# Kandidatuppsats

## IT-forensik och informationssäkerhet 180 hp

# Ransomware-hotet mot svenska sjukhus

## – en intervju- och litteraturstudie

## Digital forensik 15 hp

Halmstad 2021-06-15

Josefin Ahl och Julia Djurklou

HÖGSKOLAN
I HALMSTAD

# Ransomware-hotet mot svenska sjukhus

## – en intervju- och litteraturstudie


| | |
|---|---|
| **Författare** | Josefin Ahl och Julia Djurklou |
| **Program** | IT-forensik och informationssäkerhet, 180 hp |
| **Handledare** | Eric Järpe |
| **Examinator** | Urban Bilstrup |
| **Lärosäte** | Högskolan i Halmstad |
| **Datum** | 13 juni 2021 |

# Abstract

Statistics show an increase in ransomware activity in recent years. The increase is mainly due to the ongoing Covid-19 pandemic. Cybercriminals take advantage of the fact that hospitals worldwide are overloaded with caring for seriously ill patients in Covid-19 and perform ransomware attacks.

This thesis examines how Swedish hospitals experience and handle the increased threat of ransomware. The bachelor's thesis consists of a literature study and some in-depth interviews. The literature study is investigating ransomware as a phenomenon and finding out why it is a successful method for cybercriminals to use in digital extortion.

The purpose is also to investigate how Swedish hospitals relate to the fact that the healthcare sector has become an attractive target for cyber-attacks. The interview study examines the hospitals' IT security to determine whether they are sufficiently resistant to ransomware attacks. The interview results are discussed and analyzed against the background of the literature. The conclusion of this analysis is the basis for the proposed countermeasure.

The results show that the hospitals surveyed have suitable IT security. The most central security mechanisms for the hospitals are their backup and recovery routines in the fight against ransomware. The discussion in this work combines the results from the literature and interview studies carried out. Based on the discussion, the conclusion is that the hospitals surveyed have good security and meet most of the recommendations published by Swedish authorities. Still, there is room for some improvement which is indicated.

**Key words:** Ransomware, IT security, Backup routines, Cybercriminals, Health care sector

# Sammanfattning

Statistik visar att ransomware har ökat lavinartat de senaste åren, inte minst under den rådande Covid-19-pandemin. Cyberkriminella har kommit att utnyttja sjukhus runt om i världen som redan är överbelastade med att ta hand om patienter svårt sjuka i Covid-19.

I denna uppsats undersöks det hur de svenska sjukhusen upplever och hanterar det ökade hotet av ransomware. Den utgörs av en litteraturstudie och några djupintervjuer. Litteraturstudien görs för att utforska fenomenet ransomware och ta reda på varför ransomware är en framgångsrik metod för kriminella att använda vid utpressning. Syftet är även att undersöka hur svenska sjukhus förhåller sig till att hälso- och sjukvårdssektorn har blivit attraktiva mål för cyberangrepp. I intervjustudien undersöks sjukhusens IT-säkerhet för att kartlägga om de är tillräckligt motståndskraftiga mot ransomware-angrepp. Intervjusvaren diskuteras och analyseras mot bakgrund av litteraturen. Slutsatsen av denna analys ligger till grund för åtgärdsförslag.

Resultatet visar att sjukhusen/regionerna som tillfrågats har en bra IT-säkerhet. De mest centrala säkerhetsmekanismerna för verksamheterna är deras backup- och återställningsrutiner i kampen mot ransomware. Diskussionen i arbetet sammanfogar resultatet från både litteraturstudien och intervjustudien som genomförts. Utifrån diskussionen dras sedan slutsatsen att regionerna som tillfrågats har bra säkerhet och uppfyller de flesta av rekommendationer som publicerats av svenska myndigheter. Inte desto mindre resulterar studien i några uppslag till förbättringar i säkerhetsrutiner.

**Nyckelord:** Ransomware, IT-säkerhet, Backup-rutiner, Cyberkriminella, Hälso- och sjukvårdssektorn

# Förord

Stort tack till samtliga respondenter som medverkat i intervjustudien. Ni har bidragit med kunskap och nya, intressanta synvinklar till uppsatsen och utan er hade inte arbetet varit genomförbart.

Vi vill även tacka vår handledare, Eric Järpe, som har hjälpt och väglett oss med goda råd under arbetets gång.

# Definitioner och förkortningar

Benämningen **ransomware** har ursprung i det engelska språket och är en sammansättning av *ransom* som betyder lösensumma och *software* som betyder mjukvara på svenska [6]. Ransomware är en sorts skadlig programvara, som används av kriminella vid datorbaserad utpressning [7]. Ransomware kallas i allmänhet även för utpressningsvirus.

**Crypto ransomware** och **locker ransomware** är de mest förekommande typerna av de ransomware-attacker som utförs i dagsläget. Crypto ransomware infekterar datorer och krypterar värdefulla filer på enheter. Locker Ransomware krypterar inte offrens data utan låser ute dem från enheten och hindrar dem från att använda den. Angriparen hänvisar sedan de utsatta att betala en lösensumma i kryptovaluta för att i retur få tillbaka informationen eller få datorn återställd i funktionellt skick [9].

**ISO 27000** är ett ledningssystem för cyber- och informationssäkerhet. Standarden finns för att skydda information och eftersom den idag är digitaliserad omfattar standarden även cybersäkerhet. Dessutom har de flesta organisationer information som innefattar personuppgifter, vilket har lett till att standarden utökats till att även omfatta skydd av data [51].

| **Förkortning** | **Definition** |
|---|---|
| MSB | Myndigheten för Samhällsskydd och Beredskap |
| SÄPO | Säkerhetspolisen |
| FRA | Försvarets radioanstalt |
| IDS | Intrusion Detection System |
| IPS | Intrusion Prevention System |
| VLAN | Virtual Local Area Network |
| VPN | Virtual Private Network |
| VDI | Virtual Desktop Infrastructure |
| RDP | Remote Desktop Protocol |

# Innehåll

1. Inledning ..... 1
1.1. Bakgrund ..... 2
1.2. Koppling till tidigare forskning ..... 3
1.2.1. Ransomware in Healthcare Facilities: A Harbinger of the Future? ..... 3
1.2.2. A Socio-technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks ..... 4
1.2.3. Ransomware - Digitala kidnappare ..... 4
1.2.4. A novel method for recovery from Crypto Ransomware infections ..... 4
1.3. Problemformulering ..... 5
1.3.1. Problematisering av frågeställningar ..... 5
2. Metod ..... 7
2.1 Litteraturstudie ..... 7
2.2. Kvalitativ intervjustudie ..... 7
2.2.1. Forskningsetik ..... 8
2.3. Intervjuprocess ..... 9
2.4. Metoddiskussion ..... 9
3. Litteraturstudie ..... 11
3.1. Olika typer av malware ..... 11
3.1.1. Virus ..... 11
3.1.2. Maskar ..... 11
3.1.3. Trojanska hästar ..... 11
3.1.4. Ransomware ..... 12
3.2. Hur ransomware sprids ..... 12
3.3. Varför är sjukhus ett attraktivt mål för ransomware-attacker? ..... 13
3.4. Ransomware-attacker som drabbat hälso- och sjukvårdssektorn ..... 14
3.4.1. Medstar Health ..... 14
3.4.2. WannaCry ..... 15
3.4.3. NotPetya ..... 16
3.4.4. Düsseldorf University Clinic ..... 18
3.5. Befintliga skyddsrutiner mot ransomware ..... 18
3.5.1. Backup-rutiner ..... 18
3.5.2. Systemuppdateringar ..... 19
3.5.3. Nätverkssegmentering ..... 19
3.5.4. Brandväggar, antivirus och spamfilter ..... 20

3.5.5. Övervaka systemen ..... 20
3.5.6. Användare ..... 21
3.5.7. Script för återställning av filer ..... 23
4. Intervjustudie ..... 25
4.1. Resultat – sammanställande tabell ..... 25
4.2. Intervjuer ..... 26
4.2.1. Allmän information ..... 26
4.2.2. Informationssäkerhetsarbete och IT-policys ..... 27
4.2.3. Hårdvara/Mjukvara ..... 27
4.2.4. Nätverk och kommunikation ..... 30
4.2.5. Personal och arbetsrutiner ..... 31
4.3. Förslag på skyddsrutiner mot ransomware ..... 32
5. Diskussion ..... 37
5.1. Hur upplever och hanterar de svenska sjukhusen det ökade hotet av ransomware? ..... 37
5.2. Upprätthåller sjukhusen i Sverige säkra IT-system och lösningar för att kunna motstå en ransomware-attack? ..... 38
5.3. Hur kan säkerheten utvecklas på sjukhusen för att bättre stå emot ransomware-attacker? ..... 40
6. Slutsats ..... 43
6.1. Framtida forskning ..... 44
Referenser/Källförteckning ..... 45
Bilaga 1: ..... 51
Bilaga 2: ..... 52

# 1. Inledning

Den 10 september 2020 miste en kvinna sitt liv i samband med en ransomware-attack i Düsseldorf, Tyskland. Intrånget var anledningen till att 30 servrar kraschade och sjukhuset miste kontrollen över sina IT-system. Till följd av intrånget tvingades sjukhuset omdirigera patienter i behov av akutvård till närliggande sjukhus. En kvinna skickades till ett sjukhus i Wuppertal, 20 mil från sjukhuset i Düsseldorf. På grund av kvinnans redan livshotande tillstånd och fördröjningar av vård gick hennes liv inte att rädda [1].

Sverige är ett mycket attraktivt mål för ransomware-attacker i dagsläget eftersom landet ligger i överkant beträffande utbetalade lösensummor. Betalning av lösensumma är dock inte en garanti för att återfå kontrollen över systemen. Andra länder och myndigheter har därmed gått ut med en rekommendation att aldrig betala vid en ransomware-attack [2]. Sverige är också det land som har störst återställningskostnader efter en attack. Truesec har sett att återställningskostnader vid ett flertal tillfällen har uppgått till över 500 miljoner svenska kronor [3]. Truesecs grundare, Marcus Murray, säger även att "en framgångsrik cyberattack kan lamslå en hel organisation och orsaka enorm skada i såväl kostnader, förlorade datatillgångar och inte minst skadat anseende." [3]. Under 2019 betalade Sverige 14–16 miljarder svenska kronor i kostnader för cyberattacker. Året därpå beräknades kostnaderna att uppgå till 22 miljarder svenska kronor [4]. Detta är en underdrift, eftersom de faktiska kostnaderna landade på 30 miljarder svenska kronor, vilket är en ökning med 100 % från 2019 [5].

Den 2 november 2020 varnade Myndigheten för samhällsskydd och beredskap (MSB) organisationer inom hälso- och sjukvårdssektorn för ökad aktivitet av ransomware-attacker. Covid-19 pandemin har medfört att sjukhusen runt om i världen har överbelastats vilket utnyttjas av cyberkriminella. Benämningen ransomware kommer ursprungligen från det engelska språket och är en sammansättning av *ransom* som betyder lösensumma och *software* som betyder mjukvara på svenska [6]. Ransomware är en sorts skadlig programvara, som används av kriminella vid datorbaserad utpressning på människor, städer, organisationer, institutioner och företag. På grund av digitaliseringens framfart och utvecklingen av kryptovalutor, kan cyberbrottslingar i dagsläget tjäna snabba pengar genom ransomware-attacker med förhållandevis låg risk att åka fast. Detta medför att nya versioner av ransomware ökar lavinartat [7].

MSB har sett indikationer på riktade ransomware-kampanjer mot Sverige och har gått ut med en varning kring det ökade hotet. I ett flertal rapporter från internationella instanser som exempelvis Cybersecurity Infrastructure Security Agency (CISA) och Federal Bureau of Investigation (FBI) antyds det att organisationer inom hälso- och sjukvårdssektorn är attraktiva mål för cyberattacker. Anledningen till att cyberkriminella väljer att attackera hälso- och sjukvårdssektorn är för att medicinsk data är värdefull och har påvisats vara användbar vid utpressning. Redan i juni 2020 publicerade MSB tillsammans med Försvarets radioanstalt (FRA), Polismyndigheten samt Säkerhetspolisen (SÄPO), ett dokument innehållande rekommendationer för att öka motståndskraften mot ransomware för organisationer inom hälso- och sjukvårdssektorn i Sverige. [6]

## 1.1. Bakgrund

Digitaliseringens framfart och den växande användningen av informationsteknik inom hälso- och sjukvårdssektorn har medfört att bland annat journaler och sjukhusutrustning numera lagras respektive sköts via digitala plattformar. Detta är en av de två stora anledningarna till att sjukhusen blivit attraktiva mål för ransomware-attacker. Den andra är bristande IT-säkerhet i sjukhusens system [8]. I detta avsnitt presenteras historia gällande ransomware för att ge läsaren en djupare förståelse för hur ransomware kommit att bli ett framgångsrikt verktyg vid digital utpressning.

År **1989** skapades det första ransomware-viruset, *AIDS Trojan*, av Joseph Popp. Popp infekterade 20 000 disketter med viruset som han sedan skickade till Världshälsoorganisationens (WHO) AIDS-konferens. Med hjälp av enkel symmetrisk kryptografi kunde viruset kryptera filnamn i datorernas hårddiskar. Det dröjde sedan till **2005** innan nästa ransomware-viruset skapades. Viruset fick namnet Trojan.Gpcoder men kallades även för GP Code och GPCoder. Genom social engineering kunde viruset spridas via spammejl som innehöll en bilaga med skadlig kod. Mejlet såg ut att komma från en trovärdig källa och bilagan utgavs för att vara ett jobberbjudande. Trojan.Gpcoder skapades i Ryssland av organiserade brottslingar och viruset drabbade främst invånare i Ryssland och dess grannländer [9].

År **2006** skapades Trojan.Cryzip som medförde att ransomware blev ett populärt verktyg för kriminella att använda vid utpressning. Med hjälp av viruset Trojan.Cryzip kunde angriparna kopiera och radera originalfilerna samt lagra dem i lösenordsskyddade arkiv. Samma år skapades också Trojan.Archiveus som fungerade på liknande sätt som Trojan.Cryzip. Istället för att kräva en lösensumma beordrades offren att handla medicin från en specifik webbshop. När köpet var genomfört fick de utsatta tillgång till ett lösenord som kunde användas för att återfå filerna [9].

Under **2007** dök Locker ransomware upp. Locker Ransomware krypterar inte offrens data utan låser ute dem från deras enhet och hindrar dem från att använda den. Angriparen begär att offret betalar lösensumman i kryptovaluta, för att i retur få tillbaka informationen eller få datorn återställd i funktionellt skick [4]. Ryssland var det första landet att bli drabbat av den sortens virus. En pornografisk bild visades på offrets enhet och denne krävdes att betala för att få bilden borttagen. Betalningen skulle ske via SMS eller genom att ringa till ett betalningsnummer. Året därpå skulle Trojan.Gpcoder, som skapades 2005, återkomma i ny skepnad. **2008** kom det så kallade GPcode.AK som använde sig av RSA-kryptering med en 1024-bitars nyckel. GPcode.AK krypterade filer och lämnade ett meddelande i varje undermapp där filer hade krypterats. Angriparna begärde att offren betalade mellan $100 och $200 i specifika kryptovalutor vid namn e-gold eller Liberty Reserve [9].

I mitten av **2011** bröt ransomware-fenomenet ut ordentligt då anonyma betaltjänster blev populära. Under 2011 skapades ungefär 60 000 nya ransomware-virus. Under **2012** fortsatte ökningen av ransomware i kombination med de anonyma betaltjänsterna samt att ett toolkit vid namn Citadel dök upp på marknaden. Citadel medförde att kriminella på ett enkelt sätt kunde producera och distribuera ransomware till en kostnad av 3 000 dollar. Även toolkitet Lyposit släpptes under 2012. Detta toolkit hjälpte till att skapa ransomware som utgavs för att komma från polisiära myndigheter som baserades på datorns exakta platsinställningar. Viruset byggde på att ett pop-up-meddelande syntes på offrets skärm och påstod att enheten hade använts för barnpornografisk aktivitet, nedladdning av upphovsrättsskyddat material eller varit involverad i någon annan typ av kriminell aktivitet. Meddelandet innehöll också information gällande att

datorn har blivit låst av FBI eller annan myndighet. Denna version av Lyposit kallades Reveton [9].

Under **2013** återkom användning av crypto ransomware istället för locker ransomware eftersom det ansågs vara en mer framgångsrik metod. Den mest kända versionen av ransomware är CryptoLocker som är en typ av crypto ransomware. Crypto ransomware infekterar datorer och använder sig av både privata och publika krypteringsnycklar för att kryptera värdefulla filer på enheter. CryptoLocker begärde att en lösensumma skulle betalas inom tre dagar för offret skulle få sina filer dekrypterade igen. CryptoLocker fortsatte vara det mest populära utpressningsviruset att använda, även under **2014**. Det uppskattas att över 500 000 människor hade blivit utsatta för CryptoLocker ransomware och ungefär runt en procent betalade lösensumman. För att stoppa CryptoLocker startade rättsväsendet tillsammans med bland annat säkerhetsleverantörer *Operation Tovar*. Det resulterade i att de lyckades stänga ner servrarna som användes vid distributionen av CryptoLocker. Säkerhetsleverantörerna FireEye och Fox-IT fann databasen som lagrade alla dekrypteringsnycklar och erbjöd alla utsatta gratis dekryptering. Det uppskattades att de drabbade hade betalat närmare 27 miljoner amerikanska dollar i lösensummor till angriparna bakom CryptoLocker [9].

År **2015** passerade CryptoWall CryptoLocker i att vara den mest populära versionen av crypto ransomware på marknaden. De kriminella började använda sig av *ransomware-as-a-service* och med hjälp av en TOR-webbläsare kunde angriparna skapa ransomware-virus gratis. Under 2015 släpptes även LockerPin som inriktade sig på att infektera Android-system och byta ut deras PIN-kod. För att återfå kontrollen över sitt system begärdes en lösensumma på $500. Det dök även upp ett ransomware vid namn Linus.Encoder.1 som attackerade Linux-system. Viruset krypterade både lokala filer på datorn samt filer som användes i webbapplikationer [9].

Efter 2015 började kriminella se värdet i att attackera städer, samhällskritiska organisationer, institutioner och företag. WannaCry, SamSam och NotPetya har varit framgångsrika virus mot sjukhus runt om i världen. De här attackerna presenteras närmare i avsnitt **3.4. Ransomware-attacker som drabbat hälso- och sjukvårdssektorn**. I denna uppsats diskuteras det hur kriminella utnyttjat brister i IT-system och värdet av medicinska data för att utöva utpressning på olika sjukhus, med huvudfokus på sjukhus i Sverige.

# 1.2. Koppling till tidigare forskning

I dagsläget finns det inget underlag om hur de svenska sjukhusen bemöter och hanterar det ökade hotet av ransomware-attacker, samt om det finns IT-säkerhetsbrister inom organisationerna. Däremot finns en stor mängd tidigare forskning om ransomware, hur ransomware fungerar som utpressningsvirus och varför det är ett framgångsrikt verktyg vid cyberattacker mot olika typer av organisationer runt om i världen. Nedan finns liknande studier och artiklar som är användbara och som ligger till grund för positioneringen av denna uppsats.

## 1.2.1. Ransomware in Healthcare Facilities: A Harbinger of the Future?

En litteraturstudie som undersöker hur sjukvården har kommit att bli ett attraktivt mål för ransomware-attacker och vilka olika typer av ransomware-attacker som sjukhus runt om i USA har drabbats av. I arbetet tar de upp hur viktigt det är att utbilda personal inom informationssäkerhet, för att göra dem uppmärksamma om vilka hot som finns på nätet. De belyser också

att det är viktigt att utveckla en katastrof-återställningsplan om verksamheten faller offer för en ransomware-attack. Författarna utför dessutom två semistrukturerade intervjuer med respondenter från hälso- och sjukvårdssektorn [8]. Studien är användbar vid skrivandet av litteraturstudien, för att undersöka varför sjukhus är attraktiva mål för ransomware. Den största skillnaden från den här studien är att den inte kartlägger hur sjukhus i Sverige arbetar för att stå emot ransomware-angrepp.

### 1.2.2. A Socio-technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks

En vetenskaplig artikel som undersöker hur det på ett sociotekniskt tillvägagångssätt går att motverka ransomware-attacker och hur organisationer inom hälso- och sjukvårdssektorn kan vidta åtgärder för att säkra sina IT-system [10]. Studien diskuterar hur ransomware ska tas itu med, på ett sociotekniskt tillvägagångssätt. Det är också den största skillnaden gentemot den här studien, då den här inte använder sig av ett sociotekniskt tillvägagångssätt. Fokus i den sociotekniska rapporten ligger på hur angripare använder sig av social engineering vid ransomware-attacker. Det perspektivet tas upp även i den här uppsatsen men är inte huvudfokus.

### 1.2.3. Ransomware - Digitala kidnappare

En kvalitativ intervjustudie som granskar fyra svenska IT-företags uppfattning gällande IT-säkerhet och hur det går att gardera sig mot cyberattacker. Studien tar även upp vad ransomware är och hur det har utvecklats över tid [11]. Denna studie är användbar att utgå ifrån vid genomförandet av den kvalitativa intervjustudien. Den ligger främst till grund för utformandet av frågorna till intervjukandidaterna. Studiens främsta skillnad gentemot den här är att den kartlägger fyra svenska IT-företags uppfattning gällande IT-säkerhet och hur de skyddar sig mot ransomware. Inte desto mindre undersöker denna studie hur svenska sjukhus garderar sig mot det ökade hotet av ransomware.

### 1.2.4. A novel method for recovery from Crypto Ransomware infections

Ett arbete som analyserar fyra sorters ransomware samt utför ett experiment. Experimentet går ut på att infektera ett virtuellt system för att ta fram eventuella förslag på åtgärder för att återställa filer efter att ett system har blivit infekterat [12]. Studien skiljer sig gentemot den här eftersom den endast analyserar ransomware som fenomen och inte har något verksamhetsperspektiv. Resultat från studien är användbart för att det ligger till grund för ett av åtgärdsförslagen som ges till verksamheterna i denna studie.

## 1.3. Problemformulering

Ransomware har de senaste åren utvecklats till att bli ett mycket populärt verktyg för kriminella vid utförande av cyberattacker. Det anses vara ett effektivt sätt att utpressa personer, företag och samhällskritiska verksamheter eftersom det är svårt att skydda sig mot ransomware. En annan anledning till att ransomware blivit framgångsrikt är för att det är enkelt att utföra och kräver inte avancerad datakunskap. Dessutom kan kriminella lätt få tillgång till att köpa viruset billigt online [13].

Under rådande pandemi är sjukhusen under stor påfrestning och har inte råd att förlora kontrollen över sina system, eftersom det kan få förödande konsekvenser. Detta innebär att det är mer sannolikt att sjukhus betalar en lösensumma [14]. MSB har gått ut med att det finns ökad aktivitet av ransomware-kampanjer som är riktade mot svenska sjukhus [6]. I denna uppsats behandlas problemet gällande det ökade hotet av ransomware och kartlägger hur sjukhusen hanterar problemet. Det undersöks även huruvida de svenska sjukhusen lever upp till de rekommendationer som publicerats av MSB, FRA, Polismyndigheten och SÄPO. Utöver ovan nämnda undersökningsområden undersöks det hur sjukhusen hanterar de ökade cyberhoten och om det finns bristande IT-säkerhetsarbete inom organisationerna som måste förbättras för att minska risken för ransomware-attack.

Frågeställningar som besvaras i denna uppsats är följande:

1. **Hur upplever och hanterar den svenska sjukvården det ökade hotet av ransomware?**
2. **Upprätthåller sjukhusen i Sverige säkra IT-system och lösningar för att kunna motstå en ransomware-attack och följer de myndigheternas rekommendationer?**
3. **Hur kan säkerheten utvecklas på sjukhusen för att bättre stå emot ransomware-attacker?**

För att angripa frågeställningarna beaktas ransomware som fenomen samt kända ransomware-attacker som drabbat sjukvården runt om i världen. Frågeställningarna har valts eftersom de tar upp ett mycket aktuellt ämne. Antalet ransomware-attacker har ökat lavinartat mot samhällskritiska verksamheter, som exempelvis sjukvården de senaste åren. Därför är det viktigt att undersöka om hälso- och sjukvårdssektorn kan möta det ökade hotet. Dessutom finns det inte några tidigare arbeten som tar upp just den svenska sjukvårdens perspektiv på och hantering av ransomware-attacker.

### 1.3.1. Problematisering av frågeställningar

Uppsatsens fokus är att ta reda på hur IT-ansvariga på svenska sjukhus upplever det ökade hotet av ransomware-attacker. Fokuset är även att ta reda på vilka metoder och verktyg som verksamheterna använder sig av för att motverka att deras system infekteras av skadlig programvara. För att ge läsaren en grundläggande förståelse om vad ransomware är presenteras historiska aspekter samt hur fenomenet har utvecklats över tid. Gällande frågeställningarna kan problem uppstå på grund av att information som ligger till grund för arbetet omfattas av sekretess. Dessutom finns det risk att intervjukandidater väljer att inte ställa upp på grund av att

intervjufrågorna kan behandla konfidentiell information. Uteblivet deltagande kan leda till att frågeställningen inte kan besvaras och området blir svårt att kartlägga. Ett annat hinder som kan uppstå beträffande frågeställningarna är att få fram konkret statistik på hur ransomware-hotet har ökat mot hälso- och sjukvårdssektorn i Sverige. I dagsläget finns det begränsat med publikationer kring hur situationen ser ut i Sverige och mestadels finns det endast forskning kring hur läget ser ut i USA. Begränsningen av publikationer leder till svårigheter att hitta trovärdiga och relevanta källor för att besvara frågeställningarna.

# 2. Metod

Detta arbete utgörs av en kvalitativ litteraturstudie där information systematiskt samlas in, bearbetas och granskas. Tillsammans med den kvalitativa litteraturstudien genomförs en kvalitativ strukturerad intervjustudie för att kunna besvara arbetets frågeställningar. Vid genomförandet av en forskningsstudie är det viktigt att ha kunskap om de valda metoderna för att öka reliabiliteten och validiteten i arbetet [15]. Således presenteras i detta kapitel vilka forskningsmetoder som använts för att ge läsaren en djupare förståelse till varför arbetet är utformat som det är.

## 2.1 Litteraturstudie

En kvalitativ litteraturstudie genomförs för att ge läsaren en ökad förståelse om fenomenet ransomware och varför det är ett framgångsrikt digitalt utpressning-verktyg. Litteraturstudien har en kvalitativ ansats för att den ska beskriva ett fenomen och dess egenskaper, i detta fall ransomware [16]. Artiklar och rapporter samlas systematiskt in och analyseras för att kartlägga varför hälso- och sjukvårdssektorn är ett attraktivt mål för ransomware-attacker. Informationen ligger dessutom till grund för att skapa en förståelse för hur organisationer på ett effektivt sätt kan gardera sig mot utpressningsvirus. Den insamlade litteraturen ligger även till grund för utformandet av frågorna i den kvalitativa intervjustudien.

För att hitta relevant information genomförs en litteratursökning. Sökord som används vid framtagningen av informationen är främst; *Ransomware, Famous Ransomware attacks, Ransomware attacks against health care facilities, Ransomware sjukhus, Digitalisering sjukvård, Ransomware survey.* Sökningen sker genom olika databaser och sökmotorer; *IEEE Xplore, Web of Science Core Collection, Digitala Vetenskapliga Arkivet (DiVA),* Halmstad Högskolas *OneSearch, Google Scholar* samt *Google.se.* Källorna i litteraturstudien väljs utifrån ett källkritiskt perspektiv och autenticiteten är en övervägande faktor för att minimera risken för desinformation. Flera studier visar på att det är nödvändigt att söka information i olika databaser. Databaser som är relevanta att söka litteratur genom baseras på den frågeställning som besvaras i arbetet [16].

## 2.2. Kvalitativ intervjustudie

Studien bygger på en kvalitativ ansats och inriktar sig på att analysera, tolka och bilda uppfattning om människans personliga intryck, erfarenheter och upplevelser av omvärlden. I kvalitativ forskning, till skillnad från kvantitativ forskning, används sällan statistiska och siffermässiga metoder vid redovisning av resultat. Den kvalitativa ansatsen, med hjälp av strukturerade intervjuer, ligger till grund för att besvara frågeställningarna. Avsikten med strukturerade intervjuer är att skapa förståelse för hur respondenterna upplever en viss händelse eller ett fenomen. Den kvalitativa inriktningen ger respondenterna möjlighet att skildra sina subjektiva åsikter och på så sätt bidra till att nå målsättningen i arbetet [17].

Det finns olika inriktningar på intervjustudier; ostrukturerad, halv- eller semistrukturerad samt strukturerad intervju. I detta arbete används strukturerade intervjuer vilket innebär att frågorna är förutbestämda och ställs i samma ordning till samtliga deltagare. Målet med en strukturerad intervju är att alla medverkande ska uppfatta frågorna på ett likvärdigt sätt. En strukturerad

intervju underlättar analysen av insamlade data och datainsamlingen är fullständig efter varje genomförd intervju [17]. Intervjufrågorna utformas för att på bästa möjliga sätt besvara de frågeställningar som formuleras i arbetet. Frågorna delas in i fem huvudområden; Allmän information, Informationssäkerhetsarbete och IT-policys, Hårdvara/Mjukvara, Nätverk och kommunikation samt Personal och arbetsrutiner. Huvudområdena innehåller därefter huvudfrågor som besvaras samt eventuella följdfrågor beroende på omfattningen av deltagarnas svar. Frågorna i de strukturerade intervjuerna syftar till att undersöka hur respondenterna upplever det ökade hotet av ransomware-attacker. Syfte är även att utforska vilka metoder och verktyg som används för att motverka att systemen blir infekterade av skadlig programvara.

I kapitel **4. Resultat** sammanställs resultatet från intervjustudien i en tabell för att ge läsaren en överblick av resultatet. Detta medför att intervjustudien även har en kvantitativ inriktning eftersom resultatet presenteras i sammanställda siffror.

### 2.2.1. Forskningsetik

Den kvalitativa intervjustudien präglas av ett viktigt förhållningssätt som definieras av Vetenskapsrådet med texten:

> *En mycket viktig del av forskningsetiken rör frågor om hur personer som medverkar i forskning som försökspersoner eller informanter får behandlas. Det kan förefalla självklart att dessa personer i största möjliga utsträckning ska skyddas från skador eller kränkningar i samband med att de medverkar i forskning.* [18]

Enligt Vetenskapsrådet kan forskningsetiska krav delas in i fyra kategorier. Informationskravet innebär att de medverkande ska vara informerade om syftet för forskningen som genomförs. Att deltagarna själva styr över sin medverkan i forskningen definieras i samtyckeskravet. Konfidentialitetskravet innefattar reglering om hur konfidentiell information och personuppgifter ska behandlas på ett korrekt sätt. Slutligen får insamlade uppgifter endast användas för den publicerade forskningen och innefattas av nyttjandekravet [19]. Utifrån de fyra huvudkraven utformas ett informationsblad som förmedlas till respondenterna innan och under intervjun som förtydligar att det är frivilligt att medverka i studien och de kan själva avbryta deltagandet när som helst under studiens gång.

För att säkerställa att intervjustudien behandlas korrekt ur etiska aspekter nämns varken organisationer eller respondenter vid namn i arbetet. Information som kan användas i syfte att identifiera respondent, organisation samt konfidentiell information offentliggörs inte. Intervjuer med respondenterna spelas in och transkriberas därefter. Transkribering av intervjuerna är nödvändiga vid skrivandet av uppsatsen för att undvika desinformation. Transkriberingarna är anonyma och publiceras inte. Inspelningarna och transkriberingarna raderas efter att arbetet är genomfört. Resultatet från intervjuerna används för att undersöka huruvida de svenska sjukhusen lever upp till rekommendationer som publicerats av MSB, FRA, Polismyndigheten och SÄPO. Resultatet används även för att utforma åtgärdsförslag till verksamheterna ifall brister identifieras för att minimera risken att de faller offer för ransomware.

## 2.3. Intervjuprocess

Intervjuerna har genomförts med respondenter som ansvarar för IT-system på sjukhus runt om i Sverige. Respondenterna kommer från olika regioner, spridda över hela Sverige. Regionerna är representativa över hela landet eftersom de både är landsbygds- och storstadsregioner. Intervjuerna genomfördes med en kvalitativ strukturerad ansats. Den kvalitativa inriktningen gav respondenterna möjlighet att skildra subjektiva åsikter om det ökade hotet av ransomware-attacker mot hälso- och sjukvården. Förfrågningar skickades ut till 15 kandidater via mejl och webbtjänsten LinkedIn. Av totalt 15 kandidater var det 3 som tackade ja till att ställa upp i studien. I samband med första kontakten skickades ett informationsblad ut till respondenterna. Formuläret innehöll en sammanställning av hur konfidentiell information behandlas i studien samt att allt deltagande är frivilligt och helt anonymt. Även frågorna bifogades för att underlätta för respondenterna. Intervjuerna skedde digitalt via Zoom eller Teams och tog mellan 16–26 minuter. Samtalen spelades in och transkriberades.

## 2.4. Metoddiskussion

Valet av metoder baseras främst på vilka som använts i tidigare forskning [8, 10, 11]. Både litteraturstudie och intervjustudie med kvalitativa ansatser är vanligt förekommande inom arbeten rörande ransomware. Därför anses metoderna vara fördelaktiga vid den här typen av arbete. Eftersom litteraturstudie och intervjustudie använts frekvent inom tidigare forskning kan det vara svårt att bidra med nya infallsvinklar och tillföra något nytt inom forskningsområdet. Här undersöks dock ett område i detta arbete som inte tidigare har kartlagts, det vill säga den svenska sjukvården. På så sätt bidrar detta arbete således till forskningen trots att valet av metod är detsamma som i tidigare genomförda arbeten.

Metoderna som används i arbetet är även valda utifrån förmågan att besvara frågeställningarna som formuleras. I tidigare arbete utförs experiment för att ta reda på hur olika sorters ransomware fungerar och för att ta fram åtgärder för att stoppa dem [12, 41]. Utförande av experiment används inte i det här arbetet eftersom syftet är att kartlägga hur läget kring ransomware ser ut på sjukhus i Sverige och ta fram åtgärdsförslag utifrån det. Ingen teknisk analys behöver genomföras för att besvara frågeställningarna i arbetet och därför utförs inget experiment. Eftersom studiens syfte är att få en inblick i sjukhusens uppfattning och hantering av det ökade hotet av ransomware anses intervjustudie vara relevant.

Litteraturstudie väljs som metod för att det i dagsläget finns en stor mängd disponibel information om fenomenet ransomware. Informationens syfte är att ge läsaren en god förståelse för hur ransomware kommit att bli ett framgångsrikt digitalt utpressnings-verktyg. Det finns dessutom en mängd publikationer om hur sjukhus runt om i världen har fallit offer för utpressningsvirus och hur de ska gardera sig mot ransomware [1, 31, 32, 33, 34, 35, 36, 37, 38, 39]. Däremot finns det avsaknad av studier som visar hur Sveriges sjukhus jobbar för att motverka ransomware-attacker och skadlig mjukvara. Att använda litteraturstudie som metod anses vara fördelaktigt för att genom datainsamling kartlägga en omfattande bild beträffande ämnet. Studien i detta arbete bygger på att samla in och källkritiskt granska tidigare utgiven forskning ur ett vetenskapligt perspektiv. Detta leder till att resultatet som presenteras är sekundärdata. Nackdelen med sekundärdata är att den kan vara manipulerad och därav leda till desinformation. Detta innebär att källkritik är en viktig faktor vid granskning av denna typ av information.

Målsättningen med den kvalitativa intervjustudien är att undersöka vilka metoder och verktyg de svenska sjukhusen använder för att avvärja infektion av sina IT-system. Studiens ändamål är att utifrån intervjuerna kartlägga om det finns brister i deltagarnas system som behöver åtgärdas eller förbättras. Utifrån svaren i undersökningen tas åtgärdsförslag fram för att minimera risken att svenska sjukhus blir lätta måltavlor för cyberkriminella att utnyttja. Det finns flera fördelar med att använda kvalitativ, strukturerad intervjustudie som exempelvis att det förenklar organiseringen av insamlad data. Det försvårar också möjligheterna att påverka deltagarna, vilket medför att svaren som fås är deras subjektiva erfarenheter och åsikter inom området. Däremot existerar vissa nackdelar med metoden, som exempelvis att frågorna standardiseras vilket kan medföra att naturligheten och relevansen försämras i både frågorna och svaren under intervjun. En annan svårighet kan vara att det blir en stor mängd insamlad information som ska bearbetas, analyseras och göras förståelig för läsaren [17].

# 3. Litteraturstudie

Detta kapitel är relevant för att ge läsaren en övergripande förståelse för ransomware och varför hälso- och sjukvårdssektorn är attraktiva mål för ransomware. Även de skydd som finns mot ransomware i dagsläget redovisas i avsnittet. All information som redovisas i kapitlet är insamlad genom litteratursökningen och innefattar arbetets litteraturstudie. Allt som redovisas används tillsammans med resultatet från den kvalitativa intervjustudien vid besvarandet av arbetets frågeställningar i kapitlen **5. Diskussion** samt **6. Slutsats.**

## 3.1. Olika typer av malware

Malware är ett samlingsbegrepp som ursprungligen kommer från det engelska språket och är en sammansättning av *malicious* som betyder skadlig och *software* som betyder programvara på svenska. Malware är således en skadlig programvara som skapas av cyberkriminella med avsikten att sabotera datorer, servrar, datornätverk och IT-system eller för att stjäla konfidentiell information [20]. Det finns olika typer av skadliga programvaror som exempelvis virus, maskar, trojanska hästar och ransomware [21].

### 3.1.1. Virus

Ett virus är en skadlig programvara som kopplas till en fil eller ett dokument som stöder makron för att exekvera dess kod och sprida viruset vidare. Virus sprids ej omedelbart när de har laddats ner på en enhet, utan filen eller dokumentet innehållande den skadliga programvaran måste öppnas och användas för att de ska kunna spridas. Virus är skapta för att rubba ett systems förmåga att fungera normalt och det kan resultera i att virus kan orsaka operativa problem samt dataförlust [21].

### 3.1.2. Maskar

Maskar är ett malware som har förmåga att snabbt replikeras och spridas till enheter inom ett nätverk. Till skillnad från virus behöver inte maskar en fil eller ett dokument för att spridas. Maskar infekterar enheter och sprids via en nedladdad fil eller en nätverksanslutning och sprids sedan vidare genom att multipliceras. Maskar är även skapta för att påverka och störa en enhets funktionalitet och orsaka dataförlust [21].

### 3.1.3. Trojanska hästar

En trojansk häst är en sorts skadlig programvara som utger sig att vara ett legitimt program. Med hjälp av social manipulation så luras användare till att köra programmet som aktiverar den trojanska hästen. När den skadliga programvaran aktiverats får cyberkriminella tillgång till att spionera och stjäla konfidentiell information på offrets dator. Förövaren får också möjlighet att modifiera, blockera och radera data från offrets dator. I motsats till virus och maskar så har inte trojanska hästar förmåga att reproducera sig själv [21].

### 3.1.4. Ransomware

Ransomware är en skadlig programvara som används av cyberkriminella vid datorbaserad utpressning. Crypto ransomware och locker ransomware är de mest förekommande typerna av ransomware-virus som används i dagsläget. Crypto ransomware infekterar datorer och krypterar värdefulla filer på enheter. Locker Ransomware krypterar inte offrens data utan låser ute dem från deras enhet och hindrar dem från att använda den. Angriparen hänvisar sedan de utsatta att betala en lösensumma i kryptovaluta för att i retur få tillbaka informationen eller få datorn återställd i funktionellt skick. Vanligtvis vill skadlig programvara inte bli upptäckt av användaren, däremot måste ransomware exponeras för offret för att kunna begära en lösensumma. Eftersom locker ransomware inte krypterar filerna på enheten utan bara låser ute användaren så är det möjligt att flytta hårddisken från den infekterade enheten till en fungerande enhet. Genom att flytta en hårddisk från en infekterad enhet till en fungerande är det möjligt att ta bort den skadliga programvaran och återställa hårddisken. Det här innebär att locker ransomware anses som ett sämre alternativ för att få offret att betala ut en lösensumma [9].

Crypto ransomware är i nuläget den vanligaste typen av ransomware som cyberkriminella använder sig av. Crypto ransomware använder olika krypteringstekniker för att göra data oåtkomlig för den utsatta [22]. Denna variant av ransomware infekterar obemärkt en enhet och kommunicerar med en Command and Control (C&C) server som sköter distribution av krypteringsnycklarna. När den skadliga programvaran har infekterat enheten extraheras krypteringsnycklarna och krypterar offrets filer. När krypteringen är slutförd dyker ett meddelande upp på datorns skärm som meddelar offret att deras filer ej längre är tillgängliga och återfås när en lösensumma betalas. Om lösenkravet uppfylls lovar angriparna att skicka en dekrypteringsnyckel så att de krypterade filerna kan låsas upp [23]. Däremot finns det inga garantier för att angriparna verkligen håller sitt löfte och tillhandahåller en dekrypteringsnyckel till offren efter att de tagit emot lösensumman [24].

Beroende på vilken typ av krypteringsteknik ett crypto ransomware använder klassificeras de antingen som symmetriska-, asymmetriska- eller hybrid crypto ransomware. Symmetriska crypto ransomware använder symmetrisk kryptografi vilket innebär att samma nyckel används vid kryptering och dekryptering. Asymmetriska crypto ransomware däremot använder en publik nyckel för kryptering och en privat nyckel för dekryptering. Sedan finns hybrid crypto ransomware som både använder symmetrisk- och asymmetrisk kryptografi [25].

## 3.2. Hur ransomware sprids

Cyberkriminella använder olika typer av attack-vektorer för att lura offer till att aktivera skadlig kod. Vanligt förekommande vektorer är social engineering (phishing), brute-force authentication credentials, exploit kits, malvertising och drive-by nedladdning. De olika attack-vektorerna skiljs åt baserat på komplexitet och effektivitet [23].

Vanligtvis använder hackare social engineering för att sprida ransomware. Med hjälp av social engineering eller någon typ av psykologisk manipulation utnyttjar cyberkriminella den mänskliga faktorn till att avslöja konfidentiell information eller att användaren ska begå misstag [10]. Angriparna brukar designa falska e-postmeddelanden som ser ut att komma från en legitim källa. Phishing-mejl innehåller infekterade länkar, bilagor eller dokument som innehåller makron. Om den utsatte råkar klicka på länken, bilagan eller öppnar ett dokument i e-postmeddelandet så laddas den skadliga programvaran ner och smittar enheten [25].

Brute-force authentication credentials är en annan vanligt förekommande attack-vektor. Angriparna använder automatiserade skript som systematiskt granskar alla möjliga inloggningsuppgifter och lösenord tills de har identifierats. Sedan använder hackarna de identifierade inloggningsuppgifterna till att logga in i offrets system och sprida den skadliga programvaran [23]. Angriparna brukar vanligtvis använda brute-force authentication credentials på Remote Desktop Protocol (RDP) för att få tillgång till Windows-system. Anledningen till detta är att många RDP-portar är exponerade på internet, vilket gör dem till lätta måltavlor för att genomföra distribuerade brute-force attacker [26].

Exploit kits är toolkit som cyberkriminella också nyttjar för att sprida ransomware. Med hjälp av ett exploit kit kan angriparna skanna efter sårbarheter i system för att kunna distribuera den skadliga koden [23]. Angler, Magnitude och Neutrino är tre vanliga exploit kits som kriminella använder vid digital utpressning [25]. Sårbarheter kan exempelvis vara Windows Server 2003 och Windows Server 2008 som ej längre stöds av Microsoft och inte längre får säkerhetsuppdateringar. Det kan även vara felkonfigurerade webbservrar, backup-servrar eller elektroniska journalsystem [27].

Malvertising är när angripare gömmer en bit kod i en legitim annons på nätet. När användaren klickar på annonsen omdirigeras offret till en server som innehåller skadlig programvara. När användarens enhet är uppkopplad på den infekterade servern så utför angriparna ransomware-attacken [28].

En drive-by nedladdningsattack innebär att skadlig programvara laddas ner oavsiktligt på en enhet utan offrets kännedom. Detta betyder att användaren endast behöver besöka en webbsida utan att trycka på något eller ladda ner någon programvara. Med hjälp av drive-by nedladdning kan kriminella sedan utnyttja webbläsare, applikation eller operativsystem som innehåller säkerhetsbrister för att sprida skadlig kod [29].

## 3.3. Varför är sjukhus ett attraktivt mål för ransomware-attacker?

På grund av digitaliseringen har hälso- och sjukvårdssektorn moderniserats med innovativa IT-lösningar [6]. Det här innebär att journaler och sjukhusutrustning numera lagras respektive sköts via digitala plattformar [8]. Det finns två stora nackdelar med digitaliseringen och de är beroendet av fungerande IT-system samt att systemen exponeras. Ett annat problem som uppstår är när digitaliseringen ökar snabbare än säkerhetsarbetet i IT-miljön [6]. Om inte säkerhetsarbetet hänger med digitaliseringen så skapas det säkerhetshål som cyberkriminella kan utnyttja vid en attack [8].

En annan anledning till att cyberkriminella riktar angreppet mot hälso- och sjukvårdssektorn är för att medicinsk data är värdefull och mycket användbar vid utpressning [6]. Under rådande pandemi är sjukhusen under stor påfrestning och har inte råd att förlora kontrollen över sina system, eftersom det kan få förödande konsekvenser. Cyberbrottslingar tror således att sjukhus sannolikt kommer betala lösensumman [14]. Därför är det viktigt under pågående kris att sjukhusen följer etablerade IT-säkerhetsprocesser samt rutiner. Det är även viktigt att sjukhusens IT-personal fokuserar på löpande underhåll av systemen för att undvika säkerhetsluckor [8].

Bland de tio mest attackerade industrierna så motsvarar sjukvården 6,6% av attackerna. Det motsvarar i sin tur att sjukvården var den sjunde mest attackerade industrin under 2020. Året innan hamnade sjukvården på en tionde plats och stod för endast 3% av attackerna. Detta påvisar en markant ökning till följd av COVID-19 pandemin. Nästan 28% av alla attacker mot sjukvården 2020 bestod av ransomware-attacker [30]. Patienters liv kan äventyras om sjukhus drabbas av ransomware-attacker. En kvinna i Düsseldorf, Tyskland 10 september 2020 miste livet i samband med en ransomware-attack. Som följd av attacken tvingades sjukhuset omdirigera patienter i behov av akutvård till närliggande sjukhus. Den avlidne kvinnan skickades till ett sjukhus 20 mil bort och på grund av kvinnans redan livshotande tillstånd och fördröjningar av vård gick hennes liv inte att rädda [1]. Däremot fastställde tyska myndigheter att ransomware-attacken inte hade en avgörande roll i dödsfallet [30].

Under 2020 var ransomware utan tvekan den populäraste attack-typen som cyberkriminella använde [30]. Användandet av ransomware tredubblades under fjolåret och 49% av alla svåra incidenter utgjordes av utpressningsvirus. Ökningen tyder på att fler och fler cyberbrottslingar anser att ransomware är lönsamt. Lösensummorna ökade med 31% under fjolåret och den högst krävda lösensumman var 290 miljoner svenska kronor [31].

Av alla ransomware-attacker som utfördes under 2020 användes dubbel utpressningsstrategi till 95%. Dubbel utpressning innebär att angriparna inte enbart krypterar data, utan också stjäl den och hotar organisationerna att läcka ut känslig information om en lösensumma inte betalas. Anledningen till att cyberbrottslingar har börjat använda dubbel utpressningsstrategi är på grund av att organisationer kan välja återställa systemen med hjälp av säkerhetskopior och därmed slippa betala lösensumman. Ransomware-typerna som i dagsläget är mest framgångsrika är Sodinokibi, Nefilim, RagnarLocker, Netwalker, Maze, Ryuk och EKANS [30].

## 3.4. Ransomware-attacker som drabbat hälso- och sjukvårdssektorn

I följande avsnitt presenteras ransomware-attacker som har drabbat sjukhus runt om i världen under de senaste åren. Avsikten med detta avsnitt är att ge läsaren en insikt i vilken sorts konsekvenser en ransomware-attack kan orsaka. Syftet är också att ge läsaren en inblick i hur en ransomware-attack kan gå till och hur cyberkriminella utnyttjar sårbara system. Händelserna redovisas i kronologisk ordning.

### 3.4.1. Medstar Health

Den största vårdaktören i Maryland och Washington D.C. blev 2016 utsatta för en omfattande ransomware-attack där bland annat system innehållande information samt patientdata stängdes ner. Innan attacken skedde hade angriparna upptäckt att Medstar använde sig av en applikationsserver som då hette JBoss men idag heter Wildfly. Det är en applikationsserver som används för att implementera framförallt Java-program [32]. JBoss utvecklades av Red Hat, som framställer open source-koder som är fria för allmänheten att använda. Det fanns däremot en baksida med användning av JBoss. Mjukvaran konfigurerades ofta felaktigt, vilket gjorde det enklare för utomstående att komma in i nätverket. USA:s regering, tillsammans med bland annat utvecklarna av JBoss Red Hat Inc. gick ut med varningar att det fanns risk att utomstående

kunde få tillgång till nätverket om inte mjukvaran konfigurerats korrekt. Varningen kom ut första gången i februari 2007 och ytterligare en gång i mars 2010 [33].

För att testa och utnyttja JBoss servrar fanns ett open source verktyg vid namn JexBoss. Detta verktyg användes vid attacken för att ta sig in i systemet. När angriparna väl kommit in i systemet började de kryptera olika Windows-funktioner med hjälp av SamSam ransomware [34]. Vid attacken mot Medstar Health krävdes en lösensumma på 45 bitcoins, vilket då motsvarade ungefär 19 000 dollar för att låsa upp hela systemet. Det gick också att låsa upp enskilda datorer, vilket kostade 3 bitcoins per enhet, motsvarande ungefär 1 250 dollar. Krypteringsnyckeln skulle förstöras om inte betalningen skedde inom 10 dagar och då skulle all tillgång till systemet gå förlorat [33].

När attacken upptäcktes togs ett beslut om att alla elektroniska journalsystem skulle stängas ner vilket ledde till att all personal fick skriva allt för hand. Detta utgjorde en risk för patienterna som vårdades men det stoppade spridningen av den skadliga koden. Medstar tog också beslutet att inte betala lösensumman utan återskapade istället systemet från lagrade backuper, vilket resulterade i att 90% av funktionaliteten var säkerställd mindre än en vecka efter attacken. På grund av varningarna som kom ut till allmänheten 2007 och 2010 finns det anklagelser mot Medstar, grundade på att de borde ha åtgärdat sårbarheten som fanns i mjukvaran JBoss [33].

### 3.4.2. WannaCry

Fredagen den 12:e maj 2017 upptäcktes krypterade filer i över 300,000 datorer installerade med Microsoft Windows operativsystem. Personer och organisationer i 150 länder var drabbade. Det skulle upptäckas att de fallit offer för en ransomware-attack vid namn WannaCry. Viruset inriktade sig på en bred målgrupp, innehållande bland annat branscher som hanterar frakt och transport, energi, telekommunikation samt sjukvård [35]. Hälso- och sjukvårdssektorn i Storbritannien, Spanien och Indien blev utsatta för attacken. Den vårdansvariga myndigheten National Health Service (NHS) i Storbritannien drabbades värst av attacken, trots att de inte var en direkt måltavla för viruset [35, 36]. Ungefär en tredjedel av alla sjukhus runt om i England upplevde störningar när attacken ägde rum. Totalt en procent av NHS Englands sjukvård påverkades som en direkt följd av viruset. Attackens störningar medförde att patienter fick omdirigeras till kringliggande sjukhus, vilket i sin tur ledde till att färden till akutvård blev längre. Den 16:e maj kunde omdirigeringarna upphöra. Sammanlagt var det fem akutmottagningar som fick ge direktiv om att föra patienter till andra sjukhus. Utöver omdirigeringen av akutpatienter fick cirka 1,2% av alla planerade patientbesök ställas in under den vecka som attacken pågick på sjukhusen [36].

Viruset WannaCry efterlämnade stora kostnader för de drabbade sjukhusen, framförallt i form av arbetad övertid, återställningskostnader samt ökad IT-support. Vårdenheter som inte smittats påverkades också av attacken och flera funktioner stängdes ner för att förebygga att fler enheter blev infekterade. Till följd av nedstängningen av exempelvis mejlsystem hämmades kommunikationen och vissa svårigheter i att bedriva verksamheten uppstod. Hanteringen av attacken gjordes utifrån NHS så kallade EPRR-modell (*Emergency, Preparedness, Resilience and Response*) som består av tre faser. Första fasen varade från 12:e till 14:e maj och största fokus låg på att säkerställa akutvårdens funktionalitet. 13:e till 15:e maj varade fas två som bestod av att fastställa att primärvården hade stabil funktionalitet. Den tredje och sista fasen varade fram till attackens avslut, 19:e maj. Den innefattade reparationer av system samt

uppdatering av virusskydd och gjordes löpande. Den 19:e maj, exakt en vecka efter attackens utbrott, var alla drabbade vårdenheter återhämtade [36].

Viruset WannaCry hör till kategorin *självspridande datormaskar* och är ett ransomware-virus. Det finns flera källor på att viruset spreds genom automatiska sökningar efter sårbara system. När det fått fäste i ett nätverk krypterade det filerna och, till skillnad från tidigare crypto ransomware, sprids det vidare i det interna systemet. Viruset spreds också ut utanför det först infekterade nätverket. Efter att filerna krypterats visades ett meddelande på hela skärmen som beordrade användaren att betala 300 US Dollar i motsvarande värde av kryptovalutan Bitcoin för att åter få tillgång till filerna. WannaCry-viruset kunde spridas vidare i det interna systemet genom en bugg i Microsofts *Service Message Block*-protokoll. Däremot hade Microsoft redan i mars samma år som attacken skedde gått ut med en uppdatering som åtgärdade buggen och efter attacken gick de ut med en uppdatering för operativsystemet Windows XP [34]. En av virusets funktioner gick ut på att anropa en fiktiv domän (*iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com)* och vid svar från denna avbröts körningen av WannaCry. Genom att göra en registrering av domännamnet kunde spridningen av viruset stoppas inom systemet [37].

Flera källor påstår att det finns ett samband mellan ransomware-attacken WannaCry och den en hackergrupp vid namn Lazarus. En nordkoreansk hacker vid namn Park Jin Hyok pekades ut av FBI för att ha kopplingar till hackergruppen samt inblandning i attacken WannaCry. Han pekas även ut för att ha kopplingar till det nordkoreanska styret. Det är svårt att fastställa att hackergruppen Lazarus faktiskt låg bakom attacken men det spekuleras om tre olika scenarier. Antingen iscensatte Lazarus WannaCry, någon hade tillgång till Lazarus verktyg eller tog inspiration från gruppen. Det går inte heller att fastställa huruvida gruppen har kopplingar till Nordkorea eller inte [36].

### 3.4.3. NotPetya

I många fall kan Petya och NotPetya förväxlas för att vara olika namn på samma virus, det är inte riktigt rätt. Det är två olika virus men ingår i samma ”familj”. Närmare bestämt, NotPetya är en vidareutveckling på viruset Petya [34]. Petya kommer presenteras kort i detta avsnitt för att ge en djupare förståelse för vad NotPetya är. Fokus kommer ligga på NotPetya eftersom det var det av virusen som attackerade och infekterade enheter inom sjukvården.

Viruset Petya spreds via dokument som infekterats och skickats som bilagor i mejl. När användaren öppnade bilagan frågade Windows om administratörsrättigheter i syfte att göra ändringar i systemet. När detta beviljats började viruset att skriva över huvudstartssektorn (MBR) samt kryptera huvudfiltabellen (MFT). MFT innehåller information om var alla andra filer i systemet finns och när den krypteras tappar användaren samt systemet tillgång till filerna. Offret krävdes sedan på en lösensumma som skulle betalas i Bitcoin för att återfå förfogandet av sitt system [36].

Petya upptäcktes i maj 2016 och drygt ett år senare, 27 juni 2017, upptäcktes vad som troddes vara ett nytt utbrott av Petya-viruset. Det skulle däremot framkomma att viruset inte var detsamma men tillhörde den så kallade Petya-familjen. Viruset fick namnet NotPetya och skillnaden gentemot föregångaren var att detta virus var utformat som en mask som själv kunde spridas inom och mellan system [36]. Den första versionen av nätverksprotokollet Service Message Block innehöll en svaghet som utnyttjades vid spridningen av NotPetya. Sårbarheten har fått namnet EternalBlue [38]. Utöver utnyttjandet av EternalBlue kunde viruset samla in

uppgifter som använts vid inloggning i det redan infekterade systemet och kunde på så sätt spridas vidare. NotPetya var, enligt säkerhetsföretaget Cisco, det mest snabbspridda viruset de sett genom tiderna. NotPetya användes som alla andra utpressningsvirus för att tjäna pengar [36]. Därmed krävdes användaren på $300 i Bitcoin för att få sitt system dekrypterat [38].

Det som skiljer NotPetya från många andra utpressningsvirus är att den nyckel som användes vid kryptering och som också skulle användas vid dekryptering inte sparades. Det ledde till att användaren inte kunde få systemet återställt, trots att de betalade lösensumman. På grund av avsaknaden av möjlighet att återställa systemet är det många som anser att NotPetya inte kan räknas som ett gisslanvirus, utan en skadlig programvara vars enda syfte är att åsamka förstörelse [37].

NotPetya-attacken inleddes med att attackera det ukrainska företaget Intellect Service. Företaget står för en redovisningsmjukvara vid namn M.E.Doc som ska ha använts av ungefär 90% av näringslivet i Ukraina. Attacken skedde genom att angriparna placerade en bakdörr i programmet M.E.Doc och när kunderna installerade uppdateringen av mjukvaran medföljde också bakdörren. Genom detta kunde angriparna få tillgång till IT-systemet med den installerade mjukvaran. När systemet infekterats var det svårt att stoppa ytterligare spridning av viruset. Det upptäcktes sedan att det gick att hindra NotPetya genom att skriva i filen C:\Windows\perfc.dat och därmed stoppa den pågående attacken [36].

NotPetya drabbade flera länder runt om i världen, som exempelvis Ryssland, Indien, Sverige och Nederländerna. De länder som drabbades inom flest sektorer var dock Ukraina och USA, där bland annat hälso- och sjukvårdssektorn drabbades. I Ukraina drabbades fyra stora sjukhus samt Kievs största klinik, Boris-kliniken. På kliniken upplevdes störningar i alla datorer, utom de som användes i medicinteknisk utrustning. I Ukraina finns en lag som innebär att all patientinformation ska sparas i 25 år och indirekt bröt kliniken mot denna lag eftersom attacken slog ut deras journalsystem. Däremot fanns det säkerhetskopior av viktiga data som kunde minska förlusten av information. Personalen fick däremot arbeta manuellt med penna och papper istället för det digitala de var vana vid [36].

Det andra landet där hälso- och sjukvårdssektorn drabbades av attacken var USA. Tre sjukhus i USA föll offer för attacken, två i västra Pennsylvania och ett i West Virginia. Sjukhusen i Pennsylvania tillhörde sjukhusnätverket Heritage Valley Health Systems. En kapacitet på cirka 500 sängar på de båda sjukhusen gick förlorad under attacken och minst en operation var tvungen att flyttas fram. Patienter på sjukhusen fick dessutom omdirigeras till andra mottagningar. I West Virginia drabbades sjukhusen Princeton Community Hospital där det upplevdes störningar i leverans- och godshanteringssystem. Resultatet var att hela nätverket inom organisationen fick bytas ut [36].

IT-företaget ESET påstår att det finns kopplingar mellan NotPetya och en hackergrupp vid namn Telebots. Telebots var inblandade i ett angrepp där det upplevdes störningar i Ukrainas elnät år 2015. Kopplingarna kan dras på grund av likheter i verktyg som använts i båda attackerna. Det finns dock inga konkreta bevis på att det är hackergruppen som ligger bakom cyberattacken NotPetya. Enligt ESET har dock Telebots redan tidigare använt utpressningsvirus i andra syften än att utkräva lösensummor. Att det finns likheter i utförandet av attackerna behöver inte betyda att angriparna är desamma, menar IT-säkerhetsföretaget Kaspersky Lab. Ytterligare ett annat IT-säkerhetsföretag, FireEye, vill påstå att hackergruppen Telebots kan ha kopplingar till den ryska staten. Hackergruppen kallas även för Sandworm av företaget FireEye. National Security and Defense Council of Ukraine (NSDCU) tillsammans med säkerhetstjänsten SBU i Ukraina anklagar Ryssland för att ligga bakom attacken. De baserar anklagelserna

på att attackens syfte inte var att tjäna pengar utan snarare agera täckmantel för att skapa störningar. I november 2017 drogs slutsatsen att det var mycket sannolikt Rysslands militära underrättelsetjänst, GRU, som låg bakom attacken. Detta framkom i en hemligstämplad rapport från CIA och enligt dem arbetade skaparna bakom attacken för det så kallade Huvudcentret för Speciell Teknologi (GTsST). GTsST tillhör GRU och arbetar med offensiva cyberoperationer [36].

### 3.4.4. Düsseldorf University Clinic

Den 10 september 2020 stängdes flera system innehållande bland annat journaler ner och blev otillgängliga för personalen på ett sjukhus i Düsseldorf, Tyskland. Det skulle visa sig att sjukhuset vid namn Düsseldorf University Clinic hade utsatts för en ransomware-attack. Angriparna kom in i systemet via en så kallad ”allmänt använd” tilläggsprogramvara. Totalt krypterades 30 servrar tillhörande sjukhuset under attacken. Kliniken tvingades omdirigera patienter till närliggande sjukhus. En kvinna i livshotande tillstånd fick köras till ett sjukhus 20 mil bort men hennes liv gick inte att rädda och hon avled [1]. Däremot fastställde tyska myndigheter att ransomware-attacken inte hade en avgörande roll i dödsfallet [31].

Vid attacken fanns det ingen information om betalning. Istället fick sjukhuset kontaktuppgifter där de ombads att ta kontakt. Genom meddelandet med kontaktinformationen kunde slutsatsen dras att attacken med största sannolikhet var menad mot Heinrich Heine University. Universitetet och sjukhuset har anknytning till varandra men ligger i olika byggnader. Sjukhuset kontaktade polisen som i sin tur kontaktade angriparna enligt uppgifterna som lämnades i meddelandet i samband med attacken. När angriparna blev införstådda i att det var sjukhuset som drabbats lämnade de ut dekrypteringsnyckeln och stängde ner kommunikationen [39].

## 3.5. Befintliga skyddsrutiner mot ransomware

Även om det inte är möjligt att förhindra ransomware-angrepp, så finns det förebyggande åtgärder som organisationer kan vidta för att minimera risken att falla offer. För att säkerställa att verksamheten kan hantera en eventuell attack och begränsa skadan är det viktigt att kontinuerligt arbeta med IT-säkerhet. Det är även betydelsefullt att utbilda personal, ha bra backup-rutiner och återställningsplaner [10]. Det är även viktigt att snabbt kunna återställa IT-miljön vid en attack så att verksamheten kan återgå till normal funktion. Snabb återställning kan även vara betydelsefullt för att hålla nere kostnaderna vid hantering av ett angrepp [6].

### 3.5.1. Backup-rutiner

För att en verksamhet ska kunna stå emot en ransomware-attack är det viktigt att skapa en regelbunden säkerhetskopieringsprocess för data samt systemkonfigurationer [10, 6]. Det innebär att säkerhetskopieringen bör ske kontinuerligt, minst en gång per dygn [10]. Säkerhetskopiorna rekommenderas att lagras offline och offsite för att vara oåtkomliga för oinvigda. Dessutom är det viktigt att testa säkerhetskopiorna på daglig basis för att säkerställa att de fungerar. Det är även viktigt att ha fungerande återställningsrutiner för att systemet ska kunna återgå till normaltillstånd så snabbt som möjligt efter en attack [6, 10]. Inom organisationen är det också viktigt att IT-personalen regelbundet tränar på att återställa säkerhetskopiorna för att de ska veta hur de ska gå tillväga om en attack sker [40].

Enligt statistik från Truesec saknade 60% av de drabbade organisationerna ordentliga backuper under 2020. Att krävas på lösensumma är inte det största hotet vid en attack, det är snarare att systemet kan vara oåtkomligt under en längre period. Dessutom kan data gå förlorad och organisationer kan förlora stora summor pengar. Om en verksamhet handlar snabbt vid utbrottet av ett utpressningsvirus, kan det gå att rädda 90% av all data, med hjälp av backuper [31].

### 3.5.2. Systemuppdateringar

För att bidra till en resilient IT-miljö är det viktigt att kontinuerligt uppdatera operativsystem, applikationsprogramvaror, webbläsare och -servrar, antivirusprogram, firmware samt brandväggar till de senast släppta versionerna [10]. Skälet till detta är att säkerställa att mjukvaror och operativsystem uppfyller leverantörernas rekommendationer [6]. Genom att ständigt uppdatera systemen går det att åtgärda många fel som cyberbrottslingar utnyttjar för att sprida skadlig kod [41]. Dessutom borde sjukhusens IT-personal testa uppdateringarna med resterande delar av systemet innan de implementeras, för att säkerställa att allt är kompatibelt för att inte oförutsedda problem ska dyka upp [10].

### 3.5.3. Nätverkssegmentering

I en IT-miljö spelar säker nätverksinfrastruktur en avgörande roll. Om ett nätverk används av flera tjänster och inte är segmenterat kan angripare agera fritt i IT-miljön. En viktig del i att säkra nätverket är segmentering, det vill säga att dela upp nätverket, både fysiskt och logiskt. Fysisk separation innebär att ett nätverk är avskilt från andra nätverk och här bör den mest skyddsvärda informationen bevaras. Logisk separation innebär att nätverket är sammankopplat rent fysiskt men är istället uppdelat i exempelvis VLAN. För att säkra nätverket ytterligare måste kontrollerade trafikflöden skapas mellan segmenten, vilket leder till att oönskad trafik inte kan flöda fritt i nätverket. Icke nödvändig kommunikation mellan enheter ska stoppas eller förhindras så mycket som möjligt, vilket kan uppnås med hjälp av bland annat brandväggar, routrar och switchar [42].

Nätverkssegmentering innebär att ett nätverk delas i ett flertal mindre nätverk. Dess syfte är att öka nätverksprestandan och säkerheten. Genom segmenteringen kan trafiken övervakas och trafikflödet kan kontrolleras mellan nätverken. Vid användning av nätverkssegmentering kan trängselnätverk minskas. Exempelvis är det nödvändigt att medicinteknisk utrustning segmenteras från besöksnätverket så att utrustningen inte störs av internetsurfing. Spridningen av en attack kan också minskas genom nätverkssegmentering. Vid skadlig kod i en del av nätverket kan segmenteringen hindra att det sprids till en annan del [43]. Utöver nätverkssegmentering inom det egna nätverket är det viktigt att ha skydd mot hot från internet. Vid användning av RDP ska den inte exponeras mot internet om det inte är nödvändigt. Även servrar ska endast kopplas upp på internet om det är absolut nödvändigt för att på så sätt minska risken för att bli utsatt för en attack [6].

Det är också viktigt att enbart använda de protokoll, tjänster och nätverkskopplingar som är nödvändiga, resterande ska blockeras eller tas bort. Alla mjukvaror som används innehåller någon typ av sårbarhet och genom att inaktivera tjänster som inte används minskar risken att oinvigda får åtkomst till systemet [42]. Det är också viktigt att de protokoll som används är säkra och krypterade [6].

### 3.5.4. Brandväggar, antivirus och spamfilter

#### Brandväggar

För att skydda nätverket är det viktigt att kunna styra den ingående och utgående trafik som passerar genom nätverket. Detta görs med hjälp av brandväggar, som länge har varit den yttersta försvarslinjen i ett nätverk. Brandväggarnas syfte är att agera som en barriär mellan det säkra interna nätverket och det opålitliga som finns utanför nätverket, såsom internet [44]. Med hjälp av brandväggar kan trafik till och från olika källor blockeras eller tillåtas att passera, baserat på olika säkerhetsregler. Det är viktigt att ha robusta brandväggar som kan blockera avancerade malware från att kunna infektera nätverket. Den traditionella brandväggen har utvecklats och kommit i ny skepnad, en så kallad Next-Generation-Firewall (NGFW). NGFW kan hantera alla hot som den traditionella brandväggen men även de moderna hoten som uppkommit i takt med digitaliseringens framfart [45].

#### Antivirus

Antivirusprogram är ett sätt att förebygga att intrång sker i en enhet. Programmet söker efter igenkända hot och analyserar olika programs beteende och varnar om ett program agerar underligt. Antivirusprogrammets funktion är att blockera eller ta bort skadlig programvara direkt när det upptäcks på enheter. Det är även viktigt att säkerställa att det installerade antivirusprogrammet är uppdaterat eftersom det hela tiden kommer nya virusformer som måste kännas igen. Varje virus innehåller en identitet eller en signatur, som är unik för just det viruset. I antivirusprogrammet lagras sedan identiteterna för att lära programmet känna igen de potentiella hoten och kunna isolera, blockera och radera dem [46]. Ett problem är att cyberkriminella kan packa om den skadliga programvaran så att den får en ny skepnad som antivirusprogrammet ej känner igen. Det här innebär att det är en ständig kamp att skydda systemen mot skadlig programvara [11].

#### Spamfilter

Det är vanligt förekommande att ransomware sprids via phishing-mejl, som innehåller skadliga länkar eller bilagor. Därför är det viktigt att implementera spamfilter för att undvika att personal inom organisationen råkar klicka på en infekterad länk eller bilaga i ett spammejl [9]. Ett spamfilter fungerar genom att analysera mejlets avsändare och innehåll. Har adressen som mejlet skickats från tidigare använts i spammejl kommer den sorteras bort av filtret. Filtret poängsätter även ord, där ord som är vanligt förekommande i spammejl får högre poäng än ord som inte är vanligt förekommande. Är poängsumman för hög kommer mejlet automatiskt sorteras bort [47]. Även filändelser på bilagor kan användas för att avgöra om det är ett spammejl eller inte och följande filändelser bör sorteras bort direkt; *.exe, *.zip, *.rar, *.7z, *.js, *.wsf, *.docm, *.xlsm, *.pptm, *.rtf, *.msi, *.bat, *.com, *.cmd, *.hta, *.scr, *.pif, *.reg, *.vbs, *.cpl, *.jar [10].

### 3.5.5. Övervaka systemen

Om en organisation inte övervakar systemen kan obehöriga förflyttas fritt inom nätverket utan att bli påkomna och ouppmärksammad skadlig kod spridas i verksamhetens IT-miljö. Därför är

det viktigt att organisationer ständigt bevakar IT-miljön. Genom att samla in och analysera säkerhetsloggar kan pågående intrång upptäckas och oönskade händelser begränsas och åtgärdas direkt [42]. Enligt Truesecs grundare, Marcus Murray, var avsaknad av övervakning av system en gemensam nämnare hos de företag som drabbats av cyberangrepp under 2020 [3].

Det finns olika sätt att övervaka och analysera trafik i ett nätverk. Exempel på sådana lösningar är Intrusion Detection System (IDS), Intrusion Prevention System (IPS) samt Honeypot. IDS används för att upptäcka ett eventuellt hot mot nätverket. Den är ofta placerad utanför kommunikationen mellan källa och destination som sker i realtid. IDS har endast ett syfte; att upptäcka inkommande hot. Den vidtar inte några åtgärder för att stoppa eller blockera hotet. Allt som IDS:en upptäcker rapporteras sedan till administratören [48]. IPS är en funktion som upptäcker och motverkar hot som uppstår genom att undersöka all trafik som flödar genom nätverket. IPS är vanligtvis placerad precis bakom brandväggen, inom den direkta kommunikationen mellan källa och destination. Till skillnad från IDS kan IPS ta beslut om åtgärder om ett hot identifieras. Åtgärder kan vara att droppa ett paket som skickas, blockera trafik från en adress samt återställa anslutningen [49].

Honeypots syfte är att efterlikna det riktiga systemet med tillhörande data och applikationer för att lura cyberkriminella att tro att de är inne i det riktiga systemet. När angriparen är inne i det virtuella systemet kan tillvägagångssättet analyseras för att göra det riktiga systemet säkrare. Honeypoten är inte till för att stoppa en specifik attack, såsom exempelvis en brandvägg gör, utan snarare för att fungera som ett verktyg för att säkra det riktiga systemet. Genom att analysera angriparens tillvägagångssätt i Honeypoten kan olika information läsas ut. Exempelvis hur angriparen kom in i systemet, vilken nivå hotet ligger på, vilken data angriparen är intresserad av samt hur bra de befintliga säkerhetsåtgärderna fungerar [50].

### 3.5.6. Användare

#### Användarbehörigheter

Tilldelning och användning av konton med systemadministrativa behörigheter bör begränsas, för att minimera risken att angripare kan använda dem. Om det finns många användarkonton med systemadministrativa behörigheter, kan det vara enklare att de hamnar i fel händer. Det medför även att det är lättare för en angripare att smälta in i mängden och uppträda obemärkt i systemet. Om skadlig kod sprids av en användare med systemadministrativa behörigheter kan det ha förödande konsekvenser, jämfört med om det sprids från ett konto med lägre behörigheter [42]. Där är det viktigt att inte användare har fler behörigheter än de behöver för att utföra sina arbetsuppgifter [6].

Det är viktigt att användare har personliga inloggningsuppgifter för att spårbarheten ska kunna garanteras i systemet. Att använda gemensamma inloggningar kan underlätta för en angripare att komma över uppgifterna. Det är också viktigt att inte använda ett konto med administratörsrättigheter vid utförandet av vardagliga sysslor, såsom surfing eller mejlhantering [6].

En annan viktig faktor vid hantering av konton är behandlingen av inaktiva konton. Konton bör ej tas bort, utan snarare inaktiveras. Detta underlättar vid spårningen av äldre konton samt minskar risken för att samma kontouppgifter återanvänds vid senare tillfälle. Behörigheterna ska tas bort vid ett inaktivt konto. Konton som inte förväntas användas en längre period ska inneha en tidpunkt för inaktivering [42].

**Användarmedvetenhet**

Det är viktigt att som IT-ansvarig i en organisation göra övriga användare uppmärksamma på de hot som är vanligt förekommande på internet och hur de ska försöka avvärja dem. Det finns vissa saker som är viktiga att förmedla till medarbetarna, såsom vad de ska tänka på innan de klickar på en länk i ett mejl [10]. Eftersom de flesta ransomware-attackerna sprids via phishing-mejl är det viktigt att lägga mycket fokus på hur användarna ska behandla mejl från osäkra källor och avsändare [9]. Enligt MSB finns det sex saker att tänka på vid mottagande av mejl:

1. Är detta mejl från en förväntad källa vid en rimlig tidpunkt? *Bedrägerimeddelanden kan kännetecknas genom brådskande ärenden eller tidsbegränsade erbjudanden.*

2. Verkar ärendet rimligt? *Genom att titta på språk eller andra avvikelser från exempelvis rutiner kan det gå att avgöra om mejlet är legitimt eller inte.*

3. Ser avsändaradressen korrekt ut och borde detta mejl komma från denna avsändare? *Detta ska vägas in i föregående frågor då ett mejlkonto kan vara kapat och adressen därmed är riktigt.*

4. Finns det en länk eller fil bifogad i meddelandet? *Det är mycket viktigt att kontrollera länken alternativt filen. Ofta kan den innehålla ett namn som efterliknar en annan organisation eller på annat sätt se misstänksam ut.*

5. Rekommenderas eller uppmanas du att ändra eller uppge dina inloggningsuppgifter? *Det är inte ovanligt att många bedragare försöker efterlikna tjänsters inloggningssidor, exempelvis Google drive eller Microsoft Outlook.*

6. Innehåller meddelandet en uppmaning att avaktivera skyddad vy eller aktivera makron? *Virus kan ofta gömmas i makron eller liknande. Vid säkerhetsvarningen om att exempelvis aktivera makron är det viktigt att först kontrollera legitimiteten med avsändaren.* [6]

Vid osäkerhet är det viktigt att vidta åtgärder. En åtgärd kan vara att kontakta avsändaren på egen hand, antingen i ett nytt mejl eller via telefon för att verifiera att mejlet är legitimt. Om viss osäkerhet fortfarande existerar är det viktigt att ta kontakt med IT-ansvariga inom organisationen för att avgöra mejlets riktighet. Det är också mycket viktigt att, som ansvarig för IT-infrastrukturen, vara öppen med medarbetarna om det befintliga hotet gällande cybersäkerhet. Om det är ökad aktivitet av cyberkriminalitet i organisationen är det viktigt att förmedla detta till alla berörda personer så att de kan vara extra försiktiga och uppmärksamma [6]. Utöver att göra användarna medvetna om riskerna bör IT-personal utföra simulerade phishing-attacker. Attackerna går ut på att skicka ut falska men legitima e-postmeddelanden, innehållande "skadliga" länkar till användarna. Syftet är att träna användare att vara uppmärksamma när de går igenom mejlkorgen. På så sätt kan simulerade phishing-attacker minska risken att falla offer för ransomware [10].

### 3.5.7. Script för återställning av filer

För att kunna återställa krypterade filer efter en infektion kan ett script implementeras. De här scriptet ändrar namnet på filen *vssadmin.exe* och medför att crypto ransomware inte kan hitta och radera den. Filen vssadmin.exe lagrar säkerhetskopior som tas av den inbyggda Windows-funktionen *Shadow Copies*. Funktionen tillåter användare att ta backuper av systemet. Cyberkriminella använder ofta kommandot *vssadmin.exe Delete Shadows /All /Quiet* som raderar alla återställningspunkter som gjorts. Om cyberkriminella lyckas radera innehållet i filen *vssadmin.exe* kommer användaren inte kunna återställa systemet till tidigare lagrade återställningspunkter [12].

Scriptets funktion är att förhindra att ovan nämnda kommando körs. Detta kan göras genom att ändra namn på filen *vssadmin.exe* som leder till att ransomware inte kan hitta och radera innehållet i filen, vilket medför att systemet kan räddas även efter en infektion. Scriptet ber om administratörsrättigheter samt äganderätt till filen *vssadmin.exe* för att kunna byta namn på den. När ägar-bytet och namnändringen är gjorda skapar scriptet återställningspunkter. Scriptet re-kommen-deras att implementeras i Windows-funktionen Schemaläggaren för att på så sätt köras regelbundet en specifik tid på dygnet. Förhoppningen är att punkter ska skapas kontinuerligt och bidra till en förenkling vid återskapande av filer vid en eventuell infektion [12].

# 4. Intervjustudie

I följande kapitel redovisas resultat från de utförda intervjuerna. Eftersom allt deltagande är anonymt redovisas svaren utan inbördes ordning. Inga namn på personer, organisationer eller geografiska platser nämns i nedanstående avsnitt för att behålla anonymiteten på respondenterna. Syftet med intervjuerna är att få svar på frågeställningarna som formuleras i avsnitt **1.3. Problemformulering.**

## 4.1. Resultat – sammanställande tabell

I detta avsnitt finns Tabell 1 som sammanfattar resultat från den strukturerade kvalitativa intervjustudien. Sammanställningen är till för att ge läsaren en överblick på respondenternas svar. Tabellen består av deltagarnas aggregerade svar. I avsnitt **4.2. Intervjuer** redovisas respondenternas svar mer utförligt.

| **Hur många…** | **Antal** |
|---|---|
| … har upplevt ett ökat antal intrångsförsök i sina system? | 0/3 |
| … har blivit utsatta för en ransomware-attack? | 2/3 |
| … har en katastrof-återställningsplan? | 3/3 |
| … är certifierade enligt ISO 27000? | 1/3 |
| … har lösningar på hårdvarunivå mot ransomware? | 3/3 |
| … utför kontinuerliga backuper? | 3/3 |
| … har implementerade mejl-filter? | 3/3 |
| … begränsar användarnas behörigheter? | 3/3 |
| … uppdaterar kontinuerligt operativsystem och hårdvaror? | 3/3 |
| … använder sig av outsourcing? | 3/3 |
| … använder antivirusprogram samt brandväggar? | 3/3 |
| … övervakar ingående och utgående nätverkstrafik? | 3/3 |
| … har säkerhetslösningar för fjärråtkomst? | 3/3 |
| … har internetservrar avskilda från övriga servrar? | 2/3 |

| | |
|---|---|
| … segmenterar sitt nätverk? | 3/3 |
| … har Honeypot? | 0/3 |
| … arbetar kontinuerligt för att öka medarbetarnas kunskaper om informationssä- | 3/3 |
| … använder sig av awareness training? | 0/3 |

Tabell 1: Tabell över sammanställda svar från intervjuerna. Tabellen delas in i två kolumner. I kolumn 1 finns frågor om hur många av de tillfrågade som har vidtagit åtgärder som är viktiga för att värja sig mot ransomware. I kolumn 2 finns andelen som kan anses fullfölja åtgärderna genom det totala antalet.

## 4.2. Intervjuer

I detta avsnitt presenteras resultatet från de genomförda strukturerade intervjuerna. Därefter diskuteras resultatet i kapitel **5. Diskussion.** I diskussionen kopplas resultatet från litteraturstudien samman med resultatet från intervjustudien. I diskussionsavsnittet analyseras och jämförs det insamlade materialet, för att kartlägga huruvida svenska sjukhus är motståndskraftiga mot ransomware-attacker.

Intervjufrågorna är utformade för att på bästa möjliga sätt besvara frågeställningarna som formuleras i avsnitt **1.3. Problemformulering**. Frågorna delas in i fem huvudområden; Allmän information, Informations-säkerhetsarbete och IT-policys, Hårdvara/Mjukvara, Nätverk och kommunikation samt Personal och arbetsrutiner. I detta kapitel presenteras de fem huvudområdena.

### 4.2.1. Allmän information

Inom området ställs frågor om huruvida de har upplevt ett ökat antal intrångsförsök det senaste året, om de har drabbats av en ransomware-attack samt om de har tydliga strategier för att avvärja ransomware.

**Har ni upplevt ett ökat antal intrångsförsök i era system? Vad för typer av intrång har ni märkt är mest förekommande?**

Alla respondenter är överens om att det inte syns någon nämnvärd ökning av antalet intrångsförsök i systemen. Däremot kan de endast föra statistik över de intrångsförsök de upptäcker och därmed kan det finnas ett mörkertal gällande ökning av cyberangrepp. Å andra sidan har regionerna förhöjd beredskap, eftersom varningar från MSB gått ut om hög risk för cyber-attacker mot sjukvården. En av respondenterna menar på att trots att antalet intrångsförsök är detsamma så blir hoten allvarligare och mer sofistikerade. Spear phishing är en vanligt förekommande attack-vektor och riktar in sig på att lura noga utvalda personer att aktivera skadlig kod. Istället för att skicka bilagor innehållande skadlig kod direkt i mejlet väljer angriparna att bifoga en skadlig länk som omdirigerar offren till en hemsida med skadlig kod. Det här tillvägagångssättet upptäcks inte lika enkelt av systemen och är därmed mer framgångsrikt för förövaren.

**Har ni någon gång blivit utsatta för en ransomware-attack där angriparna lyckats kryptera er data eller låsa ert system?**

Delar av de tillfrågade har inte blivit utsatta för en ransomware-attack medan andra har det. De som svarar att de har blivit drabbade av ett ransomware-angrepp berättar att det hände för flera år sedan. Angriparna lyckades kryptera en enskild enhet i en av verksamheterna. Organisationen kunde stoppa angreppet genom att läsa tillbaka den senaste säkerhetskopian. I den andra verksamheten lyckades förövarna kryptera en delad mapp som flera användare hade tillgång till. Organisationen upptäckte angreppet i ett tidigt stadie och även de kunde stoppa attacken genom att läsa tillbaka data från backup.

**Har ni tydliga strategier för hur ni ska hantera och skydda er mot ransomware-attacker?**

Merparten av respondenterna är överens om att de inte har en specifik plan för just ransomware. Däremot har de tydliga strategier dokumenterade för cyberhot generellt. En av organisationerna har tagit fram tydliga scenarier på hur de ska agera om en cyberattack in-träffar. Främst är scenarierna utformade som stöd för hur sjukvårdspersonalen ska arbeta vid bortfall av IT-stöd. En av verksamheterna har tydliga strategier hur de ska agera vid en ransomware-attack. Dessutom arbetar de med att utveckla ytterligare förmågor och skydd mot den typen av cyberhot.

### 4.2.2. Informationssäkerhetsarbete och IT-policys

Här ställs frågor om organisationerna är certifierade enligt ISO 27000, vad organisationerna har för styrdokument och riktlinjer samt hur de följs upp.

**Är ni certifierade enligt ISO 27000?**

Det mest förekommande svaret är att organisationerna inte är certifierade enligt ISO 27000. De organisationerna som inte är certifierade har däremot informationssäkerhetspolicys som bygger på ISO 27000. Dessutom använder de ramverket i deras informationssäkerhetsarbete för att delegera ansvar och tydliggöra roller inom organisationerna. Informationssäkerhetspolicyns syfte är att skapa en tydlig struktur inom verksamheterna men de ser inget mervärde i att vara certifierade. En av organisationerna är däremot certifierade enligt ISO 27000 och respondenten vill “slå ett slag” för standarden. Respondenten berättar att det var ett omfattande arbete att implementera standarden men att det i dagsläget underlättar arbetet med IT- och informationssäkerhet. Respondenten menar även på att det finns bra riktlinjer och hygienfaktorer som ska följas och som underlättar det kontinuerliga säkerhetsarbetet. Dessutom förklarar den tillfrågade att standarden inte fastställer vad för teknologi och produkter som måste implementeras för att ha ett motståndskraftigt IT-system. Däremot är skyddsåtgärderna i standarden bra att utgå ifrån men garanterar inte verksamheten ett hundraprocentigt skydd mot cyberhot.

### 4.2.3. Hårdvara/Mjukvara

I denna kategori besvaras frågor gällande vilka försvarsmekanismer som används. Syftet är att kartlägga huruvida de har säkra IT-lösningar för att kunna stå emot och hantera en ransomware-attack. Frågorna inbjuder till både beskrivande och enkla svar, såsom ja eller nej. Anledningen

till att frågorna är formulerade på så vis är för att respondenterna inte ska behöva avslöja konfidentiell information. Däremot är frågorna nödvändiga att ställa för att besvara frågeställningarna i avsnitt **1.3. Problemformulering**.

**Har ni några lösningar på hårdvarunivå som ni använder er av för att avvärja ransomware?**

Den första respondenten svarar att de både använder säkerhetsmekanismer på hårdvaru- och mjukvarunivå för att motverka alla typer av cyberhot. Som exempelvis att motverka förlust och kryptering av data, att obehöriga får tillgång till systemen och att skadlig kod sprids. Försvarsmekanismer såsom brandväggar, antivirusprogram och spamfilter är viktiga faktorer för att avvärja olika cyberhot. Deltagaren förklarar att det i dagsläget inte går att bygga en mur och tro att den skyddar verksamheten mot alla typer av hot. Det handlar snarare om att utveckla många mekanismer som kan identifiera olika hot när de uppkommer. Respondenten berättar att den största faran inte enbart är det som kommer igenom brandväggarna. Det mest kritiska är om anställda begår misstag som kan öppna upp för sårbarheter i systemen.

Den andra och tredje respondenten berättar att de har skydd som bygger både på hårdvaru- och mjukvarulösningar.

**Utför ni regelbundet backuper och hur ofta görs det?**

Respondent ett menar att det är en självklarhet att de utför backuper på all data. Backuperna lagras sedan internt och offsite för att undvika att data hamnar i fel händer. Säkerhetskopiorna testas regelbundet och organisationen har rutiner för återläsning för att säkerställa att backuperna fungerar. Återläsningsrutinerna är centrala för verksamheten för att säkerställa att de snabbt kan återställa systemen vid en ransomware-attack. Att testa backuperna är också viktigt för att fastställa deras funktionalitet. Deltagaren förklarar även att det finns lagstiftat enligt patientdatalagen hur länge säkerhetskopiorna ska lagras.

En av de andra intervjukandidaterna berättar att det viktigaste skyddet de har mot ransomware-attacker är deras backup. Deltagaren förklarar att de backar upp all information med jämna mellanrum och intervallerna för detta är olika beroende på vilken information det gäller. Det kan handla om ett tidsspann på en timme, ett dygn eller veckovis. Även inom den här organisationen lagras säkerhetskopiorna internt och offsite. Respondenten förklarar att det inte är så enkelt som det låter att testa backuperna och det går inte att testa alla backuper fullt ut. Det skulle medfört att servern som informationen läses tillbaka på tilldelas samma IP-adress som den redan existerande servern. Det här skulle innebära att servrarna utför samma uppgift och därmed leda till en konflikt och orsaka störningar. Däremot menar respondenten att de kan testa att backuperna fungerar men inte säkerställa dess beroende av andra system och servrar.

Den tredje respondenten svarar att de regelbundet utför säkerhetskopior av data, minst en gång per dygn. Organisationen har flera datorhallar och orter som säkerhetskopiorna lagras på och flyttas mellan, det vill säga internt och offsite.

**Har ni implementerade mejl-filter som förhindrar att virus sprids via mejl?**

Alla tre respondenter ger svaret att de har implementerade mejl-filter. De alla anser att det är betydelsefullt att kunna stoppa inkommande e-post som bedöms innehålla skadlig kod. Det är viktigt att kunna identifiera skadliga bilagor eller länkar så att medarbetare inte råkar exekvera skadlig kod.

**Begränsar ni användarnas behörigheter, så att de endast har tillgång till de delar av systemet och de filer som de måste ha för att kunna genomföra sina arbetsuppgifter?**

En av respondenterna svarar att de absolut begränsar användarnas behörigheter och att de endast ska ha tillgång till de funktioner som behövs för att de ska kunna utföra arbetsuppgifterna. Deltagaren menar också på att om någonting skulle hända slår angreppet endast på en begränsad yta.

Nästa respondent berättar att även de begränsar behörigheterna för användarna och att de flesta av dem är nöjda med att inte ha administratörsrättigheter på den egna datorn. Däremot finns det anställda som skulle vilja ha fler behörigheter men organisationen försöker trots det begränsa vad användarna kan och inte kan göra. Anledningen är att begränsa skadan vid ett eventuellt cyberangrepp. Dessutom ökar spårbarheten vid begränsade rättigheter och medför att det går att loggkontrollera vem som varit var i systemet och vad personerna har gjort. Med hjälp av kontrollerna går det även att begränsa personers rättigheter så att de endast kommer åt data de är behöriga till, utifrån ett patientsäkert perspektiv.

Den sista respondenten svarar att de har begränsade användarbehörigheter. En vanlig användare är inte administratör på den egna datorn och de har inte rätt att lägga till eller ta bort program. Även IT-teknikerna har begränsade behörigheter till viss del. Alla IT-tekniker har inte samma behörigheter på alla servrar.

**Hur ofta görs uppdateringar av operativsystem och hårdvaror?**

De tre respondenterna är alla överens om att det är viktigt att uppdatera säkerhetspatchar så fort de finns tillgängliga. Mindre kritiska system uppdateras regelbundet enligt en plan beroende på vad för typ av system det är. När det kommer till medicintekniska system är det till viss del svårare att göra uppdateringar. De medicintekniska systemen måste valideras innan det går att installera en uppdatering i dem. Utöver uppdatering av mjukvara byts hårdvaror kontinuerligt ut enligt en livscykelhantering beroende på enheternas prestanda och fysiska funktionalitet.

**Används någon typ av outsourcing där ni lämnar ut tjänster till tredje part? Vilka?**

Enligt första respondenten används tredjepartsleverantörer för bearbetning av data men förklarar att ingen känslig information lämnas vidare. Dessutom ska informationen alltid finnas kvar hos verksamheten. Organisationen använder tjänster för molnlagring, såsom Office 365 men inte för personuppgifter eller annan känslig information. Verksamheten kvalitetskontrollerar alltid leverantörerna som används samt upprättar avtal med dem.

Den andra respondenten berättar att de använder sig av tredjepartsleverantörer men i väldigt liten omfattning. Exempel på outsourcade tjänster är personal- och lönesystem, inkluderat deras

fakturerings- och beställningsportal. Organisationen gör alltid en informationssäkerhetsklassning innan tjänsten driftsätts.

Den tredje respondenten svarar att outsourcing används i måttlig omfattning. Deltagaren berättar även att de nyligen har köpt in ett nytt journalsystem i form av en outsourcad molntjänst. I samband med uppgraderingen av journalsystemet kommer data även ligga hos leverantören. Även delar av serverdriften inom organisationen sköts av extern part, främst kritiska servrar som måste fungera dygnet runt. Deltagaren förklarar att vid outsourcing finns det lagstadgat vilka avtal som måste skrivas på och det har verksamheten gjort. Dessutom kvalitetskontrollerar även den här organisationen leverantörerna månatligen samt att upprättade avtal hålls.

**Används något antivirusprogram samt brandväggar specifikt mot ransomware?**

Alla tre respondenter svarar att de använder antivirusprogram från de största leverantörerna på marknaden, såsom Cisco, McAfee och Microsoft. Exakt vilka antivirusprogram verksamheterna nyttjade vill ingen respondent gå in på i detalj. En av respondenterna förklarar även att antivirus endast är en liten del i säkerhetsarbetet idag.

Gällande brandväggar använder alla respondenter avancerade brandväggar med stöd för IPS, som kan upptäcka och motverka inkommande hot.

### 4.2.4. Nätverk och kommunikation

I kategorin besvaras frågor om hur nätverk stärks för att säkerställa kommunikationen. Syftet är att kartlägga huruvida de hade säkra IT-lösningar för att kunna stå emot och hantera en ransomware-attack. Frågorna inbjuder till både beskrivande svar och enkla svar, såsom ja eller nej. Anledningen till att frågorna är formulerade på så vis är för att respondenterna inte ska behöva avslöja konfidentiell information. Däremot är frågorna nödvändiga att ställa för att besvara frågeställningarna i avsnitt **1.3. Problemformulering**.

**Övervakar ni nätverkstrafiken? Både internt och externt.**

Samtliga deltagare övervakar systemen, både ingående samt utgående trafik.

**Vad har ni för lösningar när det gäller fjärråtkomst (t.ex. RDP)? (Körs de via en VPN-anslutning?)**

Första respondenten fastslår att de använder VPN-anslutning för uppkoppling mot RDP och på så sätt kunna ha ett fjärrskrivbord.

Den andra respondenten förklarar att de använder Microsofts inbyggda lösning vid distansarbete och körs via directaccess. Det går inte att köra applikationer genom directaccess, vilket gör att organisationen även använder en VDI-lösning, det vill säga Virtual Desktop. Verksamheten använder en tjänst vid namn Horizon från VMware. Tjänsten innebär att användaren får upp en bild av en klient på insidan av den virtuella maskinen och för att komma åt den går åtkomsten genom en tunnel. Directaccess i sig är också en krypterad länk och all e-post går genom den.

Även en den tredje respondenten fastställer att VPN används vid fjärråtkomst med interna klienter. Organisationen använder Citrix vid distansarbete, som är ett annat exempel på VDI-tjänster.

**Är (alla) era servrar uppkopplade mot internet?**

En av respondenterna förklarar att de har DMZ, DeMilitarized Zone, det vill säga en specifik plats för webbservrar som exponeras på internet. Mellan zonerna sitter brandväggar som fastställer att servrar och klienter endast kommunicerar med de enheter de måste.

En annan respondent svarar att de försöker begränsa antalet uppkopplade enheter mot internet. Att exponera en server på internet innebär alltid en risk.

Den sista respondenten menar på att i grund och botten är alla servrar uppkopplade mot nätverket, vilket medför att de har tillgång till internet. Däremot kan det finnas något undantag. Respondenten hävdar att hen inte har full kännedom om hur det står till inom organisationen.

**Segmenterar ni ert nätverk?**

Alla tre organisationer segmenterar nätverken, helt eller delvis. En av respondenterna förutspår att segmentering av nätverk kommer öka i takt med att nya tekniker utvecklas. En av organisationerna håller i nuläget på att utöka nätverkssegmenteringen.

**Används Honeypot eller motsvarande som efterliknar ert system/nätverk för att analysera tillvägagångssättet på ett intrångsförsök?**

Alla respondenter svarar nej, de använder inte Honeypot eller motsvarande teknik.

### 4.2.5. Personal och arbetsrutiner

Följande avsnitt innefattar frågor gällande hur organisationerna arbetar för att öka deras medarbetares kunskap inom området informationssäkerhet.

**Hur arbetar ni för att förbättra era medarbetares kunskaper inom informationssäkerhet och kunna känna igen hot på nätet?**

Alla tillfrågade respondenter svarar att de kontinuerligt arbetar inom organisationen med att informera om informationssäkerhet. De påpekar att det var viktigt att alla inom verksamheterna har informationssäkerhet i åtanke vid utförandet av det dagliga arbetet. En respondent menar på att informationssäkerhetsarbetet överlappar patientsäkerhetsarbetet. Den tillfrågade förklarar att vid arbete med patientsäkerhet är det stränga regler för hur patientdata får delas, att datorn ska låsas om den ej används och att dokument inte får bli liggande. En av respondenterna menar även på att det skulle vara svårt att förmå all personal att gå en utbildning i informationssäkerhet. Den tillfrågade menar på att det primära intresset hos sjukvårdspersonalen inte är att gå utbildningar inom informationssäkerhet. Organisationen tillhandahåller inte desto mindre en grundutbildning inom området. Däremot har verksamheten ingen kontinuerlig uppföljning på

utbildningen. En annan respondent berättade att de ej för närvarande har någon utbildning inom informationssäkerhet men att de håller på att utforma en webbaserad utbildning rörande ämnet. Utbildningen som utformas baseras på en interaktiv utbildning som MSB tillhandahåller.

Alla respondenter är överens om att deras intranät är den viktigaste informationskällan för att upplysa medarbetarna om eventuella hot, exempelvis ransomware-attacker. Eftersom alla medarbetare har tillgång till intranätet är det en bra plattform att publicera nyheter, hot och händelser på. Exempelvis kan information publiceras på intranätet som uppmärksammar medarbetarna på vilka hemsidor de får besöka under arbetstid samt vilka de inte får besöka.

**Utför ni simulerade nätfiskeattacker för att motverka att era slutanvändare trycker på skadliga länkar som kan orsaka intrång? (Awareness training)**

Alla respondenter svarar nej på frågan. En av respondenterna förklarar att det tar tid för en verksamhet att utföra simulerade phishing-attacker. Den intervjuade menar på att awareness training inte är av högsta prioritering i nuläget på grund av den rådande pandemin. En annan deltagare förklarar att det har varit en del debatt inom deras organisation gällande awareness training. Några inom organisationen anser att det kan vara integritetskränkande och andra tycker att det ska sättas i verket. Trots att de inte har awareness training menar respondenten på att medarbetarna blir mer och mer uppmärksamma på hur de ska hantera inkommande mejl, på grund av att verksamheten, med jämna mellanrum, publicerar information om phishing-mejl och hur medarbetarna skall agera.

## 4.3. Förslag på skyddsrutiner mot ransomware

Genom litteratursökningen som gjorts i litteraturstudien samt resultatet från intervjustudien har följande lista tagits fram. Punkterna är främst baserade på åtgärder från tidigare forskningsresultat som påvisar parametrar som är motståndskraftiga mot ransomware. Förslagen är delvis framtagna utifrån identifierade brister hos de tillfrågade verksamheterna, såsom att de ej utför simulerade phishing-attacker. Riktlinjerna innefattar även åtgärdsförslag som exempelvis att verksamheterna bör implementera Honeypot för att stärka det egna systemet ytterligare. Listan består av riktlinjer som är framtagna till de verksamheter som medverkat i studien. Riktlinjerna är till för att stärka skyddet mot utpressningsvirus inom systemen samt för att snabbt kunna åtgärda och återställa allt till normal funktion om verksamheter drabbas.

1. **Säkerställ att säkerhetskopiering sker kontinuerligt**. Regelbundna säkerhetskopieringar samt snabba återläsningsrutiner är det mest centrala skyddet mot ransomware. Med hjälp av backuper kan 90% av systemen återfås vid ett intrång [31]. Säkerhetskopieringen bör ske minst en gång per dygn och lagras offline och offsite. Dessutom är det avgörande hur snabbt IT-teknikerna kan läsa tillbaka backuperna [10]. Därmed är det viktigt att träna på att återställa systemen för att fastställa att alla vet vad de ska göra om en attack inträffar [40]. En annan anledning till att testa återläsning är för att fastställa säkerhetskopiornas funktionalitet. Bristande backuprutiner kan leda till att verksamheter lamslås och orsaka förlorade datatillgångar, stora återställningskostnader samt minskat anseende [3].

2. **Övervaka systemen.** Att övervaka systemen är en viktig del i säkerhetsarbetet. Enligt Truesecs grundare, Marcus Murray, var avsaknad av övervakning av system en gemensam nämnare hos de företag som drabbats av cyberangrepp under 2020 [3]. Om en organisation inte övervakar systemen kan obehöriga uppträda fritt inom nätverket utan att bli påkomna och ouppmärksammad skadlig kod kan spridas i verksamhetens IT-miljö. Därför är det viktigt att organisationer ständigt bevakar IT-miljön. Genom att samla in och analysera säkerhetsloggar kan pågående intrång upptäckas och oönskade händelser begränsas och åtgärdas direkt [42].

3. **Uppdatera hårdvara, mjukvara och operativsystem** så fort patcher finns tillgängliga hos leverantören. Genom att ständigt uppdatera systemen går det att åtgärda många fel som cyberbrottslingar utnyttjar för att sprida skadlig kod [41]. I en resilient IT-miljö är det viktigt att kontinuerligt uppdatera operativsystem, applikationsprogramvaror, webbläsare och -servrar, antivirus-program, firmware samt brandväggar till de senast släppta versionerna [10]. Skälet till detta är att säkerställa att mjukvaror och operativsystem uppfyller leverantörernas rekommendationer [6]. Dessutom bör sjukhusens IT-personal testa uppdateringarna med resterande delar av systemet innan de implementeras, för att säkerställa att uppdateringarna fungerar [10].

4. **Installera script för återställning av filer.** Genom att implementera ett script som återställer filer efter att de krypterats kan det gå att rädda filerna i efterhand. Scriptet ändrar namn på filen *vssadmin.exe* och medför att crypto ransomware inte kan identifiera den. På så sätt kan inte utpressningsviruset radera några återställningspunkter som gjorts efter namnbytet. Vid infektion går det att med hjälp av scriptet återställa systemet till en tidigare version genom återställningspunkterna som skapats. Därmed går det att rädda filerna som krypterats. Scriptet ber om administratörsrättigheter samt äganderätt till filen *vssadmin.exe* för att kunna byta namn på den. När ägarbytet och namnändringen är gjord skapar scriptet återställningspunkter. Scriptet rekommenderas att implementeras i Windows-funktionen Schemaläggaren för att på så sätt köras regelbundet en specifik tid på dygnet. Förhoppningen är att punkter ska skapas kontinuerligt och bidra till en förenkling vid återskapande av filer vid en eventuell infektion [12].

5. **Implementera säkerhetsfunktioner** i systemen. Säkerhetsmekanismer som antivirusprogram, spamfilter och brandväggar ska installeras och konfigureras korrekt. Samtliga regioner har dessa säkerhetsmekanismer implementerade och bör ha dessa i sin IT-miljö fortsättningsvis. Säkerhetsmekanismerna är viktiga för att skydda sig gentemot ransomware.

**Antivirusprogram**

Antivirusprogrammets funktion är att blockera eller ta bort skadlig programvara direkt när det upptäcks på en enhet. Det är även viktigt att säkerställa att det installerade antivirusprogrammet är uppdaterat eftersom det hela tiden kommer nya virusformer som måste kännas igen. Anti-virusprogram söker efter igenkända hot och

analyserar hur olika program går tillväga och varnar om ett program uppträder underligt [46].

### Spamfilter

Det är vanligt förekommande att ransomware sprids via phishing-mejl, som innehåller skadliga länkar eller bilagor. Därför är det viktigt att implementera spamfilter för att undvika att personal inom organisationen råkar klicka på en infekterad länk eller bilaga i ett spammejl [9]. Ett spamfilter fungerar genom att analysera mejlets avsändare och innehåll. Har adressen som mejlet skickats från tidigare använts i spammejl kommer den sorteras bort av filtret [47].

### Brandväggar

För att skydda sitt nätverk är det viktigt att kunna styra all ingående och utgående trafik som passerar genom nätverket. Detta görs med hjälp av brandväggar och dess syfte är att agera som en barriär mellan det säkra interna nätverket och det opålitliga som finns utanför nätverket, såsom internet [44]. Med hjälp av brandväggar kan trafik till och från olika källor blockeras eller tillåtas att passera, baserat på olika säkerhetsregler. Det är viktigt att ha robusta brandväggar som kan blockera avancerade malware från att kunna infektera nätverket [45].

6. **Segmentera nätverket.** I en IT-miljö spelar säker nätverksinfrastruktur en avgörande roll. Om ett nätverk används av flera tjänster och inte är segmenterat kan angripare uppträda fritt i IT-miljön. En viktig del i att säkra nätverket är segmentering, det vill säga att dela upp nätverket, både fysiskt och logiskt. För att säkra nätverket ytterligare måste kontrollerade trafikflöden skapas mellan segmenten, vilket leder till att oönskad trafik inte kan röra sig fritt i nätverket. Icke nödvändig kommunikation mellan enheter ska stoppas eller förhindras så mycket som möjligt, vilket kan uppnås med hjälp av bland annat brandväggar, routrar och switchar [42]. Spridningen av en attack kan också minskas genom nätverkssegmentering. Vid skadlig kod i en del av nätverket kan segmenteringen hindra att det sprids till en annan del [43].

7. **Begränsa användarnas behörigheter**. Tilldelning och användning av konton med systemadministrativa behörigheter bör begränsas, för att minimera risken att angripare kan använda dem. Om det finns många användarkonton med systemadministrativa behörigheter, kan det vara enklare att de hamnar i fel händer. Det medför även att det ät lättare för en angripare att smälta in i mängden och löpa fritt i systemet. Om skadlig kod sprids av en användare med systemadministrativa behörigheter kan det ha förödande konsekvenser, jämfört med om det sprids på ett konto med lägre behörigheter [42]. Därför är det viktigt att inte användare har fler behörigheter än de behöver för att utföra arbetsuppgifterna. Dessutom är det viktigt att användare har personliga inloggningsuppgifter för att spårbarheten ska kunna garanteras i systemet. Att använda gemensamma inloggningar kan underlätta för en angripare att komma över uppgifterna [6].

8. **Simulerade phishing-attacker** bör utföras på medarbetare. Det är viktigt att som IT-ansvarig i en organisation göra övriga användare uppmärksamma på de hot som är vanligt förekommande på internet och hur de ska försöka avvärja dem. Det finns vissa saker som är viktiga att förmedla ut till medarbetarna, såsom vad de ska tänka på innan de klickar på en länk i ett mejl [10]. Eftersom de flesta ransomware-attackerna sprids via phishing-mejl är det viktigt att lägga mycket fokus på hur användarna ska behandla mejl från osäkra källor eller avsändare [9].

   Utöver att göra användarna medvetna om riskerna bör IT-personal utföra simulerade phishing-attacker. Attackerna går ut på att skicka ut falska men legitima e-postmeddelanden, innehållande "skadliga" länkar, till användarna. Syftet är att träna användare att vara uppmärksamma när de går igenom mejlkorgen. På så sätt kan simulerade phishing-attacker minska risken att falla offer för ransomware [10].

9. **Honeypot bör implementeras** för att analysera cyberkriminellas tillvägagångssätt vid ett intrång samt stärka det riktiga IT-systemet. Honeypots syfte är att efterlikna det riktiga systemet med tillhörande data och applikationer för att lura den cyberkriminella att tro att den är inne i det riktiga systemet. När angriparen har kommit in i det virtuella systemet kan tillvägagångssättet analyseras för att göra det riktiga systemet säkrare. Honeypot är inte till för att stoppa en specifik attack, såsom exempelvis en brandvägg gör, utan snarare för att fungera som ett verktyg för att säkra det riktiga systemet. Genom att analysera angriparens tillvägagångssätt i Honeypoten kan olika slags information läsas ut. Exempelvis hur angriparen fick åtkomst till systemet, vilken nivå hotet ligger på, vilken data angriparen är intresserad av samt hur bra de befintliga säkerhetsåtgärderna fungerar [50].

10. **ISO 27000** bör vara en standard som organisationen är certifierad enligt. Det är ett ledningssystem för cyber- och informationssäkerhet. Standarden finns för att skydda information och eftersom den idag är digitaliserad omfattar standarden även cyber-säkerhet. Dessutom har de flesta organisationer information som innefattar personuppgifter, vilket har lett till att standarden utökats till att även omfatta skydd av data [51].

# 5. Diskussion

I det här kapitlet återfinns en diskussion gällande huruvida svenska sjukhus är motståndskraftiga mot ransomware-attacker. Ett av målen med studien är att få reda på hur respondenterna upplever det ökade hotet av ransomware riktat mot hälso- och sjukvårdssektorn. Materialet som samlas in från intervjuerna kopplas i detta kapitel samman med den insamlade informationen från litteraturstudien. Syftet är att kunna avgöra om sjukhusen i Sverige arbetar utifrån MSB:s rekommendationer. Ytterligare ett mål är att ta reda på om verksamheterna har säkra IT-system och lösningar för att kunna motstå ransomware-attacker.

Ett liknande arbete är [11] som skiljs åt gentemot det här arbetet eftersom författaren undersöker hur svenska företag förhåller sig till ransomware. Därmed skiljer sig perspektivet på resultatet i denna uppsats från tidigare arbeten [8, 10, 12]. Den stora skillnaden är att det i den här studien undersöks det hur svenska sjukhus möter det ökade hotet av ransomware, vilket inte gjorts tidigare.

Den här studien kan inte belysa huruvida samtliga sjukhus i Sverige hanterar det ökade hotet av ransomware samt hur de garderar sig. På grund av att endast 3 regioner valde att medverka kan inte några generella slutsatser dras om hur lägesbilden ser ut i hela Sverige. Däremot kommer de respondenter som medverkar i djupintervjuerna från olika regioner som är spridda över hela Sverige. Regionerna är dessutom representativa för hela landet i bemärkelsen att de både är landsbygds- och storstadsregioner.

## 5.1. Hur upplever och hanterar de svenska sjukhusen det ökade hotet av ransomware?

Enligt statistik från Truesec har ransomware tredubblats under fjolåret och ökat till 49% av alla svåra incidenter. Det är en lavinartad ökning som tyder på att cyberkriminella anser att ransomware är en framgångsrik attack-metod för att tjäna pengar [31]. Bland de tio mest attackerade industrierna svarade sjukvården för 6,6%. Det innebär att sjukvården var den sjunde mest attackerade industrin under 2020. Året innan hamnade sjukvården på en tionde plats och stod för endast 3% av attackerna. Ungefär 28% av alla attacker riktade mot sjukvården bestod av utpressningsvirus [30]. Anledningen till att cyberkriminella lägger fokus på hälso- och sjukvårdssektorn är att medicinsk data är värdefull och har påvisats vara användbar vid utpressning [6]. Trots statistiken har ingen av de tre medverkande respondenterna upplevt någon märkbar ökning av ransomware-aktivitet i systemen. Å andra sidan menar respondenterna att de endast kan föra statistik på de intrångsförsök som upptäcks. Detta kan innebära att det kan finnas ett mörkertal gällande ökning av cyberangrepp i sjukhusens system. Däremot har samtliga respondenters organisationer förhöjd beredskap mot cyberattacker eftersom MSB har gått ut med varningar om hög risk för cyberangrepp riktade mot sjukvården.

## 5.2. Upprätthåller sjukhusen i Sverige säkra IT-system och lösningar för att kunna motstå ransomware-attacker?

Under rådande pandemi är sjukhusen under stor påfrestning och har inte råd att förlora kontrollen över sina system, eftersom det skulle kunna få än mer förödande konsekvenser än annars [14]. Därför är det viktigt under pågående kris att sjukhusen följer etablerade IT-säkerhetsprocesser samt rutiner. Det är även viktigt att sjukhusens IT-personal fokuserar på löpande underhåll av systemen för att undvika säkerhetsluckor [8]. Respondenterna är alla överens om att det är viktigt att ha säkerhetsmekanismer på både hårdvaru- och mjukvarunivå för att kunna motverka alla typer av cyberhot. Säkerhetsmekanismer såsom backup-rutiner, brandväggar, antivirus-program och spamfilter är viktiga redskap i kampen mot förlust och obehörig kryptering av data, att obehöriga får tillgång till systemen och att skadlig kod sprids.

Vikten av att ha ovan nämnda säkerhetsmekanismer framkommer även i tidigare forskning och redovisas i avsnitt **3.5. Befintliga skyddsrutiner mot ransomware**. För att en verksamhet ska kunna stå emot en ransomware-attack är det viktigt att skapa en regelbunden säkerhetskopieringsprocess för data samt systemkonfigurationer [10, 6]. Det innebär att säkerhetskopieringen bör ske kontinuerligt, minst en gång per dygn [10]. Säkerhetskopiorna rekommenderas att lagras offline och offsite för att vara oåtkomliga för oinvigda. Enligt svaren från respondenterna uppfylls de här rekommendationerna. Alla tre tillfrågade säkerhetskopierade systemen kontinuerligt och kopiorna lagras offline och offsite. Dessutom är det viktigt att IT-personal regelbundet tränar på att återställa säkerhetskopior för att de ska veta hur de ska gå tillväga om en attack inträffar [40]. Respondenterna berättar att IT-personalen ständigt testar backuperna och har återläsningsrutiner. Återläsningsrutinerna är centrala inom organisationerna för att säkerställa att de snabbt kan återställa systemen vid en ransomware-attack. I en undersökning gjord år 2021 av Truesec framkommer det att ungefär 60% av alla drabbade organisationer saknade ordentliga säkerhetskopior och rutiner under fjolåret. Konsekvenser vid bristande backup-rutiner är att data och stora summor pengar kan förloras, vilket i förlängningen kan äventyra patientsäkerheten. Undersökningen visade även att med hjälp av backuper går det att återfå 90% av systemet [31].

I en resilient IT-miljö är det viktigt att kontinuerligt uppdatera operativsystem, applikationsprogramvaror, webbläsare och -servrar, antivirusprogram, firmware samt brandväggar till de senast släppta versionerna [10]. Genom att ständigt uppdatera systemen går det att åtgärda många fel som annars kan leda till att skadlig kod sprids [41]. Alla tre respondenter håller med om vikten av att uppdatera säkerhetspatchar direkt när de släpps. Konsekvenserna av att inte uppdatera säkerhetspatchar omgående är att det kan öppna upp för säkerhetsluckor som utnyttjas av cyberkriminella.

Följder av att inte övervaka systemen är att obehöriga kan uppträda fritt inom nätverket utan att bli påkomna och skadlig kod kan spridas ouppmärksammat i IT-miljön. Därför är det viktigt att systemen ständigt övervakas [42]. Det finns olika sätt att övervaka och analysera trafik i ett nätverk som exempelvis IDS, IPS och Honeypot. En redogörelse för hur IDS, IPS och Honeypot fungerar redovisas i avsnitt **3.5.5. Övervaka systemen**. Alla respondenter berättar att de övervakar både ingående och utgående trafik. Däremot svarar samtliga att Honeypot inte används. Honeypot är ett bra verktyg för att analysera cyberkriminellas tillvägagångssätt samt stärka det befintliga IT-systemet. Exempelvis går det att analysera hur angriparen får åtkomst till systemet, vilken nivå hotet är beläget på, vilken data angriparen är intresserad av samt hur bra de befintliga säkerhetsåtgärderna fungerar [50].

Det är dessutom viktigt att ha säkerhetsmekanismer såsom brandväggar, antivirusprogram samt spamfilter implementerade. Brandväggens syfte är att styra den ingående och utgående trafik som passerar genom nätverket [44]. Det här innebär att trafik till och från olika källor blockeras eller tillåts att passera, baserat på olika säkerhetsregler. Det är viktigt att ha robusta brandväggar som kan blockera avancerade malware från att infektera nätverket [45]. Samtliga respondenter svarade att de använder robusta brandväggar som har stöd för IPS för att kunna upptäcka ransomware. Konsekvenserna av att inte ha robusta brandväggar som stödjer IPS kan vara att det blir svårt att upptäcka ett intrång. Upptäcks inte intrånget är det i sin tur svårt att stoppa en pågående attack.

Antivirusprogram är ett sätt att förebygga att intrång sker i en enhet. Programmet söker efter igenkända hot och analyserar hur olika program agerar och varnar om ett programs beteende anses underligt [46]. Alla tre respondenter svarade att de har antivirusprogram från kända leverantörer implementerade i systemen. En av respondenterna förklarade däremot att antivirus endast är en liten del av säkerhetsarbetet idag. Anledningen till detta är att cyberkriminella kan packa om den skadliga programvaran och på så sätt ge viruset en ny skepnad, vilken inte känns igen av antivirusprogrammet. Följder av att inte använda antivirusprogram är att skadlig programvara kan infektera enheter och resultera i förödande konsekvenser.

Ett spamfilter fungerar genom att analysera mejlets avsändare och innehåll. Vid misstänkt innehåll sorteras mejlet bort [47]. Alla respondenterna anser att det är betydelsefullt att kunna stoppa den inkommande e-post som bedöms innehålla skadlig kod. De tillfrågade menar även att det är viktigt att kunna identifiera skadliga bilagor eller länkar så att medarbetare inte råkar exekvera skadlig kod. Det är vanligt förekommande att ransomware sprids via phishing-mejl, som innehåller skadliga länkar eller bilagor. Därför är det viktigt att implementera spamfilter för att undvika att personal inom organisationen råkar klicka på en infekterad länk eller bilaga i ett spammejl [9].

För att ytterligare hindra att oönskat innehåll sprids i systemet är det nödvändigt att segmentera nätverket. Segmentering innebär att nätverket delas upp i mindre delar, både fysiskt och logiskt. För en mer ingående förklaring av nätverkssegmentering, se avsnitt **3.5.3. Nätverkssegmentering**. Alla respondenter var eniga om att det är viktigt att segmentera nätverken och att det är gjort inom allas respektive organisationer. En följd av bristande nätverkssegmentering kan bli att angripare får möjlighet att uppträda fritt i IT-miljön. Därför är det även viktigt att kommunikation som ej anses vara nödvändig mellan enheter stoppas [42]. Av samma anledning ska inga servrar kopplas upp mot internet om det inte är nödvändigt. Detsamma gäller även för användningen av RDP för att minska risken att attackeras.

För att minska omfattningen av ett intrång är det av stor betydelse att ha begränsade användarrättigheter. Om en angripare lyckas få åtkomst till användaruppgifter i ett system är spridningen av skadlig kod begränsad till de rättigheter användarkontot besitter. Det vill säga att om skadlig kod sprids av en användare med systemadministrativa behörigheter kan det ha förödande konsekvenser, jämfört med om det sprids från ett konto med lägre behörigheter. Därför är det även viktigt att ha få användarkonton som har systemadministrativa behörigheter för att minimera skadan om de hamnar i fel händer [42]. Samtliga tillfrågade verksamheter begränsade användarnas behörigheter. Användarna tilldelas endast behörigheter som behövs för att de ska kunna utföra dagliga arbetsuppgifter. Även IT-teknikerna har begränsade rättigheter och har inte tillgång till samma delar av systemen. Utöver att begränsa rättigheterna är det viktigt att alla användare har personliga inloggningsuppgifter. Anledningen till detta är att fastställa spårbarheten i systemen. Med hjälp av personliga konton går det att spåra vem som varit var samt vem som gjort vad.

Det är viktigt att som IT-ansvarig i en organisation göra övriga användare uppmärksamma på de hot som är vanligt förekommande på internet och hur de ska försöka avvärja dem. Det finns vissa saker som är viktiga att förmedla till medarbetarna, såsom vad de ska tänka på innan de klickar på en länk i ett mejl [10]. Eftersom de flesta ransomware-attackerna sprids via phishing-mejl är det viktigt att lägga mycket fokus på hur användarna ska behandla mejl från osäkra källor eller avsändare [9]. Alla tre respondenter svarade att de ej utför simulerade phishing-attacker. En av respondenterna menar att det inte är av högsta prioritet under rådande pandemi. En annan respondent påpekade att det kunde vara integritetskränkande. Respondenten berättade även att de med jämna mellanrum publicerar information på sina intranät hur deras medarbetare skall agera när de genomgår mejlkorgen. Så trots att de ej utför simulerade phishing-attacker är medarbetarna uppmärksamma på hur inkommande mejl ska hanteras. MSB rekommenderar förmedling av varningar till all personal inom organisationen om det förekommer ökad aktivitet av cyberkriminalitet [6].

## 5.3. Hur kan säkerheten utvecklas på sjukhusen för att bättre stå emot ransomware-attacker?

Åtgärdsförslag till de tre medverkande regionerna tas fram och publiceras i avsnitt **4.4. Förslag på skyddsrutiner mot ransomware** för att problemformuleringarna ska kunna besvaras. I följande avsnitt motiveras och diskuteras punkterna i listan för att ge en förklaring till varför de ska genomföras för att ha ett säkert skydd mot ransomware. Värt att nämna innan diskussion av punkterna är att det viktigt att ha i åtanke att alla åtgärder fungerar bäst ihop med varandra.

Alla medverkande berättar att de kontinuerligt genomför säkerhetskopiering och att all lagring sker enligt rekommendationerna som publiceras av svenska myndigheter. Verksamheterna bör fortsätta på detta sätt för att upprätthålla säkerheten. I intervjuerna framkommer det att två av organisationerna har drabbats av ransomware och bådas lösning var att återläsa backup. Det fastställer vikten av att ha bra säkerhetskopior. En hel organisation skulle kunna stå och falla med bristande säkerhetskopior och återläsningsrutiner. Det syns även tydligt i attackerna som tagits upp i avsnitt **3.4. Ransomware-attacker som drabbat hälso- och sjukvårds-sektorn** att backuper kan ha ett stort värde efter en ransomware-attack. Tillsammans med säkerhetskopiorna är det också viktigt att kunna avskärma de smittade delarna av systemet från de som inte redan har infekterats. Med andra ord är det viktigt att segmentera sitt nätverk samt använda brandväggar mellan segmenten för att i sin tur kunna återställa de drabbade delarna. Alla tre respondenter berättar även att de segmenterar sitt nätverk samt håller på att utveckla segmenteringen. Detta bör de fortsätta med och ständigt utveckla.

Att ha bra säkerhetskopior och lagra dem enligt rekommendationerna är inte ett skydd mot att bli attackerad. Det är snarare en lösning för att återfå kontroll över sina system när en attack väl har inträffat. Däremot använder cyberkriminella i dagsläget dubbelutpressningsstrategi vilket innebär att de inte enbart krypterar data. Angriparna stjäl den också och hotar organisationerna med att läcka ut känslig information om en lösensumma inte betalas. Därför är det viktigt att verksamheter skyddar sina IT-system från en infektion i så stor utsträckning som möjligt.

Samtliga regioner övervakar sina system i dagsläget och bör fortsätta med detta. Det finns varningssystem att tillgå, såsom IDS och IPS. Fastställ att brandväggarna har stöd för detta och att de fungerar. Bristande övervakning har inte varit någon övervägande faktor i huruvida en organisation har blivit drabbad av ransomware eller ej. Däremot framgår det ett flertal gånger i olika rekommendationer från myndigheter att det är viktigt att övervaka systemen för att snabbt

kunna upptäcka intrång när de sker. Att upptäcka ett intrång i ett tidigt skede kan vara avgörande för attackens omfattning. Om ingen övervakning av systemet sker kan övriga punkter nästintill ses som oväsentliga på så sätt att om inte intrånget upptäcks i tid kan övriga åtgärder vara för sena att utföra. Sjukhus kan lamslås av en attack och patienters liv kan äventyras, eftersom patienter i livshotande tillstånd kan behöva omdirigeras till närliggande sjukhus. Utöver detta tvingas verksamheterna betala stora summor pengar i återställningskostnader för att återgå till normal funktion.

Inte nog med att det är viktigt att övervaka systemen så är det även viktigt att analysera cyberkriminellas tillvägagångssätt vid ett intrång. Detta kan göras med hjälp av Honeypot. Ur en Honeypot kan information läsas ut, exempelvis hur angriparna fick åtkomst till systemet, vilken data angriparna är intresserade av samt hur bra de befintliga säkerhetsåtgärderna är. Inga av de tillfrågade berättar att de har en Honeypot. Det bör dock implementeras för att analysera vilken data som cyberkriminella är intresserade av och hur de kan säkra upp de riktiga systemen ytterligare.

Alla respondenter är överens om att säkerhetspatchar måste uppdateras direkt när de släpps och de medverkande bör upprätthålla den rutinen. Vid analys av tidigare ransomware-attacker som drabbat sjukhus runt om i världen framkommer det att flera av dem hade kunnat avvärjas genom uppdatering av mjukvara. WannaCry, Notpetya och attacken mot Medstar Health grundades på att angriparna kunde få åtkomst till systemen genom buggar eller sårbarheter som uppkommit på grund av felkonfigurerade mjukvaror. För att ge ett exempel använde Medstar Health en programvara vid namn JBoss som ofta konfigurerades felaktigt och som angriparna kom att utnyttja vid utförandet av attacken. Detta trots att myndigheter innan attacken gick ut med att organisationer som använde programvaran skulle se över konfigureringen för att minska risken att bli utsatta. Om Medtar Health hade lyssnat på myndigheternas rekommendationer och sett över konfigureringen hade attacken kunnat avvärjas. Detsamma gällde även för WannaCry och NotPetya som drabbade verksamheter världen över på grund av en bugg i Service Message Block-protokoll. Innan attackerna släppte Microsoft en ny uppdatering som åtgärdade buggen. Om verksamheterna som föll offer för WannaCry eller NotPetya utfört denna uppdatering hade de troligtvis inte drabbats.

Genom intervjuerna framkommer det att ingen av de tre tillfrågade organisationerna använder simulerade phishing-attacker i dagsläget. Dels för att det är för tidskrävande och för att det kan vara integritetskränkande. Däremot finns det färdiga phishing-test att tillgå på internet. Användandet av dessa behöver inte vara för att få statistik på vem som klickar på en skadlig länk eller inte. Snarare kan testet användas för att göra medarbetarna mer uppmärksamma på hur phishing kan se ut och vilka metoder som finns för att undersöka validiteten i ett mejl. Ett specifikt test är det som Google tillhandahåller och består av 8 frågor innehållande både äkta och oäkta mejl där användaren ska avgöra om det är nätfiske eller ej [52]. Om det inte finns tid och resurser inom organisationerna att skapa och utföra egna simulerade phishing-attacker rekommenderas detta test att förmedla till medarbetarna. Testet är inte heller integritetskränkande eftersom utövarna inte behöver delge någon resultatet. Eftersom ransomware främst sprids via phishingmejl är det viktigt att träna sina medarbetare på att kunna känna identifiera dessa typer av mejl.

Endast en av intervjukandidaterna berättar att deras verksamhet är certifierad enligt ISO 27000. De övriga två svarar att de använder ramverket i arbetet med informationssäkerhet. ISO 27000 är, som många andra standarder, mycket omfattande men mycket användbar när den väl är implementerad i det dagliga arbetet. Fördelen med att vara certifierad enligt standarden är att den även innefattar revisioner där utomstående part granskar arbetssättet. Det är inte nödvändigt att certifiera hela organisationen men delar som hanterar konfidentiell information bör omfattas

av certifieringen. Eftersom en certifiering innefattar revisioner där utomstående part granskar en verksamhets arbetssätt kan sårbarheter kontinuerligt identifieras och åtgärdas direkt. Standarden bidrar även till att organisationer systematiskt arbetar med IT- och informationssäkerhet och stärker ständigt sin IT-miljö.

# 6. Slutsats

I studien undersöks det huruvida sjukhusen/regionerna i Sverige upprätthåller säkra IT-system och lösningar för att kunna stå emot ransomware-attacker. Studien är genomförd som en kombination av litteraturstudie och kvalitativ intervjustudie, med kvantitativt inslag. I intervjustudien genomfördes tre djupintervjuer med IT-ansvariga på sjukhus runt om i Sverige. 15 potentiella intervjukandidater fick förfrågan om medverkan men endast 3 deltog. På grund av att endast 3 regioner valde att medverka kan inte några generella slutsatser dras om hur lägesbilden ser ut i hela Sverige. Däremot kommer respondenterna som medverkar i djupintervjuerna från olika regioner som är spridda över hela Sverige. Regionerna är dessutom representativa för hela landet i bemärkelsen att de både är landsbygds- och storstadsregioner.

De tillfrågade verksamheterna svarar att de inte upplevt ökad aktivitet av ransomware den senaste tiden. Det kan tyckas underligt med tanke på att all statistik visar på en lavinartad ökning av ransomware. Därför kan frågan **Hur upplever och hanterar den svenska sjukvården det ökade hotet av ransomware?** besvaras enligt följande; De tillfrågade sjukhusen har inte upplevt någon ökning av ransomware, vilket tyder på ett stort mörkertal då litteraturen tydligt anger en väsentlig ökning. Verksamheterna vidtar åtgärder för att höja säkerheten eftersom myndigheter gått ut med varningar av ökad cyberaktivitet under den rådande Covid-19-pandemin.

Frågan **Upprätthåller sjukhusen i Sverige säkra IT-system och lösningar för att kunna stå emot en ransomware-attack?** är lite mer komplex och därmed inte lika enkel att besvara. Analys och diskussion av intervjustudien leder fram till att det går att dra slutsatsen att sjukhusen/regionerna har en bra IT-säkerhet generellt. Alla tre organisationer lägger mycket fokus på säkra backup-rutiner och snabba återläsningsrutiner. All forskning trycker mycket på vikten av bra backup-rutiner och snabb återställning, vilket kan anses att organisationerna lever upp till. Alla regioner har även ett samarbete med MSB under pandemin för att säkerställa att säkerheten upprätthålls. De rekommendationer som publicerats av MSB, FRA, Polisen samt SÄPO är tagna i beaktning vid genomförandet av studien och regionerna som medverkat tycks leva upp till dem. Det medför också att de verkar ha ett så säkert system som möjligt mot ransomware-hotet. Cyberbrotten blir allt mer avancerade och genomtänkta för att inte bli upptäckta av de inbyggda systemen och det är därför omöjligt att upprätthålla ett system som kan stå emot alla typer av hot. Därtill är en av de största riskerna den mänskliga faktorn. Ransomware sprids i dagsläget främst via phishing-mejl och därför är det viktigt att lägga mycket fokus på hur användarna ska behandla mejl från osäkra källor och avsändare.

De regioner som medverkar i denna studie har bra säkerhet men överraskande nog finns det några punkter att förbättra. Åtgärdsförslag har tagits fram för öka att säkerheten ytterligare samt för att kunna besvara följande fråga; **Hur kan säkerheten utvecklas på sjukhusen för att bättre stå emot ransomware-attacker?** Bortsett från publicerade åtgärdsförslag i tidigare forskning, såsom backup-rutiner, säkerhetsmekanismer samt nätverkssegmentering, har ytterligare tre punkter tagits fram. Punkterna är framtagna för att öka verksamheternas motståndskraft ytterligare mot skadlig programvara. Den första åtgärden som lagts till är punkt **4. Installera script för återställning.** Punkten baseras på ett tidigare arbete gjort av två studenter på Högskolan i Halmstad och som presenteras närmare i avsnitt **1.2. Koppling till tidigare forskning**. I den uppsatsen görs ett experiment som utmynnar i ett framtaget script som ska kunna återställa filer även efter att enheter blivit infekterade av crypto ransomware. De flesta åtgärdsförslag som presenteras såväl i det här arbetet som i andra bygger på förebyggande handlingar. Scriptet är visserligen till viss del också förebyggande på så sätt att det ska implementeras innan en eventuell attack. Det är dock den enda insats, tillsammans med

backuper som kan återställa system och återskapa filer i efterhand. Nästa framtagna strategi är **8. Simulerade phishing-attacker.** Ingen av verksamheterna som medverkade i studien utför simulerade phishing-attacker på medarbetarna i dagsläget. Simulerade phishing-attacker är viktiga att utföra eftersom ransomware främst sprids via mejl. Den tredje och sista punkten som lagts till är **9. Honeypot bör implementeras**. Honeypot kan utveckla säkerheten på så sätt att det är ett verktyg för att analysera den cyberkriminellas tillvägagångssätt. Information som hur angriparen kom in i systemet, vilken data denne är intresserad av och vilken nivå hotet är beläget på, kan i slutändan användas för att stärka IT-miljön ytterligare. Ingen av verksamheterna har Honeypot idag.

Sammanfattningsvis har alla regioner bra säkerhet för att bemöta det ökade hotet av ransomware men den kan förbättras ytterligare.

## 6.1. Framtida forskning

Vid fortsatt forskning är det av intresse att undersöka ett större antal regioner för att kartlägga hur svenska sjukhus garderar sig gentemot ransomware på en mer generell nivå. En större omfattning kommer troligtvis visa fler likheter och skillnader mellan regionernas arbetssätt än de som förekommer i detta arbete. Det skulle även vara intressant att enbart undersöka sjukhusens backup-rutiner djupgående, för att kartlägga hur mycket information som egentligen sparas. I dagsläget framgår det i Truesecs rapport att endast 90% av säkerhetskopierat material går att återskapa efter en ransomware-attack. Det kan vara intressant att forska vidare på om det går att utveckla backup-rutinerna så att det går att återställa systemen närmare 100%.

Ransomware är ett område som ständigt utvecklas och metoderna blir mer och mer avancerade. Därför är det viktigt att ständigt forska kring hur verksamheter kan upprätta skydd mot utpressningsvirus.

# Referenser/Källförteckning


[1] Eddy, Melissa., Perlroth, Nicole. 2020. Cyber Attack Suspected in German Woman's Death. *The New York Times.* 18 September. URL: https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html (Hämtad 2021-02-15)

[2] Milchner Funseth, Sara. 2020. Sverige betalar mycket för ransomware-attacker. *SVT Nyheter*. 7 november. URL: https://www.svt.se/nyheter/inrikes/sverige-betalar-mycket-for-ransomware-attacker (Hämtad: 2021-01-27)

[3] Truesec. 2021. *Svenska företag behöver rusta upp sitt cyberförsvar.* URL: https://www.truesec.com/news/svenska-foretag-behover-rusta-upp-sitt-cyberforsvar/ (Hämtad: 2021-04-26)

[4] Truesec. 2020. *Swedish Cyber Threat Landscape.* URL: https://www.truesec.com/wp-content/uploads/2020/06/Truesec-Swedish-Cyber-Threat-Landscape.pdf (Hämtad: 2021-01-27)

[5] Truesec. 2020. *Threat Intelligence Report 2021*. URL: https://f.hubspotusercontent30.net/hubfs/5907437/threat-intelligence-report-2021%20(1).pdf?utm_medium=email&_hsmi=121734494&_hsenc=p2ANqtz-8dn4oGRAichXrD3bYTeLWxjVP5XifLAktIhCWp-1x0Lk4Aq7WHfvqo5pVK5hmfa084CdntwGSKu1gs7eB-IzTBhB0bFtQ&utm_content=121734494&utm_source=hs_automation (Hämtad: 2021-04-23)

[6] Myndigheten för Samhällsskydd och Beredskap. 2020. *Öka motståndskraften mot ransomware.* Karlstad: Myndigheten för Samhällsskydd och Beredskap. URL: https://www.cert.se/2020/06/Rekommendationer_Oka_motstandskraften_mot_ransomware_juni2020_.pdf (Hämtad: 2021-02-18)

[7] Paquet-Clouston, Masarah., Haslhofer, Bernhard., Dupont, Benoit. 2019. Ransomware payments in the Bitcoin ecosystem. *Journal of Cybersecurity.* **1**(11) DOI: https://doi.org/10.1093/cybsec/tyz003

[8] Bhardwaj, Niharika., Coustasse, Alberto., Paul, David P., Spence, Nikki. 2018. Ransomware in Healthcare Facilities: A Harbinger of the Future? *Perspectives in Health Information Management.* URL: http://perspectives.ahima.org/wp-content/uploads/2018/06/RansomwareinHealthcare.pdf

[9] Richardson, Ronny and North, Max M. 2017. Ransomware: Evolution, Mitigation and Prevention. *Faculty Publications. 4276*. **13**(1). URL: https://digitalcommons.kennesaw.edu/facpubs/4276

[10] Singh, Hardeep., Sittig, Dean F. 2016. A Socio-Technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks. *Appl Clin Inform.* **7**(2): 624–632. DOI: 10.4338/ACI-2016-04-SOA-0064

[11] Morin, Johan. 2020. *Ransomware - Digitala kidnappare.* Kandidatuppsats, Umeå Universitet. URN: urn:nbn:se:umu:diva-173959

[12] Weckstén, Mattias., Frick, Jan., Sjöström, Andreas., Järpe, Eric. 2016. *A novel method for recovery from Crypto Ransomware infections*. 2nd IEEE International Conference on Computer and Communications (ICCC). 1354-1358. DOI: https://doi.org/10.1109/CompComm.2016.7924925

[13] Gagneja, Kanwalinderjit K. 2017. *Knowing the ransomware and building defense against it - specific to healthcare institutes.* Florida Polytechnic University Lakeland, USA. DOI: 10.1109/MOBISECSERV.2017.7886569

[14] Interpol. 2020. COVID-19 cyberthreats. URL: https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats (Hämtad 2021-02-25)

[15] Holme, Idar M., Solvang, Bernt K. 1991. *Forskningsmetodik - Om kvalitativa och kvantitativa metoder.* Lund: Studentlitteratur.

[16] SBU. 2017. *Utvärdering av metoder i hälso- och sjukvården och insatser i socialtjänsten: en metodbok.* (Kapitel 4). Stockholm: Statens beredning för medicinsk och social utvärdering (SBU). URL: https://www.sbu.se/globalassets/ebm/metodbok/sbushandbok_kapitel04.pdf (Hämtad 2021-03-03)

[17] Barajas, Katarina E., Forsberg, Christina., Wengström, Yvonne. 2013. *Systematiska litteraturstudier i utbildningsvetenskap - Vägledning vid examensarbeten och vetenskapliga artiklar*. Stockholm: Natur & Kultur.

[18] Vetenskapsrådet. 2017. *God Forskningssed.* Stockholm: Vetenskapsrådet. URL: https://www.vr.se/download/18.2412c5311624176023d25b05/1555332112063/God-forskningssed_VR_2017.pdf (Hämtad: 2021-03-03)

[19] Vetenskapsrådet. 2002. *Forskningsetiska principer - inom humanistisk-samhällsvetenskaplig forskning.* URL: https://lincs.gu.se/digitalAssets/1268/1268494_forskningsetiska_principer_2002.pdf (Hämtad: 2021-03-03)

[20] Gollman, Dieter. 2011. *Computer security*. 3. uppl. Chichester: Wiley.

[21] Cisco. 2020. What is Malware?. URL: https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html (Hämtad: 2021-03-04)

[22] Hull, Gavin., John, Henna., Arief, Budi. 2019. *Ransomware deployment methods and analysis: views from a predictive model and human responses*. Hull et al. Crime Sci. **8**(2). DOI: https://doi.org/10.1186/s40163-019-0097-9

[23] Zimba, Aaron. *Malware-Free Intrusion: A Novel Approach to Ransomware Infection Vectors.* International Journal of Computer Science and Information Security (IJCSIS), 2017. **15**(2) URL: https://www.researchgate.net/publication/322940640_Malware-Free_Intrusion_A_Novel_Approach_to_Ransomware_Infection_Vectors

[24] Everett, Cath. 2016. *Ransomware: to pay or not to pay?.* Computer Fraud & Security **2016**(4): 8-12. DOI: https://doi.org/10.1016/S1361-3723(16)30036-7

[25] SalehAl-rimyMohd, Ali, Bander., Maarof, Aizaini, Modh., Sahis, Mohd, Zainudeen, Seyd. 2018. *Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions*. Computers & Security. **74**: 144-166. DOI: https://doi.org/10.1016/j.cose.2018.01.001

[26] Wang, Zihan, Liu ChaoGe, Qiu Jing, Tian ZhiHong, Cui Xiang, Su2 Shen,. 2018. *Automatically Traceback RDP-Based Targeted Ransomware Attacks.* Hindawi Wireless Communications and Mobile Computing **2018**. DOI: https://doi.org/10.1155/2018/7943586

[27] Microsoft. 2020. *Ransomware groups continue to target healthcare, critical services; here's how to reduce risk.* URL: https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/ (Hämtad: 2021-04-05)

[28] Center for Internet Security. 2020. *Malvertising.* URL: https://www.cisecurity.org/blog/malvertising/ (Hämtad: 2021-03-30)

[29] Kaspersky. 2020. *What Is a Drive by Download*. URL: https://www.kaspersky.com/resource-center/definitions/drive-by-download (Hämtad: 2021-03-30)

[30] IBM Security. 2021. *X-Force Threat Intelligence Index 2021*. URL: https://www.ibm.com/security/data-breach/threat-intelligence (Hämtad: 2021-04-01)

[31] Truesec. 2020. *Threat Intelligence Report 2021 - Swedish Summary.* URL: https://f.hubspotusercontent30.net/hubfs/5907437/Swedish-Threat-Landscape-2020-Executive-Summary.pdf?utm_medium=email&_hsmi=121733138&_hsenc=p2ANqtz-8gjGYR0e0gyDHaE4MAZEpzdyDyrm_LSJ3ABeAJBS3GooK7SL3VPB3E9xozMFt-MzPdIOB3IpJe3rwwyJFJuAAwVBVe2KzzwvT_2yzhIgGufYz3n_pM&utm_content=121733138&utm_source=hs_automation (Hämtad: 2021-04-23)

[32] DNSstuff. 2020. *What Is a JBoss Application Server? Ultimate JBoss Tutorial.* URL: https://www.dnsstuff.com/what-is-jboss-application-server (Hämtad: 2021-04-06)

[33] Hassan, Najam. 2018. *Ransomware Attack on Medstar: Ethical Position statement. SEISENSE Journal of Management:* **1**(4), 29–31 DOI*:* https://doi.org/10.5281/zenodo.1435408

[34] Basini, Nick. CISCO TALOS. 2016. *SamSam: The Doctor Will See You, After He Pays The Ransom.* URL: https://blog.talosintelligence.com/2016/03/samsam-ransomware.html?m=1 (Hämtad: 2021-04-01)

**[**35**]** Ehrenfeld, J.M. 2017. *WannaCry, Cybersecurity and Health Information Technology: A Time to Act*. J Med Syst **41**(104). DOI: https://doi.org/10.1007/s10916-017-0752-1

[36] FOI - Totalförsvarets forskningsinstitut. 2019. *Kryptomaskar och deras konsekvenser: Åtgärder för cybersäkerhet utifrån fallen WannaCry och NotPetya*. Stockholm: FOI - Totalförsvarets forskningsinstitut. URL: https://www.foi.se/rest-api/report/FOI-R--4774--SE (Hämtad: 2020-04-05)

[37] Akbanov, Maxat., Vassilakis, G, Vassilios., Logothetis, D. Michael., 2019. *Ransomware detection and mitigation using software-defined networking: The case of WannaCry*. Computers & Electrical Engineering **76**: 111-121 DOI: https://doi.org/10.1016/j.compeleceng.2019.03.012

[38] Lika, Reyner, A., Murugiah, Danushyaa., Brohi, Sarfraz, N., Ramasamy, Daksha. 2018. *NotPetya: Cyber Attack Prevention through Awareness via Gamification*. 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE), Shah Alam, Malaysia. 1-6. DOI: 10.1109/ICSCEE.2018.8538431

[39] Ikeda, Scott. CPO Magazine. 2020. *Ransomware Attack at German Hospital Responsible for First Documented Death.* URL: https://www.cpomagazine.com/cyber-security/ransomware-attack-at-german-hospital-responsible-for-first-documented-death/ (Hämtad: 2021-04-01)

[40] Pope, Justin. 2016. *RANSOMWARE: Minimizing the Risks.* Innov Clin Neurosci. **13**(11–12). PMID: 28210525

[41] Nilsson, Anton. 2018. *Att hindra en Notpetya- och WannaCry-attack - Redogörelse med förebyggande metoder och tekniker.* Kandidatuppsats, Blekinge Tekniska Högskola. URN: urn:nbn:se:bth-16288

[42] Säkerhetspolisen. 2020. *Cybersäkerhet i Sverige – Rekommenderade säkerhetsåtgärder.* URL: https://www.sakerhetspolisen.se/download/18.f2735ce171767402ba203/1591164566364/Rapport-Cybersakerhet-Rekommenderade-Atgarder.pdf (Hämtad: 2021-04-06)

[43] Cisco. 2021. *What Is Network Segmentation?* URL: https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html#~resources (Hämtad: 2021-04-06)

[44] Dunbrack, Lynne. 2016. *Providing Outside-In and Inside-Out Protection Against Ransomware and Other Intensifying Cyberthreats.* IDC Health Insights. URL: https://www.fortinet.com/resources-content/fortinet/assets/analyst-reports/file/protection-ransomware-intensifying-cyberthreats (Hämtad: 2021-04-07)

[45] Cisco. 2021. What is a firewall? URL: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html (Hämtad: 2021-04-07)

[46] Johansen, Alison G. Norton. 2019. *What is antivirus software? Antivirus definition* URL: https://us.norton.com/internetsecurity-malware-what-is-antivirus.html (Hämtad: 2021-04-07)

[47] APSIS. 2021. *Spamfilter: kontroll i många led.* URL: https://apsis.se/blogg/spamfilter-kontroll-i-manga-led (Hämtad: 2021-04-07)

[48] Palo Alto Networks. 2021. *What is an Intrusion Detection System?* URL: https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-detection-system-ids (Hämtad: 2021-04-07)

[49] Palo Alto Networks. 2021. *What is an Intrusion Prevention System?* URL: https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips (Hämtad: 2021-04-07)

[50] Kaspersky. 2021. *What is a honeypot?* URL: https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot (Hämtad:2021-04-07)

[51] SiS - Svenska Institutet för Standarder. 2020. *Detta är ISO 27000* URL: https://www.sis.se/iso27000/dettariso27000/ (Hämtad: 2021-04-22)

[52] Jigsaw. 2021. *Känner du igen nätfiskeförsök?* URL: https://phishingquiz.withgoogle.com/ (Hämtad 2021-04-26)

# Bilagor

## Bilaga 1:

### Information till intervju-kandidat:

Detta examensarbete är på kandidatnivå och skrivs via akademin för informationsteknologi vid Högskolan i Halmstad, IT-forensik och informationssäkerhetsprogrammet.

**Syfte:**

Syftet med examensarbetet är att undersöka hur de svenska sjukhusen upplever och hanterar det ökade hotet av ransomware-attacker. Med hjälp av en kvalitativ intervjustudie kommer det utforska hur IT-säkerhetsansvariga på svenska sjukhus förhåller sig till att hälso- och sjukvårds-sektorn har blivit attraktiva mål för cyberangrepp. Dessutom kommer det undersökas hur IT-säkerhetsansvariga arbetar för att skydda sjukhusens IT-system mot en attack. Resultatet från intervjuerna kommer användas för att utforma förslag till åtgärder och återställningsplaner om sjukhuset skulle falla offer för ett utpressningsvirus.

**Sekretess och publicering:**

Medverkan i intervjun är frivillig och respondenten får lov att avbryta sitt deltagande när som helst. All information kommer hanteras konfidentiellt. I det publicerade arbetet kommer inte sjukhus/region samt deltagare i intervjun att nämnas vid namn. Intervju med respondent kommer att spelas in och därefter transkriberas. Transkribering av intervjun är nödvändig vid skrivandet av uppsatsen för att undvika desinformation. Även transkriberingen är anonym och kommer inte publiceras i uppsatsen. Arbetet kommer sedan att offentliggöras på Digitala Vetenskapliga Arkivet (DiVA).

Vi är medvetna om att det är många frågor som ska besvaras men vi hoppas hinna med så många som möjligt. Om vi inte hinner med alla och Ni känner att Ni har tid och möjlighet får Ni gärna skicka resterande svar via mejl. Har Ni frågor gällande intervjun och frågorna eller vill komplettera något i efterhand är Ni välkomna att kontakta oss.

Med vänliga hälsningar,
Julia Djurklou och Josefin Ahl

# Bilaga 2:

## Intervjufrågor:

### Allmän information:

- Har ni upplevt ett ökat antal *intrångsförsök* i era system? Vad för typer av intrång har ni märkt är mest förekommande?

- Har ni någon gång blivit utsatta för en ransomware-attack där angriparna lyckats kryptera er data eller låsa ert system?
    - Hur agerade ni?

- Har ni tydliga strategier för hur ni ska hantera och skydda er mot ransomware-attacker?
    - Vad gör ni för att minimera smittorisken om ni skulle upptäcka smittade enheter i er organisation?
    - Har ni någon katastrof-återställningsplan för att minska åtgärdskostnader om ni skulle drabbas av en attack?

### Informationssäkerhetsarbete och IT-policys:

- Är ni certifierade enligt ISO 27000?
    - Varför/varför inte?
    - Om nej;
        - Har ni andra styrdokument och skriftliga riktlinjer? (*Exempelvis någon form av IT-policy för att fastställa vilka säkerhetsrisker som finns och hur dessa ska förhindras.)*
        - Görs det kontinuerlig uppföljning av hur riktlinjerna följs i praktiken?
        - Arbetar ni ständigt med informationssäkerhet i organisationen så att ni hade kunnat bli ISO-certifierade i dagsläget om ni hade velat?

### Hårdvara/mjukvara:

- Har ni några lösningar på hårdvarunivå som ni använder er av för att hämma ransomware?

- Utför ni kontinuerligt backuper och hur ofta utförs det backups?
    - Vilka anser ni är era mest betydelsefulla backup-rutiner och hur fungerar dem?
    - Lagras era backuper internt (*ex. offline och offsite*) eller externt (*molnlagring*)
    - Testar ni era backups och återställnings-rutinerna med jämna mellanrum? (*För att säkerställa att de fungerar ifall ert system blir infekterat*)

- Har ni implementerade mejl-filter som förhindrar att virus sprids via mail?
    - Om ja; vilka filter använder ni er av?
- Begränsar ni användarnas behörigheter, så att de endast har tillgång till de delar av systemet och de filer som de måste ha för att kunna genomföra sina arbetsuppgifter?

- Hur ofta görs uppdateringar av följande;
    - Operativsystem?
    - Hårdvaror? (*Servrar etc.)*

- Används någon typ av outsourcing där ni lämnar ut tjänster till tredje part? Vilka?
    - Granskar ni organisationerna som ni lämnar ut tjänsten till med jämna mellanrum för att säkerställa att informationen bibehålls i säkert förvar?

- Används något antivirusprogram specifikt mot ransomware? Vilka?

- Används några brandväggar specifikt för att motverka ransomware? Vilka?
    - Har brandväggarna stöd för IPS? *(Intrusion Prevention System)*

**Nätverk och kommunikation:**

- Övervakar ni nätverkstrafiken? *Både internt och externt.*

- Vad har ni för lösningar när det gäller fjärråtkomst (t.ex. RDP)? (*Körs dom via en VPN-anslutning?*)

- Är (alla) era servrar uppkopplade mot internet?

- Segmenterar ni ert nätverk?

- Används Honeypot eller motsvarande som speglar ert system/nätverk för att motverka att ett intrång sker i det "riktiga" systemet?

**Personal och arbetsrutiner:**

- Hur arbetar ni för att förbättra era medarbetares kunskaper inom informationssäkerhet och kunna känna igen hot på nätet?
    - Det första tecknet på en ransomware-attack är ett suspekt meddelande på skärmen. Har era medarbetare kunskap om vad detta kan innebära och hur de ska hantera det?
    - Utför ni simulerade nätfiskeattacker för att motverka att era slutanvändare trycker på skadliga länkar som kan orsaka intrång? *(Awareness training)*

Josefin Ahl
josahl@student.hh.se

Julia Djurklou
juldju@student.hh.se

HÖGSKOLAN
I HALMSTAD

Besöksadress: Kristian IV:s väg 3
Postadress: Box 823, 301 18 Halmstad
Telefon: 035-16 71 00
E-mail: registrator@hh.se
www.hh.se