Bachelor's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Sindre Hiis-Hauge
Steinar Mjøs Myhre
Jonas Brumoen Nessø
Jørgen Lillehagen Myrvold

Kryptovirus - Ahus

Bachelor's thesis in Digital Infrastructure and Cyber Security
Supervisor: Filip Holik
May 2023

NTNU
Norwegian University of
Science and Technology

Sindre Hiis-Hauge
Steinar Mjøs Myhre
Jonas Brumoen Nessø
Jørgen Lillehagen Myrvold

Kryptovirus - Ahus

Bachelor's thesis in Digital Infrastructure and Cyber Security
Supervisor: Filip Holik
May 2023

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

NTNU
Kunnskap for en bedre verden

FACULTY OF INFORMATION TECHNOLOGY AND ELECTRICAL ENGINEERING

DCSG2900 - BACHELOR THESIS BACHELOR OF SCIENCE IN DIGITAL INFRASTRUCTURE AND CYBER SECURITY

Kryptovirus – Ahus

Authors:
Sindre Hiis-Hauge
Steinar Mjøs Myhre
Jonas Brumoen Nessø
Jørgen Lillehagen Myrvold

Supervisor:
Filip Holik

21-05-2023

Abstract

Title:	Kryptovirus – Ahus
Date:	21.05.2023
Authors:	Sindre Hiis-Hauge Steinar Mjøs Myhre Jonas Brumoen Nessø Jørgen Lillehagen Myrvold
Supervisor:	Filip Holik
Employer:	Akershus universitetssykehus
Contact person:	Kåre-Magne Stennes
Key words:	Ransomware, attack tree, cyber security
Pages:	79
Attachments:	6
Availability:	Open

Abstract: In modern times, technology is becoming more advanced and sophisticated. This hectic process of development leads to an increased risk of being attacked by threat actors on the web. The most prevalent threats of this kind are crypto viruses, as these have a vast amount of attack vectors available, and are capable of causing massive damage to their victims. Thus, Akershus universitetssykehus (Ahus) has requested a review of the consequences of crypto virus attacks in the healthcare sector, due to numerous healthcare companies being attacked in Europe and the rest of the world. Ahus has also requested that this thesis includes an attack tree covering information about previous attacks performed in recent years, possible other attack vectors that are identified, and how a crypto virus attack can affect a patient's quality-adjusted life years (QALYs).

Sammendrag

Tittel:	Kryptovirus – Ahus
Dato:	21.05.2023
Forfattere:	Sindre Hiis-Hauge Steinar Mjøs Myhre Jonas Brumoen Nessø Jørgen Lillehagen Myrvold
Veileder:	Filip Holik
Arbeidsgiver:	Ahus
Kontaktperson:	Kåre Magne Stennes
Nøkkelord:	Løsepengevirus, attack tree, cybersikkerhet
Sider:	79
Vedlegg:	6
Tilgjengelighet:	Åpen

Sammendrag: I moderne tider blir teknologien stadig mer avansert og sofistikert. Denne hektiske utviklingsprosessen fører til økt risiko for å bli angrepet av ondsinnede aktører på nettet. De mest utbredte truslene av denne typen er kryptovirus, etter som at disse har et bredt antall angrepsvektorer tilgjengelig og er i stand til å forårsake betydelig skade på sine ofre. Derfor har Akershus universitetssykehus (Ahus) bedt om en gjennomgang av konsekvensene av kryptovirusangrep i helsesektoren, på grunn av mange helseforetak er blitt angrepet i Europa og resten av verden. Ahus har også bedt om at denne oppgaven inkluderer et attack tree diagram som dekker informasjon om tidligere angrep utført de siste årene, andre mulige angrepsvektorer som er identifisert, og hvordan et kryptovirusangrep kan påvirke pasientens kvalitetsjusterte leveår (QALYs).

Preface

Akershus Universitetssykehus have tasks such as patient treatment, research, teaching and patient education. They are responsible for about 560 000 inhabitants across regions such as Follo, Romerike and Kongsvinger. Thanks to Ahus, our bachelor group consisting of students from the bachelor's programme Digital Infrastructure and Cyber Security at NTNU in Gjøvik was able to learn a lot. We want to thank our thesis providers Kåre Magne Stennes and Espen Thorsen Frank for making it possible to further expand our knowledge, and thank them for helping us reach the end of the thesis. We want to thank Filip Holik for helping us reach our goals and keeping our motivation high throughout the project period. We are grateful for his continuous feedback. Lastly, we would like to thank ourselves for the continuous good work ethic and great teamwork. It has been a very exciting, challenging, educational and fun experience.

Table of Contents

List of Figures

List of Tables

Acronyms

ACL - Access Control List

AD DS - Active Directory Domain System

Ahus - Akershus Universitetssykehus

CD - Compact Disc

CVE - Common Vulnerabilities and Exposures

DVD - Digital Versatile Disc

EHS - Environment, Health, Security

GDPR - General Data Protection Regulation

ICT - Information and communications technology

IP - Internet Protocol

NHS - National Health Service

NIST - National Institute of Standards and Technology

NOK - Norske Kroner (Norwegian Kroner)

NSM - Norwegian National Security Authority

NTNU - Norwegian University of Science and Technology

QALY - Quality-Adjusted Life Year

RDP - Remote Desktop Protocol

RHA - Regional Health Authority

RVA - Risk and Vulnerability Assessment

RTLO - Right To Left Override

SMB - Server Message Block

TCP - Transmission Control Protocol

UDP - User Datagram Protocol

USB - Universal Serial Bus

VPN - Virtual Private Network

Glossary

Catchment population - Catchment population is the estimate of the population served by a hospital or other health service unit or facility [1]. 15

CIA Triad - Confidentiality, Integrity, Availability. A benchmark used when evaluating the security of digital service, software, infrastructure component etc. [2]. 54, 60

Cryptocurrency - A digital asset within the system, which is sent from one blockchain network user to another. The asset is transferred by using digital signatures with asymmetric-key pairs. [3]. 16, 34

False negative - A false negative is an outcome where the model incorrectly predicts the negative class [4]. 37

False positive - A false positive is an outcome where the model incorrectly predicts the positive class [4]. 37

GERD HRQL Questionnaire - A method that uses a questionnaire that patients fill out before and after treatment. The questionnaire consists of 10 questions regarding their physical health where the higher the score is, the worse their condition is. [5]. 19

Nessus - A vulnerability assessment tool for cyber security developed by Tenable [6]. 58

Phenomenological - Derives from Phenomenology, which is the philosophy of experience, meaning the source of all meaning in the context of the human experience [7]. 26

Playbook - A collection of scenarios and procedures to counteract them. Typically contains preparation, identification, containment, remediation and recovery. [8]. 27, 71

Scientific method - The process of objectively establishing facts through testing and experimentation. Observation, research, hypothesis, test, analysis and report are steps taken in the method. [9]. 22

Scrum - A continuous development cycle with continuous experimentation and feedback loops along the way to learn and improve as one go [10]. 5, 22

Trojan - Trojan or Trojan horses are malicious code that are disguised as safe files or programs. Unlike viruses these do not replicate. When a Trojan is activated it can cause loss or theft of data. [11]. 12, 46

Waterfall model - A Sequential development process that flows like a waterfall through all phases – analysis, design, development and testing for example. Each wrapping up before the next. [12]. 22

1 Introduction

The introduction gives an overview of what to expect throughout the thesis. It describes the background and scope of the thesis and explain why the group has been tasked with the assignment. Other relevant sections such as task description and project goals are presented to make the reader understand the different questions the thesis will answer.

1.1 Background

Akershus Universitetssykehus (***Ahus***) is owned by the Southern and Eastern Regional Health Authority (***RHA***), the largest RHA in the country. Ahus main tasks are patient treatment, research, teaching and patient education. The hospital is responsible for about 560 000 inhabitants. Their area of responsibility stretches across the southeast region of Norway and they have about 12 000 employees across regions such as Follo, Romerike og Kongsvinger. In addition, Ahus covers the northernmost parts of Oslo including Alna, Grorud and Stovner. [13]

In recent years there has been an increase in digital attacks, with a plethora of intentions, different attacker groups with differing levels of knowledge. All digital solutions that any business uses are vulnerable to an attack. This increase in activity has prompted Ahus to present this thesis for ***NTNU*** for a bachelors thesis, among other measures. Specifically, Ahus wishes for this thesis to be part of its future research with the intention of evaluating consequences of cyber attacks on the clinical field (namely, patient treatment). Ahus also wants to know what effect an attack can potentially have on a patients quality-adjusted life year (***QALY***) related to their treatments, and to consider and discuss effective countermeasures for these types of cyber attacks.

1.2 Scope

This section specifies the scope of the thesis. This includes the main issue that the thesis is relevant to, a description of the task, as well as the limitations the group has decided on for how broad of an area the thesis will cover.

1.2.1 Main Issue

The study will mainly focus on crypto virus attacks aimed towards the healthcare sector. This is due to an significant increase in cyber attacks in recent years, as mentioned in Section 1.1. Examples of these types of detrimental attacks are; the AMCA data breach of 2019 [14], the ***NHS*** ransomware attack on the 12th of May 2017 [15] and the more recent NHS ransomware attack August 4th 2022 [16].

Considering the massive attack on AMCA as well as the repeated successful attacks on the ***NHS***, the first of which further affected over 200 000 machines in 150 countries, meaning that cyber criminals represent a danger that must be taken seriously. This also displays that there is consistently a big uncertainty with digitally hosted services, as there are likely vulnerabilities in its infrastructure that can be heavily exploited. All anyone can do about it is to be as smart and knowledgeable about different attack vectors as possible, particularly social engineering (phishing, identity theft etc.). These are the more common attack vectors used towards the healthcare sector.

With all this in mind, this thesis sets out to answer the following; What are the reasons, goals and attack vectors an attacker make use of when targeting the healthcare sector, and what type of consequences can these attacks have for the patients under its care?

1.2.2 Task Description

The task description specifies that the group will discover the direct consequences of crypto virus attack for clinical activity such as; ***QALY***, privacy, HMS and economy. While assessing preventive measures to prevent and avoid future attacks. In addition, the group is tasked with creating an attack tree diagram to further study the steps in the attacking process that are based on earlier attacks. Outside of this, the group is free to interpret the contents of the thesis themselves.

1.2.3 Main Issue Limitations

The project is mainly limited to crypto virus attacks against the healthcare sector. This excludes other forms of attack. The issue is primarily limited to western countries to narrow the focus towards incidents that are

relevant to ***Ahus*** when discussing cause, agendas, potential targets and consequences.

1.3 Project Goals

Our goals for this project is divided in result goals and effect goals. Result goals are tied to the product of this project. The project leader owns the result goals and is responsible for reaching these goals. Effect goals are tied to the long term impact and benefits for the client.

1.3.1 Result Goals

- Evaluate and inform the healthcare sector about crypto virus attacks and the hidden consequences.
- Discuss and suggest effective measures to prevent and avoid attacks.
- Perform a risk assessment based on crypto virus attacks aimed towards the health sector, with a focus on ramifications that can affect patients.
- Identifying causes for attacks, avenues for attack, effects an attack can have on the victim, and effective countermeasures against attacks.

1.3.2 Effect Goals

- Acquire a greater general knowledge about crypto viruses.
- The research performed in this thesis will be used in further research relating to digital attacks towards the health sector.
- Spread awareness of crypto virus attacks in the healthcare sector to reduce the consequence of an eventual attack.

1.4 Specifications

The bachelor thesis consists of a study in the consequences of crypto virus attacks aimed towards the healthcare sector. The impact of these attacks on the ***QALY*** of patients as direct consequence. These attacks will also be

analyzed with an attack tree diagram to learn more about each step. The project period is set between 9th of January and 22nd of May. At the end of the period the group has to finish and deliver the report.

The project report is written in English, most vocabulary and information about the topics are easier discussed in English. Furthermore, the working language of the group's supervisor is English, making the language selection a natural choice.

Throughout the project period the group will mainly use Overleaf to write the main report. LaTeXis a convenient suited language for report writing and Overleaf also provides shared document writing with both peers and supervisor. ***NTNU*** also provided a template for the report which is very useful.

1.5 Target Audience

The primary intended audience of the bachelor thesis consists of the IT staff at ***Ahus***. However, the bachelor thesis providers have expressed a desire to utilize the thesis as a resource for conducting ***RVA***, which expands the target audience to other personnel at Ahus. This group primarily includes leaders and branch managers, in addition to IT personnel. The thesis can also be of use for other IT professionals within the healthcare sector, as it will discuss possible solutions and measures to defend against cyber threats.

1.6 Background of the Group

The group is on their final semester in a three year bachelor's degree in *Digital Infrastructure and Cyber Security* at the Norwegian University of Science and Technology in Gjøvik. The group consists of four students which has studied relevant curriculum for the bachelor thesis. The curriculum ranges from technical courses such as infrastructure, data communication and programming, and also theoretical courses such as operating systems, risk management and incident management. Most of the courses are relevant to the thesis, but the group must gather and understand information about topics such as ransomware, patient security and attack trees. Specifically, how older and more recent ransomware cyber attacks have affected different types of healthcare providers.

1.7 Project Plan

This section explains the general plan for the thesis. This includes the process of writing the project plan, doing research, processing the information gained from the research and developing an understanding for the issue. The goal is to provide a thesis that uphold the goals and results requested by the thesis provider.

The process described above equates to what type of development cycle the group selects. This is with the purpose of writing a complete thesis based on collected data and performed procedures for documentation.

1.7.1 Development Cycle and Methodology

For this thesis when contemplating what type of development cycle would be most fitting, the group decided on using ***Scrum***. Scrum is a framework for developing and sustaining complex products. Scrum utilizes the team structure to complete tasks in smaller pieces at a time. [10]

While Scrum is primarily utilized in developing a product, it can also be adjusted to work with a bachelor thesis. Scrum is an agile methodology and can be adjusted if needed. The short sprints are also fitting for the thesis. Altogether, the thesis seem like an extensive challenge, but the sprints enables a step by step approach. Therefore, the group figured it would be the most suitable methodology.

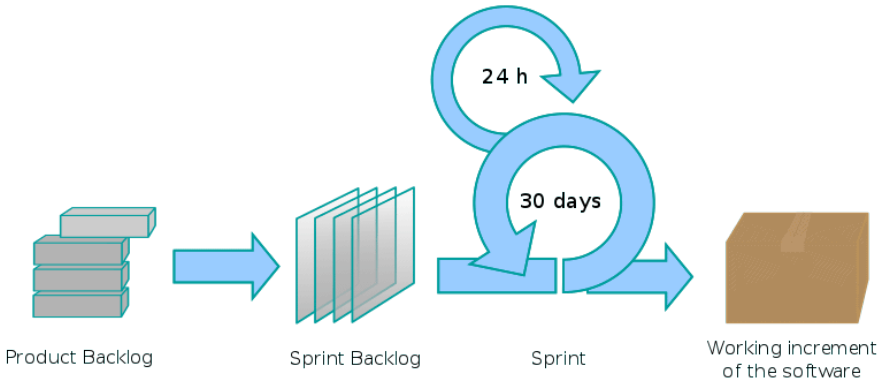


Figure 1: The process of scrumming [17]

1.8 Structure of the Report

This subsection explains the general layout of the thesis and gives the reader an idea of what to expect in the different sections. The reader can use the table of contents for easier navigation.

2. Theory: This section covers key topics presented in the thesis, including theory related to ransomware and ransomware attacks, as well as interviews, ***QALY***, and attack tree diagrams.

3. Development process: Explains the groups process throughout the project period, topics such as scrum process, meetings and documentation are included.

4. Method: This section explain how the group were able to answer the main issues of the thesis. Data collection and analysis are the two key topics included in this section.

5. Results: The results present different key findings of the research conducted throughout the project period. Results from the attack tree and paths taken are presented, as well as the consequences of a ransomware attack.

6. Discussion: In this section the results are interpreted and evaluated. Key topics such as attack tree usefulness and different unused paths are discussed alongside discussion about consequences of an attack and the groups recommended measures for ***Ahus***.

7. Conclusion: This chapter contain a summary of the project, including the results and discussions that are covered in this thesis. Relevant topics such as, group results, alternative possibilities, future work and a group evaluation are reflected.

2 Theory

The theory chapter provides information about subjects that are relevant throughout the thesis. The thesis is built on several subjects. Subjects such as ransomware, interviews, attack trees and more are presented in this chapter.

2.1 What is a Ransomware Cyber Attack?

Ransomware is defined by the National Cyber Security Centre in the United Kingdom as following:

> "*Ransomware is a type of malware which prevents you from accessing your device and the data stored on it, usually by encrypting your files. A criminal group will then demand a ransom in exchange for decryption. The computer itself can become locked, or the data on it can be encrypted, stolen or deleted. The attackers can also threaten to leak the data they steal.*" [18]

When a ransomware attack occurs there are usually several steps in which the attacker develops and implements the malware on a system. These steps are often referred to as a cyber kill chain, which will be more discussed in the section below. The attacks are swift and unnoticeable for the untrained employee, as cyber criminals are becoming more and more mature and creates malware that improves their chance of success as well as reduces their chances of getting caught.

There are several types of dangerous ransomware, but there are three main types in which the severity ranges from a little intimidating to critical getting breached, namely, scareware, screen lockers and crypto ransomware.

Scareware
Scareware is the least intimidating ransomware. Usually, there is a popup saying that the computer is infected and that the user have to pay. If the user do not pay, the user can be spammed with several popups. However, the files on the system is usually safe. It is easy to detect and respond to this type of ransomware. If the computer system is protected by a paid security software, the security software should be able to remove the mal-

ware. [19]

Screen Lockers
Screen lockers are far more serious than scareware. The Screen locker ransomware will completely lock a computer, and the user will not be able to access it. When trying to restart the computer, the user will usually be prompted that there is illegal activity on the computer. It can be intimidating, but a Judicial body will not lock a user out of a computer. The user will somehow have to erase their computer. [19]

Crypto Ransomware
This type of malware encrypt files on a computer. The encryption is usually random, and a user will have to use an encryption key in order to unlock their files. The attacker will put a ransom on the files in which they make the user pay a ransom to reacquire the files. [19]

The payment, however, is not recommended as it does not guarantee that the user get their files back. Therefore, it is recommended to keep newly updated backup files in case of an attack and a refresh of the computer system is imminent.

2.2 How is a Ransomware Attack Performed?

2.2.1 Cyber Kill Chain

Cyber kill chain is a framework for identification and prevention of cyber intrusion activity, and is developed by Lockheed Martin [20]. Businesses can utilize the cyber kill chain to stop an attack during any stage of the attack. The cyber kill chain framework consists of 7 steps:

Reconnaissance
The attacker collects data about possible targets. Attacks can utilize automatic scanners to search for vulnerabilities in the targets' system. [21]
Some examples of useful information for an attacker are: e-mails, conference information, operating systems, user IDs and physical location. [22]

Weaponization
The attacker then creates a means to attack such a malware suited

for the vulnerability [21]. The attacker then couples the exploit with a backdoor into a deliverable payload against the target [20].

Delivery
The attacker delivers the payload with the exploit. This can happen through multiple mediums such as web, email and ***USB***. [20]

Exploitation
The payload successfully reaches the target. The attacker can utilize the vulnerability to execute code on the victim's system [20]. The attacker can install tools, run scripts and modify security certificates [21].

Installation
The attacker installs malware on the targets' systems making a backdoor [21].

Command and Control
The attacker takes control over a device or identity in the targets' network [22]. The attacker can move laterally to find credentials, and gain access to privileged accounts establishing more control over the targets' network. [22][21]

Action on Objectives
The attack can now achieve it is objectives such as; gathering data, extracting and encrypting confidential information. [21]

2.2.2 Attack Vectors

An attack vector refers to the method an attacker would use in order to attack a target. This includes how an attacker would initiate their attack, how they would enter the victims digital infrastructure and in what ways an attacker can abuse existing vulnerabilities to perform a ransomware attack. The attack vector thus represents the initial entry an attacker gains and the different methods used to obtain this entry. [23]

The identification and use of an attack vector retains to the first 3 steps of the cyber kill chain, as the steps are described in section 2.2.1. In regards to the first step about reconnaissance, the attacker collects as much information about the victim as possible. This is with the intention of discovering possible attack vectors relevant for their attack. E.g. collecting

email addresses or other contact information that is connected to the company that is victimized, as well as specific high profile workers information that are connected to the company's systems. With this information the attacker can perform social engineering, as described further in section 2.2.2.1.

Furthermore, the attacker will then move to step 2 of the kill chain. This is where an attacker makes their attack payload, and then proceeds to prepare to deploy the weaponized ransomware onto the victims systems. Finally, step 3: delivery. This is the delivery mechanism employed in order to insert the attacker's ransomware payload into the victims systems. This step makes use of the reconnaissance performed by the attacker in order to find some vector to deploy their weaponized ransomware, such as social engineering or exploitation of vulnerabilities with the victims infrastructure endpoints. E.g. leaked login details, known vulnerabilities recorded in databases like Common Vulnerabilities and Exposures (***CVE***) details [24]. Even worse, some unknown vulnerability or a zero day vulnerability, meaning a "Vulnerability in a system or device that has been disclosed but is not yet patched"[25].

2.2.2.1 Attack Vectors in Use Against the Health Sector

In relation to ransomware attacks targeting the health sector, there is a multitude of different vectors that can be used by an attacker.

2.2.2.2 Social Engineering

The most prevalent attack vector used by attackers is the use of social engineering. According to P. L. Gallegos-Segovia et al. [26], the term social engineering is defined as such:

> "*Social engineering consists of a set of psychological techniques and social skills, based on influence, persuasion and suggestion, which lead the user to reveal personal/business information, or to perform actions that allow an attacker to get network access.*"

As explained above, social engineering essentially targets the weakest link of a company, the human element. This is done by use of social techniques that target the individual. This is based on extensive research from the

attackers side and is used in a wide variety of ways in order to gain the trust of the individual in order to exploit them.

Forms of attacks using social engineering are the different ways an attacker can use phishing. Phishing refers to baiting a victim into clicking a dangerous link in an email or other digital communication format that redirects the user to some endpoint where an injection can be made in order to gain entry. According to the article "Social Engineering Attacks During the COVID-19 Pandemic" [27] published by Springer Link on 6th of February 2021, there was an estimated 100 million phishing emails blocked by Google every single day, as well as a blog post from Microsoft [28] with data from 2020 indicating that phishing makes up an estimated 70% of all cyber attacks.

2.2.2.3 Phishing Attacks

Phishing attacks are defined differently depending on the information used, the target, and the goal. These definitions also vary depending on the source, though the descriptions for the different techniques mostly remain the same. This thesis will make use of the definitions described by Bhavsar, [29]. The authors describe the different types of phishing attacks as deceptive phishing, spear phishing, clone phishing, whaling, link manipulation and voice phishing.

Deceptive Phishing
Deceptive phishing, or email phishing is the most common approach to performing a phishing attack. When using this method, the attacker attempts to deceive the victim by impersonating an acquaintance or a company in order to gain sensitive information about the victim. This information is then further used as blackmail or can even be the victims login information, which allows the attacker to gain access to the victims company clearance, and potentially allows the attacker to perform a large scale attack. Unlike spear phishing, deceptive phishing is deployed more as a template for targeting different individuals at once.

Spear Phishing
Spear phishing is an altering of deceptive phishing that is specialized for a specific individual in a company, typically an administrative position or other high ranking employees at a company. Typically the

attacker will stalk the individual in order to construct a convincing fake email relating to some event that they are partaking in, e.g. the victim going to an event and the attacker posing as an event organizer baits the victim into revealing sensitive information or interacting with a malicious link.

Clone Phishing

Clone phishing is a technique where an attacker obtains access to an email and spoofs its contents, by swapping out any links or files with malicious versions. This email is then redistributed to their recipients, essentially turning the trusted email that was expected into a pseudo ***Trojan***. Instead of it being an actual Trojan in the terms of cyber security, where malicious code is disguised as a trusted program, instead the trusted email becomes the Trojan and the links and files with malicious code become the Greeks. This is all with the goal of furthering the infection either further into the victims infrastructure topology, or in order to steal out information found on the patient zero machine (the machine used for the initial cloning).

Whaling

Whaling is essentially the same as spear phishing, only the targeted victim is different. Whaling aims specifically for a wealthy and powerful entity like the rich and the famous. This is where the specific naming convention becomes apparent, the target is a whale, or big phish. The similarities with spear phishing are the use of extensive research and stalking of the victim trough social media or digital footprints.

Link Manipulation

Link manipulation refers to masking a link to a credible website or other, while the actual link under the mask leads to some spoofed or malicious website. This technique is often used in conjunction with the aforementioned forms of phishing as the hook for the bait. The victim gets hooked by the link and at that point the attacker has likely gained access to the victims email.

Voice Phishing

Voice phishing is a type of attack that differs from the other phishing methods, as it is fully done over phone calls. The attacker contacts the victim over their phone and convinces them to give up some information through either blackmail, persuasion, deception or intimidation. Examples of this are advance-fee scam (Nigerian prince

scam) where someone poses as a person of immense wealth that needs the target's bank credentials to transfer some sum of money fast, or the Indian Microsoft tech support call center scams that tells a target that there are issues with the computer and will try to remotely connect to the target's computer to "fix it".

2.2.2.4 Exploits and Known Vulnerabilities

Although social engineering is the most prominent and easily performed attack vector, there are also other possible types of attacks that are even more critical and dangerous. These are typically more advanced and difficult to counteract, but are also harder to perform.

An example of this is using internet protocols in order to send malicious packages around, for example a man-in-the-middle attack. This type of attack is performed by intercepting communications between 2 entities in order to either listen in on their private texts, or alter the contents of the messages. This technique is also used in social engineering, but is also applicable as an exploit depending on circumstance. Typically this is part of an attackers reconnaissance, but an attacker can also edit code or files in an email being intercepted to use it as an attack vector. This can be an effective attack strategy depending on the victims expertise, as there can be several signs of tampering visible to the victim. An example would be tracing the email's path to the recipient, as this path would be different than expected, or could be interacting with unknown entities on the internet. However, this is circumvented by the use of encryption and technology like ***VPN***.

Another way an attacker can make use of exploits as an attack vector is to look for vulnerabilities in the types of technologies that is used by the victim. This form of attack varies extensively depending on the targeted victim, the defences deployed by the victim and the type of attacker. [30]

Generally, attackers are divided into a few categories depending on the means, goals and size of the attacker. There are script kiddies, a wide assortment of different hatted hackers and state sponsored hackers. Hatted hackers refer to the different goals a hacker can have outside of state sponsored hackers, and there is a wide variety in what they do. 3 examples of hatted hackers are white hat, black hat and gray hat.

Script Kiddie
Script kiddie refer to beginners and amateurs using hacking tools found on the internet, usually teenagers that intend to explore and cause mischief. [31]

White Hat
White hat hackers aim to breach a victims system with the intention of informing the victim of the discovered vulnerability free of charge. [31]

Black Hat
Black hat hackers are the opposite, they intend to steal, exploit, blackmail etc. These are the individuals and organisations this paper focus on, as well as state sponsored hackers, as these are the types of attackers that aims to exploit a victim for financial or political gain. [31]

Grey Hat
Finally there are gray hat hackers, who land somewhere in between the white hats and black hats. These hackers do not necessarily intend to help or harm a victim, but simply hack for fun or to explore to discover vulnerabilities that they can either give to the victim for them to fix, or sell to another hacking organization. They can also distribute the vulnerability on forums, or not distribute them at all. [31]

2.2.2.5 Unknown Vulnerabilities and Zero Day Attacks

While there are several ways for an attacker to perform any type of digital attack against a victim, there is a relatively high chance that an attacker is able to discover a new vector for attack at any time. Any systems running on any software, or firmware are exposed to the possibility that an attacker discovers an unknown vulnerability and abuses it to attack a victim. These types of attacks are called zero day attacks, meaning a vulnerability in a type of software or firmware that any malicious entity can use to preform a cyber attack against a victim. Specifically, this attack uses a vulnerability that is unknown to the larger world and has yet to be patched, meaning anyone that is exposed to this vulnerability has no way to protect themselves from it.

2.3 Research on Previous Impact of Ransomware

This section explore some previous ransomware attacks recorded against the healthcare sector throughout the last few years. This section also explores the different consequences the attacks have had for their victims, and how the successful attacks have contributed in development of more sophisticated attack strategies.

2.3.1 National Health Service (England, 2017)

In May 2017, the global WannaCry ransomware attack took place across multiple continents and organisations. One of the most considerable causalities of this attack was the National Health Service in England. According to Ghafur et al. [32] there were over 600 organisations affected, and this included 34 infected hospital trusts and 46 affected hospital trusts.

Out of the affected hospitals there was no significant difference in total activity. Although, there was actually a minor increase in emergency admission and fewer 'accident and emergency' admissions per day. But the numbers was usually less than 1% change throughout the attack, deemed to be a normal change. However, the infected hospitals had significant changes compared to the affected hospitals. There was a decrease of total admissions per infected hospital per day, with both fewer emergency admissions and fewer elective admissions. Naturally, the attack had financial impact on the infected trusts. As Ghafur et al. [32] mentions there was a total loss of £5,9m. The financial impact was mainly based on lower activity during and after the attack. Specifically £4m was lost in inpatient admission, £0.6m lost from A&E activity, and £1.3m lost from cancelled outpatient appointments. Although not confirmed, the UK and US have on multiple occasions blamed the North Korean cybercrime group Lazarus to be responsible for the attack.

2.3.2 Benešov Hospital (Czech Republic, 2019)

Benešov hospital in the Czech Republic is a medium sized hospital with a ***catchment population*** of approximately 120 000 people, although Filipec and Plášilb [33] refers to Benešov hospital's yearly report [34], indicating a catchment population of up to 400 000 during the summer months as the city is a popular vacation destination. In December 2019, the hospital

was attacked by the ransomware group Ryuk. The attack consisted of phishing and the malware mix Emotet-Trickbot-Ryuk. Filipec and Plášilb [33] refers to Shabu's [35] research about the initial attack vector which was a large scale spam and phishing campaign with high level of sophistication. Once the phishing email was successfully triggered by a victim with access to the system, Emotet was initiated. [33] Emotet has the capability to spread to other users and download additional malware. Emotet downloads Trickbot, which can be used to manually deploy the Ryuk ransomware virus by an attacker. [36] Ryuk functions like a typical ransomware virus with the ability to encrypt data and demand ***cryptocurrency*** from the victim to restore access. [33]

2.3.3 Düsseldorf University Clinic (Germany, 2020)

The first reported death to ransomware happened in October 2020. A woman scheduled to undergo critical treatment at Düsseldorf University Clinic was unable to receive treatment due to an ongoing ransomware attack, and had to be treated at another hospital 30 km away. This delayed the treatment by an hour, and is believed to have contributed to her death. [37]
The ransomware was believed to be the DoppelPaymer ransomware. The clinic was not the the initial target as the ransom note was addressed to Heinrich Heine University. Police contacted the attackers, and the decryption key was provided. No data was lost and the clinics systems went back in to operation within a week. [37]

While this is be the first reported death to ransomware, it is certainly not going to be the last, as the number of ransomware attacks have increased year by year [38].

2.3.4 Vastaamo (Finland, 2018-2021)

The ransomware attack against Vastaamo, a Finnish psychotherapy service provider, is one of the first cases of the use of a new way for cyber criminals to extort larger sums by the use of triple extortion. Like double extortion, this method simply adds a third extortion vector to the attackers strategy. The three vectors become the primary, secondary and tertiary extortion. The primary refers to the initial sum demanded by the attacker, the secondary refers to the same vector, a second time, meaning

the attacker either attacks using the same vector again or simply demands more money. The third vector targets third party players in the attack, meaning patients, service providers, individual workers etc. It is due to this method of attack, as well as the demanded sums of both Vastaamo and its 3rd parties resulted in the clinic going bankrupt due to the attack. An estimated 40 000 patient journals were breached as a consequence of the attack, and this lead to several patients being extorted by the tertiary method of extortion. [39]

Erka Koivunen explains in Noori's publishment at "Forum för DataSkydd" [40] that there have been cases where system administrators of Vastaamo have been notified during the nights and weekends that their system is down. The administrators were tired of having to travel on-prem to fix the issues. Therefore, they created remote access to the system in 2017. However, this allowed everyone to find their system.

According to H. Tuttle [41], the attacks leading up to Vastaamo ultimately going bankrupt started in 2018, which was later followed by an attack in 2019. The extortion using this data was then later made use of in 2020. Initially, the attacker leaked 300 patient journals to indicate that they meant business and demanded a payment to be made in bitcoin. If the payment was not made, then the rest of the 40 000 journals would be leaked. The attacker also demanded a few 100 Euros in bitcoin from several patients under threat of disclosing therapy session transcripts and and personal identity codes. Tuttle then goes on to quote Adam Bangle (the vice president of Blackberry's European, middle eastern and African sector. Blackberry is an organisational software provider): "*this is one of most disturbing examples of gross misuse of patient records in recent history*".

Depending on the source, the name of this type of extortion varies, as what N. Kshetri et al. calls triple extortion, Tuttle describes similarly with either "'double extortion', 'name and shame' or 'encryption+exfiltration'". What Tuttle describes is the process of the initial encryption done by the ransomware (primary attack), that is subsequently followed by the extraction of data (secondary attack). This is then used by the attacker to extort patients (Tertiary attack). This is summarized in a simple way by Paul Ducklin from the Naked Security blog [41]: *'It's a bit like being kidnapped and blackmailed at the same time: even if you have a way out of one crisis, such as a recent and reliable backup to recover your own files, the crooks have a second hold over you.*'

2.3.5 Barcelona Hospital (Spain, 2023)

A more recent ransomware cyber attack occurred in the start of March 2023. Targeting one of the main leading hospitals in Barcelona the extortion group "RansomHouse" managed to remotely hack into the hospital network and exfiltrate different type of data. Avishai Avivi, CISO of the security company *SafeBreach* explains the attack to Mascelloni as follows:

> "*The malicious actors were able to spread laterally – considering that multiple locations were shut down (laboratories, emergency rooms, pharmacies and several external clinics). This suggests that the hospital's networks were not properly segmented and segregated from each other*". [42]

As a result of the attack the hospital had to cancel 150 non-urgent operations and about 3 000 patient checkups.

2.4 What is QALY?

QALY is a measurement used when defining the state of health of a person or group. QALY reflects a correlation between the length of life and the quality of life. Therefore, one quality-adjusted life-year is equal to one year in perfect health.

QALYs are usually calculated after a medical procedure, such as a particular treatment or intervention. After a procedure, the expected years of life left for a patient is estimated and each year is weighted with a quality-of-life score. This score is measured in terms of how a person is able to live their life. The main points are usually how a person carries out daily life activities, and freedom from pain and mental disturbance when carrying out their daily tasks. [43]

Typically, QALY is calculated using two metrics [44], the likely amount of years an individual has left to live and to what extent they live a given year in perfect health. Perfect health refers to an individuals utility value. For example, an individual can have a given 1 year and that year is lived in perfect health, this equates to 1 QALY. If instead they either have half a year (0.5 * 1) or live at exactly half of perfect health for an entire year (1 * 0.5) then their estimated QALY would be equal to 0.5.

The utility value used to calculate QALY is an estimated value based on what type of ailments an individual could be experiencing, and to what extent healthcare services are able to treat them. The ailments of an individual are measured using a ***GERD HRQL questionnaire***, which a patient fills out before and after treatment. The questionnaire itself will yield a result from the patient that numbers between 0 and 50, where 0 is full health and 50 is the worst result the questionnaire can yield. The questionnaire results are compared pre- and post-treatment, which then results in an estimate for the patients utility value for their QALY score. Finally, QALY is used in a measurement to calculate a patient's cost. This measures how much it costs to uphold a patients QALY score.

2.5 Interviews, as Relevant to this Thesis

This section explains the theory behind an interview, as in theory relating to the information gathering performed in this thesis. This specifically refers to the fundamental idea and purpose of an interview. This portion entirely bases its contents on Fontana's article [45].

2.5.1 Theory behind Interviewing

According to Fontana, interviewing is the most central way to obtain information. It is historically the most employed method and in today's society the interview is used for most social and formal interactions to obtain information on subjects when information found on the internet is lacking or unavailable. This is especially prevalent in the U.S. and by proxy most institutions with connections to the States. Examples of how interviews are used in the modern day is in formal settings like applications and work relations, and more informal settings like daily conversations and talk shows.

The article further explains that an interview consists of two key elements, the question and the answer. The significance of this exchange lies in formulating a question in such a way that the response aligns with the interviewer's intended expectations from the interviewee. The primary function is to obtain information, and obtain what the interviewer seeks, the answer also needs to meet the abstract prerequisite criteria. This means that the interviewee optimally is an individual with the proper disposition in relation to the interview being conducted. The importance of this var-

ies with the context of the interview. If the interview is informal then the interviewer is likely seeking personal information about the interviewee and not necessarily any facts relating to a subject. Disposition is more relevant in a formal setting, as the interviewer is likely to want specific information about a subject.

An interview can broadly be conducted in either a structured or unstructured manner. The difference is that a structured interview consists of a pre-established set of rigid questions and there is little room for variation in responses from the interviewee. Examples of this is group interviews and questionnaires. An unstructured interview has a set of questions prepared that work more like a template for the interviewer to direct their questions and can provide a greater yield of obtained information. This type of interview is reserved more for one on one formal interviews intended to discuss a subject. The typical unstructured interview is as directly quoted from Fontana: "*the open ended, ethnographic (in-depth) interview.*" [45].

2.6 Theory Behind a Questionnaire

According to Cint [46], a questionnaire is "a research tool featuring a series of questions used to collect useful information from respondents. These instruments include either written or oral questions and comprise an interview-style format." Questionnaires can be quantitative, qualitative or a mixture of both depending on the use of open and/or close ended questions.

2.7 Attack Tree Diagram

Attack trees are diagrams mainly used for modelling threats against information system security, but can also be implemented for electronic systems, banking systems, installation and personnel security. The advantages of using an attack tree diagram is that visualizing the attack creates a clear overview and makes it easier to create and implement relevant countermeasures. It also enables stakeholders without expertise in the field to better understand potential threats. [47]

The root node at the top of the attack tree diagram represents the goal of the attacker. The nodes at the bottom of the attack tree, referred to

as leaf node, at the means of which the attacker can achieve their goal. The "AND;" condition, represented by a half-circle, requires all children to be true for a parent node to be true. All conditions that are not "AND;" conditions are "OR;" conditions, which require only one of the children nodes to be true. [48] For instance, as figure 2 suggest, attack method 1 must have both attack assets 1 and 2 fulfilled for it to move on to attack objective 1. However, attack objective 1 need either attack methods 1 or 2 to further move on.

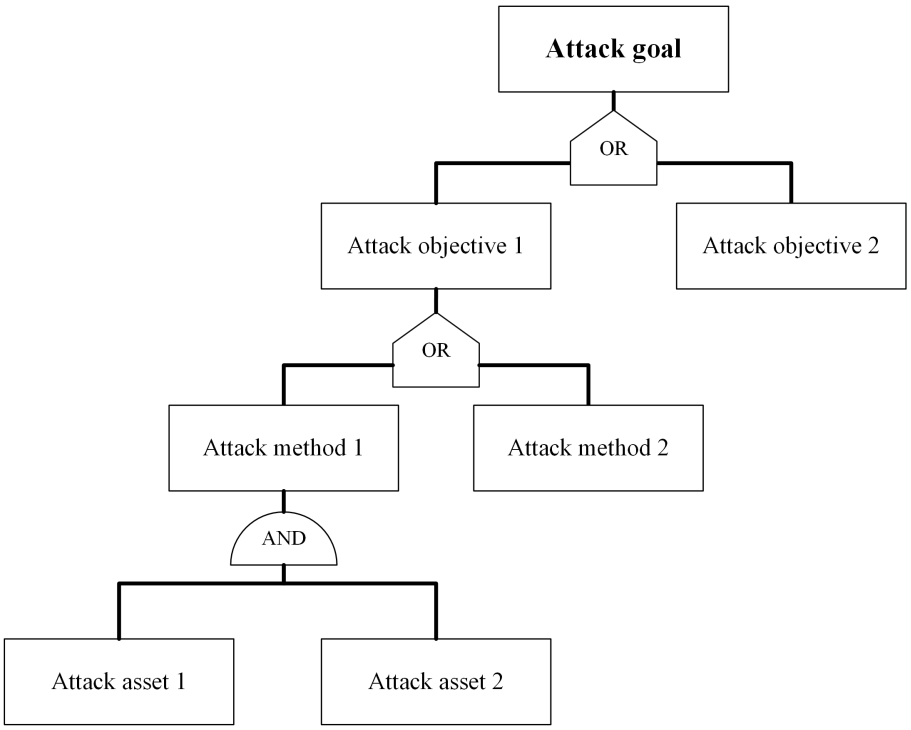


Figure 2: Attack tree diagram structure, Adapted from [49]

3 Development Process

This chapter describes the development process, and covers how the process was initially planned and how the process actually was. Some issues with the process are described alongside some thoughts the group made along the way.

3.1 Scrum Process

Early on, during the project planning phase, the group explored some different development models that could be relevant. Models such as ***Scrum***, ***Waterfall model*** and ***Scientific method*** were discussed. The waterfall model utilizes a direct approach and finishes each step before moving on to the next. Although it can be fitting for certain projects and programming assignments, the group found it not relevant for the case since the thesis is primarily an academic study. Similarly, the scientific method has a step by step approach to achieve its goals, thus it would not be quite fitting. Ultimately, at the start of the planning phase, the group found Scrum to be best fitting.

The idea was to have the project leader Jørgen as scrum master and the other group members as developers. At the start of the project period the group created a simple scrum plan. Table 1 shows how the group thought each sprint would look like.

Table 1: *Planned sprints in the project*

Type of sprint	**Sprints in period**	**Duration of one sprint**
Project plan/standardavtale	1	4 weeks
Research	3	2 weeks
Attack tree	1	2 weeks
Interviewing	1	2 weeks
Thesis development/review	4	4 weeks

In table 1 there are three different columns; *type of sprint*, *sprints in period* and *duration of one sprint*. The initial thought was that after each sprint the group would have a sprint recap where the group would discuss what

had been done. After the first sprint period the group found that the scrum process had some flaws for the specific type of thesis. It felt like the scrum method was more driven towards projects that had an end product, such as an application or involved some programming. The group concluded that it would be more fitting to have regular meetings each week to discuss different topics surrounding the thesis. Ultimately, the group used the Gantt schema created in the project plan for further guidance, see appendix E.

3.2 Meetings

During the project period, the group held meetings regularly. Internal meetings and meetings with supervisor were conducted on a weekly basis. The internal meetings were mostly conducted in order for the group to plan ahead, and discuss what work was finished and in progress, see appendix C. Supervisor meetings were conducted each Wednesday from 11am to 11:30am. Beforehand, the supervisor would check the progress and bring suggestions on how the thesis could be improved during the meeting. After the feedback the group would present the plans for the coming weeks.

Thesis provider meetings were not conducted as often as the other meetings mentioned. The group and thesis providers did not feel it was necessary to have meetings each or every two weeks. This was agreed by both parts during one of the first meetings. For the most part these meetings were held to discuss the progress of the project and to receive feedback. Feedback was important because it enabled the group to make changes that ***Ahus*** felt necessary.

During each meeting, with the supervisor and the thesis provider, the group would take meeting minutes. All of the meeting minutes can be found attached in appendix C.

3.3 Documentation

Throughout the project period the group has used a set of different documentation tools. Tools such as Microsoft Teams and Overleaf have been used. Microsoft Teams has been used in order to share documents related to the main thesis. This include documents such as meeting minutes,

Gantt schema and timekeeping. Microsoft Teams offers a built-in application called Visio. This tool was used when creating the attack trees. Overleaf enables the group to make a shared document for writing the thesis itself. The thesis supervisor recommended Overleaf and this enabled for better review, as the supervisor can easily make comments about changes without having to consult the group first.

4 Method

The method chapter explains how the group was able to answer their main issue. The chapter describes the process of collecting relevant data and literature, and how it was analyzed. Topics such as interviews and questionnaires are presented and how these were implemented to achieve the desired results.

4.1 Data Collection

Data collection was performed through several avenues, such as by analyzing data in other scientific articles and by holding interviews. The tools used to search for relevant literature included: Google Scholar, IEEE Xplore Digital library, Web of Science and Oria.

4.1.1 Literature Review

When looking for literature there were several criteria to keep in mind. Due to the nature of the task it has to be articles related to ransomware in the healthcare sector. In addition, the literature should mention the impact on the patients, systems or equipment.

When looking for literature relating to the topic, newer articles are preferred as the sheer number of attacks has increased several times in the years 2016-2021 [38], and should be expected to increase even further in the future.

4.1.2 Interviews

When building the interview template used for this thesis, the process was divided into steps:

- Choosing a method based on research and data
- Deciding a target group for the interviews
- Deciding what questions to add to the template
- Deciding the flow and structure of the interview itself

- Conducting the interviews

As mentioned in section 2.5, the interview process is based on Fontana's article [45] discussing what an interview is and the process of conducting an interview based on historical data and different methods of interviewing. The structure of interview used in this thesis is an unstructured interview, which largely entails making use of open and discussion centered questions with the intent of gaining broader and more in depth responses from the interviewees. According to Fontana's descriptions of what the different types of interview methods consists of and the different traits a type of interview has, the method used for this thesis is of the type *Field,formal*. This type of interview specifies its traits as; setting as *present, but in field*, interviewer role as *somewhat directive*, question format as *semistructured* and purpose as ***phenomelogical***.

The optimal target group for interviews were IT personnel, personnel treating critical patients and individuals with knowledge of ***QALY*** within the health sector. With this in mind, the contact log consisted of the thesis provider ***Ahus***, *Sykehuset Gjøvik*, *St. Olavs Hospital*, *Hemit*, *Oslo Universitetssykehus*, *Stavanger universitetssjukehus* and *Mental Helse Innlandet*. With this selection of potential interviews the scope of the answers likely cover all basis wanted for this thesis.

The process of deciding what questions to add to the interviews were specified after the method for interviewing was decided, and the interviewees were queried for potential interviews. The questions were constructed based on the goal of the interviewing process. This goal is gaining an understanding of how the healthcare sector maps out their critical infrastructure and how they work to secure their assets from cyber attacks. The questions were revised multiple times until a final set of questions decided on. These were divided into 3 categories (Clinical, QALY and IT competence) but were only intended on being a template for the interviewer to use, and not necessarily the entirety of the interviews contents. The final template of questions is as follows:

Clinical

- What digital systems are you dependent on to treat general patients, and critical patients?
- What type of procedures or routines for treating patients in case any digital dependencies were to be compromised?

- What consequences can potentially occur if you lose access to the aforementioned systems?

QALY

- Can you explain your process for calculating a patients ***QALY***?
- Is ***QALY*** only applicable for somatic conditions or is it calculable for psychological conditions as well?

IT competence

- What type of digital and physical security mechanisms are deployed for proactive and reactive incident management?
- Can you provide a short summary of your digital infrastructure if possible?
- How do you conduct digital forensics?
- Do you have any ***playbooks*** for incident management? And how comprehensive are they?
- What type of security threat is the most dangerous for your infrastructure and patient treatment?
- What standards for digital system development and maintenance do you follow?
- Do you perform regular ***RVA*** for your digital infrastructure?
- What type of economical consequence can occur in the case of a cyber attack?
- Would a ransomware attack affect your reputation? To what extent?
- Do you have personnel in-house or externally hired in the case of a digital attack or crisis?

The questions to be included in the interview template were decided, and thus the next step was to construct the logical flow of the interview themselves. The interviews were set to last around 30 minutes, and the total scheduled time was set to 45 minutes, giving generous leeway for extending the interview if necessary. The structure of the interview template

consisted of an introduction, questions, reflection and summary. Regarding the conduction of interviews, this is further explained in section 4.1.4 of the method.

4.1.3 Questionnaire

To ensure that the questionnaire would provide the desired results the group chose to design them based on survey theory created by Constantine Boussalis from Harward Law [50]. To achieve desired results from a questionnaire, the following four error types need to be reduced to a minimum:

- Coverage error
- Sampling error
- Non-response error
- Measurement error

To reduce coverage error it is important that all samples are collected from people with relevant knowledge and attachment to the case. On the other hand it is important to acquire samples from different departments/hospitals to achieve a degree of diversity which reduces the chance of biased answers.

Sampling error is only relevant for quantitative methods, and the group will be focusing on using a qualitative method. In a quantitative questionnaire the questions are multiple choice or single word responses. This is useful for analysing big numbers, but not for gaining new information about a topic with limited open source information. When using a qualitative method the questions are open which gives the respondents freedom to share relevant information.

Non-response error can lead to biased results if a large part of the sample group does not respond to some of the questions. To reduce Non-response error the participants need to be motivated to complete the questionnaire. According to Saul Mcleod [51], there are various ways to achieve a higher response. The longer the questionnaire is, the fewer people are likely to complete it. The questions should be short, clear and relevant to the thesis. The order of the questions also have an impact on the response percentage. The questions should progress from the easiest to hardest as getting progression in a survey will have them invested to finish it.

Measurement errors can lead to biased answers. This can be caused by poor sentence structure, wording and general design. The questionnaire should be designed from high quality theory and be quality assured to counteract measurement errors.

4.1.4 Conducting the Interviews and Questionnaires

During the conduction of the interviews and questionnaires there were several attempts on establishing contact with potential interviewees. Emails were sent to several aforementioned institutions, as mentioned in section 4.1.2; however, there were few responses. The only responses were from Hemit and Sykehuset Gjøvik. After initial contact it became apparent that neither of these institutions had available resources for further enquiry. Due to this, the only conducted interview was with personnel from ***Ahus***, and there was not a chance to distribute the questionnaire.

The interview conducted with Ahus was scheduled to take place on April 11th at 09:00 to 10:00 CET. The medium used for the interview was Microsoft Teams. The participants of the interview were 2 reperesentatives from the thesis writing group (an interviewer and a secretary), the thesis provider and assistant, and the interviewees. The interviewees were a senior consultant/emergency trainer/RVA analytic and a division facility manager/HMS(Health, environment, security)/RVA analytic. The interview was conducted without incident and adequate data was collected. The results can be found in appendix D

4.2 Data Analysis

The data analysis and data gathering for this thesis was performed in tandem. As theoretical data was collected through literature review, it was applied to the theory, attack tree and interview/questionnaire process while data collection continued. The data analysis itself was performed by making use of sources as listed in the bibliography to construct and reformulate the content of the theory section 2 and for the results presented in result section 5. This includes the analysis of the attack tree and analysis of consequences of attacks.

The attack tree was used to perform data analysis, as is presented in the attack tree diagram result section 5.1. The initial analysis for the attack

tree was through the data collection, with the goal of constructing the tree to include attack vectors used in the historical attacks (Sections 2.3.1 - 2.3.5). When this was complete, the attack tree itself became a subject for data analysis which allowed for the different branches to be individually analysed. This analysis was performed with further literature review to explain in detail how an attacker can make use of the vulnerabilities to perform an attack. The different paths that attackers have historically used, as is explained in the aforementioned sections 2.3.1 - 2.3.5, were also analysed individually.

An approach to data collection that was explored was the use of interviews and questionnaires. However, this did not result in much analyzable data, as explained in section 4.1.4. Only 1 interview was able to be performed, and therefore analysis of consequences was mostly based on historical data and the data analysed from the interview.

4.3 Attack Tree Diagram

The included attack tree is not a complete diagram of every possible attack path. Including every possibility would make the attack tree diagram needlessly complex and remove focus from the more probable attacks. As information, including confidential information, is required for a robust tree, this is a simplified and general version for attacks in the healthcare sector. In a more advanced attack tree, the tree should include the probability and cost-value and probability for each node in the tree. This would give the reader a better understanding as to what is more likely to happen, but the group decided against this feature, as the group's experience with probability and cost-value of cyber attacks is not sufficient, furthermore it is difficult to calculate the probability of each step without better insights in the healthcare systems, and analytics concerning said system.

When creating the attack tree, the group defined a set goal for the attack to branch out from. The goal of the attack in this case is to install the crypto virus. This is due to the tasks description to study a crypto virus attack, the steps leading up to the attack, and each step to the goal of the attack. Once the crypto virus is installed it is assumed that the attacker can achieve their goals, thus the group decided not to add any further steps after the installation.

Each step is a node, the goal is the root node and the start of the attack are

the leaf nodes. Leaf nodes are created with known incidents in the healthcare sector, but also filled with leaf nodes that represent known attack in other sectors. Furthermore by researching incidents and tying ***CVEs*** to attack vectors, the attack tree can further study the path attackers went to achieve their goals. The leaf nodes are generally tied to reconnaissance, as the attack would need to first discover information tied to the network. When information has been gathered from the target, the attack can shift through the information to discover a vulnerability. When a vulnerability is discovered, the attacker can then exploit the vulnerability to attack the target. Generally if the attacker has the opportunity to utilize a vulnerability, they are able to cause damage by infecting the system with malware.

5 Results

The result chapter presents different key findings of the research conducted in the study. The results of the study provide an in-depth analysis and aim to address the research questions and main issues presented in chapter 1. The findings are presented in a visualized manner with both figures and tables for clarity reasons. The chapter will present the attack tree, show paths taken from previous ransomware attacks and explain different consequences of attacks.

5.1 Attack Tree Diagram

In order to form a likely attack tree diagram scenario, it is useful to acquire some background information about both recent and older cyber attacks. The first steps taken in an attack seem to be the most vital vector. Section 2.3 informs about different types of attacks towards a number of healthcare units in the world. Ultimately, the usual goal to the attacker is to achieve command and control. By achieving control of the system they are able to gather data, extract information and encrypt confidential information.

To understand and study the ransomware installation, it is helpful to use an attack tree diagram to acquire a quick overview. Below is figure 3,

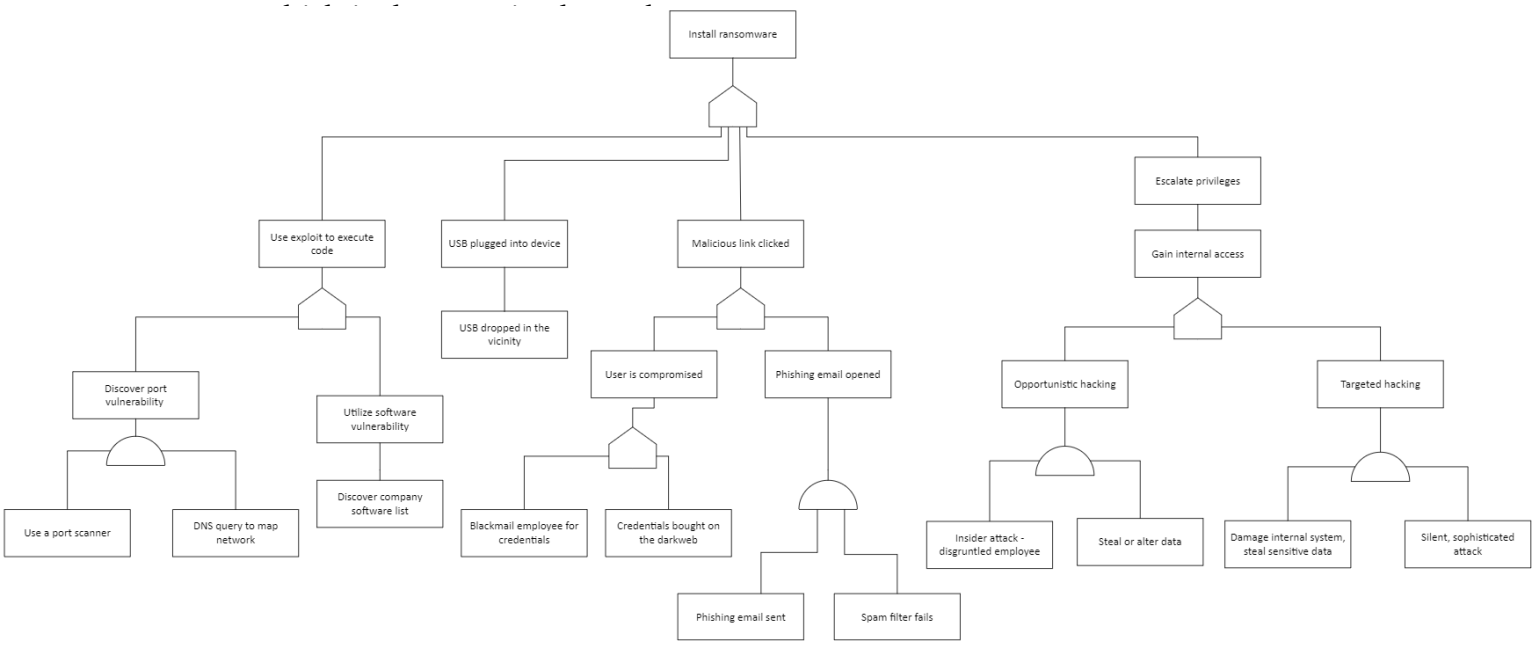


Figure 3: Attack tree with the goal; install ransomware.

5.1.1 Use Exploit to Execute Code Branch

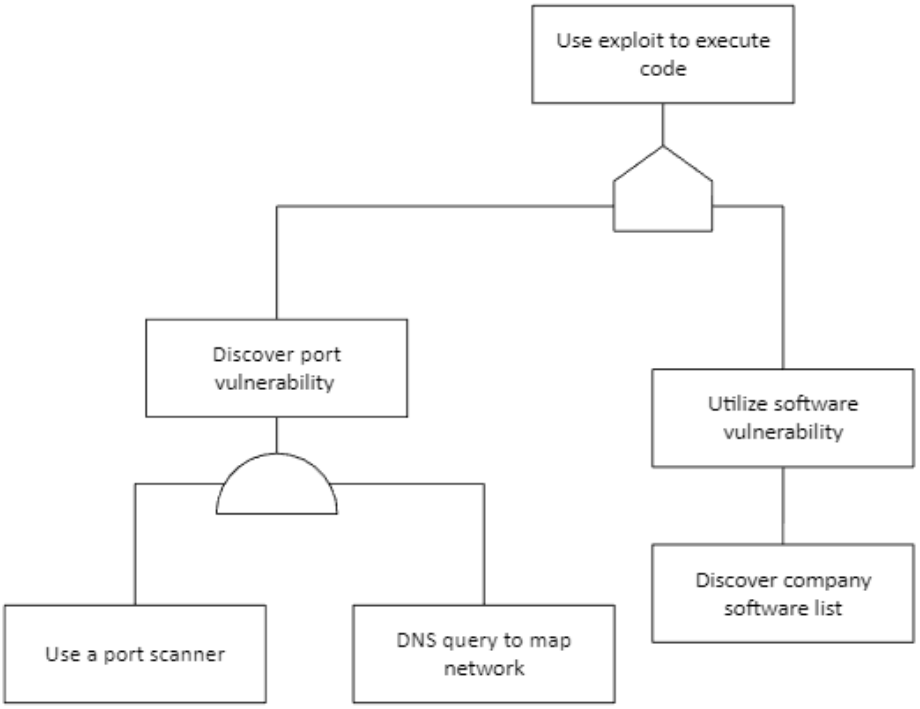


Figure 4: Attack tree branch exploit

5.1.1.1 Port Scanning and DNS Query

These nodes in the attack tree can be compared to the first step in the Cyber Kill Chain, reconnaissance. While DNS queries are not inherently dangerous and are normal part of a networks functions, an abnormal amount of scans and requests can be the indication of an attacker looking for potential targets. Port scans still have to be initiated as they are not a passive function of a network, but an action performed by a client.

There are multiple ways to find ports, but the most common is to utilize tools. There are a wide variety of different tools to scan a network, such as: ***TCP*** port scanner, Nmap, Netcat, Port Authority and more [52]. The tools will retrieve information such as: the Internet Protocol (***IP***) address, amount of ports, or even the type of service on a port. Attackers can and will utilize these tools when assessing their targets.

The attacks conducted towards ***NHS*** and Vastaamo were both enabled through ports and their protocols [32][40]. In the case of Vastaamo simply scanning for an open port, ***RDP*** in this case, could have been all it took for the attacker to gain access. While in the case of NHS the exploit was more elaborate, and required the attacker to exploit a vulnerability in

the Server Message Block (***SMB***) protocol port [53].

5.1.1.2 Discover Port Vulnerability

There are three different types of states for both ***TCP*** and ***UDP*** ports: open, closed and filtered. The vulnerabilities exist generally in open port, as closed ports are unreachable and filtered ports monitors traffic, although this does not make filtered ports impenetrable. [54] The vulnerability exploited in the WannaCry attack, was the ***SMB*** protocol service, on port 445 [54]. Another exploit is the windows remote desktop service exploit used in 2019 to hack vulnerable computers, and install a ***cryptocurrency*** miner. [55] To exploit the vulnerability the attack would have to craft a specially target request towards the remote desktop service [56]. When an vulnerability has been found, the attacker can use the exploit to move on to the next step, which in this attack tree is leveraging the exploit to execute code.

5.1.1.3 Discover Company Software List

To exploit the software a company uses, the attacker first have to discover it. There are several ways to do this. The ideal situation for an attacker is to gain access to the complete list of software the company has installed, though this is usually not feasible. There are other ways to discover individual software. A port-scan can sometimes tell the attacker which service is being used on what port, and can help to identify what version of the service is being used. Discovering the operating system and version can also be crucial for an attacker.

Simply going to a website and using the "inspect" feature built into most browsers can retrieve information. The inspect feature enables the user to edit the website source code. Used for normal purposes a web developer can test for bugs and errors. An attacker can utilize this feature to also look for bugs and errors while also learning how the website is built, which can include software used to build the website. Whilst "inspect" in itself can not hack since it is client-side, the information retrieved can sometimes be used to find vulnerabilities.

5.1.1.4 Utilize Software Vulnerability

Assuming the attack has found one or more software with a known vulnerability, at least to the attacker, the attacker can exploit the vulnerabilities. The target can have software that can detect vulnerabilities like buffer overflow, SQL injection and cross-site scripting; however, there are still a significant amount of vulnerabilities that the software does not detect [57]. Statistics pulled from National Institute of Standards and Technology (***NIST***) [57], shows an exponential increase in the amount of software vulnerabilities in the years 2016-2021. An attackers attack surface is tied to the amount of vulnerabilities and can be assumed to increase each year. The attacker can check for old software with known vulnerabilities, as it is not uncommon to use legacy systems. Older systems can have vulnerabilities that are known, but have not been patched due to the vendor dropping support in favor of newer products or ceasing operations all together [58].

5.1.1.5 Use Exploit to Execute Code

Assuming the vulnerability is significant enough, the attacker can inject malicious code to their own benefit. If the attacker can execute any code, admin privilege can be unnecessary. At this step the attack has different options. They can stay dormant while gathering information, and waiting for the right moment to strike. The attacker can attempt to move laterally in the network, further spreading malware on the targets systems. The attacker are able to achieve their goal on the infected systems by installing ransomware; however, the impact will differ depending the quantity of systems infected.

5.1.2 USB Drop Attack Branch

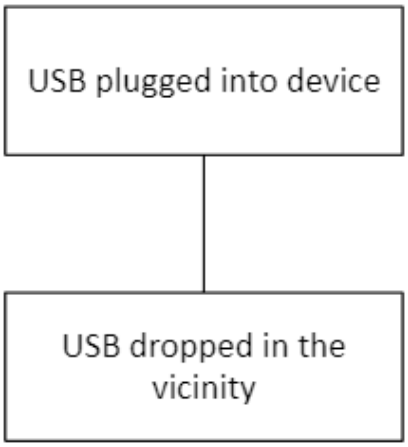


Figure 5: USB drop attack branch

5.1.2.1 USB Dropped in the Vicinity

The ***USB*** drop attack is not a sophisticated attack, it simply relies on human curiosity or altruistic motives [59]. If an attacker has access to the location, they are capable of dropping USB-sticks. The probability of the USB-stick getting to the targets system or network will vary between institutions as some locations are more restricted, such as a military base compared to a hospital. USB drop attacks are not restricted to only USB-sticks, ***CD***, ***DVD***, Secure Digital cards and Bluetooth connections are also viable mediums for an attacker.

5.1.2.2 USB Plugged Into Device

The quantity of ***USB*** attacks are relatively small compared to other social engineering attacks, but incidents are still occurring. Notable occurrences are The U.S. military cyber attack nicknamed "Operation Buckshot Yankee" [60], The Stuxnet worm attack in Iran [61], Mariposa Botnet [62] and Operation Copperfield [63]. While most attacks are most probable Advanced Threat Actors (ATP), and thus less probable. There have been attacks made against the healthcare sector, specifically by Russian hacker groups [64], and it is not improbable that the hacker groups will utilize another attack vector.

5.1.3 Malicious Link Branch

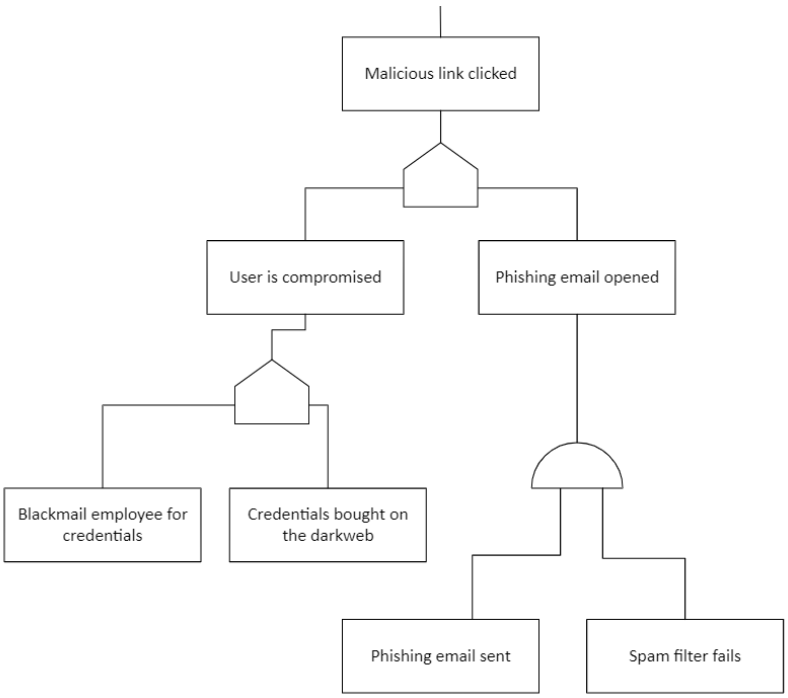


Figure 6: Malicious link branch

5.1.3.1 Phishing Email Sent and Spam Filter Fails

The attack vector with the highest quantity of attacks is by far phishing emails. They are in essence a low-cost social engineering attack. The most common type is deceptive phishing since it is usually made with larger quantity of targets in mind, while spear phishing is more tailored towards specific targets. The quantity of phishing emails received can be greatly diminished by using a spam-filter. The more common email services do have built in filter functions, including custom user set filters. The filters and algorithms are not perfect and there is bound to be ***false positives*** and ***false negatives***. [29]

5.1.3.2 Phishing Email Opened

For an email service to function it needs to be able to communicate. The amount of emails filtered will vary as some have more or better filters than others. One such filter can be only accepting internal email; however, even an internal email can be malicious, such as an email from a compromised user. An unfiltered emails will most likely be opened, and depending how

the user interacts with the email the outcome will differ. Malicious attachments masquerading as harmless files are more commonly used by advanced actors. The most common attack vector fore email phishing is including a hyperlink that sends the user to a seemingly legitimate website. The victim is deceived to hand over sensitive information such as credentials. [65]

5.1.3.3 Credentials Bought on the Dark Web

According to an article in 2022, described by Vigliarolo [66], the research team *Digital Shadows* found that there were over 24.6 billion pairs of credentials listed for sale on the dark web. From the pairs, 6.7 billion of the pairs were unique. This shows that credentials can easily be bought by threat actors to gain access to systems.

5.1.3.4 Blackmail Employee for Credentials

Although rare, an attacker can attempt to blackmail or bribe an employee. If the attacker has sufficient information about the target, the attacker can threaten to release sensitive information, or threaten the employees close friends or relatives.

5.1.3.5 User is Compromised

An attacker gaining unauthorized access to a user account compromises the account. This makes the targets systems vulnerable to further attacks from the inside, and increases the possible attack vectors for the attack. The variety of actions the attacker can take depends on the privileges of the compromised account.

5.1.3.6 Malicious Link or Attachment Clicked

When the user is compromised depending on their privileges in the system, the attacker can take a variety actions. The attacker can decide to click a hyperlink that send them to a malicious site that automatically downloads a malware. An unsuspecting user can download an email attachment, which seem harmless. One such method is Right To Left Over-

ride (***RTLO***). It is a function that enables the system to read text from right to left for languages like Hebrew or Arabic. This is further used to disguise files types to seem like another. A file can end with ".docx", but in actuality be a .exe file. However, ".exe" would still have be in the name, albeit in reverse, for this RTLO to work in the example.[67] It is, however, possible for an attacker to install malware through email attachments, such as a PDF or Microsoft Excel file.

5.1.4 Gain Internal Access

By bypassing the security measures, an attacker gains internal access, resulting in the installation of ransomware. Figure 3 describes two different ways of gaining internal access, namely, opportunistic hacking and targeted hacking. Both branches bring consequences for businesses and are a threat to be vary of. The branches are both severe and are in some cases demanding to defend against. Figure 7 is the perceived opportunistic hacking branch to the attack tree. Opportunistic hacking has attributes such as, no specific target, involves little to no preparation and leverages a situation.

5.1.4.1 Opportunistic Hacking

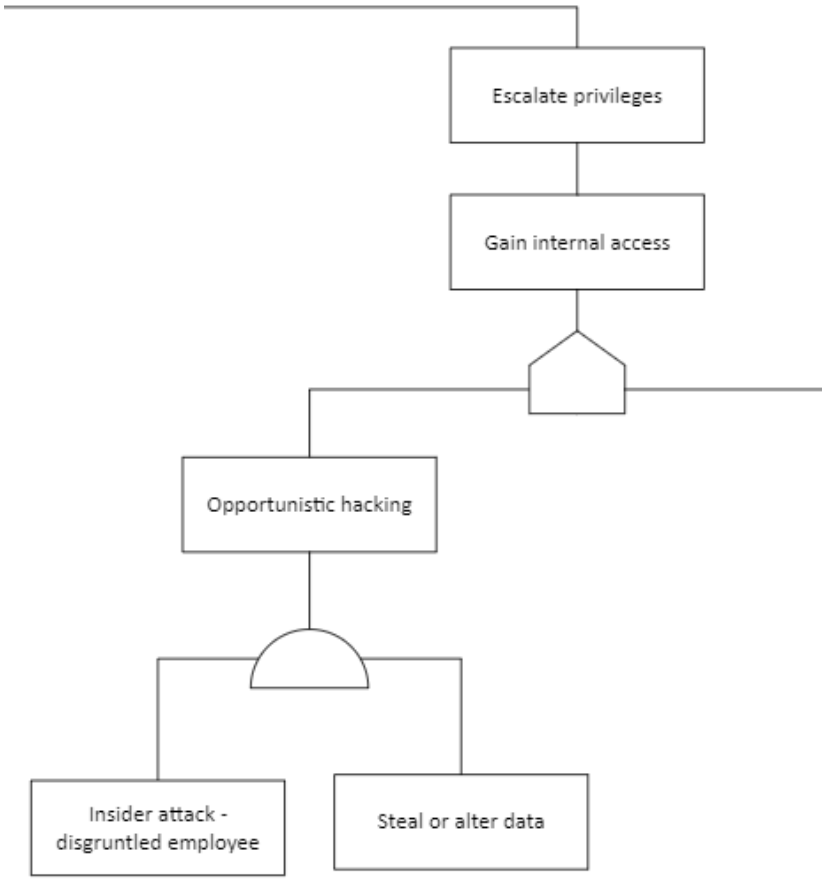


Figure 7: Attack tree opportunistic hacking branch

Opportunistic hacking is one of the trees branches which is linked to internal access. Opportunistic hacking is an unexpected type of attack and can bring severe consequences since the attacker usually wants to steal

or alter data in order to weaken or defame a company. Often times, opportunistic hackers have no intention of weakening or defame a specific company. Opportunistic hackers usually have no specific target and they often have little to no preparation. [68] Insider opportunistic attacks are probable and can be of danger to any company. For example, an employee is let go from a company and now has to find a new workplace, the whole process can provoke the employee and they can bear grudge against their former employer. Now, the employee wants to quickly leverage their remaining access rights to steal or tamper with files in order to achieve a financial outcome or to destroy the company's reputation. Since the disgruntled employee already has internal access, it is easy for them to achieve the ultimate goal of the attack tree, which is to install ransomware.

5.1.4.2 Targeted Hacking

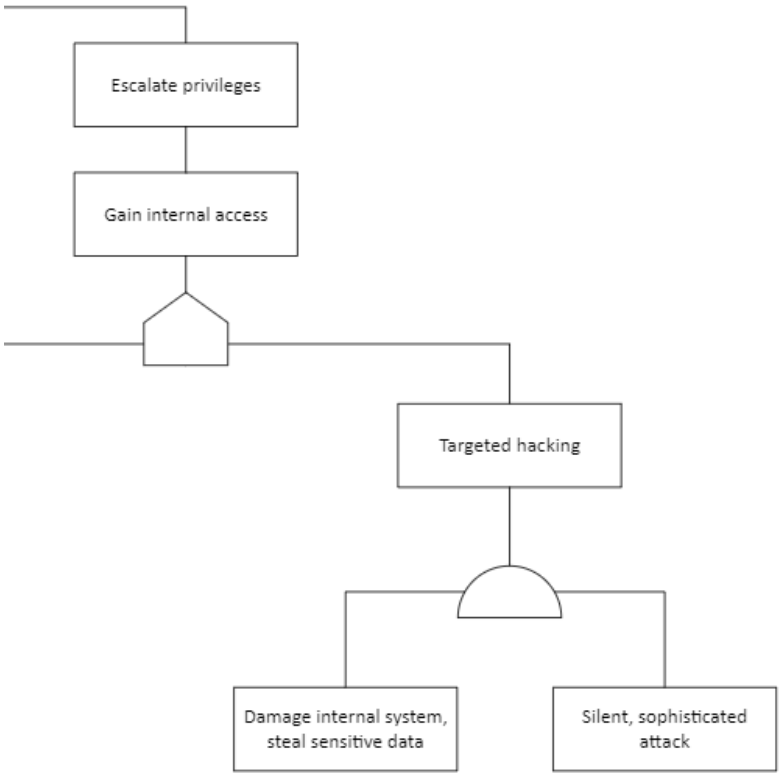


Figure 8: Attack tree targeted hacking branch

The other internal access' child node is targeted hacking, which bring severe consequences for hospitals affected. Targeted hacking are usually a worst-case scenario for most companies, because they are carried out by

IT-professionals that use a significant amount of time and resources to set up the attack. According to Trend Micro [69] there are three main criteria that have to be fulfilled in order to be considered a targeted attack.

- Specific target, spent considerable time, resources and effort.
- Infiltrate targets network and steal information.
- Persistent attack, attackers ensure the attack continues beyond the initial network breach.

A usual attack will damage internal systems and steal sensitive data, meaning that the professionals carrying out the attack will have internal access to clients, networks and databases. Targeted attacks are also extremely difficult to notice, and it can take time before it is discovered. The result of the attack can be devastating, bringing systems down and losing patient records. Ultimately, the professional attackers can install ransomware on the clients and servers they find, subsequently locking employees out of their own systems.

5.1.4.3 Escalate Privileges

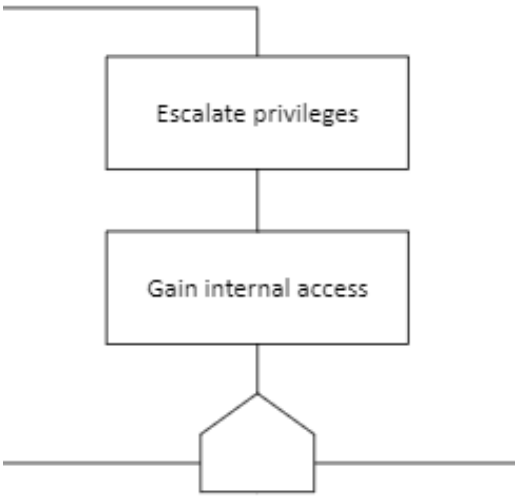


Figure 9: Attack tree escalate privileges branch

If an attacker has internal access on a system by either targeted or opportunistic hacking they probably have to escalate their privileges even

further. Privilege escalation is common among threat actors and is used to move deeper into networks. An attacker can gain initial access, but cannot do much harm with their current access rights. For example, the attacker has gained control over a user. Now the attacker is inside the network, but currently has no administrative rights. The attacker can recon the network by using different networking tools and then to either move vertical or horizontal. Vertical escalation is used when trying to gain privileges with the current user, typically to attain administrative privileges, by exploiting system vulnerabilities. On the other hand, horizontal escalation can be used to gain access to other users with the same privilege, it is less common, but can be used to gain control over multiple users. If one of the hacked users are compromised and disabled, the attacker can still access the other users. [70]

5.2 Paths Taken in Previous Attacks

Previous attacks such as, ***NHS*** ransomware attack, Benešov hospital ransomware attack and Vastaamo data breach are attacks that the thesis is built upon. But how do these attacks fit in to the attack tree? In section 2.3 relevant attacks are described in detail. This section will visualize how the different attacks fit in. Figure 10 show the different paths taken for all of the relevant attacks. The different paths have been color coded to better show how the attacks gets to its goal. Some of the attacks uses the same steps and is the same color, therefore the boxes next to "install ransomware" show which color fits to which attack. The Düsseldorf attack is green, and NHS and Vastaamo are blue, blue-green is the same as turquoise which is then connected to "install ransomware". Color-coding makes for easier interpretation of the diagram. Figure 10 show all of the attacks mentioned in a single instance; however, the picture is quite compressed. The sections below show all the different attacks in more detail.

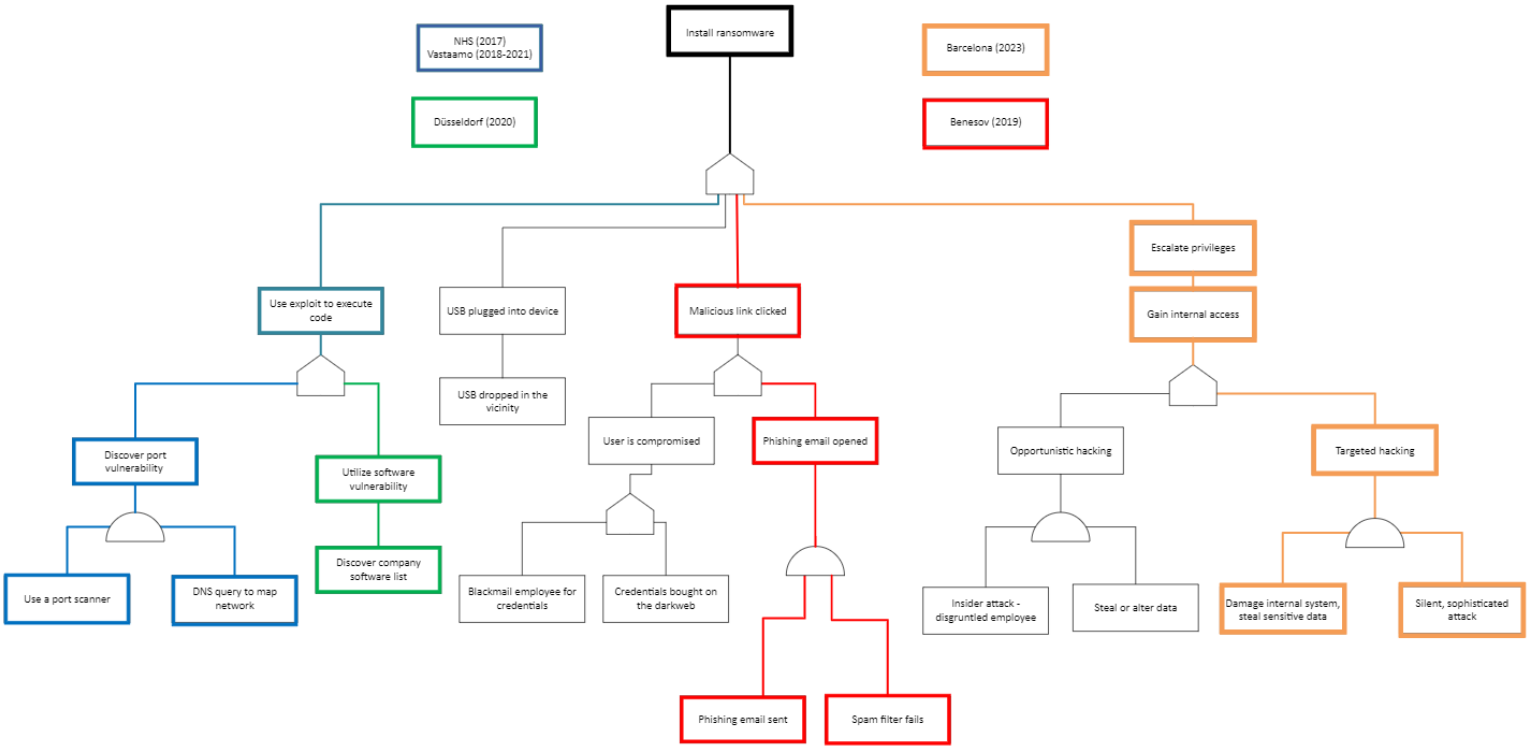


Figure 10: Different paths taken

5.2.1 National Health Service (England, 2017)

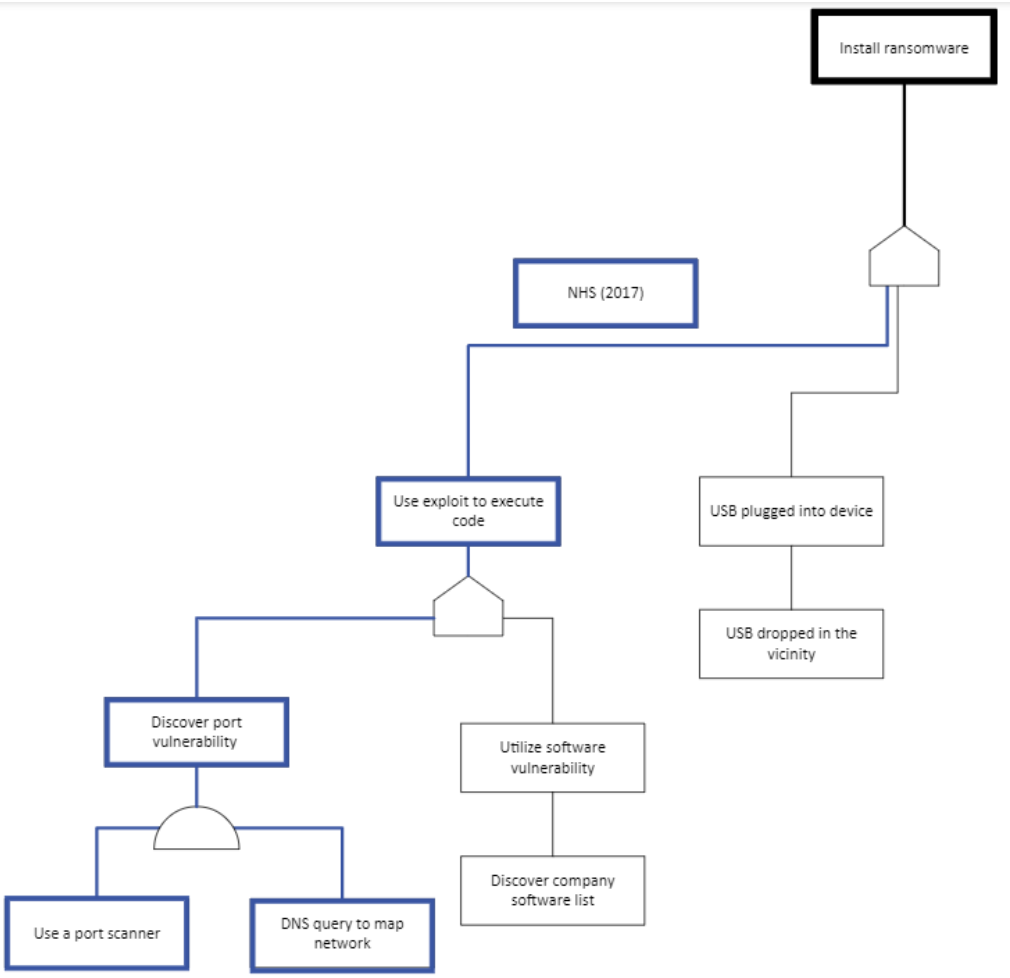


Figure 11: NHS attack path

As presented in section 5.1.1.1 the WannaCry ransomware used a port vulnerability to execute the arbitrary code. Ultimately, the code execution lead to the installation of the ransomware.

5.2.2 Benešov Hospital (Czech Republic, 2019)

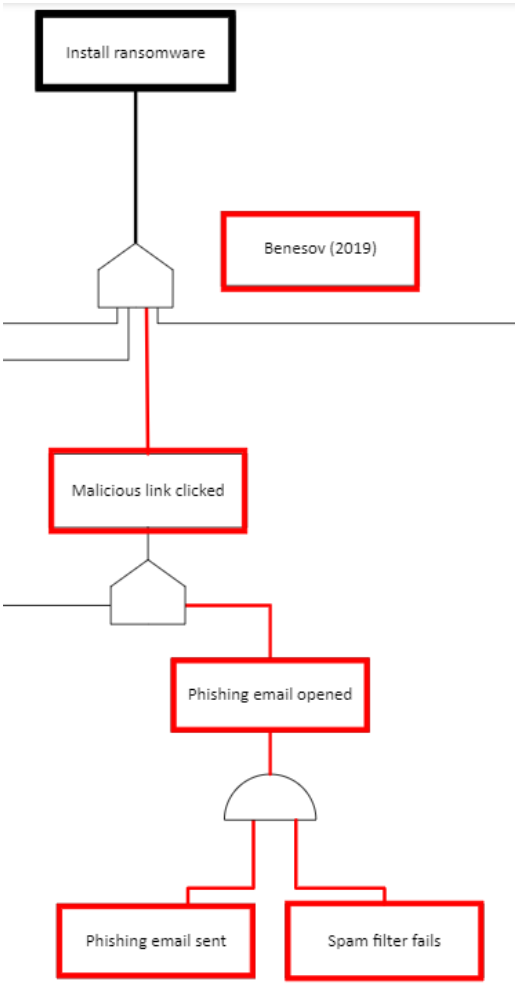


Figure 12: Benešov attack path

The Benešov incident began when a unsuspecting employee received an email disguised as an invoice. Clicking the invoice initiated the ***Trojan*** "Emotet". Emotet avoided the firewall and two anti-malware systems. Emotet spread across the network and mapped out all the processes on the targets systems. When Emotet had controll of the system it reported back to the attacker. Emotet continued the attack by installing the Trojan Trickbot. Trickbot mapped the credentials of all accounts on the system including administrators. Eventually, after securing sufficient credentials, it installs the ransomware Ryuk. [33]

5.2.3 Düsseldorf University Clinic (Germany, 2020)

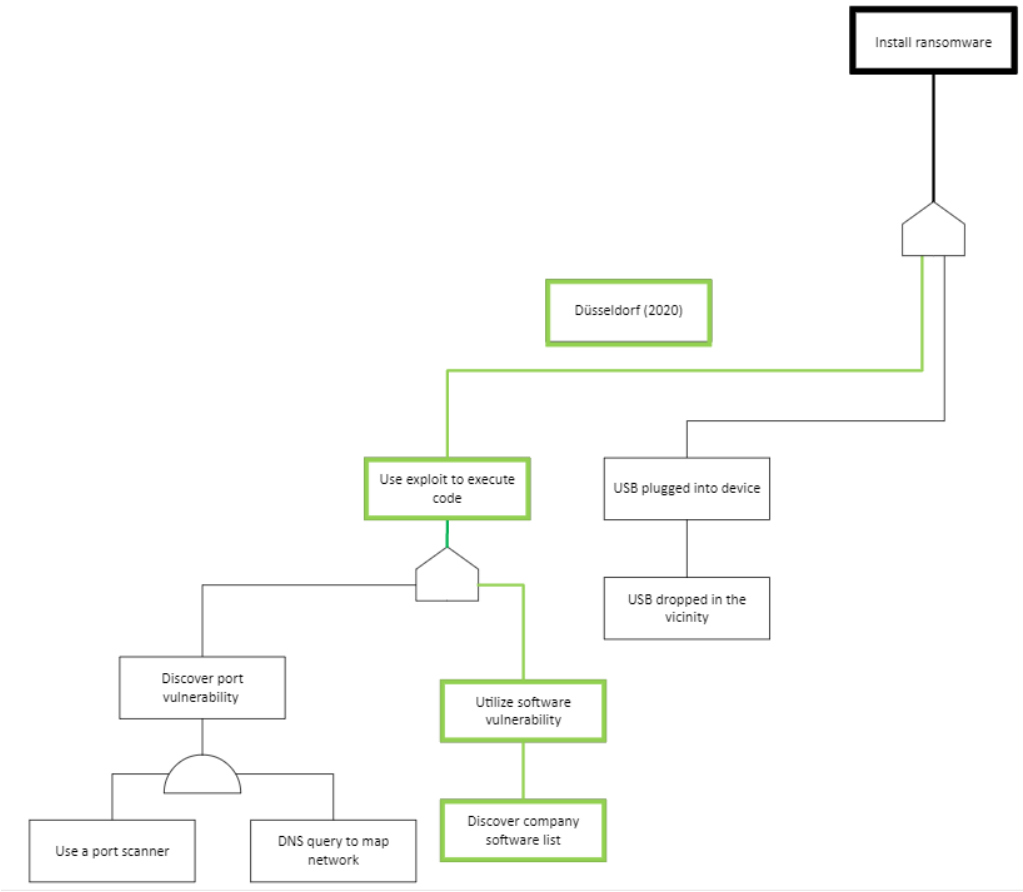


Figure 13: Düsseldorf attack path

The Düsseldorf University Clinic was hit with a ransomware. The attackers breached the systems by exploiting a vulnerability in the Citrix software (CVE-2019-1978) [37]. This exploit let the attacker send malicious requests that would otherwise be filtered. [71].

5.2.4 Vastaamo (Finland, 2018-2021)

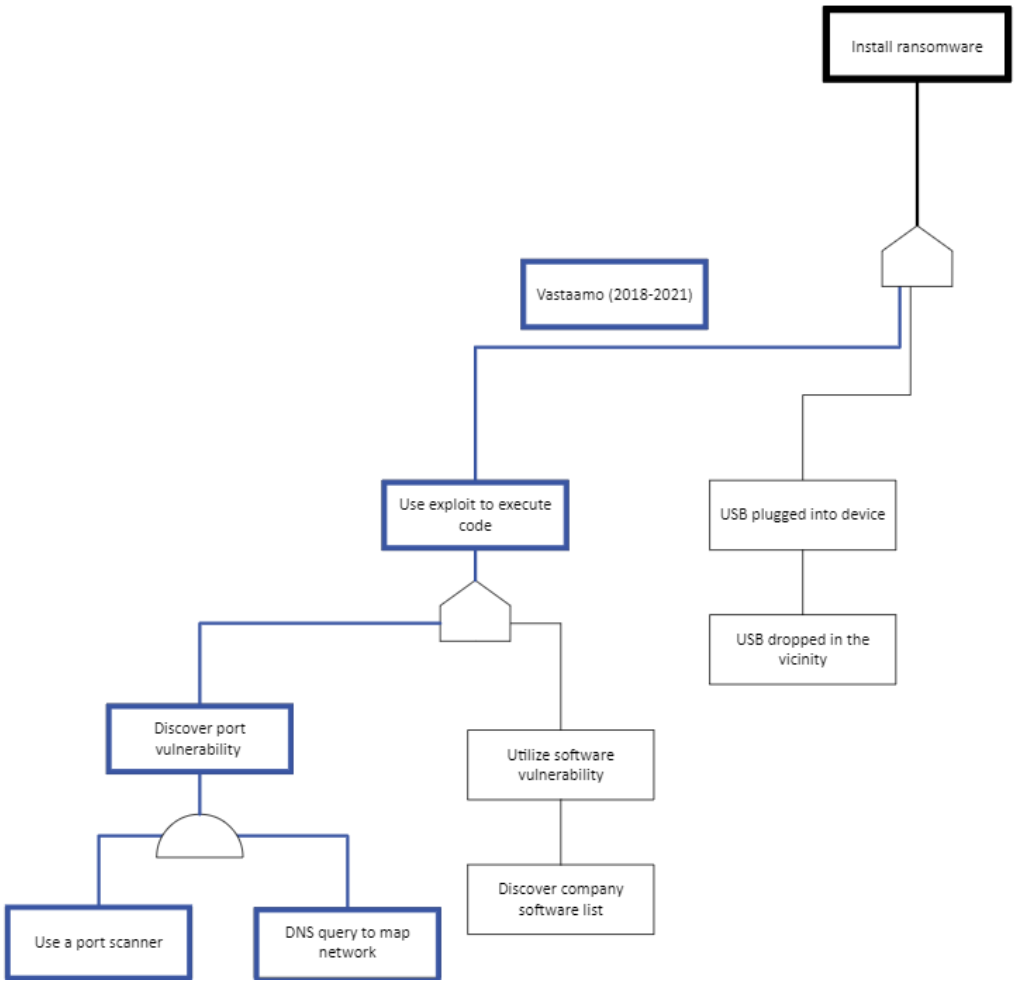


Figure 14: Vastaamo attack path

The Vastaamo data breach was conducted via an open remote access port to the system. As explained in section 2.3.4, administrators created remote access to their servers for easier off-prem administration. Although easier access for the administrators were granted, the rest of the world could also access the systems. Attackers used port scanners to find the the system open for everyone and could easily extract data such as patient journals and upload ransomware on their servers.

5.2.5 Barcelona Hospital (Spain, 2023)

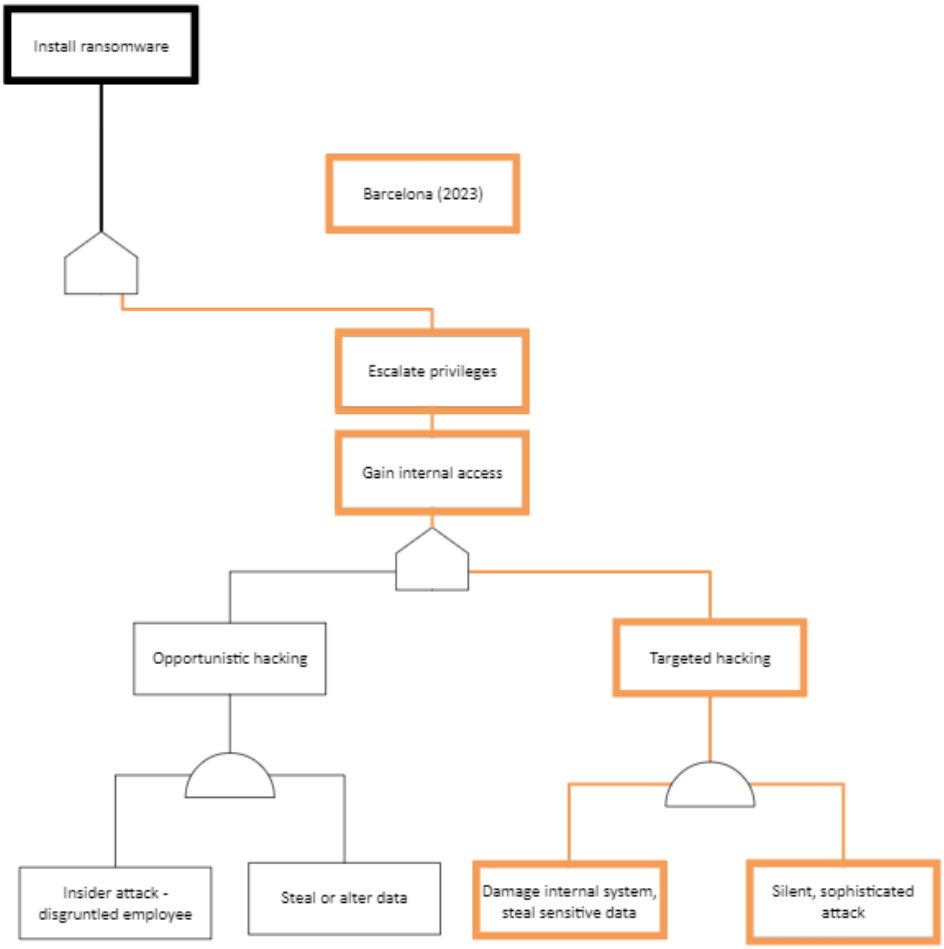


Figure 15: Barcelona attack path

The RansomHouse attack against Barcelona Hospital was a targeted attack. According to Mascellino's [42], the attackers were able to damage the internal systems unseen and were able to escalate their privileges and spread laterally. The attackers were able to install ransomware on their systems, ultimately making the hospital shut down their systems and cancelling medical appoinments.

5.3 Consequences of Ransomware Attacks in the Healthcare Sector

5.3.1 Patient Treatment

Patient treatment in modern hospitals are dependent on multiple systems. The Email correspondence with an information security consultant at ***Ahus*** hospital, showed that they have 28 critical digital systems with class one rating. These systems indicate that they are essential for daily functionality and can affect patient treatment in various degrees if access is lost. The class one ***ICT*** systems for Ahus are listed in table 2. The names of the services are nonpublic information and are replaced with generic names.

Table 2: *Critical (class one) digital systems*

Name	**Description**
System 1	Emergency medical alert system
System 2	Laboratory diagnostics system
System 3	Patient monitoring system
System 4	Certificate service for safe login on pc‘s and journal system
System 5	System for medicinal cancer treatment
System 6	Image processing and cardiological reporting system
System 7	Inventory management system for medicine
System 8	Electronic patient journal system
System 9	Cardiac monitoring system
System 10	Work schedule and competence system
System 11	Personnel and inventory transport system
System 12	Blood management system
System 13	Lab solution for pathology
System 14	Live patient information system
System 15	Maternity ward monitoring system
System 16	Prehospital systems
System 17	Personal security and violence alarm
System 18	Maternity ward maagement system
System 19	Patient alerting system
System 20	Patient signaling system
System 21	Resource and process management system
System 22	Test result transport system
System 23	Radiological information system
System 24	OpSec-Event-Alarm
System 25	Middleware for hematology instruments
System 26	Transport of waste and dirty laundry
System 27	Internal and external telephony services
System 28	Support system for switchboard/call center

The correspondence showed that while these systems are crucial for daily functionality, the most crucial systems have backup procedures in case of downtime occurring. For example, the IT staff must attend a course on how to operate an emergency server in case the clinical staff lose access to system system 8 and/or system 14. Because of these backup procedures the hospital can take care of the critical patients while scheduled routine treatments are put on hold. This solution is not meant for long terms and restoring normal operations of the system must be prioritized.

5.3.2 Patient Security

Consequences to patient security in the event of a ransomware attack varies depending on the scope of the attack and the motive of the attacker. This is apparent when analysing the historical data mentioned throughout this thesis. Depending on the attack, there can be security issues with a patients physical and/or mental well being. Extreme examples of these two factors are; the miss-directed attack on the university clinic in Düsseldorf, Germany 2020 and the repeated attacks against the Finnish psychotherapy service Vastaamo in the period 2018 to 2021. This section is discussing the specific patient security consequences regarding a ransomware attack, meaning how a patients security can be compromised, for example the consequences of a patients critical information being stolen or the consequences of a delayed treatment.

When looking at the case relating to the ransomware attack against the Düsseldorf University clinic [37], [38], there is a series of events; ultimately, leading to the death of a patient in critical treatment. This case serves as an extreme example of how a patients security can be compromised due to delayed treatment as a consequence of a ransomware attack. As displayed in table 2, ***Ahus*** has a list of class 1 critical systems. In the case of a ransomware attack disabling these critical pieces of their infrastructure, much of their capability to care for their patients would be heavily reduced and other unforeseen problematic scenarios could occur. Examples of such scenarios are loss of full patient monitoring, loss of access to patient journals or people getting stuck behind security doors or in elevators. It is safe to assume all healthcare providers included in the scope of this thesis also have similar critical infrastructure, and the denial of access to parts of or the entirety of their infrastructure would likely be catastrophic for the providers ability to care for their patients. These systems are the backbone of their modern healthcare accessibility and effectiveness, and are thus the most important digital assets Ahus to secure.

According to the interview conducted with Ahus (appendix D), the aforementioned results are further reiterated, their main concerns for consequences are partial or full system shutdowns, loss of patient data and compromised data. To counteract these consequences from occurring and minimising their probability Ahus deploys a set of security mechanisms. These include mechanisms mentioned in section 5.3.1, namely system

backups and teaching IT staff how to operate emergency servers in the short term.

Patient mental health is also a considerable concern for patient security. A patient can experience large amounts of stress and anxiety if their personal data is stolen, as was the case during the Vastaamo data breaches [39].

5.3.3 Patient Privacy

Patient privacy is one of the key concerns regarding consequences of a ransomware attack targeting a country's health sector. When considering stolen critical patient data, the malicious intentions of attackers targeting this specific value and the recent developments within the field of cyber crime tactics and the arrival of sophisticated AI, the confidentiality of an individuals personal data is becoming more important to maintain. Specifically, the type of information that is vulnerable to theft in the health sector is a patients journal and health records, which contain sensitive information on a patient.

The historical example of this type of ransomware attack mentioned in this thesis, Vastaamo (2018-2021), serves as an excellent example of how patient security is a massively consequential target for an attacker. The repeated attacks performed, and the amount of patient critical information that was stolen, as well as the way the attacker made use of this data for monetary gain is indicative of the malicious intent of these attacks. The fact that the total amount of data stolen is unknown, and who has access to the information is also unknown is a massive breach of patient confidentiality.

5.3.4 Information Security

Information security is of high importance for the healthcare sectors digital infrastructure, as is apparent from the collected data. This section is based on the conducted interview (section 4.1.2) and the historical research data [39] related to this thesis.

Keeping information related to patients in the health sector secure is important. If a patients private information is stolen in some way from their systems, the potential consequences for the patient are broad. An extreme example of these potential consequences is what the attacker behind the

Vastaamo psychotherapy service attacks (section 2.3.4) did with the patient data that was stolen. The information was used in an attempt to blackmail individual patients for monetary gain, and was also sold on the dark web. The Vastaamo was a psychotherapy service, and thus had information on patients psychological disposition, ailments and treatments. If this type of information regarding a patient were to be publicly available, it can affect these patients opportunities later in life in both social and professional settings. This example strongly argues for why information security is incredibly important to uphold.

Information security is typically upheld by the ***CIA Triad*** as a benchmark. The CIA triad is typically used in relation to ***RVA***, which is used to analyse digital systems and services. For example, CIA is applicable to most of the systems mentioned by the interviewees during the interview (Table 2).

5.3.5 Environment, Health and Safety (EHS)

The impact of a ransomware attack on ***Ahus*** (***EHS***) will have a reduced impact due to the emergency systems already in place. The emergency servers can facilitate their main systems such as system 8 and system 14 which mitigate a significant portion of an attacks ability to disable Ahus services. In regards to the interview (appendix D), environmental damage was not one of the main concerns and was not discussed. Health and safety can become an issue if a prolonged ransomware attack occurs. The attack will result in treatments that have yet to be catalogued in their systems being delayed.

5.3.6 Economy

There are different ways a successful ransomware attack can affect the economy of a hospital. Examples of this are losses from a system downtime, fines from the Norwegian Data Protection Authority and labor related to recovery, administrative tasks and legal actions. A ransomware payment can also be part of the economical losses if the organization chooses to do so. The cost of the ransomware will depend on multiple factors like the type of ransomware, severity of vulnerability, size of the organizations digital infrastructure and the ability to combat the attack. [72]

According to the interview (appendix D) with the senior consultant and

the facility manager from ***Ahus***, the hospital (Ahus) has a fixed budget. This means they will have to combat a possible attack with their own resources/funds.

In 2018 the Norwegian government passed a law regarding ***GDPR*** to protect personal data. The law stated that The Norwegian Data Protection Authority would control and provide guidance about the privacy regulations. Breaching GDPR regulations can lead to fines in various amounts. Table 3 shows examples of the 15 highest fines given from the The Norwegian Data Protection Authority before 20th of March 2023. [73]

Table 3: *The 15 highest fines from The Norwegian Data Protection Authority[74]*

Name	**Fine (*NOK*)**	**Reason**
Grindr	65 000 000	Breach of the requirements for consent in the Personal Data Protection Regulation
Sats ASA	10 000 000	Failing to comply with rights to access and deletion of data. They also lacked authorization to process data about the customers training history
Trumf AS	5 000 000	Anyone could gain access to customers shopping history and there were no verification of account ownership
NAV	5 000 000	NAV published CVs of job seekers on a publicly accessible portal without consent
Ferde AS	5 000 000	The company has illegally transferred personal data about Norwegian drivers to China
Østre Toten Municipality	4 000 000	Sensitive personal data leaked online after an extensive digital attack
Argon Medical Devices	2 500 000	Failed to report personal data breach within deadline of 72 hours
The Storting	2 000 000	Lack of security measures discovered after data breach where personal data was compromised
Asker Municipality	1 000 000	Published confidential personal data and social security numbers on its website
SPK	1 000 000	Collected unnecessary income information about approx. 24 000 people
Innovasjon Norge	1 000 000	Credit assessment without legal reason
St. Olavs hospital	750 000	Lack of access restriction for patient records
Moss Municipality	500 000	Not having secured personal data well enough
BRAbank ASA	400 000	Lack of risk assessment and testing of customer portal for banking services
Høylandet Municipality	400 000	Unsecured pictures of health information

5.3.7 Reputation

The consequences to an institutions reputation after an attack varies depending on the attacks extent. This is not to say that regarding smaller attacks the consequences are small; however, on large scale attacks the consequences greatly exceed those of the smaller variants. According to previously mentioned sources regarding previous attacks, any attack will leave a lasting impact in the populations trust of their healthcare institutions. This refers to examples like the WannaCry attack on the ***NHS*** [32], the more recent attack on the Barcelona hospital [42] and the attack on the psychotherapy service provider Vastaamo [39], [40], [41]. These examples all have a certain impact on the reputation of the respective institutions attacked, due to the data loss and theft of patient data.

If a healthcare institution shows itself to be unable to handle patients personal data, it reflects poorly on the institution and their infrastructure providers. As is previously discussed in section 5.3.6, an attack or breach of patient confidentiality can lead to large fines. This can also lead to a larger lack of funds for the healthcare service in an area, which will further contribute to the consequences to their reputation. This lack of funds and resources will contribute to delays for critical operations and general treatments, which will diminish reputation.

The populous in a region that makes use of a healthcare institution can feel large amounts of anxiety if their personal information is stolen. the resulting blame for this loss of data falls to the healthcare provider, and this will greatly affect their reputation. This can further lead to a larger general mistrust to the digital data security for an entire system, like healthcare in general in a nation or internationally, or a nations other faculties like banks, military or government.

5.3.8 Societal

If the entity of South-Eastern Norway region health authority capacity to operate is reduced due to attacks, it can have an impact on the general populaces health. Attacks that are quickly resolved seem to have little to no impact on the healthcare service as a whole, at least in the case of ***Ahus*** where they have emergency servers for their services. The increasing trend of ransomware attacks in the healthcare sector could have implications, but is yet to prove a significant effect on the overall populace.

6 Discussion

The discussion chapter provides an opportunity to interpret and evaluate findings presented in chapter 5 and discuss critical components relevant to the thesis. This chapter discusses the attack tree relevancy and different unused paths. Lastly, the discussion about consequences of an attack and the recommended measures to mitigate the consequence and probability.

6.1 Attack Tree

The attack tree covers multiple attack scenarios. It covers a wide-variety of known attack paths that are based on previous incidents. Incidents directly from the healthcare sector in addition to known attacks outside the healthcare sector. By only taking into account reported and known attacks from healthcare sector, the attack tree would neglect plausible attacks that are less common, but still bring dire consequences. It is a deliberate choice as the cost of implementing measures is significantly less costly than reacting after an incident has been discovered.

6.1.1 Attack Tree Usefulness

The use case for attack tree is primarily penetration testing, to test a system's security. Due to the generalist nature of the attack tree it is difficult to utilize without adding values to each node. The usefulness of an attack tree is found in accessing the security of a system, which is created when the cost and probability is added. The attack trees value thus lies in its function as a versatile base for attacks in the healthcare sector.

To add cost and probability to each step one would need data from previous incidents, and a certain understanding of the system being tested. It is beneficial to have analytic tools to detect vulnerabilities in the system such as a "***Nessus***" scan. The Nessus tool [6] as an example can scan infrastructure for ***CVEs***, which then can be used to assess the probability of the system security being breached. Most of these tools require administrator privileges, and the output often contain sensitive information to the system, thus are difficult to procure as an outsider.

6.1.2 Potential Unused Paths

As shown in figure 10, the attack tree currently has some paths that are not covered by existing attacks that have been described. In this section, the unused paths such as ***USB** drop attack* 5.1.2 and *Opportunistic hacking* 5.1.4.1 will be discussed, explaining both previous attacks and discussing why they were implemented in the final attack tree.

6.1.2.1 USB Drop Attack

Although the attack method is not common among cyber attackers, the ***USB*** drop attack is a possible attack method to be vary of. This method is less prevalent than other techniques such as phishing emails and port scanning, primarily due to the challenges posed in planting a USB stick outside a target business and having it be retrieved and inserted into a computer. As unlikely as it seem, there have been cases where the attack method worked out.

According to Lynn's article [60], there was a case where the *US Department of Defense* classified military computer networks were compromised. A flash drive containing "malicious computer code" was allegedly placed there by a foreign intelligence agency. The virus spread through both classified and unclassified systems, and data was transferred to servers owned by foreign countries. The incident solidifies the need for organizations to be vigilant against a broad range of potential attack vectors, including the less common USB drop attack.

6.1.2.2 User is Compromised

The *user is compromised* node consists of two different child nodes; *blackmail employee for credentials* and *credentials bought on the dark web*. The node subsequently leading to the installation of malware since the user has clicked a malicious link. Although there are billion pairs [66] of credentials listed for sale on the dark web, the group were not able to find any cases aimed towards hospitals from the research.

The attack does not seem unlikely, however. Although not found in research, the attack is likely because there it is probable that the attackers can purchase credentials linked to an employee's work email address for

instance. This way the user is compromised and the attackers are able to forward malicious links to other users without the employee being aware of it.

6.1.2.3 Opportunistic Hacking

The group were not able to find any reports of this attack type aimed towards the healthcare sector. Usually opportunistic hackers are disgruntled employees that want to cause harm to their workplace while they still have access rights [68]. Opportunistic attacks are unusual and unlikely, because there are human factors that affect the attacker. While the disgruntled employee think about trying to defame or weaken the hospital they work at, they can have second thoughts since it will likely bring more consequences than gain. An operation can be jeopardized as a result of the attack conducted by the disgruntled employee. This can bring fatal consequences since the operation cannot be completed. There is reason to believe, that this is why the attack has not occurred towards any hospitals.

6.2 Consequences and Recommended Measures

The consequences of an attack described in section 5.3 are critical for healthcare providers to avoid. This is due to the effect a consequence can bring on their ability to provide patient treatment, ensure patient security and privacy, uphold their information security, their ***EHS***, economy, reputation and societal availability. These consequences are tightly connected to a healthcare providers ability to perform ***RVA*** [75] and their understanding of benchmarks like the ***CIA Triad***.

6.2.1 Measures for identified attack tree paths

Table 4: *Identified attack vectors and recommended proactive measures to reduce the attacks probability*

Risk (PR)	**Probability Measures**
Probability risk 1: Vulnerable port	• Keeping software security mechanisms updated or patched • ACL/firewall • Penetration testing
Probability risk 2: Software vulnerability	• Keeping software security mechanisms updated or patched • ACL/firewall • Penetration testing
Probability risk 3: USB drop attack	• General information security training • USB port disabling
Probability risk 4: Compromised user	• Two-factor authentication • The principle of least privilege
Probability risk 5: Phishing email	• General information security training • Implementing anti-malware software • ACL/firewall • Penetration testing
Probability risk 6: Opportunistic hacking	• Keeping software security mechanisms updated or patched • Active directory • The principle of least privilege

Probability risk 7: Targeted hacking	• Keeping software security mechanisms updated or patched • ACL/firewall • RVA • Two-factor authentication

6.2.1.1 Discussing Measures to Attack Vectors

Probability measure 1: General information security training

Affected risks: PR3, PR5

Description:
General information security training should include an IT course once employed, and having recurring courses to keep employees up to date with current technologies. This should encompass all employees not just the IT employees.

Effect:
The organisation should maintain a level of IT competence to reduce the probability of an attack occurring. The recurring courses should increase awareness of IT security, due to the ever increasing social engineering attacks it is crucial to reduce the probability of human error. [76]

Probability measure 2: Keeping software security mechanisms updated or patched

Affected risks: PR1, PR2, PR6, PR7

Description:
Software vendors frequently update their software if there is known vulnerabilities or bugs. It should be noted that this does not apply without exception as the vendor can drop support in favor of other products, or the vendor ceasing operations. A faulty and non-secure software service that is not updated is dangerous for a business and threat actors can exploit this.

Effect:
Old security software, not up to date with the latest malware trends, cannot keep a business safe. Updating the software security mechanisms when an update releases will lower the probability of an attack.

Probability measure 3: Implementing anti-malware software

Affected risks: PR5

Description:
Anti-malware is able to detect, warn and respond to malware on a device. Anti-malware is generally able to scan all files and documents in a full system scan. Background scanning is another type of scan, scanning files that are opened from the back end providing real time feedback. [77]

Effect:
Anti-malware prevents malware attacks and warns user of suspicious files or programs reducing the probability of attacks occurring. It preemptively blocks known viruses, which filters common attacks. [78]

Adding multiple anti-malware software to different systems can improve IT security. This widens the range of detectable malware, and reduces the probability, however two anti-malware services should not run at the same time as the software will cause conflict. [78]

Probability measure 4: ACL/firewall

Affected risks: PR1, PR2, PR5, PR7

Description:
Access Control List (***ACL***) can be used to help defend the network. ACL can permit or deny network traffic from reaching areas in the network. A firewall has more capabilities and is able to examine incoming and outgoing network traffic to determine whether or not to let the traffic through.

Effect:
ACL and firewalls are able to keep foreign devices with unknown ***IP*** addresses away from the network. ACLs will deny the attackers path into the network. Firewalls are also able to limit spam emails, but the end-user should still be vary of spam and phishing attempts. Denying the attack-

ers path into the network by using ACLs, and limit their ability to send spam and phishing attempts with firewalls are great measures to reduce the probability of an attack

Probability measure 5: Active directory

Affected risks: PR6

Description:
Active Directory or *Active Directory Domain Services* (***AD DS***) [79] is a system that store data on a company's network. The data stored on the network ranges from information about user accounts to phone numbers linked to each user. The system has integrated security through logon and access control. The system uses role-based access control which makes it easier for an administrator to set rules for each role and connect the role to users. An administrator can, for example, restrict access for users across the network to active directory objects, such as phone numbers and other user accounts. This gives the administrators better overview and it enhances the security.

Effect:
The Active Directory Domain System give opportunities to defend against cyber attackers. It can highly reduce the probability of success with few, easy steps. Implementing strong password policies makes the passwords much harder to guess. Regularly forced password changes should also be implemented. Another measure is to implement roles that divide the normal users from the administrative users. The normal users should be able to carry out their normal work while the security is still implemented. They should not have access to objects that are not relevant to their day-to-day activities.

Probability measure 6: RVA

Affected risks: PR7

Description:
RVA [75] is a type of assessment used to gauge risk factors and finding measures to counteract these risks. It typically contain a case description, risk identification (with assets, threats and vulnerabilities), risk analysis

and recommended measures. The goal of a RVA is to reduce risks to an acceptable level through the identified measures.

Effect:
Risk and vulnerability significantly decreases the probability of a successful attack by enabling an organization to identify weaknesses in existing security measures and help with gaining knowledge to understand potential threats and vulnerabilities. Organizations can, for example discover software with vulnerabilities and take steps to patch or update the software.

Probability measure 7: Penetration testing

Affected risks: PR1, PR2, PR5

Description:
Penetration testing is way to assess the security of a system. During a penetration test an authorised hacker will attempt to gain control over a system. The purpose of this test is to discover vulnerabilities in the system or network. The goal of a penetration test is to be able to improve the security of the network or system [80].

Effect:
Penetration testing identifies security shortcomings helping the organization adjust their security measures, effectively reducing the probability and consequences by addressing the shortcomings. The penetration testing simulates a realistic threat, and is an invaluable opportunity for the organization to test their systems and network. [80]

Probability measure 8: Two-factor authentication

Affected risks: PR4, PR7

Description:
Two-factor authentication is an authentication mechanism where two different factors are need to authorize user login. Factors can be divided into three groups. *Knowledge*, what the user knows, such as a username and password pair. *Possession*, something the user owns, such as a keycard or bank code chip. *Inherence*, relies on intrinsic and characteristic features,

such as fingerprint, facial feature, or voice. [81]

The factors combined are utilized to determine the identity of the user, and only using one factor exposes weaknesses in the security of a system.

Effect:
Two-factor authentication limits access to a user account by only allowing access to a user with multiple factors. Restricting access to identities with multiple factors will reduce the probability of an unauthorized attacker seizing control of a user account.

Following the Norwegian National Security Authority's (***NSM***) principles of ***ICT*** security section 2.6, it is necessary to have an overview of identities and access rights [82]. NSM further recommends two-factor authentication to significantly increase security [83].

Probability measure 9: USB-port disabling

Affected risks: PR3

Description:
USB-ports should be disabled [84] when attempting to mitigate the risk of an attack with USB devices such as flash drives. Disabling USB-ports is an easy measure to implement and is not costly. An administrator can easily implement USB-port blocking in a network by using group policies.

Effect:
Blocking USB-ports in an organizations network will reduce the probability of an attack. Although not as common as other attacks, the USB drop attack, described in section 5.1.2 is still something to be vary of. It also makes it impossible for employees to use personal flash drives, which should be prevented.

Probability measure 10: The principle of least privilege

Affected risks: PR4, PR6

Description:
The principle of least privilege [85] refers to reducing an employees accessibility in the system to only what is necessary for them to perform

their work, and not permitting them access to parts of the system they have no reason to access. This is a hierarchical approach to access control that only allows a small group of user accounts to access critical portions of the system.

Effect:
Least privilege is tied to active directory and is important to reduce the probability of an attack. There is a smaller amount of vulnerable accounts that can be compromised, and the account holders are much less likely to fall victim to social engineering tactics. If an attacker takes control of a user that has minimal privileges the attacker does not have the chance to do much damage inside the hospital network. Furthermore, permitting regular users to infrastructure is critically flawed and should be avoided at all cost. A user can change or destroy something they should not.

6.2.2 Consequence Measures

Table 5: *Identified consequences and recommended proactive measures to reduce their consequence*

Risk (CR)	**Consequence Measures**
Consequence risk 1: Critical system failure due to ransomware	• The principle of least privilege • Backup Strategy • RVA • Performing penetration tests • Ransomware playbook
Consequence risk 2: Loss of backup data due to ransomware	• Backup strategy

Consequence risk 3: Patient treatment compromised due to ransomware	• Backup strategy • RVA • Ransomware playbook • Emergency procedures in case of downtime on clinical treatment systems
Consequence risk 4: Patient privacy compromised due to ransomware	• Backup strategy • RVA • Ransomware playbook • Implementing data encryption
Consequence risk 5: Lowered EHS due to ransomware	• Backup strategy • RVA • Ransomware playbook
Consequence risk 6: GDPR Breach	• Implementing data encryption • Design infrastructure based on GDPR recommendations • Review and update data protection policies
Consequence risk 7: Recovery cost after successful ransomware attack	• Backup strategy • Ransomware playbook • Implementing data encryption • Basing infrastructure design choices on GDPR recommendations

Consequence risk 8: Reputation consequences due to ransomware attack	• Ransomware playbook • Implementing data encryption • Design infrastructure based on GDPR recommendations • Review and update data protection policies • Being transparent with collaborators and providing regular updates • Communicating with third party providers for insight
Consequence risk 9: Loss of trust in the healthcare services' ability to uphold patient privacy	• Being transparent with collaborators and providing regular updates • Performing positive PR to alleviate population anxiety
Consequence risk 10: General lower healthcare availability in a region due to ransomware attack	• Being transparent with collaborators and providing regular updates • Public relation plan

6.2.2.1 Discussing Consequences Measures

Consequence measure 1: The principle of least privilege

Affected risks: CR1

Description:
Please see description in probability measure 10.

Effect:
This approach reduces the consequences of an attack. The consequences are reduced because usually any administrative accounts have access to different domains within the infrastructure, meaning that if one domain

was compromised, the entire system would not be at risk. This is accounting for the fact that the attacker has not gained access to meta information retaining to accounts in the system. Any system or domain administrator should also only make use of a non-administrative account when there is no reason to make use of their administrative privilege.

Consequence measure 2: Backup strategy

Affected risks: CR1, CR2, CR3, CR4, CR5, CR7

Description:
A backup strategy [86] aims to create periodic copies of a system in the event of an attack or issue in the system. This copy can then be deployed to restore the system to a previous state either before the attack was executed or the issue occurred. There are 3 types of backups, full backups, incremental backups and differential backups. Full backups copies all data in a system. Incremental backups copies the changed data after the previous full backup. Differential backups can be used as a substitute for full and incremental backups. Examples of such strategies are backup and restore, or the 3-2-1 backup plan [87].

Effect:
The effect a backup strategy has when reducing consequence is extensive, as it reduces the consequences of most of the technical risks that can be present. With an effective backup strategy the downtime of the system would be reduced, the monetary and time cost of an attack would be reduced and the probability of a patients treatment being postponed is reduced.

Consequence measure 3: RVA

Affected risks: CR1, CR3, CR4, CR5

Description:
An ***RVA*** [75] is a type of assessment used to gauge risk factors and finding measures to counteract these risks. They typically contain a case description, risk identification (with assets, threats and vulnerabilities), risk analysis and recommended measures. The goal of a RVA is to mitigate risks to an acceptable level through the identified measures.

Effect:
If the result of a performed ***RVA*** have been applied and the measures taken from these results have mitigated identified risk factors, then a successful attack would have a reduced consequence, as previous vulnerabilities have had their consequence reduced.

Consequence measure 4: Performing penetration tests

Affected risks: CR1

Description:
Penetration testing is way to assess the security of a system. During a penetration test an authorised hacker will attempt to gain control over a system. The purpose of this test is to discover vulnerabilities in the system or network. The goal of a penetration test is to be able to improve the security of the network or system [80].

Effect:
Penetration testing yields information about vulnerabilities in the system being tested, and these results are used to mitigate the effect of probability and consequences. Although penetration testing primarily mitigates probability factors, consequences can also be mitigated as a result of the penetration testing. The results of the test can improve the overall security of a system by, for example, highlighting vulnerabilities within user accounts management, active directory management or inconsistencies in the system relating to the principle of least privilege.

Consequence measure 5: Ransomware ***playbook***

Affected risks: CR1, CR3, CR4, CR5, CR7, CR8

Description:
As described in the ***glossary*** entry for playbooks, a playbook [8] is an incident management plan that describes proactive and reactive measures to perform in the case of a attack scenario, which typically contains steps to take when under attack. These steps are preparation, identification, containment, remediation, and recovery; however, a playbook is not locked to these rigid frames. There are differences between all playbooks depending on the attack scenario it is intended for and who is responsible for

planning the playbook.

Effect:
By making use of a playbook for a scenario, the consequence of said scenario is greatly reduced. Streamlining the process of incident management will reduce downtime and confusion surrounding the attack. Factors such as media and third party communications are more effectively handled by using the playbook. A playbook typically also contains several different methods for handling a scenario, which makes it more likely that the playbook is effective in handling an incident.

Consequence measure 6: Emergency procedures in case of downtime on clinical treatment systems

Affected risks: CR3

Description:
As mentioned in 5.3.1, ***Ahus*** have emergency procedures in case of downtime on some of the class one critical digital systems. The IT staff is trained to handle digital emergency situations, which can affect daily functionality regarding patient treatment.

Effect:
Being too reliant on digital systems for situations where critical patients are in danger is associated with high-risk. Having these emergency procedures are crucial for the hospital ability to reliably treat patients. This solution is not meant for long terms and restoring normal operations of the system must be prioritized. Choosing which systems there should be emergency procedures for, should be evaluated by the ability too treat patients without said system.

Consequence measure 7: Implementing data encryption

Affected risks: CR4, CR6, CR7, CR8

Description:
Data encryption is a process of encoding information into another form or code. Only people with the decryption key can access the information in a readable format. There are two types of encryption that is imple-

mented in modern systems. There is symmetric which uses the same key for encryption and decryption. This is a fast method and is suitable for encrypting large amounts of data but the security is not optimal. Asymmetrical encryption uses two keys and is safer, but it is slower for encryption/decryption operations. This makes it suitable for digital signatures and symmetric key exchange. [88]

Effect:
Encrypting sensitive data will reduce the consequence of an attacker successfully gaining access to the systems. The attacker will not be able to understand the sensitive information which is encrypted.

Consequence measure 8: Design infrastructure based on GDPR recommendations

Affected risks: CR6, CR7, CR8

Description:
Designing an infrastructure based on ***GDPR*** recommendation refers to following any relevant key issues found on Intersoft consulting's official website regarding GDPR [89]. This website lists all of the recommended actions or policies to implement in order to follow GDPR such as data encryption, personal data management, privacy etc.

Effect:
Following recommended GDPR guidelines will result in an effective policy for upholding the confidentiality of personal data retaining to patients. This will result in a higher degree of privacy for patients regarding their data, and makes it more difficult for an attacker to access their personal information. Following GDPR recommendations also lowers the possibility of being fined, and any fines that are handed out are likely to be lower than if GDPR is not implemented. Implementing GDPR also serves to implement other measures mentioned in this thesis, e.g. ***measure 7*** and ***measure 9***.

Consequence measure 9: Review and update data protection policies

Affected risks: CR6, CR8

Description:
Reviewing and updating data protection policies refers to performing research on proper data protection policies provided by official sources like ***GDPR*** [89] or any cyber security provider.

Effect:
Performing this type of evaluation of the data protection policies in place allows for vulnerabilities or issues with the current policies in place to be found. These can then be rectified if possible, or changed for a better system.

Consequence measure 10: Being transparent with collaborators and providing regular updates

Affected risks: CR8, CR9, CR10

Description:
Transparency is important when performing risk assessment and incident management [8], as being untruthful only negatively affects whomever is under attack. If the victim is unwilling to cooperate when being supported in dealing with an attack, or chooses to lie to either media or authorities, then the attack will be harder to deal with, the consequences of the attack can become more severe and this will lead to any fines handed out being larger.

Effect:
As mentioned in the description, not being transparent with collaborators and not providing regular updates will only lead to problems for the victim of an attack. Being transparent with media can reduce consequences to reputation. Keeping the media informed about progress with the attack shows active care about solving the problem. Being transparent with the authorities will lead to support solving the problem and shows that the attack is taken seriously.

Consequence measure 11: Communicating with third party providers for insight

Affected risks: CR9, CR10

Description:
When handling an attack, usually external insight or support is employed to deal with the attack. The contact logs for these resources are usually specified in a playbook [8]. Examples of these third party providers are incident management specialists, lawyers, media handlers, digital forensics specialists, negotiations agent etc.

Effect:
Communicating with third party providers when handling an issue is an important part of incident management. In order to repel an attack or repair a damaged system, there is a need for varied competence and ability. As exemplified in the description, there are different tasks that the victims of an attack cannot be suited to handle by themselves, and are thus in need of further contracted expertise. Making use of this will allow the target to remediate their system, reputation and losses more effectively. This will result in lower downtime, lower overall loss in time and money and faster ability to start treating patients again at the healthcare providers normal capacity.

Consequence measure 12: Public relation plan

Affected risks: CR9, CR10

Description:
When a ransomware occurs, there needs to be communication between the organization and the public. The communication should start early to give the public some information about the situation, without giving attackers insight which can be used against the hospital. The plan for public relations handling should be clear before the ransomware attack takes place. [90]

Effect:
A well formulated public relation plan can decrease negative reputation from a ransomware attack as the plan manages the public perception of the organization.

6.3 Ransomware's effect on QALY

As explained in section 2.3.5, ***QALY*** is a measurement of a patient's estimated physical living condition for a period of time. An attack can affect a patient's condition due to either delayed treatments, theft of personal data that affect their future prospects, or loss of data in the healthcare providers systems relating to a patients QALY score.

If a treatment is delayed due to a ransomware attack, a patient could possibly experience a worsening condition that affects their overall QALY score by reducing their utility due to the delayed treatment. This would lead to an overall worse health for the patient's remaining lifespan if the condition is bad enough, or could even result in the death of a patient.

A patient's mental scoring for QALY would be affected if a patients critical data were to be stolen. The patient could experience heightened anxiety as a result or lose their current prospects/ their future prospects as a result of stolen data, which would result in an overall reduction in their QALY score. Mental disorders can be developed due to the patients mental degradation as a result of anxiety or distress.

The QALY score for patients can become inconsistent or inaccurate as a consequence of data loss due to a ransomware attack. This becomes an issue, as more time and cost would be invested into QALY assessment of patients, which in turn could result in a general delay in treatment of all patients.

7 Conclusion

This chapter concludes the project and the topics covered in this thesis, including the implications of said topics. The conclusion consists of topics such as, group results, alternative possibilities, future work and group evaluation.

7.1 Group Results

This thesis initially set out to complete a set of result goals and effect goals, as described in section 1.2.3.

The result goals were completed to an extent, as their scope were somewhat inconsistent with the wishes of the thesis provider. This thesis evaluates and informs about crypto virus attacks and hidden consequences, discusses and suggests effective measures to prevent and avoid attacks. It also identifies causes, avenues and effects of an attack, and provides effective countermeasures against them. The result goals also includes a goal relating to performing a risk assessment based on crypto virus attacks in the health sector, however this ended up falling outside of the scope of the thesis. Instead recommended measures are based on identified risks, however the thesis does not include typical ***RVA*** formatting for vulnerabilities, assets, threats and risk tables or a risk matrix.

The effect goals decided for this thesis are met to completion. The work performed to complete this thesis has provided a greater general knowledge about crypto viruses for the participants. The research put into this thesis will be put to use by the thesis provider to perform further research relating to digital attacks towards the health sector. The thesis also serves to spread awareness of crypto virus attacks in the healthcare sector, which will reduce the probability and consequence of eventual attacks.

7.2 Alternative Possibilities

Throughout the development process of the thesis there have been some minor issues. Issues that for future work can be prevented by making a few changes to methods and planning. The group did not find a method or model that suited the specific type of thesis and the main focus was to follow the Gantt schema created at the start of the project period. The

Gantt schema can be found in appendix ref. As shown there are not specific activities, but the activities are general and the duration is longer than preferred. Modifying the schema with a different structure is a better alternative possibility. Tying the Gantt schema to a specific development model or method is something that could have prevented the minor issue.

Although the group did not use a specific development process model, the group was still satisfied with the time allocated to most of the main points of the project. However, there were a few issues with conducting the interview. This was an issue that could have been prevented. Firstly, the process of scheduling the interview was a hassle. The group tried to schedule the interview, but the interviewees were not as available as the group had hoped. It took several weeks to find a vacant time slot for all the parties involved. Secondly, the interview did not give all the answers the group hoped for. The time allocated for the interview did become longer than initially expected. By making the interviewees allocate a vacant time slot, the interview could have been conducted earlier and the time allocation issue could have be prevented. Although the interview was satisfactory, the group could have sent some questions prior to the interview, this way the interviewees could have given even better answers.

7.3 Future Work

Regarding future work possibilities relating to the subject of this thesis, there are a few different recommendations. These are either applicable for other theses in the future, or more limited research into specific subjects.

This thesis recommends further research into the subject of ***QALY***. QALY is related to the healthcare sector and is a vast topic with relatively vast access to information found open source, however there are some areas where private sources may be useful. This type of task is well suited for a thesis intended for students within the healthcare sector, however it may be possible to rework the basis of the task for students in IT.

Another recommended issue that may require further work is the initial task of the thesis itself, or some adjacent version of the basis. Technology is rapidly advancing, and both security mechanisms and threat actors both continuously attempt win ground against each other. This suggests that after a certain amount of time, there will be new cases of ransomware attacks using unknown attack vectors and causing unforeseen con-

sequences. By performing a rendition of this thesis at a later time, these cases would be covered.

Regarding the attack tree, this can be improved by adding weighted probability and cost in order to increase the practicality of the attack tree diagram. In order to improve the attack tress practicality, sensitive information of the systems is needed. A better understanding of the systems enables one to detect and expose more attack vectors.

7.4 Evaluation of the Group's Work

The group concludes that both the process of developing this thesis and the team working throughout the semester has been solid. The group has performed well when working together and are proud of their results regarding this thesis. The group has primarily worked together in person which has contributed to a greater collaborative effort from its members. The groups members have all improved throughout this thesis, both in terms of competence within the relevant fields of study and working in a team. By using scrum and referring to the established Gantt schema, the group has been effective with developing this thesis. Quality assurance has been performed regularly, which helped in keeping everything written uniform and has contributed in all group members becoming better writers. This allowed the group to assure that the quality of what every member wrote was adequate for this thesis. In total, the groups members are in agreement that the amount of working hours spent on this thesis is sufficient and the result is reflective of the members skill, knowledge and ability.

7.5 Final words

We are content with the result of this thesis and what we have achieved. This opportunity has let the team contribute to cyber security in the healthcare sector. Working on this project has given the team knowledge and valuable experiences.

Lastly, we want to thank Ahus for the provided thesis task, their contribution and their cooperation.

Bibliography

[1] IAHPC Pallipedia. *Catchment area*. URL: https://pallipedia.org/catchment-area/ (visited on 3rd May 2023).

[2] Kim Fenrich. *Securing Your Control System*. URL: https://www.proquest.com/trade-journals/securing-your-control-system/docview/221083013/se-2?accountid=12870 (visited on 1st May 2023).

[3] NIST. *Cryptocurrency*. URL: https://csrc.nist.gov/glossary/term/cryptocurrency (visited on 10th May 2023).

[4] Google. *Classification: True vs. False and Positive vs. Negative*. URL: https://developers.google.com/machine-learning/crash-course/classification/true-false-positive-negative (visited on 3rd May 2023).

[5] GERDhelp. *GERD Health-Related Quality of Life (GERD-HRQL) Questionnaire*. URL: https://www.gerdhelp.com/wp-content/uploads/2018/03/GERD-HRQL-PPI-Risks-download-Eng-NP02165-01D.pdf (visited on 16th May 2023).

[6] Tenable. *Nessus*. URL: https://www.tenable.com/products/nessus (visited on 5th May 2023).

[7] Groden M., Kreiswirth M. and Szeman I. *Johns Hopkins Guide for Literary Theory and Criticism*. Johns Hopkins University Press, 2005.

[8] Cyril Onwubiko and Karim Ouazzane. 'SOTER: A Playbook for Cybersecurity Incident Management'. In: *IEEE Transactions on Engineering Management* 69.6 (2022), pp. 3771–3791. DOI: 10.1109/TEM.2020.2979832.

[9] Gavin Wright. *Scientific Method*. URL: https://www.techtarget.com/whatis/definition/scientific-method (visited on 3rd May 2023).

[10] Scrum. *What is scrum*. URL: https://www.scrum.org/resources/what-is-scrum (visited on 31st Jan. 2023).

[11] Broadcom. *Difference between viruses, worms, and trojans*. URL: https://knowledge.broadcom.com/external/article?legacyId=tech98539 (visited on 11th May 2023).

[12] Adobe Communications Team. *Waterfall Methodology: A Complete Guide*. URL: https://business.adobe.com/blog/basics/waterfall (visited on 3rd May 2023).

[13] Ahus. *Akershus University Hospital*. URL: https://www.ahus.no/akershus-university-hospital (visited on 19th Jan. 2023).

[14] Advisory. *24.4M patients, 21 companies now say they were affected by AMCA data breach*. URL: https://www.advisory.com/daily-briefing/2019/08/13/data-breach (visited on 23rd Jan. 2023).

[15] Collier. R. *NHS ransomware attack spreads worldwide*. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5461132/ (visited on 23rd Jan. 2023).

[16] Milmo. D. *NHS ransomware attack: what happened and how bad is it?* URL: https://www.theguardian.com/technology/2022/aug/11/nhs-ransomware-attack-what-happened-and-how-bad-is-it (visited on 23rd Jan. 2023).

[17] Lakeworks. *File:Scrum process.svg*. URL: https://commons.wikimedia.org/wiki/File:Scrum_process.svg (visited on 26th Jan. 2023).

[18] NCSC UK. *A guide to ransomware*. URL: https://www.ncsc.gov.uk/ransomware/home (visited on 17th Feb. 2023).

[19] Hilde Martinsen. *Ransomware - Hva er det og hvordan unngår du det på bedriftens enheter?* URL: https://www.telenor.no/bedrift/blogg/sikkerhet/ransomware (visited on 21st Feb. 2023).

[20] Lockheed Martin. *The Cyber Kill Chain*. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (visited on 20th Feb. 2023).

[21] Pratik Dholakiya. *What Is the Cyber Kill Chain and How It Can Protect Against Attacks*. URL: https://www.computer.org/publications/tech-news/trends/what-is-the-cyber-kill-chain-and-how-it-can-protect-against-attacks (visited on 20th Feb. 2023).

[22] Crowdstrike. *What is the Cyber Kill Chain?* URL: https://www.crowdstrike.com/cybersecurity-101/cyber-kill-chain/ (visited on 20th Feb. 2023).

[23] Mary E. Shacklett. *attack vector*. URL: https://www.techtarget.com/searchsecurity/definition/attack-vector (visited on 20th Feb. 2023).

[24] *CVE*. 2023. URL: https://www.cvedetails.com/ (visited on 20th Feb. 2023).

[25] Trendmicro. *Zero-Day Vulnerability*. URL: https://www.trendmicro.com/vinfo/us/security/definition/zero-day-vulnerability (visited on 20th Feb. 2023).

[26] Pablo L. Gallegos-Segovia et al. *Social engineering as an attack vector for ransomware*. 2017. DOI: 10.1109/CHILECON.2017.8229528.

[27] Sushruth Venkatesha, K. Rahul Reddy and B. R. Chandavarkar. *Social Engineering Attacks During the COVID-19 Pandemic*. DOI: 10.1007/s42979-020-00443-1. URL: https://doi.org/10.1007/s42979-020-00443-1 (visited on 21st Feb. 2023).

[28] Tom Burt. *Microsoft report shows increasing sophistication of cyber threats*. URL: https://blogs.microsoft.com/on-the-issues/2020/09/29/microsoft-digital-defense-report-cyber-threats/ (visited on 10th May 2023).

[29] Vaishnavi Bhavsar, Aditya Kadlak and Shabnam Sharma. 'Study on Phishing Attacks'. In: *Int. J. Comput. Appl* 182 (2018), pp. 27–29.

[30] Malwarebytes. *Hacking*. URL: https://www.malwarebytes.com/hacker (visited on 27th Feb. 2023).

[31] UNext Editorial Team. *Types Of Hackers Based On Their Intent | Who Are Ethical Hackers?* URL: https://u-next.com/blogs/cyber-security/different-types-of-hackers/ (visited on 27th Feb. 2023).

[32] S. Ghafur et al. 'A retrospective impact analysis of the WannaCry cyberattack on the NHS'. eng. In: *NPJ digital medicine* 2.1 (2019), pp. 98–98. ISSN: 2398-6352. DOI: https://doi.org/10.1038/s41746-019-0161-6.

[33] Ondřej Filipec and David Plášilb. 'THE CYBERSECURITY OF HEALTHCARE The Case of the Benešov Hospital Hit by Ryuk Ransomware, and Lessons Learned'. eng. In: *Obrana a strategie* 21.1 (2021), pp. 27–51. ISSN: 1214-6463.

[34] BENEŠOV HOSPITAL. *Výroční zpráva Nemocnice Rudolfa a Stefanie Benešov.*

[35] Martin Shabu. *Ukliknutí „stálo" nemocnici v Benešově 40 milionů. Kyberútok začal otevřením přílohy*. URL: https://www.lidovky.cz/domov/ukliknuti-stalo-nemocnici-v-benesove-40-milionu-kyberutok-zacal-kliknutim-na-prilohu.A200115_201359_ln_domov_vlh (visited on 29th July 2020).

[36] Adam Kujawa. *Ryuk ransomware attacks businesses over the holidays*. URL: https://www.malwarebytes.com/blog/news/2019/01/ryuk-ransomware-attacks-businesses-over-the-holidays (visited on 27th Feb. 2023).

[37] 'Ransomware claims first fatality as healthcare under renewed assault'. eng. In: *Computer fraud & security* 2020.10 (2020), pp. 1, 3–1, 3. ISSN: 1361-3723.

[38] Hannah T. Neprash et al. 'Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021'. eng. In: 3.12 (2022), e224873–e224873. ISSN: 2689-0186.

[39] Nir Kshetri and Jeffrey Voas. 'Ransomware: Pay to play?' In: *Computer* 55.03 (2022), pp. 11–13.

[40] Kave Noori. *A case study of Vastaamo, the hacked psychotherapy app*. URL: https://dpforum.se/npa2022-a-case-study-of-vastaamo-the-hacked-psychotherapy-app/ (visited on 6th Mar. 2023).

[41] Hilary Tuttle. 'Ransomware Attackers Turn to Double Extortion'. eng. In: 68 (2021), pp. 8–9.

[42] Alessandro Mascellino. *Ransomware attack against Barcelona hospital disrupts operations*. URL: https://www.infosecurity-magazine.com/news/ransomhouse-target-barcelona/ (visited on 23rd Mar. 2023).

[43] National Institute for Health and care Excellence. *Quality-adjusted life year*. URL: https://www.nice.org.uk/glossary?letter=q (visited on 20th Feb. 2023).

[44] Prieto L and Sacristán JA. *Problems and solutions in calculating quality-adjusted life years (QALYs)*. *Health Qual Life Outcomes*. DOI: 10.1186/1477-7525-1-80. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC317370/ (visited on 15th May 2023).

[45] Andrea Fontana and James H Frey. 'The interview'. In: *The Sage handbook of qualitative research* 3 (2005), pp. 695–727.

[46] Cint. *What Is a Questionnaire and How Is It Used in Research?* URL: https://www.cint.com/blog/what-is-a-questionnaire-and-how-is-it-used-in-research (visited on 28th Apr. 2023).

[47] Isograph. *Attack Tree Modeling in AttackTree*. URL: https://www.isograph.com/software/attacktree/creating-an-attack-tree/ (visited on 20th Feb. 2023).

[48] B. Schneier. 'Attack trees'. eng. In: *Dr. Dobb's Journal* 24.12 (1999), pp. 21–29. ISSN: 1044-789X.

[49] Alastair Ruddle et al. *Security requirements for automotive on-board networks based on dark-side scenarios*. URL: https://zenodo.org/record/1188418#.Y_inhXbMI2w (visited on 24th Feb. 2023).

[50] Constantine Boussalis. *Basic Survey Theory and Design*. URL: http://hnmcp.law.harvard.edu/wp-content/uploads/2012/02/Constantine-Boussalis-Training-on-Basic-Survey-Theory-and-Design.pdf (visited on 20th Apr. 2023).

[51] Saul Mcleod. *Questionnaire: Definition, Examples, Design And Types*. URL: https://www.simplypsychology.org/questionnaires.html (visited on 25th Apr. 2023).

[52] Chandan Kumar. *10 Port Scanner Tools for Advanced Scanning by Network Administrators*. URL: https://geekflare.com/port-scanner-tools/ (visited on 10th Apr. 2023).

[53] NIST. *CVE-2017-0143 Detail*. URL: https://nvd.nist.gov/vuln/detail/CVE-2017-0143 (visited on 10th Apr. 2023).

[54] Dirk Schrader. *Open port vulnerabilities list*. URL: https://blog.netwrix.com/2022/08/04/open-port-vulnerabilities-list/ (visited on 13th Apr. 2023).

[55] Andy Greenberg. *The First BlueKeep Mass Hacking Is Finally Here—but Don't Panic*. URL: https://www.wired.com/story/bluekeep-hacking-cryptocurrency-mining/ (visited on 2nd May 2023).

[56] Microsoft. *Remote Desktop Services Remote Code Execution Vulnerability*. URL: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2019-0708 (visited on 13th Apr. 2023).

[57] Hazim Hanif et al. 'The rise of software vulnerability: Taxonomy of software vulnerabilities detection and machine learning approaches'. eng. In: *Journal of network and computer applications* (2021), p. 103009. ISSN: 1084-8045.

[58] Min-Seok Pang and Hüseyin Tanriverdi. 'Strategic roles of IT modernization and cloud migration in reducing cybersecurity risks of organizations: The case of U.S. federal government'. eng. In: *The journal of strategic information systems* 31.1 (2022), p. 101707. ISSN: 0963-8687.

[59] Matthew Tischer et al. 'Users Really Do Plug in USB Drives They Find'. eng. In: *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2016, pp. 306–319. ISBN: 1509008241.

[60] William J. Lynn III. *Defending a new domain*. URL: https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain (visited on 20th Apr. 2023).

[61] James P. Farwell and Rafal Rohozinski. 'Stuxnet and the Future of Cyber War'. eng. In: *Survival (London)* 53.1 (2011), pp. 23–40. ISSN: 0039-6338.

[62] CISA. *Mariposa Botnet*. URL: https://www.cisa.gov/news-events/ics-advisories/icsa-10-090-01 (visited on 20th Apr. 2023).

[63] Gregory Hale. *ICS alert: usb malware attack*. URL: https://www.isssource.com/ics-alert-usb-malware-attack/n (visited on 20th Apr. 2023).

[64] NRK. *Norske sykehus trues av russiske hackergrupper*. URL: https://www.nrk.no/norge/norske-sykehus-trues-av-russiske-hackergrupper-1.16275175 (visited on 20th Apr. 2023).

[65] Beatrice M. Cerda and Shengli Yuan. 'A Study of Anti-Phising Methodologies and Phishing Detection Algorithms'. eng. In: *Proceedings of the International Conference on Security and Management (SAM)*. Athens: The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2019, pp. 79–83.

[66] Brandon Viglialoro. *There are 24.6 billion pairs of credentials for sale on dark web*. URL: https://www.theregister.com/2022/06/20/in_brief_security/ (visited on 25th Apr. 2023).

[67] Daniel Iwugo. *What is RTLO in Hacking? How to Use Right-to-Left Override and Defend Against it*. URL: https://www.freecodecamp.org/news/rtlo-in-hacking/ (visited on 27th Apr. 2023).

[68] Ekran System. *Opportunistic Attackers: Who Are They and How Can You Deter Them?* URL: https://www.ekransystem.com/en/blog/opportunistic-insiders (visited on 13th Apr. 2023).

[69] Trend Micro. *Understanding Targeted Attacks: What is a Targeted Attack?* URL: https://www.trendmicro.com/vinfo/no/security/news/cyber-attacks/understanding-targeted-attacks-what-is-a-targeted-attack (visited on 13th Apr. 2023).

[70] Derrick Rountree. *Privilege Escalation*. URL: https://www.sciencedirect.com/topics/computer-science/privilege-escalation (visited on 13th Apr. 2023).

[71] NIST. *CVE-2019-1978 detail*. URL: https://nvd.nist.gov/vuln/detail/CVE-2019-1978 (visited on 4th May 2023).

[72] Tyler Chancey. *How Much Ransomware Recovery Really Cost?s*. URL: https://www.scarlettcybersecurity.com/how-much-ransomware-recovery-really-cost (visited on 12th May 2023).

[73] Arild Aspøy. *Datatilsynet*. URL: https://snl.no/Datatilsynet (visited on 1st May 2023).

[74] Anders Svensson and Jan Ove Skogheim. *15 største GDPR bøter vedtatt av Datatilsynet i Norge*. URL: https://gdprcontrol.no/gdpr-boter-norge/ (visited on 1st May 2023).

[75] Niru Nirupama. 'Risk and vulnerability assessment: a comprehensive approach'. In: *International Journal of Disaster Resilience in the Built Environment* 3.2 (2012), pp. 103–114.

[76] Ron Torten, Carmen Reaiche and Stephen Boyle. 'The impact of security awarness on information technology professionals' behavior'. eng. In: *Computers & security* 79 (2018), pp. 68–79. ISSN: 0167-4048.

[77] Nishant Patnaik. 'The Best Antivirus, Antimalware Solution for Home Owners And Corporates'. eng. In: *International journal of advanced research in computer science* 6.7 (2015). ISSN: 0976-5697.

[78] NIST. *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*. URL: https://csrc.nist.gov/publications/detail/sp/800-83/rev-1/final (visited on 15th May 2023).

[79] Microsoft. *Active Directory Domain Services*. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview (visited on 14th May 2023).

[80] Yaroslav Stefinko, Andrian Piskozub and Roman Banakh. 'Manual and automated penetration testing. Benefits and drawbacks. Modern tendency'. In: *2016 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET)* (2016), pp. 488–491.

[81] Karola Marky et al. '"Nah, it's just annoying!" A Deep Dive into User Perceptions of Two-Factor Authentication'. eng. In: *ACM transactions on computer-human interaction* 29.5 (2022), pp. 1–32. ISSN: 1073-0516.

[82] Nasjonal sikkerhetsmyndighet. *NSMs Grunnprinsipper for IKT-sikkerhet versjon 2.0*. 2020. URL: https://nsm.no/getfile.php/133735-1592917067/Filer/Dokumenter/Veiledere/nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf (visited on 14th May 2023).

[83] Nasjonal sikkerhetsmyndighet. *Råd og anbefalinger om passord*. 2019. URL: https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/rad-og-anbefalinger-om-passord (visited on 14th May 2023).

[84] Currentware. *How to disable USB ports and block USB mass storage*. URL: https://www.currentware.com/blog/how-to-disable-usb-ports/ (visited on 15th May 2023).

[85] Microsoft Corporation. 'Implementing Least-Privilege Administrative Models'. In: (). Ed. by Microsoft Corporation. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models (visited on 13th May 2023).

[86] Adam Marget. 'Backup Strategy: What It Is and How to Create One'. In: (). URL: https://www.unitrends.com/blog/backup-strategy (visited on 13th May 2023).

[87] Fredrik Magnusson. *Implementing a Backup-Scheme with the 3-2-1 Strategy: A Comparison of the Active Solution with a New Implemented 3-2-1 Backup-Scheme*. URL: https://www.diva-portal.org/smash/record.jsf?pid=diva2%5C%3A1246434%5C&dswid=722 (visited on 13th May 2023).

[88] Datatilsynet. *Data encryption*. URL: https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/data-encryption/ (visited on 14th May 2023).

[89] *Key Issues*. https://gdpr-info.eu/issues/. Accessed: 2023-05-14.

[90] Lyndsi Stevens. *The Rise Of Ransomware: What Communication Executives Need To Know*. URL: https://www.forbes.com/sites/forbescommunicationscouncil/2021/09/08/the-rise-of-ransomware-what-communication-executives-need-to-know/?sh=61b54d4e1a5b (visited on 15th May 2023).

Appendix

A Standardavtale

NTNU
Norges teknisk-naturvitenskapelige universitet

Fastsatt av prorektor for utdanning 10.12.2020

STANDARDAVTALE

om utføring av studentoppgave i samarbeid med ekstern virksomhet

Avtalen er ufravikelig for studentoppgaver (heretter oppgave) ved NTNU som utføres i samarbeid med ekstern virksomhet.

Forklaring av begrep

Opphavsrett
Er den rett som den som skaper et åndsverk har til å fremstille eksemplar av åndsverket og gjøre det tilgjengelig for allmennheten. Et åndsverk kan være et litterært, vitenskapelig eller kunstnerisk verk. En studentoppgave vil være et åndsverk.

Eiendomsrett til resultater
Betyr at den som eier resultatene bestemmer over disse. Utgangspunktet er at studenten eier resultatene fra sitt studentarbeid. Studenten kan også overføre eiendomsretten til den eksterne virksomheten.

Bruksrett til resultater
Den som eier resultatene kan gi andre en rett til å bruke resultatene, f.eks. at studenten gir NTNU og den eksterne virksomheten rett til å bruke resultatene fra studentoppgaven i deres virksomhet.

Prosjektbakgrunn
Det partene i avtalen har med seg inn i prosjektet, dvs. som vedkommende eier eller har rettigheter til fra før og som brukes i det videre arbeidet med studentoppgaven. Dette kan også være materiale som tredjepersoner (som ikke er part i avtalen) har rettigheter til.

Utsatt offentliggjøring
Betyr at oppgaven ikke blir tilgjengelig for allmennheten før etter en viss tid, f.eks. før etter tre år. Da vil det kun være veileder ved NTNU, sensorene og den eksterne virksomheten som har tilgang til studentarbeidet de tre første årene etter at studentarbeidet er innlevert.

1. Avtaleparter

Norges teknisk-naturvitenskapelige universitet (NTNU) Institutt for informasjonssikkerhet og kommunikasjonsteknologi
Veileder ved NTNU: E-post og tlf.
Ekstern virksomhet: Akershus universitetssykehus HF Ekstern virksomhet sin kontaktperson, e-post og tlf.: 1. Kåre Magne Stennes, kamste@ahus.no, 90083520 2. Espen Thorsen Frank, Espen.Thorsen.Frank@ahus.no, 95487688
Student: Jørgen Lillehagen Myrvold Fødselsdato: 22. august 1999
Student: Jonas Brumoen Nessø Fødselsdato: 10. september 1992
Student: Steinar Mjøs Myhre Fødselsdato: 01. Oktober 2001
Student: Sindre Hiis-Hauge Fødselsdato: 30. juni 1996

Partene har ansvar for å klarere eventuelle immaterielle rettigheter som studenten, NTNU, den eksterne eller tredjeperson (som ikke er part i avtalen) har til prosjektbakgrunn før bruk i forbindelse med utførelse av oppgaven. Eierskap til prosjektbakgrunn skal fremgå av eget vedlegg til avtalen der dette kan ha betydning for utførelse av oppgaven.

2. Utførelse av oppgave

Studenten skal utføre: (sett kryss)

Masteroppgave	
Bacheloroppgave	x
Prosjektoppgave	
Annen oppgave	

Startdato: 09. januar 2023
Sluttdato: 22. mai 2023

Oppgavens arbeidstittel er: AHUS - kryptovirus

Ansvarlig veileder ved NTNU har det overordnede faglige ansvaret for utforming og godkjenning av prosjektbeskrivelse og studentens læring.

3. Ekstern virksomhet sine plikter

Ekstern virksomhet skal stille med en kontaktperson som har nødvendig faglig kompetanse til å gi studenten tilstrekkelig veiledning i samarbeid med veileder ved NTNU. Ekstern kontaktperson fremgår i punkt 1.

Formålet med oppgaven er studentarbeid. Oppgaven utføres som ledd i studiet. Studenten skal ikke motta lønn eller lignende godtgjørelse fra den eksterne for studentarbeidet. Utgifter knyttet til gjennomføring av oppgaven skal dekkes av den eksterne. Aktuelle utgifter kan for eksempel være reiser, materialer for bygging av prototyp, innkjøp av prøver, tester på lab, kjemikalier. Studenten skal klarere dekning av utgifter med ekstern virksomhet på forhånd.

Ekstern virksomhet skal dekke følgende utgifter til utførelse av oppgaven: **Ingen utgifter er avtalt for denne oppgaven.**

Dekning av utgifter til annet enn det som er oppført her avgjøres av den eksterne underveis i arbeidet.

4. Studentens rettigheter

Studenten har opphavsrett til oppgaven[1]. Alle resultater av oppgaven, skapt av studenten alene gjennom arbeidet med oppgaven, eies av studenten med de begrensninger som følger av punkt 5, 6 og 7 nedenfor. Eiendomsretten til resultatene overføres til ekstern virksomhet hvis punkt 5 b er avkrysset eller for tilfelle som i punkt 6 (overføring ved patenterbare oppfinnelser).

I henhold til lov om opphavsrett til åndsverk beholder alltid studenten de ideelle rettigheter til eget åndsverk, dvs. retten til navngivelse og vern mot krenkende bruk.

Studenten har rett til å inngå egen avtale med NTNU om publisering av sin oppgave i NTNUs institusjonelle arkiv på Internett (NTNU Open). Studenten har også rett til å publisere oppgaven eller deler av den i andre sammenhenger dersom det ikke i denne avtalen er avtalt begrensninger i adgangen til å publisere, jf. punkt 8.

5. Den eksterne virksomheten sine rettigheter

Der oppgaven bygger på, eller videreutvikler materiale og/eller metoder (prosjektbakgrunn) som eies av den eksterne, eies prosjektbakgrunnen fortsatt av den eksterne. Hvis studenten skal utnytte resultater som inkluderer den eksterne sin prosjektbakgrunn, forutsetter dette at det er inngått egen avtale om dette mellom studenten og den eksterne virksomheten.

[1] Jf. Lov om opphavsrett til åndsverk mv. av 15.06.2018 § 1

Alternativ a) (sett kryss) Hovedregel

X	Ekstern virksomhet skal ha bruksrett til resultatene av oppgaven

Dette innebærer at ekstern virksomhet skal ha rett til å benytte resultatene av oppgaven i egen virksomhet. Retten er ikke-eksklusiv.

Alternativ b) (sett kryss) Unntak

	Ekstern virksomhet skal ha eiendomsretten til resultatene av oppgaven og studentens bidrag i ekstern virksomhet sitt prosjekt

Begrunnelse for at ekstern virksomhet har behov for å få overført eiendomsrett til resultatene:

6. Godtgjøring ved patenterbare oppfinnelser

Dersom studenten i forbindelse med utførelsen av oppgaven har nådd frem til en patenterbar oppfinnelse, enten alene eller sammen med andre, kan den eksterne kreve retten til oppfinnelsen overført til seg. Dette forutsetter at utnyttelsen av oppfinnelsen faller inn under den eksterne sitt virksomhetsområde. I så fall har studenten krav på rimelig godtgjøring. Godtgjøringen skal fastsettes i samsvar med arbeidstakeroppfinnelsesloven § 7. Fristbestemmelsene i § 7 gis tilsvarende anvendelse.

7. NTNU sine rettigheter

De innleverte filer av oppgaven med vedlegg, som er nødvendig for sensur og arkivering ved NTNU, tilhører NTNU. NTNU får en vederlagsfri bruksrett til resultatene av oppgaven, inkludert vedlegg til denne, og kan benytte dette til undervisnings- og forskningsformål med de eventuelle begrensninger som fremgår i punkt 8.

8. Utsatt offentliggjøring

Hovedregelen er at studentoppgaver skal være offentlige.

Sett kryss

X	Oppgaven skal være offentlig

I særlige tilfeller kan partene bli enige om at hele eller deler av oppgaven skal være undergitt utsatt offentliggjøring i maksimalt tre år. Hvis oppgaven unntas fra offentliggjøring, vil den kun være tilgjengelig for student, ekstern virksomhet og veileder i

denne perioden. Sensurkomiteen vil ha tilgang til oppgaven i forbindelse med sensur. Student, veileder og sensorer har taushetsplikt om innhold som er unntatt offentliggjøring.

Oppgaven skal være underlagt utsatt offentliggjøring i (sett kryss hvis dette er aktuelt):

Sett kryss		Sett dato
	ett år	
	to år	
	tre år	

Behovet for utsatt offentliggjøring er begrunnet ut fra følgende:

Dersom partene, etter at oppgaven er ferdig, blir enig om at det ikke er behov for utsatt offentliggjøring, kan dette endres. I så fall skal dette avtales skriftlig.

Vedlegg til oppgaven kan unntas ut over tre år etter forespørsel fra ekstern virksomhet. NTNU (ved instituttet) og student skal godta dette hvis den eksterne har saklig grunn for å be om at et eller flere vedlegg unntas. Ekstern virksomhet må sende forespørsel før oppgaven leveres.

De delene av oppgaven som ikke er undergitt utsatt offentliggjøring, kan publiseres i NTNUs institusjonelle arkiv, jf. punkt 4, siste avsnitt. Selv om oppgaven er undergitt utsatt offentliggjøring, skal ekstern virksomhet legge til rette for at studenten kan benytte hele eller deler av oppgaven i forbindelse med jobbsøknader samt videreføring i et master- eller doktorgradsarbeid.

9. Generelt

Denne avtalen skal ha gyldighet foran andre avtaler som er eller blir opprettet mellom to av partene som er nevnt ovenfor. Dersom student og ekstern virksomhet skal inngå avtale om konfidensialitet om det som studenten får kjennskap til i eller gjennom den eksterne virksomheten, kan NTNUs standardmal for konfidensialitetsavtale benyttes.

Den eksterne sin egen konfidensialitetsavtale, eventuell konfidensialitetsavtale den eksterne har inngått i samarbeidprosjekter, kan også brukes forutsatt at den ikke inneholder punkter i motstrid med denne avtalen (om rettigheter, offentliggjøring mm). Dersom det likevel viser seg at det er motstrid, skal NTNUs standardavtale om utføring av studentoppgave gå foran. Eventuell avtale om konfidensialitet skal vedlegges denne avtalen.

Eventuell uenighet som følge av denne avtalen skal søkes løst ved forhandlinger. Hvis dette ikke fører frem, er partene enige om at tvisten avgjøres ved voldgift i henhold til norsk lov. Tvisten avgjøres av sorenskriveren ved Sør-Trøndelag tingrett eller den han/hun oppnevner.

Denne avtale er signert i fire eksemplarer hvor partene skal ha hvert sitt eksemplar. Avtalen er gyldig når den er underskrevet av NTNU v/instituttleder.

Signaturer:

Instituttleder: Dato:
Veileder ved NTNU: [signature] Dato: 26. JANUAR 2023
Ekstern virksomhet: Ahus v/ Kåre M. Stennes Dato: 25. januar 2023
Student: Jørgen L. Myrvold Dato: 26. januar 2023
Student: Steinar M. Myhre Dato: 26 januar 2023
Student: Sindre His-Haugen Dato: 26. Januar 2023
Student: Jonas Brumoen Nesse Dato: 27 Januar 2023

B Project plan

NTNU
Kunnskap for en bedre verden

FACULTY OF INFORMATION TECHNOLOGY AND ELECTRICAL ENGINEERING

DCSG2900 - BACHELOROPPGAVE BACHELOR I DIGITAL INFRASTRUKTUR OG CYBERSIKKERHET

Project plan for Bachelor Thesis Kryptovirus - Ahus

Authors:
Sindre Hiis-Hauge
Steinar Mjøs Myhre
Jonas Brumoen Nessø
Jørgen Lillehagen Myrvold

27-01-2023

Table of Contents

List of Figures

List of Tables

Glossary

AHUS - Akershus Universitetssykehus

ALARP - As low as reasonably practicable

AMCA - American Medical Collection Agency

NHS - National Health Service

QALY - Quality-Adjusted Life Year

1 Introduction

This section of the project plan introduces the key factors behind the thesis such as the background, the goals as well as specifications.

1.1 Background

The project plan is made for a bachelor thesis proposed by Akerhus Universitetssykehus (Ahus).

Ahus is owned by Southern and Eastern Norway Regional Health Authority, the largest RHA in the country. Ahus main tasks are patient treatment, research, teaching and patient education. The hospital is responsible for about 560 000 inhabitants. Ahus stretches across the southeast of Norway and have 12 000 employees across regions such as Follo, Romerike and Kongsvinger. They also cover the northernmost parts of Oslo; Alna, Grorud and Stovner. [1]

In recent years there has been an increase in digital attacks, with a plethora of intentions, different attacker groups with differing levels of knowledge. All digital solutions that any business uses are vulnerable to an attack. This increase in activity has prompted Ahus to present this thesis for NTNU for a bachelors thesis, among other measures. Specifically, Ahus wishes for this thesis to be part of its research with the intention of evaluating consequences of cyber attacks on the clinical field (namely, patient treatment). Ahus also wants to know what effect an attack could potentially have on a patients quality-adjusted life year (QALY) related to their treatments, and to consider and discuss effective countermeasures for these kinds of cyber attacks.

1.2 Project Goals

Our goals for this project is divided in result goals and effect goals. Result goals are tied to the product of this project. The project leader owns the result goals and is responsible for reaching these goals. Effect goals are tied to the long term impact and benefits for the client. [2]

Result Goals

- Evaluate and inform the healthcare sector about crypto virus attacks and the hidden consequences.
- Discuss and suggest effective measures to prevent and avoid attacks.
- Perform a risk assessment based on crypto virus attacks aimed towards the health sector, with a focus on ramifications that may affect patients.
- Identifying causes for attacks, avenues for attack, effects an attack may have on the victim, and effective countermeasures against attacks.

Effect Goals

- Acquire a greater general knowledge about crypto viruses.
- The research performed in this thesis to be used in further research relating to digital attacks towards the health sector.
- Spread awareness of crypto virus attacks in the healthcare sector to reduce the consequence of an eventual attack.

1.3 Specifications

The bachelor thesis consists of a study in the consequences of crypto virus attacks aimed towards the healthcare sector.
The project period is set between 9th of January and 22nd of May. At the end of the period the group has to finish and deliver the report.

2 Scope

This section specifies the scope of the thesis itself. This which includes the main issue that the thesis is relevant to, a description of the task, as well as the limitations the group has decided on for how broad of an area the thesis will cover.

2.1 Main Issue

The study will focus on crypto virus attacks in the healthcare sector. This is due to an increase in cyber attacks in recent years as mentioned in Section 1.1. Examples of these types of detrimental attacks are; the AMCA data breach of 2019 [3], the NHS ransomware attack on May 12th 2017 [4] and the more recent NHS ransomware attack August 4th 2022 [5].

Considering the massive attack on AMCA as well as the repeated successful attacks on the NHS, the first of which further affected over 200 000 machines in 150 countries, meaning that cyber criminals represent a danger that must be taken seriously. This also displays that there is always a big uncertainty with digitally hosted services, as there are likely vulnerabilities in its infrastructure that can be heavily exploited. All anyone can do about it is to be as smart and knowledgeable about different attack vectors as possible, particularly social engineering (phishing, identity theft etc.). These are the more common attack vectors used towards the healthcare sector.

With all this in mind, this thesis sets out to answer the following; What are the reasons, goals and attack vectors an attacker makes use of when targeting the healthcare sector, and what kind of consequences can these attacks have for the patients under its care?

2.2 Task Description

The task description specifies that the group will discover the direct consequences of crypto virus attack for clinical activity such as; QALY, privacy, HMS and economy. While assessing preventive measures to prevent and avoid future attacks. In addition, the group is tasked with creating an attack tree diagram to further study the steps in the attacking process. Outside of this, the group is free to interpret the contents of the thesis themselves.

2.3 Main Issue Limitations

The project is mainly limited to crypto virus attacks against the healthcare sector. This excludes other forms of attack. The issue will also be limited to western countries, so that the focus can be related more towards incidents that are relevant to Ahus when discussing cause, agendas, potential targets and consequences.

3 Project Organization

This section specifies several elements of the inner workings for the bachelor group. This includes the different responsibilities of each participant, the distribution of roles in the group, as well as routines and rules for the collaborative work. The group has decided to divide responsibilities and roles between the members. The roles, their distribution and the role responsibilities are specified in the subsections below.

3.1 Roles

Team Leader	Jørgen
Meeting planner	Jonas
Archivist	Sindre
Generalist	Steinar

Table 1: *Table containing information retaining to roles*

3.2 Responsibilities

Team Leader

- General overview of project
- Making sure deadlines are met
- Resolving potential problems within the group
- Primary communication with thesis provider

Meeting Planner

- Planning meetings for group activities
- Booking rooms
- Planning meeting with Thesis provider

Archivist

- Organizing documents
- Keeping track of uploads, and general documentation
- Gathering notes for minutes document

Generalist

- General contribution in all aspects retaining to the thesis
- Filling in for other roles whenever necessary
- Responsible for quality control

3.3 Group Rules

The group has defined a set of rules that each member has agreed with and intend to uphold. Descriptions of consequences for both general rule breaking and specific cases are defined under repercussions (Section 3.5).

Rules relating to general group workflow:

- Every group member is responsible for making the work environment a positive space for collaboration.
- Every group member is responsible for doing their share of the work.
- Every group member is responsible for supporting other group members with their work, given that they fall behind. This is the primary job of the Generalist, and secondary to other roles.
- Breaks during a work session are encouraged. Every member has the right to 10 minutes of break time every working hour and a 30 minutes break for sessions exceeding 5 hours.

Rules relating to meetings:

- Every group member is expected to be present for all meetings.
- If a group member or other participant is absent for a meeting, they are expected to give a 24-hour notice.
- If a group member is delayed past 15 minutes to a planned meeting, they are obligated to bring a snack for the group to share.
- If a group member is both absent and without a 24-hour notice, they are obligated to order food for a work-session.
    - If any health issues occur within the 24-hour notice period, an exception will be made.
    - If any unexpected serious non-health issues occur within the 24-hour notice, an exception will be made.

3.4 Routines

The group has a static schedule for Wednesday, Thursday and Friday. Every Wednesday at 11:00, the group will meet the supervisor for feedback and guidance. Thursday and Fridays are designated workdays when the group comes together on campus and work on the project. Monday and Tuesday are more flexible and designated for working digitally.

3.5 Repercussions

All breaches of the rules will be taken seriously throughout the project period. Although, some of the repercussions will vary based on the severity. Smaller breaches will result in a verbal warning. This should not effect the groups workflow. Bigger breaches or repetitive smaller breaches, should be taken more seriously. If the verbal warning within the group did not help, the group will consult their NTNU supervisor. Bigger breaches of the rules which could jeopardize the project, have to be resolved. The team leader is responsible for de-escalation and will communicate with the NTNU supervisor and the NTNU course coordinator if needed.

4 Planning, Follow-up and Reporting

This section explains the general plan for the thesis. This includes the process of writing the project plan, doing research, processing the information gained from the research and developing an understanding for the issue. The goal is to provide a thesis that uphold the goals and results requested by the thesis provider.

The process described above equates to what kind of development cycle the group selects. This is with the purpose of writing a complete thesis based on collected data and performed procedures for documentation.

4.1 Development Cycle

Methodology
For this given thesis when contemplating what sort of development cycle would be most fitting, the group decided on using Scrum. Scrum is a framework for developing and sustaining complex products. Scrum utilizes the team structure to get work done in small pieces at a time. [6]
While Scrum is primarily utilized in developing a product, it can also be adjusted to work with a bachelor thesis. Scrum is an agile methodology and can be adjusted if needed. The short sprints are also perfect for our thesis. Altogether, the thesis seem big and unreachable, but the sprints enables a step by step approach. Therefore, the group figured it would be the most suitable methodology.

Roll Distribution
The group has decided to divide the roles for scrum according to the scrum distribution standard. This specifies a Scrum master, developers and product owners. Jørgen is designated the Scrum master role, the rest of the group members are developers. The product owner is a mix of both our thesis provider, Ahus and NTNU.

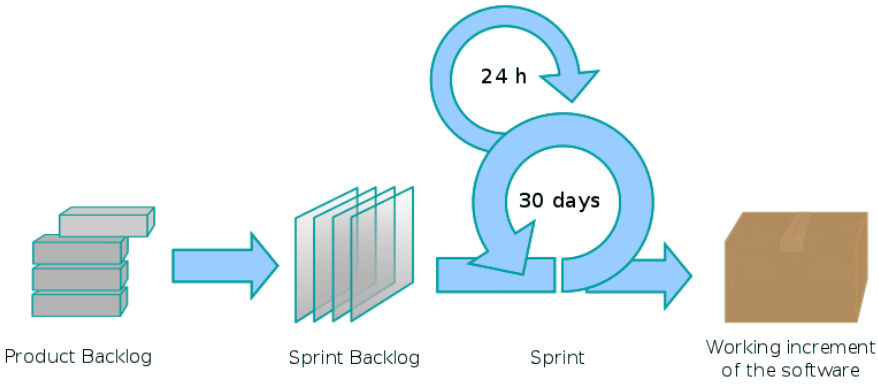


Figure 1: The process of scrumming. [7]

4.2 Plan for Status Meetings and Decision-making

The group will have continuous meetings with the NTNU supervisor. The meetings are scheduled every Wednesday at 11:00. The meetings are flexible and could be rescheduled if needed. The main purpose is to get feedback and ask questions. In the case of absence, the meetings can be rescheduled or cancelled. Furthermore, the meeting could be rescheduled to either Thursday or Friday within the time frame 11:00 to 16:30.

Meetings with the thesis provider, Ahus will be conducted every 14^{th} day. The meetings are scheduled to be on Tuesdays at 12:30. They will mainly consist of presenting what has been done since the last meeting. In the case of absence, the meetings can be rescheduled or cancelled. Furthermore, the meeting could be rescheduled to a later time the same day, if not then on Wednesday after the meeting with the supervisor. If this is not possible, the meeting will be postponed to the next week.

5 Organization Quality Assurance

5.1 Documentation Standards and Tools

Microsoft Teams will be used to get a general overview during the project period. It is mainly a communication platform between the group and the NTNU supervisor. Teams will also be used to arrange work sessions and meetings within the group. The Teams channel will be used to share and store some documents, like "Standardavtale", meeting minutes, time lists and Gantt schema. Meetings with our thesis provider will be held on Zoom. Email is the main communication platform between the group and the thesis provider.

Throughout the project period the group will use Overleaf as the main document writing tool. It is an easy approach, as we are able to share the document with our supervisor. This enables a better way for the group to get feedback throughout the project period. Overleaf has a history function which allows us to roll back to older versions.

Quick Notes from meetings will be shared in a private Discord channel between the group members, other notes such as questions directed to our supervisor will also be shared here. Discord allows for easy access voice channels where the group will conduct their online work sessions.

5.2 Plans for Quality Assurance

Assurance and Policy
In order to have effective quality assurance, there needs to be defined a set of quality assurance policies that serve the most optimal course of action when undertaking the thesis.

- The group will allocate time at the end of each work week to assess the quality of research, reviews, revisions etc.
- The group will thoroughly fact check any information in order to verify information integrity through multiple sources.
- The group will make use of several review methods in order to verify the integrity of any written notes, reviews, research, revisions etc.
- The group will continuously and rigorously follow the specified procedures of the quality assurance policies during the entire time frame dispensed for work on the thesis.

Quality Review
During the execution of this thesis, the group will make use of different forms of reviewing methods in order to both develop a high quality thesis and define key elements in its development. These review methods are self reviews, peer reviews and external reviews. Specifically, self reviews will be done continuously during the thesis. The peer reviews will be done as part of the collaborative effort in the group as well as inputs from the NTNU supervisor. The external reviews will primarily be done in collaboration with the thesis provider in regards to research and making sure that the group stays on the right track. Other parties may be privy to information discussed in the thesis and will thus be used for the same purpose.

Data Collection
Collection of data and information will be conducted through primarily research and study. Data collection will also be performed through interviews, discussions with the thesis provider and NTNU supervisor, and some other yet to be explicitly defined methods.

5.3 Risk assessment in relation to the project itself

Risk is an important factor to consider when working on big projects. Even small incidents can cause problems over time. This can lead to bigger problems over time and create friction in the group. By mapping possible risks in advance, we will be prepared to solve the possible unwanted incidents. When performing our risk analysis we choose to use the ALARP(As low as reasonably practicable) principle. The goal of ALARP is to reduce the risk to a reasonable level without using unnecessary resources. We are assessing the risks and implementing relevant mitigation to lower the potential negative outcome. [8]

No.	Risk	Mitigation	Residual probability	Residual consequence
#1	Underestimate time use in the beginning of project and failing to reach desirable goals.	Use tools like Gantt, Project description group rules and continuous planning.	2	4
#2	Continuous breach of group rules.	Actively following the repercussion section of project plan.	2	3
#3	Internal conflict.	Following group rules, de-escalation from other members and contact supervisor if needed.	2	3
#4	Illness (low severity).	Other members can cover workload while affected person recover. Non time sensitive tasks can be delayed.	4	1
#5	Illness (high severity).	Other members must cover workload and role tasks.	2	4
#6	Data loss	Backup should follow the 3-2-1 backup strategy.	1	2

Figure 2: ALARP risk table

	Acceptable	No additional mitigation needed.
	Tolerable	Consider further review and mitigation.
	Unacceptable	Risk reducing measures is required.

Figure 3: ALARP tolerance table

Probability / Consequence	1 Rare	2 Unlikely	3 Possible	4 Likely	5 Almost certain
5 Catastrophic					
4 Major		#1, #5			
3 Moderate		#2, #3			
2 Minor	#6				
1 Insignificant				#4	

Figure 4: ALARP risk matrix

6 Execution Plan

This section explains the specific plan and timeline the group has created for the completion of the thesis, specifically a Gantt schema, as well as an explanation of specific milestones. These serve to further elaborate on the use of Scrum in accordance to the entirety of the execution of the thesis.

6.1 Gantt Schema

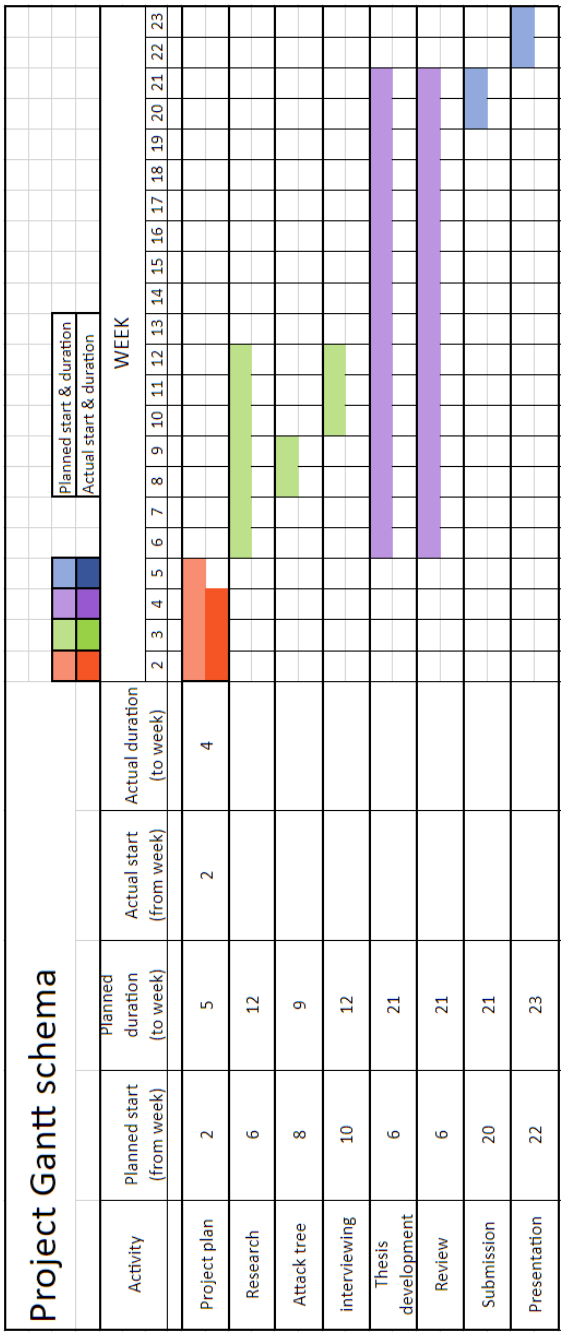


Figure 5: Gantt schema

Bibliography

[1] Ahus. *Akershus University Hospital*. URL: https://www.ahus.no/akershus-university-hospital (visited on 19th Jan. 2023).

[2] Køster. C. *Hva er forskjellen på resultatmål og effektmål?* URL: https://www.prosjektbloggen.no/hva-er-forskjellen-p%C3%A5-resultatm%C3%A5l-og-effektm%C3%A5l (visited on 26th Jan. 2023).

[3] Advisory. *24.4M patients, 21 companies now say they were affected by AMCA data breach*. URL: https://www.advisory.com/daily-briefing/2019/08/13/data-breach (visited on 23rd Jan. 2023).

[4] Collier. R. *NHS ransomware attack spreads worldwide*. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5461132/ (visited on 23rd Jan. 2023).

[5] Milmo. D. *NHS ransomware attack: what happened and how bad is it?* URL: https://www.theguardian.com/technology/2022/aug/11/nhs-ransomware-attack-what-happened-and-how-bad-is-it (visited on 23rd Jan. 2023).

[6] Scrum. *What is scrum*. URL: https://www.scrum.org/resources/what-is-scrum (visited on 31st Jan. 2023).

[7] Lakeworks. *File:Scrum process.svg*. URL: https://commons.wikimedia.org/wiki/File:Scrum_process.svg (visited on 26th Jan. 2023).

[8] Health and Safety Executive. *ALARP at a glance*. URL: https://www.hse.gov.uk/managing/theory/alarpglance.htm (visited on 26th Jan. 2023).

C Meeting Minutes

Meeting minutes 10th of January

Minutes		
Thesis provider Kåre-Magne, Aleksander	Present: Kåre Magne, Aleksander, Steinar, Sindre, Jonas and Jørgen	Secretary Steinar

Plan

- First meeting with thesis provider
- General discussion retaining to the provided thesis

Notes

- Background for the thesis
    - Interest in the consequences of crypto virus attacks in the healthcare sector?
    - Putting life and health in danger?
    - Services that are relevant for the patients
    - Opportunities
    - Home help for patients, an attack vector could be emergency buttons and phoning
    - Attacks against individuals, blackmail of medical journal holders and patients
- Motivation, consequences, attack forms, what happens when an incident occurs? Dangerous digital meeting places. How attacks choose their targets.
- Examples of incidents
- In Germany, England, multiple American hospitals

Meeting minutes 11th of January

Minutes		
Supervisor: Filip	Present: Filip, Steinar, Sindre, Jonas and Jørgen	Secretary Sindre

Plan

- First meeting with supervisor

Notes

- Introduction to thesis writing

Meeting minutes 18th of January

Minutes		
Supervisor Filip	Present: Filip, Steinar, Sindre, Jonas and Jørgen	Secretary Sindre
Plan - Questions regarding project plan - Methodology and general project plan setup		

Meeting minutes 25th of January

Minutes		
Supervisor Filip	Present: Filip, Steinar, Sindre, Jonas and Jørgen	Secretary Sindre
Plan - Questions about the project plan - Sources and paragraph references - Suggestions for roles - General questions regarding scrum - Questions about font size for the document and general document layout - Questions regarding the Gantt schema Notes - Minor feedback from supervisor, such as: typos, citing and coherency in the project plan. - The roles were fine but could be more fleshed out i.e., generalist. - There is no strict requirement for Gantt schema, and the template shown was fine.		

Meeting minutes 1st of February

Minutes		
Supervisor Filip	Present: Filip, Steinar, Sindre, Jonas and Jørgen	Secretary Sindre
Plan - Verifying the project plan in its current state - Questions regarding recommendations for starting the bachelor thesis - Where to find different sources - How to specify the scope of the different articles to use Notes - Recommended using google scholar, oria.no (ntnu database), IEEE xplore, web of science - Using the project description and our own intuition for finding, using and exploring different sources		

Meeting minutes 9th of February

Minutes		
Thesis provider Kåre Magne og Espen	Present Sindre, Steinar, Jonas and Jørgen	Secretary Sindre

Plan
Recap what we have been working on so far.
- Projectplan, do they want a copy?

ICU (Intensive Care Unit) interviews?

Attack tree diagram.
What do they want the attack tree diagram to focus on? Vector, exploit, consequences?

QALY? Breach of privacy, does it have psychological consequences, or is it just somatic effects?

Notes
- One of the thesis provider contacts has been changed. Aleksander is substituted for Espen.
- Espen got a quick introduction about the thesis, so he got up to date.
- They wished for a copy of the project plan, which they now have gotten.
- Discussed some different cyber attacks that we found interesting. Kåre Magne also had some interesting cyber attacks, like the one in Finland targeting Vastaamo.
- The thesis providers will try to arrange an interview for us with the ICU (Intensive care unit).
- Attack tree – The thesis provider is going to discuss further what they want included.
- Mainly somatic about QALY, we should try to find proper data about this.

Meeting minutes 15th of February

Minutes		
Supervisor Filip	Present Sindre, Steinar, Jonas and Jørgen	Secretary
Plan: - Keep supervisor up to date. Notes: - Mention other forms of attacks? - Interview other hospitals if possible. - Include questionaries.		

Meeting minutes 22nd of February

Minutes		
Supervisor Filip	Present Sindre, Steinar, Jonas and Jørgen	Secretary
Plan: – Keep Filip up to date, what have done since last time. – How to cite our own sources/images. – Method or methodology? – Other sections in the theory? Notes: – If it's redrawn, we need to cite the source. – Methodology like scrum. – Confirmed where and how to cite sources in the text.		

Meeting minutes 1st of Mars

Minutes		
Supervisor Filip	Present Sindre, Jonas, Jørgen	Secretary Sindre
Plan - No plan, just keep supervisor up to date Notes - More incidents? - Footnotes - Friday meeting next week, gone the entire week in 2 weeks.		

Meeting minutes 9th of March

Minutes		
Thesis provider Kåre Magne and Espen	Present Jørgen, Steinar, Sindre, Jonas	Secretary
Plan: Questions regarding interviews - What kind of personnel is the most relevant to interview? - Do you have any contacts that we can make use of for interviews? - What extent of coverage would you call enough interview data? - Talking points are; where, who and why. - What cybersecurity measures are already in place? - Passwords, 2FA, cybersecurity course, etc Notes: - (Ruttan)? Gullbekk - Senior advisor - medicine and health - Forms? Share on Linkdn - Information security course - Measures through partners		
Supervisor mentioned webpages: Helsetilsynet – forsvarlig pasient behandling uten ikt Helsetilsynet – Hvordan er sykehusene forberedt på ikt bortfall kartlegging ved fem virksomheter		

Meeting minutes 10th of March

Minutes		
Supervisor Filip	Present Sindre and Steinar	Secretary Sindre
Plan Notes - Questionaries and interviews brief, what have done so far - Surveymonkey - We are using google forms. It will be anonymous - Describe the process in method perhaps - We want to send the forms to multiple hospitals		

Meeting minutes 22nd of March

Minutes		
Supervisor Filip	Present Sindre, Steinar, Jonas, Jørgen	Secretary Sindre
Plan Interviews and questionnaire attack tree Notes - Hospitals will not respond to English emails - We have contacted multiple parties, hospitals ++ - We want to finish Attack Tree and interviews before we start writing. - Attack tree, ip scan -> port scan -> port vuln - Discussion around questionnaire and surveys - Provided source for phising article - Phising email, compromised - Path down the attack tree for known attacks?		
Articles Filip mentioned: - Investigation into Phishing Risk Behaviour among Healthcare Staff - Assessing the Legal Aspects of Information Security Requirements for Health Care in 3 Countries: Scoping Review and Framework Development		

Meeting minutes 29th of March

Minutes		
Supervisor Filip	Present Jonas, Jørgen, Steinar	Secretary Jørgen
Plan - Questionnaire vs. Survey? Notes - Hospitals have now responded to our emails - Discussed some plans for interviews - Try to explain differences in method (questionnaire and survey) - Attack tree, explained some changes - Discuss path from older attacks, show paths with markings (known attacks) - Change vocabulary so it is even across each node		

Meeting minutes 5th of April

Minutes		
Supervisor Filip	Present Jørgen, Steinar, Sindre	Secretary Sindre
Plan Notes - Method for interviewing, back it up with a source or structure. - The group will pick up the pace after interviews		

Meeting minutes 12th of April

Minutes		
Supervisor Filip	Present Jørgen, Sindre, Jonas, Steinar	Secretary Steinar
Plan Notes - Begin writing, timeframe/deadline for draft 1, approx. 2.5 weeks - Define source for interview format - Feedback on attack tree diagram - Path highlighting for the attack tree - Appendixes, include questionnaire and interviews		

Meeting minutes 19th of April

Minutes		
Supervisor Filip	Present Jørgen, Sindre, Jonas, Steinar	Secretary Sindre
Plan Should we use text under paths taken? References to interview? Sources from results Notes - We wanted to look at results - Nobody answered questionaries - How to refer to interview, we could do a summary - Update method section with interview - What, why, how when writing method - Referring to prior theory section when writing about that topic - It Does not hurt to cite a source again - Ahus might want to restrict some of the information, like the system/software list - One picture for our attack tree - All attacks together, color coded. Easier to explain - Consider readability - “Our attack tree” do not reference it like that - Rename results? Findings? - Recommendations later - Group needs to re-assess structure		

Meeting minutes 26th of April

Minutes		
Supervisor Filip	Present Steinar, Sindre, Jørgen, Jonas	Secretary Sindre
Plan How/where to explain lack of response/interest in interview objects? Method or results Source/citing Notes Do more subsections Add 1 more subsection how it went Design phase, something like this Implementation, why it did not work out Mention at start of the section, to reduce the amount of cites Source after et al, if you mention it by name Just mentioning once at the top Repeating, (et al name -> paper) If it is 2 people you will not put both, when citing If you do not cite, it is not necessarily a big issue. Bachelor method section		

Meeting minutes 3rd of May

Minutes		
Supervisor Filip	Present Steinar, Sindre, Jørgen, Jonas	Secretary Sindre

Plan
punctuation at end of sentence in tables
names of libraries
Perhaps this would be better fitting in discussion/measures section
maybe mention that it is an active attack (not passive)
table 3

Notes
Measure in discussion
Glossary multiple page entries, acronyms back to list, but not the other way
Table 3 is fine, no worries, could make column 1 taller, fine size -> fine (nok)
Punctuation, not needed, but keep it consistent
Data Analysis in method? Steinar got it
Do not split 24 000
ROS

Meeting minutes 5th of May

Minutes		
Thesis provider Espen and Kåre	Present Steinar, Sindre, Jørgen	Secretary Sindre

Plan
Contents of Discussing Consequences and CIA section: (which ones do we do)
- Include risks found in the attack tree and write measures for these
- Create more extensive ROS
- Only measures
- Measures to prevent specific consequences

Notes
Espen can send information about the hospital-partners, if that is not sufficient, the team can try sending a questionnaire or hold an interview.

Team should not go to in-depth. Stuff that affects the hospital, rough features.
The consequences for hospital operation, losing data, re-diagnosis, moving patients denial of service, difficulties setting a price on the attacks.
Going through bachelor thesis table of contents.

If someone clicks something, it should be possible to reduce the damages
Building an infrastructure with shadow boxing, reducing risk?
Thoughts about tables, always good.
It is easier to discuss details, although if you think about the budget is spent to prevent attacks, it will be dependent on the business management level, some words are the consequences are significant.

Do not make it too expensive. It is serious if it happens to Ahus. It is serious, ergo Ahus must spend money to protect themselves.
The consequences of spending money.
Ahus will skim the thesis.
Fake environment

Meeting minutes 10th of May

Minutes		
Supervisor Filip	Present Steiner, Sindre, Jørgen, Jonas	Secretary Sindre
Plan Review feedback with supervisor Notes Change theory headlines No comma in headlines Keep capitalization consistent Direct citation tabbed in above 3 lines. 5.1 strange start of the chapter		

Meeting minutes 16th of May

Minutes		
Supervisor Filip	Present Steinar, Sindre, Jørgen, Jonas	Secretary Sindre
Plan email correspondence in appendix itemize or regular text in 1.8 structure of report? Should reference list be included in the page count Writing form in reflection Notes Keep space with 4 digits, example 3 000 Refer to meeting minute for bachelor provider and meetings Reflection writing form, can be flexible, introduction is Conclusion objective Filip can read it today Protective measures Introduction in the discussion parts, consequences and probability reducing Conclusion task giver 15 highest fines list, reduce the length, and remove the date, mention it above in the text Work Tuesday, Friday, and weekend to finish, maybe Thursday as well		

D Interview results

Oppsett av intervjuene

- Intro
- Spørsmål
- Refleksjon
- Avslutning
- Avsatt tid: 45 min

Introduksjon

Intervjuobjekt 1

Senior rådgiver og beredskaps opplæring, veiledning, risikoanalyse og beredskap

Intervjuobjekt 2

Division facility management, HMS og risikoanalyser

Spørsmål (Klinisk)

Hvilke digitale systemer er dere avhengige av for å behandle pasienter?

- En hel liste[redacted], [redacted]
  ([redacted] (Tjeneste liste oversendt) [redacted]. eks IKT

Har dere prosedyrer/rutiner for behandling dersom nødvendige digitale systemer går ned?

- De har nød rutiner
- Delplan IKT med 30 systemer som er kritisk
- Liste med kritikalitet 1
- IKT telefoni – beredskapsplan
- Nød-printere kan skrive ut nød-rapporter fra server for [redacted]

Hvilke konsekvenser vil kunne forekomme hvis dere mister tilgang til nevnte systemer?

- Over lengre tid så kan det ha en effekt.
- Utsetter behandlinger, de som er i system vil bli behandlet.

Spørsmål (QALY)

Kan du fortelle litt rundt prosessen om beregning av QALY (Hvordan regnes det ut, regnes det ut for alle pasienter (eller bare kritiske), hva brukes QALY til?)

- Ukjent

Gjelder QALY bare for somatiske tilstander eller er psykiske tilstander inkludert (Eks frigjøring av personlig informasjon påvirker psyken).

- Ukjent

Spørsmål (IT kompetanse)

hvilke sikkerhetsmekanismer er det dere bruker? (digitale midler, opplæring I digital sikkerhets kunnskaper hos helsepersonell, backups osv.)

- De ulike systemene eller sykehuspartnere kan svare på det, de vet ikke. De har ikke noe opplæring. Sikkerhets-uker med litt digitalopplæring.
- må også ta informasjonssikkerhet e-læring ved ansettelse

Kan dere gi en kort beskrivelse av dere digitale infrastruktur?

- Kan ikke svare på. Trine Brena kan svare. sykehuspartnere

Hvordan gjennomfører dere digital etterforskning?

- Sykehuspartnere har ansvaret sammen med Ahus.
- Administrerende direktør hvis det er bredere. Helse sør-øst hvis det blir større.

Har dere etablerte playbooks? Hvor omfattende er disse?

- Intervjuobjekter henviser til sykehuspartnere

Hvilken sikkerhetstrussel frykter dere mest skal inntreffe?

- Alt som tar ned systemene bekymrer. Det å miste pasient data. Eller komprimerer data.

Hvilke standarder følger dere for digital systemutvikling og oppretthold?

- Intervjuobjekter henviser til sykehuspartnere

Gjennomfører dere regelmessige ROS analyser, i så fall hvor ofte?

- Til de ulike, spør sykehuspartnere eller Trine Brenna (MTE, daglig oppfølging)

- Gjennomføres 1 gang i året.

Økonomiske konsekvenser?

- Tap i statlig støtte, tror ikke det. Bot fra datatilsynet. Bare opprette systemer og avvik. Hvis det er varige skader. Har ikke hørt om noen der det har påvirket rammene.
- De får ikke ekstramidler hvis de tabber seg ut.

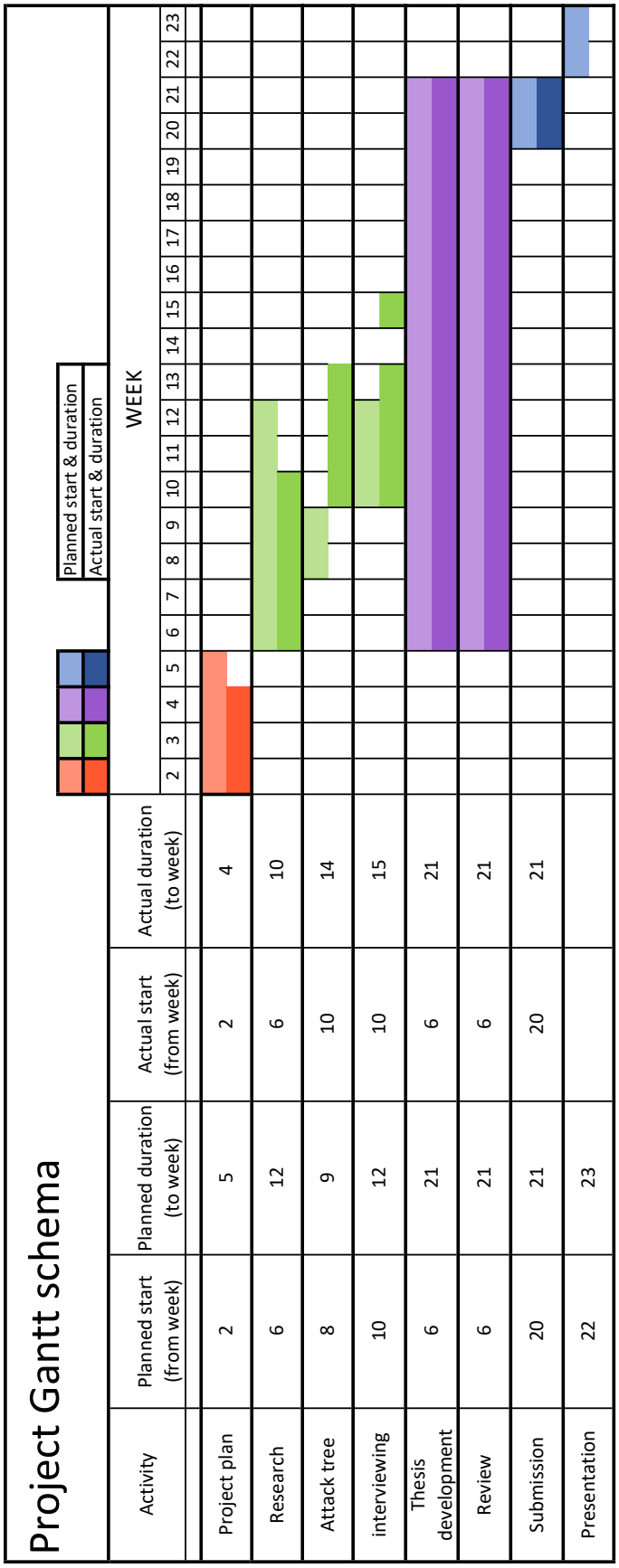
Kan ransomware påvirke omdømmet?

- Ja, helt innlysende. Vil synke drastisk.

Rammer det et helseforetak eller flere. Mer alvorlig hvis det rammer hele helse sør-øst.

- Man nå være sjapp på å forklare ting for å ikke miste omdømme. Avhengig av hva som skjer og når. Kan oppnå tillitt hvis man er fornuftig

E Gantt Schema



F Time logs

Hours (January)

January	Week 2							Week 3							Week 4							Week 5		
	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues	
	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	Total H/Person
Jonas B. Nessø	3	2	3	7						4					6	6	3	6	7				6	53
Jørgen L. Myrvold	3	2	3	7				2	2	4	5	5			6	6	3	6	7				6	67
Steinar M. Myhre	3	2	3	7	3	1			2	4	5	5			6	6	3	6	7				6	69
Sindre Hiis-Hauge	3	2	3	7	4					4	5	5			6	6	3	6	7				6	67
Total Hours daily	12	8	12	28	7	1	0	2	4	16	15	15	0	0	24	24	12	24	28	0	0	0	24	256

Division of labour (January)

January	Week 2							Week 3							Week 4							Week 5	
	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues
	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Jonas B. Nessø	3, 8	2,3	1,3,8	4						1,3,8					4	4	1,3,8	4,9	4,9				4,9
Jørgen L. Myrvold	3, 8	2,3	1,3,8	4				5	5	1,3,8	4	4			4	4	1,3,8	4,9	4,9				4,9
Steinar M. Myhre	3, 8	2,3	1,3,8	4	5	5			5	1,3,8	4	4			4	4	1,3,8	4,9	4,9				4,9
Sindre Hiis-Hauge	3, 8	2,3	1,3,8	4	5					1,3,8	4	4			4	4	1,3,8	4,9	4,9				4,9

#	Type of work
1	Supervisor meeting
2	Thesis provider meeting
3	Group meeting
4	Project plan
5	Research
6	Interview
7	Report writing
8	Planning
9	Quality control
10	Attack tree diagram
11	Questionnaire

Hours (February)

February	Week 5					Week 6							Week 7							Week 8							Week 9		
	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	Total H/Person
Jonas B. Nessø	4	7	7			6			6	6			4		4	6	5			7	7	4	7	6			6	6	98
Jørgen L. Myrvold	4	7	7			6			6	6			4		4	6	5			7	7	4	7	6			6	6	98
Steinar M. Myhre	4	7	7			6			6	6			4		4	6	5			7	7	4	7	6			6	6	98
Sindre Hiis-Hauge	4	7	7			6			6	6			4		4	6	5			7	7	4	7	6			6	6	98
Total Hours daily	16	28	28	0	0	24	0	0	24	24	0	0	16	0	16	24	20	0	0	28	28	16	28	24	0	0	24	24	392

Division of labour (February)

February	Week 5					Week 6							Week 7							Week 8							Week 9		
	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	
Jonas B. Nessø	1,3	5,8	5,8			5,8			2,5	3,5			3,7		1,3	7	7			7	7	1,3	7	7			7	7	
Jørgen L. Myrvold	1,3	5,8	5,8			5,8			2,5	3,5			3,7		1,3	7	7			7	7	1,3	7	7			7	7	
Steinar M. Myhre	1,3	5,8	5,8			5,8			2,5	3,5			3,7		1,3	7	7			7	7	1,3	7	7			7	7	
Sindre Hiis-Hauge	1,3	5,8	5,8			5,8			2,5	3,5			3,7		1,3	7	7			7	7	1,3	7	7			7	7	

#	Type of work
1	Supervisor meeting
2	Thesis provider meeting
3	Group meeting
4	Project plan
5	Research
6	Interview
7	Report writing
8	Planning
9	Quality control
10	Attack tree diagram
11	Questionnaire

Hours (March)

March	Week 9					Week 10							Week 11							Week 12							Week 13					
	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur	Fri	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	Total H/Person
Jonas B. Nessø	3	7	6			7		4	5	4			6			7	6				4	4	7	6			5	7	4	7	6	105
Jørgen L. Myrvold	3	7	6			7		4	5	6			6			7	6				4	4	7	6			5	7	4	7	6	107
Steinar M. Myhre	3	7	6			7		4	5	6			6			7	6				4	4	7	6			5	7	4	7	6	107
Sindre Hiis-Hauge	3	7	6			7		4	5	6			6			7	6				4	4	7	6			5	7	4	7	6	107
Total Hours daily	12	28	24	0	0	28	0	16	20	22	0	0	24	0	0	28	24	0	0	0	16	16	28	24	0	0	20	28	16	28	24	426

Division of labour (March)

March	Week 9					Week 10							Week 11							Week 12							Week 13					
	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur	Fri	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
Jonas B. Nessø	1,3	6,7	6,7			5,7		9	6,7	1,7			6		1,3	6	6				3,9	1,3	7	7			8	5	1,3	5	5	
Jørgen L. Myrvold	1,3	10,6	10,6			5,7		9	10,6	1,7			10		1,3	10,7	10,7				3,9	1,3	7	7			8	5	1,3	5	5	
Steinar M. Myhre	1,3	6,7	6,7			5,7		9	6,7	1,7			6		1,3	6	6				3,9	1,3	7	7			8	5	1,3	5	5	
Sindre Hiis-Hauge	1,3	10,6	10,6			5,7		9	10,6	1,7			10		1,3	10,7	10,7				3,9	1,3	7	7			8	5	1,3	5	5	

#	Type of work
1	Supervisor meeting
2	Thesis provider meeting
3	Group meeting
4	Project plan
5	Research
6	Interview
7	Report writing
8	Planning
9	Quality control
10	Attack tree diagram
11	Questionnaire

Hours (April)

April	Week 13		Week 14							Week 15							Week 16							Week 17							
	Sat	Sun	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Total H/Person
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
Jonas B. Nessø			6	7	3					6	2	3	7	7				7	1	7	6			8	8	1	7	6			92
Jørgen L. Myrvold			6	7	3					6		3	7	7			6	7	1	7	6			8	8	1	7	6			96
Steinar M. Myhre			6	7	3					6		3		4			6	7	1	7	6			8	8	1	7	6			86
Sindre Hiis-Hauge			6	7	3					6	2	3	7	7			6	7	1	7	6			8	8	1	7	6			98
Total Hours daily	0	0	24	28	12	0	0	0	0	24	4	12	21	25	0	0	18	28	4	28	24	0	0	32	32	4	28	24	0	0	372

Division of labour (April)

April	Week 13		Week 14							Week 15							Week 16							Week 17						
	Sat	Sun	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur	Fri	Sat	Sun
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Jonas B. Nessø			3,5	7	1,3					8	6	1,3	7	7				7	1,3	7	7			7	7	1,3	7	7		
Jørgen L. Myrvold			3,5	7	1,3					8		1,3	7	7			7	7	1,3	7	7			7	7	1,3	7	7		
Steinar M. Myhre			3,5	7	1,3					8		1,3		7			7	7	1,3	7	7			7	7	1,3	7	7		
Sindre Hiis-Hauge			3,5	7	1,3					8	6	1,3	7	7			7	7	1,3	7	7			7	7	1,3	7	7		

#	Type of work
1	Supervisor meeting
2	Thesis provider meeting
3	Group meeting
4	Project plan
5	Research
6	Interview
7	Report writing
8	Planning
9	Quality control
10	Attack tree diagram
11	Questionnaire

Hours (May)

	Week 18							Week 19							Week 20							Week 21							Week 22			
	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	
May	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	Total H/Person
Jonas B. Nessø	8	8	8	7						8	8	8	7	7	7	8		7	8	8	7											114
Jørgen L. Myrvold	8	8	8	7	7					8	8	8	7	7	7	8			8	8	7											114
Steinar M. Myhre	8	8	8	7	7					8	8	8	7	7	7	8			8	8	7											114
Sindre Hiis-Hauge	8	8	8	7	7					8	8	8	7	7	7	8			8	8	7											114
Total Hours daily	32	32	32	28	21	0	0	0	0	32	32	32	28	28	28	32	0	7	32	32	28	0	0	0	0	0	0	0	0	0	0	456

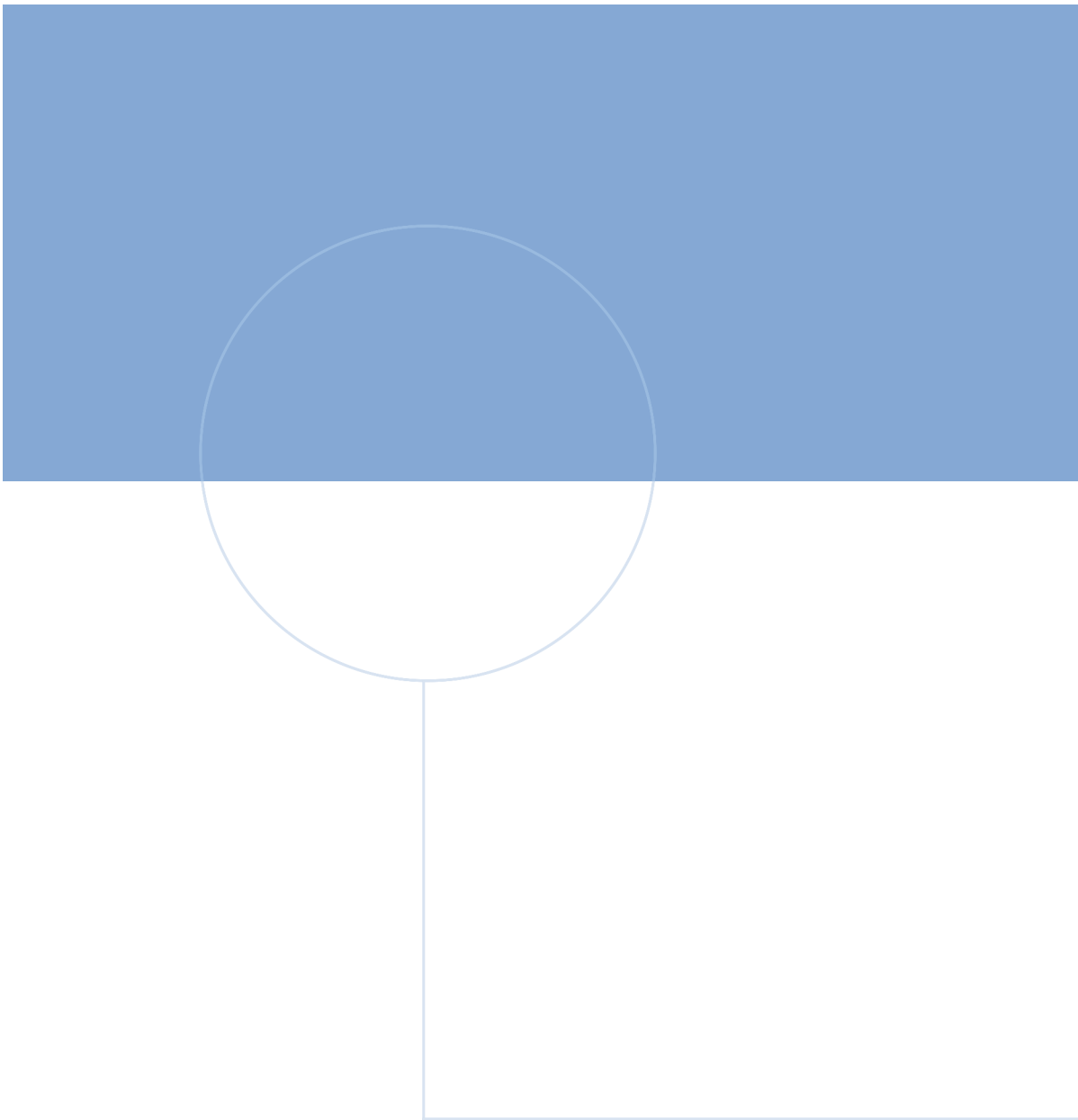
Division of labour (May)

	Week 18							Week 19							Week 20							Week 21							Week 22		
	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed
May	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Jonas B. Nessø	7	7	1,7	7,11						1,7,9	7	7	7	7	7,9	1,8,9		9	9	9	9										
Jørgen L. Myrvold	7	7	1,7	7	7					1,7,9	7,9	7	7	7	7,9	1,8,9			9	9	9										
Steinar M. Myhre	7	7	1,7	7	7					1,7,9	7	7	7	7	7	1,8,9			9	9	9										
Sindre Hiis-Hauge	7	7	1,7	7	7					1,7,9	7,9	7	7	7	7	1,8,9			9	9	9										

#	Type of work
1	Supervisor meeting
2	Thesis provider meeting
3	Group meeting
4	Project plan
5	Research
6	Interview
7	Report writing
8	Planning
9	Quality control
10	Attack tree diagram
11	Questionnaire

Total hours worked

Jonas	462
Jørgen	482
Steinar	474
Sindre	484
	1902



NTNU

Norwegian University of
Science and Technology