-up questions were removed for each respondent individually in case the question became obsolete by an answer already given. For example, in case the respondent stated that no firewall was present on the company network, the following questions regarding firewalls were omitted.

One of the most doubtful questions within the questionnaire included jumping over reasonable questions within the questionnaire based on the malware protection used by

the respondent. The basis of this was to cover the questions as closely resembling the CREST v.3.1, which specifically stated jumping over questions based on the answer to question No. 36. The question and its possible responses were as follows:

“Which of the following is in use within the organisation?

a. Anti-virus or Malware protection

b. Application whitelisting

c. Application Sandboxing

d. None of the above

This provided several ways to understand the purpose of the question. The approach taken in this survey derived from an understanding that the different solutions did not exclude one another, but companies that employed application whitelisting were extremely likely to also include anti-virus or malware protection software on their end-user devices. Similarly, a respondent claiming to use application sandboxing would be likely to already have anti-virus and malware protection in place, as well as application whitelisting.

It is, however, possible to understand the purpose of the question in the opposite way – as these solutions being exclusive compared to one another, and therefore each segment should be graded as a full set of sub-section questions.

This problem became apparent during data analysis and only after the data was already collected. In order to make up for the loss in data, the sub scores for the malware protection section were calculated by using only the available answers, rather than all the answers in the subsection. That said, for any future implementations of such a questionnaire, this section should be reconsidered and evaluated in a manner that would allow the companies that use application whitelisting or sandboxing to also answer to questions regarding anti-virus and malware protection software.

2.1 Economic cost of hardening the average company's IT infrastructure

So how big is the cost of getting a single company's IT infrastructure hardened at least well enough to pass the Cyber Essentials test? First, a few assumptions need to be made based on known averages. The average number of employees in a company in Estonia is 5, as determined earlier. Trying to prepare for the worst-case scenario, let us assume each employee has a personal workstation, a smart phone that is connected to company email and at least a few of the employees also use personal computers to connect to the company network. This would bring the total number of end-user devices alone to 12, adding in a router and a switch which are most likely a single device for a small company, and a server or service for a server.

Table 3. Estimated time consumption on hardening the devices in a company with 5 employees. Estimates based on authors experience.

Device	Quantity	Time req. per unit	Total
Workstation	10	1h	7h
Smartphone	5	0.5h	2.5h
Router/Switch	1	3h	2h
Server	1	10h	5h

At the very least, a VPN connection would be required, firewall rules checked, update policy set and all the devices updated, password policy revised, end-point security set up and unnecessary user accounts and software removed. Documentation for the aforementioned would also be required.

A rough estimate of the time required to harden all the devices in an average company is displayed in table 2. Including updates, setting up backups, reviewing software, etc and taking into account that several workstations can be handled at once, the average time spent per machine would be an hour. The total time spent on revising every device and hardening it in a calm and methodical manner would therefore be 23.5h, or 3 full workdays. The average market price of a system administrators hourly charge in Estonia in 2017 is € 60/h, which would bring the total cost of hardening to € 1440 + VAT. This would be our baseline for further feasibility considerations, comparing it to losses to cybercrime.

An enquiry to an Estonian service provider for system administration and hardening services provided data to verify the estimated costs mentioned in the previous paragraph. According to Mr. Edik Must, a board member of Digifi Eesti OÜ, a company with 10 employees with a personal computer each, a router and a server with unknown number of services, would normally require between 20 to 30 hours of work, in case the company contacts for a one-time project to harden their devices. Standard services provided in such a case would include infrastructure mapping, hardening of devices and setting up access, as well as password policies, testing and documentation. Generally customers can expect a price tag of € 1000 to € 2000 for such a project, while the price would depend on the number and age of services used within the company, previous practices, but also the existence of appropriate infrastructure elements, such as a business grade router. (Must, 2018)

2.2 Survey results

A total of 40 responses were gathered, of which 1 was declared invalid and removed from the selection based on every possible answer given being negative and skipping as many answers as possible. 38 of the respondents had chosen to use the Estonian version of the questionnaire, while only one response was received to the questionnaire in English. The results in both languages were combined for the analysis and responses scored based on the logic described beforehand.

The geographical distribution between respondents matches the general trends of population distribution in Estonia. More than half of the respondents were from the capital county of Harju, while the second and third largest counties of Tartu and Pärnu provided 5 respondents each. The rest of the country seems to be rather under-represented though, with no responses from 7 out of 15 counties. Figure 1 displays the distribution of respondents by county.

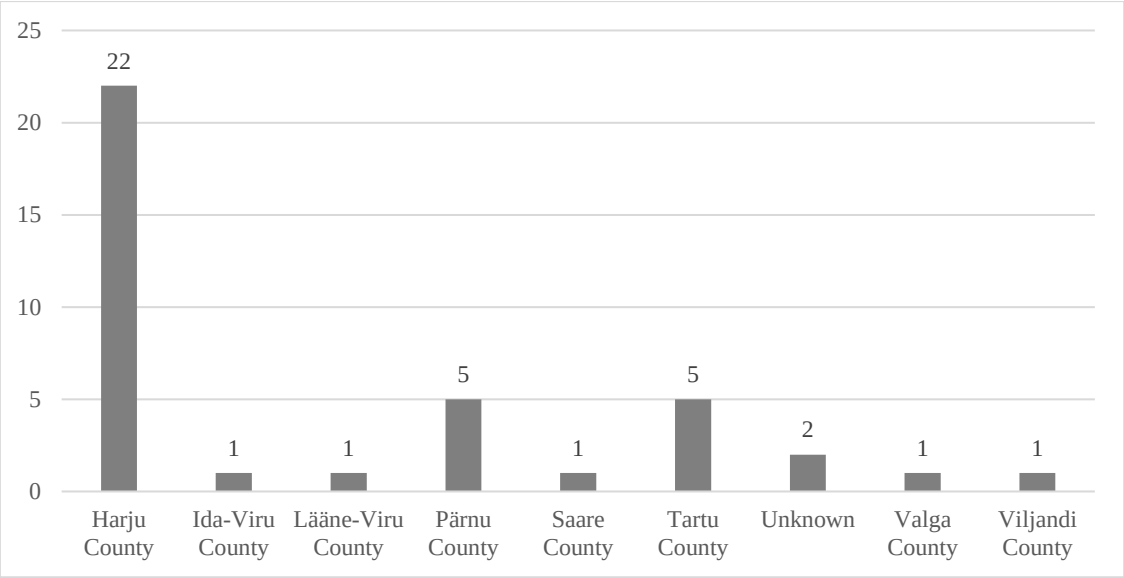

Figure 1. Count of respondents from each Estonian county. Source: Survey results

The distribution of respondents based on their main economic activity, defined by EMTAK 2008, is displayed on figure 2.

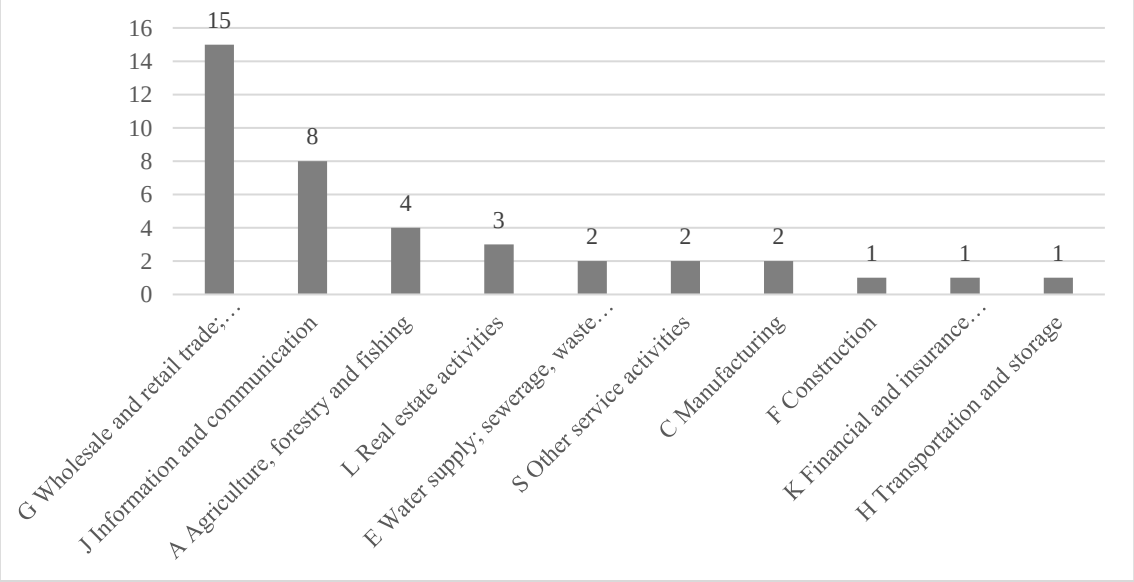

Figure 2. Count of respondents by main field of activity according to EMTAK 2008. Source: Survey results

Over a third of the respondents were active in wholesale and retail trade with 15 respondents, followed by Information and Communication activities with 8 respondents and Agriculture, forestry and fishing industry with 4 respondents.

Last of the descriptive data on respondents is the number of employees in their companies. Distribution of respondents based on the number of people employed is seen on the following figure.

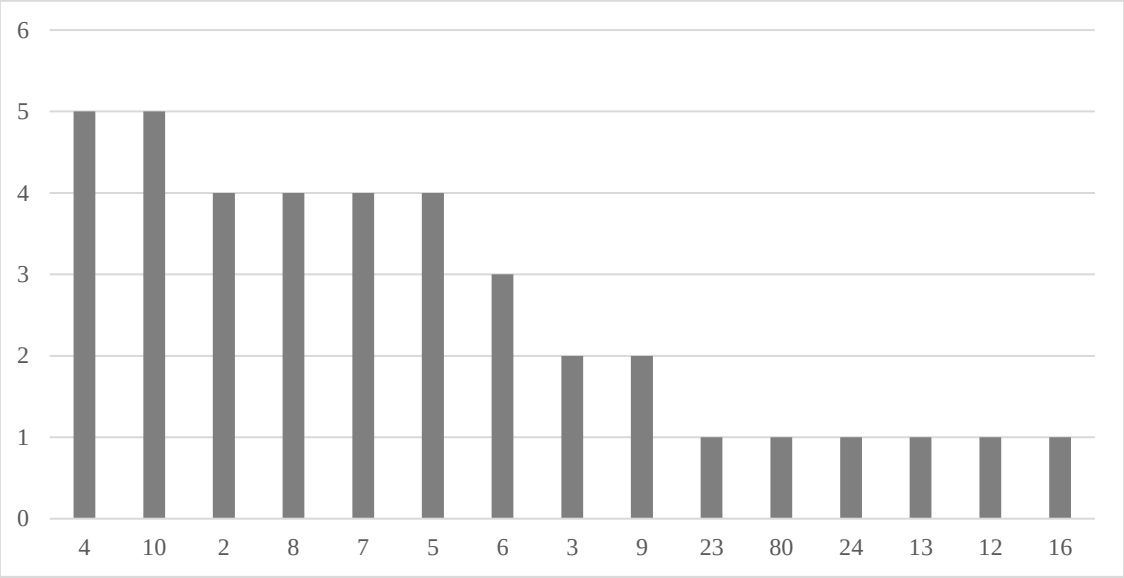

Figure 3. Count of respondents by number of employees in their companies.

As seen on figure 3 the majority of the respondents fell well within the target criteria of companies with less than 10 employees. That said, 6 respondents also originated from companies with a greater number of employees, with the largest one employing 80 people at the moment of responding to the questionnaire.

It is worth mentioning that a couple of companies also specifically asked for a permission to respond to the questionnaire despite employing more than 10 people. The argument for including them in the survey was enabling comparison of microbusinesses with companies that employ more resources, to determine whether the cause for the lack of security is mainly a question of general attitude towards cyber security, size or something else.

Authentication methods distribution was another aspect investigated by the survey. The time of gathering responses was merely a few months after the largest scandal involving Estonian ID-cards' vulnerability had become public. Other authentication methods were

not exposed to this particular threat. The question this raised, was if and how this had had an impact on the popularity and trust of the ID-cards (Estonian Information System Authority (RIA), 2017). Secondly, although bank-issued code cards have lost much of their usability due to limitations on the size of transactions possible, it was worth investing how common they were exactly. According to private media correspondent Aivar Pau (Pau, 2017), code cards are also subject to be removed from selection of available authentication methods with financial institutions by the end of 2019, after the approval of a change of legislation regarding entities that handle payments and e-money. (Parliament of Estonia, 2017)

Since using one authentication method does not rule out using another either for redundancy or simply various purposes within the company, several options could be chosen.

The following figure demonstrates the authentication methods used by the respondents.

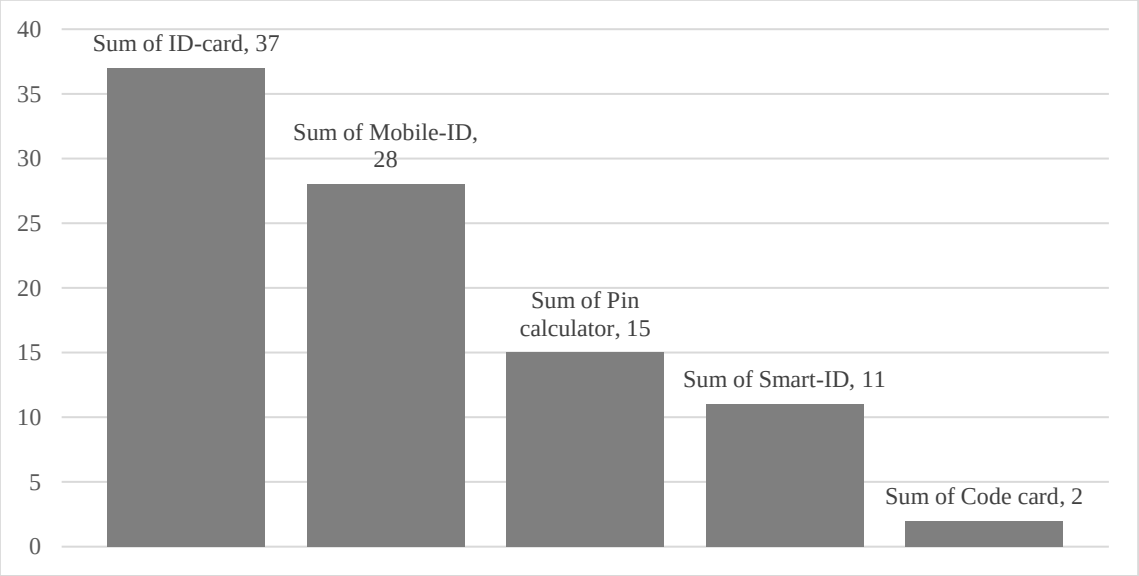

Figure 4. Count of authentication methods used by respondents, total. Source: Survey results.

Surprisingly, ID-card is the most commonly used method of authentication within the group of respondents, at 37 out of 39 respondents using this method to either authenticate or sign documents using it. Mobile-ID was the go-to suggestion by the Estonian authorities once the ID-card vulnerability was disclosed. Almost a third less of the respondents also use Mobile-ID. Pin-calculator is still popular, with slightly less than a third of the respondents claiming to use this method. Smart-ID, the newest addition to

authentication methods with banks and other major partners for Estonian microbusinesses, along with code cards, which are the oldest technology among the 5 options, are the least popular., with only 2 respondents using code cards and 11 Smart-ID.

2.3 Past Experiences with Cyber Crime

The survey also enquired about the respondents past experience with cybercrime, in order to find reasons for possible outcomes. Respondents were asked whether they had had ever been on the receiving end of a cybercrime and if so, how large were the damages approximately.

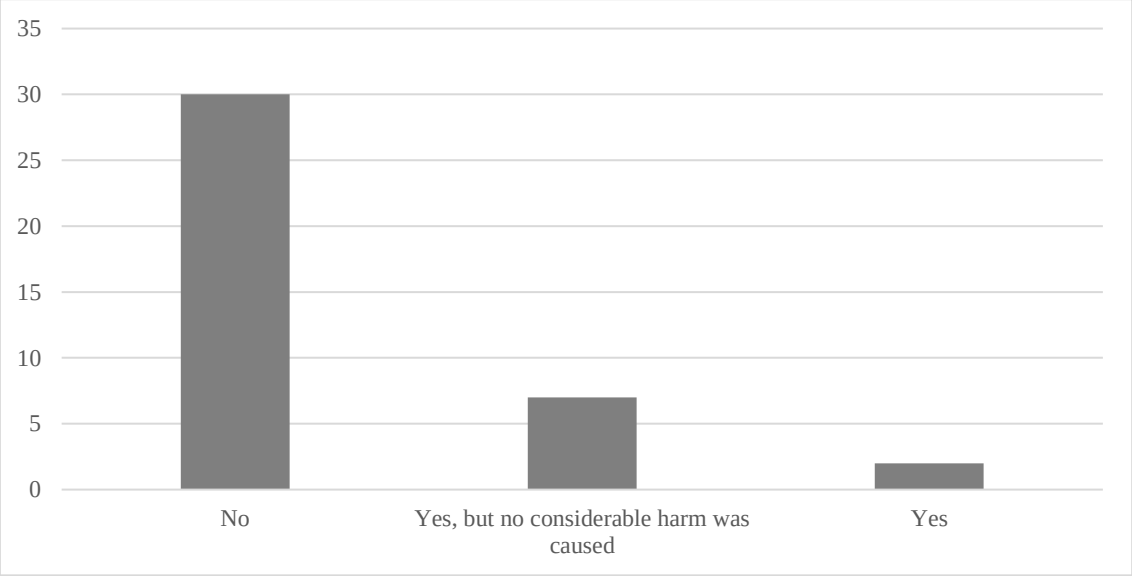

Figure 5. Respondents' distribution by past experiences with cybercrime.

A clear majority, three quarters, of the respondents claim to never have been affected by cybercrime, while 9 companies claim to have experienced some form of crime in the cyber domain. Only 2 of the companies claim to have suffered some form of damages because of a cybercrime, leaving the share of the companies hit by cybercrime at 5%.

Although the share of the respondents that have suffered from cybercrime is too small to be able to generalize these results on a larger scale, it is worth mentioning that one of the companies suffered damages in excess of € 5000, while the other considered the damages

remained under € 1000. It should be assumed that more companies have been affected, possibly without their knowledge, though.

Judging by types of incidents registered by the Estonian Information System Authority in 2016 (Estonian Information System Authority (RIA), 2017, p. 8), over half of the incidents are malware and botnet infections, which, for obvious reasons, are more complicated to notice than phishing or defacement attacks.

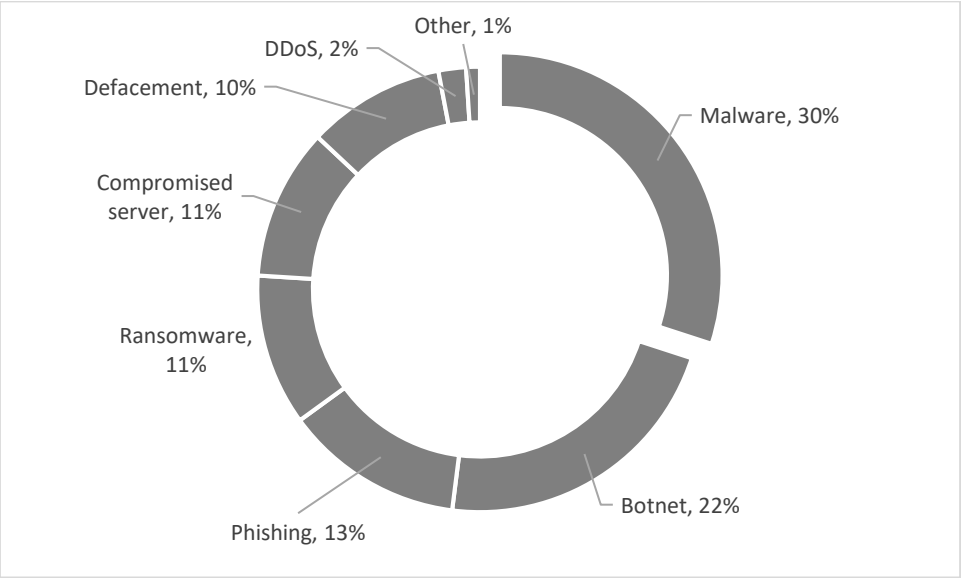

Figure 6. 2016 incidents by category. Source: Estonian Information System Authority (2017) "*Annual Cyber Security Assessment 2017"*, p. 8.

The last few questions in the general section focused on investigating whether the respondents' companies were trying to improve their cyber security level or not. Out of 39 respondents, 28 claimed they did use some methods to increase their cyber security, while 11 claimed they did not.

Figure 7. Responses to the question "Do you use any methods to increase cyber security?". Source: Survey results

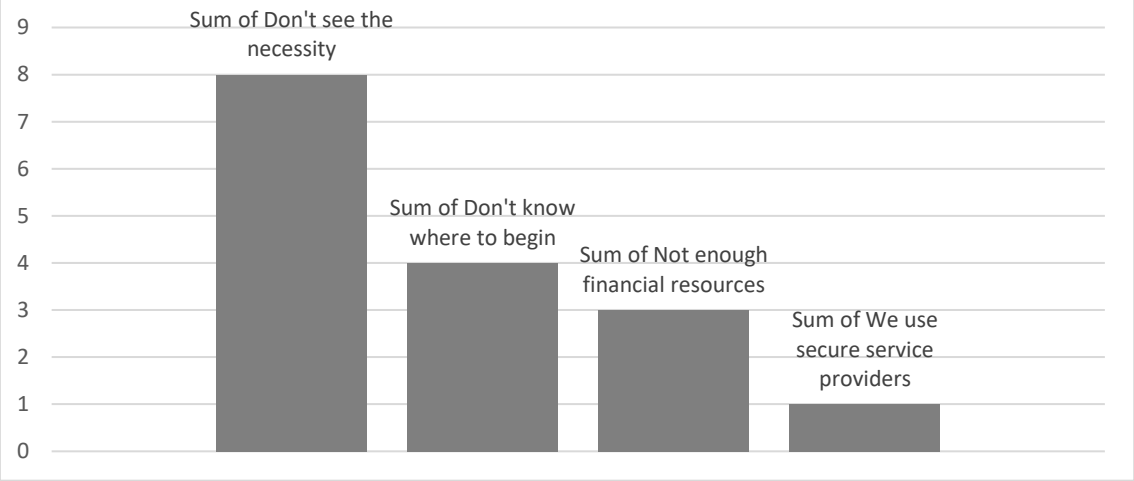

Figure 8. Reasons for not investing more into cyber security. Source: survey results

Before looking at the scores and overall performance of the companies, a quick glance can be taken at the reasons for not investing more into cyber security. Several reasons could be chosen in the questionnaire to give reasons for not investing more in cyber security. The majority claimed, they simply don't see the necessity in it, while 4 respondents claimed they don't know where to begin and 3 thought they didn't have enough financial resources.

2.4 Total scores

The different rankings were as seen on the table below.

Table 4. Difference of rankings of the responses. Comparison of standardized vs non-standardized sub-section scores.

Respondents No.	Total Score	Total Score without sub-section standardization	Ranking with Sub Section Standardized Scores	Ranking Based on Total Non-standardized Scores
1	**16.99**	186.67	30	30
2	**12.50**	117.50	36	36
3	**21.09**	224.17	28	28
4	**21.33**	226.67	27	27
5	**26.59**	263.33	22	22
6	**16.37**	146.67	32	35
7	**45.69**	482.50	1	1
8	**16.75**	181.67	31	31
9	**32.51**	334.17	13	13
10	**27.29**	282.50	19	21
11	**15.49**	150.00	34	34
12	**6.99**	81.67	37	37
13	**28.97**	291.67	18	18
14	**17.95**	197.50	29	29
15	**29.65**	285.00	17	19
16	**38.99**	395.00	5	5
17	**26.75**	301.67	20	17
18	**24.31**	240.00	25	26
19	**36.90**	370.83	7	9
20	**32.50**	335.00	14	12
21	**26.68**	284.17	21	20
22	**31.16**	326.67	15	15
23	**39.84**	406.67	3	4
24	**36.41**	368.33	9	10
25	**35.95**	364.17	10	11
26	**37.64**	390.00	6	6
27	**6.25**	65.00	38	38
28	**14.40**	150.83	35	33
29	**31.11**	307.50	16	16
30	**15.56**	157.50	33	32
31	**36.76**	378.33	8	7
32	**23.01**	250.83	26	25
33	**35.25**	371.67	11	8
34	**24.70**	259.17	23	23
35	**42.08**	437.50	2	2
36	**39.84**	419.17	3	3
37	**4.68**	40.83	39	39
38	**33.50**	328.33	12	14
39	**24.63**	256.67	24	24

Finally, the total scores were calculated using the sub scores for each section. The sub scores and total scores for all the respondents are seen in Appendix 2.

The average scores for each sub section are also noteworthy. The maximum score for each sub section is 10. The radar chart in figure 9 depicts an overall picture of how Estonian companies fared in the survey. Access control seems to receive the highest amount of attention among companies, while ensuring the security of configurations receives the least. Despite firewalls being completely disregarded by 28% of the respondents, the companies that use firewalls bring the average up significantly, to 5,2 points out of the maximum 10.

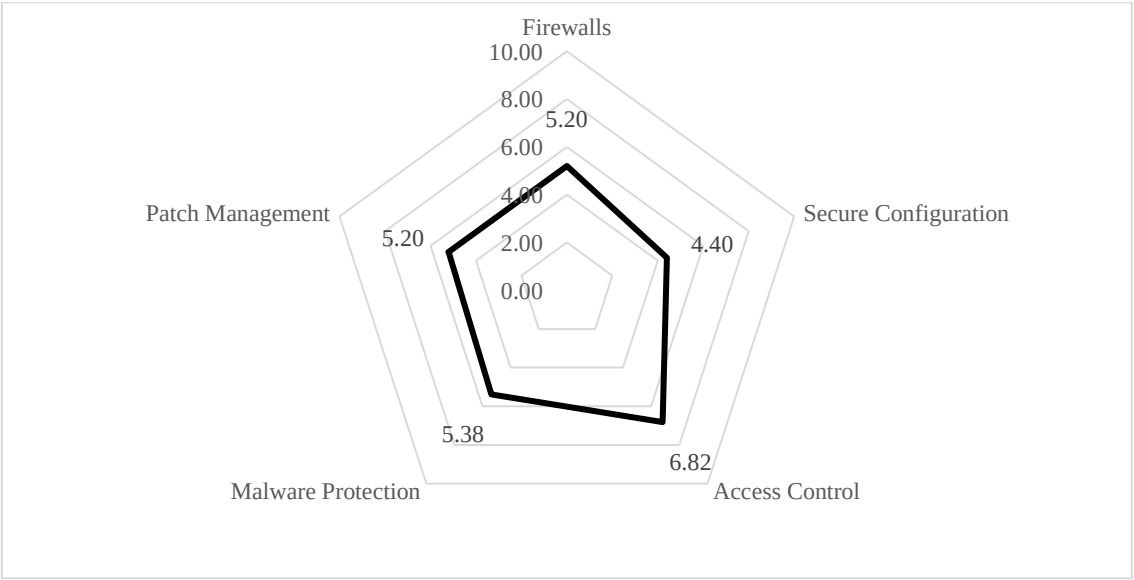

Figure 9. Overall average scores for all respondents for each sub section.

The overall average score among respondents to this particular study was 27 points out of the maximum of 50. In other words, a 54% achievement rate on the survey, which can be considered a barely passing achievement. An 80% improvement of the current score is theoretically possible, by implementing CE on a mandatory scale, along with internal and external vulnerability scans. An 80% improvement to the currently achieved score would have to bring the average score to 48.6 points. It would, however, prove to be of considerable cost to the micro-businesses, at € 1000 - € 2000 per company. The benefit

would be reducing the 5% margin of companies that have suffered from considerable damages by a cyber-attack.

The downside of making such a framework mandatory would be focusing heavily on the current controls, while sacrificing flexibility to react to new threats that are likely frontrunners compared to the framework control mechanisms.

It is apparent that making Cyber Essentials mandatory in Estonia would be unlikely to increase the overall performance score by 80%. Nor is it possible that by fixing only 20% of the questions in the questionnaire would be sufficient to improve the score by 80%, given the scoring system developed for this instance.

The Estonian ID-card and X-road solutions prove a rare level of security for companies and individuals alike, apparent already by the lack of such questions from the original version of the Cyber Essentials questionnaire. Since the questionnaire did not explicitly touch on the topic of authentication methods used by companies, further enforcing one authentication method over another would accomplish very little within this framework.

The cost-analysis proves the cost of increasing the cyber security of a company as a one-time project is, in fact, reasonable. It would therefore be advisable to microbusinesses to make this investment.

2.4 Descriptive data of respondents.

First, it is worth investigating whether there's a specific trend among sectors and their average score on the Cyber Essentials scheme.

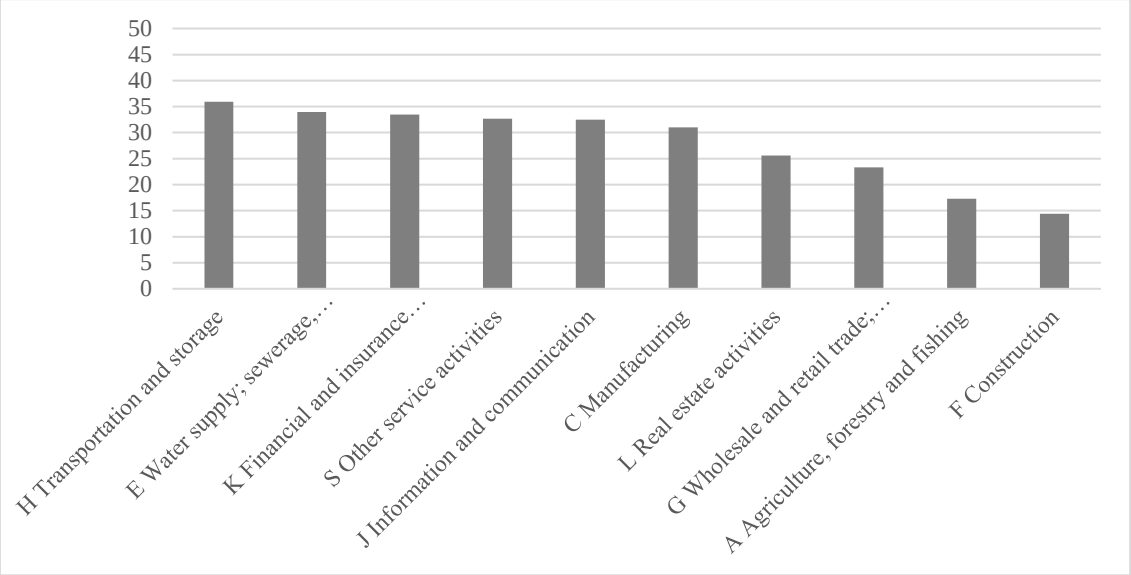

Figure 10. Average scores on the Cyber Essentials scheme by main field of activity. Source: Survey results.

The graph above depicts the average scores of the respondents by field of activity. The absolute maximum score for the questionnaire would have been 50, which remained unreachable for any of the respondents. 2 companies reached a score of over 40 points, 14 companies scored between 30 and 40 points, the next 12 companies scored between 20 and 30 points, and 11 companies scored below 20 points, 3 of which scored below 10 points.

The highest scoring companies belonged to Manufacturing and Information and Communication sectors, as seen in the raw data table in Appendix 2. However, the highest average scores by sectors were received by Transportation and storage and Water Supply sectors. The fact the highest scoring individual companies did not end up in the highest scoring sectors average raises questions though. As a first impulse, perhaps companies with less employees that also belong in these sectors, brought the average score down for others in the same sectors. Due to the small number of respondents, this can be verified

with descriptive statistics, by studying the average scores by number of employees in the companies.

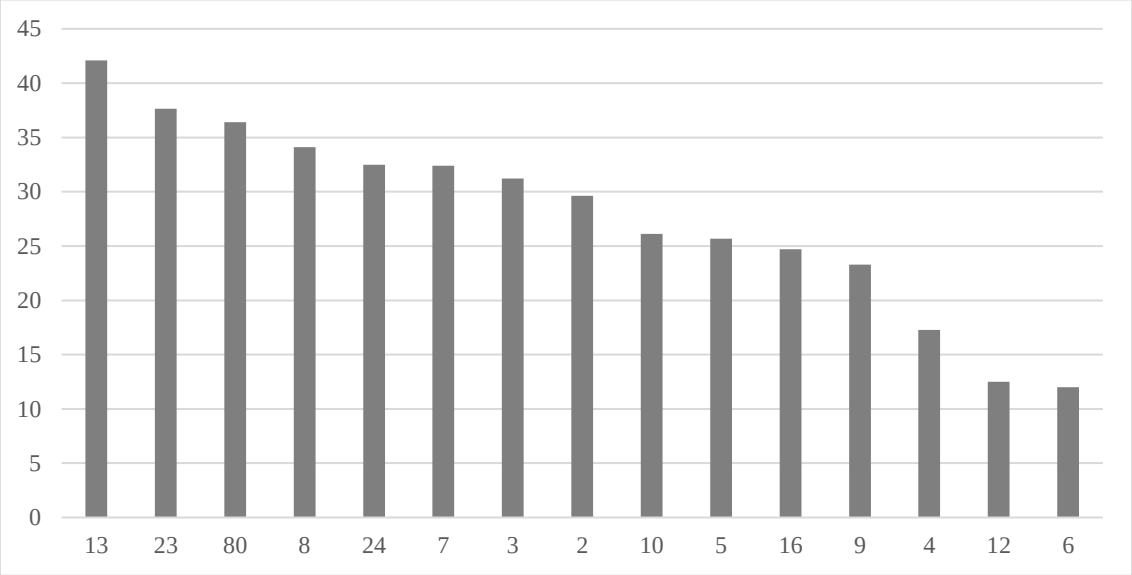

Figure 11. Average scores based on the number of employees in the company. Average scores presented on the Y-axis, number of employees presented on the X-axis.

The graph above presents data on the average scores on the Cyber Essentials questionnaire based on the number of employees in the companies. The fact that the average scores for companies with 13 and 12 employees, as well as companies with 8 and 6 employees, are at the opposite sides of the spectrum makes it apparent that this is an unreliable indicator for future predictions. Looking at the number of companies in the

2.5 Sub scores for firewalls

A score of 40 points would equal completely disregarding one of the 5 sections, such as Firewalls, and is therefore worrying. The firewalls section received, in fact, the highest number of responses that had completely ignored every aspect of this security control and received a score of 0 for the whole section thereafter. 11 out of 39, or 28% of the respondents received no score for this sub section.

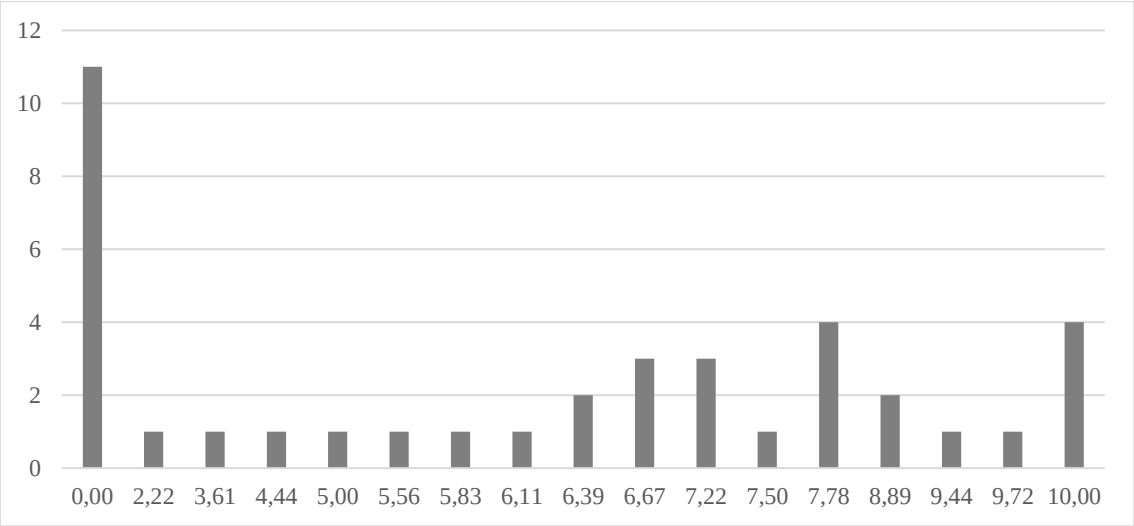

Figure 12. Distribution of scores for the Firewall section in the survey.

The following graph describes the average scores received for each question within the firewalls section. The majority of respondents had a firewall in place on the boundary of the network and the default administrative password changed on the device, according to the first 2 questions. The lowest scores were received by questions No. 6 and 7. Firewall rules are not frequently reviewed and computers rarely prevented from initiation connections when they don’t need to among the respondents.

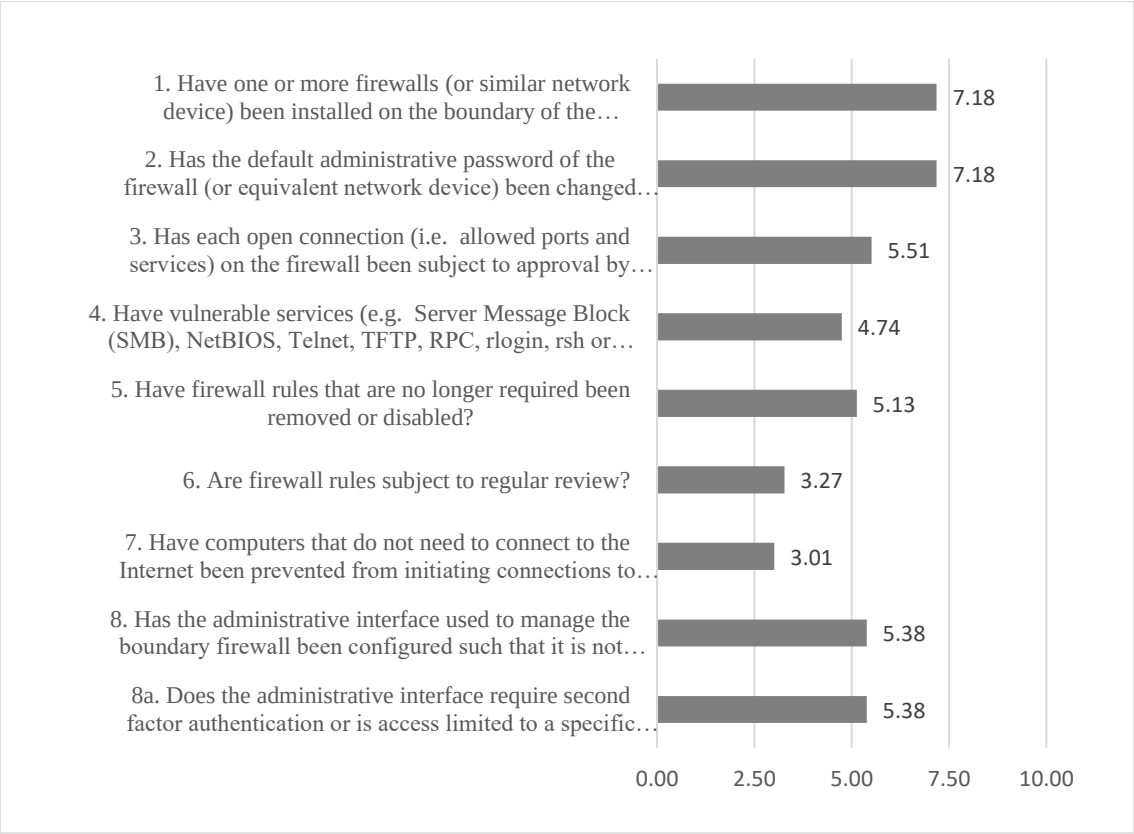

Figure 13. Average scores for each question on the firewall section in the survey.

2.6 Sub scores for Secure Configuration

The overall average score for the secure configuration section was 4.4 out of maximum of 10, which made it the lowest average aspect among the companies that responded. Looking at the individual test scores more closely, the lowest scores were produced by questions No. 25, “Is a Mobile Device Management solution in place for hardening and controlling all mobile platforms in use within the organisation?” (average score of 0.72), question No. 21 “Are log files retained for operating systems on both servers and workstations?” (average score of 1.97) and question No. 26 “Remote (Internet) access to commercially or personal sensitive data and critical information requires authentication.” (average score of 2.11).

This is not unexpected, however, as it is common for companies to not provide smart phones for their employees and therefore lack the ad hock responsibility for maintaining them. As a minimum requirement, a certificate requirement should be in place for smart devices that provide access to company e-mail.

A few of the questions listed in the secure configuration section suggest improving cyber security levels through limiting users' free access to the Internet and/or privacy, such as questions No. 18 and 22. Discussion on the effect of these questions on end-users would be an interesting one, but unfortunately out of scope for this survey.

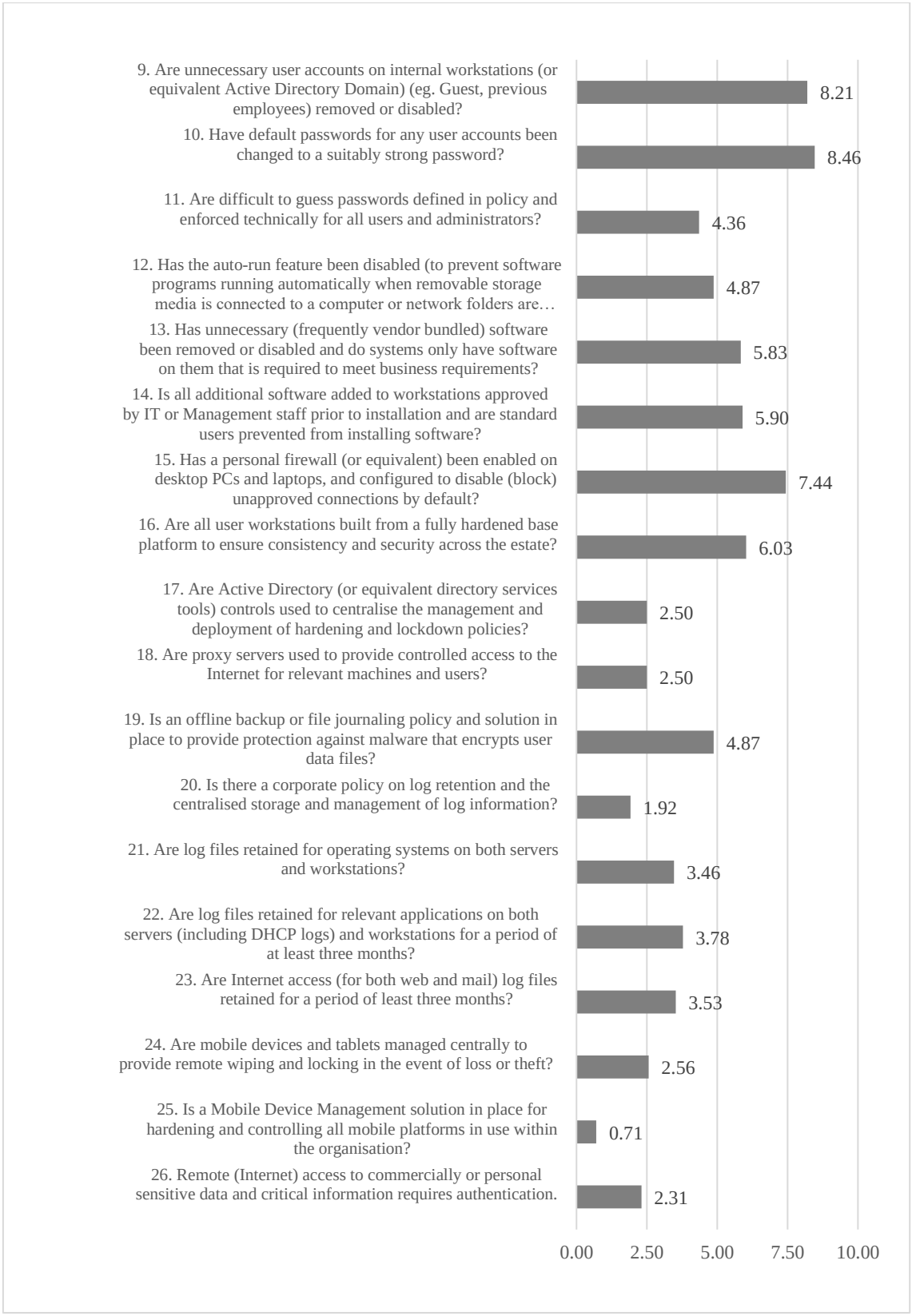

Figure 14. Average scores for each question on the secure configuration sub section

Looking at descriptive statistics, who was more likely to score higher in the Secure Configuration sub-category, no clear indicators could be found that would be reliable. No clear distinction could be found between high-scorers and low-performers, as the possible answers to number of employees, county, main field of activity are all found on both ends of the spectrum.

2.7 Access Control

The average score for the access control sub-section of the survey was the highest of the sub-sectors, at 6.82 points. Not even one respondent received 0 points for this section and 24 of the 39 respondents received 7 points or more for the subsection, equalling fulfilling 70% of the answers with the best qualifications possible. The highest scoring question in the whole survey belongs to this sub-section – "Are system administrative access privileges restricted to a limited number of authorised individuals?" with an average of 8.78 points. This can be attributed to not necessarily deliberately focusing on increasing cyber security against outside threats, but against inside threats, both deliberate and accidental.

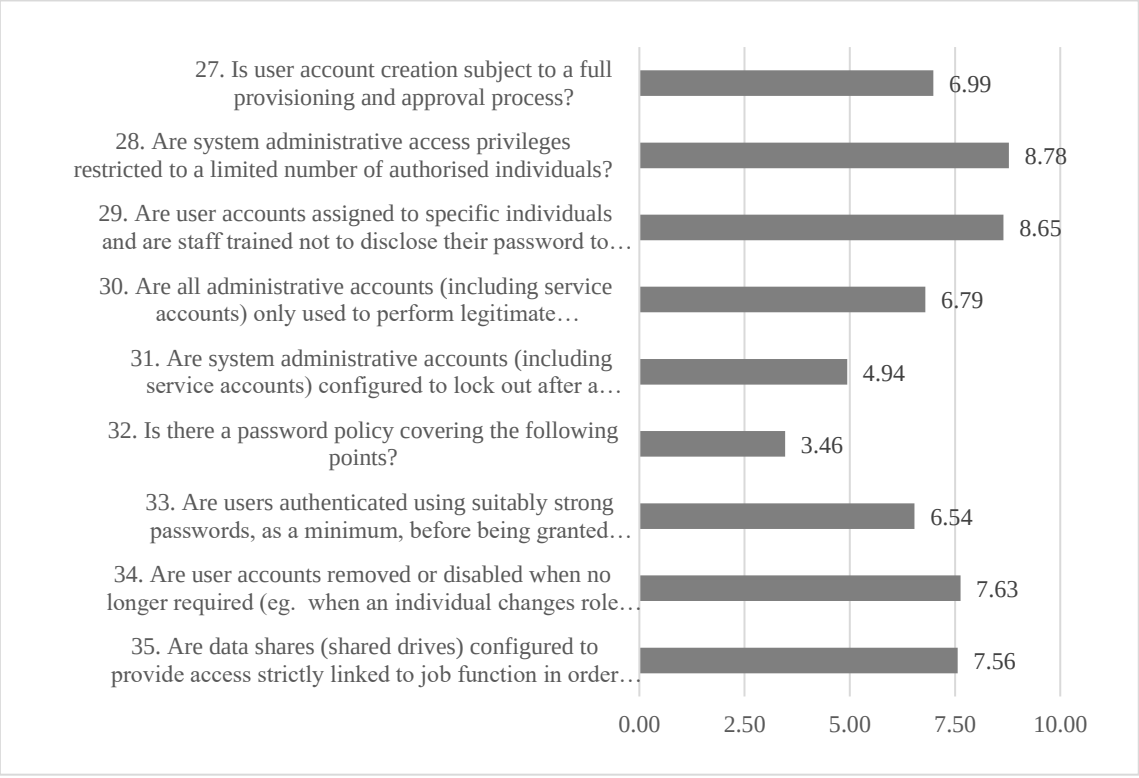

Figure 15. Average scores for each question on the access control sub section of the survey.

2.8 Malware Protection

The fourth section of the survey touched on the practices used to protect against malware within the companies. The results in this section are seen as mostly positive of the Estonian companies.

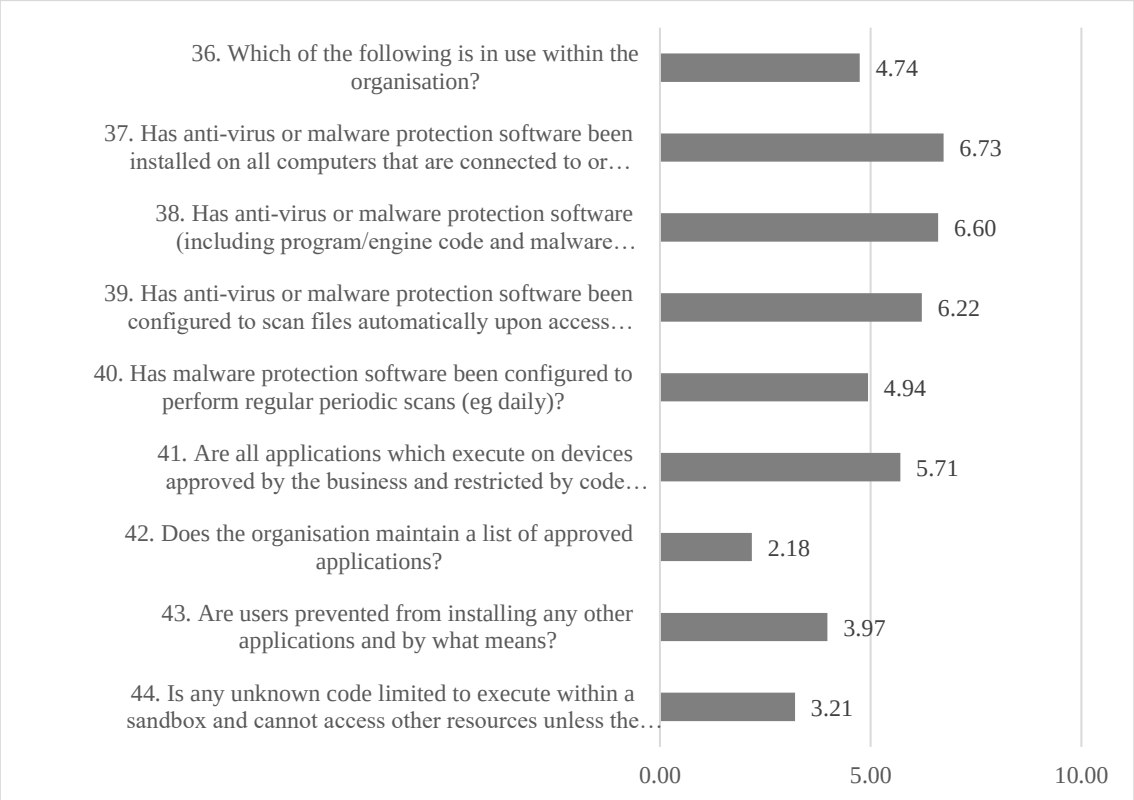

Figure 16. Average scores for each question on the malware protection sub section

Although the average score for question No. 36 was 4.74, the majority of respondents claimed to either have anti-virus of malware protection software in place, using whitelisting of applications or sandboxing. Only 5 respondents claimed not to have any of these controls in place, while 29 (or 74%) claimed to have anti-virus or malware protection software used within the organization. This is an indication of these tools being perceived as somewhat mandatory. The question for future surveys would be determining the difference in present threats and which tools would be more effective – signature based anti-virus software, vs endpoint security packages that rely on active monitoring.

2.9 Patch management

The last section to be covered within the CREST questionnaire was patch management, which ranges from platform-dependant updates to performing security vulnerability scans periodically. Unexpectedly the highest scores in the section were received by questions No. 45 and 46, which are the easiest requirements to fulfil. Also unexpectedly, questions No. 50, 51 and 52 received the lowest scores. Tablets have provided little use within most office environments and therefore generally unpopular in number compared to smartphones, laptops or desktop PC-s. Both internal and external network vulnerability scans are also expectedly rare, seeing as they can be costly for SME-s and microbusinesses. These questions relate well with the Cyber Essentials Scheme used in the UK, where external and internal scans are part of the certification. Internal network vulnerability scans are part of the more advanced certificate to receive Cyber Essentials Plus certificate.

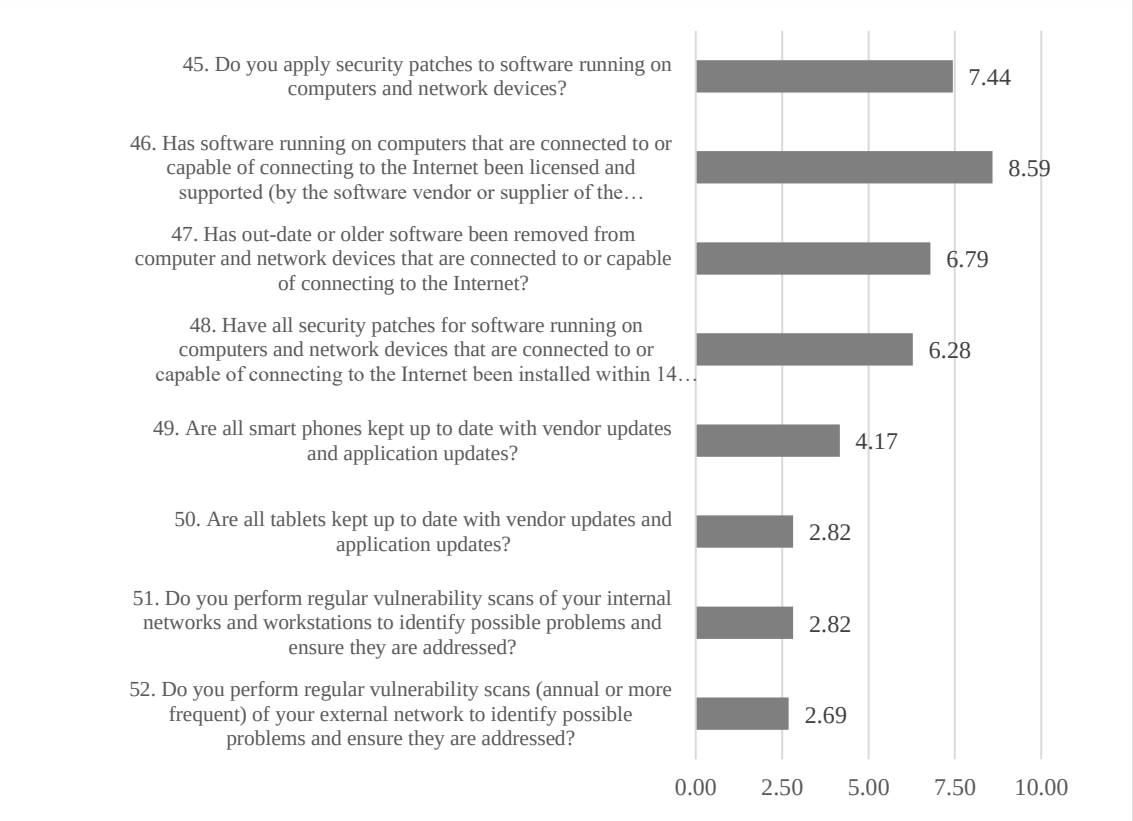

Figure 17. Average scores for each question on the patch management sub section.

3 Summary

The thesis focused on studying the level of cyber security among Estonian SME-s, with priority set on microbusinesses with up to 10 employees. Key aspects of the study included translating the questionnaire to Estonian, finding a way to deliver the study to respondents, coming up with a scoring system, analysing the results and comparing the cost-benefit ratio to hardening of systems.

Chapter 1 focused on the methodology of the study and preparation, as well as limitations. All of the limitations proved to be correctly assumed – far less companies responded to the questionnaire than anticipated – around 1% rather than the anticipated minimum of 5%. Comparable statistics were unavailable, as the Estonian Information System Authority keeps statistics on the type of attacks, rather than attack vectors or point-of-entries.

Chapter 2 described the unexpected and expected findings based on the questionnaire. Surprisingly, almost half of the respondents claimed to not use any kind of network boundary firewall whatsoever. At least a quarter of the Estonian micro-businesses are extremely vulnerable to a cyber-attack of any kind.

A mandatory cyber security scheme, such as Cyber Essentials, would greatly improve the safety of the micro-businesses, but at the same time also make it far more complicated to start and run a company in Estonia. A further distinction between micro-businesses based on size should be made in case either Cyber Essentials or a similar scheme was to be made mandatory country-wide for small or medium-sized enterprises. The distinction should not be made based on the number of employees solely, but also take into consideration the number of workstations and complexity of the IT-infrastructure within the company. An accounting company with 2 employees is unlikely to require the same amount of security as a web-hosting company with 1 employee and 3 servers. The control mechanisms that would enforce such a mandatory framework would be a challenge to say the least.

Companies received the lowest average score of the 5 sub-sections in the survey for the next section – secure configuration. The secure configuration section encompassed the largest number of questions, which made achieving the maximum score comparatively

more difficult in this section than in others. The lowest scores were received by questions regarding mobile device management (0.71 points on average), log policy (1.92 points), using proxy servers (2.5 points) and using directory services for centralised hardening and management activities. An argument can be made that these aspects are all more relevant for companies with more employees than 10 and therefore the low scores are not surprising. On the other hand the highest scoring question also belonged to this particular sub-section, checking for respondents habits of changing default passwords.

Results for user access control subsection – third in the questionnaire – proved to be a positive surprise. The average score was 6.82 out of the maximum of 10 points. An explanation for this can be that companies are more worried about internal threats than external, therefore focusing on limiting employee's access before worrying about a boundary firewall.

As described in the chapter on methodology, the malware protection sub-section hides flawed logic, which should be addressed in future studies. That said, majority of responses reflected using at least anti-virus software, with several also stating the use of application whitelisting and sandboxing.

Last but not least, patch management section proved most of the companies are using legitimate software and are regularly updating their devices, although not with a meticulous religion.

4 References

CREST. (2017). *Cyber Essentials* . Retrieved 09 15, 2017, from Cyber Essentials: http://www.cyberessentials.org/system/resources/W1siZiIsIjIwMTcvMDkvMTUvMDdfMjBfMTNfMzg4X0NSRVNUX0N5YmVyX0Vzc2VudGlhbHNfUXVlc3Rpb25uYWlyZV92My4xLnBkZiJdXQ/CREST%20Cyber%20Essentials%20Questionnaire%20v3.1.pdf

Estonian Information System Authority. (2017). *Annual Cyber Security Assessment 2017.* Retrieved from Republic of Estonia - Information System Authority: https://www.ria.ee/public/Kuberturvalisus/RIA_CSA_2017.PDF

Estonian Information System Authority. (2017, 06). *ISKE Portaal*. Retrieved 01 02, 2018, from ISKE Portaal: https://iske.ria.ee/8_03

Ministry of Economic Affairs - Republic of Estonia. (2017, 12 13). *Eelnõude infosüsteem.* Retrieved 01 02, 2018, from Kooskõlastamiseks esitatud eelnõud: http://eelnoud.valitsus.ee/main/mount/docList/775b7e36-09e2-480f-9217-81fb79ed293b?activity=3#fEOZX1JB

Must, E. (2018, 01 02). Mr. (J. Kaalep, Interviewer)

Rhodes, C. (2017). *Business statistics.* London: House of Commons Library. Retrieved 12 1, 2017, from https://www.google.ee/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwiEoveBxenXAhVkEpoKHfeMBIIQFggnMAA&url=http%3A%2F%2Fresearchbriefings.files.parliament.uk%2Fdocuments%2FSN06152%2FSN06152.pdf&usg=AOvVaw2y6Z0G3REThCb261Q4nyMJ

Statistics Estonia. (2017, 04 11). *Statistics Estonia*. Retrieved from FS025: ENTERPRISES' EMPLOYMENT AND HOURS WORKED by Year, Economic activity (EMTAK 2008), Number of persons employed and Indicator: https://tinyurl.com/ycfo4hzd

Appendix 1 – Cyber Essentials Scheme Questionnaire in English

The questionnaire below is mainly based on CREST Cyber Essentials Questionnaire v3.1, with minor tweaks to response options and additional questions added in the General information section.

4.2.1 General information

This information will be used to try and find common identifiers between company locations, number of employees. field of activity and cyber security practices.

Main field of activity of the company (EMTAK)

A Agriculture, forestry and fishing

B Mining and quarrying

C Manufacturing

D Electricity, gas, steam and air conditioning supply

E Water supply; sewerage, waste management and remediation activities

F Construction

G Wholesale and retail trade; repair of motor vehicles and motorcycles

H Transportation and storage

I Accommodation and food service activities

J Information and communication

K Financial and insurance activities

L Real estate activities

M Professional, scientific and technical activities

N Administrative and support service activities

O Public administration and defence; compulsory social security

P Education

Q Human health and social work activities

R Arts, entertainment and recreation

S Other service activities

T Activities of households as employers; undifferentiated goods and services producing activities for households for own use

U Activities of extraterritorial organisations and bodies

Which county is the main place of activity of the company?

Harju County

Hiiu County

Ida-Viru County

Jõgeva County

Järva County

Lääne County

Lääne-Viru County

Põlva County

Pärnu County

Rapla County

Saare County

Tartu County

Valga County

Viljandi County

Võru County

Number of employees in the company?

Short answer text

Which authentication methods do you use for business practices, including log-ins and signing of documents?

ID-card

Mobile-ID

Smart-ID

Pin-calculator

Code card

Has Your company ever fallen a victim of a cyber crime?

Yes

Yes, but no considerable harm was detected

No

How big were the estimated damages?

Less than € 1000

Between € 1000 and € 2000

Between € 2000 and € 5000

More than € 5000

Do you use any methods to increase cyber security?

Yes

No

What are the main reasons for not investing more in cyber security?

Don't really know where to begin

Don't really see the necessity

Not enough financial resources

Other…

4.2.2 Boundary firewalls and Internet Gateways

1. Have one or more firewalls (or similar network device) been installed on the boundary of the organisation’s internal network(s)?

Yes

No

No firewall present

2. Has the default administrative password of the firewall (or equivalent network device) been changed to an alternative difficult to guess password?

Yes

No

3. Has each open connection (i.e. allowed ports and services) on the firewall been subject to approval by an authorised business representative and documented (including an explanation of business need)?

Yes always

In most cases

Sometimes

Rarely

Never

4. Have vulnerable services (e.g. Server Message Block (SMB), NetBIOS, Telnet, TFTP, RPC, rlogin, rsh or rexec) been disabled (blocked) by default and those that are allowed have a business justification?

Yes always

In most cases

Sometimes

Rarely

Never

5. Have firewall rules that are no longer required been removed or disabled?

Yes

No

6. Are firewall rules subject to regular review?

Yes

No

7. Have computers that do not need to connect to the Internet been prevented from initiating connections to the Internet (Default deny)?

Yes

No

8. Has the administrative interface used to manage the boundary firewall been configured such that it is not accessible from the Internet?

Yes

No

8a. Does the administrative interface require second factor authentication or is access limited to a specific address?

Yes

No

4.2.3 Secure configuration

9. Are unnecessary user accounts on internal workstations (or equivalent Active Directory Domain) (eg. Guest, previous employees) removed or disabled?

Yes always

In most cases

Sometimes

Rarely

Never

10. Have default passwords for any user accounts been changed to a suitably strong password?

Yes always

In most cases

Sometimes

Rarely

Never

11. Are difficult to guess passwords defined in policy and enforced technically for all users and administrators?

Yes always

In most cases

Sometimes

Rarely

12. Has the auto-run feature been disabled (to prevent software programs running automatically when removable storage media is connected to a computer or network folders are mounted)?

Yes always

In most cases

Sometimes

Rarely

Never

13. Has unnecessary (frequently vendor bundled) software been removed or disabled and do systems only have software on them that is required to meet business requirements?

Yes always

In most cases

Sometimes

Rarely

Never

14. Is all additional software added to workstations approved by IT or Management staff prior to installation and are standard users prevented from installing software?

Yes always

In most cases

Sometimes

Rarely

Never

15. Has a personal firewall (or equivalent) been enabled on desktop PCs and laptops, and configured to disable (block) unapproved connections by default?

Yes always

In most cases

Sometimes

Rarely

Never

16. Are all user workstations built from a fully hardened base platform to ensure consistency and security across the estate?

Yes always

In most cases

Sometimes

Rarely

Never

17. Are Active Directory (or equivalent directory services tools) controls used to centralise the management and deployment of hardening and lockdown policies?

Yes always

In most cases

Sometimes

Rarely

Never

18. Are proxy servers used to provide controlled access to the Internet for relevant machines and users?

Yes always

In most cases

Sometimes

Rarely

Never

19. Is an offline backup or file journaling policy and solution in place to provide protection against malware that encrypts user data files?

Yes always

No

20. Is there a corporate policy on log retention and the centralised storage and management of log information?

Yes always

In most cases

No

21. Are log files retained for operating systems on both servers and workstations?

Yes always

In most cases

Sometimes

Rarely

Never

22. Are log files retained for relevant applications on both servers (including DHCP logs) and workstations for a period of at least three months?

Yes always

In most cases

Sometimes

Rarely

Never

23. Are Internet access (for both web and mail) log files retained for a period of least three months?

Yes always

In most cases

Sometimes

Rarely

Never

24. Are mobile devices and tablets managed centrally to provide remote wiping and locking in the event of loss or theft?

Yes always

For most devices

Sometimes

Rarely

Never

N/A

25. Is a Mobile Device Management solution in place for hardening and controlling all mobile platforms in use within the organisation?

Yes always

For most devices

Sometimes

Rarely

Never

N/A

26. Remote (Internet) access to commercially or personal sensitive data and critical information requires authentication.

Yes

No

4.2.4 Access control

27. Is user account creation subject to a full provisioning and approval process?

Yes always

In most cases

Sometimes

Rarely

Never

28. Are system administrative access privileges restricted to a limited number of authorised individuals?

Yes always

In most cases

Sometimes

Rarely

Never

29. Are user accounts assigned to specific individuals and are staff trained not to disclose their password to anyone?

Yes always

In most cases

Sometimes

Rarely

Never

30. Are all administrative accounts (including service accounts) only used to perform legitimate administrative activities, with no access granted to external email or the Internet?

Yes always

In most cases

Sometimes

Rarely

Never

31. Are system administrative accounts (including service accounts) configured to lock out after a number of unsuccessful attempts?

3 Failures

6 Failures

10 Failures

>10 Failures

Never

32. Is there a password policy covering the following points?

a. How to avoid choosing obvious passwords (such as those based on easily-discoverable information).

b. Not to choose common passwords (use of technical means, using a password blacklist recommended).

c. No password reuse.

d. Where and how they may record passwords to store and retrieve them securely.

e. If password management software is allowed, if so, which.

f. Which passwords they really must memorise and not record anywhere.

33. Are users authenticated using suitably strong passwords, as a minimum, before being granted access to applications and computers?

Yes always

In most cases

Sometimes

Rarely

Never

34. Are user accounts removed or disabled when no longer required (eg. when an individual changes role or leaves the organisation) or after a predefined period of inactivity (eg. 3 months)?

Yes always

In most cases

Sometimes

Rarely

Never

35. Are data shares (shared drives) configured to provide access strictly linked to job function in order to maintain the security of information held within sensitive business functions such as HR and Finance?

Yes always

In most cases

Sometimes

Rarely

Never

4.2.5 Malware protection

36. Which of the following is in use within the organisation?

a. Anti-virus or Malware protection

b. Application whitelisting

c. Application Sandboxing

d. None of the above

37. Has anti-virus or malware protection software been installed on all computers that are connected to or capable of connecting to the Internet?

Yes always

In most cases

Sometimes

Rarely

Never

38. Has anti-virus or malware protection software (including program/engine code and malware signature files) been kept up-to-date (either by configuring it to update automatically or through the use of centrally managed service)?

Yes always

In most cases

Sometimes

Rarely

Never

39. Has anti-virus or malware protection software been configured to scan files automatically upon access (including when downloading and opening files, accessing files on removable storage media or a network folder) and scan web pages when accessed (via a web browser)?

Yes always

In most cases

Sometimes

Rarely

Never

40. Has malware protection software been configured to perform regular periodic scans (eg daily)?

Yes always

In most cases

Sometimes

Rarely

Never

41. Are all applications which execute on devices approved by the business and restricted by code signing or other protection mechanisms?

Yes always

In most cases

Sometimes

Rarely

Never

42. Does the organisation maintain a list of approved applications?

Yes

No

43. Are users prevented from installing any other applications and by what means?

Yes

No

44. Is any unknown code limited to execute within a sandbox and cannot access other resources unless the user grants explicit permission?

Yes

No

4.2.6 Patch management

45. Do you apply security patches to software running on computers and network devices?

Yes always

In most cases

Sometimes

Rarely

Never

46. Has software running on computers that are connected to or capable of connecting to the Internet been licensed and supported (by the software vendor or supplier of the software) to ensure security patches for known vulnerabilities are made available?

Yes always

In most cases

Sometimes

Rarely

Never

47. Has out-date or older software been removed from computer and network devices that are connected to or capable of connecting to the Internet?

Yes always

In most cases

Sometimes

Rarely

Never

48. Have all security patches for software running on computers and network devices that are connected to or capable of connecting to the Internet been installed within 14 days of release or automatically when they become available from vendors?

Yes always

In most cases

Sometimes

Rarely

Never

49. Are all smart phones kept up to date with vendor updates and application updates?

Yes always

In most cases

Sometimes

Rarely

No updates available

N/A

50. Are all tablets kept up to date with vendor updates and application updates?

Yes always

In most cases

Sometimes

Rarely

No updates available

N/A

51. Do you perform regular vulnerability scans of your internal networks and workstations to identify possible problems and ensure they are addressed?

Yes always

In most cases

Sometimes

Rarely

No

52. Do you perform regular vulnerability scans (annual or more frequent) of your external network to identify possible problems and ensure they are addressed?

Yes always

In most cases

Sometimes

Rarely

Appendix 2 - Cyber Essentials Scheme Questionnaire in Estonian

4.2.7 Üldine info

Selle info abil on loodetavasti võimalik leida seoseid või erinevusi piirkondade, ettevõtte suuruse ning tegevusala osas seoses küberturvalisusega.

Ettevõtte peamine tegevusala (EMTAK)

A Põllumajandus, metsamajandus ja kalapüük

B Mäetööstus

C Töötlev tööstus

D Elektrienergia, gaasi, auru ja konditsioneeritud õhuga varustamine

E Veevarustus; kanalisatsioon, jäätme- ja saastekäitlus

F Ehitus

G Hulgi- ja jaekaubandus; mootorsõidukite ja mootorrataste remont

H Veondus ja laondus

I Majutus ja toitlustus

J Info ja side

K Finants- ja kindlustustegevus

L Kinnisvaraalane tegevus

M Kutse-, teadus- ja tehnikaalane tegevus

N Haldus- ja abitegevused

O Avalik haldus ja riigikaitse; kohustuslik sotsiaalkindlustus

P Haridus

Q Tervishoid ja sotsiaalhoolekanne

R Kunst, meelelahutus ja vaba aeg

S Muud teenindavad tegevused

T Kodumajapidamiste kui tööandjate tegevus; kodumajapidamiste oma tarbeks mõeldud eristamata kaupade tootmine ja teenuste osutamine

U Eksterritoriaalsete organisatsioonide ja üksuste tegevus

Millises maakonnas ettevõte peamiselt tegutseb?

Harju maakond

Hiiu maakond

Ida-Viru maakond

Järva maakond

Jõgeva maakond

Lääne maakond

Lääne-Viru maakond

Pärnu maakond

Põlva maakond

Rapla maakond

Saare maakond

Tartu maakond

Valga maakond

Viljandi maakond

Võru maakond

Töötajate arv ettevõttes?

Short answer text

Milliseid autentimisvahendeid kasutate äritegevuses vajalikuks suhtluseks, sh sisselogimisteks ja allkirjastamiseks?

ID-kaart

Mobiil-ID

Smart-ID

Pin-kalkulaator

Koodikaart

Kas Teie ettevõte on kunagi sattunud küberkuriteo ohvriks?

Jah

Jah, aga mingeid kahjusid ei kaasnenud

Ei

Kui suur oli umbes tekitatud kahju?

Vähem kui € 1000

Vahemikus € 1000 ja € 2000

Vahemikus € 2000 ja € 5000

Üle € 5000

Kas rakendate küberturvalisuse tõstmiseks mingeid meetmeid?

Jah

Ei

Mis on peamised takistusted, mis piiravad suuremat tähelepanu küberkaitsele?

Ei oska kuskilt alustada

Ei näe vajadust

Pole piisavalt finantsressurssi

Muu…

Tulemüürid ja Interneti kättesaadavus

1. Kas olete kohaliku võrgu ja välisvõrgu piirile paigaldanud tulemüüri (Firewall) või mõne muu seadme?

Jah

Ei

Tulemüüri pole

2. Kas kõikide Internetti vahetult ühendatud tulemüüride salasõnad ja kasutajanimed on muudetud algseadetest turvaliste vastu? (st seadmed on ettevõttesse sisse tuleva interneti ühenduse esmane kontakt)

Jah

Ei

3. Kas kõik tulemüüridel ja muudel seadmetel avatud pordid ja teenused on põhjendatult avatud ning saanud dokumenteeritud heakskiidu kvalifitseeritud spetsialistilt, koos selgitusega ärihuvide jaoks?

Jah, alati

Enamik

Valdav enamus

Üksikud

Mitte ükski

4. Kas levinumad rünnakute ohvriks langevad teenused on tulemüürides ja muudes vahetult Internetti ühendatud seadmetes välja lülitatud või blokeeritud (nt Server Message Block (SMB), NetBIOSm tftp, RPC, rlogin, rsh, rexec)

Jah, kõik

Enamik

Mõned

Üksikud

Mitte ükski

5. Kas kõik tulemüüri reeglid, mida enam ei ole vaja, on kustutatud või välja lülitatud?

Jah

Ei

6. Kas tulemüüri reegleid vaadatakse regulaarselt üle?

Jah

Ei

7. Kas arvutid, mis ei vaja otseselt Internetiühendust, on seadistatud selliselt, et nad ei saa ise ühendusi Internetti alustada (Default deny)?

Jah

Ei

8. Kas tulemüüri administraatori konto on selliselt seadistatud, et sellele ei pääse välisest võrgust ligi?

Jah

Ei

8a. Kas administraatori õigustega kasutaja on turvatud kahe-astmelise autentimisega või on juurdepääs piiratud konkreetse IP-aadressiga?

Jah

Ei

4.2.8 Turvaline seadistus

9. Kas ebavajalikud kasutajakontod ettevõtte arvutites ja serverites on kustutatud või välja lülitatud?

Jah, kõik

Enamik

Mõned

Üksikud

Mitte ükski

10. Kas kasutajakontode algsed paroolid on muudetud sobivate tugevate paroolide vastu?

Jah, alati

Enamasti

Mõnikord

Harva

Mitte kunagi

11. Kas paroolide keerulisuse nõuded on eraldi dokumendis sätestatud ja tehniliselt ka seadistatud kõikide tavakasutajate ja administraatorite kontode jaoks?

Jah, alati

Enamasti

Mõnikord

Harva

Mitte kunagi

12. Kas auto-run funktsionaalsus on välja lülitatud (st funktsionaalsust, kus USB-pulga või mõne analoogse seadme sisestamisel arvutisse hakkab seadmel asuv programm automaatselt tööle).

Jah, alati

Enamasti

Mõnikord

Harva

Mitte kunagi

13. Kas ebavajalik tarkvara (tihti uue arvutiga kaasa tulevad tootjapoolsed programmid) on arvutitest eemaldatud või välja lülitatud ning kas arvutites on üksnes see tarkvara, mis on ettevõtte tööks vajalik?

Jah, alati

Enamasti

Mõnikord

Harva

Mitte kunagi

14. Kas kõik täiendav tarkvara, mis on töötajate arvutitesse installitud, on ka saanud heakskiidu IT-toelt või juhtkonna poolt ning kas tavakasutajatel on keelatud ise tarkvara installida?

Jah, alati

Enamasti

Mõnikord

Harva

Mitte kunagi

15. Kas isiklikud tulemüürid (nt Windows Firewall) või selle analoogid, (nt ESET Endpoint, vms) on kõikides arvutites ja laptopides sisse lülitatud ja seadistatud selliselt, et loata ühendused väljastpoolt on blokeeritud?

Jah, alati

Enamasti

Mõnikord

Harva

Mitte kunagi

16. Kas kõik kasutajate arvutid on ehitatud ühele lõplikult turvatud platvormile (nt korralikult puhastatud ja seadistatud Windowsi süsteem, mida on kastutatud ka teiste arvutite seadistamisel alusena), tagamaks ühetaolised süsteemid ja turvalisuse kogu ettevõttes?

Jah, alati

Enamasti

Mõnikord

Harva

Mitte kunagi

17. Kas kasutate Active Directory (või mõne muu kaustadega seonduvate teenuste tööriista, ingl. k. directory services tool) tööriistu, millega keskselt teostada süsteemide haldust ja turvapoliitika elluviimist?

Jah, alati

Enamasti

Mõnikord

Harva

Mitte kunagi

18. Kas kasutate proxy ehk vaheservereid, et pakkuda kontrollitud juurdepääsu Internetile vastavalt süsteemidele ja kasutajatele?

Jah, alati

Enamasti

Mõnikord

Harva

Mitte kunagi

19. Kas on seadistatud offline-backup'id või failide muutuste logi (journaling policy), tagamaks kaitset krüptoviiruste eest?

Jah, alati

Ei

20. Kas logide pidamise kohta on olemas hoiustamise ja haldamise poliitika/kord?

Jah, kõikide kohta on olemas

Enamike kohta on olemas

Ei

21. Kas operatsioonisüsteemide logifaile hoitakse nii serveris kui kasutajate arvutites?

Jah, alati

Enamasti

Mõnikord

Harva

Mitte kunagi

22. Kas olulisemate programmide logifaile (sealhulgas DHCP logifailid) säilitatakse nii serverites kui kasutajate arvutites vähemalt kolm kuud?

Jah, alati

Enamasti

Mõnikord

Harva

Mitte kunagi

23. Kas Internetti juurdepääsu (nii veebi kui e-mailide) logifaile hoitakse alles vähemalt kolm kuud?

Jah, alati

Enamasti

Mõnikord

Harva

Mitte kunagi

24. Kas mobiiltelefone ja tahvelarvuteid hallatakse keskselt, et oleks võimalik kaugelt nende sisu kustutada ja seadmed lukustada juhul, kui seade läheb kaotsi või varastatakse?

Jah, alati

Enamike seadmete osas

Mõnikord

Harva

Mitte kunagi

Ei puuduta meid

25. Kas ettevõtte kasutab Mobiiltelefonide Haldamise Süsteemi (Mobile Device Management), et kaitsta ja hallata kõiki mobiiltelefoni platvorme, mis ettevõttes kasutusel on?

Jah, alati

Enamike seadmete osas

Mõnikord

Harva

Mitte kunagi

Ei puuduta meid

26. Kas ettevõtte tööga või personaliga seotud tundlikele andmetele on võimalik väljastpoolt sisevõrku autentimisega (authenticated access) juurde pääseda?

Jah

Ei

4.2.9 Juurdepääsude tagamine

27. Kas uute kasutajate loomisega kaasneb kõikide vajalike õiguste andmine ja nendele õigustele ka heakskiidu saamine?

Jah, alati

Enamasti

Mõnikord

Harva

Mitte kunagi

28. Kas administratiivne juurdepääs süsteemidele on piiratud arvul volitatud isikutel?

Jah, alati

Enamasti

Mõnikord

Harva

Mitte kunagi

29. Kas kasutajakontod on määratud konkreetsetele inimestele ning töötajad koolitatud paroole mitte jagama?

Jah, alati

Enamasti

Mõnikord

Harva

Mitte kunagi

30. Kas kõiki administratiivkontosid (sh teenuste kontosid) kasutatakse ainult eesmärgipäraseks administratiivseks tegevuseks, ilma juurdepääsuta välisele e-mailile või Internetile?

Jah, alati

Enamasti

Mõnikord

Harva

Mitte kunagi

31. Kas süsteemide administratiivkontod (sh teenuste kontod) on seadistatud lukustuma pärast teatud arvu ebaõnnestunud sisselogimise katseid?

3 ebaõnnestunud sisselogimise katset

6 ebaõnnestunud sisselogimise katset

10 ebaõnnestunud sisselogimise katset

>10 ebaõnnestunud sisselogimise katset

Mitte kunagi

32. Kas paroolide jaoks on olemas eraldi reeglistik, mis katab järgmiseid punkte?

a. Kuidas vältida ilmselgete paroolide valimist (mis põhineksid lihtsasti leitaval infol);

b. Ei tohiks kasutada levinud paroole (mis oleks võimalik sõnaraamatut kasutades ära arvata);

c. Samu paroole ei tohiks kasutada korduvalt;

d. Kuhu ja kuidas võib paroole salvestada, et need oleksid turvaliselt hoitud ja kättesaadavad;

e. Juhul kui paroolihaldustarkvara on lubatud, siis milline;

f. Millised paroolid on kasutajatele kohustuslikud pähe õppida ning mitte kuskile salvestada.

33. Kas kasutajad vähemalt autentitakse, kasutades piisavalt tugevaid paroole, enne kui nad pääsevad arvutites ligi erinevatele programmidele?

Jah, alati

Enamasti

Mõnikord

Harva

Mitte kunagi

34. Kas kasutajakontod eemaldatakse või blokeeritakse kui neid enam vaja ei ole (näiteks kui inimene saab organisatsioonis uue rolli või lahkub organisatsioonist) või pärast eelnevalt paika pandud perioodi, mil konto on olnud tegevusetu (näiteks 3 kuud)?

Jah, alati

Enamasti

Mõnikord

Harva

Mitte kunagi

35. Kas jagatud andmed (jagatud kaustad) on seadistatud selliselt, et üksnes neil kasutajail on juurdepääs, kellele konkreetsed andmed on tööülesannete jaoks vajalikud (näiteks personali või finantsüksuse andmed/kaustad)?

Jah, alati

Enamasti

Mõnikord

Harva

Mitte kunagi

4.2.10 Kaitse pahavara eest

36. Millist alljärgnevatest lahendust kasutatakse Teie organisatsioonis?

a. Viirusetõrje või pahavara eest kaitsev tarkvara;

b. Heakskiidu saanud tarkvara nimekiri (application whitelisting);

c. Tarkvara ja programmide testimine Liivakastis (application sandboxing)

d. Mitte ühtegi

37. Kas viirusetõrje või pahavara eest kaitsev tarkvara on paigaldatud kõikidesse arvutitesse, mis on ühendatud või võimelised ühenduma Internetti?

Jah, alati

Enamasti

Mõnikord

Harva

Mitte kunagi

38. Kas viirusetõrje või pahavara eest kaitsev tarkvara (sh programmi lähtekood ja pahavara signatuurid) hoitakse uuendatud (näiteks automaatsete uuenduste seadistamise teel või läbi kekselt hallatava teenuse)

Jah, alati

Enamasti

Mõnikord

Harva

Mitte kunagi

39. Kas viirusetõrje või pahavara eest kaitsev tarkvara on seadistatud automaatselt faile analüüsima kohe kui need muutuvad kättesaadavaks (sh Internetist alla laetud, USB-pulgalt või võrgukettalt kättesaadavad failid, jne) ning analüüsima külastatavaid veebilehti?

Jah, alati

Enamasti

Mõnikord

Harva

Mitte kunagi

40. Kas pahavara eest kaitsev tarkvara on seadistatud teostama perioodilisi skanneeringuid (nt kord päevas)?

Jah, alati

Enamasti

Mõnikord

Harva

Mitte kunagi

41. Kas kõik programmid, mis ettevõtte seadmetes töötavad, on ettevõtte poolt valitud/heakskiidetud ning samas mingi kaitsemehhanismiga piiratud, näiteks ainult signeeritud koodi lubamisega?

Jah, alati

Enamasti

Mõnikord

Harva

Mitte kunagi

42. Kas ettevõte peab nimekirja lubatud programmidest?

Jah

Ei

43. Kas kasutajatel on piiratud muude programmide installimine?

Jah

Ei

44. Kas kõik tundmatu kood on piiratud jooksma ainult liivakastis (ingl. k. sandbox) ning ei pääse ligi ühelegi muule ressursile ilma, et kasutaja talle spetsiaalselt loa annaks?

Jah

Ei

4.2.11 Uuenduste haldamine

45. Kas paigaldate arvutites ja võrguseadmetes töötavale tarkvarale turvauuendusi (security patches)?

Jah, alati

Enamasti

Mõnikord

Harva

Mitte kunagi

46. Kas Internetti ühenduvatel arvutitel on litsenseeritud ja tootja poolt toetatud tarkvara, mis tagaks, et turvauuendused tuntud haavatavustele on saadaval?

Jah, alati

Enamasti

Mõnikord

Harva

Mitte kunagi

47. Kas aegunud või lihtsalt vana tarkvara on Internetti ühendatud arvutitest ja võrguseadmetest eemaldatud?

Jah, alati

Enamasti

Mõnikord

Harva

Mitte kunagi

48. Kas kõikidele arvutitele ja võrguseadmetele paigaldatakse (või uuendatakse automaatselt) turvauuendused 14 päeva jooksul nende avaldamisest?

Jah, alati

Enamasti

Mõnikord

Harva

Mitte kunagi

49. Kas kõiki nutitelefone uuendatakse regulaarselt tootjapoolsete süsteemiuuenduste ja äppide uuendamistega?

Jah, alati

Enamasti

Mõnikord

Harva

Uuendusi pole saadaval

Ei puuduta meie ettevõtet

50. Kas kõiki tahvelarvuteid uuendatakse regulaarselt tootjapoolsete süsteemiuuenduste ja äppide uuendamistega?

Jah, alati

Enamasti

Mõnikord

Harva

Uuendusi pole saadaval

Ei puuduta meie ettevõtet

51. Kas teostate regulaarseid haavatavuste kaardistamisi oma sisemisel võrgul ja tööjaamadel, et leida võimalikud probleemid ja tagada nende lahendamine?

Jah, alati

Enamasti

Mõnikord

Harva

Ei

52. Kas teostate regulaarselt haavatavuste otsimisi (vulnerability scans) oma välise võrgu (external network) osas, et leida probleeme ning neile lahendused leida?

Jah, alati

Enamasti

Mõnikord

Harva

Ei

Appendix 3 – Total scores and Sub Scores of the Survey Respondents

Table 5. Scores of the respondents for each sub-section, in descending order by highest total score.

Field of Activity	Nr of Employees	Firewalls	Secure Configuration	Access Control	Malware Protection	Total Score
C Manufacturing	7	10,00	8,75	10,00	9,44	**45,69**
J Information and communication	13	9,44	7,36	9,44	8,33	**42,08**
G Wholesale and retail trade; repair of motor vehicles and motorcycles	8	10,00	6,25	8,24	7,22	**39,84**
J Information and communication	2	5,00	7,78	9,63	8,06	**39,84**
J Information and communication	10	7,78	5,69	10,00	8,33	**38,99**
L Real estate activities	23	10,00	6,39	9,72	5,28	**37,64**
G Wholesale and retail trade; repair of motor vehicles and motorcycles	5	6,39	5,14	8,43	9,44	**36,90**
E Water supply; sewerage, waste management and remediation activities	8	9,72	5,83	8,70	7,50	**36,76**
S Other service activities	80	7,78	5,56	8,98	4,72	**36,41**
H Transportation and storage	7	8,89	5,28	8,24	6,67	**35,95**
G Wholesale and retail trade; repair of motor vehicles and motorcycles	2	7,22	6,81	7,13	7,22	**35,25**
K Financial and insurance activities	3	7,22	3,89	7,87	6,39	**33,50**
J Information and communication	8	6,67	5,28	8,52	6,11	**32,51**
G Wholesale and retail trade; repair of motor vehicles and motorcycles	24	5,56	5,69	8,33	4,17	**32,50**
J Information and communication	10	6,67	6,11	7,41	2,22	**31,16**
E Water supply; sewerage, waste management and remediation activities	9	8,89	3,75	7,50	4,72	**31,11**

G Wholesale and retail trade; repair of motor vehicles and motorcycles	10	7,50	2,64	6,67	7,22	**29,65**
S Other service activities	3	5,83	4,03	7,96	5,83	**28,97**
G Wholesale and retail trade; repair of motor vehicles and motorcycles	8	7,78	4,44	6,94	5,00	**27,29**
G Wholesale and retail trade; repair of motor vehicles and motorcycles	5	6,67	7,22	8,80	0,00	**26,75**
L Real estate activities	2	6,11	5,28	6,57	5,28	**26,68**
J Information and communication	7	10,00	3,19	8,70	0,00	**26,59**
G Wholesale and retail trade; repair of motor vehicles and motorcycles	16	3,61	4,86	7,69	1,67	**24,70**
J Information and communication	4	7,22	4,03	7,41	4,72	**24,63**
J Information and communication	6	7,78	2,78	5,28	4,72	**24,31**
A Agriculture, forestry and fishing	4	0,00	5,28	7,31	6,67	**23,01**
A Agriculture, forestry and fishing	7	0,00	4,44	7,41	4,17	**21,33**
G Wholesale and retail trade; repair of motor vehicles and motorcycles	5	0,00	4,17	7,13	6,67	**21,09**
A Agriculture, forestry and fishing	5	6,39	4,31	0,28	4,17	**17,95**
G Wholesale and retail trade; repair of motor vehicles and motorcycles	4	0,00	4,17	4,35	4,72	**16,99**
G Wholesale and retail trade; repair of motor vehicles and motorcycles	2	0,00	3,89	4,63	4,17	**16,75**
C Manufacturing	10	2,22	0,28	5,74	5,00	**16,37**
G Wholesale and retail trade; repair of motor vehicles and motorcycles	4	0,00	2,36	4,72	4,72	**15,56**
G Wholesale and retail trade; repair of motor vehicles and motorcycles	9	4,44	1,53	2,78	3,61	**15,49**
F Construction	10	0,00	2,64	3,70	5,56	**14,40**
L Real estate activities	12	0,00	1,11	5,00	1,39	**12,50**

A Agriculture, forestry and fishing	6	0,00	2,22	3,52	0,00	**6,99**
G Wholesale and retail trade; repair of motor vehicles and motorcycles	4	0,00	1,25	2,50	0,00	**6,25**
G Wholesale and retail trade; repair of motor vehicles and motorcycles	6	0,00	0,00	2,59	0,83	**4,68**
Average	**9,44**	**5,20**	**4,40**	**6,82**	**4,92**	**26,54**
Median	**7,00**	**6,39**	**4,44**	**7,41**	**5,00**	**26,75**
Mode	**10**	**0**	**5,28**	**7,41**	**4,72**	**39,84**