Bachelor's Thesis

Business and Administration

NINBOS14

2017

Joonas Koljonen

FINNISH SME'S AWARENESS ABOUT INTERNET SECURITY

– SSL-certificates for personal data security

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Bachelor of Business and Administration

2017 | 43

Author: Joonas Koljonen

FINNISH SME'S AWARENESS ABOUT INTERNET SECURITY - SSL-certificates for personal data security

This thesis was made on inspiration and interest gathered in author's internship placement in IT business services, Euronic Oy, Turku, Finland. The research goal was to find out the level of awareness about internet security within Finnish SME's especially on part of securing personal data with SSL-encryption.

The research was made firstly by author's own observations, then deepened the knowledge with relevant articles, books and reports. These sources clearly showed how the internet security is coming more serious business as European Union has approved General Data Protection Regulation. This regulation with the existing Finnish regulation sets more pressure for companies to verify that are on point of them before enforcement date. SME's employ most of the workforce in Finland, above all the other company types, and are also the majority in Euronic Oy's customer base. This means that these legislations will affect their business when it contains any personal data.

A survey was conducted to Euronic Oy's customers in order to find out how aware Finnish SME's on company's customer base are on the subject and how do they react on it. The survey itself was created by qualitative methods.

The result of the survey pointed out that majority of SMEs are aware of the issue, but are not reacting to it, as they are either negligent on the issue or counting it to be handled by third party.

KEYWORDS:

IT business services, SSL certificate, Finnish, SME, internet security, personal data act, EU GDPR.

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Bachelor of Business and Administration

2017 | 43

Tekijä: Joonas Koljonen

SUOMALAISTEN PIENTEN JA KESKISUURTEN YRITYSTEN TIETOISUUS INTERNET-TURVALLISUUDESTA - SSL SERTIFIKAATTI HENKILÖKOHTAISEN TIEDON SUOJAKSI

Tämä tradenomitutkinnon opinnäytetyö tehtiin kirjoittajan IT-alan työharjoittelupaikan luoman kiinnostuksen ja inspiraation johdosta, harjoittelupaikkana oli Euronic Oy, Turku. Opinnäytetyön tarkoitus on selvittää suomalaisten pienten ja keskisuurten yritysten tietoisuutta internet-turvallisuudesta, aiheena erityisesti henkilökohtaisten tietojen salaaminen SSL-salauksella.

Opinnäytetyö tehtiin ensisijaisesti omien havaintojen perusteella, jonka jälkeen aihetietoa kerättiin lisää artikkeleilla, kirjoilla ja raporteilla aiheesta. Nämä lähteet osoittivat selkeästi, kuinka internet-turvallisuus on nousemassa tärkeäksi liikennetoiminnaksi Euroopan Unionin asettaman tietoturva-asetuksen myötä. Tämä asetus jo olemassa olevan suomalaisen lainsäädännön kanssa luo paineita yrityksille varmistaa siihen liittyvät asiat ennen asetuksen käytäntöön panoa. Pienet ja keskisuuret yritykset työllistävät suurimman osan suomalaisesta työvoimasta ja niitä on eniten kaikista yritysmuodoista. Ne ovat myös enemmistö Euronic Oy:n asiakaskunnasta. Tämä tarkoittaa, että nämä lait ja asetukset vaikuttavat heidän liiketoimintansa kautta siihen, miten heidän sivuiltaan kerättävät yksilöivät henkilötiedot ovat salassa.

Opinnäytetyön viimeisenä osana on Euronic Oy:n asiakkaille suunnattu kysely, jossa selvitettiin asiakaskunnassa olevien pienten ja keskisuurten yritysten tietoisuutta ja reagointia tähän tietoturva-aiheeseen. Kysely toteutettiin määrällisiä tutkimuskeinoja käyttäen.

Kyselyn tulokset osoittivat, että suurin osa pienistä ja keskisuurista yrityksistä on tietoisia asiasta, mutta ei reagoi siihen joko vastahakoisen asenteen takia tai sen vuoksi, että katsoo kolmannen osapuolen olevan sivustojensa salauksesta vastuussa.

ASIASANAT:

Tietotekniikan palveluala, SSL sertifikaatti, suomalaiset pienet ja keskisuuret yritykset, henkilötietolaki, EU:n tietosuoja-asetus.

CONTENT

LIST OF ABBREVIATIONS **6**

1 INTRODUCTION **6**

2 EURONIC OY **8**

3 LITTERATURE REVIEW **9**
3.1 SSL - Secure Socket Layer 9
3.2 Legislation 9
3.3 Certificate authorities 11
3.4 Illegal actions and problems 11
3.5 Finnish SMEs 13

4 METHODOLOGY **15**
4.1 Survey 15
4.2 The background and the creation of the survey 17
4.3 Hypothesis and other expectations of the survey 18
4.4 Analysis of the survey questions 19
4.5 Ideas for further research and development of the survey 21

5 ANALYSIS OF THE SURVEY RESULTS **22**
5.1 Answers about customers' company size and their internet usage 1-4 22
5.2 Questions concerning outside threats 5-7 25
5.3 Questions concerning secure connection and use of SSL-encryption 8-10 28

6 CONCLUSION **31**

REFERENCES **33**

APPENDICES

Appendix 1 Survey in Finnish 1
Appendix 2 Survey in English 3
Appendix 3. Email template sent to customers in Finnish 6
Appendix 4. Email template sent to customers in English 7

FIGURES

Figure 1 – What is the size of your company/organisation? 22
Figure 2 – Are you working directly for end customers or companies? 23
Figure 3 – What are the most important intensions for you to keep websites? 24
Figure 4 – How many inquiries or transactions you get on a month via your site, IF you have some kind of form to fill in? 24
Figure 5 – How often have you had attacks that has visibly harmed the function of your website? 25
Figure 6 – How have you taken under consideration the website security against possible threats? 26
Figure 7 – How would you handle the situation after the attack? 27
Figure 8 – How are you reacting yourself (or a colleague) that the browsers have started to warn visitors about unsecure sites (http) by a grey icon or even warning on the address bar, instead of secure sites (https) showing lock and safety status on it if the connection is encrypted? 28
Figure 9 – How important matter are you considering the encryption of customers data when filled on your website? 29
Figure 10 – How do you encrypt your customers' data when they are filling them on your website's forms? 30
Figure 11 – How companies with a form on their sire react to encrypting the data flow on it 32

PICTURES

Picture 1, Not Secure - Chrome , 2017 11
Picture 2, Secure - Chrome , 2017 11

TABLES

Table 1, Survey type – Pros&Cons (Wang & Doong, 2007) 16

LIST OF ABBREVIATIONS

Abbreviation	Explanation of abbreviation
GDPR	General Data Protection Regulation
HTTP	Hypertext transfer protocol
HTTPS	HTTP over SSL/TLS
ISP	Internet service provider
SSL	Secure Socket Layer
TLS	Transfer Layer Security
URL	Universal Resource Locator

1 INTRODUCTION

Interest towards the subject started growing from the author's internship place within IT business in Euronic Oy. Author's work there combines analysing and selling domain services to business clients. This brought up the idea of figuring out how aware they are about the ongoing change regarding internet security, and how the awareness could be raised and taken into action. The offered services to the clients are SSL-encryption certificates, website building tools, and web shop applications that can be linked to warehousing and direct invoicing. The main customers of the services are small and medium size enterprises and private entrepreneurs. The main challenge is to introduce the products to them as they are not usually aware of how whole entity works on the internet, not even on their own site. What would be the best way to introduce these certain internet security matters to them and ensure they understand the importance of encryptions and secure connection for their businesses? These small but significant differences create the companies' internet imago nowadays. The added value of padlock on the address bar and staying on-date with internet policies cannot be underestimated in the modern internet world.

SMEs cover a big ground of Finnish business economy, 359479 registered SMEs in 2015 (Suomen virallinen tilasto (SVT), 2016). Definition of SME is employing under 250 employees, and having turnover less than 50 million euros and balance sheet total less than 43 million euros. SMEs cover 99,9% of Finnish companies and they employ 67% of the workforce (Suomen virallinen tilasto (SVT), 2017). This research focuses on Finnish SMEs which are clients of Euronic Oy as they can be approached by a survey and an initial in person connection by author.

Other aspect than customer service and maintaining good connections with the present client firms is to research how customers act on this ongoing trend of browsers informing users about the security of the sites. Indeed, the major browsers such as Mozilla Firefox and Google Chrome have started to inform visitors about unsecure connections during 2017 (Ian, 2017). Google Chrome is the most used browser and Mozilla Firefox stands on 4th place (W3counter, 2017). These actions and reactions are crucial information when we start to think how SMEs, particularly Euronic's clients, could be taught more of the trending issue of marking HTTP sites insecure, which leads them being less appealing for the visitor. How aware are SMEs about the risks that are included when

being on non-secure site and asked to add their personal data on it? And if they pay any attention to it, how will they react on the issue?

This research discusses around these phenomena by figuring out answers to following research questions:

1. What HTTPS and SSL encrypted connection are?
2. How aware are the SMEs about potential threats regarding their clients' personal data security, and how they are reacting to it?
3. How aware are they of protecting their sites from external threats?

This research conducts basic information from secondary sources like other theses, reports and journals, but also primary data in form of a customer survey towards Euronic Oy's customers. This survey was performed in order to gather more specific information of client companies' awareness regarding their internet security, especially on the difference between HTTP and HTTPS, and reactions to it. In process author can gain extensive knowledge on how customers are acting now as the browsers have started to inform users about possible risks on different websites.

Firstly this research presents theoretical background explaining the technical difference of secure and non-secure connection, the present and upcoming legislation regarding the issue, how it has been violated, and how it might effect people on their everyday life. Secondly it deals with methodologies used in the creation of the survey and explanations to the survey questions. Last two chapters discuss the numerical results of the survey and the conclusions drawn from it.

2 EURONIC OY

Euronic Oy is a Finnish ISP, internet service provider, company offering mainly domain and webhosting services worldwide by operating name of Domainkeskus. Even though it has customers on every continent, major part of them are Finnish SMEs, organisations and private customers that need all kind of internet services. All of company's activities are located in Turku, data center, IT and customer service, and sales department employing 12 persons in total.

Euronic Oy was founded in 2000 and is one of the oldest Finnish company still functioning on the internet services. They firstly bought server space from American retailer and started to ease .fi domain registration for Finnish companies. After this they have grown by opening their own data center, offering more services than only the registration. Nowadays they have wide scale of services for companies and organisations that operate online; webhosting, virtual private servers, cloud services, website design and e-commerce applications, and server space for automation usage.

Since November 2016 Euronic Oy has been operating with two brand names, Domainkeskus and acquired Nettihotelli Oy (Euronic Oy, 2016). That company acquire still effects on field when doing customer service and sales towards the customers. Both brand names are still in use and they have their respective clients. This provides a great opportunity within this thesis as research can be done to two different customer groups, as Nettihotelli is offering low cost services and Domainkeskus is offering premium services.

3 LITTERATURE REVIEW

On the following part, the most relevant topics and factors that should be known for the full understanding of the research will be discussed.

3.1 SSL - Secure Socket Layer

SSL certificate is used for encrypted communication between web browser and web server. Web browser stands for applications such as Internet Explorer, Google Chrome and Mozilla Firefox that visitors use to access websites backed by web servers that are physical routers and network services provided by various companies. Browsers ask the page that visitor wants to see by URL from the backing server, and servers deliver the information of that specific address in matter of seconds. (Orgera, 2017) Web servers are normally hardware that contain the information that appears as the searched website. All the data could be for example, on the website owner's own computer, but in that case the computer should be on everytime someone wants to visit the site. So, using a third-party server has its pros: it is always on, is always connected to Internet, and has the same IP-address every time the consisting data is asked. (Mozilla Foundation, n.a.)

SSL certificate's two main functions are to authenticate the safety and the identity of the website to the visitor, and to encrypt the information that is transmitted to and from the site (Verisign, 2017). In other words, all the information is going on HTTP over SSL, becomes shortened as HTTPS, rather than less secure HTTP, Hypertext Transfer Protocol. HTTPS's main function is to ensure that the client is visiting the intended website, not a fake one, and that two-way communication between the client and server is encrypted and cannot be forged nor read by any third party.

3.2 Legislation

This encryption of the websites will become more imperative as EU has defined more detailed regulation (EU, 2017) to align all member countries to the same personal data regulation starting from 25.5.2018 with the General Data Protection Regulation (Lehtola, 2016). Besides of this upcoming legislation, Finnish law already has section on its own personal data act stating the following:

> *"The controller shall carry out the technical … measures necessary for securing personal data against unauthorised access, … manipulation, disclosure and transfer and against other unlawful processing. The techniques available, … as well as the significance of the processing to the protection of privacy shall be taken into account when carrying out the measures."Ch.7, section 32* (FinLex, 1999)

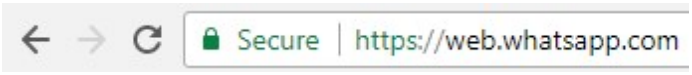
Controller meaning the owner of the website. These acts already show the importance of the correct internet browsing security is getting higher and also the data flowing through is involving more personal information as more and more business services can be done through internet. Based on the Finnish act nowadays, each company asking any customer data, like name and email, should provide necessary methods to protect their customers' information from getting into wrong hands. This could be done by SSL certificate that ensures the encryption and authentication of the website. Also redirecting the customer to third party website like Google Docs solves the issue. Unfortunately, as it is not punishable by any means it has not been taken that seriously.

These acts have become more relevant in the modern world where more sensitive information moves through internet, people sign into their multiple services running online with their own personal information which may even include addresses, phone numbers and banking rights. This has been an issue since the start of the Internet era, but has only been taken under consideration from the legal aspects recently. This might be because of the rise of worldwide users as from year 2010 to 2016 there has been growth of 16 percentage point to the point that 46% of world population is using internet (International Telecommunication Union, 2016). IT companies have been trying to come up with more secure ways to transfer data online. The SSL certificates are the way to have the encryptions and authentications between web servers and users' web browsers, which happens every day. SSL certificates are only one tool to protect against internet security threats. The other parts of internet security are controlled by internet service providers and the other associations working on it. These include for example, cyber espionage, ransomware, financial heists, and distributed denial of service attacks (DDoS attacks) (Symantec , 2017).

Therefore, encryption of every day connection has become a vital issue in the connected world that we are living in. There has been numerous researches and theses done about the subject of SSL certificate and keeping them up to date, normally from the purely electronical side. For example, (Puumalainen, 2017)'s thesis tells about how the encryption works deep down in the roots of internet data transfer level.

Because of these acts and other issues, as more specified general data flow through internet, the authentication is shown by the most used browsers such as Google Chrome, Mozilla Firefox, Apple Safari and Internet Explorer by a notification on the address bar (pictures 1 and 2 below) or even pop ups when they do not recognise the necessary level of encryption or security means on the site. These normally occur when the site has different kind of forms and questionnaires to fill up by personal information. Nevertheless, many of these personal information forms and user registrations still run on unsecured sites, that do not offer any kind of encryption for the users' personal information. These issues should be tackled away by any companies that provide their services online.

Picture 1, Not Secure - Chrome , 2017



Picture 2, Secure - Chrome , 2017

3.3 Certificate authorities

There are only four main SSL certificate providers, also known as certificate authorities, worldwide sharing almost 90% of the whole SSL certificate market. It can be verified rather fast if some illegal actions are breaching to the markets. These four are all private companies; Comodo, IdenTrust, Symantec Group, and GoDaddy Group. (W3techs, 2017) They usually use retailers ISPs, such as Euronic Oy, to sell their certificates. They are responsible for the functionality of their certificates' safety measures of encryption and authentication and they back up the possible breaches.

3.4 Illegal actions and problems

When website owners are not using encryption on their fillable forms online, it can lead for example into a situation where automated programs can gather an extensive amount of personal data. That data can be just emails and names or addresses, and it can be

used to personified spam mail towards these people whose connection was not secure when filling for example, a mail list order.

A notion to remember is that there are always illegal actions taken when there is an opportunity for business, especially this growing one, that browser companies are planning to set up HTTPS iniative for every website in order to secure all of clients' information (Kan, 2017). Therefore, there has been many fake, or at least unsafe, certificates on the market that might interest customers by their cheap price or immediate installing time. One of these is Let's Encrypt which offers free SSL certificates that are not recognised by the biggest internet security firms and have caused problems by giving illegitimate sites authentications for bigger scam operations. One of them was to authenticate phishing sites with PayPal term or word on the domain, for example paypal.com.anypossibledomain.net, which makes it subdomain of anypossibledomain.net and its owners can collect the information filled on it. Yet with SSL certificate it looks authentic enough to collect peoples PayPal sign in -information (Lynch, 2017) .This has been the case since Let's Encrypt has been issuing free certificates as an automated certificate authority, which leads to the problem that they are giving domain validation to phishing sites as they are not controlling the sites' business function or purpose by any mean (Vänskä, 2017). However, it does not stop there. Other domain names with big corporation names have been authenticated as well. The trick is that it can be done with every possible sign-in page for example appleid.com.anypossibledomain.net leading the information to end up in use of the owner of this misleading domain. For example, on mobile devices this works well as the full domain does not fit on the address bar.

> *PayPal is a high-value target and Let's Encrypt had already issued nearly 1,000 certificates containing the term PayPal, more than 99% of which were intended for phishing sites. With expanded research, we found our previous claim was a major underestimate. Let's Encrypt has actually issued 15,270 PayPal certificates. This reveals the previously unknown extent of the Let's Encrypt phishing phenomenon.* (Brenner, 2017)

This means that people cannot trust on the padlock on the address bar anymore (Picture 2), and they are again on their own to figure out if it is legitimate site or business running it. That is a high amount and it is to increase as Let's Encrypt is aiming to authenticate 20 000 more sites with their certificate. (Brenner, 2017) Their mission is noble as they want the same than web browser companies and other certificate authorities: to make

the internet safer for the users by putting the personal data flow behind the secure connection. They are providing secure connection to the sites, but this encrypted information is flowing to the cybercriminals running these secure, but misleading, sites, so source and media criticism is still left to the end user, as they cannot trust every secure connection on the market. One of the causes for this is that they do not validate the company, its functions or its owner by even with a mail from the domain that certificate will be issued. This has led to conversations about putting Let's Encrypt certificates on black list so the browsers would not notify it as secure domain validation on PayPal sites. Yet many are defending Let's Encrypt and raising awareness on the media criticism that every internet user should have (Helme, 2017).

> *This figure is more than ten times larger than previous estimates that have been published. The vast majority of this issuance has occurred since November – since then Let's Encrypt has issued nearly 100 "PayPal" certificates per day. Based on a random sample, 96.7% of these certificates were intended for use on phishing sites.* (Lynch, 2017)

This same issue can come up with any other certificate authority as well, but as they have longer authentication path and they ask a payment for it, it has not been on such high levels than with Let's Encrypt as the certificates cannot be ordered in masses for some phishing or scam operation. For example, registering look-a-like domains of web banks and securing all of them to collect customers banking rights. In this case, longer authentication path is better to ensure the internet security for the end users.

3.5 Finnish SMEs

95% of Finnish companies own a website for their business (Suomen Virallinen Tilasto, 2016). Many of these sites still run on unsecure domains due to lack of awareness. Despite of not having their website running on a secure domain, they have questionnaires and forms for their clients to fill in with personal data. This opens opportunities for IT businesses to offer security for these domains, but also opportunities for cyber criminals to collect the personal data and use it on their purpose to gain profit over this unsecure state of domains. The unawareness might be caused by the fast development of IT services, which may be the stumbling block for many long-term businesses that have started their action already before the Internet era. Some of these old companies have sites online but they might not consider them as a major marketing

channel as they have been doing business long before the internet came a phenomenon. They might be familiar only to positive sides of the internet and have not even heard of the downsides that are mentioned above. They might have taken re-education on internet security matters on this millennium but still might be lacking the newest information published on the latter years of this decade.

People who have been active on IT field of business are expert of these kind of issues but the ones working for example on logistics, hairdressers etc. might not be aware of the risks related to modern internet security even if they are regular internet users. In this research, we will dig in what do they know about the internet security and then analyse how this important matter can be published better to reach the audience, to make them believe on its importance, and act accordingly.

4 METHODOLOGY

This thesis was made to find out how aware Finnish SMEs are about internet security and to cover the facts why it should be important to everyone, companies and end users. This subject was led from author's work in IT industry and by the recent legislative changes on general data protection regulations in EU level. These subjects have not been researched beforehand from this specified perspective and therefore there was a need for this kind of research.

Research for this was conducted by extensive use of secondary data found on topic of internet security, especially on SSL certificates. Besides of that it includes discussions about the backgrounds of internet security, possible pros and cons regarding to SSL certificates and CAs, Finnish SMEs on internet, and findings made from secondary and primary source. To obtain primary data, a web-based survey was executed to the target group 10 251 customers of Euronic Oy, in order to understand their current awareness and to point out how it could be raised in the future.

4.1 Survey

As the survey was made with a wide scale and it possesses the most important data towards conclusion to research problem the process of making it will be gone through carefully to gain validation of its credibility.

The survey was chosen to be web based as the whole topic is related to internet. Also, it is the most cost-efficient way to approach thousands of customers at once. Web-based surveys have their pros and cons of course and those should be mentioned to justify the right selection of survey type. Web based surveys tend to have low answers rates, when compared to more personal surveys made face-to-face or by business letters, but their reach and time and cost efficiency makes them a suitable tool for many companies.

Survey Type	Population	Pros.	Cons.	Suggested Alternatives
Web-based Survey	***UNKOWN POPULATION*** e.g. pop-up window, banner, online pools	Low access cost; easy to design and implement; may collect great responses quickly if the topic is interesting or the incentive is attractive.	Lack of clear population leading to questionable representativeness and generalizability; Multi-entry problem caused by agent attack; lower control over respondents.	Disclose how the data was collected in detail in the methodology section; discuss how the population/sample problems may impact the findings in the research limitation; examine the population/sample profile by chi-square technique.
	KNOWN POPULATION e.g. member-based e-shopping or e-community Website	Complete population and sampling frame; can use sampling design; can estimate the sampling error, sample representativeness , and non-response error.	Difficult to get the Website sponsorship due to data and privacy protection laws; High cost to buy data from the marketing firm's database.	Researchers can only contact respondents via the Website's employees to protect member data. E.g. employees can conduct the sampling process and send/receive email questionnaire following researcher's instruction.

Table 1, Survey type – Pros&Cons (Wang & Doong, 2007)

This table shows which kind of usabilities web-based surveys carry within. In the case of this thesis the known population row is the one to look for, as our survey is addressed towards known customer base. All the mentioned cons were outcome by the fact that the survey was send to the existing active customers base, not bought from any third party, and by the fact that school provides online survey tool, Webropol, to be used on researches.

As the survey type was chosen, the design was made so that gained answers are easy to analyse and that they would be answering the given research questions. For this kind of big sample, it was the most convenient to give them rather multiple choices questions than open ended questions to ease latter analysis of them. The quantitative method like multiple choices questions is easier to analyse. This lead to further research to find out suitable answers which might come up to the answerers' mind. Also, the psychical layout matters was used to diminish the possible measurement error. (Lippincott & Wilkins/Wolters, 2012)

Qualitative method could have been used as many of the customers are contacted on some kind of yearly basis by phone, but going through this vast crowd by phone just for

a research would have been too time consuming. It would have also diminished the amount of questions that can be asked as phone surveys tend to take more time.

Contacting customers via phone has been the author's task during the summer so it can be stated as random sampling made on the customer group to draw some conclusions even though they have not been recorded, but rather driven author into certain direction to understand the reaction of the customers about the secure connections.

Prototypes of the survey were launched within the company, towards authors' friends and to the thesis supervisor in order to modify the answer field so that it would not be too directive and have the right answer possibilities to any possible scenario that might be answered. This whole process took approximately three days a week for three weeks to finish the survey.

4.2 The background and the creation of the survey

A web based customer survey was conducted to the vast customer base of Euronic Oy to collect researchable data to answer the research questions. The survey was created in cooperation with the coworkers and CEO as it is an important publication for the company and expresses the company image to the present customers. In addition to questions concerning the internet security, CEO wanted to have also section for customer satisfaction and usage of WordPress publishing tool as they do not do these kind of customer surveys often. In total, the survey consisted 26 multiple options questions, 10 of them concerning the thesis research topic. Also, it is important to contain valuable data for the customers and it is an important part of expressing company image and attitudes to the customers.

First demo part of the survey was introduced on Euronic Oy's internal Slack-channel on 9th of September to point out all the errors on grammar and on subjects concerning WordPress as the author is not the expert on WordPress. The small modifications and ideas for further development were made with thesis supervisor on 11th and then it was sent to CEO of the company on 15th of September. After that the survey was sent 18th of September to the thesis supervisor to obtain opinion about survey methods. By the time survey returned to author it was sent to first 410 customers, who are the most active or possess some kind of special prices on their products and services. This selection of

prototype group was made to gain exaggerated responses as there were mostly retailers and experts of the field. Prototype was sent on 28th of September.

This prototype survey to abovementioned test group was quickly analysed as only 15, 3,65%, of them answered. This created an alarming forecast what would be the actual response rate. Otherwise it was to see if there were some mistakes to correct before sending the survey to all of the customers.

The final form of the survey questions was finalized on 2nd of October, (Appendix 2). It was made mainly with multiple choices questions due the number of recipients to ease the final analysis made on base of the survey. Only one open ended question was added to gain development ideas for the company from the customers.

4.3 Hypothesis and other expectations of the survey

In order to be a concluding survey, it should have surpassed 25% answer rate., in the case it would mean over 2563 answers. This was not reached. Only 3,14% answer rate was gained, which means that survey result can be used only as a guideline of how Euronic's customers react on the issue.

> *DESIRED RESPONSE RATE. Self-administered mail surveys typically achieve very low response rates, often less than 50% of the original sample when a single mailing is used. Techniques have been developed to yield strikingly high response rates for these surveys, but they are complex and more costly. Face-to-face and telephone interviews often achieve much higher response rates, which reduces the potential for nonresponse error.* (Visser;Krosnick;& Lavrakas, n.a.)

The author expected to surpass the 25% response rate as the raffle reward, building a new website and securing it by SSL for a year, created interest for the customers to fill it and as the survey contains a lot of actual information and added value to the customers, as well to Euronic Oy.

Other expectations were to gain a negative majority on knowledge of internet security, to share information to vast range of customers in interesting way, and most importantly to gain general knowledge of customers' internet security measures and awareness. Negative majority meaning that the customers awareness over the internet security was not on the level to correctly answer or react all the questions.

Company expected to reach additional sales on SSL and Woo through this survey as an additional marketing tool. This cannot be concluded as it might have been such a small increase as many of the customers obtain SSL certificate already and Woo sales take normally a bit more effort and time from both ends to change into.

4.4 Analysis of the survey questions

Throughout this part all the questions will be analysed separately to create more justified and concrete background to the questions. On the next chapter, the author will draw conclusions based on the results, how these results could be used in order to answer research questions and raise the awareness on internet security amongst the Finnish SMEs.

Results about the customer satisfaction and usage of Word Press publishing tool will not be analysed nor showed at all as they have no relevance towards thesis research problem and questions.

4.4.1 Questions to find out company size and their internet usage 1-4 (appendix 1 in Finnish and appendix 2 in English)

First two questions are to separate different types of companies by asking what size they are and towards which kind of market they work as the author expects that the bigger companies working towards other companies, not towards end users, are more aware of the internet security than smaller companies working to private customers. The possible options to define company size most likely will have a meaning when concluding the level of awareness between bigger and smaller companies. This can be a result of the overall resources at hand to invest in these kinds of issues that are not so necessary to the business itself. This same reason might cause that different organisations and associations have lower measures to secure their connection even though the awareness might be on higher level as they normally have members from different areas of business.

Questions 3 and 4 are to find different reasons to possess a website and to find out how many have some kind of form for visitors to fill in. The answers to these questions will show what is the difference of people only having informative sites and those having

more actions on their sites. As completely static sites do not necessary need SSL or any other security measures to ensure their connection as they do not have any traffic going back and forth. In that case, the SSL-certificate is only a mean to validate the domain itself which, which has a positive impact on Google searches for example, also removing the security warning as it comes up to every unsecure site, even it is static or not. Finding out how many people have some kind of form on their site can be compared to upcoming question about the use of SSL to conclude how many of the sites with forms are still without a proper connection encryption.

4.4.2 Questions concerning outside threats 5-7

Questions 5 to 7 are to find out how many times customers' sites have been visibly harmed, how they are preventing it to happen and how they would solve out a possible case of outside breach to their sites. So firstly, question five was to find out how regular these kinds of attacks are amongst the customer base, so it can be compared to the awareness of the measures against it and the measures of acting after such events. Secondly this set is there to separate these outside breaches from encrypted connection. The author noticed this to be the matter that most of the customers mix up when it comes to encrypting the connection to the website during his four-month internship time. So, these questions are to separate outside threats and secure connection apart, for the readers of this thesis and for the customers. Specially for the customers there is an information section after this set of questions to clarify the means and actual answers to these questions.

4.4.3 Questions concerning secure connection and use of SSL-encryption 8-10

Question from 8 to 10 are to find out how people in companies react towards the security warning given by most of the browsers, how important they think it is and how they are managing their own site on that concern. This set of questions was the major point of the survey and the results of the answers will give out the overall awareness and importance Euronic Oy's customers give into internet security, especially on part of personal data protection. Firstly, question number eight shows their authentic reaction and affect of it to their use of internet. Number nine their measures the level of importance towards the subject and number ten their final action that they have made to clear this threat that is

possessed to their own customers. Again, this set of questions is followed by information section to clarify the functions of encrypted connection to raise their awareness on subject.

4.5 Ideas for further research and development of the survey

Internet security itself contains various other points than only the encryption of the connection. The upcoming EU GDPR already consists multiple other sections that could have been studied further in a perspective of its affect to Finnish SMEs, for example how the gathered personal, or general, data should be conserved and contained within banking, healthcare, and legal business areas so that the data is not accessible outside of the company and that it is correctly deleted after it has lost it validity to companies working in those areas. (EU, 2017) Due the size limit of bachelor thesis, and the lack of the realistic opportunities, these cannot be further researched but for example with a help of Finnish Communications Regulatory Authority, these issues could be surveyed more extensively. Even this thesis' questionnaire would give more valid data if it could be sent out to everyone owning .fi top level domain, which are all regulated and granted by Finnish Communications Regulatory Authority.

Other instance besides of GDPR that could be studied is how commonly web users' information end up in different spam mailing lists because of the lack of proper internet security when conserving or collecting general data. This could be tested out for example by creating fictional internet identity, and then filling up this information to all non-secure forms to find out if spam mail will find into email box. Of course, spam mailing is also generated to find out different possibilities with most common mail services domains. Spam mailing as it is nowadays could be also a great subject to study further, as it covers 95% of sent emails nowadays. Spam mails may contain links the phishing sites, sites with malware or just be used for effective advertisement of legitimate companies. (Runbox Solutions AS, 2017)

5 ANALYSIS OF THE SURVEY RESULTS

The answers from the customers were gathered in two parts, separately from the side of Domainkeskus and Nettihotelli as they have been recently fused together. These survey results are analysed together as long as the answers are similar, yet if there is a noticeable difference for a question between clients of Domainkeskus and Nettihotelli, it is brought up. The answers will be analysed by same categories as the questions in previous chapter. The survey sent to Domainkeskus gathered 142 finished surveys out of 5254 customers contacted by email. The survey sent to Nettihotelli gathered 180 finished surveys out of 4997 customers contacted by email. A total of 322 answers were gathered for this thesis out of 10251 contacted customers. This was a lot less than expected but also understandable because companies receive many online surveys, raffle reward was inadequate and contact information outdated. Part of the emails, approximately 5%, bounced back as the email addresses were not valid on the day of launching the survey. Response rate was approximately 3,14%, which is not enough to draw stable conclusions but rather to be used as guidelines towards understanding the awareness of internet security within the customers of Euronic Oy.

5.1 Answers about customers' company size and their internet usage 1-4

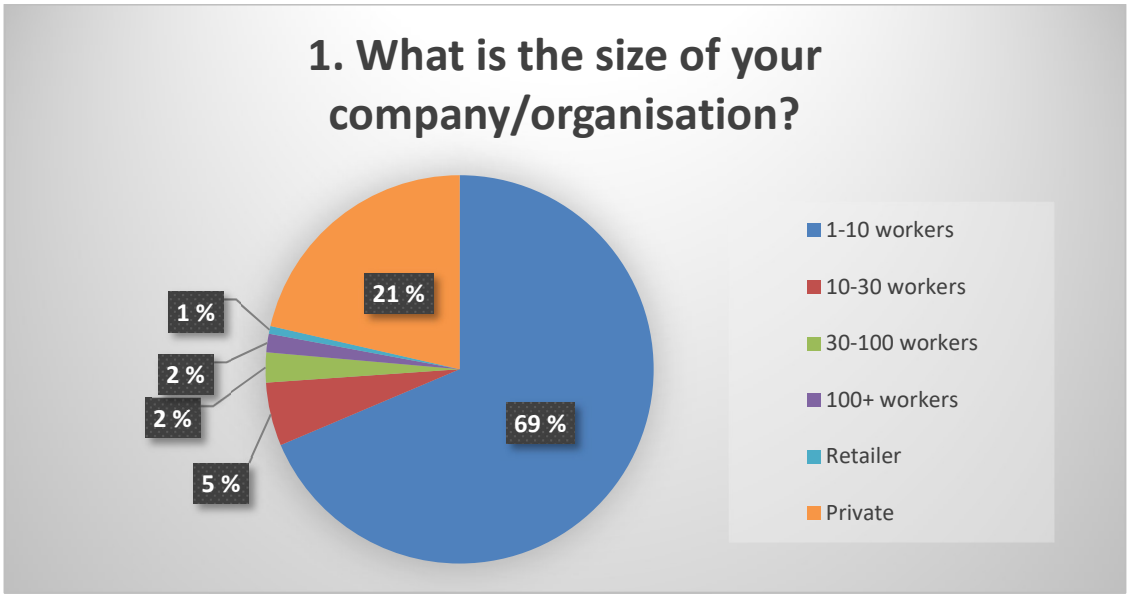


Figure 1 – What is the size of your company/organisation?

221 respondents out of 322 said that they were from a company that has 1 to 10 workers which fits to common knowledge that most of the companies are small. 69 respondents said that they are individual or private person, and therefore they were guided straight forward as this survey was towards the companies not individuals. This also inclines the number of countable answerers to 253 as 69 respondents were moved over to the security part.

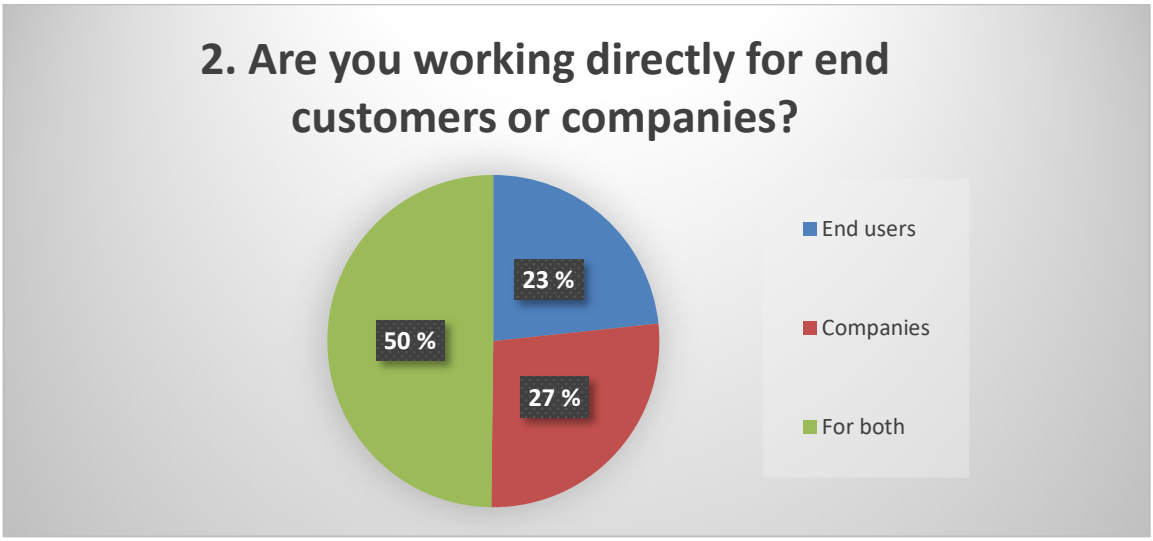


Figure 2 – Are you working directly for end customers or companies?

Majority of the 253 companies were working for both end users and companies. Only 23 percent of the answerers were working straight to the end users. This was expected and will be taken on toll when it comes to compare the awareness between the ones working with end users only versus both or just for companies.

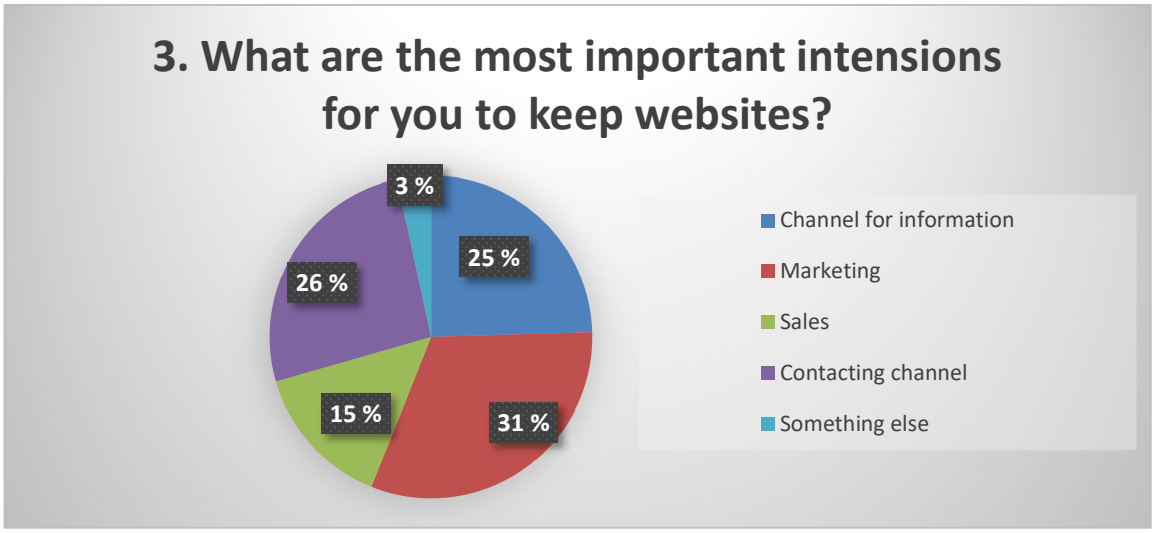


Figure 3 – What are the most important intensions for you to keep websites?

The most important intensions and/or reasons to have websites were marketing as first and then contacting and information channel as divided second place. This goes quite well together with percentage of people having some kind of form on their site, contacting channel, sales and marketing needs to be contacted via websites.

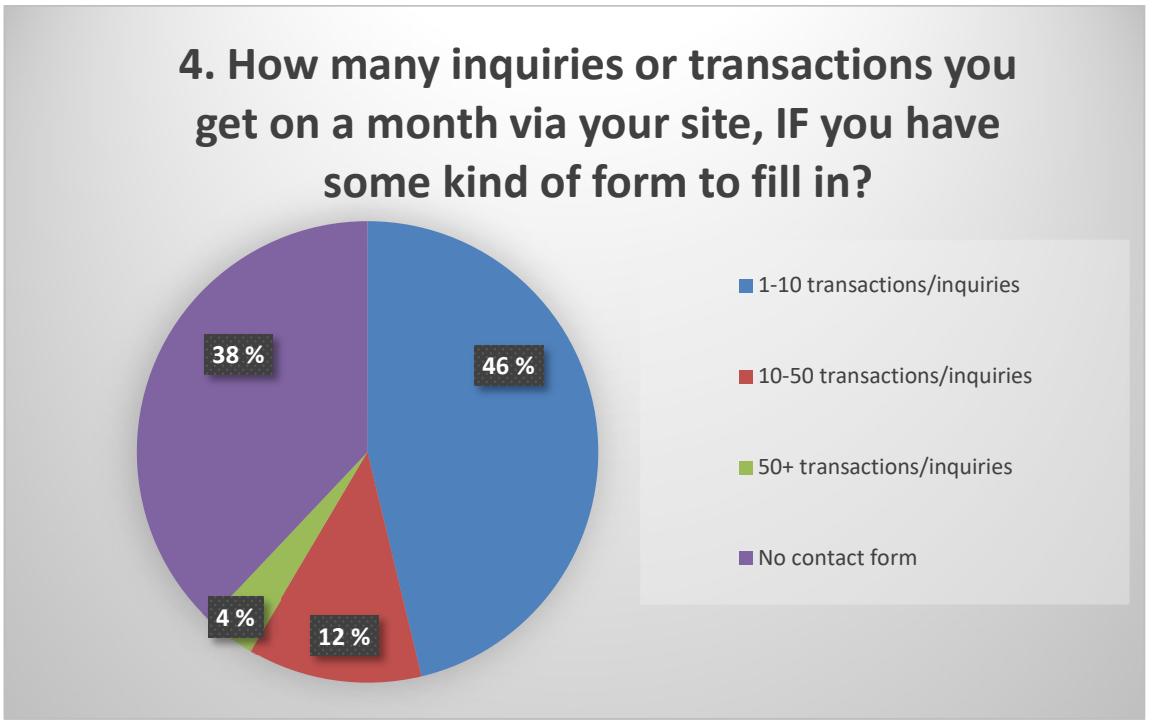


Figure 4 – How many inquiries or transactions you get on a month via your site, IF you have some kind of form to fill in?

Figure 4 shows that a bit over one third of the answerers did not have any kind of form so therefore not that urgent need for SSL -certificate, but the rest of the respondents had some kind of traffic flowing through their sites. This is latter compared to how many of these companies with a form used encryption on their site.

5.2 Questions concerning outside threats 5-7

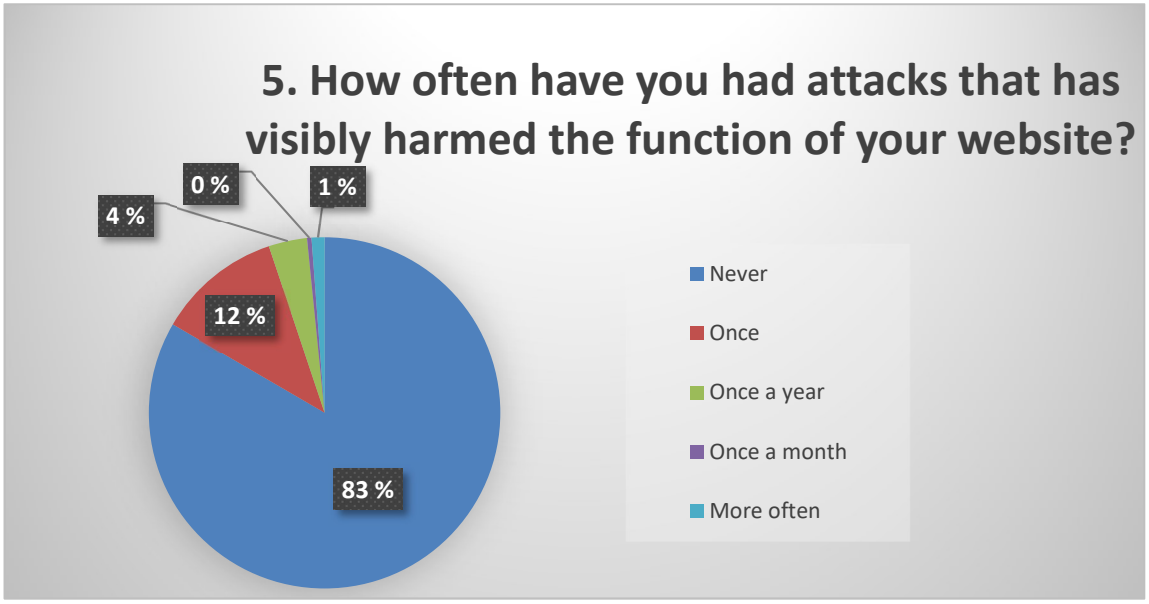


Figure 5 – How often have you had attacks that has visibly harmed the function of your website?

These answers show the possibility and the frequency of how often customers sites have been hacked, over 80% said that they have never confronted any kind of visible attack on their site or that they have not noticed it. These answers were not that expected as author supposed to have more visibly harmed sites based on his work experience, but it is a positive point regarding the customers. Therefore, this section was not as effective as it was meant to be to compare the knowledge to protect themselves from possible threats as the actual attacks were only a rare part of answerers' experiences.

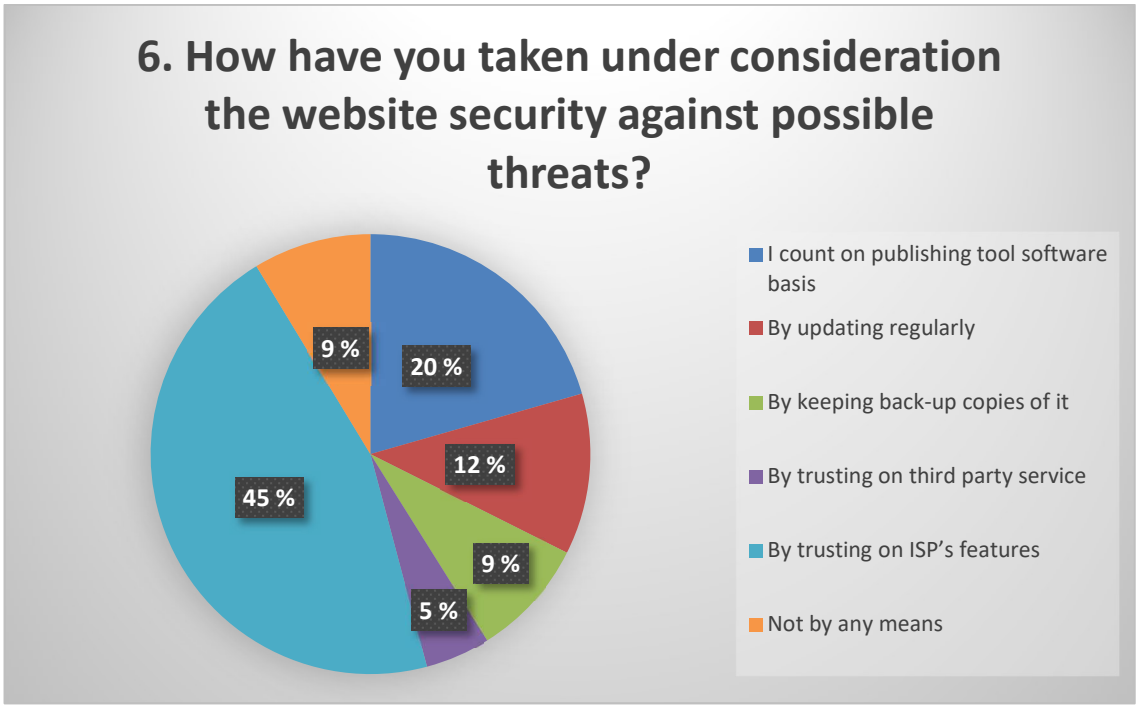


Figure 6 – How have you taken under consideration the website security against possible threats?

Figure 6 shows how companies are taking care of possible threats, most of the clients are counting on their internet service provider's features, even though the right answer would be to update the publishing tool and its applications/plug-ins and keep back-up files of the site so it can be easily fixed. But the after attack fix is normally fastest to be taken care of by the client himself or the ISP's back-ups, so they were not wrong either. The author noticed also that the question could have been stated better by asking "how to prevent possible attacks against your website."

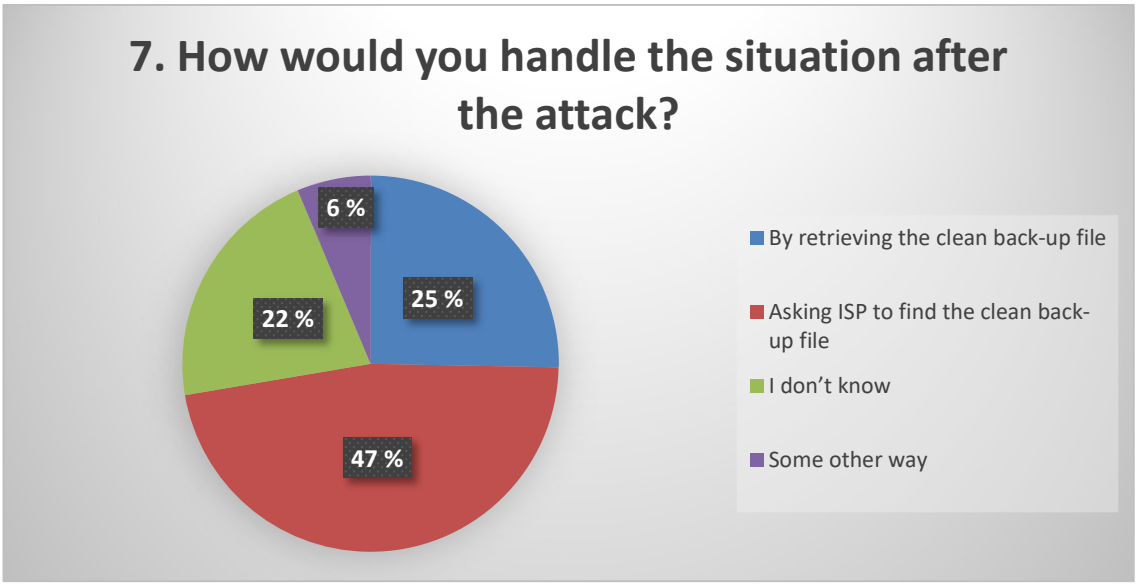


Figure 7 – How would you handle the situation after the attack?

Figure 7 shows that majority of the customers were aware of how to handle situation after possible attack on the site correctly by retrieving the back-up file by themselves or via ISP. This is a positive point versus the author's expected answer generated by his work experience.

All in all, this set of questions shows that customers are well aware of how to react on these possible attacks, even though most of them have not experienced those situations at all.

5.3 Questions concerning secure connection and use of SSL-encryption 8-10

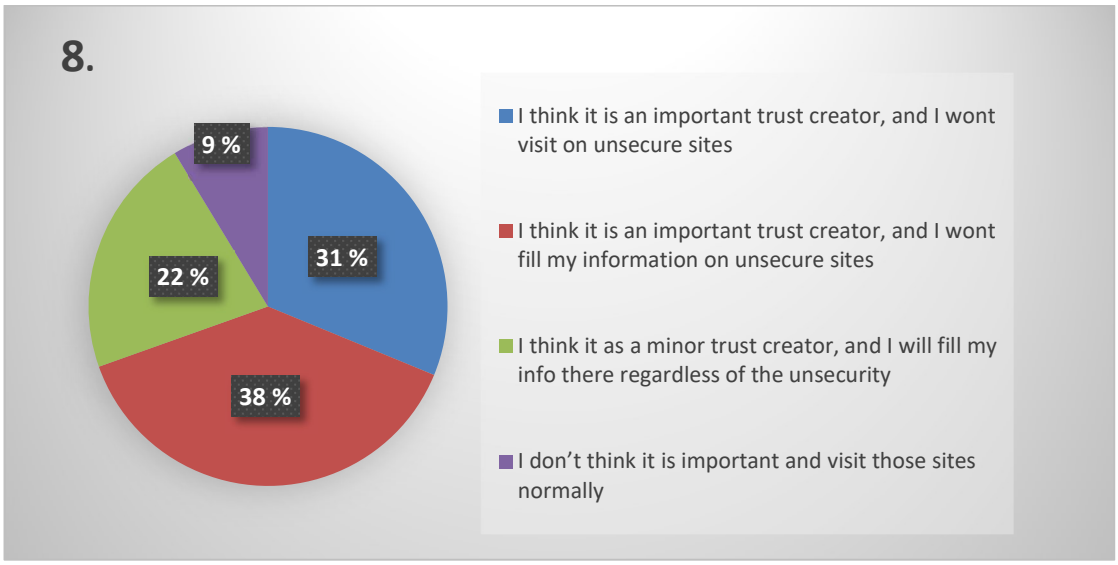


Figure 8 – How are you reacting yourself (or a colleague) that the browsers have started to warn visitors about unsecure sites (http) by a grey icon or even warning on the address bar, instead of secure sites (https) showing lock and safety status on it if the connection is encrypted?

Figure 8 shows the level of importance that companies give to the encryption of the sites, which shows that most of them think is as important trust creator when visiting different sites. The answer is clear, majority of the answerers thought that the HTTPS padlock on the address bar is an important trust creator when it comes to visiting websites. This ratio did not change regarding on the company size as the author expected, which draws a conclusion that this matter was equally known to all sizes of the companies.

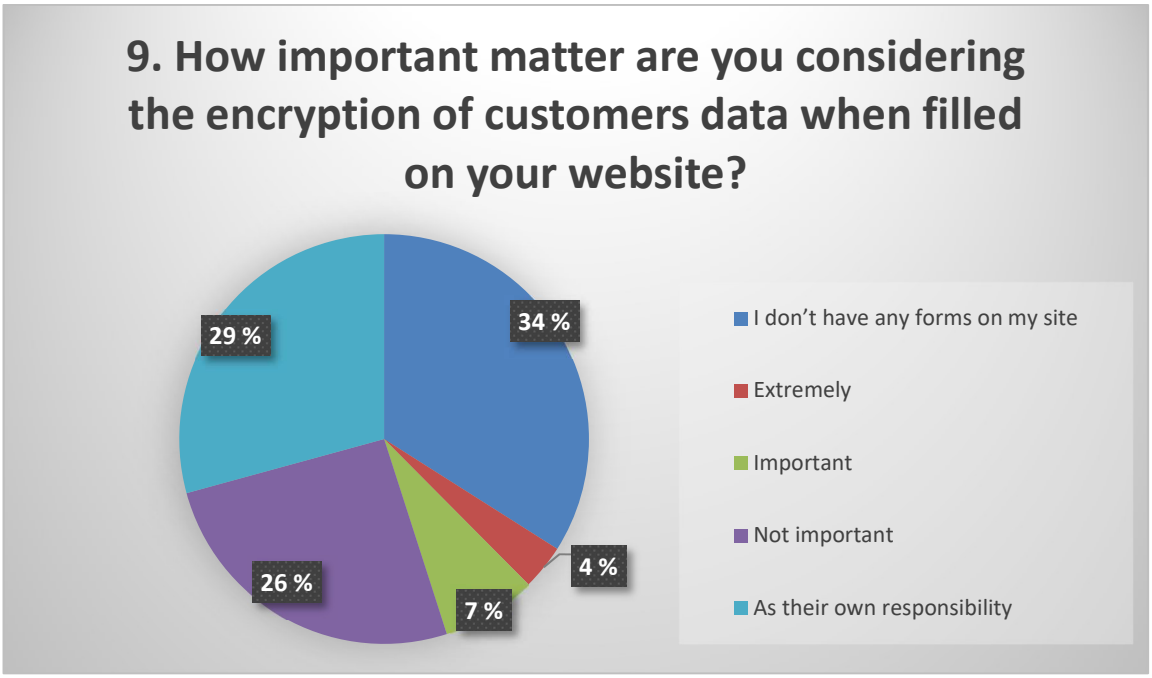


Figure 9 – How important matter are you considering the encryption of customers data when filled on your website?

Figure 9 shows that when it comes to their customers on their website they consider it mostly to be customer's own responsibility even though the customers on their own have no way to affect the matter other than to leave the form unfilled. This can be a serious problem for some companies waiting for contacts with a variety of detailed questions as people are not filling it up at all as they consider it unsafe.

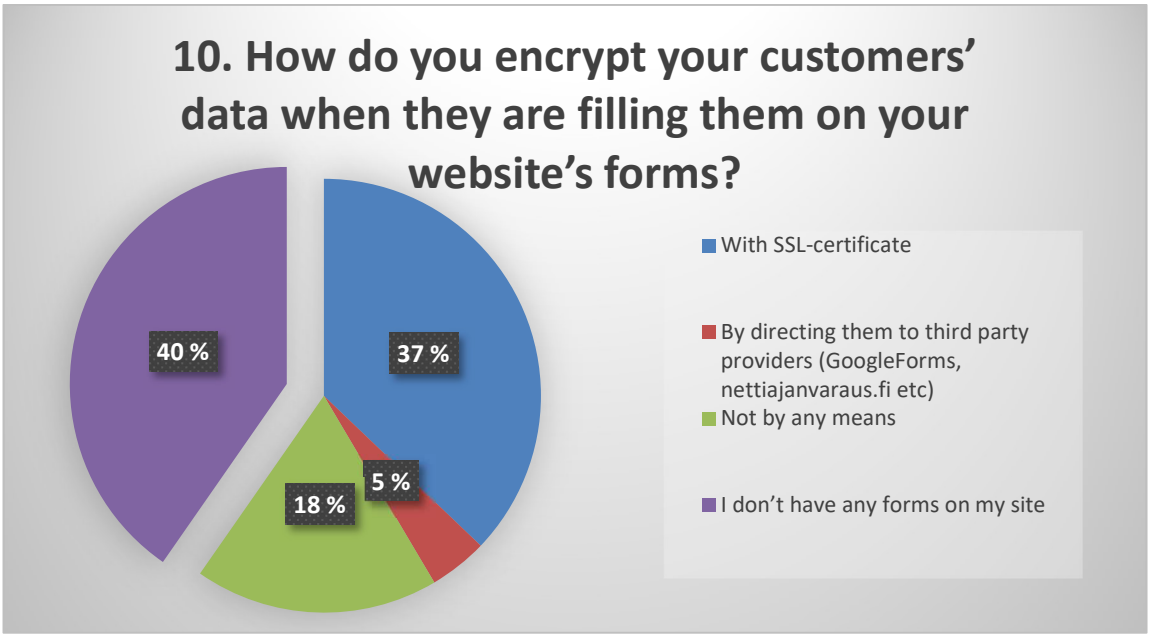


Figure 10 – How do you encrypt your customers' data when they are filling them on your website's forms?

The most crucial question was to find out how many of the respondents are using SSL on their sites if they have some kind of form there as it may lead to leaking customers' personal data to unwanted third parties. As it appeared in the previous two questions it was not on everybody's mind to have encryption on their sites nor giving it lot of importance in the first place. This question showed how this awareness was put into action. 40% percentage of the respondents said not to have a form on their site, which leaves them out of the urgent need of it. Still 60% of the respondents, 152 answerers were left to analyse. This analysis shows rather good percentage, 69%, of an action regarding SSL encrypted sites as over half of them were either encrypted or redirected to third party provider to tackle away the threat.

6 CONCLUSION

This part is to analyse the main findings from the survey and to figure out how do they correspond on the main research goal – to figure out how aware Finnish SMEs are of the internet security and SSL encryption.

When comparing company sizes to the question number eight and the reaction on SSL encryption, the difference between the answers of the companies with 1-10 employees and the companies with more than 10 employees was not expectedly large, couple of percentage points only. So, small companies and big companies react on the same manner when they see notification about the lacking SSL certificate. This way of reacting is acknowledging the problem and mostly not filling out the form locating on the site. 59-62% of the answerers would visit the site normally but not fill in any of their information. This states that their awareness of the issue is on a good level.

When it comes into the importance of encrypting own customers data or pushing it to the customers responsibility, there was a double amount of companies pushing it to customers' shoulders on the smaller enterprises than on bigger ones, difference of 4 percentage points. The same difference was also on usage of fillable form on the site, the bigger companies tend to have forms more certain than the smaller ones. This shows that bigger companies tend to be more aware also about the legislative matters and know their responsibility of encrypting the forms on the behalf of their customers.

When it comes into way of taking care of this matter company size did not have a huge difference. But when comparing how companies said to have form and how they are taking care of them was alarming. First of all, 18% of them answered in the end of the security part that they do not have any type of form on their site (Figure 11). Secondly, 25% of the companies who have a form on their website answered that they are not taking any measures on the issue. This shows that many clients are unaware of the measures that should be taken under consideration on many sites regarding the encryption of the connection when filling in personal data.

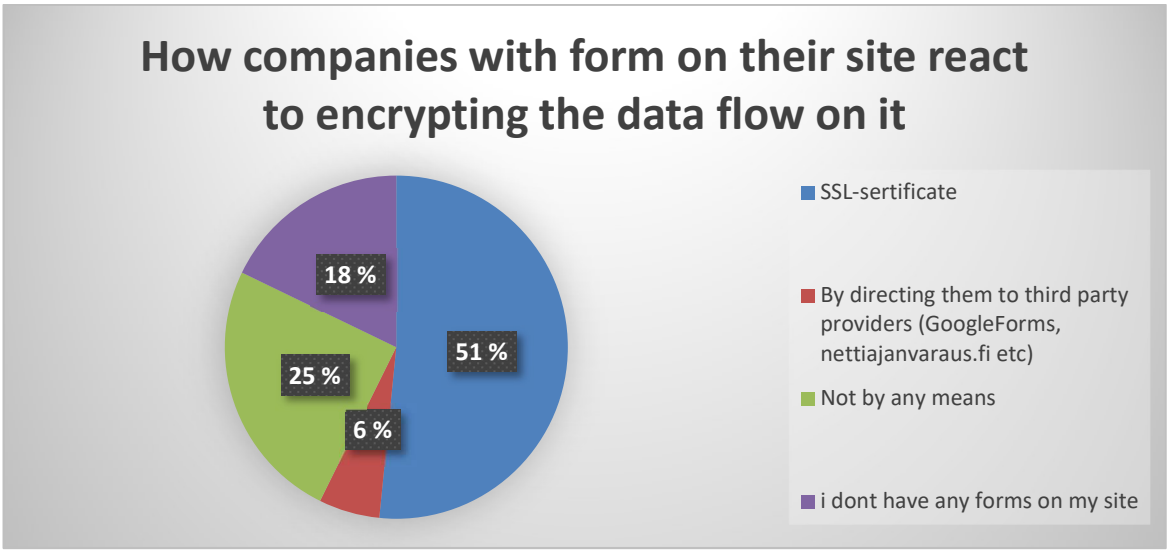


Figure 11 – How companies with a form on their sire react to encrypting the data flow on it

This means that 43% of sites with a form where their client can fill in sensitive information were under threat of leaking personal information of their customers to the public. Even though many of the sites having a form claimed it to be important or very important issue (64%) they have not taken the needed measures to react on it. Or as it shows the customer who did not think it as important issue had not taken any measures towards it, as it is nearly the same percentage.

All in all, it can be concluded from these survey results that the awareness should be raised on the topic of internet security, both from external threats on sites and by encrypting the data flow from the sites as companies think it is on customer's responsibility or do not consider it important. Question 9 shows this clearly as only 16% of the answerers with the form on their site thought the encryption was somehow important for their customers personal data.

As the General Data Protection Regulation is going to be set on 25.5.2018 it is important for the companies to focus on matters like this to avoid possible law cases that it might generate in European and Finnish level of business. Many IT companies, particularly in the health care industry, offer their services to guide Finnish SME's for a safer, regulated way to run their business with personal data flowing on internet.

REFERENCES

Brenner, B. (2017, 3 30). *Sophos*. Retrieved 9 5, 2017, from Let's Encrypt issues certs to 'PayPal' phishing sites: how to protect yourself: https://nakedsecurity.sophos.com/2017/03/30/lets-encrypt-issues-certs-to-paypal-phishing-sites-how-to-protect-yourself/

EU. (2017, n.a. n.a.). *EU General Data Protection Regulation*. Retrieved from Key Changes: http://www.eugdpr.org/key-changes.html

Euronic Oy, /. N. (2016, 11 2). *Nettihotelli - Tiedotteet*. Retrieved from Nettihotellin sivusto: https://www.nettihotelli.fi/?Tiedotteet/2016/2.11.2016%3A_Euronic_Oy_on_ostanut_Nettihotelli_Internet_Oy%3An

FinLex. (1999). *FinLex*. Retrieved 5 7, 2017, from http://www.finlex.fi/en/laki/kaannokset/1999/en19990523.pdf

Helme, S. (2017, 3 6). *Scott Helme*. Retrieved from Let's Encrypt are enabling the bad guys, and why they should: https://scotthelme.co.uk/lets-encrypt-are-enabling-the-bad-guys-and-why-they-should/

Ian, P. (2017, 1 26). *PC World*. Retrieved from Chrome, Firefox start warning users when websites use insecure HTTP logins: https://www.pcworld.com/article/3161778/software/chrome-firefox-start-warning-users-when-websites-use-insecure-http-logins.html

International Telecommunication Union. (2016). *ICT Facts and Figures*. Retrieved 5 7, 2017, from http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf

Kan, M. (2017, 4 28). *Google's Chrome will soon start warning you more about HTTP pages*. Retrieved from PCWorld: https://www.pcworld.com/article/3193143/security/googles-chrome-will-soon-start-warning-you-more-about-http-pages.html

Lehtola, S. (2016). *EmCe*. Retrieved 5 7, 2017, from https://www.emce.fi/blog/uusi-eun-tietosuoja-asetus-astuu-voimaan-25-5-2018-keta-koskee-mitka-keskeisimmat-muutokset/

Lippincott, W., & Wilkins/Wolters, K. (2012, n.a. n.a.). *PubMed Central* . Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4059192/figure/f1/

Lynch, V. (2017, 3 20). *Hashed Out*. Retrieved from PayPal Phishing Certificates Far More Prevalent Than Previously Thought: https://www.thesslstore.com/blog/lets-encrypt-phishing/

Mozilla Foundation. (n.a., n.a. n.a.). *Mozilla Developer*. Retrieved from What is a web server?: https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_web_server

Orgera, S. (2017, 9 8). *Lifewire*. Retrieved from Lifewire - What is web browser?: https://www.lifewire.com/what-is-a-browser-446234

Puumalainen, L. (2017). *SSL-sertifikaattien päivittäminen ja hallinnointi palvelinympäristössä.* Espoo, Leppävaara: Laurea Ammattikorkeakoulu.

Runbox Solutions AS. (2017, n.a. n.a.). *Runbox* . Retrieved from What is spam and how to avoid it: https://runbox.com/email-school/what-is-spam-and-how-to-avoid-it/

Saunders, M., Lewis, P., & Thornhill, A. (2012). *Research Methods for Business Students 6th ed.* Essex: Pearson Education Limited.

Suomen virallinen tilasto (SVT). (2016, 12 16). *Suomen virallinen tilasto (SVT)*. Retrieved from Yritykset 2015: http://tilastokeskus.fi/tup/suoluk/suoluk_yritykset.html

Suomen virallinen tilasto (SVT). (2017, 9 21). *Suomen virallinen tilasto (SVT)*. Retrieved from Käsitteet - Pienet ja keskisuuret yritykset: http://www.stat.fi/meta/kas/pienet_ja_keski.html

Suomen Virallinen Tilasto. (2016). *SVT - Tietotekniikan käyttö yrityksissä*. Retrieved 5 9, 2017, from http://www.stat.fi/til/icte/2016/icte_2016_2016-11-30_kat_002_fi.html

Symantec . (2017, 4 n.a.). *Symantec*. Retrieved from Internet Security Threat Report: https://s1.q4cdn.com/585930769/files/doc_downloads/lifelock/ISTR22_Main-FINAL-APR24.pdf

W3counter. (2017, 8 n.a.). *W3counter*. Retrieved from Browser & Platform Market Share August 2017: https://www.w3counter.com/globalstats.php

W3techs. (2017). *W3techs*. Retrieved 5 7, 2017, from https://w3techs.com/technologies/overview/ssl_certificate/all

Wang, H.-C., & Doong, H.-S. (2007, n.a. n.a.). Retrieved from Validation in Internet Survey Research: Reviews and Future Suggestions: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.104.6984&rep=rep1&type=pdf

Verisign. (2017). *Verisign - SSL certificate*. Retrieved 5 7, 2017, from https://www.verisign.com/en_US/website-presence/website-optimization/ssl-certificates/index.xhtml

Visser, P. S., Krosnick, J. A., & Lavrakas, P. J. (n.a., n.a. n.a.). *Stanford*. Retrieved from Survey Research: http://web.stanford.edu/dept/communication/faculty/krosnick/Survey_Research.pdf

Vänskä, O. (2017). *Mikrobitti - HUIJAUSSIVUISTA TEHTIIN ”LUOTETTAVIA”: 15 000 SSL-SERTIFIKAATTIA AIVAN VÄÄRIIN KÄSIIN*. Retrieved 5 9, 2017, from https://www.mikrobitti.fi/2017/03/huijaussivuista-tehtiin-luotettavia-15-000-ssl-sertifikaattia-aivan-vaariin-kasiin/

Appendices

On this page, attach an enclosed document as its own entity. Instructions for attaching different kinds of enclosures (e.g. docx and pdf) are available in the thesis instructions in Messi.

Appendix 1 Survey in Finnish

Tämä kysely keskittyy suomalaisen yrittäjän tärkeimpiin tietoihin liittyen heidän nettisivujensa turvallisuuteen.

Internet turvallisuus on noussut huolenaiheeksi monelle yritykselle lähivuosina. Yrityksenne nettisivusto on Euronic Oy ylläpidossa ja me olemme kiinnostuneita ymmärtämään mitä keinoja te käytätte pitääksenne sivustonne turvassa ja myös mahdollisen asiakkaidenne sinne täyttämän datan.

Päätarkoituksena on kerätä tietoa kuinka turvallisuusasiat ovat tiedossa ja käytössä jo tällä hetkellä. Prosessissa siis haluamme saada tietoomme kuinka te olette reagoineet teidän sivustojanne koskeviin uhkiin ja selventää mitä mahdollisuuksia on olemassa niiden minimoimiseksi.

Lisäksi kartoitamme asiakastyytyväisyyttä ja WordPress-julkaisuohjelman käyttöä.

Kyselyyn vastanneiden kesken arvomme Woo® -kotisivukoneella tehdyn sivustouudistuksen ja SSL suojauksen vuodeksi.

Kyselyyn vastaaminen kestää noin 10 minuuttia.

(Kysely on osa ammattikorkeakoulua suorittavan opiskelijan lopputyötä "Suomalaisten pienten ja keskisuurten yrityksien tietämys internetsivustojen turvallisuudesta" ja vastauksia käsitellään anonyymisti opinnäytetyön tutkimusmateriaalina.)

1. Minkä kokoinen yritys/yhdistys olette? (Yksityisasiakkaat valitkaa "Yksityinen" ja siirrytte suoraan asiakastyytyväisyys/WordPress kyselyyn.)
    a. 1-10 työntekijää
    b. 10-30 työntekijää
    c. 30-100 työntekijää
    d. 100+ työntekijää
    e. Jälleenmyyjä
    f. Yksityinen
2. Työskentelettekö suoraan kuluttaja-asiakkaille vai yrityksille?
    a. Kuluttaja-asiakkaille

   b. Yrityksille
   c. Molemmille
3. Mitkä ovat teille tärkeimpiä syitä internetsivustojen pitämisessä?
   a. Tiedotuskanava
   b. Markkinointi
   c. Myynti
   d. Yhteydenottokanava
   e. Jokin muu
4. Kuinka monta kontaktointia/transaktiota saatte kuukaudessa sivujenne kautta mikäli teillä on jonkinlainen myynti-, palaute- tai yhteydenottolomake?
   a. 1-10 yhteydenottoa/transaktiota
   b. 10-50 yhteydenottoa/transaktiota
   c. 50+ yhteydenottoa/transaktiota
   d. Ei ole lomaketta
5. Kuinka usein sivustollenne on hyökätty niin että se on näkyvästi haitannut sivuston toimintaa?
   a. Ei koskaan
   b. Kerran
   c. Kerran vuodessa
   d. Kerran kuukaudessa
   e. Useammin
6. Millä tavalla suojaudutte mahdollisilta ulkopuolisilta hyökkäyksiltä sivustoillenne?
   a. Luotan julkaisuohjelman päivityksiin
   b. Päivittämällä sivustoa säännöllisestu
   c. Pitämällä varmuuskopioita sivustosta
   d. Turvautuen ulkoiseen tekijään
   e. Luottaen palveluntarjoajan ominaisuuksiin
   f. En millään tavalla
7. Kuinka toimitte/toimisitte mahdollisen hyökkäyksen jälkeen?
   a. Etsisin puhtaan varmuuskopion ja ottaisin sen käyttöön
   b. Pyytäisin palveluntarjoajaa palauttamaan puhtaan varmuuskopion
   c. En tiedä
   d. Jokin muu

Hyvä apukeino sivustojen hakkerointia vastaan on säännöllinen sivuston ja sen mahdollisten lisäosien päivittäminen. Näin tietoturvataso on julkaisuohjelmien suosituksen mukainen ja verkkorikollisten mahdollisuus aiheuttaa sivustoille vahinkoa on minimissään.

Mikäli näin pääsee tapahtumaan, meillä on varmuuskopiointi aina käytössä ja pystytte näihin varmuuskopioihin pääsemään käsiksi itsenäisesti, tai olemalla yhteydessä meidän asiakaspalveluun.

Sivustoihin vaikuttavia muita uhkia voivat olla erilaiset palvelimeen koskevat hyökkäykset, jotka estävät palvelimien toimimisen ja näin ollen sivustojen näkyvyyden. Näihin reagoimme itse pitämällä palvelimien versioita päivitettynä ja suojattuna.

8. Kuinka itse tai yrityksen sisäisesti reagoitte kun huomaatte selaimen varoituksen salaamattomasta yhteydestä (http) harmaalla ikonilla ja varoituksella

osoiterivillä sen sijaan että se antaisi merkinnän salatusta yhteydestä (https) näyttämällä vihreän lukon ja turvallisuusstatuksen?

a. Pidän asiaa tärkeänä luottamuksen tuojana, enkä asioi turvattomalla sivustolla
b. Pidän asiaa tärkeänä luottamuksen tuojana, enkä täytä tietojani
c. Pidän asiaa kohtuullisen tärkeänä, mutta täytän tietoni sinne suojattomuudesta riippumatta
d. En pidä asiaa tärkeänä ja asioin sivustolla normaalisti

9. Kuinka tärkeänä pidätte asiakkaan tietojen salaamista heidän täyttäessään lomakkeita sivustoillanne?
    a. Ei ole lomaketta
    b. Heidän omana vastuunaan
    c. Ei tärkeänä
    d. Tärkeänä
    e. Erittäin tärkeänä
10. Kuinka suojaatte asiakkaan tiedot heidän niitä syöttäessään lomakkeisiin tai yhteydenottopyyntöihin?
    a. SSL-sertifikaatilla
    b. Ohjaamalla heidät toisaalle (GoogleForms, nettiajanvaraus tms)
    c. En millään tavalla
    d. En käytä lomakkeita sivustollani

SSL sertifikaatti validoi domainin ja salaa ylimääräisellä salausavaimella sieltä lähtevän liikenteen. Domainin validointi auttaa niin Google optimoinnissa kuin tarjoamalla luottamusta tuovan vihreän "turvallisuuslukon" osoiteriville, lähetetyn tiedon salaamisen lisäksi.

Niitä tarjoaa maailmassa muutama iso yritys, joiden sertifikaatit ovat luotettavia. Tämän lisäksi on useita ilmaisia sertifikaatteja, joista osaa on käytetty huijaus- ja tietojenkalastelusivustoilla.

Pienimpiäkin yksilöiviä tietoja voidaan käyttää roskapostin lähettämiseen asiakkaille kun automaatioidut ohjelmat keräävät sähköpostiosoitteet ja oikean nimen.

Appendix 2 Survey in English

This survey focuses on the main concerns of Finnish entrepreneurs when it comes internet safety and safety of their company/ organisation website.

Besides of gathering knowledge of internet security at the present state, this survey's function is to point out facts how internet security should be seen, known, and reacted by the entrepreneurs. During this process it will also teach the most vital factors that have to be concerned when setting up a company page.

Besides of that we are surveying customer satisfaction and usage of WordPress publishing tool

We are organising a raffle between the respondents and the winner will have (rebuild website by Woo website builder and SSL certification

(This survey is part of a bachelor thesis on "Finnish SMEs and internet security" and the answers will be used anonymously as a needed research material)

1. What is the size of company/organisation are you? (Private clients please choose private and you will be redirected to customer satisfaction and WP survey)(retailers)
    a. 1-10
    b. 10-30
    c. 30-100
    d. 100+ workers
    e. retailer
    f. private
2. Are you working directly for end customers or companies?
    a. end customers
    b. companies
    c. for both

Internet as a channel of sales and marketing

3. What are the most important intensions for you to keep websites? (multiple choice)
    a. channel for information
    b. marketing
    c. sales
    d. contacting customers
    e. Something else…
4. How many inquiries or transactions you get on a month via your site , IF you have some kind of form to fill in?
    a. 1-10
    b. 10-50
    c. 50+ transactions/inquiries
    d. no contacting form
5. How often have you had attacks that has visibly harmed the function of your website ?
    a. never
    b. once
    c. once a year
    d. once a month
    e. more often
6. How have you taken under consideration the website security against possible threats?

   a. I count on publishing tool software basis
   b. By updating regularly
   c. By keeping back-up copies of it
   d. By trusting on third party service
   e. By trusting on ISP's features
   f. Not by any means
7. How would you handle the situation after the attack?
   a. By retrieving the clean back-up file
   b. Asking ISP to find the clean back-up file
   c. I don't know
   d. Some other way….

Good action is to keep the websites updated in order to prevent the possible threats of hacking. Then your security level is on recommended level of the publishing tool and the possibility to get harmed is minimal. Even if this happens, our backup-feature is always on and these back-ups can be accessed individually or by contacting our customer service.

Other possible threat opportunities are attacks on servers that will directly be seen as the websites on the harmed server cannot be seen for the public

8. How are you reacting yourself (or a collegue) that the browsers have started to warn visitors about unsecure sites (http) by a grey icon or even warning on the address bar, instead of secure sites (https) showing lock and safety status on it if the connection is encrypted.
   a. I think it is an important trust creator, and I wont visit on unsecure sites
   b. I think it is an important trust creator, and I wont fill my information on unsecure sites
   c. I think it as a minor trust creator, and I will fill my info there regardless of the unsecurity
   d. I don't think it is important and visit those sites normally
9. How important matter you are considering the encryption of customers data when filled on your website?
   a. Extremely
   b. Important
   c. Not important
   d. As their own responsibility
   e. I don't have any forms on my site
10. How do you encrypt your customers' data when they are filling them on you website's forms?
   a. With SSL-certificate
   b. By directing them to third party providers (GoogleForms, nettiajanvaraus.fi etc)
   c. Not by any means
   d. I don't have any forms on my site

SSL certificate validates the domain and encrypt all leaving data by an extra encryption key. Validation of domain helps both in Google optimisation and creating confidence by giving the "safety" symbol on the address bar. There are couple of bigger companies in the world that provides the most trustfully certificates, besides of them there are many free certificates, which unfortunately have been used on phishing sites as they don't confirm company backgrounds so carefully.

Even a smallest identifying data can be used for creating spam mail to the customer as automated systems collect the mail addresses with the name.

Appendix 3. Email template sent to customers in Finnish

Arvoisa "yrityksen x" edustaja,

Haluaisimme selvittää asiakkaidemme tietämystasoa liittyen internetin käyttöturvallisuuteen osana työntekijämme opinnäytetyötä, "suomalaisten pienten ja keskisuurten yritysten tietämys internet turvallisuudesta - henkilökohtaisen tiedon suojaaminen SSL-sertifikaatilla".

Kysely sisältää myös osion liittyen WordPressin käyttöön ja asiakastyytyväisyyteen.

Kyselyllä on tarkoitus herättää kiinnostusta nykyaikaiseen internetin käyttöön ja kerätä ideoita kotisivukoneemme parantamiseksi.

Kyselyyn vastaaminen kestää noin 10 minuuttia. Vastaukset käsitellään anonyymisti.

Vastanneiden kesken arvomme uudelle Woo-kotisivukoneella tehdyn sivustouudistuksen sekä sille SSL-sertifikaatin vuodeksi.

https://www.webropolsurveys.com/S/59F0ADEB1FC5DB01.par

Vastausaikaa on 10.10.2017 asti.

Kiitoksia vastauksista jo etukäteen!

Terveisin,

Euronic Oy

Appendix 4. Email template sent to customers in English

Dear “company x” representative,

We would like to research our customers awareness on internet security as part of our employee’s bachelor thesis, “AWARENESS OF FINNISH SMES ABOUT INTERNET SECURITY- SSL-certificates for personal data security”.

Survey includes also sections concerning the use of WordPress and customer satisfaction.

This survey intends to raise interest on modern day internet usage and to collect ideas to develop our website builder.

Answering to this survey takes approximately 10 minutes. Answers will be handled anonymously.

Between the respondents we will raffle one to rebuild their website on our new Woo-website builder and give one year of SSL-certificate.

https://www.webropolsurveys.com/S/59F0ADEB1FC5DB01.par

Survey closes on 10.10.2017.

Thank you for the answers already in beforehand!

Best regards,

Euronic Oy