TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Dennis Bykov 201723IVSB

Payment Security Aspects and Implementation of Necessary Safeguards in the Start-Up Infrastructure

Bachelor's thesis

Supervisor: Toomas Lepikult
PhD

Tallinn 2023

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Dennis Bykov 201723IVSB

Makse turvaaspektid ja vajalike kaitsemeetmete rakendamine startup-ettevõtte infrastruktuuris

Bakalaureusetöö

Juhendaja: Toomas Lepikult
PhD

Tallinn 2023

Author’s declaration of originality

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

Author: Dennis Bykov

24.04.2023

Abstract

This bachelor's thesis aims to provide a comprehensive overview of the key payment security aspects necessary to ensure the reliable and seamless operation of a start-up payment system. The study will delve into the measures that are essential for protecting payment system-related business operations.

This study will undertake a thorough analysis of the key safeguards necessary for ensuring the security of payment systems, including PCI compliance, data encryption, tokenization, address verification service, card verification value, 3-D secure, and physical infrastructure.

The author of this thesis aims to develop a comprehensive manual that will serve as a practical guide for companies seeking to establish a payment system that inspires trust and confidence among their clients. The manual will provide valuable insights into the various security measures and protocols that are critical for maintaining the integrity and reliability of payment systems.

This thesis is written in English and is 59 pages long, including 5 chapters, 0 figures and 0 tables.

Annotatsioon

Makse turvaaspektid ja vajalike kaitsemeetmete rakendamine startup-ettevõtte infrastruktuuris

Antud bakalaureusetöö eesmärk on anda põhjalik ülevaade olulisematest makseturvalisuse aspektidest, mis on vajalikud alustavate maksesüsteemide usaldusväärse ja tõrgeteta toimimise tagamiseks. Uurimus keskendub meetmetele, mis on vajalikud maksesüsteemiga seotud äriliste protsesside kaitsmiseks.

Antud uurimus teostab põhjaliku analüüsi maksesüsteemide turvalisuse tagamiseks oluliste kaitsemeetmete kohta, sealhulgas PCI-nõuete täitmise, andmete krüpteerimise, tokeniseerimise, aadressikinnitusteenuse, kaardikontrollväärtuse, 3-D Secure ja füüsilise infrastruktuuri kohta.

Töö autor eesmärk on välja töötada kõikehõlmav juhend, mis toimiks praktilise abivahendina ettevõtetele, kes soovivad luua maksesüsteemi, mis tekitaks nende klientides usaldust ja kindlustunnet. Juhend pakub väärtuslikke teadmisi erinevate turvameetmete ja protokollide kohta, mis on olulised maksesüsteemi usaldusväärsuse ja terviklikkuse tagamiseks.

Lõputöö on kirjutatud inglese keeles ning sisaldab teksti 59 leheküljel, 5 peatükki, 0 joonist, 0 tabelit.

List of abbreviations and terms

3DS	3-D Secure
AVS	Address Verification System
CAV	Card Authentication Value
CDE	Common Data Environment
CID	Card Identification Number
CNP	Card not Present
CRM	Customer Relation Management
CVC	Card Validation Code
CVV	Card Verification Value
DDoS	Distributed Denial of Service
DMZ	Demilitarized Zone
ERP	Enterprise Resource Planning
FIM	File Integrity Monitoring
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IT	Information Technology
LAN	Local Area Network
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
OS	Operating System
PAN	Primary Account Number
PC	Personal Computer
PCI DSS	Payment Card Industry Data Security Standard
PIN	Personal Identification Number
POS	Point of Sale
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Socket Layer

TLS	Transport Layer Security
WAN	Wide Area Network
VPN	Virtual Private Network

Table of contents

1 Introduction

As the world becomes more reliant on technology, new companies are emerging in a variety of industries, including the industry of online payment processing. However, startups are especially susceptible to cyberattacks due to their lack of experience, limited resources, and limited financial resources. Developing and sustaining a secure infrastructure is essential for the survival of start-up businesses, particularly in the online payment industry. [1]

There are numerous factors why payment-related businesses must maintain a secure infrastructure. First, as cybercrime has increased over the past few years [2], the need for robust security measures has become more important than ever. Due to the substantial financial advantages that can be obtained by exploiting security flaws, payment systems and businesses are among the top targets for cybercriminals. A single security breach can result in the loss of sensitive consumer information, reputational harm, and substantial financial loss.

Secondly, payment-related businesses must adhere to the Payment Card Industry Data Security Standard (PCI DSS) in order to maintain a positive relationship with customers. PCI DSS is a set of standards designed to assure the security and dependability of payment systems. The standard incorporates storage, processing, and transmission requirements for payment card data. To achieve PCI compliance, businesses must implement particular security measures and procedures to safeguard their payment systems and consumer data.

PCI and other established security standards are incorporated into the guidelines for establishing a secure infrastructure for payment-related services offered by new companies. These measures are scalable and adaptable for businesses of varying sizes, and they are applicable outside of the payment industry.

Companies can ensure their infrastructure is secure and compliant with regulations by utilizing the best security practices based on established security standards. Compliance with these standards not only reduces the risk of data intrusions and cyber-attacks, but also promotes customer confidence, reduces the likelihood of legal repercussions, and preserves operational stability.

This thesis focuses on the security of payment systems and the implementation of necessary measures to guarantee a secure environment in startup infrastructures. The thesis seeks to resolve two major issues. It will first address the difficulty of establishing a secure infrastructure for payment-related startups. Second, it will investigate the techniques and best practices necessary to implement effective safeguards in the infrastructure to ensure maximum security. The primary objective of this research is to produce a comprehensive guide on how to establish a secure start-up infrastructure and to examine the process of developing and implementing the necessary safeguards to achieve this objective.

1.1 The Concept of Payment Related Start-Up

The word “start-up” is both confusing and pervasive. The Oxford English Dictionary Online describes it as “a firm that is in the process of launching”, typically in the context of a “start-up company”. For the time being, it appears that the term “start-up” is more connected with tech-based businesses, even ones that are already well-established, because these are frequently the most successful and conspicuous. Nevertheless, this visibility is contingent on more than just success. [3]

A start-up firm is a company or organization in its earliest stages, which are often marked by high levels of uncertainty and risk. Typically, a startup is a newly established business, but it can also be an established company undergoing a period of significant change or transformation.

Start-up is sometimes used synonymously with small business and new business. Yet, there are significant distinctions between start-ups and small firms. Start-ups are typically distinguished by their new goods or services, distinctive business methods, and rapid growth. Small enterprises, in comparison, are often more mature organizations with more consistent revenue sources.

Yet, there are a few qualities that are frequently used to describe start-ups. Start-up features include:

- Frequently recognized for their innovative products and services. They frequently attempt to tackle a problem in an original or novel manner.
- Typically possess a business model that is distinct from that of more established companies.
- Generally, they enjoy rapid growth, frequently at a significantly faster rate than more established enterprises.
- Frequently high-risk and high-uncertainty ventures due to their lack of history and experience.
- Frequently created by a group of individuals who are committed to the success of their firm.

The objectives of a start-up are to introduce an innovative item or service to the marketplace, build client traction, and become profitable. Often, the earliest phases of a startup are the most difficult, as the firm is still establishing its foundation and attempting to prove its worth in the market. At this period, it is crucial for the firm to remain focused on accomplishing its fundamental objectives.

Branding is one of the most significant objectives for a new product or service. This can be difficult since the business must find a means to distinguish itself in a crowded market. Nonetheless, it is vital for the company to expose its item of business to potential clients in order to begin producing revenue.

A further essential objective for a business is to acquire client traction. This necessitates that the startup has a strategy for attracting and retaining clients. This can be challenging, as customers may be apprehensive to test a startup's new product or service. Yet, the likelihood of success will increase if the firm can deliver value to its clients and establish a solid relationship with customers.

A startup must also concentrate on being profitable. This might be an issue, as starting income may not arrive immediately. To ensure its long-term viability, the firm must, nevertheless, prioritize generating revenue. [4]

Nonetheless, it is impossible to be profitable for business without any payment process concept. Therefore, it is crucial to define the payment process concept.

Generally, a payment process for businesses consists of many processes that permit the transfer of payments between a client and an organization. Note that the payment procedure may differ based on the type of business and payment method chosen.

Payment is often initiated by the consumer, who selects a payment mechanism such as a credit or debit card. This can be accomplished in person, online, or via phone.

When the consumer has picked a method of payment, the payment must be authorized by the payment processor. This include confirming the customer's payment details, ensuring they have adequate funds, and examining their account for unusual behavior.

After authorization, the payment processor executes the payment by moving funds from the customer's account to the business's account. Often, this entails sending the funds via the payment gateway, which works as an intermediary between the customer's bank and the business's bank.

When the payment has been completed, the money is deposited into the company's bank account. Depending on the payment type used, this might take anything from a few hours to a few days.

Next, the company must reconcile the payment with its accounting records to confirm that the payment was recorded and accounted for correctly. [5]

Nevertheless, every company can outsource payment process for several reasons. Firstly, payments can be a quick and efficient option for businesses that wish to switch to a paperless process and improve workflows without introducing a large number of new procedures. Secondly, a good method for reducing processing expenses and scaling your organization without increasing personnel. [6]

In contrast, there are pros for creating a custom payment gateway [7]:

- Over time, reduced monthly and per-transaction costs.
- Complete control over payment processing.

- The capacity to develop individualized experience.
- It is possible to offer custom payment gateway services to other businesses to increase your earnings.

In conclusion, this part of the thesis gives a brief overview of basic concepts. First, a start-up company is a corporation or organization in its initial phases, which are frequently characterized by elevated levels of uncertainty and risk. Second, the payment process can differ in every organization. Therefore, this thesis will not focus on the outsourcing payment process.

1.2 The Challenges of Online Payment Industry

Cyberattacks follow patterns possibly more than any other sort of crime. When security experts develop new ways to defend against outdated approaches, attackers find new ways to breach enterprise defences. Cybercrime may be profitable, since researchers estimate that by 2025 it would cost the globe $10.5 trillion yearly. In response to this expanding danger, the world's digital defences have strengthened, but many hackers have embraced a new tactic. With social engineering, they target the most susceptible assets of enterprises, the people whom software cannot fully protect. [8]

Social engineering is a form of attack that takes advantage of human mistakes to acquire confidential information, access, or assets. In social engineering, attackers can use a number of ways to coerce unwitting consumers, workers, or third parties into disclosing information, hence distributing malware.

In a business environment, social engineering attacks frequently aim to obtain and exploit knowledge regarding the target organization's business processes, decision-making structures, and any underlying gaps or control weaknesses.

Also, social engineering assaults range from bulk emails that are relatively easy to recognize as an attempt to scam a person to emails and phone calls that target an individual customer or employee. [9]

The propagation of malware has increased rapidly. The initial surge increased the number of harmful files and programs attacking the Internet. In subsequent years, the rate of expansion may have slowed, but it has not halted. Even with antivirus software incorporated into the most recent operating systems, there is more malware than ever before on the Internet. [10]

Malware, an abbreviation for malicious software, refers to a broad category of hostile or invasive software. Malware is created by cybercriminals to compromise computing operations, steal data, circumvent access restrictions, and cause damage to host systems, client devices, and their applications or data.

Malware is one of the most significant risks to cyber security today. Malware includes viruses, worms, remote access tools, rootkits, Trojans, spyware, and adware, among many more.

Malware exploits software vulnerabilities in browsers, third-party applications, and operating systems to obtain access to the device and its data and resources. To propagate, malware also employs social engineering tactics to deceive people into installing and executing the harmful code.

Another common type of threat is Distributed Denial of Service (DDoS). DDoS is the process of incapacitating the systems of an organization, often customer-facing websites, by flooding them with malicious digital traffic. While they are commonly available for purchase on the dark web, these assaults are often carried out by threat actors of a lower tier. Although the impact on a targeted financial institution's soundness is minimal, it may result in reputational harm and/or impede customer service. [9]

In recent years, the frequency of DDoS assaults has significantly increased. According to research by Cloudflare, ransom DDoS assaults climbed by over a third between 2020 and 2021 and spiked by 75% in the fourth quarter of 2021 compared to the preceding quarter. In 2021, there were more DDoS attacks than in previous years. [11]

The other type of fraud is monetization channels. A thief who has successfully established a fake payment transaction (whether authorized or not) is aware that investigators will soon follow the trail and that the transaction amount may be blocked and refunded. Thus, he seeks to instantly leverage a monetization channel: a cash withdrawal, a purchase (that leaves no trace), a money transfer, or a transfer to another bank account from which a withdrawal, purchase, or transfer may be undertaken. Examples of purchases that leave no trace include the purchase of crypto currencies, casino credits, or things that are quickly redeemable online. [9]

Despite all the fraud challenges, another difficulty that start-ups may encounter is compliance. PCI compliance, as one of the well-known regulators, requires merchants and other companies to handle credit card information securely, therefore reducing the possibility that cardholders' sensitive financial account information may be compromised. If merchants do not manage credit card data in accordance with PCI regulations, the data might be compromised and used for a variety of fraudulent activities. Moreover, sensitive cardholder information might be utilized for identity theft. [12]

To sum up, there is a plethora of different challenges and security questions that make a start-up life more difficult. It can be a group of hackers that want to get sensitive information or steal money. Yet, there is a positive challenge intended to make the payment industry more secure.

1.3 Creation and Maintenance of a Secure Infrastructure

Nowadays, it is crucial to understand that it is possible to create different types of infrastructure. Traditional infrastructure and cloud infrastructure are the two primary types of information technology (IT) infrastructure. A regular IT infrastructure consists of the standard hardware and software components, including facilities, data centres, servers, networking devices, desktop personal computers (PC), and corporate application software solutions. This infrastructure architecture often takes more power, space, and money than other infrastructure designs. Typically, a conventional infrastructure is established on-premises for exclusive or private corporate usage. Another type is cloud infrastructure. A cloud computing system infrastructure and classical infrastructure are comparable. Using virtualization end users may access the infrastructure over the internet and utilize computer resources without installing them locally. Virtualization links physical servers maintained by a service provider in a variety of geographical locations. Then, it partitions and abstracts resources, such as storage, to make them accessible to users almost everywhere an internet connection can be established.

Before security is implemented on each layer of the infrastructure, it is crucial to understand the components of each element.

In general, IT infrastructure is composed of interconnected pieces, with hardware and software being the two primary groupings. Hardware requires software, like an operating system (OS), to work. Similarly, an operating system handles hardware and system resources. With networking components, operating systems also establish links between software applications and physical resources.

IT infrastructure configurations vary based on company needs and objectives, although certain objectives are fundamental to all businesses. The best infrastructure will give a firm with high-performance storage, a network with low latency, security, an efficient wide area network (WAN), virtualization, and zero downtime. Secure infrastructures include information access and data availability control systems. It may also protect a corporation from data breaches and cyberattacks wherever the data lives, preserving consumer confidence. [13]

2 Payment Security Aspects

In this section of the paper, author outlines crucial security aspects in payment industry. The key concepts are PCI Compliance, Data Encryption, Tokenization, Address Verification System, Card Verification Value, 3-D Secure. Nevertheless, the concept of physical infrastructure of a payment processing company is described.

2.1 PCI Compliance

The PCI Data Security Standard is a set of criteria or guidelines that businesses must adhere to in order to be declared PCI DSS compliant. Achieving these requirements permits them to conduct business with credit card and debit card issuers and to process their transactions. PCI DSS stands for Payment Card Industry Data Security Standard. The PCI Data Security Standard is regulated by the PCI Security Standards Council. The PCI SSC is a global forum that implements the PCI Data Security Standard's rules and requirements. In other words, they verify that businesses are PCI DSS-compliant or certified.

The PCI DSS standards include twelve regulations mandating firewalls, encryption, and security protocols to prevent unauthorized personnel from reading sensitive data. All these measures are in place to protect consumers and businesses against fraud and theft.

In addition to adhering to PCI DSS regulations, businesses must also undergo a yearly audit by an approved PCI auditor in order to maintain Level 1 certification. These auditors evaluate corporate security systems and procedures to ensure that businesses comply with PCI regulations. [14]

PCI DSS applies to all merchants, processors, acquirers, issuers, and service providers involved in payment card processing. All other entities that store, handle, or transport cardholder data and/or sensitive authentication data must comply with PCI DSS. Cardholder data and sensitive authentication data are defined as follows:

- Primary Account Number (PAN),
- Cardholder Name,

- Expiration Date,
- Service Code,
- Full track data (magnetic-stripe data or equivalent on a chip),
- Card Authentication Value 2 (CAV2), Card Validation Code 2 (CVC2), Card Verification Value 2 (CVV2), Card Identification Number (CID),
- Personal Identification Value (PIN).

The primary account number defines cardholder information. If cardholder name, service code, and/or expiration date are stored, transmitted, or otherwise present in the cardholder data environment (CDE), they must be safeguarded in line with applicable PCI DSS rules. Some PCI DSS rules may also apply to businesses that have outsourced their payment operations or CDE management. In addition, firms that outsource their CDE or payment operations to third parties are responsible for ensuring that the third party protects account data in accordance with PCI DSS rules. [15]

2.2 Data Encryption in the Online Payment Industry

Encryption transforms data into unintelligible language that can only be read by those who possess encryption keys. Without the key, the encrypted data (also known as ciphertext) is illegible. Encrypting data does not prevent data theft from occurring. Yet, in the event of data theft, it stops the person or entity from reading the information. Data encryption in payment processing protects your clients against credit card fraud.

Encryption protects transferring digital data on the cloud, computers, and point-of-sale devices. These algorithms assist security measures such as integrity, authentication, and non-repudiation in addition to protecting data. They begin by authenticating the origin of a message. Once the origin has been verified, the content's integrity is examined. The non-repudiation initiative precludes senders from denying valid activity as a final precaution.

This method is applicable to a wide range of data protection needs, including government-classified information and credit card transactions. [16]

2.3 Tokenization in Payment Processing

Tokenization is a procedure that replaces a high-value credential (such as a payment card main account number or a Social Security number) with a surrogate value that is used in place of the original credential in transactions.

Tokenization can transfer a high-value credential to a new value that is in a different format or a format that is similar to the original format. The goal of tokenization in payments is to remove account data from the payment environment and replace it with something that is useless outside of the environment in which the token was formed. Tokenization is one method for preventing the theft and misuse of payment information for fraudulent transactions. Tokenization may allow merchants to decrease the scope of a PCI DSS audit.

There are various token types and methods for their creation. A token may be vendor specific. It can be used once or multiple times. It can be kept and controlled in the cloud, a token vault, or at the location of the merchant. Using a procedure described by the token solution provider, a token is generated. Once a token has been generated, it can be associated with a card on file, a specific transaction, a payment card, or a device.

The adoption of secure tokenization products is projected to reduce the number of locations, systems, and networks where cardholder information is stored, processed, or sent. A secure tokenization system may aid in minimizing the retention of credit card data in an organization's environment, hence facilitating PCI DSS compliance. [17]

2.4 Address Verification System as a Fraud-Prevention Measure for Card Not Present Transactions

The Address Verification Service (AVS) is a mechanism for preventing fraud and chargebacks that can aid in their reduction. AVS checks that the billing address given by the client matches the billing address connected with the credit card account of the cardholder.

The address verification is performed as part of the merchant's credit card transaction authorization request. In a non-face-to-face transaction, the credit card processor returns a response code to the merchant showing the degree of address matching, thereby confirming ownership of a credit or debit card. This procedure assists the merchant in determining whether to accept or reject a card transaction.

Major credit card companies use AVS extensively to prevent card-not-present (CNP) fraud. However, the system is not foolproof. The billing address provided by a genuine cardholder may not always match the card issuer's records. For instance, an address may not match if the cardholder has just relocated or if the address on file is inaccurate. In such circumstances, the merchant risks rejecting a valid transaction.

A customer's billing address is compared to the address on file with the issuing bank during the checkout procedure. After comparing the two addresses, the issuing bank returns an AVS code to the merchant. This AVS code can help merchants discern how to proceed with the transaction.

AVS response codes are single-letter codes that are returned to the merchant through their processing platform during the authorization procedure. These codes assist in determining the subsequent action, which may be to approve or deny the transaction.

Typically, AVS authentication is employed as part of a multilayered fraud protection system to ensure that only valid transactions are authorized, and dubious ones are denied. [18]

2.5 Purpose of Card Verification Value and 3-D Secure

A validation code is a series of three or four numbers located on the front or rear of a credit card. It is also known as a CVV, CV2, or CVV2 code. It is intended to provide an additional layer of protection for online and telephone credit card transactions.

The risk posed by identity theft and other forms of credit card fraud has grown in severity. The use of validation codes when making credit card purchases is one measure taken to attempt to mitigate this risk.

A client will typically be required to provide their name, billing address, card number, expiration date, and validation code during a transaction. Although many of these details, including the name and address, could conceivably be obtained from other sources, the card number, expiration date, and validation code could only be obtained by physically possessing the card. Generally, the validation code is printed on the rear of the card as an added security measure, making it more difficult for thieves to obtain all the necessary information from a single photograph of the credit card.

Consumer protection laws prohibit merchants from storing customers' validation codes after a purchase has been made; however, dishonest sellers may still capture this information illegally. Personal identification numbers that cardholders must input when making payments at point-of-sale (POS) terminals provide an additional layer of security. [19]

Another important security control is 3-D Secure. 3DS is utilized by payment card issuers and merchants to authenticate consumers and prevent CNP fraud. 3DS permits the exchange of data or communications between the merchant and the issuer in order to authenticate the consumer and authorize the transaction. The data includes transaction, payment method, and device information. Using this data, issuers can quickly and accurately identify and prevent fraudulent card transactions without adding unneeded friction to the payment process, which frequently results in abandoned purchases. [20]

When a consumer tries to make a purchase on a website using a credit or debit card, 3DS necessitates cardholders to perform an additional verification step when paying. Typically, a person is redirected to an authentication page on their bank's website, where they input the card's password, or a code sent to their phone. [21]

2.6 Physical Infrastructure of a Payment Processing Company

IT infrastructure refers to the hardware, software, network resources, and services required for the existence, administration, and operation of an enterprise. Infrastructure enables an organization to provide technology solutions and services to its employees, partners, and/or consumers. Therefore, the infrastructure itself can be divided into different domains: hardware, software, and network infrastructure.

Hardware is one of the components of an IT infrastructure, and it consists of all the elements required to support the fundamental operation of the machines and devices that make up the infrastructure. For instance, hardware is — servers, computers, storage and data centres, switches, ports, and routers, in addition to all other equipment including power, cooling, cabling, and dedicated rooms.

Nevertheless, another crucial element of the infrastructure is software. It refers to all enterprise applications used both internally and externally to provide services to consumers. Web servers, enterprise resource planning (ERP), customer relationship management (CRM), productivity applications, and the operating system are examples of software. The operating system is the most essential software component because it manages the hardware and connects physical resources to the network infrastructure.

Furthermore, all elements and devices must establish internal and external communication through the network. The network component consists of all hardware and software components required for network enablement, internet connectivity, firewall protection, and security. It ensures that personnel can only access stored and transferred data through rigorously controlled access points, thereby reducing the risk of data loss or theft. [22]

Another important concept of the network is Local Area Network (LAN) which is typically used in corporate networks. LAN connects multiple computers and facilitates the sharing of resources such as files, printers, and other applications. A computer connected to a LAN can access and share data and programs with another computer connected to the same LAN. Users can also use the LAN to communicate with one another through e-mail and messaging sessions. Each device in a local area network is connected to a network switch. The network switch is connected to a router, which serves as the LAN's gateway.

Each branch of the financial institution has a LAN. Each computer in the branch is connected to a network switch or switches. The router is connected to the network switch. If a company has 100 branches, each branch will have 100 routers installed. All routers are interconnected to form a WAN. All routers are linked via the telephone network, leased lines, or satellites. They are referred to collectively as communication media. For example, the Internet is the greatest WAN currently in existence.

So, WAN is a computer network that encompasses a relatively large geographical area. WANs typically connect multiple local area networks. Users and computers in one location are able to connect with users and computers in other locations using a WAN. Many WANs are constructed for a single organization and are therefore private. Others, constructed by Internet Service Providers (ISP), connect the LAN of an organization to the Internet.

When it comes to creating LAN and WAN, hub/network switch and router are the key components to compose a proper network. For a financial institution, which deals with money and, as such, places a premium on security, additional security devices such as firewalls are required at the data Center, and each branch. Between the switch and router, a firewall is implemented. The firewall ensures that commands entering the data center originate from the designated branch.

A firewall is a component of a computer system or network that prevents unauthorized access while allowing authorized communications. It is a device that is programmed to allow or deny access to computer applications based on a set of rules and other criteria. Hardware, software, or a combination of both can be used to implement firewalls. Firewalls are commonly used to prevent unauthorized Internet users from accessing Internet-connected private networks.

Nonetheless, providing internet connectivity in the data center necessitates heightened security precautions. The internet access servers should be located in the Demilitarized Zone (DMZ). In computer security, a DMZ or demilitarized zone is a physical or logical subnetwork that contains and exposes an organization's external services to a larger, typically Internet-based, untrusted network. The purpose of a DMZ is to add an extra layer of security to a company's LAN; an external intruder has access only to the equipment in the DMZ and not to the rest of the network. [23]

3 Implementation of the Safeguards

In this part of the work, the author proceeds with the practical part of the paper. Firstly, the manual is created. Secondly, the process of implementing the safeguards is described.

3.1 Writing a Manual

It is crucial that all the described measures are applied to all system components, including individuals, processes, and technologies included in the cardholder data or cardholder data environment, as well as the storage, processing, and transmission of card data linked to that setting.

The guideline is divided into 6 targets and 12 measures which are intended to create a solid data security foundation to safeguard your company and sensitive card information. [15]

3.1.1 Target 1: Establish and Protect a Secure Network

Measure 1: Install and deploy firewalls to safeguard cardholder information.

Firewalls, as described in the theoretical part of the thesis, regulate the data transmission between a company's trusted internal networks and untrusted external networks, as well as the traffic in sensitive areas of internal networks. Firewalls are necessary to prevent unauthorized system entry. If other parts of the system provide the firewall's capabilities, those systems should also be included in the requirement's scope.

Measure 1.1: Develop and implement configuration standards for firewalls and routers

- The configuration standards for all firewalls and routers must be established, reviewed on a regular basis, and enforced.
- Changes to firewalls and routers are subject to review and approval.
- Between all Internet connections and demilitarized zones and the local network with network access and egress, a firewall should be utilized.

- Define the divisions, roles, and responsibilities used to manage network components.

- Documenting the security measures implemented to insecure protocols is required. For all permitted services, protocols, and ports, business justifications and approval documentation must be drafted.

- Every six months, the configuration rules of your router and firewall should be reviewed to identify and eliminate any outdated, irrelevant, or hazardous rules.

- Every six months, the configuration rules of your router and firewall should be reviewed to identify and eliminate any outdated, irrelevant, or potentially dangerous rules

Measure 1.2: Establish a firewall and router configuration that limits communications between untrusted networks and all cardholder data environment system components

- Between a trusted internal network and an untrusted external network, firewalls must be utilized.

- Limit incoming and outgoing network traffic to only the connections required for the cardholder's data medium and reject all other traffic.

- Guard and maintain the router's configuration files and synchronize them with all relevant devices.

- Install firewalls and set them to block traffic between all wireless networks and the cardholder's data environment. If this traffic is necessary for business purposes, it will only be permitted between the wireless medium and the cardholder's data medium.

Measure 1.3: Restrict global Internet access to any system component of the cardholder data storage medium

- Create a DMZ to restrict incoming traffic to components of the system that provide only publicly accessible authorized services, protocols, and ports.

- Restrict inbound Internet traffic to IP addresses that are located within the DMZ.
- Implement anti-spoofing countermeasures to the IP anti-counterfeit firewall in order to detect and prevent the entry of fake IP addresses into the network. For instance, internet traffic with a local IP address can be blocked.
- Block unauthorized Internet traffic from entering the cardholder data environment.
- Only allow connections to pre-established network connections.
- Locate system components that store cardholder data outside the demilitarized zone and other unreliable networks.
- Avoid disclosing private IP addresses and route data to unknown parties. Using techniques such as NAT or proxy servers, avoid identifying and viewing local network data over an external network.

Measure 1.4: Install mobile firewall software on every mobile device that has connections to the internet and is used to access the network outside of the network

- To access credit card information, it is necessary to configure a personal firewall on all portable computer equipment that connects to the internet outside the local network and to ensure that it is operational.
- Ensure that the user cannot alter the firewall rules.

Measure 1.5: Ensure that the security protocols and operational procedures for managing firewalls are documented, in usage, and well-known by everyone involved

- Related employees must have a thorough understanding of the organization's security policies and operational procedures in order to ensure the continuous and desired administration of firewall and router configurations.

Measure 2: Avoid using the vendor-supplied defaults for system usernames and passwords.

The default configuration settings and parameters for a variety of common applications and devices are well-known to attackers, and they can use these values with ease. Before any system is installed on the network, the preset settings and values provided by the manufacturer must be modified, and unimportant default accounts must be disabled or deleted. Without exception, this requirement pertains to all default passwords.

Measure 2.1: Before installing any system on a network, you should always alter the default settings and values provided by the manufacturer and eliminate or disable any unnecessary default accounts

- This rule applies to all devices, applications and systems within the scope of the manual.

- Modify the default values and settings for all wireless systems, including wireless encryption keys, passwords, and SNMP strings.

Measure 2.2: Develop configuration standards for all system components

- Ensure that the configuration standards handle all known vulnerabilities and are consistent with industry-accepted standards for strengthening the system.

- On the exact same server, functions requiring various levels of security should not be executed. Check the system configuration to ensure that a single server performs only one primary function. Web servers and database servers, for example, must be deployed and operated separately.

- Allow only the necessary functions, protocols, and services for the system to operate. Eliminate unnecessary system functions, protocols, and services. Implement additional security measures for functions, protocols, or services that can be considered dangerous but necessary for the operation of the system.

Measure 2.3: Encrypt all non-console access to devices using secure encryption

- Set up protocols such as SSH, VPN, or SSL/TLS for all administrative web-based and non-console access. In addition, ensure that no dangerous remote logon commands are used by examining the parameter and configuration files for non-console access.

Measure 2.4: Maintain an inventory of every component of the system

- To ensure compliance, the catalog of software and hardware components should be kept relevant. Some system components may be neglected if inventory is not maintained or updated, resulting in inadequate coverage definition.

Measure 2.5: To handle the manufacturer's default settings and other safety parameters, ensure that security policies and operational procedures are documented, in use, and understood by all affected parties

- Personnel must be aware of and knowledgeable about the information security policies and daily business procedures of their organization. To this purpose, the policy's implementation should be reviewed. Additionally, the documentation should be made available to all stakeholders.

Measure 2.6: Providers of shared hosting must safeguard the environment and cardholder data hosted by each organization

- This requirement applies to hosting service providers that provide hosting on one server and share the system with multiple clients. Compliance with these requirements is intended to protect cardholder data in shared environments by providing a secure environment for shared hosting service providers.

3.1.2 Target 2: Safeguard Cardholder Data

Measure 3: Secure saved cardholder information.

Account information storage should be limited, and policies, protocols, and mechanisms for data preservation and removal should be implemented. Never store information such as card chip or magnetic strip content, CVN (card verification number) or PIN (personal identification number). Whenever information must be held, it must be stored securely. Encryption, trimming, hiding, and hashing are the crucial components of cardholder data protection. Even if assailants bypass other security measures, they will be unable to read and use encrypted data without access to the proper encryption keys. Therefore, the cryptographic keys must be secured and restricted to the bare minimum number of holders who require access.

Measure 3.1: Establish and enforce policies, procedures, and processes for data retention and deletion of cardholder data (CHD) to minimize cardholder data storage

- Compliance with this requirement can be attained by establishing an official data retention policy. The policy will determine which types of data require protection and which should be deleted when they are no longer required.
- Reduce the quantity and duration of information keeping and retention to the time necessary to satisfy regulatory or business requirements.
- Create procedures to delete and eliminate data in a secure manner when they are no longer required.
- Every three months, examine cardholder data that exceeds the retention period specified in the rules and properly delete it if discovered.

Measure 3.2: Even if encrypted, do not keep private authentication information after authorization

- When receiving sensitive authentication data, delete all information irreversibly after authorization is complete.
- If there is a business justification for retaining sensitive data and the information is kept securely, service-providing organizations may store sensitive authentication data.
- In routine business operations, the magnetic stripe may contain information such as the cardholder's name, expiration date, and service code. To minimize risk, retain only the data necessary for the task.
- Do not retain the credit card's verification code or value after validation.

Measure 3.3: If the primary account number (PAN) must be displayed, it must be masked in order to be viewed

- The utmost number of digits that can be displayed is the primary account number's first six and last four digits. The first six and last four digits of the card number can only be viewed by personnel with legitimate business requirements.

Measure 3.4: Wherever the primary account number is stored, it should be made unreadable

- At all storage locations, the primary account number (PAN), including portable digital media, backup media, and archives, should be unreadable.

- The primary account number (PAN) can be stored after an operation, but it must be rendered unintelligible through encryption, truncation, or hashing.

- If the disk encryption method is employed, logical access should be managed independently of the local operating system's authentication and access control mechanisms. Additionally, encryption credentials should not be linked to user accounts.

Measure 3.5: Create and implement procedures to safeguard the keys used to secure cardholder data which is stored

- The safeguarding of cryptographic keys is crucial, as unauthorized access to the key allows the data to be decrypted and utilized for malicious purposes.

- The keys should be kept in the least accessible location, and only the fewest number of individuals should have access to them. Encryption keys for both keys and data should be stored separately.

- Service providers should produce a document explaining cryptographic procedures. The cryptographic process documentation should include information about the algorithms, protocols, and keys used to secure cardholder data, as well as the key's strength and expiration date.

Measure 3.6: All key management methods and encryption key procedures used to encrypt cardholder data should be documented and implemented

- Documents pertaining to key management should include key management components such as the generation of robust encryption keys, the secure distribution of cryptographic keys, and the safekeeping of encryption keys.

- For keys that have reached the end of their encryption lifetime, industry-standard encryption key modifications must be implemented.

- If the key's integrity is compromised or exposed, the key must be removed or replaced.

- It is necessary to prevent the unauthorized replacement of cryptographic keys, and cryptographic key administrators must formally acknowledge that they understand and embrace their responsibilities.

Measure 3.7: To protect stored cardholder data, security policies and operational procedures must be documented, implemented, and known to all affected parties

- To meet this requirement, personnel should be regularly informed of security policies and procedures for handling the secure storage of cardholder data.

Measure 4: Encrypt customer information transmitted over public networks.

To protect sensitive cardholder data during transmission over public networks prone to malicious attacks, it is essential to employ robust security protocols and robust cryptographic encryption. Public networks consist of wireless, GPRS, Internet, and satellite communications technologies. It is essential to implement industry-standard authentication and encryption procedures. In addition, security policies and procedures for encrypting cardholder data transmission must be documented and communicated to all relevant parties.

Measure 4.1: To protect sensitive cardholder data during transmission over open, public networks, it is necessary to implement robust security protocols and encryption techniques

- To ensure secure encryption, it is essential to only accept and employ trusted encrypted keys and certificates, as well as to support secure versions and configurations of the relevant protocols. Moreover, the encryption strength must be suitable for the selected encryption method.

- When transmitting cardholder data over wireless networks or connecting to an environment containing cardholder data, it is necessary to use an authentication mechanism and employ robust encryption methods.

Measure 4.2: It is crucial to never transmit Primary Account Number information via end-user messaging technologies without a password.

- A written policy should be enforced to prohibit the transmission of PAN information over end-user messaging platforms without encryption or protection.

Measure 4.3: To encrypt the transmission of cardholder data, it is necessary to document and implement security policies and operational procedures and to ensure that all relevant parties are aware of them

- To ensure the security of cardholder data transmitted over the network, stringent policies and procedures must be implemented. For the transmission of sensitive data, the use of certificates with robust encryption procedures, encrypted protocols, and a secure key will provide the necessary security.

- It is essential to communicate these policies and procedures to each individual and ensure that they are understood and followed by all parties.

3.1.3 Target 3: Implement a Vulnerability Management Program

Measure 5: To safeguard all systems, it is crucial to protect them against malware and regularly update anti-virus software.

Anti-virus applications that are capable of identifying and eliminating malware should be installed on systems that are frequently infected with malware to provide protection. Regular analysis of evolving software threats is required to determine if antivirus software is required for protection. It is essential to ensure that antivirus systems are active and efficient. In cases where permission is granted, antivirus systems may be disabled.

Measure 5.1: To mitigate the effects of malware, it is recommended to install anti-virus software on any vulnerable systems

- To protect against malware, it is advised to install anti-virus software on systems that are frequently infected, such as personal devices and servers.

- To protect the systems, it is essential to ensure that the anti-virus software can detect, and quarantine all known varieties of malware.

- To protect against malware threats that are constantly evolving, it is necessary to routinely check systems that are typically unaffected by malware.

Measure 5.2: To ensure the security of the systems, it is essential to validate the proper operation of all anti-virus mechanisms

- It is crucial to regularly update anti-virus software, as even effective anti-virus software that does not receive updated virus data cannot provide adequate protection.

Measure 5.3: Anti-virus software must be effective and incapable of being disabled by users to provide adequate protection against malware

- Anti-virus software must operate effectively and cannot be disabled by users unless authorized by the administrator for a limited time.

- It is only permissible for the administrator to temporarily disable the anti-virus software for technical reasons, and this action should be properly documented. During the period when the anti-virus protection is inactive, additional security measures may be required to maintain the system's security.

Measure 5.4: To protect systems from malware, it is essential to document and implement security policies and operational procedures that are known to all parties

Establishing and distributing anti-malware institutional policies and procedures is essential for ensuring that every employee is aware of the organization's security policies and operational procedures, and for maximizing network protection against malware.

Measure 6: Construct secure systems and applications.

To ensure that cardholder data security is not compromised, organizations should establish a method for identifying and prioritizing vulnerabilities based on risk level. Critical security updates must be implemented within one month of their release.

Whether developed internally or externally, software applications must be developed in a secure and safe manner. To accomplish this, industry standards and best practices must be adhered to, and information security considerations must be incorporated into all phases of software development.

Measure 6.1: To identify vulnerabilities, reputable external sources should be utilized, and newly discovered vulnerabilities should be ranked according to their risk level

- To ensure the security of the systems, it is necessary to implement a system of regular monitoring that maintains track of potential vulnerabilities. This can be accomplished by subscribing to newsgroups, mailing lists, RSS feeds, or reputable websites that provide updates on field developments.

- After identifying vulnerabilities, a risk evaluation system should be established based on industry best practices and the vulnerability's potential impact.

- Risk ranking should identify all environmental vulnerabilities deemed "high risk" and prompt action should be taken to mitigate them.

Measure 6.2: It is essential to implement valid security patches provided by the vendor for all system components and software to protect against known vulnerabilities. This should be done as soon as feasible following the release of patches to reduce the risk of exploitation by attackers

- Installing critical-level security updates within one month of their release is essential for ensuring the security of system components and software. The risk ranking method should be used to identify these crucial areas. For vulnerabilities of moderate severity, patches can be installed within two to three months.

Measure 6.3: Develop software applications with a concentration on security to protect them from potential threats and flaws

- Integrate industry best practices and standards for secure software development throughout the lifecycle of software development. This applies to both internally developed and externally developed software. Considerations for information security must be an integral component of the development process.

- Before deploying applications, accounts, user IDs, and passwords for development, test, and custom apps should be removed to prevent unauthorized access to sensitive data.

- To ensure the security of software development, it is essential to execute manual and automated source code reviews. These assessments should determine whether the code adheres to secure coding standards and guidelines. Before the code can be implemented in a production environment, any vulnerabilities discovered during the evaluation must be fixed and approved by a manager.

Measure 6.4: Establish a change control mechanism and observe the procedure for all system component modifications

- To ensure proper administration, it is essential to differentiate development/test environments from production environments and to implement access control measures to limit user access. Management of these environments should take into account the separation of duties.

- It is imperative to eliminate test data and accounts from system components prior to system deployment and to avoid using actual card data in test or development environments.

- To ensure that the system's security is not compromised, change control procedures should include an impact analysis, approval by authorized personnel, affirmation of the change, and functionality testing. In addition, there should be guidelines for the withdrawal of modifications.

Measure 6.5: Identify and correct common software development process vulnerabilities

- It is suggested that software developers receive training on secure code development on an annual basis in order to promote applications based on secure coding practices. In addition, it is essential to update training and procedures in accordance with the most recent industry standards for vulnerability management.

Measure 6.6: It is essential to maintain continuous monitoring of emerging threats and vulnerabilities for open web applications and to take the necessary precautions to protect them from known attacks

- Utilizing either manual or automated vulnerability detection tools, it is recommended to scan web applications at least once a year and after any changes.

- It is recommended to deploy an automated technical solution, such as a web application firewall, to identify and inhibit web-based attacks against web-enabled applications.

Measure 6.7: For the growth of secure systems and applications, it is essential to document security policies and operational procedures, to implement them, and to ensure that all relevant parties are aware of them

- It is essential to establish detailed processes and procedures for secure software development and to provide relevant personnel with training based on these documents in order to develop secure software. In addition, it is recommended to conduct an annual review to ensure that all pertinent documentation is accurate and up to date.

3.1.4 Target 4: Implement Robust Access Control Measures

Measure 7: Limit access to cardholder data in accordance with business requirements.

Unauthorized access to a system by misusing authorized accounts and user privileges is one of the most prevalent and difficult to detect types of attacks. Therefore, it is crucial to establish documented procedures to restrict access to sensitive data by limiting access permissions. Access control mechanisms should adhere to the principle of default denying all access. Access should be granted based on the "need to know" principle and the defined job responsibilities of authorized personnel.

Measure 7.1: Limit access to system components and cardholder data to only those who need it to perform their job duties

- Determine the access requirements for each role and specify the system components and data sources to which each role must have access in order to fulfill their job responsibilities.

- Establish the essential privilege levels for accessing resources. Restrict access to privileged user IDs to the bare minimum of privileges required to perform job duties.

Measure 7.2: Develop secure access control systems

- It is essential to establish an access control system for system components that operate under the "need to know" principle and are configured to "deny all" unless specifically authorized.

- All system components should be subject to access control. The granting of privileges to employees should be based on their employment classification and function.

Measure 7.3: Ensure that security policies and operational procedures that restrict cardholder data access are documented, implemented, and communicated to all relevant parties

- It is essential to document, implement, and communicate to all relevant parties all security policies and procedures pertaining to restricted access to cardholder data.

Measure 8: Establish identification and authentication protocols for accessing system components.

Individual user identification not only restricts network access to authorized personnel, but also permits auditing and review of any unauthorized activity. Therefore, it is essential to implement documented policies and procedures to monitor user identity across all system components, especially for administrative accounts. It is essential to assign unique identifiers to each user and administer identity identification in accordance with strict guidelines. Implement multi-factor authentication (MFA) mechanisms and use controlled user authentication management for remote access connections.

Measure 8.1: Set up and follow policies and procedures for maintaining accurate user identities across all system components for both users and administrators

- Ensure that each user has a unique identity before granting access to system components or cardholder information.

- Manage the generation, removal, and modification of user IDs, credentials, and other forms of identification.

- Accounts that are inactive for any reason should have their access revoked promptly. Within 90 days, inactive user accounts should be disabled or deleted.

- Accounts used by third parties for remote access, support, or maintenance of system components should only be enabled for the required time and disabled when not in use to increase security. It is essential to monitor these accounts while they are in use to identify any unauthorized access or suspicious activity.

- After six failed login attempts, the user ID is locked to prevent unauthorized access. Set the exclusion duration to a minimum of 30 minutes or enable an administrator account.

Measure 8.2: Implement effective user authentication management for both users and administrators across all system components

- Implement multifactor authentication methods that utilize something the user knows, such as a password, something the user possesses, such as a smart card, and at least one method that verifies something the user is, such as biometrics, to ensure proper authentication of user identities.

- All authentication information should be protected through strong encryption methods during transmission and storage across all system components, ensuring that the data is unreadable.

- Before making any changes to authentication information, it is important to verify the user's identity to ensure that only authorized individuals can access the system.

- Generate unique, one-time passwords for each user and require that they be changed immediately after their first use.

Measure 8.3: Implement multi-factor authentication for all individual administrative access and remote access to the CDE to ensure secure access

- To achieve multi-factor authentication, at least two of the three authentication methods must be used for authentication purposes.

- Establish a multi-factor authentication system for any external network entry, including remote access by users and administrators, as well as third-party connections for assistance or maintenance purposes.

Measure 8.4: Create and disseminate documentation outlining authentication policies and procedures to all users

- Advise and enforce users to use strong passwords.

- The protocols should encompass the selection of potent authentication credentials, safeguarding of users' authentication information, directives against reusing previous passwords, and guidelines for changing passwords in case of exposure.

Measure 8.5: Avoid the use of group, shared, or public IDs, passwords, or any other form of authentication methods

- In the event of a security breach, it becomes unfeasible to trace the accountable individual when multiple users utilize the same passwords or user account. To avoid this scenario, each user must have distinct credentials and passwords.

- Deactivate or eliminate public user IDs. Refrain from sharing user IDs for system management and other essential functions. Avoid using shared or public user IDs for the administration of any system components.

Measure 8.6: In case of other authentication mechanisms being utilized, their allocation should be as follows

- Examples of other authentication mechanisms may comprise physical or logical security tokens, smart cards, or certificates.

- The allocation of authentication mechanisms should be to an exclusive account and not shared. Adequate physical or logical controls must be established to guarantee that solely the designated account for gaining access can employ this mechanism.

Measure 8.7: Restriction of access to databases containing cardholder data

- Review the database and application configuration settings to verify that authentication of each user occurs before granting access.

- All user activities such as accessing databases, executing queries, and performing actions should be carried out through programs. Only database administrators must have direct access or query privileges to the databases.

Measure 8.8: Document the security policies and operational procedures for authentication and identification, implement them, and make them known to all relevant stakeholders

- It is imperative to document security policies and operational procedures related to authentication and identification processes, put them into practice, and ensure that all relevant parties are aware of them. Regularly inform employees about these policies and procedures.

Measure 9: Limit physical entry to cardholder data.

Data loss can occur not only through electronic breaches but also due to insufficient controls over physical access to systems. It is crucial to enforce appropriate measures to monitor and restrict physical entry to systems. Follow protocols to differentiate between employees and visitors and restrict physical access to sensitive areas accordingly.

Measure 9.1: Implement and employ suitable facility access controls to restrict and oversee physical entry to systems within the cardholder data environment

- Physical security measures should be implemented in data centers, server rooms and all other facilities where confidential data is stored, thus preventing unauthorized access.

- Use video cameras or access control mechanisms to oversee physical entry into sensitive areas.

- Apply physical or logical controls to public network connectors to restrict access. Restriction of physical access to gateways, wireless access points, handsets, network equipment, and telephone connections.

Measure 9.2: Create protocols to differentiate between employees and visitors with ease

- Check the authorization of each visitor entering the premises and ensure that the means to differentiate visitors from employees are readily accessible.

Measure 9.3: Restrict physical entry to sensitive areas for employees in the following manne

- Grant access to sensitive areas solely to employees with business requirements and authorized to visit such areas.
- Immediately revoke access upon termination and ensure that all physical entry mechanisms such as keys or access cards issued for entry are returned.

Measure 9.4: Adhere to protocols for identifying and authorizing visitors

- Implement strong procedures to verify whether visitors are authorized to enter sensitive areas of the facility. These measures and controls can help minimize unauthorized access to the cardholder data environment by malicious individuals.
- Record and document the name of the visitor, the represented company, and the person who authorized physical access in a logbook. Keep visitor logs and records for a minimum of three months, unless required by law to keep them for a more extended period.

Measure 9.5: Secure all media that contains physically sensitive data

- Securely store backups of sensitive data, preferably in an alternate or secondary data center. Review the security of the location where sensitive data is stored annually.

Measure 9.6: Implement strict limits on the distribution and transmission of all media, both internally and externally

- Cardholder data should not be distributed in electronic or paper format unless it is deemed necessary.

- To ensure the security of sensitive data, it is necessary to classify all media devices in order to determine which ones contain such data. In addition, records should be kept for all media sent outside the organization, and a dependable courier should be used to dispatch and track the media.

Measure 9.7: Ensure strict controls are in place for the storage and access of media

- It's important to establish a documented media storage policy and regularly maintain an inventory.

Measure 9.8: It is important to dispose of media once it is no longer necessary for business or legal purposes

- To prevent the regeneration of information, printed materials should be destroyed by crushing, burning, or pulping in a manner that ensures their irreversibility. For this purpose, safe storage containers or warehouses should be utilized to carry out the destruction process.

Measure 9.9: It's crucial to safeguard payment card data receiving devices that involve physical interaction, to prevent tampering and substitution

- All card-reading devices used at the point of sale should be regularly examined for any physical damage or suspicious activity.

- Only authorized individuals should be permitted to conduct examinations if anything unusual happens to the device.

Measure 9.10: To restrict physical access to cardholder data, it's important to have well-documented security policies and operational procedures in place

- It is imperative to formally document all security policies and operational procedures aimed at restricting physical access to cardholder data. These policies and procedures should be implemented within the organization and communicated directly or indirectly to all parties involved in the storage, processing, and transmission of cardholder data.

3.1.5 Target 5: Conduct Regular Monitoring and Testing of Networks

Measure 10: It is essential to trace and monitor all network resources and cardholder data access.

Log systems are essential for preventing, detecting, and mitigating data security threats. When system user activities are not recorded, potential violations cannot be identified. Therefore, it is necessary to implement secure and controlled means that link all system component access to specific individuals and record their actions. It is advised to keep all log files for at least one year. A routine examination of these records and security events should be conducted to detect any abnormal or suspicious behavior.

Measure 10.1: A process should be established that associate's access to system components with individual users

- Maintaining a log of all system component access is crucial because it facilitates the identification of the user responsible in the event of an unauthorized network modification.

- The network activities of every user, notably administrators, should be monitored. It is recommended to generate regular reports listing users with access to system objects.

Measure 10.2: Establish a mechanism for the automatic evaluation of logs to recreate events

- Manually tracking access to system components can result in the omission of crucial events, particularly when a large number of components are involved. Consequently, it is advised to automate access monitoring, control, and reconstruction processes.

Measure 10.3: At a minimum, the following information should be recorded for all system component events

This facilitates the identification of any data intrusion, including who, when, where, what, and how it occurred:

- User ID,

- type of the event,
- date and time,
- success or fail indicator,
- the origin of the event,
- the identity or name of the impacted data, asset, or system component.

Measure 10.4: Utilize time synchronization technology to synchronize all time- and clock-sensitive system components

- Time synchronization is essential for ensuring that time is accurate and consistent across critical systems. To ensure accuracy and dependability, time data should be maintained, and time parameters should be obtained from industry-recognized time sources.

Measure 10.5: Keep the records in an unchangeable format

- Access to log files should be limited to those with a legitimate business need, and log files should be protected from unauthorized modifications.
- Log files should be transmitted to and stored on a central log server that is difficult to modify or access without proper authorization.
- Utilize file integrity monitoring or change-detection software to guarantee that extant log data cannot be altered without triggering alerts or warnings.

Measure 10.6: It is essential to examine logs and security events for all system components on a regular basis in order to identify any anomalies or suspicious activity

- All system components that store, process, transmit, or indirectly affect cardholder data should have their logs reviewed. To satisfy this requirement, automated instruments for log collection, separation, inspection, and alerting can be utilized.

Measure 10.7: Keep the log history for a minimum of one year and have at least three months of data available for analysis

- It is recommended to keep audit logs for at least one year and to make sure that at least three months' worth of log records are readily accessible.

Measure 10.8: Establish and enforce procedures to promptly detect and report any failures in critical security control systems for service providers

- This requirement only applies to service providers, who must establish and adhere to procedures for timely detection and reporting of critical security control system failures. Firewalls, intrusion detection/prevention systems (IDS/IPS), file integrity monitoring (FIM) software, antivirus software, physical and logical access controls, audit logging mechanisms, and segmentation controls, if used, are examples of critical security control systems.

Measure 10.9: To monitor all access to network resources and cardholder data, it is essential to document and implement security policies and operational procedures that are known to all parties involved in the storage, processing, and transmission of cardholder data

- It is essential to inform employees of all security policies and procedures and to monitor their implementation.

Measure 11: Regular monitoring of security processes and systems is required.

Consistent testing of system components, systems, and applications is necessary to identify and address security vulnerabilities in a timely manner, given the constant exploitation of newly discovered vulnerabilities. At least once a year, or after any significant change to the network, qualified personnel should conduct internal and external vulnerability scans, and intrusion detection/prevention systems should be utilized to identify or prevent unauthorized network activity. In addition, it is crucial to monitor and prevent unauthorized operations on essential file integrity software and files.

Measure 11.1: Quarterly tests should be conducted to detect the presence of wireless access points and identify both authorized and unauthorized access points

- It is necessary to conduct regular wireless network tests and related procedures to detect and identify all unauthorized wireless access points on a quarterly basis. If an inventory of authorized wireless access points is maintained and unauthorized ones are identified, incident response procedures should be applied to disable them.

Measure 11.2: It is recommended to perform internal and external network vulnerability assessments every three months and after any significant network changes

- These assessments utilize automated scanning techniques to test all internal and external network systems for potential vulnerabilities.

- Combining multiple scan reports can provide evidence that all systems have been scanned on a quarterly basis and that any vulnerabilities identified have been addressed. In certain circumstances, additional documentation may be required to corroborate that any outstanding vulnerabilities are being actively addressed.

Measure 11.3: It is essential to implement a structured methodology for conducting penetration testing

- It is necessary to conduct internal and external network penetration tests annually and after significant infrastructure or application changes, and to conduct a second test to ensure that any vulnerabilities discovered during the first test have been addressed.

Measure 11.4: To identify or prevent any unauthorized network access, it is needed to employ intrusion detection or intrusion prevention techniques

- It is suggested that both network-based and host-based IDS/IPS be used to monitor network traffic within the cardholder data environment in order to prevent data breaches. These systems can detect and prevent network intrusion attempts.

- It is essential to monitor all traffic around critical points in the cardholder data environment and alert staff of any suspicious activity. Regularly update the configurations and signatures of all intrusion detection and prevention software or devices.

Measure 11.5: Establish a mechanism for detecting unauthorized modifications to critical system files, configuration files, and content files

- These tools can detect file system changes and notify management of any unauthorized modifications.
- Configure change detection or file integrity monitoring tools to perform weekly comparisons of critical files as a bare minimum.
- When a change detection or file integrity monitoring instrument generates an alert indicating an unauthorized change, a well-defined process must be implemented to respond to the alert.

Measure 11.6: Ensure that security monitoring and testing policies and operational procedures are properly documented, implemented, and communicated to all parties

- To maintain compliance, it is essential to regularly review all security policies and procedures related to this requirement, implement them consistently across the organization, and communicate them in a standardized manner to all relevant parties.

3.1.6 Target 6: Maintaining the Information Security Policy on a Continuous Basis

Measure 12: Create a policy for information security that applies to all personnel in the organization.

It is essential for organizations to establish and publish a security policy that is reviewed and updated annually to account for the changing risk environment. In addition, a process for risk assessment should be implemented to identify potential hazards and vulnerabilities. Clearly defined usage policies for critical technologies and security responsibilities for all personnel must be developed. A formal information security awareness program should also be implemented to bolster a security culture.

Measure 12.1: A policy for information security should be developed and made accessible to the public

- It is vital to create a comprehensive policy that complies with applicable regulations and addresses business needs. In addition, an organization should implement a policy that addresses all other corporate issues, and it should be reviewed and updated at least once a year or whenever the business process changes.

Measure 12.2: Create and put in place a method for assessing potential risks

- Establishing and executing a risk assessment process is a crucial aspect of effective risk management. It involves identifying critical assets, potential threats, and vulnerabilities, and reviewing the process at least once a year or when there are significant changes in the environment.

Measure 12.3: Establish acceptable usage policies for critical technologies and to explicitly specify their proper application

- Establishing formal policies governing the use of crucial devices and technologies is essential. These policies should either prohibit the use of related technologies by employees or outline their appropriate application. These technologies consist of remote access and wireless technologies, laptops, tablets, portable electronic devices, e-mail, and Internet use.

Measure 12.4: It is essential to make sure that security policies and procedures clearly outline the information security responsibilities of every employee

- The effectiveness of an information security policy is determined by its ability to precisely define employee responsibilities and communicate policy requirements. Consequently, it is essential that security policies and procedures clearly define the information security responsibilities of every employee.

Measure 12.5: Designate an individual or a group with information security management responsibilities

- Through an appropriate policy, it is essential to ensure that each individual or team is aware of their information security management responsibilities.

- These duties should include creating, documenting, and publishing security policies and procedures, monitoring and forwarding safety alerts to the appropriate personnel, establishing and publishing security incident response procedures, managing user accounts, and controlling access to sensitive data.

Measure 12.6: Establish a structured information security awareness program to educate all personnel on the significance of safeguarding cardholder data

- It is advised that employees get training in information security awareness upon hire and annually afterward.

- Annually, employees are required to confirm that they have read and comprehended the security policy and procedures.

Measure 12.7: To reduce the possibility of a local attack, pre-employment background checks should be conducted on candidates

- Hence, it is vital to conduct a thorough background check to eliminate the likelihood of recruiting an individual with a criminal record. Examples of such checks include verifying previous employment history, criminal records, credit history, and references.

Measure 12.8: Develop and execute policies and procedures to govern service providers with access to or influence over the security of cardholder data

- Formal policies and procedures should be created for service providers who have access to cardholder information, and these documents should be disseminated to relevant stakeholders.

Measure 12.9: Service providers are obligated to inform their clients in writing that they bear the responsibility of securing the cardholder data they store, process, or transmit on behalf of said clients

- The service provider must agree to a written contract in which the client commits to protecting cardholder data by all means possible and adhering to all applicable regulations.

Measure 12.10: Develop and implement an incident response plan

- Review and test the incident response plan on a regular basis, placing special emphasis on designating personnel to respond 24/7 and training personnel with breach response responsibilities.

- Incorporate alerts from security monitoring systems such as intrusion detection, intrusion prevention, firewalls, and file integrity monitoring systems to respond to security incidents in a timely manner.

Measure 12.11: The personnel of service providers should be evaluated quarterly to ensure compliance with security policies and operational procedures

- The review process for compliance with security policies and operational procedures should include daily log evaluations, analysis and review of firewall rule sets, application of configuration standards to new systems, response to security alerts, and change management processes.

- Additionally, service providers must maintain documentation of the quarterly review procedure and its results.

3.2 Implementation of the Safeguards in the Company's Infrastructure

Implementing safeguards within a company's infrastructure is essential for guaranteeing the security and protection of sensitive data and assets. Technical controls, policies and procedures, and physical security measures are all types of safeguards.

Before starting to perform actual safeguarding activities, the security framework was established. In this framework, the infrastructure was divided into 16 domains:

1. Asset Management,

2. Endpoint Security,

3. Server Security,

4. Access Control,

5. Data Privacy and Security,

6. OT Security,

7. Mobile Security,
8. Network Security,
9. Application Security,
10. HR Security,
11. Technical Vulnerability Management,
12. Threat Monitoring and Detection,
13. DR and IT Service Continuity,
14. Incident Response and Breach Management,
15. Security Governance Structure,
16. Risk and Compliance.

After organizing all the initial points, assigning a domain lead to each domain was a crucial step in tracking the progress and monitoring all activities being performed. The author of this thesis was assigned with the responsibility of overseeing two specific domains, including endpoint and mobile security. However, due to the nature of the project, the author was also involved in other domains such as server and OT security. The author's involvement in multiple domains allowed for a broader understanding of the project and facilitated a more comprehensive approach to addressing potential issues. By working across different domains, the author was able to implement more effective security measures to protect the entire system. This multi-domain involvement was critical in ensuring the project's success and achieving the desired outcomes.

An audit system was established to monitor the progress of the security project. This system incorporates various elements such as indicators, target and actual percentage, ranking and a score system. By using this audit system, the project team can track the project's performance against established benchmarks and identify areas for improvement. The audit system provides valuable insights into the project's overall progress and helps ensure that the project is meeting its objectives in a timely and efficient manner.

With approximately 10,000 endpoint devices, including laptops, workstations, and production servers, it was necessary to establish priorities for the security project. As a result, endpoint security was identified as one of the top priority domains. This domain encompassed five indicators, including:

1. Exceptions from Standard Endpoint Security Solution — The percentage of the exceptions where computer system is connected to the network but cannot have EDR agent installed.

2. EDR Agent Update Compliance — The percentage of systems with EDR agent (N-2) updates.

3. Threat Detection Response SLA Compliance — The time frame of how fast it is possible to respond to the threat after detection.

4. Threat Detection Closure SLA Compliance — The time frame of how long it takes to triage and address the threat detection.

5. Software Firewall Deployment Compliance — The percentage of endpoints which has software firewall implemented.

To effectively address the first, second, and fifth indicators, certain measures were essential, which involved incorporating a new tool into the organization's infrastructure — CroudStrike. This required adapting the tool to the company's requirements and enrolling it into the system to ensure its smooth integration. By implementing these necessary actions, the company can effectively work with the identified indicators and achieve its desired goals.

Therefore, the deployment of this agent to Windows and Linux machines was made centrally via domain controllers across the company. With the new tool, proper configuration of firewall rules is crucial for preventing any production delays that may negatively impact the main business process. A small error in configuration can lead to significant consequences, hence it is essential to ensure that the rules are set up correctly. To maintain the effectiveness of the firewall rules, regular testing and improvement by both central units and local teams is imperative. Moreover, establishing consistent communication between these teams is essential to minimize the risk of errors and ensure optimal performance.

Despite being outsourced to another company with access to our CroudStrike system, the third and fourth indicators are currently in the process of being migrated to our central unit. In accordance with this transition, all relevant policies and procedures have been thoroughly documented and communicated to all relevant parties involved.

To conclude, the work done with endpoint security domain contributed to the first target of the manual — Establish and Protect a Secure Network. These are the measures that have been done:

- Develop and implement configuration standards for firewalls.
- Establish a firewall and router configuration that limits communications between untrusted networks.
- Ensure that the security protocols and operational procedures for managing firewalls are documented, in usage, and well-known by everyone involved.
- Maintain an inventory of every component of the system.
- Providers of shared hosting must safeguard the environment by each organization.

Although mobile security was not announced as a top priority domain, the author of this thesis has undertaken some preparatory efforts in this regard. This involved establishing communication with Mobile Device Management (MDM) service providers and securing trial licenses. The next step is to conduct tests to ensure a seamless integration of the proposed solution into the company's infrastructure.

After a thorough examination, two potential approaches were identified to incorporate mobile devices into the network. The first approach entails maintaining complete control over the devices, whereas the second approach involves implementing a Bring Your Own Device (BYOD) policy. While both options are feasible, a final decision has not been reached. As a result, the mobile security project is currently in its preliminary stage.

4 Analysis of the Experience

The practical component of the thesis comprises two parts. The initial segment aimed to generate a manual detailing the process of creating and maintaining a secure infrastructure. This output encompasses six distinct objectives and several measures outlining how to proceed and safeguard the environment.

The first objective aimed to construct and secure a network within an organization. The primary safeguard mechanism described in the first measure was the firewall. The author provided possible scenarios on how to establish a proper way of utilizing a firewall to secure the network and infrastructure.

After creating and analysing the measures from the first target, the author believes that safeguarding computer systems from unauthorized access via untrusted networks is crucial, irrespective of the source. Even seemingly insignificant paths may offer unprotected access to vital systems. Firewalls act as a barrier between trusted and untrusted networks, making them a vital security mechanism. They limit access to authorized users and filter out malicious traffic, thereby establishing secure network perimeters and reducing the risk of cyberattacks.

The second target of the manual was to safeguard cardholder data. Based on the authors manual, it is possible to say that the utilization of protection techniques such as encryption, truncation, masking, and hashing are fundamental constituents of safeguarding cardholder data. In the event that an unauthorized individual manages to bypass existing security measures and access encrypted data, said data remains illegible and impracticable to said individual, provided that the appropriate cryptographic keys are absent. It is advisable to examine other efficacious means of securing stored data as a means of mitigating potential risks. A noteworthy example of such methods is to abstain from storing cardholder data unless it is necessary.

The third objective necessitates the implementation of a vulnerability management program to maintain network compliance with regulatory standards. In essence, the prescribed measures entail managing anti-virus software and malware protection, in addition to prioritizing vulnerabilities based on their respective risk levels. After analysing security measurements from the third target, it is imperative that anti-virus software be installed on all systems susceptible to malware, to protect against contemporary and future threats from malicious software. Furthermore, all systems must receive all necessary software updates and patches to forestall any malicious exploitation or compromise of cardholder data.

Target number 4 emphasizes the importance of implementing robust access control measures. These measures entail restricting access to critical data solely to authorized personnel and having systems and processes in place to limit access based on the principle of least privilege and commensurate with job responsibilities. It is imperative to establish identification and authentication protocols and to restrict physical access as well. By implementing the measures outlined above, it is possible to increase overall security.

The next target entails the monitoring and testing of all requisite networks within the organization. The author believes that the implementation of a logging system is of utmost importance in order to prevent, identify, and mitigate security threats. In addition, regular monitoring of all network resource access and subsequent testing is imperative.

With regards to the final objective, the author proposes that a robust security policy establishes the overall security culture of the organization and communicates to employees what is required of them. Thus, all staff members must be aware of the confidentiality of data and their obligation to safeguard it.

The primary aim of the thesis was to create a manual detailing the process of establishing a secure infrastructure and implementing appropriate security controls within a company's environment. The author acknowledges that while this goal was achieved, it was not without its limitations. A lack of experience in determining critical details to include presented a significant challenge when developing the guide. To strike a balance, the author focused on providing brief and relevant information regarding this vast subject matter. Nonetheless, there is still room for improvement in this regard.

However, the second part of the goal can be regarded as a success. The author implemented the recommended security measures, although only with a focus on securing the network and endpoints of the company. All the measures that were implemented made a contribution to the overall cybersecurity of the organization, as evidenced by the fact that they were able to meet the target deadline of securing 99% of all endpoints.

5 Summary

The thesis aimed to produce a manual on establishing a secure start-up infrastructure and implementing security controls in the company's environment. The author faced a lack of experience in identifying all important aspects to describe in the manual but tried to keep all the measurements relevant. The implemented security measures contributed to the overall cybersecurity of the organization, achieving the main target of 99% of all endpoints. The research highlights what constitutes a start-up, the role of PCI DSS compliance in ensuring security, and the various security measures employed to strengthen infrastructure. As well as the importance of maintaining a log system, monitoring, and testing networks, and enforcing a strong security policy. The conclusion emphasizes the need for continuous improvement in cybersecurity and the potential for further research in the field. Moreover, the author is of the opinion that this manual will not only be beneficial for start-ups, but it is also relevant and applicable to medium-sized organizations.

References

[1] FasterCapital, “Why startups are more prone to risk and what you can do about it,” FasterCapital, 5 January 2023. [Online]. Available: https://fastercapital.com/content/Why-startups-are-more-prone-to-risk---------and-what-you-can-do-about-it.html. [Accessed 1 April 2023].

[2] threatcop, “An Increase in Cybercrime Continues to Haunt Cyber World,” threatcop, [Online]. Available: https://threatcop.com/blog/increase-in-cybercrime/. [Accessed 1 April 2023].

[3] Oxford Learner's Dictionaries, “Definition of start-up,” Oxford Learner's Dictionaries, [Online]. Available: https://www.oxfordlearnersdictionaries.com/definition/english/start-up_1?q=start-up. [Accessed 1 March 2023].

[4] FasterCapital, “The characteristics of a startup company,” FasterCapital, 16 March 2023. [Online]. Available: https://fastercapital.com/content/The-characteristics-of-a-startup-company.html#The-challenges-faced-by-startups. [Accessed 2 April 2023].

[5] Stripe, “Introduction to collecting online payments,” Stripe, [Online]. Available: https://stripe.com/en-ee/guides/introduction-to-online-payments. [Accessed 4 April 2023].

[6] B. Mongold, “Pros and Cons of Outsourcing AP Payments,” MEKORMA, 15 October 2021. [Online]. Available: https://mekorma.com/resources/blog/details/mekorma-blog/2022/05/19/pros-and-cons-of-outsourcing-ap-payments#. [Accessed 5 April 2023].

[7] GoCardless, “How to Create a Payment Gateway,” GoCardless, March 2023. [Online]. Available: https://gocardless.com/guides/posts/how-to-create-a-payment-gateway/. [Accessed 5 April 2023].

[8] D. Partida, “Social engineering cyberattacks and how they’re impacting businesses,” Endeavor Business Media, 22 December 2020. [Online]. Available: https://www.securityinfowatch.com/cybersecurity/article/21203580/social-engineering-cyberattacks-and-how-theyre-impacting-businesses. [Accessed 8 April 2023].

[9] European Payments Council AISBL, “Payment Threats and Fraud Trends Report,” European Payments Council AISBL, Brussels, 2022.

[10] B. Jovanovic, “A Not-So-Common Cold: Malware Statistics in 2023,” DataProt, 7 April 2023. [Online]. Available: https://dataprot.net/statistics/malware-statistics/. [Accessed 22 April 2023].

[11] Cloudfare, “DDoS Threat Landscape Report,” Cloudfare, 2022.

[12] J. Kagan, “PCI Compliance: Definition, 12 Requirements, Pros & Cons,” Investopedia, 5 September 2022. [Online]. Available: https://www.investopedia.com/terms/p/pci-compliance.asp. [Accessed 18 April 2023].

[13] IBM, “What is IT Infrastructure?,” IBM, [Online]. Available: https://www.ibm.com/topics/infrastructure. [Accessed 18 Aprill 2023].

[14] R. Jermakov, “What Is PCI DSS Compliance and Why Is it So Important to Us?,” Wallester, 16 September 2022. [Online]. Available: https://wallester.com/blog/business-insights/what-is-pci-dss-compliance?gclid=CjwKCAjw_YShBhAiEiwAMomsEFuVy4AXE1yhAhXN_NT6JfzIY5WtNunWux3U4v6S5-XAyLkGtKz3EBoCxjQQAvD_BwE. [Accessed 18 April 2023].

[15] PCI Security Standards Council, “PCI_DSS_v3-2-1.pdf,” May 2018. [Online]. Available: https://www.commerce.uwo.ca/pdf/PCI_DSS_v3-2-1.pdf. [Accessed 18 April 2023].

[16] B. Jovanovski, “What Is Data Encryption? Definition, Meaning, & More,” PaymentCloud, 4 April 2023. [Online]. Available: https://paymentcloudinc.com/blog/data-encryption/. [Accessed 19 April 2023].

[17] A Smart Card Alliance Payments Council, “EMV-Tokenization-Encryption-WP-FINAL.pdf,” A Smart Card Alliance, October 2014. [Online]. Available: https://www.emv-connection.com/downloads/2014/10/EMV-Tokenization-Encryption-WP-FINAL.pdf. [Accessed 20 April 2023].

[18] J. Chen, “Address Verification System,” Investopedia, 1 March 2023. [Online]. Available: https://www.investopedia.com/terms/a/address-verification-system.asp. [Accessed 20 April 2023].

[19] J. Fernando, “Validation Code Defenition,” Investopedia, 15 March 2021. [Online]. Available: https://www.investopedia.com/terms/v/validation-code.asp. [Accessed 20 April 2023].

[20] EMVCo, “EMV 3-D Secure,” EMVCo, [Online]. Available: https://www.emvco.com/emv-technologies/3-d-secure/. [Accessed 20 April 2023].

[21] stripe, “Card authentication and 3D Secure,” stripe, [Online]. Available: https://stripe.com/docs/payments/3d-secure. [Accessed 20 April 2023].

[22] M. Rouse, “What is IT Infrastructure?,” techopedia, 25 April 2022. [Online]. Available: https://www.techopedia.com/definition/29199/it-infrastructure#site-header. [Accessed 20 April 2023].

[23] A. K. M. S. a. N. T. Prianka, “IT in Banking,” Institute of Bankers, 2013. [Online]. Available: http://it-in-banking.blogspot.com/2013/10/networking-and-computer-hardware-for.html. [Accessed 20 April 2023].

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Dennis Bykov

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Payment Security Aspects and Implementation of Necessary Safeguards in the Start-Up Infrastructure”, supervised by Toomas Lepikult
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

24.04.2023

[1] The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.