LAPIN AMK
Lapland University of Applied Sciences

ESTABLISHING A SECURE B2C E-COMMERCE SYSTEMS WITHIN SME - ANALYSIS OF COMMON SECURITY THREATS

Bui Le Duy

Bachelor's Thesis
School of Business and Culture
Degree Programme in Business Information Technology
Bachelor of Business Administration

2015

LAPIN AMK
Lapland University of Applied Sciences

Abstract of thesis

School of Business and Culture
Degree Programme in Business
Information Technology

Author	Le Duy Bui	Year	2015
Supervisor	Tuomo Lindholm		
Commissioned by	N/A		
Title of thesis	Establishing a secure B2C e-commerce systems within SME: Analysis of common security threats		
No. of pages + app.	78		

This research is focusing on exploring the applications of ICT security within the B2C e-commerce SMEs in Finland. More specifically, this research pursues possible improvements in the areas of security and e-commerce to provide a set of recommendations.

This thesis explores ICT security within B2C e-commerce systems to find the most common security vulnerabilities. The concepts of these two disciplines are not new. However, in terms of security there is room for improvement, considering the rapid advancement of technology and negligence to cyber threats. Moreover, there has been an increase in interest for breaching the security networks within hacker groups. The primary objectives of this research are to explore and propose methods that will provide useful knowledge for implementing a secure platform for both starting and existing B2C e-commerce systems.

This thesis uses both explanatory and descriptive research methodology for conducting the research. In order to answer the research questions and achieve the objectives of the thesis, relevant data were collected from scientific sources in the form of printed or electronic materials, which were published by established authors. The research is of theoretical nature.

The outcome of the thesis research is information about ICT security within B2C e-commerce acquired by analyzing different commonly recognized threats. Resulting in organizations are regarding ICT security and cyber threats in more secure approach by taking appropriate actions and raising awareness within organizations. Moreover, because technology within security develops fast, one should manage security properly. Further research into this topic is suggested as web security is an actively developing field.

Keywords: cyber-threats, e-commerce, ICT security, threats, DDOS, malware, code injections

ACKNOWLEDGEMENTS

I would like to thank you Cristi Marin, Lian Heng, Delia-Catalina Chiuariu and Oluwasegun Famakinwa for sharing their views, knowledge, and time on number of issues relevant to the thesis. Further, I would like to express my deepest gratitude to my supervisor Mr. Tuomo Lindholm for guiding and providing me with invaluable constructive criticism, knowledge, views and motivation.

I would also like to thank Dr. Pirjo Alatalo and Dr. Vladimir Ryabov for support and guidance. I would also like to express my warm thanks to my loved ones, who have supported me throughout the entire process.

Thank you, Bui Le Duy

FIGURES

TABLES

1 INTRODUCTION

This chapter covers the choices of this thesis, and justifies the motivation for conducting the research. Additionally, the target audience for the thesis research are specified with a narrowed scope of the topic suitable for the readers. Moreover, a background introduction to the topic, to aid the readers to comprehend the research is presented. Further, the objectives and motivation for the research work are explained, and the general structure of the thesis is described at the end of this chapter.

1.1 Topic and background

The main topic of the research is the concept of information and communication technology (hereinafter ICT) security threats. The research work explores the business to customer (hereinafter B2C) e-commerce from the perspective of ICT security. In this research, common ICT security threats, different tools, and attacking methods are analyzed to suggest recommendations for enhancing security in the small and medium enterprises (hereinafter SME) B2C e-commerce systems. The cost and benefits of applying potential solutions are discussed as well. The research also examines how recommended security measures can be implemented to create a usable and secure e-commerce environment, which does not hinder business performance.

The primary outcome of the research is a set of recommendations of how existing and starting SME e-commerce organizations may enhance their security systems. A company, which employs less than 250 employees, is referred to as SME in Finland. According to a statistic provided by Yrittäjät (2014), Finland has a total of 322,183 enterprises, from which 99.8% are SMEs. Moreover, these enterprises generate about 50% of all turnovers of Finnish businesses along with the responsibility of 13% on Finland’s export revenue. E-commerce is becoming an increasingly more common phenomenon; therefore enhancing security to attract customers from abroad may help SMEs in Finland to generate additional revenues.

Suggested recommendations presented in this thesis may prepare the organizations indirectly for future threats. Additionally, for the continuation of online businesses, protecting assets should be one of the top priorities. Therefore, this research provides useful information to motivate and persuade the management level of the organizations to actively participate in securing company's assets.

E-commerce is one of the most rapidly growing business models. The world, today has reached an era, where the Internet is the one the necessities of life. The Internet allows one to exercise most of the daily necessities. The convenience and comfort of managing everyday needs, such as communicating, searching for information and shopping has brought the Internet to be one of the most important aspects of one's life. To emphasize the uses of the Internet, approximately 40% of the world population are using the Internet at present, and it is rising in numbers every year (Internetworldstats 2014; Internetlivestats 2015). Moreover, the utilization of the Internet has also brought opportunities to create new technologies, which emerge continuously.

The Internet has developed since it was publicized for the citizens notably. E-commerce has also taken on a large role in taking advantage of the Internet. Consequently, the use of conducting businesses by exploiting the Internet is growing as illustrated in Figure 1.

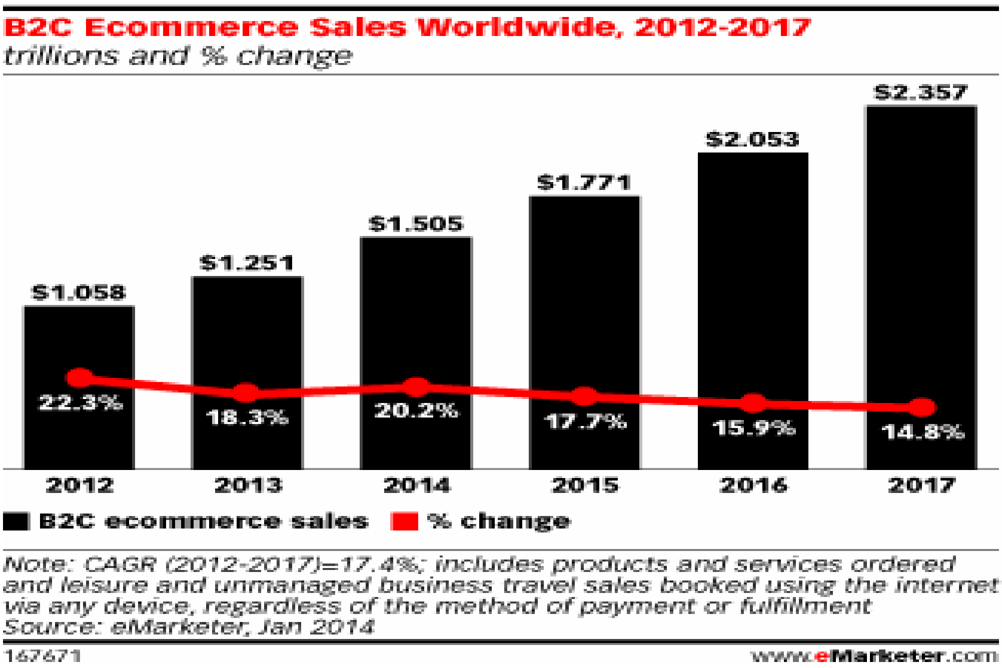


Figure 1 B2C e-commerce sales forecast for following years (adopted from eMarketer 2014)

The trend visible in Figure 1 illustrates the growth of B2C e-commerce sales between 2012 and 2015 and a prediction of sales in the following two years. In Figure 1, the prediction of changes in percentage is decreasing, whereas in sales volume the number is increasing. Moreover, the new thriving industry of mobiles and tablets has brought about new opportunities, which may add even more potential to the B2C e-commerce market, especially in Finland.

Finland is acknowledged as one of the leading countries to adopt new technologies as currently 86% of 16-89-year-old are using the Internet (Statistics Finland 2014). In addition, according to the research conducted on Finnish online behavior, nearly 3.2 million in the 15-79 age range have made a purchase online. Therefore, based on the research that leaves about 24% of Finnish adults who have not purchased online yet. (TNS Gallup 2014.) Additionally, in 2013 the growth of e-commerce sales compared to 2012 is +8.7% and that converts in 10.5 billion euros (TNS Gallup 2013). Therefore, e-commerce may become one of the most profitable business models since both potential buyers and sellers are increasing by the year.

E-commerce is referred to as a buying and a selling process using the Internet. According to Chaffey (2010, 10) “People immediately think of consumer retail purchases from companies such as Amazon”. Nevertheless, e-commerce is much more complex than electronically processed financial transactions between customers and vendors. Chaffey (2010, 10) further states that all electronically processed transactions between an organization and any third party is considered as e-commerce. As such, non-financial transactions, such as customer request for further information are also considered as e-commerce.

Building an e-commerce business may be lucrative, as there are more opportunities compared to physical stores. The opportunities e-commerce presents may be a wider geographical customer reach, 24/7 availability, convenience of customers and less cost of running the business (Shum 2010). Customers are one of the essential elements in running a successful Internet business. Therefore today the Internet is geared towards a user-friendlier approach in satisfying customers. Moreover, different operations are run in the background, such as recommendation and targeted advertisement systems. These systems may be used for gathering information on customer preferences to gain competitive advantages.

The approach of prioritizing customers’ needs when e-commerce business is established may be beneficial. However, the approach may present different obstacles and security discussions. In order to address these different discussions, security should be viewed as a primary foundation preceding attractive and user-friendly e-commerce. However, an attractive and user-friendly e-commerce should not be disregarded as this approach will complement the creation of a successful e-commerce business.

Everything involving ICT may have a vulnerability to some extent because the systems are coded by human beings. Coding is work, which needs 100% concentration, and even then there may be some mistakes. Therefore, there are practices for inspecting written codes. However, regardless of an attempt to review the codes, there may be minor bugs that may never be fixed. These bugs are the ones with a potential to become vulnerabilities.

Following example is presented to emphasize the size and range of ICT vulnerabilities existence. Many new advanced technologies released are bound to have vulnerability. The vulnerability may be there in one form or another, and producers may not know it or may ignore it. Therefore, to conduct the proof of concept research, students of the Switzerland ETH University tested the security of a new technology adopted in newly manufactured cars. The research relayed messages from the car to the key in Passive Keyless Entry System allowing unauthorized access. Therefore, attackers can steal a car without being in physical contact with the key. (Francillon, Davev & Capkun 2010.) With this vulnerability in mind, one should not brush aside security issues. Especially not in the e-commerce systems if the purpose is to establish a successful online business as the e-commerce security may be more complicated than the example. However, according to the research conducted on security issues, it can be seen that security cannot be perfected (Odlyzko, 2010). Nonetheless, by building a secure, operational, and user-friendly system based on the organization’s capacity should be sufficient at first.

1.2 Objective and Motivation

The main objectives of this research are to find solutions to defend or at the very least mitigate security issues within SME e-commerces. This research is focused on Finnish SMEs’ e-commerce systems by providing example cases while presenting potential damages caused by threats. This thesis research is conducted mainly for SMEs, who own an e-commerce system. In addition, this research can be used by SMEs, who want to establish e-commerce business, as it provides useful insight into security issues within e-commerce. As the text written is intended to provide useful information for the management teams or owners of e-commerce SMEs, the research does not cover technical details. However, the research does cover information necessary to motivate to treat security issues with greater importance. Additionally, threats, dangers and effects of not recognizing ICT security threats are emphasized from a management aspect.

An analysis of the most used attack methods and tools is conducted to accomplish the research objectives. This thesis emphasizes the importance of security within SME e-commerce systems. Rather than writing a step-to-step guide, recommendations with arguments are presented concerning different threats and tools. Additionally, possible solutions to defend and mitigate are suggested, and effects of applying the presented solutions are discussed. The knowledge attained from the thesis may be applied and modified to suit the needs and policies of various organizations. However, as the thesis research focuses on B2C SME security issues, therefore it is suggested to be applied in B2C e-commerce businesses.

1.3 Scope

As was discussed previously, this research focuses on motivating the management level to participate actively in the development of the ICT security in their SME e-commerce systems. This research identifies, analyzes and proposes approaches to carry out the protection for the B2C e-commerce organizations.

For the purpose of the thesis work, the research is carried out with selected literature relevant to e-commerce, networking, and web applications. Additionally, security-related literature is used. The scope of the thesis is narrowed down to include mainly external threats executed over the Internet. External threats are actions executed outside of the organization’s network in order to cause losses.

However, there may also be internal threats. Internal threats are mainly threats caused by carelessness, mistakes, and errors. This thesis covers different network and cyber security issues. However, this thesis does not cover instructions on how each system, tool, network are set up.

Additionally, this research does not cover the issues related to the security of operating systems of mobile phones and tablets. Moreover, this thesis does not cover extensive research on third-party systems, such as PayPal. However, recommendations are given to extent of comparison of similar third party business companies, which may complement the B2C e-commerce security. Moreover, law is a complex issue, as the legislation varies depending on business models and geographic location. Therefore, legislation, terms and conditions for the purpose of protecting organizations are taken into consideration throughout this research but are not covered, as this thesis focuses mainly on ICT security.

1.4 Structure of the thesis

Chapter 1 has provided an introductory background to this research, the objectives, motivation and scope of the thesis research. The remaining structure of the thesis is laid out as follows. Chapter 2 discusses the research questions and research methodology. Chapter 3 provides an introduction to ICT security to relate one to the thesis topic. Chapter 4 covers different tools and methods of attacks and motivates the protection against them. Chapter 5 outlines a path and a direction a secure B2C organization should follow, considering its establishment model. Moreover, an importance of security as a whole for an organization is discussed and explained. Chapter 6 concludes the research and discusses the results, and suggests a potential direction for future research.

2 RESEARCH QUESTIONS AND RESEARCH METHODOLOGY

As mentioned in Chapter 1, there is a need to improve the security concerns of ICT as e-commerce is a growing business model. Therefore, this research seeks to find solutions by addressing the three research questions. This chapter also introduces and motivates the methodology for conducting the research.

2.1 Research questions

Based on the research objectives, the research questions are addressed, and steps necessary to answer the questions are presented below.

1. Which are the most common attacking methods within SME B2C e-commerce platforms?

The most popular and common attacking methods are the exploits that attackers will most likely use first. Thereby, these methods must be recognized and understood to gain understanding how SMEs can implement solutions. The attacking types and tools are analyzed, explored, described, and proposed, based on the literature review. Further, news, forums, and videos are examined for deeper understanding to be used for the research. Answers to this research question are discussed in Chapters 3 and 4. In these chapters, background and concept of the B2C e-commerce are covered, along with ICT security. Moreover the detailed analysis of the tools and attacking types are analyzed and defined.

2. What ICT Security measures need to be taken to protect B2C e-commerce organizations from the most common attacking methods?

The research discusses the need of the security within the B2C e-commerce systems and, thereby, to propose a suitable security measures the question has to be addressed. In order to answer this question, the basic concepts of e-commerce and the security related to the B2C e-commerce are needed. The thesis discusses both of the concepts in Chapter 4 and 5. Understanding the attacking types, which is also discussed in Chapter 4 is needed in order to recommend solutions to protect the B2C e-commerce.

3. How can management level staff be motivated to participate actively in protecting their organizations' assets?

In order to answer this question, previous two research questions need to be addressed first. In fact, this question is answered in Chapter 3, 4 and 5. In addition, to motivate people, there has to be a reason for taking the actions and throughout the thesis different reasonings are presented. Moreover, analysis of this research is presented in the conclusion, which is needed as well to strengthen the answer. This question is needed to be answered as this will affect the objective of the thesis, as management level controls the resourcing in organizations. Therefore to motivate the management to take action to secure the organization, convincing management of dangers for neglecting ICT security is needed.

2.2 Research methodology

This research is an explanatory qualitative research. In addition, selected elements of descriptive research are used to further emphasize data gathered. The research is conducted based on the literature review and analysis, along with little empirical data. Different tools, attacking methods and necessary knowledge about computing were attained by exploring various source types. The sources and source types are outlined later in this chapter with criteria for selection. The descriptive research method is an appropriate approach to the research as B2C e-commerce, and ICT security are not new concepts. However, both concepts require further exploring as they are evolving at a fast rate as far as technology is taken into consideration.

The motivation for conducting the research is to develop a set of recommendations for managers. Therefore, another research method was needed, as a descriptive method does not provide a reason to motivate people to take action based on recommendations. The explanatory research was chosen as “theory is created to answer why and how questions” (Cooper & Schindler 2000, 13). The descriptive method describes the phenomenon; on the other hand, the explanatory method explains the reasons for the phenomenon. With explanatory research, the objective of the research can be fulfilled, as it is complementing descriptive research method in this research work.

The descriptive method, on other hand can yield rich data that lead to important recommendations. Moreover, Sachdeva (2009, 15) states that the objective of the descriptive method is to describe things. The descriptive method provides answers to questions as who, what, when and where. However, the method does not provide answers to why and how. According to Krishnaswami and Satyaprasad (2010, 12) this type of research is a “fact-finding investigation”. Based on the citation, the research method is suitable for the thesis, as it provides detailed data on a particular subject. However, the thesis objective is to motivate the management level of the organizations, and this method does not provide answers to answers why and how. Therefore, explanatory research is needed to fill the gap that the descriptive method leaves. Due to the theoretical nature of the research, literature reviews are a primary source of data. For secondary data, journals, articles, videos are used. Tertiary data were gathered from fewer academic sources for understanding and widening the knowledge of the researcher.

The decision for using and searching literature sources is that the sources should be relevant, current as possible and published by established authors by the terms of Lapland UAS. Most of the sources required for conducting the research were found using the Google search engine using relevant keywords respective to subjects required to achieve the objectives. Further, books from libraries and online, in the form of e-books were analyzed to build up credibility on sources found through Google. Secondary sources were found using Google Scholar, EzineArticles and other reputable article directories. There were also sources, which were provided by other means, such as searching websites, which had relevant information. Tertiary sources, such as YouTube were used as references to provide additional information. Tertiary information was used for analyzing the data gathered. The tertiary sources were gathered in forms of videos, interviews found from the Internet, forum discussions. Tertiary sources are noted as less reliable sources compared to academic sources. Therefore, the tertiary data gathered was critically analyzed against academic sources to discover similarities to support the claims from tertiary sources.

3 INFORMATION AND COMMUNICATIONS TECHNOLOGY SECURITY

In this chapter, an introduction on ICT security is presented, and the ICT security is defined as the main objective for e-commerce system development. This chapter also discusses the root of the security i.e., confidentiality, integrity and availability of information. Furthermore, this chapter discusses how security is defined and why it is important.

3.1 Importance of the security of an e-commerce

Security as the foundation is recommended for establishing a successful e-commerce business, as the security level of a system determines the trust that customers have in the organization. Thereby, security should be treated seriously, as it is one of the factors to attract a customer base. For example, customers may examine whether, the website looks appealing and trustworthy. However, when the customers are ready to pay, they analyze the methods of transaction. From this point of view, e-commerce business is recommended to apply security principles into businesses from the very beginning as it will help in building trust between customers and organizations. An advanced B2C e-commerce system can be compared with that of a big city with a vast complex neighborhood, buildings, tunnels, and city areas (Nahari & Krutz 2011, 110). Furthermore, these areas have their smaller tasks to ensure people stay healthy and safe. The comparison of a big city to the security system is similar, except that instead of the city, there is an IT infrastructure. The infrastructure consists of hardware, software, and interconnecting communication network to ensure the safe information transferring.

In e-commerce business, the IT infrastructure design should be secure to ensure the long term business. Many businesses, which do not treat security issues seriously, will most likely fail in the beginning, as there may be little customers who are willing to take a risk to trust unsecured website. Additionally, businesses should be established in a secure manner that will allow all the information is going in and out of the Internet to follow the principles of confidentiality, integrity, and availability (hereinafter C-I-A). However, the security context is not as simple as ensuring information flow. As there is a need to configure, update, and maintain the hardware and software continuity (Nahari & Krutz 2011, 111-112). Besides, the security measures have to be placed and tested against known threats to ensure the effectiveness of a security plan.

There are many different means to create a threat for organizations; supposedly, a distributed denial of service (hereinafter DDOS) is executed at an organization that has a weak security. While the organization focuses on fixing and mitigating damages caused by the DDOS attack, a backdoor virus is sent unnoticed by an attacker. While everyone's attention is focused on the DDOS attack, this allows an attacker to access the database with customers' credit card information. In this example, the DDOS attack was a decoy, and a real attempt was sending the virus to create a backdoor for an attacker. This attack could have been easily prevented if the organization knew how to defend from DDOS attacks. More on DDOS attack and denial of service attack is discussed in Chapter 4.3.

Securing an organization properly is an important work. However, it is necessary for the organization to share a same principle of proactivity. One should think in terms of 'what if – then' principle, for example 'what if DDOS was to happen, then the focus should be on mitigating the unwanted traffic as fast as possible'. One should be proactive and think of scenarios that are likely to occur, whereas thinking of any situation not happening is being naive. Due to a reason there is always a possibility of new threats and new vulnerabilities being used in other situations. The principle of organization policy is one of the factors deciding the dedication the organization has for the security and importance it presents for the organization. Moreover, by applying the principle of prioritizing the security, security may improve over time, and the organization may prevent unseen threats, which do not exist yet.

Security is not static; rather it is an ongoing process where the security has to be always improved to fight off new threats. Attackers have an advantage that the e-commerce organizations do not have i.e. new technology and timing. New viruses, malware, and other malicious software are the new technology. Attackers can create the malicious software out of nothing but codes, or they can find vulnerabilities in current software to create scripts to bypass the security by exploiting the vulnerabilities. Attackers also have the advantage of determining the timing of the attacks. The attack can be prepared for months to create satisfactory malicious code before the attempted attack is executed (Russell, Kaminsky, Puppy, Grand, Graham, K2, Ahmad, Flynn, Dubrawsky, Manzuik, Permeh, Johnson, Pfeil & Lynch 2002, 19). Therefore, to defend from the attacks actively as it happens is futile attempt as no one knows when and how the attacks may happen. However, to proactively defend there are methods allowing one to find those vulnerabilities on a timely basis and to defend assets from probable attacks.

Before building up an organization, there is a need for planning as this will reveal the objectives of the organization and the focus to reach the objective to help the organization to stay on the right path. The first step in establishing a successful e-commerce is to create the business plan (Sage Publications 2015, 6; Banerjee 2007). This thesis focuses on the security aspect; therefore the analysis of the business plan mostly covers the technology plan. Even though it should be kept in mind there are other plans that complement the businesses. The technology plan should outline the equipment and services to be used. Moreover, their functions, weaknesses, properties, and other aspects of the services and equipment should be covered in the technology plan as well (Abrams 2003, 219). As the technology plans are made in accordance with the purpose of the business, C-I-A principles may be applied to the business model.

3.2 Transaction security

As far as security is concerned, both the virtual world and the real world are complex. In addition, there are hypes and advertisements to worsen the situation, as they claim their products secure and the best, thus creating more confusion among consumers. Before the Internet era, there was commerce, which is still going on to this day. In the commerce business model, the customer shops in physical store and pays by credit or debit or any other card that has a sufficient amount of money.

A correct PIN code is needed for making purchases in physical stores. Afterwards, customer's banks and vendors do everything required to confirm the purchase and transfer the correct amount to make the purchase successful. A process of transaction is fast and automatic, and the customer may not know steps of process. However, as long as the purchase is successful, the process is not paid attention to.

If cards that require PIN code are stolen in real life, the card is deemed useless, unless one has the necessary skills for cracking the PIN code. Further, authentication process may be required for shopping with PIN required card. Sales clerks are obligated to check the identity document card (hereinafter ID card) to verify, whether the name matches the one on a credit card. Occasionally, a signature is needed on the receipt to verify the signature matching the back of the card. This verification process assures the consumers the safety use of cards for paying and enhances the security of card payments. Nevertheless, taken into consideration of card security processes, there is a little opportunity for a card from being used by unauthorized personnel. However, a process is more complicated when purchase is performed online, and this is where security may become an issue.

However, the difference between the real world and the Internet is that anyone who gets a hold of one’s card information can use it for making a successful purchase online on websites which do not require further identification. Required information on cards for making successful purchases are owner's name, card number, expiration date, and Card Verification Value number (henceforth CVV number). Furthermore, all the necessary information is located on the card! Therefore, anyone who owns an online or B2C e-commerce business should be extra cautious to not let third party access these card information (Nahari & Krutz 2011, 118). To have a successful business, one has to create a trust relationship between a customer and an organization. Especially online, where the first impression of a website is important, as it can either ward off or acquire a customer, which in time will become owner’s bread and butter. Thus, one should build an e-commerce business based on security as a foundation, by applying policies such as ‘always think of the safety of the customer' policy. However, if the focus is solely on the security, it will affect the attraction of the website. Therefore, the security features should be run in the background.

3.3 Confidentiality, integrity and availability

The C-I-A triad is a widely accepted information security model. The C-I-A triad is an important part of security and when implemented correctly, may significantly reduce the attack possibilities on the organization’s e-commerce platforms (Nahari & Krutz 2011, 77). Moreover, if the principle of C-I-A is applied to the organization’s terms and rules, it can convince consumers that their information is safe. Thus, by creating credibility in organizations will turn into potential income.

Confidentiality refers to a policy of “preventing the leak of data to people who are not authorized to know it” (McEwan 2010). Since the beginning of times, people learned to keep valuable information in secret through experience. The information has to be kept secret for maintaining a competitive advantage. Today, a common sense for merchants is to keep information related to businesses confidential or rather; it is an expectation of the consumers that their personal information will be protected from disclosure. Information, which may be disclosed, can be divided into three categories: customer information, organization information and vendor information.

The information such as credit card information, addresses, and phone numbers can be considered as customer information. Essentially, any information, which is recorded and may point to an individual by analyzing the information, is regarded as personal information. The organization information is the information that can be used against the organization to create damages, such as the topology of the network, website design, and configuration settings. The information such as custom pricing, custom scheduling, and contractual details are vendor information, and they are expected not to be sent to third parties intentionally or unintentionally. The information shared between parties is confidential to build trust relationships between the parties involved. Even though confidentiality as a concept is widely accepted, it is hard to execute to the fullest. However, all confidential information has one property in common. The confidential information could cause a significant amount of damage to the company if it were to be disclosed.

Integrity means that information is protected against unauthorized changes that are undetectable to authorized users (Molie 2005). Integrity is something that one almost takes for granted. Such as web server hosts assume that the database files on their web server will remain untampered, or they believe that the proprietary database system is good enough to maintain the records of their sales correctly. However, all of these examples presented are just one’s beliefs and should not be taken for granted as it may not be true. Therefore, without any integrity checking, one will likely fail. Integrity checking may be the validation of the data to determine the origin of the data and detection of alteration of the data (Nahari & Krutz 2011, 79). As an example of the range of damage the integrity of data may cause, imagine one of the computers within the company is infected with a simple virus that does not do anything serious. The virus modifies all number fives within Excel sheets found by the virus into number twos. The virus then duplicates the Excel sheets across all computers within the network. The virus will not only influence the company, but also business partners that may have the information shared on the network. The virus did not do anything serious however the damage the virus causes may be massive.

Availability means the accessible resources are available to authorized parties at any given time without a failure (Molie 2005). Availability is essential for the business continuation in the long-term. Consumers require access to e-commerce system to purchase the goods, or the business will fail quickly. In the other words, availability may be referred to as the reliability of the system. However, availability and reliability should not be confused with each other. Availability requires that utilized hardware and software are operational and accessible at any given time to its intended authorized users, such as humans and processes. The goal of availability is for the website to be at least 99.99% of the time operational according to the organizations' service-level agreement (hereinafter SLA) (Correia & Abreu & Amaral 2011, 560). For example, if an organization's SLA is agreed upon to be 20 hours online, six days a week, then approximately allowed downtime for the organization is 104 days and 4 hours per 365 days where uptime would be 71.5% (Hazrati 2008). While taking availability into consideration, the software has to be resilient against attack; therefore the software that is used must have features such as self-protection (Nahari & Krutz 2011, 80). Moreover, if the hardware were to fail, the downtime has to be kept in minimal taking into account the ideal 99.99% of the online time. However, 99.99% uptime do not account for maintenance performance. Additionally, topology has to be designed to avoid a single point failure. The single point failure is a state where one of the hardware is not functioning properly, then the whole network is down, and this is not wanted under any circumstances.

In e-commerce business, every moment counts. Many companies had set four-hour downtime as a benchmark for turnaround time before the Internet was dominant. However, such an outage in a Finnish SME e-commerce in modern day could cost on average company thousands of euros (Force10 2007, 1). The process of continual security assessment has been invented to guide organizations in keeping downtime to minimum. Figure 2 presented below is a 3-step continual assessment process.

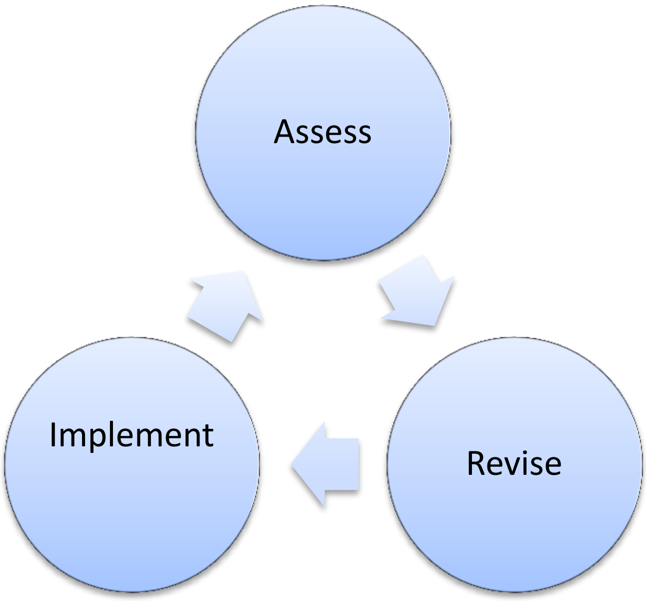


Figure 2. 3-step continual assessment process

As illustrated in Figure 2, a process does not have a starting point or ending point. The process depends on problems in the network of an organization. For example, the organization may need to perform maintenance activities, such as first step would be to implement a patch in a testing environment. For safety purposes, the testing environment should be similar to the one currently in use. After the implementation is performed, the system is to be tested which is second step. An assessment of the influences of the system has to be analyzed and verified on the basis of testing. Additionally, assessment is necessary to verify if there is any new vulnerability created while applying the new patch, as there is possibility that the configuration files may replace the old ones with default settings during implementation. Thus, potentially leading additional services and protocols to be opened or re-enabled. Therefore, the third step is to revise and verify the effect of the patch on security and availability. The process is ongoing and should be performed with new software, hardware, patches and updates before application on real system. The process displayed in Figure 2 is a simplified version and can be further broken down into different variations to include more detailed actions within each step to accommodate the business plans.

4 THREATS AND TOOLS

This chapter is dedicated to discussing common threats, tools, and attacks used by with malicious users. According to KPMG report, Finland has a false sense of security within organizations. Moreover, nearly half of the organizations who participated in the study by KPMG have been breached by a third party. (KPMG 2013, 2.) As mentioned in Chapter 1, this chapter does not cover in great detail of how the tools can be used, as it is not the scope of the thesis. However, the chapter focuses on analyzing the effects of different cyber threats on Finnish SMEs. The following criteria is used for selecting the tools, methods and threats. First of all they are common according to different sources; secondly they cause damages; thirdly they are deemed dangerous; fourthly they are difficult to handle and lastly they may render businesses useless.

4.1 Malicious users

A hacker as a word merely suggests an experienced computer technician. In other words, hackers are referred to as computer experts, who may have a deeper knowledge of a specific subject (Neder 2012; Freedman 2007). Subjects such as creating open source software or specializing in compromising computer securities are common features in hacker society.

In coding culture, those who may know a little about computers, such as ‘script kiddie’ and ‘hacktivist’, are not considered hackers. Truly, there are only three types of hackers, which can be divided into white hat hackers (hereinafter WHH), black hat hackers (hereinafter BHH) and gray hat hackers (hereinafter GHH). Blue hat hacker is not taken into consideration as they perform similar activities to WHH, but blue hat hackers are usually offered by third party services, such as organizations offering pen-testing services (Witherspoon 2010).

WHH can be referred to as security experts, as their main purpose is to find vulnerabilities within systems to enhance the security system (Murray 2011; Lindsay 2007). Recently, many big organizations such as Google and Yahoo!

implemented ‘bug bounty program’, where WHH would find vulnerability in exchange for a payment. WHH are considered good hackers or ethical hackers as they follow ethics and do not use their hacking skills for malicious activities.

BHH are the opposite of WHH and they are the hackers which media usually focuses on. BHH violates security vulnerabilities for personal gains, criminal activities, or purely for maliciousness taken by their emotions. BHH are considered computer criminals, which perform illegal activities. These types of hackers are dangerous, and organizations should be aware of the threats they represent (Franklin 2007). Moreover, BHH will do anything to gain access to data if they find even the slightest vulnerability in the target system.

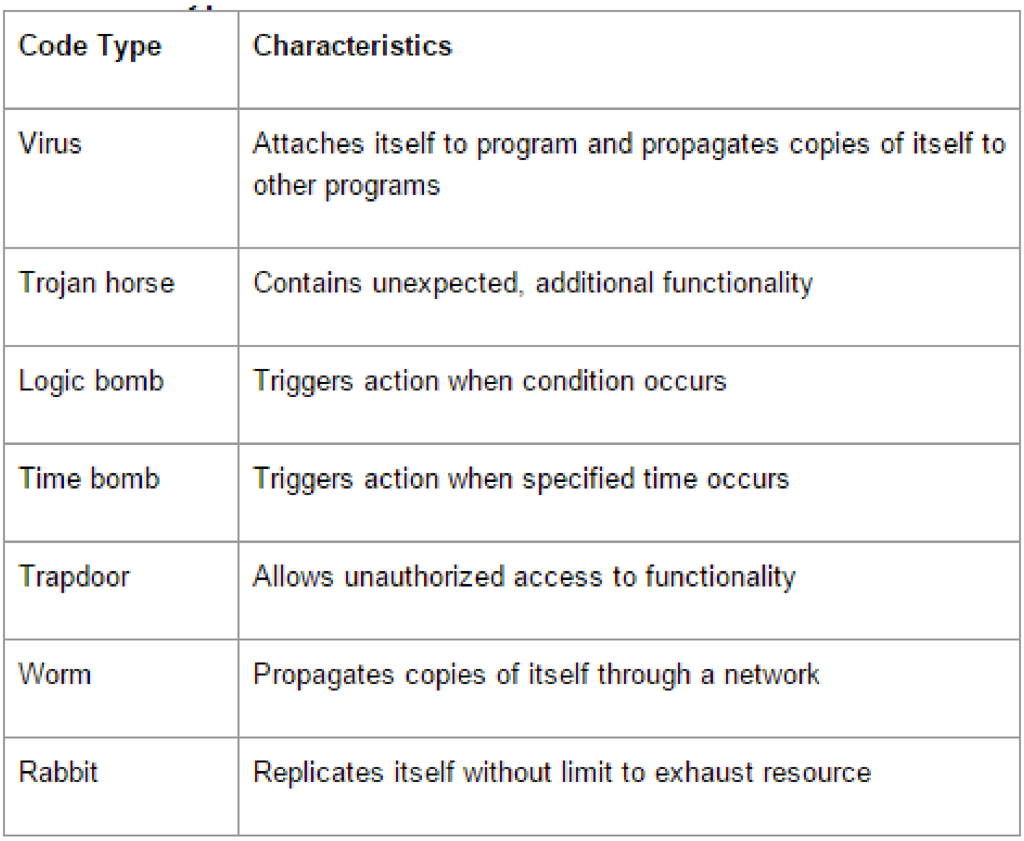
Lastly, there are GHH, and these are hackers, who do not fit WHH or BHH behavior. GHH may not work for their personal gains; however they may commit unethical practices (Witherspoon 2010). For example, WHH asks permission before compromising a system and then reports the results of the system vulnerabilities back to the organization. On the other hand BHH compromises the system without permission, in order to gain some data, which may be useful for blackmailing or selling information to third party. GHH on other hand would compromise the organization’s system without permission, and they might notify the organization afterward, or disclose the vulnerability publicly. In GHH example, GHH did not use their access for criminal purposes. However, compromising the system without permission is labeled an illegal activity by law. On security perspective, GHH could also be considered as a dangerous entity.

Major ethical differences allow for differentiating between the three types of hackers. However, a hacker might not continue to operate under the same ethics for a prolonged period. Thus, BHH could become GHH or GHH become WHH. Therefore, organizations should be prepared for every possible scenario.

4.2 Malicious software (malware)

Malware is software, which has a malicious code integrated into it. Malicious code is a term used to describe written codes that cause damages to computers or a system. Forms of malicious codes may include executable scripts, worms, viruses, Trojan horses, logic bombs, time bombs, and backdoors. Table 1 presents the types of malicious codes with their characteristics.

Table 1. Characteristics and malicious code types (adopted from Pfleeger & Pfleeger 2003)



Code Type	Characteristics
Virus	Attaches itself to program and propagates copies of itself to other programs
Trojan horse	Contains unexpected, additional functionality
Logic bomb	Triggers action when condition occurs
Time bomb	Triggers action when specified time occurs
Trapdoor	Allows unauthorized access to functionality
Worm	Propagates copies of itself through a network
Rabbit	Replicates itself without limit to exhaust resource

Table 1 describes the characteristics of each malicious code type, and as described, each of them differs in behaviors. These malicious codes will turn into malware in final stages when they are ready-to-use software. Most common malicious code types encountered are viruses, worms, and Trojan horses.

However, it would benefit organizations to keep in mind the existence of other malware and their characteristics as well.

The damage caused by security incidents to an organization is related to the size of it, which means, the larger the organization, the greater the damage. There is a clear trend that shows security incidents grew globally in 2014 by 48% compared to 2013. This growth is equivalent to 117,339 attacks per day. (PwC 2015.) Therefore, increase in awareness of ICT security is required urgently, as it is evident that security incidents are increasing rapidly. The most frequent news about cyber threats in Finland is about phishing attempts. The latest scam where a fake website tricked people to give banking credentials using different reputable collecting companies' names, such as Finnish national post organization, Posti and customs, Tulli. The scam cost SME enterprises and individuals in total approximately half a million euros (Vänskä 2015).

4.2.1 Viruses and worms

A virus attaches itself to a file and spreads itself as a copy to other computers through a network. The difference between the two is hard to distinguish, as a worm is a subtype of a virus. However, a virus needs human interaction, or a pre-command of time trigger in order to spread. On other hand, worms can replicate itself without human interaction, thereby worms may be considered more dangerous. Additionally, worms can spread to other networks if there are vulnerable flaws in the network of the organization.

Viruses and worms can be used in conjunction with other malicious methods in order to create new threats to organizations. Worms and viruses are deployed with malicious activity in mind, regardless of a goal of being financial gain, blackmailing or crippling the network (Whitty 2014). There is a need to protect against worms and viruses if a secure e-commerce system is an aim. Very frequently, the viruses and worms are spread through e-mail or files sent by attacker. Therefore, hackers will most likely target organizations' email system. There are no exact methods to determine the damages viruses and worms could cause an organization. Regardless, one should keep in mind that viruses and worms are dangerous to every organization it affects.

There are no definite methods to protect or defend from viruses and worms. The only choice is to increase the security and abandon the bad habits of opening unknown files and attachments. The least that can be done is keeping the system updated, installing a quality firewall, monitoring traffic, downloading files only from reputable websites, and not opening suspicious files or emails. However, there is estimation that roughly 50% of the recipients working in the Finnish organization still open e-mail attachments which are unknown and not related to work (KPMG 2013, 5). Additional layer of defense is to have the best available anti-virus (hereinafter AV) at the time. According to Selinger (2014) at the present, the best AV is BitDefender. If these guidelines are followed, one should be safe. However, no one can be 100% safe, as there is news of NASA, the Pentagon, and even the White House being infected by new viruses. The term ‘zero day virus’ is often used to describe previously unknown computer viruses or malware.

4.2.2 Trojan horses

In the computer world, a Trojan horse has a same hidden function as the wooden horse in Trojan War. The Trojan horse term is from a Trojan War tale where ancient Greek soldiers were hidden inside a giant wooden horse as a gift. While Trojan soldiers were sleeping at night, the Greeks took over the city of Troy by surprise, once the Trojans took the wooden horse inside the city. The Trojan horse malware itself is not harmful, but it releases a group of malware, such as viruses, worms, adware, spyware, key loggers and bots and in this aspect it resembles its origin. The characteristic of Trojan horse is to look like a legitimate program, which may intrigue users to open it. In order to protect an organization from malware, the most important factor is to have a good anti-malware tool or software. Choosing between the multitudes of available options may be difficult, but according to test done in 2014 by Selinger (2014), the best one at this moment is Malwarebytes. Malwarebytes is free but has an upgraded version to include AV as well. For those people who believe that paying may get one better quality, BitDefender is the option. However, even if one has the best tools but is not aware of actions in regards of what to download and what to open. There is still a high risk of being infected.

4.2.3 Backdoor

Backdoor is a method of bypassing authentications and securing unauthorized access to a computer. Backdoor can be either a virus or “an undocumented entry point to a module” (Pfleeger & Pfleeger 2003, 4). An entry point backdoor is usually created by the manufacturer, and it may not be created with ill intention, but for testing, or for the maintenance purpose of the finished program. Many times, these backdoors are created in a production state and are either intentionally forgotten or indeed forgotten once the project is finished. Either way, the backdoor is a threat to users.

An example of backdoor access could be an ATM built by a company that has a PIN code to access the admin system. The ATM manufacturer has set the PIN code to default and this PIN is documented on the Internet for instruction purposes. Nevertheless, the criminals who found this PIN exploited countless ATMs manufactured by the company. Thus, the criminals gained access to the admin rights, and they can operate the ATM to release all the available money. The purpose of the PIN code that leads to a backdoor exploit may not have been intentional, but it was a mistake that was abused with ill intention. Moreover, it could have been avoided if the company were more alerted.

Another type of backdoor is created by hackers by using malicious codes, such as Trojan horses, worms and viruses allowing them to have illegal access to a system. Hackers use these malicious codes to set a backdoor for themselves to access a system without the authorization of the system owner. Thus, attacks through backdoors may endanger the confidentiality of customer data. As noted in Chapter 3, confidentiality is a policy to prevent unauthorized personnel to see data that were not meant to be seen. However, as these backdoors are created using the malicious code; therefore the protection uses technology of ICT. Most of all, the detection, and the protection software should be up to date, as the backdoor access works only if the system is infected with malware sent by hackers.

Joomla is one of the most popular content management systems (hereinafter CMS) along with WordPress and Drupal used in Finland. Joomla CMS was found to have a core integrated code by developers that allowed the attackers to create a low profile backdoor. This backdoor is proven to be vulnerable and not easily detectable (Souza 2014). As such, one should be aware of vulnerabilities within each CMS to be able to create more secure e-commerce if the website is built using CMS.

4.3 Denial of service attacks and distributed denial of service attacks

DDOS, which is an advanced version of its precedent, Denial of service (hereinafter DOS), are attacks to slow the victim's server. There is a difference between DOS and DDOS. In DOS, a large number of requests are executed from one computer, making a server block the attacks easier. However, in DDOS, the attack is carried out by using multiple devices simultaneously. The attacks are executed by sending a large number of false data that imitates the real data to the server. The attacker is trying to block the server from retrieving data from legitimate users, who want to access the data. DDOS and DOS undermine the availability of service for the customers, thereby endangering the business-customer relationship.

As an example, attackers bombarded Osuuspankki bank with a large number of data requesting the server to search some terms (Yle 2015). While the server is busy with all the requests sent by an attacker, other customers may have a slowed connection to the banking service, or may encounter timeout errors. DOS and DDOS represent overflowing the server, thus making the server unable to accept other requests from other users. However, many businesses in

Finland require accessing online banking services for business transactions and by not being able to do so may bring businesses to halt.

In order to protect a business from DDOS or DOS attacks, e-commerce organizations should undertake activities to mitigate the effects of these attacks. These activities are such as acquiring network routes that are capable of identifying attacks and acting on transferring unwanted traffic away to reduce the bandwidth usage of the server.

The DDOS are most of the time executed with a help from botnets. Botnets are networks compromised of infected and unaware computer users. By flooding a server with possibly ten of thousand simultaneous requests from different computers, the stability of a system becomes challenging task to maintain, even for the most security organizations in the world. As mentioned in Chapter 3, attacks such as DOS or DDOS are intended to threaten the availability of services and with such attempt, many organizations may be brought down by causing massive damages. Moreover, the tools for executing DOS and DDOS attacks are not difficult to obtain. These tools are readily available to anyone on the Internet freely or in exchange for charges as little as 6 dollar (Protalinski 2014; Shankdhar 2013). Allowing even the most basic users of computers can execute DOS attack, as it is easy as clicking a button. Therefore, organizations should treat this threat with greater attention.

A Botnet is a cloud-based distributed network under one’s remote control. Thus, botnet can be referred to as an army of online robots. Botnet computers are sometimes referred as ‘zombie computers’. The attackers will have computers under their control without the owners consent and knowledge by spreading malware across the Internet. These controlled computers can be used to achieve the desires of the attackers. As these botnets are mostly used for the purpose of criminal activities, the attackers are, therefore, cyber criminals.

There is little that can be done in preventing DDOS from happening because the attack is brute-force that uses the Internet itself. However, the mitigation of

DDOS attacks is possible. One could use an Internet service provider (hereinafter ISP) for mitigating DDOS, as usually ISPs have more bandwidth thus, they can handle more requests or traffic. However, there are few problems if an ISP is used for mitigation because ISPs are selling bandwidth, which means their core interest is not protecting businesses. Therefore, their resources may not provide up-to-date DDOS solutions. Additionally, enterprises nowadays tend to have multiple ISPs to prevent single point of failure; therefore it may be little costly if multiple ISPs offer DDOS mitigation service. Further, ISPs only mitigate DDOS attacks on their network, not the ISPs linked within the organization network.

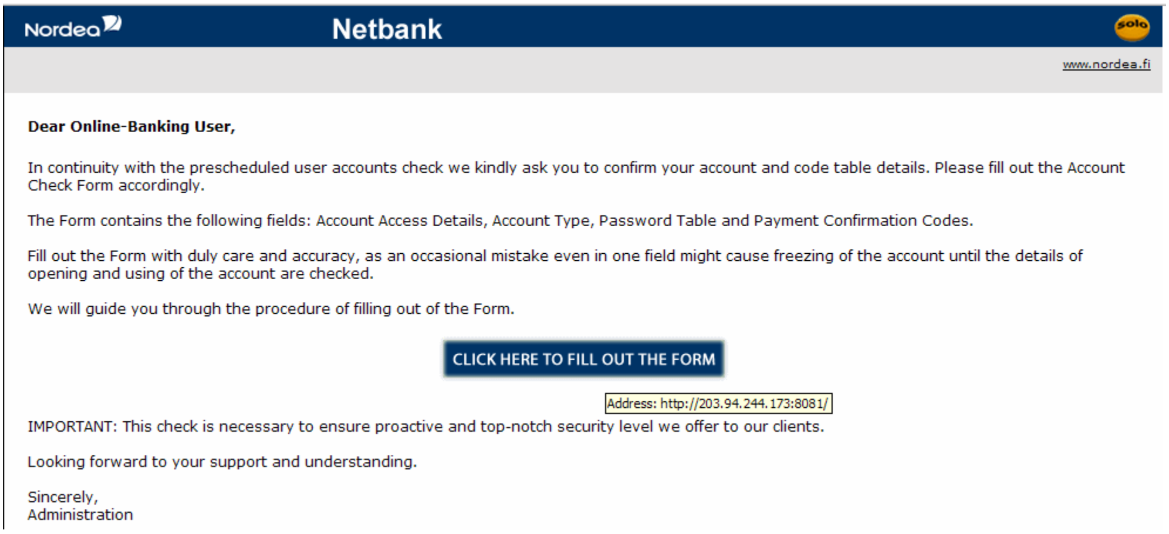
In order to attempt to filter bad requests, there are some DDOS specialized physical devices, which can be placed in between the organization network and the Internet. However, these are costly and require skilled security experts working on updating and maintaining these devices. Therefore, the solution of ISP and physical device may not be optimal for starting companies or companies that are in difficult position because of financial matters.

The current recommended practices for mitigating DDOS involve cloud mitigation provider. Cloud mitigation providers are specialized in providing DDOS mitigation from the cloud (Leach 2013). The mitigation providers have large bandwidths, network and security experts and necessary hardware for the job. These solutions offered are to be used for enterprises which need DDOS protection. For those with e-commerce platform, it is recommended to inquire about the DDOS policy within the platform or service providers selected.

4.4 Deceptive attempt to gain confidential information

This chapter discusses various method hacker uses for gaining confidential information. The threat itself may not be directly related to the organization security, but these threats should be studied to enhance the security for customers. For instance, a report states that mistakes caused by insiders can cause more damages than external threats (PwC 2015). Moreover, Finnish organizations deemed phishing attacks, along with malware, as the greatest threats (Kauppakamari 2015). Therefore, the threats may not be cyber-related, but it damages organizations if it is neglected.

Phishing is popular scam. Phishing is referred to a criminal activity attempting to gain sensitive information through e-mail. Many times, the criminals will act as a bank or any other credible organization requesting personal information or tempting the staffs to open a malicious link. These links, which direct to a website, may not be legitimate regardless how the outlook appear similar to the origninal website. Therefore, there is a need for verifying the authenticity of the link. An attempt of replicating a legitimate website for stealing personal information is called spoofing. Figure 3 depicts a possible fake spoofing website.



Dear Online-Banking User,

In continuity with the prescheduled user accounts check we kindly ask you to confirm your account and code table details. Please fill out the Account Check Form accordingly.

The Form contains the following fields: Account Access Details, Account Type, Password Table and Payment Confirmation Codes.

Fill out the Form with duly care and accuracy, as an occasional mistake even in one field might cause freezing of the account until the details of opening and using of the account are checked.

We will guide you through the procedure of filling out of the Form.

CLICK HERE TO FILL OUT THE FORM
Address: http://203.94.244.173:8081/

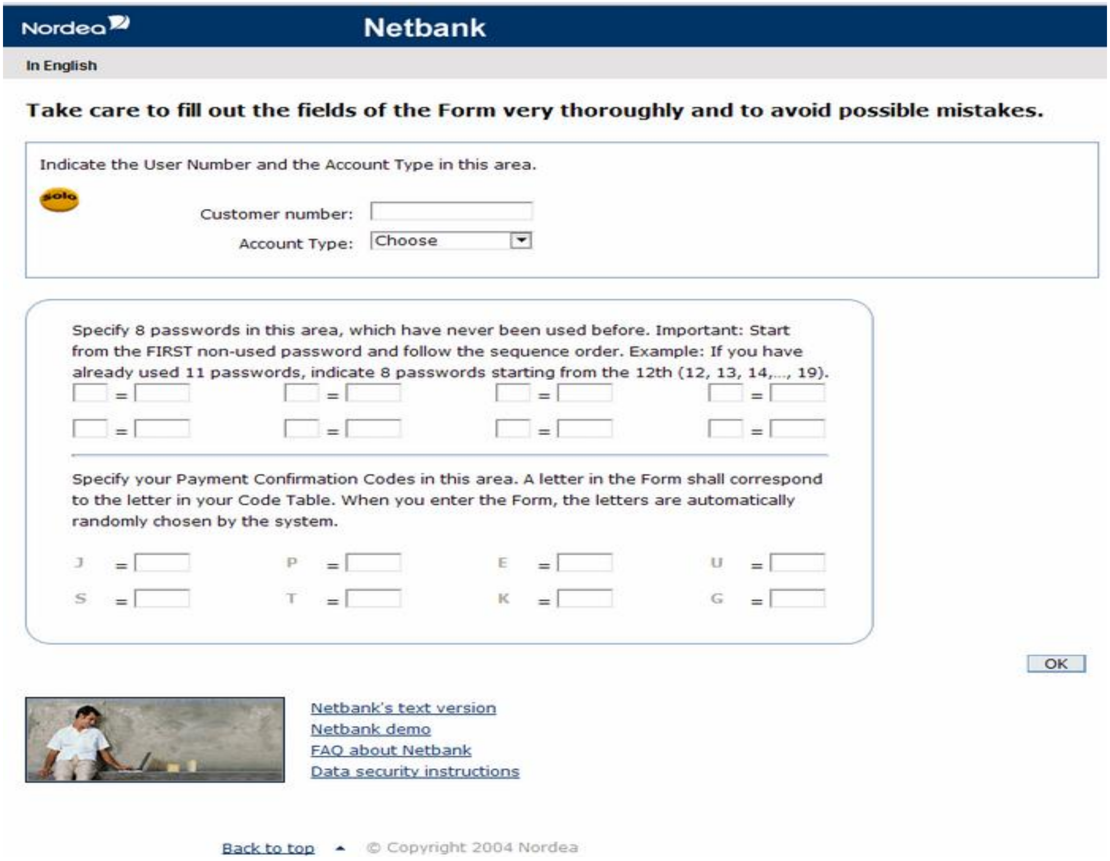
IMPORTANT: This check is necessary to ensure proactive and top-notch security level we offer to our clients.

Looking forward to your support and understanding.

Sincerely,
Administration

Figure 3. Scamming site – Nordea part 1 (adopted from ICT Driving License 2014)

Figure 3 illustrates a common scamming method, which exploits the identity of reputable organizations through the fake website, such as banking websites or different organizations' websites. The purpose of this scamming method is to act as an authority to gain confidential data from victims. In the case of Figure 3, the authority is the administration of Nordea bank. These kinds of messages can trick people who have a little knowledge of cyber threats and computers. Therefore, in most cases with the urgency message, victims will click on the link attached to an email. However, Figure 3 illustrates a verification process to determine the authenticity of the source by moving a mouse on top of the button ‘Click here to fill out the form’. A small window appears when moving the mouse on the button, which helps in verifying genuinity of the website. The Figure 3 example is a fraud website as real the address of Nordea would be starting with ‘https://nordea.fi/’. With this practical action, the address in Figure 3 is confirmed to be a fake website, and as such it should not be clicked on. However, if one does click on the button, Figure 4 illustrates the next step that criminals would possibly perform.



Take care to fill out the fields of the Form very thoroughly and to avoid possible mistakes.

Indicate the User Number and the Account Type in this area.

Customer number: □

Account Type: Choose ▾

Specify 8 passwords in this area, which have never been used before. Important: Start from the FIRST non-used password and follow the sequence order. Example: If you have already used 11 passwords, indicate 8 passwords starting from the 12th (12, 13, 14,..., 19).

□ = □ □ = □ □ = □ □ = □

□ = □ □ = □ □ = □ □ = □

Specify your Payment Confirmation Codes in this area. A letter in the Form shall correspond to the letter in your Code Table. When you enter the Form, the letters are automatically randomly chosen by the system.

J = □ P = □ E = □ U = □

S = □ T = □ K = □ G = □

Figure 4. Scamming site – Nordea part 2 (adopted from ICT Driving License 2014)

As mentioned previously in Figure 3, after the button is clicked new website appear requesting for the confidential information. As Nordea banking system uses one-time login passwords with unique customer number, therefore the criminals are requesting them on the website presented in Figure 4. Moreover, confirmation codes, which are also requested by criminals as these are needed to confirm payments in the online bank of Nordea. Therefore, if one was to fill the information requested and clicked OK. The information would not be updated on the official Nordea website, but that information will be sent to the criminals. Therefore, there is a need to learn little about cyber threats and the policies of the trusted organizations. For an example Nordea has announced they never ask customers for their confidential information through online.

Besides phishing, other methods of obtaining confidential data are pharming, vishing, and smishing. Each of them, similarly with phishing, represents an attempt to gain sensitive information from users by acting as a legitimate organization. The only difference between pharming, phishing, vishing and smishing is in the methods of executing attacks.

Pharming may be directed at organizations. As in this scam, hackers install malicious code on a server or a computer (Intuit 2013). The purpose the malicious code is to redirect clicks on an original website to another fraudulent website without users' knowledge or consent. To protect one from such scam, avoiding entering financial information on a website that looks different or suspicious is the best option. Moreover, the verification of the safety of websites by clicking on a lock sign next to the website address is advisable. By clicking on the sign, one can confirm if the website has a verified signature by a reputable third party.

Vishing is related to phishing, but the purpose of vishing is to use social engineering techniques to trick one to provide information needed by a criminal over the phone. The information provided by a victim is used to create new credit cards or commit fraud in the victim's identity. To avoid being used by criminals, one should not pick up phone calls from unknown numbers. In addition, one should look up the organization’s customer service number online rather than calling the numbers provided in e-mail or phone call.

Smishing is another form of phishing, but the means of scamming victims is by using text messages. Text messages often include a website address or phone number. The phone numbers usually have an automated message, and similar to other scamming form, the smishing text messages request an immediate action. According to Intuit (2013), smishing message uses a ‘5000’ number instead of displaying an actual phone number. The ‘5000’ number indicates that message was sent via e-mail and not from another phone number. As phones are not as secure as computers, one should not click on website addresses on the phone unless it is confirmed to be safe.

The scamming methods themselves do not cause harm or damage. However, the human reaction to these scams causes the damages. Therefore, if one follows common knowledge and does not respond to those attempts that ask for any personal information, such as suspicious emails, phone calls, and links, then there is very little chance of being scammed. Moreover, by verifying the content with someone else, such as a friend, an IT expert, customer services of a suspicious e-mail, one will know if the content was sent by a legitimate organization. In Finland phishing attacks are considered to cause the most damage to the organizations; therefore to warn the customers of such attempts is the right action to take (Kauppakamari 2015, 9). There are not many options to protect customers from being scammed, as it is out of organizations jurisdiction. However by taking the initiative and warning customers on scamming attempts, one will not hurt the organization's reputation and there is less trouble when facing the law. The key to protecting customers and organization is to enlighten them about cyber threats. If the staff has knowledge about the cyber threats, many of the mistakes that cost organizations can be easily avoided (Kauppakamari 2015, 45).

4.5 Database attacks

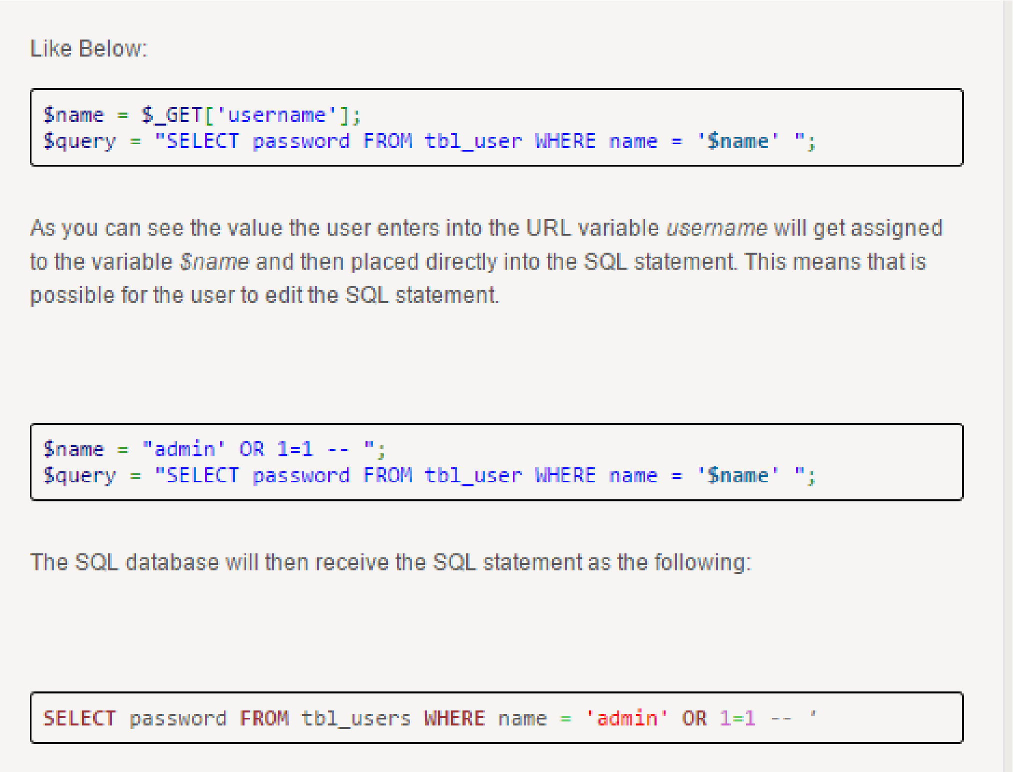
The database attacks are threats, misusages and exploitation of database data for malicious uses. The database is a place where collections of various types of data are stored, and information is recalled from it to produce an output (Yariv, 2011). The attacks can be executed from both external and internal sources. Some of the attacks are extremely easily executable, as one may only need to manipulate the source code of the website. Protection of such data is critical as the information include confidential data, such as passwords and customers' personal information.

As an example, WordPress CRM plugin was found to have vulnerability within Custom Contact Forms extension which allowed attackers to take control of the website in 2014 (Viestintävirasto 2014). This vulnerability is allowing them to access backend of the website to add, modify, delete the database, and acquire confidential data.

4.5.1 SQL injection

SQL injection is one of the most popular methods that can be used to steal valuable information from a database through a browser. Considering the means dynamic websites are built today, the database is a valuable asset and thus should be well secured. However, many developers overlook the security of strings and queries. SQL injection is a method applied on the application security level, thus a process can be executed from a browser. SQL queries are "used to allow legitimate website visitors to submit and retrieve data to/from a database over the Internet using their preferred web browser" (Vella 2006). Therefore, if the inputs are not filtered properly, they can be manipulated by malicious users to request unwanted data using custom SQL queries and exploiting errors. SQL injection is violating the policy of confidentiality of information, and if the information is altered, then the policy of integrity of data is violated as well.

Web applications, which provide dynamic content, such as login pages, or shopping carts, may allow SQL commands. SQL commands enable hackers to view unauthorized information from the database or even wipe it out (Linn 2010). Adopted Figure 5 is an example of how SQL injection works.



Like Below:

```
$name = $_GET['username'];
$query = "SELECT password FROM tbl_user WHERE name = '$name' ";
```

As you can see the value the user enters into the URL variable *username* will get assigned to the variable *$name* and then placed directly into the SQL statement. This means that is possible for the user to edit the SQL statement.

```
$name = "admin' OR 1=1 -- ";
$query = "SELECT password FROM tbl_user WHERE name = '$name' ";
```

The SQL database will then receive the SQL statement as the following:

```
SELECT password FROM tbl_users WHERE name = 'admin' OR 1=1 -- '
```

Figure 5. SQL injection example (adopted from Wikihow 2014)

In Figure 5, the query presented is sent to database to search for the password, associated with the username requested. However, because this example is easy to exploit, a hacker would use “admin’ OR 1=1 - -“; query for the $name variable. As such, the command will find all the passwords that belong to username=admin or username=true. Thus, the final query will return all the passwords from ‘tbl_users’ instead of one password for the username.

In order to prevent SQL injections, a new feature was introduced by PHP, prepared statements that use bound parameters. The prepared statements consist of a process of preparation and execution (PHP 2014). Therefore, prepared statements do not process variables with SQL queries, but SQL query and variables are sent separately hence the variables are interpreted as strings and not part of SQL query. The process of variables being interpreted as strings render SQL injection useless, as SQL injection modifies SQL statements to attack databases. From Finnish SME organizations' perspective, appropriate attention should be given to attacks that cause them to lose confidential information. Moreover, the database is the place where all the information is kept. Therefore, losing confidential information represents a big loss for the company's finance, credit and time.

4.5.2 Directory traversal attack

Directory traversal attack or path traversal attack is the exploitation of insufficient verification of user-supplied input requests. The requests are needed in order to access a file that was not intended to be accessible. Directory traversal attack can be easily fixed, but many developers and even security teams tend to be ignorant of the damages it could cause (Chickowski 2013). A professional hacker using directory traversal attack would be able to obtain information about the structure of the organization to leverage his next move. In the worst case, the hacker could access the main hard drive of the organization and steal valuable information or spread a virus.

Directory traversal attack is not well-known as SQL injection, where one exploits weakly written codes. However, traversal attack can cause a significant amount of damage when taking into consideration the confidential information it reveals about the organization. Simply explained, directory traversal attacks is using '..\' in Windows and '../' in UNIX systems to access a higher archive, until a root directory is reached, where assumedly all important information is residing (Makker 2011). The example of using / or \ presents a simple principle as how traversal attacks are executed.

The exploit exists because of developers, who like to embed directory traversal for it being convenient for programming (Chickowski 2013). Therefore, the first step in mitigating the risk of being under directory traversal attack is not to include it in the coding practices. There are many other methods that can be used to mitigate the directory traversal attack. For example, by disabling custom address being typed in the address bar, meaning that any custom typed address will be redirected back to a homepage. Another method would be to validate incoming requests. Additionally, having a controlled environment with an access control list would help as well.

4.6 Advanced attacking types

This chapter covers the other attacks, which appear to be straightforward to execute from the point of view of the attacker if the vulnerability exists. The attacks do not much in common with each other, except that they do lots of damages if actions for prevention are not executed properly. There are two different attacks, cross-site scripting (hereinafter XSS) and cross-site request forgery (hereinafter CSRF).

4.6.1 Cross-site scripting

XSS is a method where an attacker uses a web browser to inject malicious script into a website that has XSS vulnerability. Originally there were two types of cross-site scripting, reflected XSS and stored XSS (OWASP 2014a). However in 2005, Amit Klein found another type of XSS, which he named document object model (hereinafter DOM) XSS (Klein 2005). DOM XSS exploits the URL of the website in order to inject malicious script. Many big credible organizations, such as FBI, EBay, CNN, Microsoft and Apple have been affected by one of these XSS attacks (Linn 2010). The most used programming language for XSS is JavaScript because dynamic websites are built nowadays dependent on JavaScript.

Reflected XSS is a vulnerability that does not last, in other words, reflected XSS is a temporary threat. The threat can be executed on any website, which has not encoded and validated input correctly. The attack can be executed on any fields that allow the users to input a value. However, the point of reflected XSS is for an attacker to test whether the website is vulnerable to further XSS attacks such as stored XSS or DOM XSS. The script used for testing is usually harmless, and it is not typed in a comment, shout box or any other fields that display the results to other users. The reason is that the attackers do not want to be noticed. Scripts usually used for reflected XSS can be as simple as <script>alert(”Test”)</script> and if the website is vulnerable, a popup window will show a text with ‘Test’. Reflected XSS is usually first phase before moving onto stored XSS or DOM XSS. With stored XSS, one would write a script in the forum, shoutbox, comments and other fields that are displayed to the public. Stored XSS is persistent because it is stored on a server and the damage it can cause depends on the knowledge and motivations of the attackers. Examples of what can be done with XSS are, setting up an overlay login page for a banking website to steal credentials, redirecting users to a malicious website, or running the software necessary for hacking.

4.6.2 Cross-site request forgery

CSRF is a malicious attack in a sense that a malicious user can inherit the identity and privileges of the victim submitting requests to an authenticated website, for instance, a banking website. CSRF, sometimes referred to as XSRF, is vulnerability in web applications. In comparison of CSRF with XSS, SQL injection and other types of injection threats, CSRF is less common. Therefore, CSFR gets less attention compared to other types of injection threats as they are more acknowledged. However, in recent years CSRF has surfaced increasingly, and it may be a destructive attack, depending on how the attack is executed.

CSRF is a vulnerability, which works by exploiting the trust a site has for its users (Vella 2006). The means by how CSRF exploit operates allows malicious users to do anything on behalf of the victims, without their knowledge and their consent (Acunetix 2014). “Therefore, if the user is currently authenticated to the site, the site will have no way to distinguish the forged request sent by the victim from a legitimate request sent by the victim.” (OWASP 2014b).

One method malicious users do is creating an interesting website with malicious code embedded in the website to request the victims' information. As CSRF objective is to cause a state of change on a server, the malicious code would, for example, change a password, purchase items, or in the worst case, send money to attacker's bank account. To successfully execute a CSRF attack, a victim has to visit the malicious website or open the malicious URL from the same browser while doing something else in another web tab, such as banking. To illustrate CSRF attack Figure 6 is depicted below.

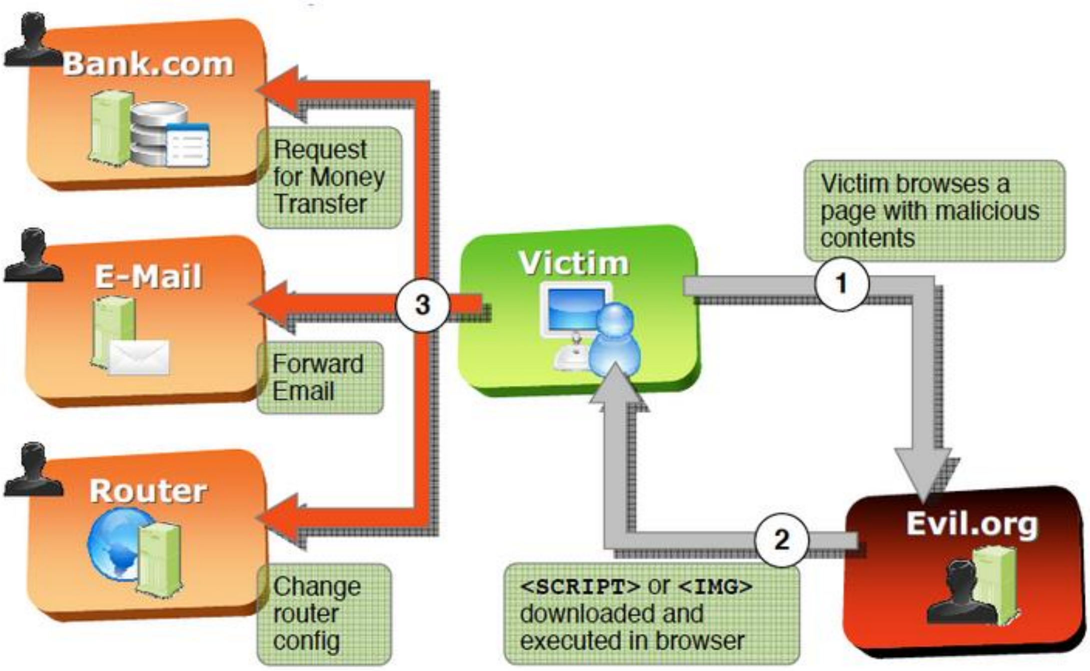

Bank.com
Request for Money Transfer
E-Mail
Forward Email
Router
Change router config
3
Victim
Victim browses a page with malicious contents
1
2
Evil.org
<SCRIPT> or <IMG> downloaded and executed in browser

Figure 6. CSRF in action (adopted Djuliy 2014)

In the adopted illustration, a victim is browsing his bank, email, and router admin page, and while doing so, he decided to open another tab and found an interesting website which is a malicious website, evil.org. The malicious web site has hidden codes, which are run in the background not visible to the victim, and it is executed once someone visits evil.org. Therefore, the requests are made to transfer money to evil.org bank account, forward all e-mails the victim receives to evil.org e-mail account and change router settings on behalf of the victim. All the requests are made in the background; therefore the victim would not be aware of this until it is too late.

There are many methods to protect one from CSRF attacks. However, those methods cannot be applied from user’s end and have to be encoded in the web application provided to the users. The proven method for securing and preventing CSRF attacks is to “append unpredictable challenge tokens to each request and associate them with the user’s session.” (Dupaul 2015). Therefore, web application that uses a one-time randomly generated token for each session and request sent by the user for authentication restricts malicious requests to be accepted by web application. One should use a randomly generated secret token, which cannot be copied. Moreover, the most important elements that the secret token should be applied to are links and forms in the web application. These are the most used element on the website that has a state changing function. All aspects that have state changing functions should have the token applied on them as CSFR attack targets those. Another method that can be applied to prevent CSRF in addition to the token method is to use ‘Completely Automated Public Turing test to tell Computers and Humans Apart’ (hereinafter CAPTCHA) (Garofolo 2014).

CAPTCHA is a verification process to validate whether the request was initiated by a human being or an automated script. CAPTCHA is usually executed by requiring a person to type in what is seen as random letters or words. CAPTCHA may be used as a verification method for proving requests are executed by human, as CSFR is an automated process by using a browser.

4.7 Potentially unwanted software

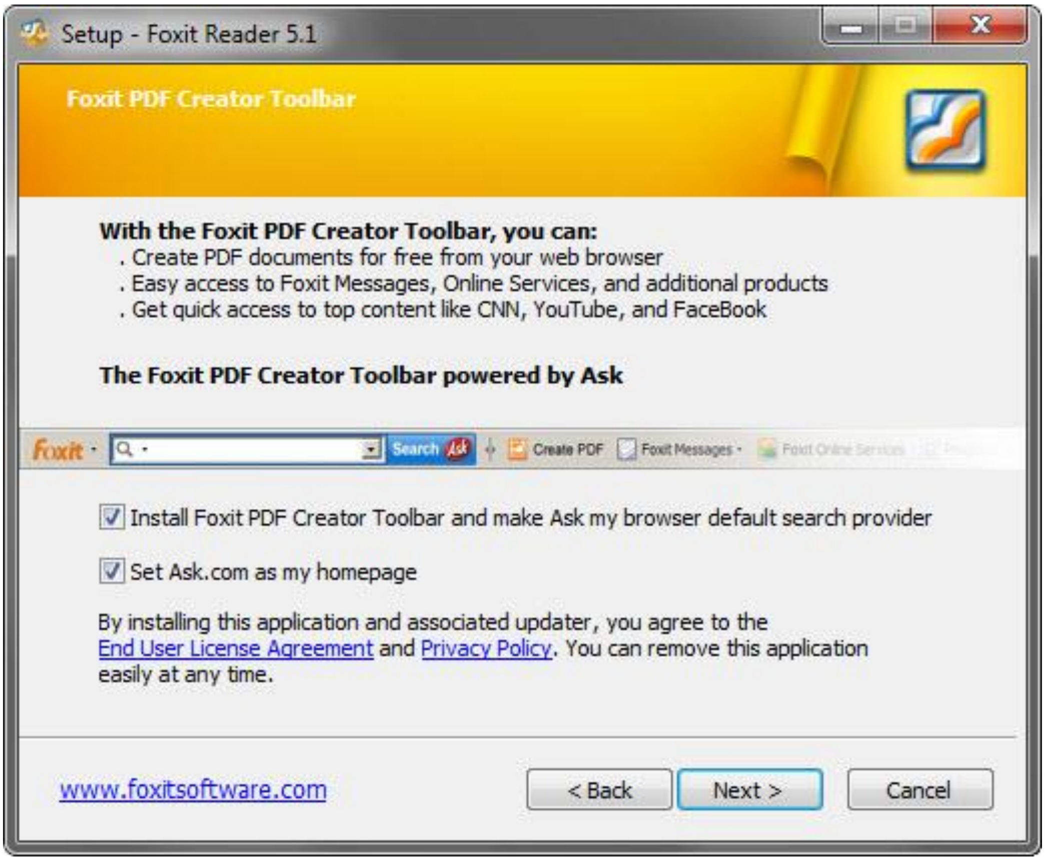
This section provides more information about other types of software. However, it is up to users to determine whether these are malware or not. The software provided in this chapter is rather controversial as some can cause damage, and some are used by legitimate companies for gathering intelligence.

4.7.1 Adware

Adware is software created for the purpose of advertising. In many cases, adware are installed as extra software with legitimate software. These are not stealing information or data unless it is tampered with viruses or other malware. However, having installed too many adware is disturbing user by slowing down computers up to the point computer is rendered useless. Usually, the disturbance of adware is expressed as pop up of unwanted advertisements at any given time. Adware are not detected by AV software first-hand because users are agreeing to install them when installing intended legitimate software.

If the installation has an option to decline, then it means there is a probability of unwanted software being installed if one was to click on ‘agree’. Therefore, the recommended practice is to follow the installation screen closely before clicking on ‘agree’ or ‘next’ to save the trouble of uninstalling adware later. Additionally, by reading other user’s review, one should have a clear idea what is contained in the software. CNET.Download and many other reputable websites have a comment section, where one can look up what other users comment about the software.

However, even reputable websites, such as CNET.Download, have malware and adware installations. There is some anti-adware software on the market, such as Malwarebytes for deleting adware, but it may not be able to delete every adware. Therefore, manual deletion has to be done through program uninstallation which may tedious work. Figure 7 and Figure 8 illustrates examples of adware installation.



Foxit PDF Creator Toolbar

With the Foxit PDF Creator Toolbar, you can:
. Create PDF documents for free from your web browser
. Easy access to Foxit Messages, Online Services, and additional products
. Get quick access to top content like CNN, YouTube, and FaceBook

The Foxit PDF Creator Toolbar powered by Ask

☑ Install Foxit PDF Creator Toolbar and make Ask my browser default search provider

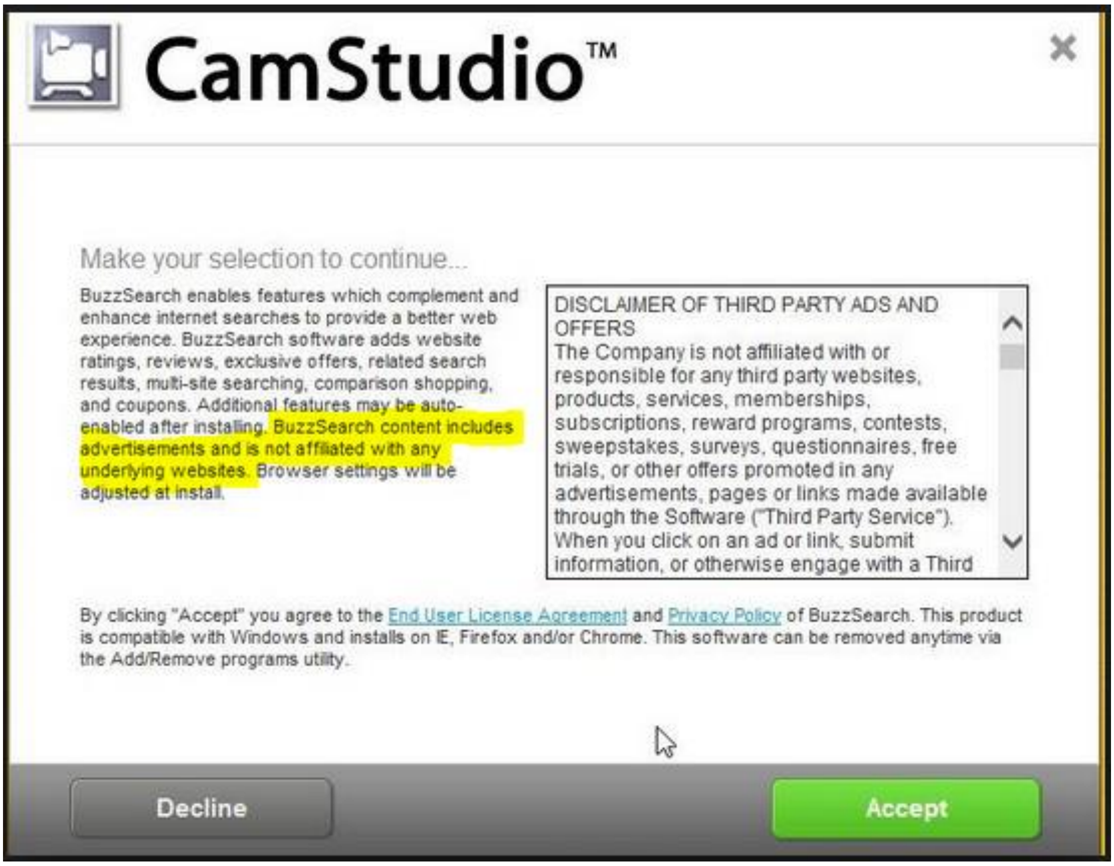
☑ Set Ask.com as my homepage

By installing this application and associated updater, you agree to the End User License Agreement and Privacy Policy. You can remove this application easily at any time.

www.foxitsoftware.com

Figure 7.Tricking users into installing unwanted software (adopted from Brinkmann 2012)

Figure 7 illustrates the older method of how users were tricked into installing all unwanted software and settings. In the Figure 7, the toolbar and default search engine with a new homepage ask.com would be installed if one was not to untick the boxes. However, virus or worms may be installed without users noticing if the user was to install the software without paying attention such as presented in Figure 8.



Make your selection to continue...

BuzzSearch enables features which complement and enhance internet searches to provide a better web experience. BuzzSearch software adds website ratings, reviews, exclusive offers, related search results, multi-site searching, comparison shopping, and coupons. Additional features may be auto-enabled after installing. BuzzSearch content includes advertisements and is not affiliated with any underlying websites. Browser settings will be adjusted at install.

DISCLAIMER OF THIRD PARTY ADS AND OFFERS
The Company is not affiliated with or responsible for any third party websites, products, services, memberships, subscriptions, reward programs, contests, sweepstakes, surveys, questionnaires, free trials, or other offers promoted in any advertisements, pages or links made available through the Software ("Third Party Service"). When you click on an ad or link, submit information, or otherwise engage with a Third

By clicking "Accept" you agree to the End User License Agreement and Privacy Policy of BuzzSearch. This product is compatible with Windows and installs on IE, Firefox and/or Chrome. This software can be removed anytime via the Add/Remove programs utility.

Figure 8. Option to decline from an offer

Figure 8 is a newer method to trick users into installing unwanted software on computers. The method was developed as the users’ habit of clicking on the highlighted button became a pattern. With this newer method, the advertisers could plant more than one adware in single legitimate software to be installed. Adware will install many unwanted software that renders computer slow, almost impossible to work with, which on another hand will bring troubles to organizations because workstations may not function properly.

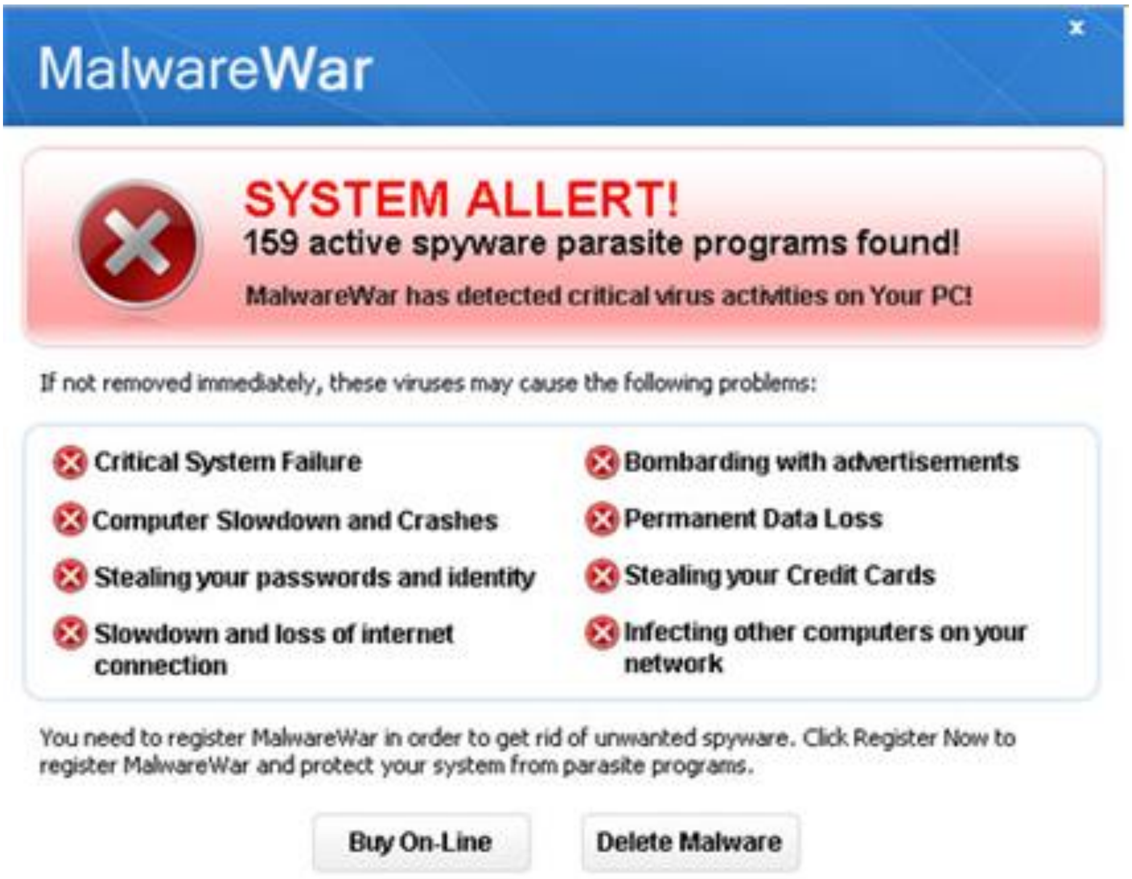
4.7.2 Spyware

Spyware is software installed without owner’s consent for gathering intelligence for organizations. The methods for unauthorized installation may be victim clicking on a bad link, or installing false software on a malicious website. The term spyware is controversial, as some experts categorize spyware and malware together while others separate spyware and malware from each other (Microsoft 2014; CIBC 2014). Spyware is a dangerous threat to an organization and organization’s security. Therefore, spyware could be considered a malware, as it can be set to execute malicious activities. A spyware can collect users' personal information, scan computer’s hard drives, read cookies, open applications and transfer information over the Internet to an attacker. “In short, spyware is a program that utilizes a user's computer to benefit a third party” (Paretologic 2014).

As mentioned previously, spyware may be installed without user’s consent through various file-sharing programs, even legitimate ones. Even legitimate sharing websites are being compromised, as they do not scan the files uploaded by the users. The best choice would be not to install any software, unless one is certain, why any software is being installed, and source of installation is confirmed to be secure. Another good practice is to close the pop-ups that prompt for installation by clicking on ‘X’ in the upper right corner (Boston University 2014).

In some cases, if a user clicks on ‘cancel’ or ‘no’, then the software may still get installed. Kaspersky (2014) mentions if one have done nothing wrong; there is still a chance of being infected by spyware. Therefore, besides being careful with the installations and website browsing, one should have reliable AV software with detection and proactive protection solution. Moreover, as there is free AV software available, they do not offer all necessary features, such as a virtual encrypted keyboard, or anti-spam filter. Therefore, many organizations should restrict the installation of the software on workstations and laptops to be performed by the IT department. Moreover, there is a need for discussion between staffs, IT experts and management to decide which software is to be installed to set up secure working environment. Further, the freedom of authorizing the staffs to install any software on workstations should be determined by management while considering both security and convenience aspects.

There are also many companies offering tools for spyware removal in case of being infected or suspects of being infected by spyware or similar malicious software. However, one should keep in mind there are also fake spyware removal tools, which in reality are spyware software themselves. Many of these fake spyware removal tools have advertisements for prompting users for installation, by displaying hoax errors or danger messages, an example is presented in Figure 9. In order to avoid such mistake, it is advisable to do research and search for spyware, which is created by reputable companies or are suggested by ICT experts.



MalwareWar

SYSTEM ALLERT!

159 active spyware parasite programs found!

MalwareWar has detected critical virus activities on Your PC!

If not removed immediately, these viruses may cause the following problems:

- ☒ Critical System Failure
- ☒ Computer Slowdown and Crashes
- ☒ Stealing your passwords and identity
- ☒ Slowdown and loss of internet connection
- ☒ Bombarding with advertisements
- ☒ Permanent Data Loss
- ☒ Stealing your Credit Cards
- ☒ Infecting other computers on your network

You need to register MalwareWar in order to get rid of unwanted spyware. Click Register Now to register MalwareWar and protect your system from parasite programs.

Figure 9. Fake spyware error warning (adopted from Webtoolsandtips 2009)

Figure 9 is an example of a hoax message for prompting users to install spyware and malware. As Figure 9 shows, an inexperienced user seeing this advertisement will think they have 159 spyware on their computer and would click on either of the options presented. However, an installation of the software may still run on the computer without the users’ knowledge and consent if one was to click ‘buy on-line’ or ‘delete malware’. In most cases, this software is spyware or malware. Therefore, the best option would be to close the advertisement by clicking ‘x’ in the top right corner.

5 BUILDING A SECURE E-COMMERCE SYSTEM

This chapter explores the necessary tools needed for starting a secure e-commerce system. This chapter is intended for those who are starting or planning to start an e-commerce business, such as eBay but do not have enough money for setting up their own business. The chapter reviews various third party companies, which in combination with each other will offer solutions for creating a secure e-commerce site. The recommendations are for SME B2C e-commerce businesses. However, with some alterations the recommendation may suit other e-commerce systems as well. Moreover, the important role of security within organizations is defined, and the need of educating the staff with sufficient knowledge about cyber threats is motivated.

5.1 Ready solution offered by market

Designing a website might be an exhausting task. However, "if you're a one- to two-person firm, [you have] someone on your staff [who] can design a website and you only sell a few products, there's no reason not to do it yourself, particularly with the out-of-the-box solutions available nowadays" (Campanelli 2006). Therefore, if one likes challenges and having full control over their website, then creating a website is suggested. However, if there is no such option available, one can hire a professional web developer, but it may be costly. While the point is to make the website attractive, it should be kept in mind that, reviewing code for bugs and vulnerabilities is a necessary task.

There are platforms for those, who need to make use of a website quickly. These platforms offer a graphic user interface (hereinafter GUI), easy-to-install, ‘no experience needed’ type of services. These are not recommended from a security perspective, as they come in ‘packages’. In order to reach the best possible results, it is recommended to use separate companies, which specializes in a particular service. All these types of services are paid per month, and one should be careful when selecting the ‘best’ platform. One should choose the platform that presents the most optimal features that would benefit their businesses.

Three platforms were chosen for ready e-commerce packages, Magento, WooCommerce, and Frosmo. These platforms were selected because each of them have a great number of features available for an affordable price. Moreover, the platforms have many years of experience in creating stores and tens of thousands of customers. In addition, the platforms are recognized by various companies around the world and the most importantly they hold a most market share in Finland (Datanyze 2015).

The platforms, which offer website creation for e-commerce, are recommended if the organization wants to be in business quickly. Such as the business is used as a short term solution, temporary solution or for gaining experience. In addition, the e-commerce may be treated as a side-business. However, as a foundation for successful business, it does not offer a solution for a long-term solution. As the e-commerce system becomes more complicated as it grows.

A shopping cart is needed to do business online. The shopping cart is a program or service, which processes the orders, including transport costs, sales taxes and sending order notifications. Two options were found as other shopping cart services have expanded into offering more features, such as the whole e-commerce package. X-cart provides an easy GUI interface allowing users to buy and add products to a cart, and a backend system, which allows admins to keep track of the orders. Another shopping cart, ShopSite is not as user-friendly as X-cart. However, ShopSite offers to install the software on their partner hosting servers. Both shopping cart software offers multiple additional modules alongside their shopping cart, but with an additional cost.

Both shopping cart software is secure if they are enhanced with authorization processes, in other words, payment gateway, which is the means to verify a secure transaction. Both shopping carts come with their respective payment methods. However, a better choice would be to use a more reputable, credible and reliable payment method.

A payment gateway is a service where a request for credit card information authorization is executed in real time. For the purpose of SME, it is recommended using Flagshipmerchantservices (Hereinafter FMS) as they are working together with Authorize.net to create a secure payment method. Furthermore, FMS accept major credit cards (Flagmerchantservice 2014). Even though, Finland has developed its payment system called Paytrail (Yle 2014), it is not as reputable as FMS abroad. Therefore, it may not attract customers from abroad, as they may not trust the new payment service offered by Finland yet. Moreover, FMS has the tools and methods of detecting frauds and illegal transactions. Additionally, the price and payment gateways are tailored for the businesses and customized for the best practices for online businesses.

Another payment gateway, which is used worldwide, is PayPal. PayPal service is to keep the money as a middle man that is sent from consumers to verify their credits, after which the payment is sent to the organization’s bank account. The service offered by PayPal takes a small percentage of every transaction made. Moreover, the customers should have a PayPal account linked to their payment cards to use this payment method. For those organizations who want to target the Asian market, CyberSource is recommended as the payment gateway, along with PayPal, as this will give an organization a wider range of customers. CyberSource accepts most of the Asian paying methods, such as Alipay from China, Korean Cyber payments by Korea, and PayPal. The purpose of a payment gateway is to create a trust relationship between customers and the organization. Figure 10 illustrates methods, which can be used to pay online. The figure does not cover all methods, but some of them.

Figure 10. Payment Gateway (adopted from Seksek 2014)

Figure 10 emphasizes that these payment gateways are needed to be shown on a website. People may feel safer by using the websites that display the logos in Figure 10, the reason being that these logos reflect popular methods of paying online. However, displaying a logo alone is not enough. The organization should apply the payment gateway on the website and their policy. Organizations that are using payment gateways from reputable companies will have a method to catch the scammers. Such methods allow retrieving the money easier for both the consumers and the organizations. Moreover, there is a standard process to follow to ensure the safety of purchases and such practice is governed by a Payment Card Industry (hereinafter PCI) security standards council.

5.1.1 Payment card industry data security standards

The PCI data security standards (hereinafter PCI DSS) were developed by the PCI security standards council (Flagmerchantservice 2014). The Council was founded by the various notable credit/debit card service industry leaders, such as American Express, VISA, and MasterCard. Moreover, each of these enterprises promotes the PCI DDS in their own respective program. VISA promotes cardholder information security program (hereinafter CISP), Mastercard promotes Site data protection (hereinafter SDP) and American Express promotes Data security operating policy (Flagmerchantservice 2014). Regardless of having that many programs in different organizations, the aim of the standard is to enhance payment account data security, in other words, the protection of customers' data.

An example of practices within PCI DSS is never to store the cardholder's information on the servers, and merchants need to complete a self-assessment questionnaire annually to be accepted in the program continually (VISA 2014). Moreover, the PCI categorized the rules are based on the number of sales made. The large enterprises, which sell millions annually, are required to make a report or fill higher-level self-assessment along with other forms to ensure the credibility of PCI DSS, thus assuring customers the safety of purchases. While, SMEs, which may make six figure annually file simple self-assessment, which is confirmed by credit card organizations.

5.1.2 Secure sockets layer encryption

Secure sockets layer (hereinafter SSL) is a standard security technology that allows a secure transaction over the Internet by encrypting data. SSL is mainly used for securing online transactions and is presented by a padlock along with URL starting with 'HTTPS' or through the URL bar being colored in green. SSL encryption is necessary when e-commerce platforms are asking customers to type in sensitive data, such as credit card information and addresses (Coburn 2012).

In order to create a more secure environment, there are SSL certificates, which are provided by third parties such as DigiCert and VeriSign, even though those certificates can be created with adequate programming knowledge. However, by using the best SSL services, a symbol of trust is built, and security is the best if provided by professionals. Moreover, browsers such as Chrome and

Firefox comes with a set of trusted certificate authorities (hereinafter CA). Therefore, the self-created certificates will be marked as unsecure and browser will notify the user of an insecure SSL website, whereas trusted CA certificates do not show a warning. SSL certificates come with a pair of keys, a public key and a private key for browsers and servers to securely communicate with each other. To illustrate how SSL connection between server and browser is established, Figure 11 is adopted.

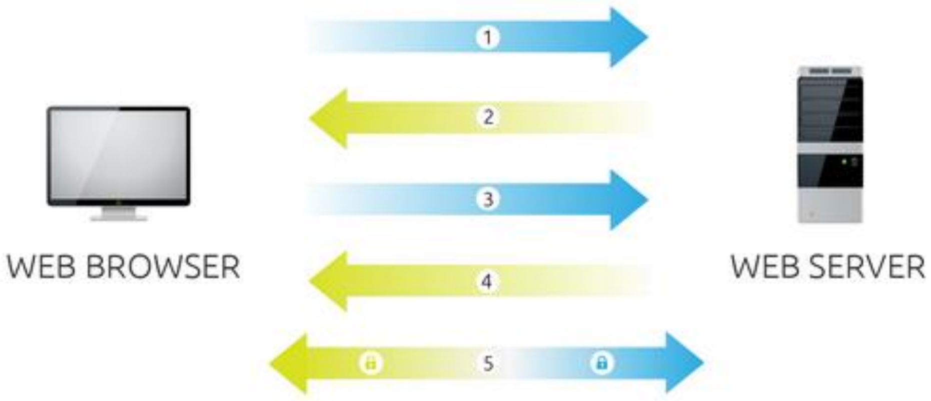


Figure11. SSL connection steps (adopted from DigiCert 2014)

Figure 11 depicts the process of SSL connection between a web browser and web server. Each step presented has to be completed and agreed by both parties before moving onto next step. As stated previously, HTTPS secured website is required for a web browser to execute SSL connection. The steps are presented below as a list.

1. A web browser connects to HTTPS website secured with SSL (server). The web browser requests that the website (server) identify itself.
2. The website (server) sends a copy of its SSL certificate and its public key to identify itself.
3. The browser runs the copy of the SSL certificate against its trusted CA list and verifies if there is any existing problem, such as an expiration date. Once verification is finished, and the web site (server) is trusted by

the browser. The browser creates, encrypts and sends session key using the website's (server's) public key.

4. The website (server) decrypts the session key by using its private key and sends back an acknowledgment encrypted with the session key to start communication
5. The browser and the website (server) now have established an encrypted SSL connection. Everything transmitted between the two will be encrypted using the session key.

The process of SSL connection is called SSL handshake (DigiCert 2014). Even though, the handshake 'has several steps, it is instant'. All the steps in the process are done invisibly to users, and the users will not notice anything while browsing websites.

5.1.3 Creating an e-commerce using ready platforms

This sub-chapter is intended for individuals who are not planning to scale up their businesses in the future and are satisfied with SME e-commerce system, without worrying too much about security issues.

Firstly, a catchy name and a domain name are needed. Holding a domain name for the organization ensures that no one else can use the same domain. After a domain is bought, a web host is needed. However, some e-commerce platforms offer both domain and web host. Though, it would be recommended purchasing a separate domain and web host, but the decision is up to the organization.

Currently, Shopify is the best e-commerce platform for a reasonable price. However, Shopify is not very popular in Finland. Nonetheless, for people getting accommodated to their platform, an offer of the 14-day trial is offered to sign up using an e-mail account. According to Shopify (2014), they offer a number of different templates. Moreover, to create an easy website attractive website, with a shopping cart, different features are provided, such as a store management system, various payment gateways, search engine optimization, web hosting, and mobile support.

Choosing Shopify appears to be a good choice. However according to a practical vulnerability test conducted by the researcher, where 10 of the test sites were tested. The sites were chosen randomly from example shops provided on www.Shopify.com, and the criteria were, that the sites had a good design, and the products were attractive. The test result gave 9/10 were vulnerable to the most basic method hackers would use. From outlook the Shopify shops looks professional and adequate with security. However, after doing the test, it was noted that the security depends on the knowledge of the owners. Ten random websites built using Shopify platform were used to check how hard it was to find the admin login page. The results show that it was extremely easy 90% of the time.

Commands added behind each shops' URL was /admin, /administrator, /admin_area and /login for testing. There are plenty more to try, however, using only these 4, the vulnerability of the site was exposed, and results are that hackers can find where the admin area is without difficulty. The next step is to try SQL injection, bruteforce and other attacking methods to get the username and password to access the backend of the websites.

What is needed to be emphasized here is that even though Shopify claims to be secure, it is up to user's knowledge how secure the website can be. Therefore, it is recommended to learn the basics of security vulnerabilities and not purely rely on service providers' statements.

5.2 Building own e-commerce system

As the plan comes into its final stages, it is time for implementation. To directly translate the plan into products and process is tedious and dangerous from the point of the security. Most often, compromises have to be made in terms of budgets, timeframes and technical requirements and plenty of times this results in weakened security. One has to keep in mind that the security becomes more complicated as the company is involved more with the Internet and grows.

There are two ways to implement the plan. The first option is to implement the plan on a new B2C e-commerce website. This option gives an opportunity to start everything from the beginning, thus allowing one to establish a B2C e-commerce business from a point of view of the security. However, if the first option is not possible, there is another approach. Implementing the security features on an existing e-commerce platform. Implementing security on an existing e-commerce system is troublesome as the system may already be online and running. Additionally, making it worse than the first option is, an identical testing environment is required for testing, reviewing and implementing to identify possible issues. The testing environment is required to ensure the safe implementation of security measures on the existing e-commerce system. The most important fact to consider is that the system should not be online until everything is tested as defined in organization’s plans.

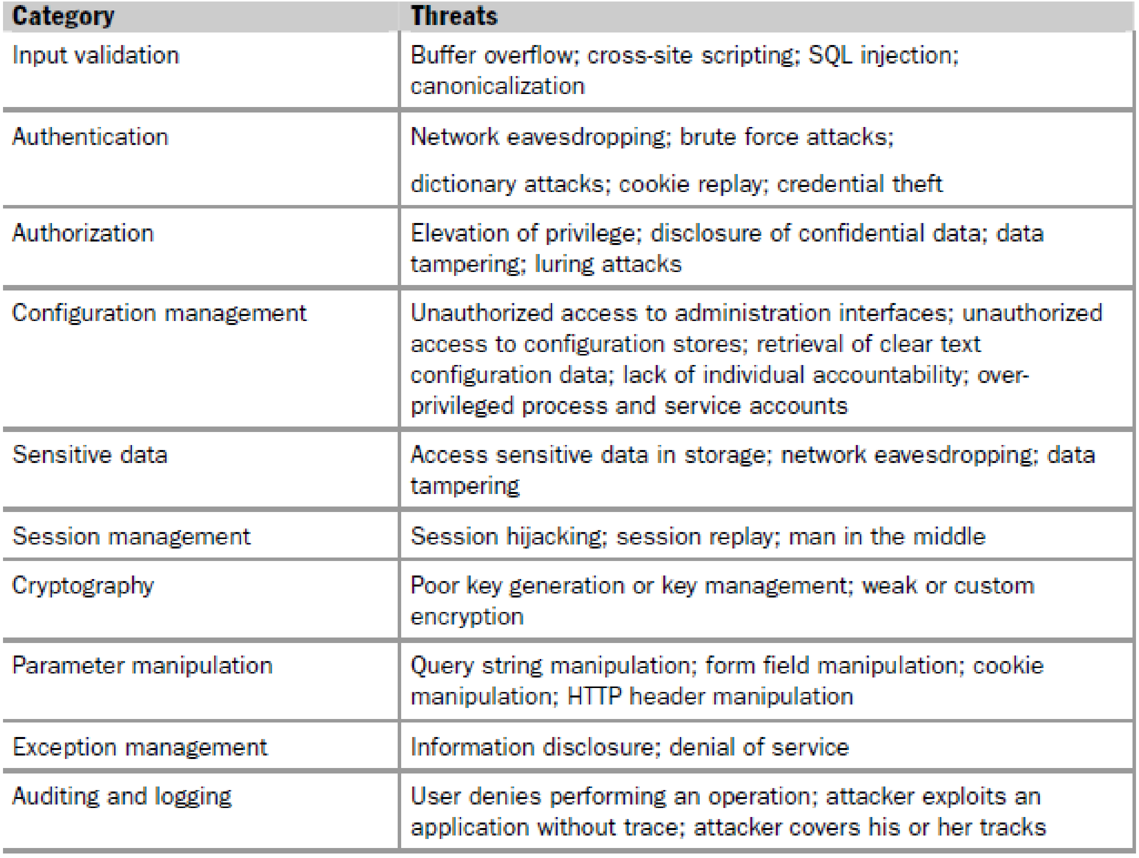
5.2.1 Applying security for a new site

The first step in starting a new e-commerce site is to start planning. By creating a security plan on layers from the surface to deeper levels helps define the proper requirements for security. A security plan is comprised of individual parts of various projects that consist of tools, methodologies, and policies formally implemented together. When creating a security plan, one should not create it only for application level, which is the most basic level of the network. The security plans should be created for as many layers as possible.

An application security plan is where the focus is on applications, software, and websites. The plan encircles of measures applied on the lifecycle of the applications. The goal is to prevent mistakes and exceptions in the security policies of the application or the system continuously. Prevention is done through designing, development, deployment, upgrading or maintenance (Microsoft 2003, lxxi). There is possibility to see problem patterns if one was to analyze and review the top threats, mistakes, and flaws in a web. Thus, by organizing these patterns into categories, the problems are easier to solve. These patterns are the vulnerability categories of application and system. To start off, one should evaluate the weak points that the system may have.

To measure the resilience of the application and system, one could evaluate the vulnerability categories. Application security profiles are created, and these will determine the security strength of the application by evaluating the vulnerability categories (Microsoft 2003, 9.) Table 2 presents the threats in categorized approach.

Table 2. Threats by category (adopted from Microsoft 2003, 24)



Category	Threats
Input validation	Buffer overflow; cross-site scripting; SQL injection; canonicalization
Authentication	Network eavesdropping; brute force attacks; dictionary attacks; cookie replay; credential theft
Authorization	Elevation of privilege; disclosure of confidential data; data tampering; luring attacks
Configuration management	Unauthorized access to administration interfaces; unauthorized access to configuration stores; retrieval of clear text configuration data; lack of individual accountability; over-privileged process and service accounts
Sensitive data	Access sensitive data in storage; network eavesdropping; data tampering
Session management	Session hijacking; session replay; man in the middle
Cryptography	Poor key generation or key management; weak or custom encryption
Parameter manipulation	Query string manipulation; form field manipulation; cookie manipulation; HTTP header manipulation
Exception management	Information disclosure; denial of service
Auditing and logging	User denies performing an operation; attacker exploits an application without trace; attacker covers his or her tracks

In Table 2 the categories are organized with a description of what types of flaws there might be in an application or a system. Additionally, example threats and attacks are presented next to their respective category. Besides categorizing, one should also pay attention to extra processes. These processes should be continuously applied.

On a network level, the plan should cover authentication, authorization, and accountability. There needs to be a policy in place to control who is allowed to access, how the access is executed, when and where the access comes from. The policy itself is not enough for calling the system secure. However, the policy will mitigate the chance of attackers accessing the system. In order to have a simple and secure network, passwords should be protected because they grant access without authenticating. To make sure the passwords cannot be accessed, layers of protection and authentication methods such as certificates and data encryption should be applied. Security can be enhanced further with different tools, such as a firewall to prevent unwanted traffic when configured correctly.

The router also has some useful functions, such as setting an access list only to allow the devices which the router recognizes to access the system. However, the infrastructure should not be too complicated as it will be difficult to configure. All the peripherals involved in the e-commerce system should be surveyed, and all the unnecessary services and ports should be closed. The system will be more secure if there are no entry points for potential attackers to access by closing unnecessary services and ports. Unnecessary and unused ports and services are commonly the vulnerability that the attackers exploit for creating a backdoor access. Additionally, by disabling the ports and services that are not in use, the overall performance of the e-commerce system may increase, as the network traffic is more controlled.

Moreover, organizations may invest in additional security devices such as intrusion detection systems and intrusion prevention systems for enhanced security. These devices may be placed between the Internet and the organization to identify malicious activity, log the activity and attempt to block it. Even though securing systems with different devices and software are important, one should not undermine the importance of bringing security awareness and dangers of the Internet to the people. Mandiant reports that part of the methods used to compromise corporations in America was done by e-mail phishing (Mandiant APT1 2013, 27-30).

Chapter 4 mentioned e-mail phishing is one of the social engineering acts where an attacker sends a legit looking e-mail acting as someone the receiver knows. The e-mail is attached with a link, and the goal is to get the receiver to open the link to allow the attack to happen. People tend to make many mistakes intentionally or unintentionally, especially during social engineering attempts. According to Goodchild (2012) and Mabute (2009), social engineering is an act where the attacker manipulates people into divulging confidential information about themselves or the company by exploiting human psychology. Educating the staffs and raising awareness of such attempts will reduce the chances of social engineering attacks being successful, and the key is to be as careful and suspicious as possible when working.

Having proper equipment to secure the network is not enough, as e-commerce systems are built with codes. Therefore, there has to be a practice to revise the written codes. Such practice is called code review and this practice is the most vital one. If code review is not a regular practice in organizations, then every effort spent on creating the e-commerce will be in vain. Reviewing the codes that are written by someone else is important if one wants to successfully fend off the attackers. Therefore, when writing the codes, extra attention is needed. Such mistakes as leaving semicolon off or writing the syntaxes incorrectly are common mistakes in programming world.

The objectives of the reviewing code should be accomplished, but not limited to as follows. The first objective is to ensure the source code follows the design of the organization. The second objective is to check that source code agrees with the organization’s coding standards. Moreover, by verifying that code is within organization’s coding standards, one may find any defects prior to unit testing. Lastly, the code review process is used to measure the progress of the work within the project. “This is done by tracking the number of defects, the type of defects, the cause of defects, and so on, so that progress may be fully tracked as fixes are applied.” (Forristal 2001, 504.) This process ensures that there are little to no mistakes.

However, when creating a security plan, there has to be someone who will manage the security plan. The purpose is to make everyone understand how important the security is for the company. The whole process of planning involves not only the quality assurance, network administrators, staff, developers, but also the management team of the company (Bakari & Tarimo & Yngström & Magnusson & Kowalski 2006, 45-47). The management team is in the critical position, as they will make final decisions.

5.2.2 Implementation on an existing site

Building e-commerce systems from scratch with security as priority is an excellent choice, as this makes the process easier. However, there is a possibility of applying the three principles of the C-I-A triad on existing, operational sites as well. New e-commerce sites can adopt the mindset of prioritizing security from the very beginning, and it is easier and cheaper to implement. However, operational e-commerce sites have an advantage of applying more effort, time, and money to enhance the existing system. The downside of applying on existing infrastructure is the cost is much higher compared to newly established e-commerce. The downside of new e-commerce is the security will not be as efficient as the one in an existing e-commerce system, but it should be sufficient for a startup. There are both positive and negative remarks on both methods.

The concept of applying C-I-A triad on existing sites is a little different from the new sites, but most of the concepts are the same. The principles of C-I-A triad do not change, but what changes are when and where to apply them. The problem with existing sites is that, they need to be 99.99% online according to their respective SLA agreement. Therefore, a mirror site is required. The topology, the system, the applications, everything that is on the original existing site must be on the mirror site. The purpose of creating the testing site is to ensure that no changes are made to existing site unless the suggested improvements are tested and fully functional. However, it should be kept in mind that mirroring the existing site as it is 100% may be costly. Another purpose to have a test site is for creating a laboratory environment, where one can fix the known bugs, do hypothesis testing and create possible scenarios for future attacks.

Firstly, a company needs to identify risks. The need for identifying vulnerabilities and risks within the organization’s system are the crucial starting point. From then on each of those existing risks should be examined and filtered with a risk factor along with impact influence. However, one should keep in mind that even small vulnerabilities may become high-level threats. To evaluate the high-risk vulnerabilities, one should relate the risks to the assets that are needed to protect. Further those assets should be evaluated to verify which of the assets the company holds valuable and where those assets are located. On this basis, as long as there is a chance of compromising those assets, which the company views as valuable, then it is of high risk.

These high-risk vulnerabilities should be fixed first. The fixes have to be tested, evaluated and revised on the testing environment before applying to the operational site. Depending on the results of these tests, one might need to go back to reviewing them. When satisfying results are achieved, a document should be written on the process, results, tests, notes and the other output for future references. Each test or process that is related to the vulnerabilities has to be documented fully. Documentation may help in the future and also may create an opportunity for creating security methods for threats that do not yet exist in the organization.

5.3 Importance of security for internally

The tools of security and the mindset of prioritizing security are essential for creating a secure e-commerce system. However, the most important key is to have sufficient knowledge and awareness of cyber threats within the organization among employees. According to a study, many SMEs in Finland are not prepared for breaches and attacks (Kauppakamari 2015, 44-45). Moreover, the majority of organizations have security plans that have never been practiced by the employees (Kauppakamari 2015, 40). The study shows how Finnish SMEs treat security as an insignificant aspect of the business. However, the study further points out that the organizations understand the dangers of neglecting ICT security and they also assume that the biggest threat is ignorance they have for cyber threats (Kauppakamari 2015, 11). Thus, convincing the management and head of organizations of SMEs to achieve the feat where ICT security and cyber-threats are taken seriously is needed.

A case study conducted where the objective is to bridge the communication barrier between general management, and ICT technicians may be an answer in Finland (Bakari et al. 2006, 44). The objective can be achieved by convincing everyone in an organization starting from top management taking a top-to-down approach. The most important is to convince the CEOs to understand the importance of ICT security, as this may be new to them. When convincing CEO, the organization is needed to be considered in a holistic view with risks, consequences, and the value of the organization if it was attacked. Moreover, the effect on the organization from reaching its mission, goal and objective should be pointed out if security was neglected (Bakari et al. 2006, 45). On the account that the CEO and top management are convinced of the importance of ICT security, then the mission of raising awareness among employees is not difficult.

Moreover, the management is needed to be convinced that the responsibility for ICT security is not only the duty of the IT department but it is responsibility of the whole company. In fact, the IT department would only cover technical problems. According to Bakari et al. (2006, 49), ICT problems consist of “business problem, with an ethical/culture dimension, an awareness dimension, a corporate governance, dimension, an organizational dimension, a legal dimension, an insurance dimension, a personnel/human dimension, an audit dimension, and finally a technical dimension.” Therefore, for example, the human resource should be responsible for raising awareness of ICT security within the staffs and as such this is not a technical problem (Bakari et al. 2006, 49). In Finland SMEs, if this solution is implemented where ICT security is treated as more than a technical problem, the organizations would have a clear idea when it amounts to ICT security. Therefore, the employees' mistakes may be reduced, and it may also reduce the risks of getting attacked. The study conducted by Kauppakamari (2015, 11) shows that second most answer chosen after neglecting security is insufficient knowledge of ICT security and cyber-threats. Therefore, by giving the employees necessary knowledge about ICT security and cyber threats, the organizations' security is improved.

6 CONCLUSION

The aim of this research was to discover how to establish a secure Finnish SME e-commerce by prioritizing security without affecting performance. Therefore, C-I-A principle was researched, and it was found to be a critical role in enhancing the security of ICT depending on the application of it in organizations as Chapter 5 noted. Additionally, in section 5.3, it was found that the cyber threat knowledge is an important factor to determine the security of organizations in Finland. Further, many employees within organizations did not have the necessary knowledge to act upon the threats. Moreover, the negligence of security was discovered to be high in Finland, as many do not yet understand thoroughly the danger of the cyber vulnerabilities.

As was noted in Chapter 3, the C-I-A principle represents a small section of ICT security, as it is an important set of principles for starting companies that do not prioritize security yet. The principle of C-I-A allows one to comprehend the importance of security when doing business. Useful, practical examples were given according to C-I-A principles for clarification.

Based on the findings of this research, security is proven to be an important aspect in ICT, as well as online businesses. Computers and the Internet are increasing in usage, as well as new threats are found every day. Therefore, a mindset of setting security as a priority within the online business is needed. Even though, some of the threats presented in this thesis are old in technique or technology, it does not mean the threats are harmless as can be seen from illustrations in Chapter 4.

In addition, Chapter 4 illustrates that most functions of online businesses are vulnerable to security attacks if the system is not secured properly. These functions can be such as login form, address bar, and picture or image. Therefore, for organizations it is important to be always one step ahead of attackers, which was suggested throughout this thesis by being prepared for every possible scenario by being proactive instead of reactive. Moreover, by being proactive one may solve unseen problems, which may have already existed in a company, by doing the hypotheses testing on possible attacks. However, as this thesis research may suggest, building a secure online business is not an easy task and certainly is not cheap. Therefore, organizations should decide on how important security should be, and this decision on its own will provide a better understanding of how much money should be spent on security.

For those interested in building an e-commerce utilizing ready platforms, some popular e-commerce platforms were presented in section 5.1. However, for security reasons, recommendations were given as when to use them, such as for short-term solution. Moreover, a simple test was done. The test was practical, but from a security point of view, a small mistake of exposing backend login system may allow unauthorized access to the system allowing attackers to plan their next attacks. Lastly, an idea for creating a secure e-commerce organization as a holistic picture is presented in addition to those discussed in the thesis which was discussed in section 5.2. Further, motivation for raising awareness of the employees and convincing the managements of organizations to take actions to improve security was presented in section 5.3. Additionally, by changing the perspective of ICT security within organizations not being only responsibility of the IT department, but ICT security is a problem of every department, security can be improved.

This research may serve as a basis for the future ICT security theses related to e-commerce and other online platforms, thus further enhance cyber security knowledge. Moreover, the analyses of the research can be altered to include other elements, such as new systems and new technologies to further improve the security. Therefore, this research can be used as an additional input when evaluating new possibilities of integration of ICT security.

The present research was limited by the extent of Bachelor’s Thesis. Therefore, the scope of this study was narrowed down to include mainly the collaboration between the e-commerce and ICT security and mainly external threats. However, the essential elements such as the tools, methods, threats, the role of ICT security within organizations and the customers were analyzed to increase the validity of the findings. This limitation means that the current research was not designed for optimal results in long-run. Thus, the optimization of implementation is needed according to the speed of new technologies emerging. The reason being the Internet is a fast-developing field and today it is fully utilized in many projects.

There is an opportunity for a study on how the e-commerce could be further improved security and performance wise. There is also a need for assessing how the SMEs in Finland will perceive ICT security in the following years. For future research directions, transaction security systems may be one of the topics to be researched on, as transactions are one of the targets of cyber criminals. As such management information system (hereinafter MIS) was discovered during research, and it suggests to be a solution for most of the transaction security issues. Therefore, further research on security is recommended to be conducted in MIS perspective in conjunction with this research. Additionally, constant threats with identity thefts call for an opportunity to research different authentication systems to provide a most suitable solution for e-commerce systems. Additonally, this research did not cover mobile and tablets security, however tablets and mobile is new technology which seems to have taken place of computers. Therefore, research on the security of mobile and tablets is suggested.

For business perspective, a system that allows anonymous browsing and hiding one’s identity online will provide another layer of protection. As today, businesses have used VPN and different proxies to hide themselves, but NSA or other government organizations can still identify entities. Therefore, new technology called TOR was invented. Furthermore, this technology may help e-commerce system organization to become more secure from espionage or such Internet attacks. As such, TOR may be an interesting topic to research on how it functions with e-commerce systems to create more secure environment for consumers.

REFERENCES

Abrams, R. 2003. The successful business plan: Secrets & Strategies 4th Edition. US: Planning Shop.

Acunetix 2014. CSRF Attacks, XSRF or Sea-Surf – What They Are and How to Defend Against Them. Referenced 14.11.2014. http://www.acunetix.com/websitesecurity/csrf-attacks/

Bakari, J., Tarimo, C., Yngström, L., Magnusson, C. & Kowalski, S. 2006. Bridging the gap between general management and technicians – A case study on ICT security in a developing country. Referenced 2.3.2015. http://www.sciencedirect.com/science/article/pii/S0167404806001568

Banerjee, S. 2007. Business Plans – Your Roadway to Success. Referenced 30.1.2015. http://ezinearticles.com/?Business-Plans---Your-Roadway-To-Success&id=695295

Boston University 2014. Preventing & removing spyware. Referenced 19.9.2014. http://www.bu.edu/tech/services/support/desktop/software/removal/security/spyware/preventing/

Brinkmann, M. 2012. How Programs Trick You Into Installing Adware On Your Computer. Referenced 13.10.2014. http://www.ghacks.net/2012/02/20/how-programs-trick-you-into-installing-adware-on-your-computer/

Campanelli, M. 2006. How to Set Up an E-Commerce Site. Referenced 10.10.2013. http://www.entrepreneur.com/article/84250

Chaffey, D. 2009. E-business and e-commerce management 4th Edition. Strategy, implementation and practice. United Kingdom: Financial Times.

Chickowski, E. 2013. Don't Underestimate Directory Traversal Attacks. Referenced 17.10.2014. http://www.darkreading.com/vulnerabilities---threats/dont-underestimate-directory-traversal-attacks/d/d-id/1140306?

CIBC 2014. Spyware and removal. Referenced 14.10.2014. https://www.cibc.com/ca/legal/spyware-info.html

Coburn, R. 2012. Importance Of SSL Encryptions For The Business Website. Referenced 2.2.2015. http://ezinearticles.com/?Importance-Of-SSL-Encryptions-For-The-Business-Website&id=7053724

Cooper, R. & Schindler, P. 2000. Business Research methods. United Kingdom: McGraw-Hill.

Correia, A., Abreu, F. & Amaral, V. 2011. SLALOM: a Language for SLA Specification and Monitoring. Referenced 23.9.2013. http://arxiv.org/ftp/arxiv/papers/1109/1109.6740.pdf

Datanyze 2015. E-commerce Platforms market share in Finland. Referenced 2.3.2015. https://www.datanyze.com/market-share/e-commerce-platforms/Finland

DigiCert 2014. What Is SSL (Secure Sockets Layer) and What Are SSL Certificates? Referenced 26.12.2014. https://www.digicert.com/ssl.htm

Djuliy, M. 2014. Create CSRF protect on your site! Referenced 18.7.2014. http://www.devbattles.com/sand/post-51-Create-CSRF-protect-on-your-site-

Dupaul, N. 2015. Cross-Site Request Forgery Guide: Learn All About CSRF Attacks and CSRF Protection. Referenced 2.2.2015. http://www.veracode.com/security/csrf

eMarketer 2014. Worldwide Ecommerce Sales to Increase Nearly 20% in 2014. Referenced 17.12.2014. http://www.emarketer.com/Article/Worldwide-Ecommerce-Sales-Increase-Nearly-20-2014/1011039

Flagmerchantservice 2014. Referenced 12.10.2014. http://www.flagshipmerchantservice.com/e-commerce.php

Force10 2007. Benchmarking Uptime for Your Business: Methodology and Best Practices. Referenced 2 2.2015. http://www.networld.com.au/docs/BenchmarkingUptime.pdf

Forristal, J. 2001. Hack proofing your web applications. Syngress Publishing Inc.

Francillon, A., Danev, B. & Capkun, S. 2010. Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars. Referenced 20.9.2013. https://eprint.iacr.org/2010/332.pdf

Franklin, W. 2007. Computer Hackers Wanted For Organized Cyber Crime. Referenced 6.5.2015. http://ezinearticles.com/?Computer-Hackers-Wanted-For-Organized-Cyber-Crime&id=538008

Freedman, E. 2007. Protect Your Computer From Hackers. Referenced 6.5.2015. http://ezinearticles.com/?Protect-Your-Computer-From-Hackers&id=774615

Garofolo 2014. ANATOMY OF A CROSS-SITE REQUEST FORGERY ATTACK. Referenced 2.2.2015. http://www.learnallthenodes.com/episodes/34-anatomy-of-a-cross-site-request-forgery-attack

Goodchild, J. 2012. Social Engineering: The Basics. Referenced 19.12.2014. http://www.energycollection.us/Energy-Security/Social-Engineering-Basics.pdf

Hazrati, Vikas 2008. The Truth About Availability: What does 99.99% mean? https://vikashazrati.wordpress.com/2008/10/24/truth-about-availabilit/

ICT Driving license 2014. Avoiding Online scams. Referenced 28 October 2014. http://blogs.helsinki.fi/ict-driving-licence/5-information-security-and-privacy-protection/5-2-protecting-yourself-from-threats/avoiding-online-scams/

Internetlivestats 2015. Internet users. Referenced 13.2.2015. http://www.internetlivestats.com/internet-users/#trend

Internetworldstats 2014. Internet growth statistics. Referenced 13.2. 2015. http://www.internetworldstats.com/emarketing.htm

Intuit 2013. Phishing, pharming, vishing and smishing. Referenced 30.10.2013. https://security.intuit.com/phishing.html

Kaspersky 2014. What is spyware & what does it do? Referenced 21.9.2014. http://usa.kaspersky.com/internet-security-center/threats/spyware

Kauppakamari 2015. Yrityksiin kohdistuvat kyberuhat 2015. Referenced 26.3.2015. http://www.digipaper.fi/kauppakamari/127242/

Klein, A. 2005. DOM Based Cross Site Scripting or XSS of the Third Kind. Referenced 14.11.2014.
http://www.webappsec.org/projects/articles/071105.shtml

KPMG 2013. Unknown threat in Finland. Referenced 26.3.2015.
http://www.kpmg.com/FI/fi/Ajankohtaista/Uutisia-ja-julkaisuja/Neuvontapalvelut/Documents/unknown-threat-in-finland.pdf

Krishnaswami, O. & Satyaprasad, B. 2010. Business Research Methods. India: Global Media.

Leach, S. 2013. Four ways to defend against DDoS attacks. Referenced 5.12.2014.
http://www.networkworld.com/article/2170051/tech-primers/four-ways-to-defend-against-ddos-attacks.html

Lindsay, S. 2007. Security – An Ethical Hacker? Referenced 6.5.2015.
http://ezinearticles.com/?Security---An-Ethical-Hacker?&id=700657

Linn, M. 2010. What is SQL Injection? Referenced 2.3.2015.
http://ezinearticles.com/?What-is-a-SQL-Injection-Attack?&id=4410585

Mabute, A. 2009. Hackers and Social Engineering Techniques. Referenced 6.5.2015.
http://ezinearticles.com/?Hackers-and-Social-Engineering-Techniques&id=3324656

Makker, A. 2011. Directory Transversal Vulnerability - Explained thoroughly. Referenced 17.11.2014.
http://www.explorehacking.com/2011/01/directory-transversal-vulnerability.html

Mandiant APT1 2013. Exposing One of China’s Cyber Espionage Units. Referenced 24.3.2015.
http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

McEwan, H. 2010. What is information security and why does it matter? Referenced 2.2.2015.
http://ezinearticles.com/?What-is-Information-Security-and-Why-Does-it-Matter?&id=4724526

Microsoft 2003. Improving web application security. Threats and countermeasures. Referenced 19.8.2013.

http://www.microsoft.com/en-us/download/details.aspx?id=1330

Microsoft 2014. What is spyware? Safety & Security Center. Referenced 14.11.2014.
http://www.microsoft.com/security/pc-security/spyware-whatis.aspx

Molie, C. 2005. Computer security – What exactly is it?
Referenced 19.3.2015.
http://ezinearticles.com/?Computer-Security---What-Exactly-Is-It?&id=31194

Murray, W. 2011. Pen Testing – The World Of The Ethical Hacker. Referenced 6.5.2015.
http://ezinearticles.com/?Pen-Testing---The-World-Of-The-Ethical-Hacker&id=5853790

Nahari, H. & Krutz, R. 2011. Web Commerce Security: Design and Development. US: Wiley Publishing Inc.

Neder, M. 2012. What You Need to Know About Protecting Yourself From Hackers. Referenced 6.5.2015.
http://ezinearticles.com/?What-You-Need-to-Know-About-Protecting-Yourself-From-Hackers&id=7075283

Odlyzko, A. 2010. Providing Security With Insecure Systems. Referenced 26.9.2013.
http://www.dtc.umn.edu/~odlyzko/doc/wisec2010.pdf

OWASP 2014a. Types of Cross-Site Scripting. Referenced 12.11.2014.
https://www.owasp.org/index.php/Types_of_Cross-Site_Scripting

OWASP 2014b. Cross-Site Request Forgery (CSRF). Referenced 13.11.2014.
https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)

Paretologic 2014. Spyware Info, Advice, Facts & More. Referenced 19.9.2014.
http://www.paretologic.com/resources/paretolabs/as/index.aspx

Pfleeger, S. & Pfleeger, C. 2003. Program security. Referenced 12.10.2013.
http://www.informit.com/articles/article.aspx?p=31782&seqNum=3

PHP 2014. Prepared statements. Referenced 28.10.2014.
http://php.net/manual/en/mysqli.quickstart.prepared-statements.php

Protalinski, E. 2014. Lizard Squad launches DDoS tool that lets anyone take down online services, starting at $6 per month. Referenced 30.3.2015.

http://venturebeat.com/2014/12/30/lizard-squad-launches-ddos-tool-that-lets-anyone-take-down-online-services-starting-at-5-99-per-month/

PwC 2015. Global State of Information Security Survey: Key findings and trends. Incidents and financial impact continue to soar. Referenced 26.3.2015.
http://www.pwc.com/gx/en/consulting-services/information-security-survey/key-findings.jhtml

Russell, R., Kaminsky, D., Puppy, R., Grand, J., Graham, R., K2, Ahmad, D., Flynn, H., Dubrawsky, I., Manzuik, S., Permeh, R., Johnson, N. Jr., Pfeil, K. & Lynch, W. 2002. Hack proofing your network 2nd edition. US: Syngress Publishing Inc.

Sachdeva, J. 2009. Business Research Methodology. India: Global Media.

Sage Publications 2015. Business Planning and Marketing Strategy in a Nutshell. Referenced 17.1.2015.
http://www.sagepub.in/upm-data/61130_Chapter_1.pdf

Seksek, T. 2014. Payment Gateways in the #UAE. Referenced 15.9.2014.
http://interactiveme.com/2012/02/payment-gateways-in-the-uae/

Selinger, M. 2014. 17 software packages in a repair performance test after malware attacks. Referenced 19.9.2014.
http://www.av-test.org/en/news/news-single-view/17-software-packages-in-a-repair-performance-test-after-malware-attacks/?=

Shankdhar, P. 2013. DOS Attacks and Free DOS Attacking Tools. Referenced 30.3.2015.
http://resources.infosecinstitute.com/dos-attacks-free-dos-attacking-tools/

Shopify 2014. Try Shopify for 14 days free, with no risk. Referenced 15.9.2014.
http://www.shopify.com/pricing

Shum, T. 2010. Moving your business online. Referenced 13.2.2015.
http://ezinearticles.com/?Moving-Your-Business-Online&id=3900953

Souza, F. 2014. Highly Effective Joomla Backdoor with Small Profile. Referenced 2.3.2015.
http://blog.sucuri.net/2014/02/highly-effective-joomla-backdoor-with-small-profile.html

Statistics Finland 2014. Usage of the internet. Referenced 13.2.2015.

http://www.stat.fi/til/sutivi/2014/sutivi_2014_2014-11-06_kat_001_fi.html

TNS Gallup 2013. Verkkokauppatilasto 2013. Referenced 2.3.2015. http://www.tns-gallup.fi/doc/digi/Verkkokauppatilasto_2013.pdf

TNS Gallup 2014. Nettrack 2014. Referenced 2.3.2015. http://www.iab.fi/media/pdf-tiedostot/verkkomainonnan-abc/nettrack-2014_iab.pdf

Vella, K. 2006. On the Origin and Evolution of Computer Viruses. Referenced 2.3.2015. http://ezinearticles.com/?On-the-Origin-and-Evolution-of-Computer-Viruses&id=165078

Viestintävirasto 2014. WordPress lisäosassa kriittinen haavoittuvuus. Referenced 2.4.2015. https://www.viestintavirasto.fi/kyberturvallisuus/haavoittuvuudet/2014/haavoittuvuus-2014-095.html

VISA 2014. Merchants. Referenced 20.10.2014. http://usa.visa.com/merchants/protect-your-business/cisp/merchant-pci-dss-compliance.jsp

Vänskä, O. 2015. HS: Suomalaisten pankkitunnuksilla varastettiin 550 000 euroa - oikeudenkäynti alkaa tänään. Retrieved 2.4.2015. http://www.tivi.fi/Kaikki_uutiset/2015-02-11/HS-Suomalaisten-pankkitunnuksilla-varastettiin-550-000-euroa---oikeudenk%C3%A4ynti-alkaa-t%C3%A4n%C3%A4%C3%A4n-3215580.html

Webtoolsandtips 2009. What is a fake security warning. Referenced 12.10.2013. http://webtoolsandtips.com/remove-spyware/fake-security-warnings-how-to-stop/

Whitty, B. 2014. Why do people create viruses. Retrived 26.3.2015. https://www.technibble.com/why-do-people-create-computer-viruses/

Wikihow 2014. How to prevent SQL injection in PHP. Referenced 2.3.2015. http://www.wikihow.com/Prevent-SQL-Injection-in-PHP

Witherspoon, J. 2010. Types of Hackers. Referenced 6.5.2015. http://ezinearticles.com/?Types-of-Hackers&id=5357804

Yariv, E. 2011. Database Security for Businesses and How It Relates to PCI-DSS Compliance. Referenced 30.8.2014. http://ezinearticles.com/?Database-Security-for-Businesses-and-How-It-Relates-to-PCI-DSS-Compliance&id=5804430

Yle 2014. Jyväskyläläinen Paytrail jyrää verkkokaupassa. Referenced 2.3.2015. http://yle.fi/uutiset/jyvaskylalainen_paytrail_jyraa_verkkokaupassa/7531934

Yle 2015. OP still under attack, Danske Bank also down. Referenced 2.3.2015. http://yle.fi/uutiset/op_still_under_attack_danske_bank_also_down/7720113

Yrittäjät 2014. The small and medium-size enterprises. Referenced 30.9.2014. http://www.yrittajat.fi/en-GB/federation_of_finnish_enterprises/entrepeneurship_in_finland/