MASTEROPPGAVE

Emnekode: SO330S

Navn på kandidat: Silje Furulund

Er cybersikkerheten god nok?

En studie av organisatoriske forutsetninger for cybersikkerhet i helsesektoren

Dato: 15.05.19

Totalt antall sider: 105

NORD universitet

www.nord.no

SAMMENDRAG

Da Helse Sør-Øst og Sykehuspartner ble utsatt for et målrettet cyberangrep i januar 2018 viste det for alvor at etterretningsaktivitet mot Norge ikke er begrenset til politiske og militære mål. Helse- og omsorgstjenesten er en bærebjelke i samfunnet vårt, og befolkningens liv og helse er noe av det mest sårbare vi har. Helsesektoren digitaliseres raskt, og sykehusene er i økende grad avhengig av digitale systemer i sin daglige drift og pasientbehandling. Helsesektoren må derfor bevare sikkerheten vår ved å håndtere truslene som oppstår i det digitale rom. Cybersikkerhet er et forholdvis nytt fenomen, og spørsmålet er hvorvidt helseforetak kan håndtere sårbarhetene, truslene og risikoen som oppstår når pasientbehandlingen forflyttes til det digitale rommet.

Studiens problemstilling er dermed: *Hvor forberedt er norske helseforetak på cybertruslene?* Formålet er å undersøke organisatoriske forutsetninger for cybersikkerhet i helsesektoren, og undersøke hvordan helsesektoren bør jobbe med egen cybersikkerhet.

Studien har en kvalitativ tilnærming der dataen er hentet ved dokumentanalyser og intervjuer. Datagrunnlaget er består av relevante dokumenter og åtte intervjuer med nøkkelpersoner innen cybersikkerhet i helsesektoren. Studiens teoretiske grunnlag omfatter en begrepsavklaring av «cybersikkerhet», teori om organisasjonskultur, med fokus på sikkerhetskultur, og teori om digital risiko – som innebærer begrepsavklaringer på sårbarhet, trussel og innen risiko.

Resultatet fra studien viser at helsesektoren er på vei til å få en helhetlig forankring av cybersikkerhet. Dette innebærer å ha kontroll på egne trusler, verdier og sårbarheter, og å jobbe med rask deteksjon og respons ved hendelser. Likevel er det noen rådende svakheter ved dagens cybersikkerhet. Helsesektoren mangler blant annet spisskompetanse innen cybersikkerhet, generell IKT-kompetanse hos sine ansatte og en robust sikkerhetskultur. Trusselaktørene arbeider stadig mer målrettet og profesjonelt, noe som er en viktig årsak til å betydelig heve IKT-kompetansen i helsesektoren, drive kontinuerlig opplæring og bevisstgjøring av ansatte og å utføre grundige og veldokumenterte risiko-, verdi- og sårbarhetsvurderinger.

Studien konklusjon er at helsesektoren ikke er forberedt på cyberangrep fra avanserte aktører i dag fordi de ikke har muligheten. De mangler kompetanse, ressurser, rett fokus og robust sikkerhetskultur. Dataangrepet mot Helse Sør-Øst har vært en viktig påminnelse om at cybersikkerhet må få økt fokus og bedre organisatorisk plassering i helseforetakene.

FORORD

Denne oppgaven er skrevet som siste del av mastergradsutdanningen innen samfunnssikkerhet og terrorismestudier ved Nord Universitet, fakultetet for samfunnsvitenskap. Arbeidet har pågått fra høsten 2018 til våren 2019.

Jeg vil først og fremst takke Stig Ole Johannessen, professor ved Nord Universitet, for støtten, tilbakemeldingene og veiledningen jeg har fått underveis i oppgaveskrivingen.

Jeg vil også takke alle informantene som har stilt opp til intervju. Dere har alle en travel hverdag, men brukte likevel arbeidsdagen deres på å snakke med meg. Takk for det – og ikke minst: takk for åpenheten.

Jeg vil også benytte anledningen til å rekke en stor takk til min storebror Håkon, som har fungert som en mentor og ikke minst en viktig støttefigur for meg i denne prosessen. Takk for at du har lest gjennom oppgaven min og gitt meg konstruktiv kritikk, og takk for at du har motivert meg til å gjennomføre. Jeg ønsker med det samme å takke mamma og pappa, som siden studiestart har støttet meg og presset meg til å fullføre.

Jeg må absolutt ikke glemme å takke Niklas, som har vært der for meg hele veien. Han har trøstet meg når jeg har vært nede, støttet meg både da jeg ville gi opp, og støttet meg da jeg bestemte meg for å fullføre likevel. Han har håndtert alle mine oppturer og nedturer. Tusen takk for at du holdt ut med en emosjonell og utslitt masterstudent.

Bodø, 15. mai 2019

Silje Furulund

INNHOLDSFORTEGNELSE

Sammendrag I
Forord II
Innholdsfortegnelse III
Forkortelser V
Kapittel 1: Innledning 1
1.1 Studiens tema 1
1.2 Litteraturgjennomgang 2
1.3 Formål og problemstilling 3
1.4 Begrepsgjennomgang 5
1.5 Oppgavens struktur 5
Kapittel 2: Bakgrunn og kontekst 6
2.1 Digitalisering 6
2.2 Organisering av helsesektoren 8
2.2.1 Organisering av IKT i helsesektoren 9
2.3 Cybersikkerhet i helsesektoren 11
2.3.1 Styringssystem for informasjonssikkerhet 11
2.3.2 Hard law and soft law 11
2.4 Trusler og sårbarheter 14
2.4.1 En øyeåpner for helsesektoren 14
2.4.2 Trusselbildet 15
2.4.3 Digitale sårbarheter 17
Kapittel 3: Teori 20
3.1 Tidligere forskning 20
3.2 Cybersikkerhet 23
3.3 Sikkerhetskultur 25
3.4 Digital risiko 27
3.4.1 Risikovurdering 29
3.4.2 APT-angrep 29
Kapittel 4: Metode 30
4.1 Valg av metode 30
4.2 Dokumentanalyse 31
4.2.1 Utvalg og presentasjon av dokumenter 31
4.3 Kvalitative dybdeintervjuer 33
4.3.1 Utvalg og presentasjon av informanter 33

4.3.2 Forberedelse og gjennomføring av intervjuene 36
4.4 Studiens kvalitet 37
4.4.1 Styrker og svakheter ved valgt metode 37
4.4.2 Pålitelighet 38
4.4.3 Gyldighet 40
Kapittel 5: Presentasjon av empiri 41
5.1 Digitalisering 41
5.1.1 Avhengighet til systemer 42
5.1.2 Fremtidens digitalisering 44
5.2 Dataangrep 45
5.2.1 Tiltak og læringspunkter 48
5.2.2 Fremtidig sikkerhet 51
5.3 Sikkerhetskultur 53
5.3.1 Bevisstgjøring og opplæring 57
5.3.2 Styringssystem 60
5.3.3 Ledelsen 63
5.4 Digital risiko 66
5.4.1 Risikovurdering 67
5.4.2 Trusselbildet 69
5.4.3 Sårbarheter 72
5.5 Oppsummering av empiri 76
Kapittel 6: Analyse og drøfting 78
6.1 Kjenner helseforetakene godt nok til den digitale risikoen? 78
6.2 Hvordan håndteres cybertruslene? 83
6.3 Hvordan er sikkerhetskulturen i helseforetakene? 85
Kapittel 7: konklusjon 88
7.1: Forslag til videre forskning 89
Vedlegg 90
Intervjuguide 90
Informasjonsskriv 92
Samtykkeerklæring 94
Referanser 95

FORKORTELSER

APT: Advanced Persistent Threat (No.: Avansert vedvarende trussel)

CERT: Computer emergency response team

DSS: Departementenes sikkerhets- og serviceorganisasjon

Difi: Direktoratet for forvaltning og IKT

DSB: Direktoratet for samfunnssikkerhet og beredskap

EKOM: Elektronisk kommunikasjon

EPJ: Elektronisk pasientjournal

E-tjenesten: Etterretningstjenesten

GDPR: General Data Protection Regulation

Hdir: Helsedirektoratet

HDO: Helsetjenestens driftsorganisasjon for nødnett HF

HF: Helseforetak

HoD: Helse- og Omsorgsdepartementet

IKT: Informasjons- og kommunikasjonsteknologi

ISO: International Organization for Standardization

IT: Informasjonsteknologi

IoT: Internet of things

Meld. St.: Melding til Stortinget

MTU: Medisinsk teknisk utstyr

NHO: Næringslivets hovedorganisasjon

NHS: National Health Service

NOU: Norges offentlige utredninger

NSM: Nasjonal sikkerhetsmyndighet

NUPI: Norsk Utenrikspolitisk Institutt

PST: Politiets sikkerhetstjeneste

RHF: Regionale helseforetak

ROS: Risiko- og sårbarhet

KAPITTEL 1: INNLEDNING

1.1 STUDIENS TEMA

Én av tre nordmenn bekymrer seg for at Norge skal rammes av terrorangrep (DSB, 2018, s. 4). Nesten like mange, altså rundt 30 prosent av befolkningen, er bekymret for at viktige styringsområder skal bli slått ut av cyberangrep (ibid.). Ekspertene mener at spørsmålet ikke lenger dreier seg *om* Norge rammes av cyberangrep – det er heller ikke kun snakk om når. I dag er det snakk om hvor ofte og hvor alvorlige angrepene kan bli – og hva eller hvem som vil rammes.

I 2012 ble cyberangrep for første gang tatt med på listen over de mest sannsynlige hendelsestypene (World Economic Forum, 2012, s. 12). Ett år senere ble cyberangrep fremhevet som en av risikoene med både høyest sannsynlighet og høyest konsekvens (DSB, 2014b, s. 182). I følge *The Networked Readiness Index 2016* (Baller et al., 2016, s.16) er Norge et av verdens mest digitaliserte land (nr. 4 av 139). Det gjør oss ekstremt sårbare for cyberangrep – en trussel som stadig øker. Av de fire trussel- og risikovurderingene som utgis årlig, blir digitale angrep mot kritisk infrastruktur[1] nevnt i samtlige. I dag er spørsmålet om hvordan vi kan sikre de digitale systemene våre på best mulig måte for å unngå at trusselaktører får tilgang til informasjonen vår, og hvorvidt man er godt nok forberedt når krisen først rammer. Angrep i det digitale rom er et økende problem, noe som gjør at organisasjoner er nødt til å sette seg inn i sin egne digitale risiko – og ikke minst hvordan cyberangrep og cyberkriminalitet kan oppdages raskest mulig.

Digitaliseringen har endret hvordan organisasjoners kan kontrollere prosesser, komplekse operasjoner og infrastruktur. Det er tverrpolitisk enighet om at effektiv digitalisering av offentlig sektor er et sentralt virkemiddel for å møte de utfordringene samfunnet står overfor når det gjelder produktivitet og effektivisering. De aller fleste virksomheter og næringer har et ønske om å digitalisere, og de digitale avtrykkene en person i Norge legger igjen blir større.

Antall enheter som er tilkoblet Internett øker eksplosivt (NSM, 2018b, s. 13). Uten tilstrekkelig sikring av internettilkoblede enheter og god sikkerhetsbevissthet, mener Nasjonal sikkerhetsmyndighet (NSM) at den digitale utviklingen vil utfordre oss på avgjørende måter. Digitaliseringen har gjort det mulig å gjøre ting enklere og smartere for både individer, bedrifter og samfunnet. Næringslivets Hovedorganisasjon (NHO) påpeker likevel at «svekket tillit til

[1] Tap/forstyrrelser i funksjonaliteten kan få alvorlige konsekvenser for offentlig sektor (NOU 2018:14, s. 137)

digitale løsninger vil kunne redusere bruken av de digitale løsningene med størst potensial» (2018). Det betyr at nærings- og samfunnslivet taper gevinster dersom brukerne ikke har tillit til at digitale løsninger er trygge å bruke. Man må derfor bevare tilliten i digitale systemer, men det forutsetter at sektorer og bedrifter har kunnskap om hvordan teknologien skal sikres.

Norges regjering har lenge hatt et stort fokus på å digitalisere offentlig sektor, og helsesektoren har kommet langt i digitaliseringsprosessen (Meld. St. 27 (2015-2016), s. 67). Norske sykehus bruker tusenvis av digitale systemer, og er svært avhengig av at systemene fungerer. Men avhengigheten av systemer som styres av programvare øker raskere enn evnen til å sikre dem (Tønseth, 2017). Når alt kobles til Internett, blir vi mer sårbare for hacking. Dette er ikke lenger kun snakk en trussel mot informasjonssikkerhet og personvern, men også liv og helse.

Brukerne av digitale tjenester forventer at teknologien blir brukt, men det forventes også at den skal gå fremover. Befolkningens liv og helse er sårbart, noe som gjør en fungerende helsesektor til noe av det viktigste et samfunn kan ha. Det er viktig at sykehusenes systemer er tilgjengelig og optimaliserte hele tiden. Det kan være kritisk at sykehusenes systemer er utilgjengelige. Samtidig er det et grunnleggende krav om informasjonssikkerhet, og som pasient forventes det at informasjonen som sykehusene innehar kun er tilgjengelig for de som er berettiget.

Befolkningens liv og helse er noe av det mest sårbare vi har. Med et digitalisert helsevesen er helsen vår mer sårbar enn noensinne. Et cyberangrep mot sykehus kan ramme både strøm- og vannforsyninger og elektronisk kommunikasjon (EKOM). Dette kan sykehus klare seg uten i noen få dager, men ikke lenger. I verste fall kan flere liv gå tapt på grunn av nedsatt eller mangel av funksjonsevne av kritisk infrastruktur (DSB, 2014a, s. 81). Disse problemstillingene er hyperaktuelle i helsesektoren. Livskritisk medisinsk utstyr og systemer som inneholder sensitiv pasientinfo, kobles i økende grad opp mot Internett. Målet er effektivisering og bedre behandling. Men da må brukerne kunne stole på den digitale teknologien.

I denne avhandlingen skal jeg argumentere for hvorvidt digitaliseringen skaper økte digitale sårbarheter og trusler i helsesektoren, og hvilke elementer som må håndteres og inkluderes for å minimere digital risiko. Jeg skal altså argumentere for cybersikkerhet i helsesektoren.

1.2 LITTERATURGJENNOMGANG

Det finnes mange forskningsartikler og studier innen cybersikkerhet, noe som trolig henger sammen med økt faglig interesse for feltet i tråd med utfordringene som følger med dagens digitalisering. I litteraturgjennomgangen fant jeg flere interessante vitenskapelige artikler og

masteroppgaver, men avdekket samtidig at organisatoriske forutsetninger for cybersikkerhet i det norske helsevesenet er et lite undersøkt område i dag[2].

Sentrale myndigheter understreker at Norge er sårbart for angrep i det digitale rom, og at det mangler forskning innen feltet. Meld. St. 38 (2016-2017) om IKT-sikkerhet og Norges offentlige utredninger (NOU) 2015:13 *Digitale sårbarheter – sikkert samfunn* tar opp viktige problemstillinger knyttet til IKT-sikkerhet i Norge. Samtidig rettes oppmerksomheten mot cybersikkerhet i helsesektoren, og det nevnes hvilke vurderinger og tiltak som må gjennomføres. Meld. St. 38 (2016-2017, s. 61) viser til punkt 17.2.2 i NOU 2015:13 (s. 200), der det poengteres at man mangler forskning på IKT-sikkerhet i helse- og velferdsteknologien. I utvalgets problembeskrivelse kommer det frem at det er behov for en spisset forskningsinnsats for å se på sikkerhetsaspektene ved teknologien. Samtidig må man ivareta de mulighetene og utfordringene som ny helse- og velferdsteknologi gir (ibid.).

Jeg fant flere studier om cybersikkerhet i ulike organisasjoner og sektorer. Digitaliseringen og trusselbildet er i utvikling, og det var derfor viktig for meg å finne nyere studier og undersøke eventuelle forskningshull. Jeg fant forskning som tar for seg cybersikkerhet ved britiske sykehus etter dataangrepet mot National Health Service (NHS), og forskning som tar for seg problemstillinger knyttet til cybersikkerhet, som også berører helsesektoren i Norge. Jeg fant imidlertid få studier som fokuserer på organisering av cybersikkerheten i norske helseforetak. Det er mangel på nyere forskning som tar for seg hvordan sikkerhetssjefer ved helseforetakene konkret jobber med cybersikkerhet, cybertusler og bevisstgjøring og opplæring av ansatte. Denne problemstillingen er viktig å undersøke etter IKT-skandalen i Helse Sør-Øst, da det viste at den norske helsesektoren er et aktuelt mål. Den foreliggende avhandlingen er et vitenskapelig bidrag til å forstå organisatoriske forutsetninger for cybersikkerhet ved norske helseforetak.

1.3 FORMÅL OG PROBLEMSTILLING

Formålet med denne studien er å undersøke organisatoriske forutsetninger for cybersikkerhet i helsesektoren, og bidra til kunnskap om hvordan sektoren kan og bør jobbe med cybersikkerhet. Jeg skal skissere noen mulige løsninger, men også svakheter ved dagens cybersikkerhet. Det innebærer å undersøke helseforetakenes forståelse av egen digital risiko. Jeg retter altså et kritisk blitt mot forankringen av cybersikkerhet, og undersøker hvorvidt norske helseforetak er

[2] Se kapittel 3.1 for gjennomgang av tidligere forskning innen cybersikkerhet og sikkerhetskultur i helsevesenet.

forberedt på å møte cybertruslene som dominerer i samfunnet vårt og hvor motstandsdyktige de er mot denne type angrep. Jeg skal sammenligne synspunkter og erfaringer rundt cybersikkerheten ved ulike helseforetak, samt sentrale problemstillinger og utfordringer. Oppgaven retter seg mot ledelsen ved helseforetakene og skal bidra med å øke kunnskapen om viktigheten av cybersikkerhet. Dette vil ikke bli løsningen på dagens digitale utfordringer, men et forslag til hvilken tilnærming man kan ha til cybersikkerhet, noe som kan videreføres til andre sektorer. Det er opp til virksomhetene å vurdere hva som er relevant og nødvendig for egen fremdrift.

Med dette i bakhodet tar studien for seg problemstillingen: *Hvor forberedt er norske helseforetak på cybertruslene?* For å svare på problemstillingen har jeg valgt tre forskningsspørsmål:

1. Kjenner helseforetakene godt nok til den digitale risikoen?
2. Hvordan håndterer ledelsen cybertruslene?
3. Hvordan er sikkerhetskulturen i helseforetakene?

For å besvare problemstillingen har jeg kartlagt cybersituasjonen i helsevesenet, samt hvilke vurderinger som er blitt gjort av situasjonen. Jeg innhentet først informasjon fra relevante rapporter og trussel- og risikovurderinger. Deretter gjennomførte jeg semistrukturerte intervjuer for å få førstehåndsinformasjon fra sikkerhetssjefer i helseforetakene.

AVGRENSNING

Helsesektoren er stor sektor og kompleks, og inneholder flere tekniske komponenter og systemer. Av den grunn vil jeg poengtere at dette ikke er en teknisk oppgave der tekniske systemene blir grundig studert. Fokuset i studien legges på organisering av cybersikkerhet, og hovedsakelig menneskelige faktorer. Dermed fokuseres det på relaterte sårbarheter og trusler, samt hvilke utfordringer som knyttes til det å etablere god cybersikkehet. Hovedfokuset i studien er altså de organisatoriske forutsetningene for cybersikkerhet og hvilke synspunkter sikkerhetssjefer ved helseforetakene har. For å avgrense oppgaven har jeg valgt å undersøke de regionale helseforetakenes IKT-leverandører, samt ett av de lokale helseforetakene underlagt RHF-et, ved bruk av kvalitative dybdeintervjuer. På denne måten skal jeg forsøke å generalisere funnene mine, og sammenligne de ulike synspunktene rundt cybersikkerhet og IKT-ledelse.

Jeg ser på problemstillingen i lys av dataangrepet som rammet Helse Sør-Øst januar 2018, da dette er det største cyberangrepet Norge har opplevd, samtidig som det viste tydelig at helsesektoren er et aktuelt mål for statlige aktører. Det vil si at jeg vil undersøke helseforetakenes holdninger og rutiner rundt cybersikkerhet, hvilke sikkerhetstiltak de iverksatte da angrepet var et faktum og hvorvidt de har gjort endringer i etterkant av angrepet – og eventuelt hvorfor endringer har blitt gjennomført.

1.4 BEGREPSGJENNOMGANG

Advanced Persistent Threat (APT): APT er en vedvarende, avansert trussel. En APT forutsetter at trusselaktøren besitter store ressurser. De har god tid, høy kompetanse og avanserte verktøy. Angrepene er målrettede og i noen tilfeller også støttet av en statlig aktør.

CEO-fraud (Direktørsvindel): Defineres som svindel utført ved hjelp av e-post eller telefon fra personer som utgir seg for å være i ledelsen i virksomheten (HelseCERT, 2018, s. 5).

Denial-of-service attack (DDoS): DDoS er et tjenestenektangrep der man hindrer at noen eller noe (f. eks. en person eller et system) får tilgang til informasjon, eller ressurser de skal ha tilgang til, ved at tjenesten "bombarderes" med trafikkmengder langt ut over det den er designet for å takle i en normal belastningssituasjon (HelseCERT, 2018, s. 5).

Malware: Et sammensatt begrep for «Malicious Software», skadevare. Det er en ondsinnet kode designet for å få tilgang på en maskin ved å lure brukeren til å installere et program. Malware ses for det meste i form av keyloggere, virus, ormer eller spyware. Malware kan brukes for å stjele sensitiv informasjon eller spre spam via e-post.

Ransomware: En form for skadevare, som en ondsinnet kode, som låser din maskin ved å kryptere data/informasjon og som krever løsepenger for at informasjonen skal bli dekryptert (HelseCERT, 2018, s. 5). Det kreves stort sett i form av Bitcoins. Individuelle filer kan også krypteres ved bruk av en privat nøkkel som kun forfatterne av ransomware-viruset kjenner.

1.5 OPPGAVENS STRUKTUR

Oppgavens struktur legger opp til en logisk og dyptgående gjennomgang av temaet:

- *Kapittel 1:* Presentasjon av studiens tema, formål, problemstilling og avgrensning, samt litteraturgjennomgang, før relevante begreper innen cyberkriminalitet belyses.
- *Kapittel 2:* Oppgavens bakgrunn og kontekst klargjøres for å gi leseren forståelse over organiseringen av helsesektoren og sentrale elementer som i diskuteres i studien.
- *Kapittel 3:* Tidligere forskning studien relateres til, samt studiens teoretiske grunnlag.
- *Kapittel 4:* Bakgrunn for valgt metode, samt diskusjon av studiens kvalitet.
- *Kapittel 5:* Presentasjon av empiri gjort på bakgrunn av intervjuer og dokumentanalyser.
- *Kapittel 6:* Oppsummering av studiens viktigste funn, samt analyse og drøfting av empiri opp mot utvalg teori.
- *Kapittel 7:* Avsluttende konklusjon og forslag til videre forskning.

KAPITTEL 2: BAKGRUNN OG KONTEKST

Helsevesenet er en stor og kompleks sektor som har gjennomført flere reformer knyttet til organisering og styring, herunder IKT-sikkerhet. Helsevesenet har kommet langt i bruken av digitale systemer, noe som har gjort sektoren sårbar for cybertrusler. Dette ble høyst aktuelt for den norske helsesektoren i 2018, da Helse Sør-Øst ble rammet av et cyberangrep. For å sette teori og tidligere forskning i kontekst til avhandlingens tema og problemstilling, skal jeg redegjøre for sentrale elementer som fremkommer i denne oppgaven.

2.1 DIGITALISERING

«Digitalisering» får stadig økt oppmerksomhet. Digitalisering er ikke et nytt fenomen i seg selv, men omfanget og hastigheten kan derimot sies å være relativ ny. Digitaliseringens raske utvikling skaper nye og flere utfordringer knyttet til sikkerhet på nett. Det kan stilles spørsmålet om hvorvidt man er klar over digitaliseringen faktisk innebærer og hvordan det vil påvirke oss.

Begrepet digitalisering brukes først og fremst om konvertering av analoge data til digitale data, men også om innføringen av digital teknologi eller verktøy som erstatter, effektiviserer eller automatiserer manuelle eller fysiske oppgaver (Bratbergsengen, 2017). Konkrete eksempler er digitaliseringen av offentlig sektor, EKOM, e-post og elektroniske pasientjournaler (EPJ).

Digitaliseringen har allerede endret måten vi styrer prosesser på, flyttet grenser for hva som er mulig å få til og gitt et mangfold av tjenester (NHO, 2018). NHO påpeker at det er en positiv utvikling som øker samfunnets totale produktivitet, men at vi er nødt til å ha *tillit* til teknologien (ibid.). Et grunnleggende prinsipp er at vi må ha tillit til at teknologien er trygg å bruke, men likevel ser man at digitalisering fører til en digital usikkerhet (ibid.).

Flere samfunnskritiske funksjoner er avhengige av digitale verdikjeder, som ofte strekker seg på tvers av sektorer og land (NOU 2015:13, s. 15). Det gjør at sårbarheten øker. Samtidig kobles flere enheter til Internett, noe som øker kompleksiteten og sårbarhetene i systemene. I følge NSM (2018c, s. 13) er kompleksitet den største sårbarheten i det norske digitale samfunnet. Når digitale økosystemer kobles sammen, blir avhengighetene uoversiktlige. Potensielle angripere kan dermed utnytte det svakeste leddet i en verdikjede og lete etter den enkleste veien til målet.

Økende bruk av IoT-teknologi («Internet of things») betyr at vi nærmer oss en situasjon der nesten alt koblet til nett. Det reiser et dilemma om avhengighet, men også om sikkerhet. Før snakket man om «datasikkerhet», men nå dreier datasikkerhet seg om sikkerhet i absolutt alt vi bruker. Det handler om sikkerheten til kritiske samfunnsprosesser, men også om egen sikkerhet.

UTFORDRINGER VED DIGITALISERINGE AV HELSESEKTOREN

Helsesektoren har kommet langt i digitaliseringen grunnet høyt fokus fra regjeringen og de omfattende helsereformene som har foregått de siste 10 årene. En viktig og vesentlig del av de gjennomførte og pågående reformene er styring, herunder effektivitets- og sikkerhetsmål ved bruk av IKT, og sammenlignet med andre land var Norge var tidlig ute med å bruke IKT på mange områder i helsesektoren (NOU 2015:13, s. 185).

Når man snakker om IKT i helse- og omsorgstjeneste brukes betegnelsen «E-helse». De siste årene har det blitt etablert flere viktige nasjonale e-helsetjenester, som kjernejournal, m-helse, EPJ og e-resept. Disse tjenestene bidrar til forenkling og forbedring for både pasienter og helsepersonell, og samtlige har vært fornøyde med flere av løsningene (Meldt. St. 27 (2015-2016), s. 67). Tjenestene gir også omfattende gevinster for samfunnet og kan i beste fall redde liv. Likevel er det viktig å være klar over hvilke utfordringer som følger med e-helsetjenesten.

Helsesektoren digitaliseres for å levere bedre og mer effektive tjenester til pasientene, og sektoren har kommet langt i digitaliseringsprosessen. I følge Meld. St. 27 (2015-2016, s. 67) går utviklingen av IKT i helse- og omsorgstjenesten raskt, og det har bidratt til store endringer. Informasjonshåndteringen i helsesektoren blir stadig mer digitalisert og automatisert, og de moderne og gode IKT-løsningene skal gi pasientene mulighet til å ta egne valg rundt egen helse og helsetilbud. I Meld. St. 27 (ibid.) kommer det frem at helse- og omsorgssektoren er en av de mest kunnskaps-, teknologi- og informasjonsintensive sektorene.

Digitalisering kan forbedre og forenkle samfunnet og helsesektoren på mange måter, noe ny teknologi allerede har bevist. Likevel kan endringer i samfunnet sjelden skje uten hindringer eller utfordringer. Digitale systemer er stadig i endring; de blir mer komplekse og mer uavhengige, noe som kan skape problemer når en sektor skal forsøke å få nye digitale systemer til å fungere optimalt. Dessuten har den moderne utviklingen både organisatoriske, tekniske og menneskelige utfordringer. Derfor er det viktig å være klar over utfordringer knyttet til både privatliv, sikkerhet, tilgjengelighet, avhengighet, kompleksitet, risiko, endring og kompetanse.

Bruk av IKT en vesentlig del av de gjennomførte og pågående reformene i sektoren, spesielt med fokus på effektivitets- og sikkerhetsmål. I dag har sykehusene egne systemer for bl.a. pasientstyring, laboratoriestyring, radiologistyring, operasjonsstøtte og klinisk overvåkning, som igjen består av flere undersystemer, noe som gjør at også infrastrukturen internt i sykehusene er svært kompleks. I NOU 2015:13 (2015, s. 185) kommer det frem at det stilles

grunnleggende krav til taushetsplikt, dokumentasjonsplikt og behovet for tilgang til nødvendige opplysninger til helsehjelpsformål i IKT-systemene i helsesektoren.

Digitale helsetjenester er stadig i endring, noe som gjør det viktig å være oppmerksom på hvilke digitale sårbarheter som finnes i den digitaliserte helsesektoren. I SINTEF-rapporten *Digitale sårbarheter i helsesektoren* (Omerovic & Gjære, 2015) kommer det frem en rekke utfordringer som helsesektoren står ovenfor. Tilgjengelighet av IKT-systemer og beredskap mot nedetid blir trukket frem som sentrale utfordringer i SINTEF-rapporten og i NOU 2015:13. Helsevesenet har så små marginer at liv kan gå tapt dersom IKT-systemene er nede over lengre tid. Det finnes gode manuelle rutiner og mulighet for utskrifter på papir, noe som gjør at sykehuset kan holde driften i gang noen timer – men ikke over flere dager. Manglede kompetanse når det gjelder cybersikkerhet er også en utfordring helsesektoren står ovenfor. Mangel på IKT-kompetanse blant helsepersonell vil i en tid med digitalisering være en stor utfordring.

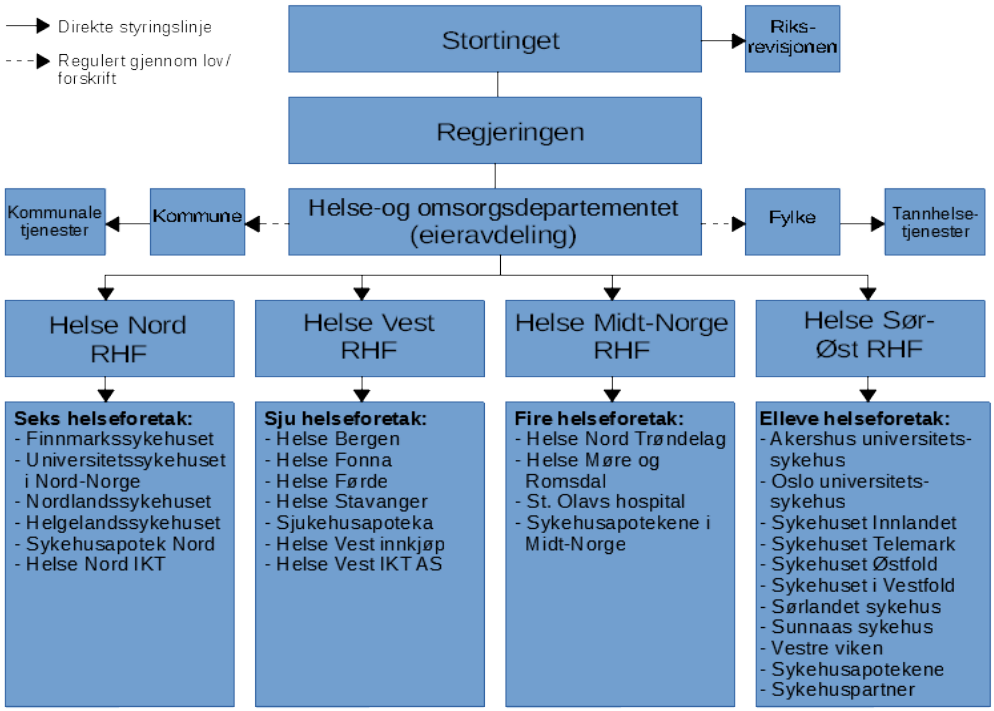
2.2 ORGANISERING AV HELSESEKTOREN

Helsevesenet er en av Norges største samfunnssektor, med over 300.000 ansatte fordelt på 17.000 virksomheter i offentlig og privat sektor. Sektoren er kompleks, bestående av mange administrative styringsnivåer, organisatoriske enheter, styringssystemer og verdikjeder (NOU 2015:13, s. 185 og 199). Ettersom jeg skal undersøke de organisatoriske forutsetningene for cybersikkerhet i helsesektoren, skal jeg sette organiseringen av helsevesenet i kontekst. Deretter spesifiserer jeg hvordan IKT-sikkerhet organiseres.

Siden begynnelsen av 2000-tallet har sektoren vært gjennom flere omfattende reformer (NOU 2015:13, s. 185). Reformene er gjennomført ved flere særlover. F. eks er styringssystemet i helseforetaksmodellen fra 2002 formalisert i helseforetaksloven, der reformens hovedelementer beskrives i Ot.prp. nr. 66 (2000-2001). Det første elementet ved reformen var at staten overtok eierskapet til fylkeskommunale sykehus og øvrige virksomheter innenfor spesialisthelse-tjenesten, slik at det offentlige eierskapet ble samlet på statens hånd (NOU 2016:25, s. 30).

Det andre elementet i helseforetaksreformen var at virksomhetene ble organisert i foretak. De ble dermed egne rettssubjekter og styrt av uavhengige styrer, og har ansvar for driften og styringen av de lokale helseforetakene. De er imidlertid ikke en integrert del av den statlige forvaltningen (ibid.). Overordnede helsepolitiske mål og rammer fastsettes av staten og ligger til grunn for styring av foretakene. Staten har et helhetlig ansvar for spesialisthelsetjenesten, både når det gjelder sektoransvaret, finansiering og eierskapet (ibid.). Spesialhelsetjenesten eier og styrer de fire regionale helseforetakene (ibid., s. 41). De lokale helseforetakene er på sin side

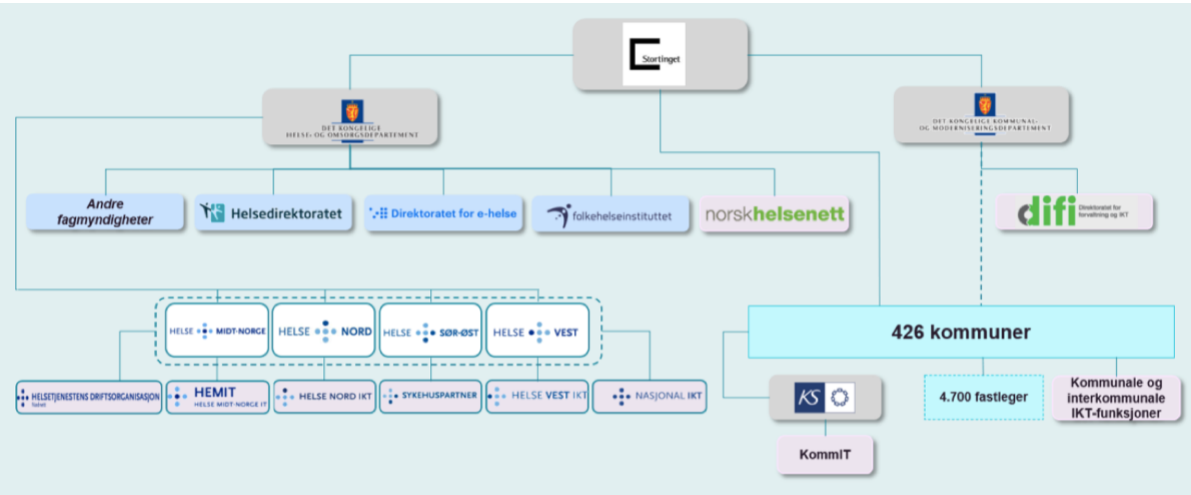
selvstendige juridiske enheter med eget ansvar som arbeidsgiver, og har derfor et styre og en ledelse med klare fullmakter (Ringard et. al., 2014, s. 25-26). I dag er det fire regionale helseforetak. Det er ikke gjort nevneverdige endringer siden helseforetaksloven ble vedtatt i 2001, og helsevesenet har siden den gang blitt organisert slik vi kjenner den i dag (se figur 1).



Figur 1: Oversikt over det norske helsesystemet, inspirert av Ringard (2014, s. 13). HOD eier og styrer RHF-ene, som igjen eier og styrer de lokale helseforetakene.

2.2.1 ORGANISERING AV IKT I HELSESEKTOREN

Aktørbildet i helse-og omsorgssektoren er komplekst, med ca. 17.000 aktører som bruker IKT til å realisere målene sine (Direktoratet for e-helse, 2017, s. 7). Figur 2 gir et overblikk over aktørene som er spesielt relevante for digitaliseringen i helsesektoren, samt styringslinjene. Nedenfor gir jeg en kort beskrivelse av aktørene som hovedsakelig tilknyttes spesial-helsetjenesten og informasjonssikkerhet i helseforetakene.



Figur 2: Aktørbildet (Direktoratet for e-helse, 2017a, s. 37)

HOD har det strategiske ansvaret for IKT-utviklingen sektoren. Departementet har overordnet ansvar for informasjonssikkerhet og objektsikkerhet, og styrer RHF-enes arbeid med beredskap og sikkerhet (NOU 2015:13, s. 187). HOD eier RHF-ene og Norsk Helsenett SF, og har flere underliggende departementer som ivaretar faglige og juridiske roller innen IKT (ibid., s. 37).

Helsedirektoratet (Hdir) er et fag- og myndighetsorgan med ansvar for å iverksette politikk og IKT-tiltak, samt å forvalte lov og regelverk, innenfor helse- omsorgssektoren (NOU 2015:13, s. 187). Direktoratet har det overordnede ansvaret for at de nasjonale strategiene for elektronisk samhandling og standardisering blir fulgt opp og realisert. I tillegg mottar Hdir oppdrag fra HOD angående myndighetsoppgaver knyttet til informasjonssikkerhet (ibid.).

Direktoratet for e-helse er et fagdirektorat for HOD. Direktoratet har nasjonal myndighet og premissgiverrolle på e-helseområdet og skal være en pådriver i utviklingen av digitale tjenester i helse- og omsorgssektoren. Ledelse og styring knyttet til standarder og retningslinjer innen IKT-området er sentrale oppgaver for direktoratet (Direktoratet for e-helse, 2017a, s. 38).

Norsk Helsenett SF (NHN) ble etablert som et statsforetak etter initiativ fra RHF-ene. NHN styres med oppdragsbrev fra HOD og skal sikre at det ligger en sikker, robust og egnet nasjonal IKT-infrastruktur for samhandling mellom aktørene i sektoren. NHN bidrar til forenkling, effektivisering og kvalitetssikring av elektroniske tjenester, og utarbeider risikovurderinger for nye eller endringer av eksisterende tjenester, i tillegg til å gjennomføre sårbarhetskartlegginger i egen infrastruktur (Direktoratet for e-helse, 2017a, s. 39; NOU 2015:13, s. 188).

De regionale helseforetakene (RHF-ene) har ansvar for spesialisthelsetjenesten, forskning og undervisning, samt et «sørge for»-ansvar og tilretteleggingsansvar for at helseforetakene kan yte helsetjenester. I tillegg mottar RHF-ene styringsføringer fra politiske mål og strategier, også for IKT-området. For å ivareta IKT på en best mulig måte har RHF-ene opprettet en felles IKT-tjenesteleverandør som ivaretar utvikling, drift og forvaltning av løsningene til RHF-et og deres tilhørende HF (Direktoratet for e-helse, 2017a, s. 38; NOU 2015:13, s. 187). Hvert RHF har ebalert en egen IKT-tjenesteleverandør. IKT-leverandørene er organisert på ulike måter:

	Helse Sør-Øst RHF	**Helse Vest RHF**	**Helse Midt-Norge RHF**	**Helse Nord RHF**
IKT-leverandør	Sykehuspartner HF	Helse Vest IKT	Helse Midt IT (Hemit)	Helse Nord IKT
Organisering	Helseforetak	Aksjeselskap	Egen avdeling	Helseforetak

Tabell 1: Oversikt over IKT-tjenesteleverandører og organisering i RHF.

2.3 CYBERSIKKERHET I HELSESEKTOREN

Den økte digitaliseringen i helsevesenet har gjort sektoren mer sårbar og utsatt for cyberangrep. Samtidig øker utfordringen rundt informasjonssikkerhet og personvern. Personvern og informasjonssikkerhet er to nøkkelord for helsesektoren, spesielt når det gjelder beskyttelse av informasjon og teknologi. Som et svar på de nye sårbarhetene har helsesektoren fokus på å sikre at både personvern og informasjon blir sikret på best mulig måte. Viktige aktører for sikring av IKT-systemer er Norsk Helsenett og HelseCERT. I tillegg er helsesektoren underlagt ulike lover og forskrifter som skal sikre informasjonssikkerheten.

2.3.1 STYRINGSSYSTEM FOR INFORMASJONSSIKKERHET

Virksomheter har behov for systematikk i styring og kontroll for å sikre at man oppnår mål og resultatkrav, etterlever lover, arbeider effektivt og har pålitelig rapportering på flere områder (Difi, 2019). Ett av områdene er informasjonssikkerhet, der formålet er å sikre at man har tilstrekkelig internkontroll på sikring av konfidensialitet, integritet og tilgjengelighet av informasjon. Dette gjelder både for ekstern og intern informasjonsbehandling (ibid.). Styringssystemet har hjemmel i obligatoriske og anbefalte krav.

Styringsdokumentet som sikrer informasjonssikkerheten i helsesektoren er Styringssystem for informasjonssikkerhet, som utgis av Direktoratet for e-helse (2018). Styringssystemet skal gjennomføres ved behandling av person- og pasientopplysninger, og sikrer at arbeidet med personvern og informasjonssikkerhet blir en kontinuerlig prosess og ivaretatt på en systematisk og dokumentert måte. Det består videre av en styrende, kontrollerende og gjennomførende del.

Styringssystemet er et ledelsessystem, og er derfor spesielt relevant for virksomhetens leder/ledelse, sikkerhetsleder og dataansvarlig (ibid.). Styringssystemet har hjemmel i Personvernforordningen, samt Pasientjournalloven §§ 22 og 23, men viser også til anbefalte standarder som Normen, ISO/IEC 27001:2013 (ibid.). Styringssystemet består av 54 faktaark, der hvert enkelt faktaark har ulike virkeområder og ulike målgrupper.

2.3.2 HARD LAW AND SOFT LAW

Helsesektoren er underlagt flere lover som verner om helse- og personopplysninger og informasjonssystemer. Helsepersonelloven av 1999, pasientjournalloven av 2014 og personopplysningsloven, samt ny sikkerhetslov av 2019 er noen av dem. Stortinget vedtok ny personopplysningslov i 2018, som består av nasjonale regler og EUs personvernforordning

(GDPR - General Data Protection Regulation) (Datatilsynet 2018b). Personvernforordningen stiller krav til tilstrekkelig informasjonssikkerhet ved innføring av egnede tekniske og organisatoriske tiltak (Datatilsynet, 2018a). Forskrift om IKT-standarder i helse- og omsorgssektoren, med hjemmel i pasientjournalloven, skal bidra til at virksomheter som yter helsehjelp bruker IKT-standarder for å fremme sikker og effektiv elektronisk samhandling (2015, § 1). Videre har ikrafttredelsen av ny sikkerhetslov av 2019 åpnet for at helse- og omsorgssektoren underlegges loven. Tidligere var ikke IKT-systemene i helsesektoren underlagt sikkerhetsloven, men ny sikkerhetslov gjelder grunnleggende nasjonale funksjoner. På denne måten tar den i større grad opp i seg at også IKT-systemer støtter opp under nasjonal sikkerhet, noe som åpner for at den vil bli gjeldende også for helsesektoren.

SIKKERHETSLOVEN

Trussel- og sårbarhetsbildet endrer seg raskt, noe som gjør at sikkerhetsloven må endre seg i takt med de nye sikkerhetsutfordringer. Det er bakgrunnen for at ny lov om nasjonal sikkerhet (sikkerhetsloven) ble tredd i kraft 1. januar 2019, som en modernisering av loven om forebyggende sikkerhetstjeneste av 1998 (Prop. 153 L (2016-2017), s. 7). Ny sikkerhetslov forebygger, avdekker og motvirker sikkerhetstruende virksomhet, og imøtekommer trussel- og sårbarhetsbildet ved å være dynamisk og fleksibel (ibid.; Sikkerhetsloven, 2018, § 1-1).

Sikkerhetsloven av 1998 la vekt på beskyttelse av gradert informasjon, men ny sikkerhetslov vil i tillegg kunne omfatte informasjonssystemer, infrastruktur og objekter av sentral betydning for nasjonal sikkerhet (Regjeringen, 2018c). Behovet for ny sikkerhetslov begrunnes spesielt i teknologiutvikling og globalisering der strukturer er avhengig av hverandre. Loven er utformet slik at den skal virke bedre i et samfunn med rask digital utvikling og stadig nye trusler, og den vil på så måte kunne bidra med å beskytte Norge bedre mot dataangrep (ibid.). Årsaken er at den nye loven styrker kravene til IKT-objekter, som utgjør at flere av objektene som skal sikres. Ansvaret for helseforetakene er dermed utvidet til å omfatte objektsikring og IKT-infrastruktur.

Ny sikkerhetslov fokuserer i større grad på hva virksomhetene skal *oppnå* enn hva de skal gjøre (ibid.). Det betyr at virksomhetene som er underlagt sikkerhetsloven vil få større selvstendig ansvar for egen forebyggende sikkerhet. De generelle kravene til forebyggende sikkerhets-arbeid innebærer dokumentasjons- og varslingsplikt, etablering av styringssystem for sikkerhet, gjennomføring av risikovurderinger, sikkerhetstiltak og øvelser. Sikkerhetsloven gjelder for statlige, fylkeskommunale og kommunale organer, i tillegg til leverandører av varer og tjenester i forbindelse med en sikkerhetsgradert anskaffelse (Sikkerhetsloven, 2018, § 1-2).

SOFT LAW

Mange virksomheter følger veiledere og standarder som ikke er regulert gjennom lov eller forskrift når det gjelder krav om IKT-sikkerhet. Virksomheter kan ha egne bransjestandarder som følges, som benyttes i tillegg til standarder av mer generell karakter. De mest relevante veiledningene på cybersikkerhetsområdet er NSMs grunnprinsipper for IKT-sikkerhet og ISO 27000-serien. Disse trekkes frem som viktige veiledere for helsesektoren. Samtidig har helsesektoren utarbeidet *Norm for informasjonssikkerhet og personvern i helse- og omsorgs-tjenesten* (Normen), som betegnes som den viktigste kilden til IKT-sikkerhet i sektoren (NOU 2018:14, s. 110). Samtlige standarder betegnes som *soft law,* som betyr at forpliktelsene *ikke* er bindende

NORMEN

Normen er ikke en egen lov eller forskrift, men en samling av krav om personvern og informasjonssikkerhet basert på regulering, og betegnes derfor per definisjon som *soft law*. Likevel er virksomheter knyttet til helsenettet forpliktet til å oppfylle kravene i Normen (NOU 2015:13, s. 185.). Normen bidrar til informasjonssikkerhet og personvern hos hver enkelt virksomhet og i sektoren generelt. Bransjenormen skal også bidra til at det etableres mekanismer hvor virksomhetene kan ha gjensidig tillit til at øvrige virksomheters behandling av helse- og personopplysninger gjennomføres på et forsvarlig sikkerhetsnivå (ibid.).

Teknologien og behandlingen av opplysninger som brukes i helsetjenesten kan bli utsatt for både utilsiktede og tilsiktede hendelser. Sektoren må derfor bygge og forvalte robust teknologi, organisasjon og sikkerhetskultur, i tillegg til å ha gode tiltak for å sikre at dette fungerer og samtidig håndtere tilfeller der det ikke fungerer. Normen bidrar i gjennomføringen av dette.

NSMS GRUNNPRINSIPPER FOR IKT-SIKKERHET

NSMs grunnprinsipper for IKT-sikkerhet definerer et sett med prinsipper, anbefalinger og underliggende tiltak for å beskytte informasjonssystemer (maskinvare, programvare og tilknyttet infrastruktur), data og tjenestene de tilbyr mot uautorisert tilgang, skade eller misbruk.

Grunnprinsippene beskriver hva en virksomhet bør gjøre for å sikre et IKT-system. Prinsippene beskriver hvorfor det bør gjøres, men ikke hvordan. NSM (2018a, s. 5) påpeker at grunnprinsippene ikke erstatter en virksomhets sikkerhetsstyringsarbeid, men at det er en komplettering. NSMs grunnprinsipper bygger på anerkjente standarder og rammeverk både i Norge og EU, deriblant ISO 27000-serien (NOU 2018:14, s. 119).

ISO-STANDARDER

ISO er en verdensomfattende sammenslutning av nasjonale standardiseringsorganer (NOU 2018:14, s. 120). Organisasjonen utarbeider og publiserer internasjonale standarder. En standard kan f. eks. være en måleenhet eller et styringssystem (ibid.). Standardene i ISO/IEC 27000-serien har til hensikt å sikre virksomheters informasjon og å ha et system for dette (ibid.).

ISO-serien inneholder råd for god praksis, sertifiseringsstandarder og retningslinjer for hjelp ved innføring. I Norge har Direktoratet for forvaltning og IKT (Difi) tilgjengeliggjort standarder i ISO/IEC 27000-serien for statsforvaltningen og inngått en rammeavtale med Standard Online, Standard Norges salgsselskap, om tilgang til standarder for 203 statlige enheter (ibid.).

2.4 TRUSLER OG SÅRBARHETER

2.4.1 EN ØYEÅPNER FOR HELSESEKTOREN

Bakgrunnen for denne studien er cyberangrepet rettet mot Helse Sør-Øst i 2018, da det viste at også helsesektoren er et aktuelt mål for statlige aktører som med ulik motivasjon er på jakt etter sensitiv informasjon. Jeg skal gi en kort oppsummering av hendelsesforløpene under angrepet for å vise hvordan angrepet ble håndtert fra start til slutt.

8. januar 2018 avdekket HelseCERT unormal aktivitet mot datasystemer i Helse Sør-Øst (HelseCERT, 2018). Helse Sør-Øst har ansvar for helsetjenestene til 2,9 millioner nordmenn, sensitiv forskning, laboratorier og apoteker. Både Helse Sør-Øst og Sykehuspartner gikk i beredskap og satte i gang flere tiltak for å få stoppet dataangrepet så fort som mulig (Mordt og Neumann, 2018). Som et sikkerhetstiltak ble pasientsystemet «MinJournal» stengt i flere uker etter angrepet (Didriksen, 2018). Etterhvert ble det kjent at dataangrepet var mer langt mer alvorlig enn det man først antok, men ingenting tyder på at pasientsikkerheten, pasientdataen eller pasientbehandlingen ble påvirket av angrepet (HelseCERT, 2018).

I forkant av angrepet hadde trusselaktøren avdekket mulige svakheter som kunne utnyttes til å gjennomføre et innbrudd (HelseCERT, 2018). Det er ukjent hvem som står bak angrepet, men det bærer preg av at det er gjennomført av svært profesjonelle aktører (Mordt og Neumann, 2018). Angrepet regnes som så stort og profesjonelt at man sannsynligvis aldri vil finne ut nøyaktig hvilke opplysninger inntrengerne har hentet ut eller hva de etterlot seg av bakdører i systemene (ibid.). Håndteringen av saken fikk høy prioritet, og alle tilgjengelige ressurser ble satt på saken – bl.a. NSM, PST, Etterretningstjenesten og Kripos (Flaarønning, 2018).

PST etterforsket saken for mulig brudd på straffeloven §121: «Bestemmelsen rammer ulovlig etterretningsvirksomhet som kan skade grunnleggende nasjonale interesser knyttet til samfunnets infrastruktur» (PST, 2018b). Etterforskingen viste at det dreide seg om kompromittering av en server i ekstern sone, som var åpen ut mot Internett. Mistenkte klarte deretter å ta seg inn i intern sone (ibid.), og skaffet seg administratortilganger og tilgang til nettverk med pasientopplysninger, forskningsdata og beredskapsplanverk. PST kan ikke fastslå om opplysningene er stjålet, men det er påvist at påloggingsinformasjon og filer tilknyttet en læringsapplikasjon er hentet inn av aktøren (ibid.). PSTs etterforsking avdekket svakheter i den ytre sikkerheten til systemene, som muliggjorde kompromitteringen i ekstern sone. Det ble videre avdekket manglende risiko- og verdivurderinger hos Helse Sør-Øst og Sykehuspartner. 5. desember 2018 ble saken henlagt grunnet manglende opplysninger om gjerningspersonen.

2.4.2 TRUSSELBILDET

«Nettverksangrepet mot Helse Sør-Øst i januar viser med all tydelighet at etterretningsaktivitet mot Norge ikke er begrenset til tradisjonelle politiske og militære mål» (E-tjenesten, Fokus 2018, s. 30).

NSM (2018b, s. 7) ser en negativ utvikling i trusselbildet. Endringen i trusselbildet knyttes bl.a. til økende profesjonalisering av grupperinger som ønsker å utnytte IKT-systemer (NOU 2015:13, s. 50). Beslutningstakere trenger derfor tilstrekkelig informasjon om IKT-trusselbildet (ibid., s. 257). Deler av IKT-trusselbildet formidles av aktører som Politiets sikkerhetstjeneste (PST), Etterretningstjenesten (E-tjenesten), NSM og DSB. Det utgis også sektorvise rapporter.

PST, NSM og E-tjenesten påpeker, gjennom trussel- og risikovurderinger i 2018 og 2019, at digital spionasje er den største risikofaktoren for norske virksomheter. Et utviklingstrekk innen nettverksoperasjoner er at statlige aktører tester og utvikler evnen til å gjennomføre alvorlig digital sabotasje, og at infrastrukturen hos norske virksomheter kompromitteres for å gjennomføre nettverksoperasjoner mot en tredjepart (E-tjenesten, 2019, s.16). Dataangrepet mot Helse Sør-Øst i januar 2018 viste for alvor at også helsesektoren er et mål for avanserte trusselaktører, noe som beskrives som en øyeåpner for sektoren. I NOU 2015:13 (s. 114) står det at tilbyderne og myndighetene må forholde seg til et dynamisk trusselbilde og se trussel-bildet i lys av samfunnets avhengighet av EKOM.

Helsesektoren var tidlig ute med å bruke IKT på flere områder. Pasientbehandling og pasientsikkerhet blir i økende grad avhengig av IKT. Digitale angrep kan forårsake nedetid på kritiske systemer i helsesektoren og påvirker dermed pasientsikkerheten. Denne trenden fortsetter å øke i takt med digitaliseringen av helsetjenestene, og nedetid er en alvorlig trussel

(Hdir, 2017, s. 19; HelseCERT, 2018, s. 4). HelseCERT (ibid.) poengterer at økt bruk av underleverandører og utsetting av tjenester fører til en økning av lange, uoversiktlige og svake verdikjeder som kriminelle kan utnytte. F.eks. kan det være sikkerhetshull i programvare eller manglende kunnskap hos underleverandører, og slik får trusselaktørene en større angrepsflate.

Cyberangrep øker i omfang og hyppighet, men evnen til å håndtere hendelsene er varierende. Helsedirektoratets risiko- og sårbarhetsvurdering (2017, s. 19) hevder dette skyldes svakheter i styring av forebyggende sikkerhet, lite tilfredsstillende lederforankring og at det er lett å hente informasjon. Oppsummert er det forbundet stor risiko for IKT-angrep i helsesektoren.

MANGELFULLT GRUNNLAG FOR HELHETLIG IKT-RISIKOBILDE

Det finnes ikke en helhetlig statistikk over omfanget av digitale angrep i Norge, og heller ikke en helhetlig fremstilling av IKT-trusselbildet (NOU 2015:13, s. 263). Aktørene som er involvert i å avdekke, håndtere og etterforske digitale angrep har ofte egen statistikk over saker de er involvert i, men dette samles ikke på ett sted (ibid.) Enkelte sektorer stiller krav om rapportering av hendelser, men det er ingen entydig kategorisering eller samling av denne typen rapporter. Manglende rapportering av IKT-hendelser begrenser evnen til å få et felles og korrekt IKT-trusselbilde, og dermed evnen til å forebygge og håndtere digitale hendelser (Ibid.)

Manglende forståelse for IKT og informasjonssikkerhet blir trukket frem som en del av det totale trusselbildet. Mangel på bred faglig oppdatering og forståelse i virksomhetene, og spesielt blant ledere, medfører at for mange fremdeles har en trusseloppfatning som ikke er oppdatert, og dermed ikke ser hele bildet. (Hdir, 2017, s. 22). I dag benytter både statlige og private trusselaktører flere vektorer og hybride metoder. I følge Hdir (ibid., s. 21) må IKT-trusselbildet derfor ses i sammenheng med tradisjonell fysisk sikkerhet og andre sikringstiltak.

TYPISKE ANGREPSMETODER

HelseCERT (2018, s. 4) hevder at cyberkriminalitet som phishing, CEO-fraud, ransomware og DDoS-angrep er cybertruslene man ser mest av i helsesektoren. Målrettede angrep fra avanserte trusselaktører utgjør imidlertid den største trusselen mot helsesektoren (ibid.). Dette er aktører som har stor kompetanse og kapasitet (ibid.). Trusselaktørene benytter seg oftest av metoder der de utnytter sårbarheter i tjenester som finnes på Internett eller gjennom bruk av målrettede e-poster (ibid.). I følge HelseCERT er dette kriminalitet som virksomhetene enkelt kan sette inn effektive tiltak mot, slik at det blir vanskeligere for trusselaktørerene å lykkes med angrepene. Det krever derimot kjennskap til eget trusselbildet, som aktuelle trusselaktører, sårbarheter, trusler og angrepsvektorer (angrepsmetoder).

NSM (2017, s.11), PST (2019, s. 8) og NOU 2015:13 (s. 59) poengterer at angrepsmetoder preges av e-post og kompromitterte websider med skadelig innhold (vannhull). Videre skriver NSM at utnyttelse av tjeneste- og underleverandører også brukes som en indirekte vei til målet gjennom sammenkoblede nettverk eller felles brukere (s. 11). I følge Hdir er det er et bredt spekter av angrepsvektorer mot sykehus og pasienter (Hdir, 2017, s. 21). Dette skyldes at helsesektoren er et massivt, komplekst og sammenkoblet økosystem med flere tusen endepunkter, systemer og brukere. Størrelsen, kompleksiteten og funksjonene i sykehusenes økosystemer skaper store og uforutsigbare angrepflater.

I rapporten *Securing Connected Hospital* kommer det frem at trusselaktører bruker følgende angrepvektorer for å infiltrere/sabotere systemene på sykehus (Fuentes & Huq, 2018, s. 6-7):

- *Phising* – Fisking etter sensitiv informasjon gjennom e-post.
- *DDoS-angrep* – Hackere forsøker å hindre andre i å få tilgang til en tjeneste eller ressurs.
- *Utnyttelse av svakheter/sårbarheter i programvare* – Bevisst bruk av kjente svakheter i programvarer. I 2017 måtte US Food and Drug Administration (FDA) trekke tilbake en halv million pacemakere grunnet sårbarheter i programvaren som tillot hackere tilgang.
- *Malware* – Det finnes flere eksempler på at ransomware, keyloggers, ormer, trojanere og andre skadevarer har påvirket helsevesenet.
- *Misbruk av tilgangsrettigheter* – En hacker fikk tilgang til en helsearbeiders nettverk via en installert tredjepartsprogramvare med svake passord og tillat administratoradgang.
- *Datamanipulasjon* – I 2015 advarte FDA mot sikkerhetsproblemer som tillater hackere å manipulere data i infusjonspumper som brukes for doseberegninger.

2.4.3 DIGITALE SÅRBARHETER

Når flere enheter, prosesser og tjenester kobles sammen og til Internett, skaper det rom for flere sårbarheter. S*årbarhet* defineres som «et uttrykk for de problemer et system får med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet» (NOU 2015:13, s, 31).

Risikoen for at uvedkommende får innsyn i sensitiv informasjon har økt med digitaliseringen (ibid.). Risikoen Norge står overfor øker fordi sårbarhetene blir flere og vanskeligere å kontrollere (NSM, 2018b, s. 9). Økt fokus på digital sikring av verdier innebærer at trusselaktører i større grad innretter seg med andre metoder og sårbarheter. Sårbarhetene som gjør oss utsatt for angrep er enten *menneskelige*, *organisatoriske* og/eller *tekniske*.

Mennesket i seg selv har i større eller mindre grad sårbarheter en trusselaktør kan utnytte, og en ansatt utgjør dermed en sårbarhet fordi vedkommende forventes å ha tilgang til verdier (NSM, 2018b, s. 15). Menneskelige egenskaper og vår evne til la oss lure er derfor blant de menneskelige sårbarhetene som trekkes frem av NSM (2015a, s. 15). Personlige helse-opplysninger er et eksempel på sensitiv informasjon som kan utnyttes. Det utgjør derfor både en personvernutfordring og en sikkerhetsutfordring dersom denne type informasjon kommer på avveie (NSM, 2018b, s. 16). Lav motivasjon til å følge sikkerhetsbestemmelser, og manglende kunnskap og evner, er andre menneskelig sårbarheter som trekkes frem av NSM.

Blant organisatoriske sårbarheter dreier det seg i følge NSM (ibid.) bl.a. om manglende lederforankring og styring av arbeidet med sikkerhet. NSM skrivet at «mangel på tydelig ansvarsdeling og bevisstgjøring er ytterligere kompliserende for sikkerhetsarbeidet» (ibid.). Det er generelt sårbarheter knyttet til at IKT-driftsmiljøer kan være små og mangle ressurser og kompetanse. I følge NSM varierer virksomheters fokus på sikkerhet i IKT-systemer stort.

NSM (ibid., s. 16) trekker frem en rekke tekniske sårbarheter. Dataprogrammer som ikke er oppdatert kan være en inngang som brukes til å bryte seg inn i datasystemene til en virksomhet. NSM påpeker at det kan finnes sårbarheter i maskinvarer, operativsystemer og applikasjoner, samt IKT-produkter som inneholder implementasjons- og designfeil (ibid). I følge Enisa Threat Landscape (Marinos, 2014, s. 24) er svak informasjonssikkerhet den viktigste årsaken til datainnbrudd. Trusselaktørene utnytter sikkerhetssvakhetene effektivt når de blir kjent. NSM (2018b, s. 16) hevder at flere av funnene i ENISAs rapport samsvarer med egne funn, og de erfarer at trusselaktørene gjør gode vurderinger av hva som er informasjon av høy verdi. Trusselaktørene arbeider altså stadig mer målrettet, og stadig mer profesjonelt.

DIGITALE SÅRBARHETER I HELSESEKTOREN

Jeg skal nå gå gjennom noen av de viktigste digitale sårbarhetene i helsesektoren, hovedsakelig med utgangspunkt i Helsedirektoratets overordnede risiko-og sårbarhetsvurderinger (2017).

Avhengighet til systemer og infrastruktur: I NSMs kartlegging av risikobildet i 2016 kom det frem at «Datasystemer ved sykehus er sårbare og sykehuspersonell er avhengig av tilgang til systemer og elektroniske pasientjournaler for å redde liv» (NSM, 2016, s. 19). Økt digitalisering forsterker avhengigheten til sentrale systemer og infrastruktur, noe som gjør at man blir sårbare for hacking. Helsedirektoratet (Hdir) mener det er nødvendig å ivareta sikkerheten gjennom komplekse tjenestekjeder, ikke bare i det enkelte system (Hdir, 2017, s. 20).

Avhengighet av EKOM, strøm og vann: Sykehus er avhengig av vann og avløp, og må stenge etter få timer hvis det bortfaller (NOU 2015:13, s. 192). EKOM-tjenester anses som en spesielt etterretningsutsatt kritisk infrastruktur, og tjenestene er i økende grad avhengig av digitaliserte prosesser (PST, 2017). Helsesektoren er sårbare for bortfall og vil få store praktiske problemer og redusert effektivitet dersom EKOM-tjenestene faller bort. Kommunikasjon mellom sykehusene vil stoppe opp og tilgang til pasientjournaler er avhengig av IKT-systemer. Uten dette er det vanskelig å opprettholde forsvarlig drift (NOU 2015:13, s 192).

Manglende høytilgjengelighet: Tilgjengelighet av IKT-systemer og beredskap mot nedetid er en utfordring i helsesektoren (NOU 2015:13, s. 191). Flere av sykehusenes digitale tjenester mangler tilstrekkelig redundans: «Digitaliserte prosesser, verktøy og produkter i helsesektoren har i varierende grad redundans, reservedrift og 24/7-support» (Hdir, 2017, s. 21).

Uoppdatert programvare: Erfaring viser at IKT-utstyr i sektoren ofte er utenfor support, noe som hovedsakelig skyldes manglende IKT-investeringer og avhengighet til eldre IKT-løsninger (Hdir, 2017, s. 21). Et stort antall av gamle IKT-systemer i sektoren er ikke utviklet til å beskytte seg mot trusler fra nettet og utgjør dermed en risiko (NOU 2015:13, s. 194).

Utfordringer i elektronisk meldingsutveksling: Epikriser, henvisninger og laboratoriesvar er eksempler på elektronisk meldingsutveksling i helsesektoren. Variasjon i tekniske løsninger fører til særlige utfordringer i elektronisk meldingsutveksling mellom helseforetakene og primærhelsetjenesten (Hdir, 2017, s. 21; NOU 2015:13, s. 193).

Manglende kompetanse: Ansatte som mangler tilstrekkelig sikkerhetsbevissthet, generell IKT-kompetanse og spesialistkompetanse, påpekes som en risikofaktor og sårbarhet. I følge NOU 2015:13 (s. 195) er dette en gjeldende utfordring i helsesektoren. Kompetansebehovet øker, og høy kompetanse på overordnet og detaljert teknisk nivå er viktig for å kunne forebygge og håndtere utilsiktede IKT-hendelser i helsesektoren. Tilstrekkelig sikkerhetskompetanse lokalt er avgjørende for å få en effektiv håndtering (NOU 2015:13, s. 190). Opplæring i sektoren er viktig, og det nevnes at helsepersonell sliter med å forstå systemene (ibid., s. 190).

Lange verdikjeder og manglende oversikt: Kritiske samfunnsfunksjoner har blitt avhengige av lange digitale verdikjeder, som spenner over sektorer, forvaltningsnivå og land. Det utgjør en sårbarhet fordi trusselaktøren får økt angrepsflate (NOU 2015:12, s. 289), som forsterkes av et komplekst aktørbilde der ansvaret for de ulike løsningene, produktene og verdikjedene er uoversiktlig (Hdir, 2017, s. 21).

KAPITTEL 3: TEORI

I dette kapittelet presenteres det teoretiske rammeverket oppgaven hviler på. Årsaken til gitt teori er å gi leseren forståelse for de ulike konseptene i denne oppgaven, noe som kan være nyttig for å forstå oppgavens forskningsspørsmål, diskusjon og konklusjon.

3.1 TIDLIGERE FORSKNING

Fritzvold har undersøkt cybersikkerheten i tre bransjer i Norge: helse, jernbane og kraftfordeling (Fritzvold, 2017, s. 2). Han mener det var uventet å se hvordan organisasjonene håndterer sikkerhetsutfordringene (ibid., s. 152). Han konkluderer med at de fremstår fremtidsorienterte og har en praktisk tilknytning til risiko og sårbarheter i digitale systemer. Samtidig viser de vilje til å investere i sikkerhetsteknologi og tiltak, og å utvikle kompetanse og erfaring (ibid.). Fritzvolds resultater viser at organisasjonene bruker IKT for å forbedre sikkerheten. Han mener at fokuset på sårbarheter i digitale systemer har utviklet seg, og at endringen og utviklingen er et svar på den voksende trusselen mot digitale systemer (ibid.).

I Perakslis´ studie om cybersikkerhet i helsevesenet kommer det fram at data og infrastruktur i helsesektoren kan være minst like sårbart som økonomiske og militære data (Perakslis, 2014, s. 395). Perakslis viser til at Helseinstitusjoner står overfor høy økonomisk risiko ved datatyveri grunnet mengdene data som lagres, men at trusler mot MTU og kritisk infrastruktur er av større bekymring grunnet pasientenes helse og sikkerhet (Perakslis, 2014, s. 396). Perakslis viser til Ponemon-studien (2013, s. 3) som antyder at organisasjoner kan redusere økonomisk risiko ved å endre holdninger til cybersikkerhet, ansette en informasjonssikkerhetssjef og bygge sterke reaksjonsevner ved hendelser. I følge Perakslis er det nødvendig med en aktiv tilnærming til læring for å prioritere og sikre strategier og taktikker innen cyberbeskyttelse. Det krever evne til å forstå det komplekse samspillet og dynamikken mellom utvendige trusler, egne sårbarheter, risikoer og systemets motstandskraft, i helsevesenets kontekst (Perakslis, 2014, s. 397).

Nigrin har studert hacking av sykehus i lys av cyberangrepet mot Boston Children's Hospital i 2014 (Nigrin, 2014). Angrepet viste at sykehusene var utsatt for en ny type risiko; istedenfor at hackerne gjorde systemene helt utilgjengelige, gjorde de kun visse funksjoner utilgjengelige. F.eks. kunne klinikere lage og skrive resepter, men de kunne ikke rute dem elektronisk til apotek (ibid., s. 394). Nigrin peker derfor på at sykehus bør utvikle egne beredskapsplaner for hvert klinisk system som er digitalt, fordi forberedelser på nedetid tradisjonelt har fokusert på totalt tap av nettverk eller tilgang (ibid.). Avslutningsvis peker Nigrin på at helsesektoren må

investere mer tid og ressurser i IT-sikkerhetssystemer og operativ beste praksis for å sikre at de er forberedt på å tåle og forsvare seg mot nye trusler (ibid., s. .395).

I en vitenskapelig artikkel om malware-angrepet mot NHS i 2017, hevder Clarke og Youngstein (2017, s. 410) at den største overraskelsen ved angrepet var at det tok såpass lang tid – ikke at det skjedde. Opplevelsen med cyberangrep har mer nyanserte og generaliserbare implikasjoner (ibid.). Hendelsen avslørte at helsepersonell ikke har vurdert den fysiske skaden som rammer pasientene dersom en ekstern, ondsinnet part tar over systemene (ibid., s. 411). Realiseringen viser nødvendigheten av å utstyre sykehus med tilpasset IT. Digital sikkerhet var ikke prioritert ved NHS før de ble rammet av det største cyberangrepet på kritisk infrastruktur i britisk historie (ibid.). For legene var det en «wake-up call». Til tross for at de mest sårbare pasientene klarte seg gjennom krisen, mener Clarke og Youngstein at helsepersonell har ansvar om å opplyse seg selv om de nye truslene og kreve midler for å sikre at programvarene er oppdatert og sikret.

Murphy har undersøkt mulighetene for cybersikkerhet i helsevesenet (Murphy, 2015). The Nationale Insititute for Standards (NIST) og International Organization for Standardization (ISO) har lagt rammene til de fleste metodene for risikovurderinger. Murphys studie viser til at cybersikkerheten i helsevesenet ikke kan baseres fullstendig på disse metodene, men at metodene for risikovurdering og cybersikkerhet må skreddersys til helsevesenet (ibid., s. 53). Murphy peker på at det må etableres og iverksettes utdanning- og sertifiseringskrav for å kunne utvikle en profesjonell sikkerhetstjeneste i helsevesenet som gir trygghet til både pasienter og arbeidsgivere (ibid., s.56). Det innebærer at fagfolk skreddersyr verktøyene og praksisen som brukes til å beskytte informasjonen, uten at det hindrer tilgjengeligheten (ibid., s. 57).

Fuentes og Huq har forsket på eksponeringen av medisinske systemer og risikoen ved leverandørkjeder (Fuentes & Huq, 2017). Gjennom undersøkelser av cybertrusler mot sykehus kom det frem at det er høy risiko for at sykehusenes systemer og informasjonssikkerhet kan bli utsatt for et målrettet angrep (ibid., s. 4-5). Økonomisk vinning er hovedmotivasjonen for angrepene (ibid., s. 6). Resultater fra undersøkelsen viser at den største trusselen for medisinske enheter er DDoS-angrep, som er lett å utføre. Trusler mot sykehusenes informasjonssystemer utgjør høy risiko da de har direkte innvirkning på alle sykehusbrukere og er enkle å gjennomføre (ibid., s. 43). Forskerne mener at forebyggende strategier mot cyberangrep og datainnbrudd bør bli en integrert del av sykehusenes daglige drift (ibid., s. 38). Cyberangrep og datainnbrudd er uunngåelig, så det er kritisk å ha effektive varslings- og skadebegrensingsprosesser (ibid.). Det sentrale prinsippet er å identifisere og reagere raskt på løpende sikkerhetsbrudd, kontrollere

sikkerhetsbruddet, hindre tap av sensitive data, forhindre angrep på forhånd ved å sikre alle utnyttbare veier, og å bruke erfaringer til å styrke forsvaret og hindre gjentatte hendelser (ibid.).

College of Health Professions (CHP) har gjennomført en systematisk gjennomgang av trusler og trender i helsevesenet, med formål om å identifisere mulige løsninger (Kruse et. al., 2017). Resultatet etter analyser av 31 artikler viste at helsevesenet ligger etter i sikkerheten sammenlignet med andre bransjer og næringer (ibid., s. 4). I følge forskerne bør helsevesenet definere sikkerhetsoppgaver for ansatte, etablere prosedyrer for oppgradering av programvarer og håndtering av datainnbrudd, bruke virtuelt lokalnettverk (VLAN), samt lære opp ansatte til å bli bevisste på cybersikkerhet (ibid., s. 7). Forskerne konkluderer med at helsesektoren er et ettertraktet mål for medisinsk informasjonstyveri fordi de henger etter i sikring av vitale data. Helsesektoren må derfor investere tid og midler i å opprettholde og sikre helseteknologi og konfidensialiteten til pasientinformasjon fra uautorisert tilgang (ibid., s. 8).

ISACA og CMMI Institute (2018) har studert IKT-sikkerhetskultur i USA. Studien viser at 95% av organisasjonene i studiene har kulturelle problemer knyttet til cybersikkerhet. Kun 5% av organisasjonene mener IKT-sikkerhetskulturen er tilstrekkelig til å sikre dem mot innvendige og utvendige trusler (ibid., s. 4). 9/10 av respondentene tror at etablering av sterkere IKT-sikkerhetskultur vil øke organisasjonens lønnsomhet eller levedyktighet (ibid., s. 3).

En stor andel studier viser til viktigheten av sikkerhetskultur. I følge Halligan og Zecevic (2011, s. 338) gjelder dette i økende grad også i helsesektoren. Studiene har imidlertid fokusert lite på å utvikle et felles sett av definisjoner, dimensjoner og tiltak (ibid.). Halligan og Zecevic har gjennomgått 135 engelskspråklige studier fra 1980-2009 om sikkerhetskultur i helsevesenet (ibid.). Resultatene tyder på at det er uenighet blant forskere om hvordan sikkerhetskultur skal defineres, samt hvorvidt begrepet «sikkerhetskultur» varierer fra begrepet «sikkerhetsklima». Denne variansen strekker seg inn i dimensjonene og måling av sikkerhetskultur og tiltak for å påvirke kulturendring (ibid). De mener helseorganisasjoner må gi konseptet en klar definisjon og kontekst for å kunne forbedre sikkerhetskulturen. Nieva og Sorra (2003, s. 17) hevder at helsevesenet gir økt oppmerksomhet mot betydningen av å endre organisasjonskulturen for å forbedre pasientsikkerheten. Økende interesse for sikkerhetskultur har vært ledsaget av behovet for vurderingsverktøy som fokuserer på kulturelle aspekter av forbedringsarbeidet for pasientenes sikkerhet (ibid.). I sin studie diskuterer de bruken av sikkerhetskulturvurdering som et verktøy for å forbedre pasientsikkerheten. Disse verktøyene kan brukes til å måle organisatoriske forhold som fører til bivirkninger og pasientskader, og for å utvikle og evaluere sikkerhetsforbedrende tiltak i helsevesenet (ibid., s. 21).

Tidligere forskning viser at helsesektoren er dårlig rustet til å håndtere cyberangrep. Forskere mener at helsesektoren trenger egne rutiner og metoder for risikovurderinger, da utfordringer knyttet til informasjonssikkerhet må ses i sammenheng med cybersikkerhet. Helsesektoren samler og lagrer store mengder helseinformasjon. Sektoren står i en særstilling når det kommer til å beskytte informasjonen – samtidig står de ovenfor en situasjon med økte datainnbrudd. Forskere er enige i at helsesektoren må vie mer tid og ressurser til cybersikkerhet, noe som innebærer kompetente IT-team, spesialkompetanse innen cybersikkerhet, økt kompetanse om cybersikkerhet og bedre sikkerhetskultur. Et tiltak er å innføre egne beredskapsplaner for hvert enkelt system. Forskerne er enige om at dagens cybersikkerhet ikke er tilstrekkelig, og sektoren er nødt til å ta grep da cybertrusselen øker. Det handler ikke nødvendigvis om å beskytte seg mot eller hindre dataangrep, men om å håndtere situasjonen når den oppstår.

3.2 CYBERSIKKERHET

Digitaliseringen har både skapt økt tilkobling *og* avhengighet av IKT og digitale systemer. Som følge av dette har risikoen for cyberangrep blir større, og en naturlig respons er cybersikkerhet. De siste årene har det digitale rommet utviklet seg raskt, noe som har gitt cybersikkerhet global interesse og betydning. Over 50 nasjoner har allerede publisert en form for strategidokument som beskriver deres offisielle holdning til cyberspace, cyberkriminalitet og/eller cybersikkerhet (Von Solms & Van Niekerk, 2013, s. 97). Norge lanserte sin internasjonale cyberstrategi i september 2017, som gjør rede for Norges styrende prinsipper og strategiske prioriteringer innenfor hele spekteret av internasjonal cyberpolitikk, deriblant cybersikkerhet.

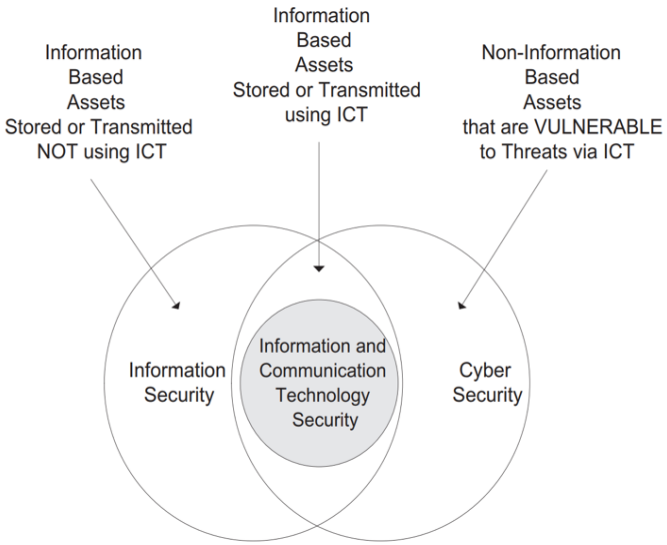
I følge Hans-Inge Langø er cybersikkerhet umoden som faglig nisje, og det foregår fortsatt en akademisk debatt rundt begrepet. Det finnes flere tilnærminger til cybersikkerhet, hvorav flere står i motsetning til hverandre. Samtidig er debatten om sikkerhetsutfordringene i cyberspace avhengig av en grundig og bred forståelse av de ulike problemstillingene (Langø, 2013, s. 229). Langø mener at en fruktbar tilnærming til studien av cyberspaces strategiske og politiske nytteverdi er «den økologiske skolen». Bidragene og fagfolkene som utgjør denne skolen fokuserer hovedsakelig på ideen om cybermakt i ulike former (ibid, s. 235). Likevel peker Langø på konsekvensene av å velge en økologisk tilnærming være mange: «Implisitt er det en antagelse at eksisterende analytiske rammeverk ikke er tilstrekkelige» (ibid., s. 238).

Flere begreper knyttet til sikkerhet på nett brukes ofte om hverandre, noe som gjør det viktig å ha forståelse over hva de ulike begrepene faktisk omfatter. Datasikkerhet, IT- og IKT-sikkerhet,

informasjonssikkerhet og cybersikkerhet brukes ofte som synonymer, men det betyr forvirrende nok ikke det samme. De ulike begrepene kan ha ulike nyanser, noe som i følge NSM utfordrer samhandling og koordinering dersom man ikke er bevisst på forskjellene (2015a, s. 40).

Noen av begrepene er mindre kompliserte og dermed enklere å skille enn andre. Informasjonssikkerhet handler om å bevare konfidensialitet, tilgjengelighet og integritet av informasjon – uavhengig om informasjonen er lagret digitalt eller ikke (Von Solms & Van Niekerk, 2013. s. 98). IKT-sikkerhet handler på sin side om å sikre informasjons- og kommunikasjonsteknologi, altså programvare og maskinvare (ibid.); man må beskytte *teknologien* som informasjonen er lagret og formidlet på for å kunne beskytte informasjonen. I dagens samfunn blir det meste av informasjon formidlet og lagret ved bruk av IKT, noe som kan være en årsak til at begrepene informasjonssikkerhet og IKT-sikkerhet blandes. IT-sikkerhet handler om å sikre informasjonsteknologi, og det er i praksis ingen forskjell på IT og IKT-sikkerhet. Datasikkerhet handler om sikring av data (ibid., s. 99). «Data» omfatter all slags informasjon som kan lagrer og overføres ved hjelp av teknologiske hjelpemidler (Schjølberg, 2017, s. 19).

Von Solms og Van Niekerk (2013, s. 99) påpeker at en rekke publikasjoner bruker begrepene cybersikkerhet og informasjonssikkerhet om hverandre. Til tross for at begrepene er noe overlappende, argumenterer de for at noen viktige forskjeller må tas i betraktning (se figur 3). Sikkerhet handler alltid om beskyttelse av eiendeler fra ulike trusler som skyldes visse iboende sårbarheter. Sikkerhetsprosesser handler vanligvis om valg og implementering av sikkerhetskontroller som hjelper med å redusere risikoen som følge av sikkerhetsproblemene.



Figur 3: Forholdet mellom informasjonssikkerhet, IKT-sikkerhet og cybersikkerhet (Von Solms & Van Niekerk, 2013, s.101).

Cybersikkerhet er ikke et nytt fenomen, men det kan virke nytt ettersom bruken av begrepet har eksplodert de siste årene. Cybersikkerhet dreier seg ikke om sikring av «cyberspace» i seg selv, men om å sikre det som er sårbart via IKT, samt informasjon og eiendeler som kan nås gjennom cyberspace (ibid., s. 101). Cybersikkerhet handler om å beskytte nettverk, programmer og systemer fra digitale angrep – der formålet kan være å få tilgang til, ødelegge eller endre informasjon, utpresse folk eller forstyrre forretningsvirksomheter.

Mange tenker kanskje ikke over er at også en rekke *fysiske* ting er sårbare via IKT med dagens teknologi. Dersom styringssystemene til et kraftverk er IKT-basert, kan kraftverket faktisk bli utsatt for fysisk skade via en ondsinnet programvare. Ved å bruke IKT kan hackere styre alle systemene som er basert på IKT, også i helsesektoren – noe som betyr at de i teorien kan endre injiseringsdosen i en automatisk insulinmaskin eller øke frekvensen i en pacemaker.

Betegnelsene «cybersikkerhet» og «cyberkriminalitet» har blitt vanligere i Norge som et ledd i tilpasningen til den internasjonale utviklingen (Schjølberg, 2017, s. 18). I rapporten *Sikkerhetsfaglig råd* (2015a, s. 11 og 40) foreslår NSM å erstatte begrepet IKT-sikkerhet med cybersikkerhet i politiske og strategiske dokumenter. NSM hevder at begreper som IKT-sikkerhet og cybersikkerhet brukes om hverandre som synonymer (ibid.). Det samme gjelder begreper som cyberangrep og dataangrep, samt IKT-trusler og cybertrusler. Med bakgrunn i NSMs anbefalinger forholder jeg meg til begrepene cyberangrep og dataangrep som synonymer, samt cybertrusler og cybersikkerhet. Unntaket er der jeg henviser direkte fra andre.

3.3 SIKKERHETSKULTUR

Sikkerhetskultur blir et gjennomgående tema i denne avhandlingen, særlig i forbindelse med presentasjonen av empiri. Dette bunner i at Hdir (2017, s. 24) etterspør sterkere sikkerhetskultur i helsesektoren. Samtidig viser akademisk litteratur at «sikkerhetskultur» som fenomen og begrep er omdiskutert og unyansert. Begrepet «sikkerhetskultur» ble for første gang introdusert i INSAGs ulykkes-rapport etter Tsjernobyl-ulykken i april 1986 (Choudhry et. al., 2007, s. 996). Ulykken beviste at det fantes teknologiske sårbarheter, og understreket behovet for organisatorisk sikkerhet (ibid.). Siden dette har konseptet blitt omfavnet av flere næringer for å forbedre sikkerheten, spesielt i høyrisikoorganisasjoner. Nylig har fokuset på å bygge god sikkerhetskultur også flyttet seg til helsevesenet (Halligan & Zecevic, 2011, s. 338).

Til tross for alt som har blitt skrevet om sikkerhetskultur i senere tid, er det fremdeles ikke enighet om hva det faktisk betyr (Hopkins, 2006, s. 4). Litteraturen om sikkerhetskultur er uklar, så derfor viser mange forskere til teori om *organisasjonskultur* for å forstå begrepet (DeJoy, 2005, s. 107). Men som flere begreper i samfunnsvitenskapen skal det likevel vanskelig gjøres å finne én enkel definisjon på begrepet «organisasjonskultur». Bang viser til definisjoner presentert av samfunnsforskere som Kroeber og Kluckhohn (1952), Deal og Kennedy (1982), Hofstede (2010), Schein (1993) og Beyer (1993), og inkorporerer de tre mest brukte kjerneelementene i litteraturen om organisasjonskultur til å etablere en egen definisjon: «de sett

av felles normer, verdier og virkelighetsoppfatninger som utvikles i en organisasjon når medlemmene samhandler med hverandre og omgivelsene, og som kommer til uttrykk i medlemmenes handlinger og holdninger på jobben.» (Bang, 2010, s. 337).

I følge NSM (2014) handler sikkerhetskultur om atferd knyttet til sikkerhet, for eksempel i forhold til informasjon eller objekter, og definerer det som «summen av de ansattes kunnskap, motivasjon, holdninger og atferd som kommer til uttrykk gjennom virksomhetens totale sikkerhetsatferd». Noen forfattere hevder at hver organisasjon har en sikkerhetskultur, som enten kan beskrives som sterk eller svak, positiv eller negativ. Andre forfattere hevder at det kun er organisasjoner med et overordnet engasjement for sikkerhet som kan sies å ha en sikkerhetskultur (Hopkins, 2003, s. 4). Med bakgrunn i dette hevder Hopkins at de færreste organisasjoner har en sikkerhetskultur og henviser til Reason som mener at «a safety culture is something that is striven for but rarely attained» (1997, s. 220, sitert i Hopkins, 2003, s. 4).

Det finnes flere definisjoner av sikkerhetskultur i akademisk litteratur. Choudhry (et. al, 2007, s. 996) har undersøkt omfanget av litteratur om sikkerhetskultur, og fant at kun 8 av 27 studier fra 1998-2007 har definert sikkerhetskultur. De fleste definisjonene som finnes er relativt like i trosperspektivet, men har ulike fokus og variasjon i folks tanke- og handlemåte rundt sikkerhet (ibid.). Definisjonene har en tendens til å forkaste oppfatningen om at sikkerhetskultur er noe organisasjon «er» istedenfor noe en organisasjon «har». Choudry (ibid) mener definisjonene vedtatt av Hale (2000) og Cooper (2000) er de mest praktiske, da de eksplisitt skisserer innholdet i sikkerhetskultur. Hale referer til sikkerhetskultur som «holdninger, tro og oppfatninger som deles av naturlige grupper som definerer normer og verdier, som bestemmer hvordan de handler og reagerer i forhold til risiko og risikostyringssystemer» (ibid., s. 999). Cooper definerer sikkerhetskultur som «den observerbare grad av innsats som alle organisasjonsmedlemmer retter sin oppmerksomhet og handlinger mot å forbedre sikkerheten på daglig basis» (ibid.).

The Advisory Committee on the Safety of Nuclear Installations (ACSNI. 1993) gir følgende definisjon av sikkerhetskultur, som i følge Nieva og Sorra (2003, s. 18) kan tilpasses pasientens sikkerhet i helsevesenet:

> *«The product of individual and group values, attitudes, perceptions, competencies, and patterns of behavior that determine the commitment to, and the style and proficiency of, an organization's health and safety management. Organizations with a positive safety culture are characterized by communications founded on mutual trust, by shared perceptions of the importance of safety and by confidence in the efficacy of preventive measures.*» (ACSNI, 1993, sitert i Nieva & Sorra, 2003, s. 18).

Verdier, holdninger, meninger, kunnskaper og handlinger som knyttes til sikkerheten i det digitale rom kan oppsummeres i begrepet «IKT-sikkerhetskultur» (Meld. st. 10 (2016-2017), s. 70). Bredden av sikkerhetskultur som illustreres i ACSNIs definisjon, reflekteres i det brede spekteret av temaer som dekkes av vurderingselementer av sikkerhetskultur (Nieva & Sorra, 2003, s. 18). Disse instrumentene vurderer ofte verdier, holdninger, bevegelser og normer for organisasjonsmedlemmer. De kan også fokusere på oppfatninger av organisatorisk kontekst, som ledelsesmessige prioriteringer, tilstrekkelighet av opplæring og ressurser, og retningslinjer og prosedyrer. Sikkerhetskultur henger altså tett sammen med organisasjonskulturen.

Enkelt forklart kan man si at sikkerhetskultur handler om organisasjoners evne til å styre sikkerheten, og at det er den delen av organisasjonskulturen som et rettet mot sikkerhet. I følge Hdir (2017, s. 24) kjennetegnes god sikkerhetskultur ved at ansatte er oppmerksomme på problemstillinger knyttet til personvern og informasjonssikkerhet, samtidig som de har tilstrekkelig kompetanse om det aktuelle trusselbildet, trusselaktører, teknologi, etc. Videre bør ansatte kjenne sin egen rolle og være klar over virksomhetens styringssystem og rutiner. Hdir hevder helsesektoren må bygge bedre sikkerhetskultur i møtet med det nye trusselbildet (ibid.).

3.4 DIGITAL RISIKO

«Trusselaktørene blir stadig mer profesjonelle, målrettede og kompetente, og for å stoppe dem må vi ha kontroll på våre egne sårbarheter og oversikt over vår egen risiko.» NSM, *Risiko 2018* (s. 30)

Økte tilkoblingsmuligheter eksponerer samfunnet for flere digitale sårbarheter, og cyberangrep er i dag en av de største truslene vi står ovenfor (NSM, 2018b; PST, 2019; E-tjenesten 2019). IKT-systemer er utsatt for risiko gjennom teknisk, menneskelig og organisatorisk svikt. Videre kan uønskede hendelser forårsakes av aktører gjennom ulike former for cyberangrep. Derfor er det viktig å kartlegge egen digital risiko.

Risiko handler alltid om hva som kan skje i fremtiden og forbindes derfor med usikkerhet. Usikkerheten knytter seg til om en bestemt uønsket hendelse vil inntreffe og hva konsekvensene vil bli. NSM (2015a, s. 10) definerer risiko som forholdet mellom de tre faktorene «verdier», «trusler» og «sårbarheter», ofte omtalt som risikotrekanten. *Sårbarhet* defineres som «et uttrykk for de problemer et system får med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet» (NOU 2015:13, s, 31). *Trussel* kan defineres som «en mulig årsak til en uønsket hendelse» (ibid, s. 32). NSM (2015a, s. 10) forbinder *trusler* og *risiko* med tilsiktede uønskede handlinger.

En tilsiktet hendelse er forårsaket av at noen gjennom målrettede handlinger utløser den uønskede hendelsen (NOU 2015:13, s 32). Kjennetegn på uønskede tilsiktede hendelser er at man ikke kan si når, hvor og med hvilke metoder en trusselaktør vil slå til. Det betyr at trusselbildet ligger utenfor det de fleste har mulighet til å gjøre noe med (NSM, 2015a, s.10). Sikkerhetsfaglig råd poengterer derfor at sikkerhetsarbeidet må rette fokus mot det vi *kan* gjøre noe med: «Det vil si å identifisere verdiene og interessene som kan være mål for trusselaktørene, og redusere sårbarhetene som kan utnyttes» (ibid.). Trusselaktører vil systematisk identifisere og utnytte det sikkerhetsmessig svakeste leddet i en virksomhet (NSM, 2018b, s. 15).

Aven (2015, s. 13) understreker at risiko består av to dimensjoner; konsekvenser (*K*) og usikkerhet (*U*). Aven (ibid.) forklarer at en gitt aktivitet vil lede til fremtidige konsekvenser (*K*) som er ukjente – altså usikre (*U*). Komponentene *K* og *U* utgjør altså en risiko fordi aktiviteten fører til usikre (*U)* konsekvenser (*K).* Konsekvenser er ofte fokusert på uønskede og negative konsekvenser, men Avens definisjon av risiko skiller ikke mellom positive og negative konsekvenser av aktiviteter. Det er imidlertid et krav at minst én av konsekvensene er uønsket eller negativ for at noe skal kunne betegnes som en risiko. En risikobeskrivelse oppnås ved å spesifisere hendelsen og antatte konsekvenser, samt ved å bruke en beskrivelse av usikkerhet (ibid.). Tabell 1.1 og tabell 1.2 viser hvordan digital risiko og risikoberskivelse kan beskrives:

Tabell 2.1: Digital risiko (Aven, 2015, s. 15)

Digital risiko
Konsekvens: Et cybeangrep av en kjent eller ukjent type og dets tidsforløp og konsekvenser for en organisasjon (IKT-bortfall, tap av informasjon, osv.)
Usikkerhet: Man vet ikke om eller når en organisasjon vil bli utsatt for en eller flere cyberangrep, og man vet ikke hva konsekvensene vil bli.

Tabell 2.2: Digital risikobeskrivelse (Aven, 2015, s. 15)

Digital risikobeskrivelse
Hendelse: Organisasjonen er utsatt for en bestemt type cyberangrep neste år.
Konsekvens: Organisasjonens konsekvenser forenkles i fire kategorier: 1) Organisasjonen lider av produksjonsstopp, 2) redusert produksjonshastighet, 3) tap av viktige data, 4) ingen.
Usikkerhet: Basert på kunnskapen vi har fått gjennom prosessen, kan vi uttrykke sannsynlighet for en slik begivenhet og konsekvensene. Dette kan være et kvantitativt eller et kvalitativt uttrykk av usikkerheten.
Kunnskap: Kunnskapen vi har basert på vurderingene er data, informasjon, modeller, berettiget tro og forutsetninger.

3.4.1 RISIKOVURDERING

Risikovurdering er et begrep i risikostyring, som dekker tre steg: risikoidentifisering, risikoanalyse og risikoevaluering (Difi, u.å.). En risiko og sårbarhetsanalyse-analyse (ROS) kan brukes for å beskrive og kartlegge risiko. ROS-analyser hovedsakelig en kvalitativ risikovurdering, bygget på faglig skjønn og erfaring (Brudvik, 2010), noe som viser seg som et effektivt verktøy for å definere forbedringsområder. Ved å kartlegge sannsynlighet og konsekvenser av uønskede hendelser, kan man prioritere risikoområder og planlegge tiltak for å forhindre dem eller redusere konsekvensen av dem dersom de skulle oppstå (ibid.).

Det finnes flere metoder for risikoanalyser. Et fellestrekk for de mest brukte metodene er lav brukerterskel og medvirkning av virksomhetens egne ansatte og tilknyttede medarbeidere under selve analysen (DSB, 2017.) ROS-metoden gir som resultat et bilde av risikonivået med nødvendige tiltak for de ulike tjenester eller de ulike delene av en tjeneste.

3.4.2 APT-ANGREP

Uønskede hendelser forårsakes av aktører med onde hensikter gjennom ulike former for cyberangrep. I dag er digital spionasje og økt interesse for personopplysninger en av de store digitale truslene helsesektoren står ovenfor, og bevissthet rundt svakheter i systemene er nødvendig for å unngå angrep. Det er svakhetene i systemene som trusselaktørene utnytter, og de mest vellykkede angrepene krever nøye planlegging og research over lengre tid, samt tilgang til verktøy og programvare som kan utføre oppgaven. Figur 4 viser de typiske trinnene i et «flerstegs»-angrep (eng.: «multi-stage attack»), som gjerne utøves av såkalte APT-aktører.

Baldwin og Shiu (2010, s. 15) hevder at flerstegs-angrep går ut på at angriperne får fotfeste i en virksomhet, sprer seg inn i andre IT-systemer og til slutt fjerner verdifulle data. De mest sofistikerte angrepene, ofte kjent som en «Advanced Persistent Threat» (APT), følger trinnene i figur 4 (ibid.). Baldwin og Shiu forklarer at angriperne «play the long game», med gjentatte forsøk på å fullføre målet. Det betyr at utvinning av data kan ta flere måneder, og at de skaffer seg litt og litt informasjon frem til de har nok til å få fotfeste i virksomhetens systemer. Angriperne oppnår som regel målene ved å blande sosialteknikk og malware, samtidig som de er nøye med å skjule sporene sine. De retter seg hovedsakelig mot enkeltpersoner og informasjon. Når fotfestet i virksomheten er sikret, sprer angriperne seg inn i andre systemer.

Figur 4: Typiske trinn i et «flerstegs»-angrep (Baldwin & Shiu 2010, s. 15)

KAPITTEL 4: METODE

Denne oppgaven er basert på akademisk litteratur, rapporter, trusselvurderinger, publikasjoner og intervjuer. Jeg har valgt å ha en kvalitativ tilnærming, og i dette kapittelet skal jeg presentere og redegjøre for de metodiske valgene jeg har gjort gjennom forskningsprosessen. Formålet er å beskrive forskningsprosessen fra start til slutt, forklare hvorfor jeg har tatt de valgene jeg har tatt og hvordan dette kan ha påvirket resultatene.

4.1 VALG AV METODE

Denne studien ble gjennomført fra oktober 2018 til mai 2019. Formålet har vært å undersøke cybersikkerhet i helsesektoren. En problemstilling gir retningslinjer for de metodiske og faglige valgene som tas i løpet av forskningsprosessen – samtidig må den være tilstrekkelig avgrenset for å realiseres innenfor gitte rammer (Thagaard, 2011, s. 51). Jeg har sett på problemstillingen: «Hvor forberedt er norske helseforetak på cybertruslene?». Helsesektoren er stor og kompleks, så jeg ville fått en enorm oppgave foran meg hvis jeg skulle studert *hele* helsesektoren. Av den grunn har jeg valgt å fokusere på de regionale helsefortaktene, og studert hvordan nøkkelpersoner knyttet til IKT ser på problemstillinger rundt cybersikkerhet. Hensikten er å finne ut hvor forberedt helseforetakene er på cyberangrep, og hvordan IKT-ledelsen jobber for å sikre informasjon. Jeg ønsker å utvikle forståelse rundt fenomener som er knyttet til arbeid med cybersikkerhet ved helseforetakene på bakgrunn av fyldige data om personer og situasjoner (ibid. s. 12), og derfor har jeg valgt å ha en kvalitativ tilnærming for å besvare problemstillingen. Kvalitative metoder egner seg godt fordi metoden kan gi meg detaljerte data.

Digitalisering og cyberangrep er nokså nye, men voksende fenomener. Det finnes dermed en rekke dokumenter jeg kan ta utgangspunkt i for å studere det nærmere, bl.a. risiko- og sårbarhetsvurderinger og Stortingsmeldinger. Nettverksoperasjoner mot norske virksomheter har vært et aktuelt tema de siste årene, men at helsesektoren er et aktuelt mål for statlige aktører ble for alvor satt på agendaen da Helse Sør-Øst ble utsatt for et omfattende dataangrep i 2018. Helse- og omsorgsektoren består av kritisk infrastruktur, så beskyttelse av infrastruktur var allerede et tema på Stortinget før angrepet skjedde. Det har gitt meg et godt grunnlag for dokumentanalysen, men det finnes likevel ikke nok dokumenter til at det kan svare på problemstillingen alene. Jeg har ikke lyktes med å finne dokumenter som gir meg et tilstrekkelig bilde av IKT-ledelsen i helseforetakene og hvordan fokuset på cybertrusler har endret seg etter angrepet mot Helse Sør-Øst. Derfor kombinerer dokumentanalyse og kvalitative intervjuer.

Dokumentanalysen ble primært brukt for å hente informasjon, men funnene brukes som et hjelpemiddel under diskusjonen av empirien. Ved bruk av dokumentanalysen undersøkte jeg hvordan cybersikkerhet er forankret i helsesektoren, samt for å få et bilde på dagens trusselbilde. Intervjuene gir meg svar på hvordan ledelsen i helseforetakene arbeider med cybersikkerhet på et organisatorisk, menneskelig og teknologisk nivå. Ved å kombinere dokumentanalyse og intervju vil jeg se om policy og praksis samsvarer i helseforetakene, og kan samtidig undersøke eventuelle ulikheter og likheter. Datainnsamlingen for denne studien ble utført fra oktober-april.

4.2 DOKUMENTANALYSE

Når man skal gjennomføre dokumentanalyse er det ønskelig å finne relevant informasjon. Jeg må derfor kategorisere innholdet i dokumentene, og registrere det som er faktisk interessant. Ved å gjennomføre en dokumentanalyse vil jeg undersøke sentrale dokumenter som tar for seg retningslinjer for organisering av IKT og styringssystem, samt trussel- og sårbarhetsbildet i helsesektoren. Silverman fremhever verdien av å bruke «naturlige forekommende data», som foreliggende tekster (2011: 229-234, I: Thagaard, 2011, s. 58). Fordelen med denne type data er at det er etablert uavhengig av min medvirkning og kan ikke bli påvirket av datainnsamling og analysen, de er lett tilgjengelige og har ikke etiske begrensninger. Begrepet *dokumenter* brukes om tekster som er etablert uten forskeres medvirkning, og med *dokumenter* menes alle skriftlige kilder som er tilgjengelig for forskerens analyser (ibid., s. 59). Thagaard understreker at studier av tekster kan benyttes i tillegg til andre data, og at det ofte fungerer som et supplement til andre metoder (ibid., s. 13 og 58). Derfor kombinerer jeg det med intervjuer.

4.2.1 UTVALG OG PRESENTASJON AV DOKUMENTER

Dokumentutvalget i denne studien er formålsorientert, som vil si at jeg har valgt enheter som gir meg relevant informasjon til å belyse problemstillingen (Jacobsen, 2015, s. 194). Jeg har gjennomført et utvalg av registrerte og tilgjengelige data, og en utfordring er at det kan ha oppstått frafall av data i en utvalgsprosess da jeg ikke registrerer alt som finnes – eller at noe ikke er offentlig tilgjengelig. I en studie skjer likevel utvalget parallelt med datainnsamlingen. Det vil si at problemstillingen min belyses bedre når jeg leser og tolker ulike tekster underveis. Dokumentene jeg registrerer fører meg derfor videre til flere dokumenter som også er relevante.

Ettersom jeg ikke har teknisk bakgrunn, ønsket jeg å samle inn så mye informasjon om cybersikkerhet som mulig på forhånd. Jeg studerte en rekke dokumenter for å få oversikt over IKT-sikkerheten og trusselbildet i helsesektoren, samt om problematikken som eksisterer i

feltet. I studien er jeg ute etter å undersøke hvilke cybertrusler sykehusene står ovenfor, hvordan det er forventet at helseforetakene jobber med cybersikkerhet, samt hva ledelsen faktisk gjør. Jeg har derfor fokusert på dokumenter som dreier seg om dette. Målet med dokumentanalysen var å få et helhetlig bilde på styringssystemet og IKT-organiseringen i helsesektoren, trusler og sårbarheter, og hvordan sikkerhetsarbeidet er forankret i helseforetakene. I utvalgsprosessen ønsket jeg derfor å finne bredde og relevans i dokumentene. Etter omfattende søk fant jeg et tilfredsstillende utvalg, og har for ordens skyld valgt å dele dokumentene inn i tre kategorier:

Den første kategorien er *regelverk og retningslinjer*. Med *regelverk* mener jeg lover, som sikkerhetsloven samt tilhørende forskrifter. Et viktig styringsdokument for cybersikkerhet er sikkerhetsloven av 2019. Den nye sikkerhetsloven førte til at helsesektoren blir underlagt sikkerhetsloven. De viktigste forarbeidene til sikkerhetsloven er Prop. 153 L (2016-2017) og NOU 2016:19. Med *retningslinjer* mener jeg helseforetakenes styringssystemer og Normen, som gir meg informasjon om hvordan ledelsen ved helseforetakene jobber med cybersikkerhet.

Den andre kategorien er *rapporter og trusselvurderinger*, som gir meg nyttig data om det aktuelle trusselbildet, samt trender og endringer de siste årene. Denne kategorien utgjør bl.a. risiko-og sårbarhetsvurderingene til PST, NSM og e-tjenesten. I tillegg har jeg brukt Helsedirektoratets egne oversikt over det aktuelle trussel- og sårbarhetsbildet (2017), samt HelseCERTs rapport *Situasjonsbilde* (2018), som er spesielt gjeldene i sektoren. NSMs grunnprinsipper for IKT-Sikkerhet (NSM, 2018a) og *Nasjonal e-helsestrategi 2017-2022* (Direktoratet for e-helse, 2017b og 2019), samt andre rapporter om cybersikkerhet og digitalt risikobilde produsert for helsevesenet, går inn i denne kategorien. Jeg har også sett på rapporten *Nasjonal strategi for digital sikkerhetskompetanse* (Regjeringen, 2019).

Den tredje kategorien, *Stortingsdokumenter*, utgjør hovedsakelig Stortingsmeldinger, men også offentlige utredninger. Jeg har sett på dokumenter som tar for seg digitalisering, sikkerhet, IKT og IKT-utfordringer i helse- og omsorgsektoren. Stortingsmeldinger og offentlige utredninger har vist seg spesielt nyttig, særlig med tanke på å få et bilde på hvordan IKT-organiseringen foregår, hvilke sårbarheter myndighetene fokuserer på og hvilke tiltak som må settes i gang. Flere av dokumentene har egne kapitler for helse- og omsorgsektoren, og det er først og fremst disse jeg har sett på – i tillegg til kapitler som tar for seg det generelle IKT- og sårbarhetsbildet. Et sentralt dokument for denne studien har vært NOU 2015:13 *Digital sårbarhet – sikkert samfunn*, fordi det er en nyere utredning som dermed er oppdatert på situasjonen i helsesektoren. I tillegg er vektlegges cybersikkerhet i utredningen.

4.3 KVALITATIVE DYBDEINTERVJUER

Dokumenter er ofte skreddersydd til det formålet datainnsamleren opprinnelige hadde, noe som begrenser hva jeg kan få ut av det (Jacobsen, 2015, s. 171). Dokumentanalysen ga derimot et informasjonsgrunnlag, samt et utgangspunkt for hva jeg kan undersøke nærmere, noe som er et godt utgangspunkt til intervju. Jeg ønsker å forstå deltakernes tanker, erfaringer og opplevelser knyttet til cybertrusler og cyberangrep, og hvordan IKT-ledelsen konkret arbeider med dette. Intervjusamtaler er et godt utgangspunkt for å få kunnskap om hvordan enkeltpersoner opplever og reflekterer over en situasjon, og kan samtidig gi fyldig informasjon om synspunkter og perspektiver (Ibid., s. 95). Jeg har valgt å gjennomføre kvalitative dybdeintervjuer fordi det finnes lite forskning om de organisatoriske forutsetningene for cybersikkerhet ved norske helseforetak. Derfor vil jeg ha mest mulig detaljert informasjon fra nøkkelpersonen innenfor dette, noe som best lar seg gjøre ved kvalitative intervjuer.

4.3.1 UTVALG OG PRESENTASJON AV INFORMANTER

Valg av informanter er avgjørende for hvilke funn man får, og det er nødvendig å ha et sett med informanter som er representative og relevante for problemstillingen (Jacobsen, 2015, s. 180). Thagaard (2013, s. 65) sier at antall deltaker i studien ikke bør være større enn at det er mulig å gjøre omfattende undersøkelser fordi analyser er tid- og ressurskrevende. Samtidig må intervjumaterialet gi et tilstrekkelig grunnlag for analyse. Antall informanter er derfor en omdiskutert problemstilling, men det er vanlig å vurdere størrelsen på utvalget i forhold til et «metningspunkt» (ibid.). Det vil si at man vurderer utvalgets størrelse i løpet av forsknings-prosessen, og stopper når man føler at intervjuene ikke gir mer informasjon.

Informantene i studien er strategisk utvalgt med bakgrunn i kvalifikasjoner som er strategisk ut fra problemstillingen (Thagaard, 2013, s. 60). Formålet var å sikre rik informasjon om et tema som er relativt lite undersøkt, basert på et representativt utvalg. Dermed kan jeg på best mulig måte sikre at funnene kan generaliseres. Jeg har spurt nøkkelpersoner innenfor IKT-sikkerhet i helseforetakene om å delta. Et generelt utvalgskriterium var at informantene sitter i ledelsen for IKT-sikkerhet ved foretaket og har kunnskap om IKT-systemer- og sikkerhet. Utvalgsstørrelsen var bestemt på forhånd, da jeg ønsket å intervjue to nøkkelpersoner fra hver helseregion.

De fire helseregionene er grunnsteinen i metoden, da utvalget i undersøkelsen består av åtte personer som er ansvarlige for IKT-arbeidet i sitt helseforetak. Med IKT-arbeid menes her arbeid knyttet til cybersikkerhet, informasjon, styring og ledelse. I utgangspunktet ønsket jeg å

hente informasjon fra øverste ledelse innenfor cybersikkerhet i RHF-ene, samt øverste ledelse ved ett av helseforetakene underlagt RHF-et. Det er imidlertid slik at RHF-ene er ulikt organisert når det gjelder IKT-sikkerhetsledelse, og det er ulike navn på stillingene som omhandler cybersikkerheten. Derfor måtte jeg basere utvalget ut fra dette, noe som skapte noe variasjon blant informantene. Informantene skulle likevel oppfylle følgende kriterier:

- *De sitter i ledelsen for cybersikkerhet eller har ansvar for informasjonssikkerhet*
- *De kan svare på spørsmål knyttet til ledelse og kompetanse innenfor IKT, opplæring, rapportering av hendelser, risiko-og trusselvurderinger og sårbarhetsbildet.*

For å få et utvalg som oppfylte mine kriterier tok jeg kontakt med RHF-ene, der samtlige henviste meg videre til relevante personer hos deres IKT-leverandør. IKT-leverandørene har ansvar for sikkerhet og drift av IKT-systemene til helseforetakene, samt opplæring og bevisstgjøring av ansatte. Noen av IKT-leverandørene er i dag etablert som helseforetak under RHF-ene, mens andre ikke er det (se kapittel 2.2.1). Av den grunn valgte jeg å skille utvalget mellom tilhørende helseregion, fremfor tilhørende RHF. Utvalget mitt består av fagpersoner eller sikkerhetsledelse ved RHF-enes IKT-leverandør. Unntaket er IKT-leverandøren til Helse Nord RHF, da sikkerhetssjefen ikke hadde mulighet til å stille til intervju og henviste meg videre til Helse Nord RHFs informasjonssikkerhetsansvarlig. Videre består utvalget av sikkerhetsledelsen ved ett av helseforetakene underlagt RHF-ene. Jeg mener utvalget er representativt og kan gi meg fyldig informasjon. Her er nærmere beskrivelse av utvalget[3]:

REGION SØR-ØST

Sykehuspartner HF ble i 2015 etablert som et eget helseforetak i Helse Sør-Øst RHF. Sykehuspartner har rundt 1.400 ansatte, noe som gjør virksomheten til en av Nordens største virksomheter innen fellestjenester til sykehussektoren. Jeg har intervjuet Christian Jacobsen, som er informasjonssikkerhetsleder ved Sykehuspartner HF.

Sunnaas Sykehus HF er Norges største spesialsykehus innen fysikalsk medisin og rehabilitering, og ett av elleve helseforetak underlagt Helse Sør-Øst RHF. Sunnaas sykehus er et av de minste helseforetakene i Helse Sør-Øst med ca. 759 ansatte. Jeg har intervjuet Sissel Ertenstein, som er personvernombud og informasjonssikkerhetsleder ved Sunnaas Sykehus HF. Hun sitter i beredskapsutvalget og i kriseledelsen ved Sunnaas sykehus, og har fagansvar for både informasjonssikkerhet og personvern. Hun har det organisatoriske og styrende ansvaret for sikkerheten ved Sunnaas, mens Sykehuspartner har det operative sikkerhetsansvaret.

[3] Informasjonen om informantene og virksomhetene fremgår fra intervjuene og virksomhetenes nettsider.

REGION VEST

Helse Vest IKT AS ble etablert som et aksjeselskap i 2004 og er 100% eid av det regionale helseforetaket Helse Vest RHF. Helse Vest IKT har rundt 560 ansatte fordelt på 10 kontorer, hvorav fire personer jobber med informasjonssikkerhet på fulltid. Jeg har intervjuet Lars Erik Baugstø-Hartvigsen, IKT-sikkerhetsleder i Helse Vest IKT.

Helse Bergen HF (Haukeland Universitetssykehus) har ca. 12.000 ansatte og er det største blant de lokale helseforetakene som eies av Helse Vest RHF. Helse Bergen HF behandler nesten 600.000 pasienter hvert år, og består av 20 enheter som driver pasientbehandling og åtte enheter med støttefunksjoner og andre funksjoner. Jeg har intervjuet Kenneth Oppedal, IKT-sikkerhetsleder i Helse Bergen HF.

REGION MIDT-NORGE

Helse Midt-Norge IT (Hemit) er Helse Midt-Norges IKT-enhet, og er organisert som en egen avdeling i Helse Midt-Norge RHF. Hemit har ca. 336 ansatte. Jeg har intervjuet informasjons-sikkerhetsrådgiver Åsmund Ahlmann Nyre, som også har fagansvar innenfor informasjons-sikkerhet i IT-divisjonen i Hemit.

St. Olavs Hospital HF (Universitetssykehuset i Trondheim) er en sammenslutning av alle offentlige sykehus i Sør-Trøndelag, og er i dag det største helseforetaket i Helse Midt-Norge RHF. Med 10.483 ansatte er St. Olavs Hospital også et av Norges største helseforetak. Jeg har intervjuet Erlend Vandvik, beredskapssjef ved St. Olavs Hospital. Han er også sikkerhetsleder ved helseforetakets sikkerhetsorganisasjon.

REGION NORD

Helse Nord RHF ble stiftet i 2002 og har ansvar for den offentlige spesialisthelsetjenesten i Nord-Norge og på Svalbard. Helse Nord RHF eier seks helseforetak, bl.a. Helse Nord IKT, som ble etablert som et helseforetak i 2017. Helse Nord RHF har i dag over 19.000 ansatte i foretaksgruppen. Jeg har intervjuet Ida-Kristin Martinussen, informasjonssikkerhetsleder i Helse Nord RHF. Hennes oppgaver er informasjonssikkerhet og personvern i Helse Nord RHF. Denne stillingen var nyopprettet i 2016, og er ikke en stilling som er etablert hos alle RHF-ene.

Universitetssykehuset Nord-Norge HF (UNN) er et universitetssykehus som eies av Helse Nord RHF. Sykehuset har 6.300 medarbeidere og er et av landsdelens største arbeidsplasser. Jeg har intervjuet Per Norleif Bruvold, som er sikkerhetssjef i UNN.

4.3.2 FORBEREDELSE OG GJENNOMFØRING AV INTERVJUENE

På forhånd utformet jeg intervjuguider der temaene og spørsmålene var utarbeidet på bakgrunn av problemstillingen, dokumentanalysen og teorien. Intervjuguiden var semi-strukturert og sikret at jeg gikk gjennom spørsmål og temaer som var relevante for min studie, samtidig som det åpnet for å stille spørsmål med utgangspunkt i informantenes beskrivelser og utsagn for videre utdyping og avklaring. Semi-strukturerte intervjuguider er ikke fullstendig styrende, da den åpner for oppfølgingsspørsmål og en mer åpen samtale med informantene.

Da jeg kontaktet informantene på e-post, la jeg til et informasjons- og samtykkeskriv, samt en bekreftelse på studien. I informasjonsskrivet sto det forklart hva studien dreier seg om, hvorfor jeg kontaktet dem og informasjon rundt intervjuets rammer. Jeg understreket tydelig at det var frivillig å delta, og at de kan trekke seg uten begrunnelse. Det ble også vektlagt at alle som deltar kan være anonyme, og at ønske om anonymitet kunne innvilges etter at intervjuene var gjennomført. Deler av informasjonen rundt helseregionens arbeid med cybersikkerhet kan være konfidensiell informasjon om samfunnskritisk infrastruktur, og det kan være begrensninger i hvilken grad informanter åpent kunne gi informasjon om temaet. Ingen ønsker anonymitet.

Intervjuene ble gjennomført i februar-mars. Det sikrer at svarene fra informantene er aktuelle opp mot publiseringen av studien, samtidig som jeg fikk rom for analysearbeidet. Flere trussel-vurderinger kommer i løpet av årets første måneder, og 1. januar 2019 ble ny sikkerhetslov iverksatt, noe som er interessant og aktuelt å diskutere med informantene. Grunnet manglende ressurser ble intervjuene gjennomført over Skype. Dette skal ikke ha påvirket resultatet eller respondentenes åpenhet, ettersom intervjuenes tema ikke er sensitivt. Intervjuene tok ca. 1 ½ time. Jeg tok opptak av samtalen etter samtykke fra informantene, men brukte ekstern opptaker for å sikre meg mot hacking. Alle intervjuene ble transkribert i sin helhet i ettertid.

Jeg gjennomførte gruppeintervjuer bestående av to informanter. Gruppen var satt sammen av de to informantene som tilhører samme helseregion. Det er hovedsakelig to grunner til at jeg valgte å gjøre det på den måten. Den første årsaken var rett og slett for å spare tid. Den andre årsaken er derimot at gruppeintervjuer er et nyttig verktøy når man skal få innsikt i holdninger og meninger hos personer innenfor det feltet man skal studere (Thagaard, 2013, s. 99). Ved å intervjue to personer som sitter i IKT-ledelsen, ved hver sin virksomhet underlagt samme helseregion, kunne jeg på samme tid undersøke om de hadde ulike tanker knyttet til temaet. Samtidig kunne informantene gi respons til hverandres utsagn, eller legge til noe, og ulike holdninger ble synliggjort. For selve intervjuets sin del skapte det også en bedre flyt i samtalen.

4.4 STUDIENS KVALITET

Til nå har jeg redegjort for mine fremgangsmåter knyttet til dokumentene, informantene og metodene jeg har brukt. Jeg har forsøkt å ha et ærlig og kritisk blikk på forskningsprosessen for å ivareta studiens kvalitet underveis, men det kan likevel være punkter som er mangelfulle. Derfor skal jeg nå å belyse studiens kvalitet i et helhetlig perspektiv. Det vil si at jeg skal gå gjennom svakheter ved metoden, men også studiens reliabilitet, validitet og generalisering.

Troverdighet i vurderingen av forskning er vesentlig, og begrepene *reliabilitet*, *validitet* og *generalisering* har blitt sentrale (Thagaard, 2013, s. 202). Reliabilitet viser til hvorvidt en som anvender de samme metodene ville kommet frem til samme resultat. Validitet dreier seg om man måler det man vil måle. Generalisering handler om funnene har en mer generell gyldighet og kan gjelde flere enn de som er undersøkt (Jacobsen, 2015; Thagaard, 2013). Disse begrepene er midlertid mindre egnet i kvalitativ forskning fordi det ikke måler fenomener eller resultater i tall. Kvalitative studier er fortolkende. Derfor foretrekker kvalitative forskere å bruke begrepene troverdighet, gyldighet og overførbarhet (Thagaard, 2013). Troverdighet går på om forskningen er utført på en tillitvekkende måte. Gyldighet knyttes til kvaliteten i tolkninger som gjøres, og om prosjektet kan støttes av andre undersøkelser. Overførbarhet dreier seg om resultatene fra undersøkelsen kan gjelde i andre situasjoner. Jeg velger å bruke disse begrepene når jeg vurderer forskningens kvalitet. Først skal jeg drøfte svakheter og styrker ved metoden.

4.4.1 STYRKER OG SVAKHETER VED VALGT METODE

I forskning vil man alltid finne svakheter i metoden eller faktorer, perspektiver og områder som ikke er inkludert og som påvirker påliteligheten eller gyldigheten. Kvalitetskravet i kvalitative undesøkelser er knyttet til forskeren evne til å reflektere over samspillet mellom forskningen og resultatene (Jacobsen, 2015, s. 246).

På forhånd hadde jeg utarbeidet en omfattende intervjuguide med flere temaer for å få et nyansert og detaljert bilde av helseforetakenes arbeid med cybertrusler og cybersikkertet, noe som gjorde at jeg av tidsmessige årsaker var nødt til å gjøre et utvalg. På grunn av oppgavens omfang har det ikke vært mulig å få snakket med mer enn et visst antall mennesker i forbindelse med intervjudata. Jeg måtte derfor avgrense utvalget, men samtidig sørge for at funnene er troverdige og generaliserbare. Totalt har jeg intervjuet åtte personer, hvor alle jobber i ledelsen innen informasjonssikkerhet i helseforetakene. Jeg har intervjuet to personer som tilhører samme RHF. Jeg mener imidlertid at to nøkkelpersoner fra hvert RHF har gitt meg et grunnlag

til å få et svar på problemstillingen. En svakhet med utvalget er at det er variasjon i utvalget. Jeg skulle helst utelukkende hatt et intervju med personer i nøyaktig samme rolle, men ulik organisering gjorde at dette ikke var mulig. Samtidig kunne jeg fått et bredere og mer nyansert resultat dersom jeg intervjuet representanter fra HOD, som har det overordnede ansvaret for IKT-sikkerhet i helsesektoren. Jeg ser også at det kunne vært interessant å intervjue helsepersonell for å få deres syn på cybersikkerhet ettersom jeg går inn på sikkerhetskultur og IKT-kompetanse blant ansatte. Likevel er det de organisatoriske forutsetningene jeg undersøker, og utvalget må derfor tilpasses nettopp dette.

Jeg stiller et stort spørsmål, og det kan være vanskelig å få et nyansert svar basert på intervjuer med kun åtte personer som jobber med cybersikkerhet i helseforetakene. Intervjuene er basert på semistrukturerte, åpne spørsmål, noe som gir informantene mulighet til å tilføye informasjon. Under datainnsamlingen har jeg dermed fått informasjon jeg kanskje ikke ville fått tilgang til ellers. Det er likevel viktig å ha i bakhodet at informantenes synspunkter kan være subjektive, og representerer ikke nødvendigvis virksomheten eller helsesektoren.. De har naturlig et annet syn på sikkerhet enn andre medarbeidere i sektoren, og det er derfor grunn til tro at de har et annet fokus og ønske om andre prioriteringer. Det er dessuten viktig å ha i bakhode at de kan han ønske om å forsvare de valg som er gjort i helseforetaket når det kommer til sikring av systemer og informasjonssikkerhet, og enkelte temaer kan være konfidensielle. Derfor har jeg brukt relevante rapporter og dokumenter gjennom hele prosessen for å få et objektivt bilde.

4.4.2 PÅLITELIGHET

Reliabilitet er knyttet til spørsmålet om en kritisk vurdering av prosjektet gir inntrykk av at forskningen er utført på en tillitvekkende måte (Thagaard, 2013, s. 201). Reliabilitet handler altså om forskningens troverdighet. I samfunnsvitenskapelig forskning, der det er mennesker som forholder seg til hverandre, må man argumentere for reliabilitet ved å argumentere for hvordan dataene er blitt trukket i løpet av forskningsprosessen (ibid., s. 202). De som undersøkes kan bli påvirket av undersøkeren, og undersøkeren kan påvirkes av relasjonene som oppstår. I tillegg kan slurv i nedtegning og analyse av data true troverdigheten (Jacobsen, 2015, s. 241 og 245). Man må derfor være konkret og spesifikk i rapporteringen av undersøkelsesopplegget, datainnsamling og analysen, og anerkjenne at dette faktisk kan påvirke resultatet. Seale (1999, s, 140 i Thagaard, 2013, s. 202) kaller dette *intern reliabilitet*, og knytter det til grad av samsvar i konstruksjon av data mellom forskere som arbeider innenfor samme tema.

Reliabiliteten styrkes ved å gjøre forskningsprosessen «gjennomsiktig», noe som innebærer å gi en detaljert beskrivelse av forskningsstrategi og analysemetode (ibid.). I metodekapittelet har jeg synliggjort fremgangsmåten min ved å beskrive og begrunnet hvilke valg jeg har gjort. Påliteligheten ivaretas ved å legge frem dokumentasjon av data, metoder og avgjørelser som er tatt. En del av prosessen har gått ut på samtaler og drøfting av metode og datamaterialet som samles inn, som er sentralt for å bekrefte samsvar mellom problemstilling og materialet. Jeg har diskutert framgangsmåte og materiale med medstudenter, en tidligere masterstudent og veileder. Forskningsresultatet får økt pålitelighet man vet hva jeg har tenkt gjennom prosessen.

I denne studien har jeg benyttet dokumentstudier og intervju. Store deler av empirien er altså innhentet, noe som fører til enklte problemstillinger. For det første var intervjumetoden semi-strukturert, noe som gjør at det dukker opp oppfølgingsspørsmål basert på det informantene forteller. Til tross for intervjuguiden kan det dermed komme frem informasjon fra enkelte informanter som ikke kommer frem fra andre. Likevel er en intervjuguide med på å øke reliabiliteten ved at intervjuene blir tilnærmet like. Videre kan informantene ha ulikt forhold til cybersikkerhet, og meningene som fremkommer i intervjuet er i stor grad subjektive. Jeg har vært nøye med å understreke hvilke meninger som er subjektive. Samtidig har jeg også brukt dokumenter som styrker reliabiliteten da de fremstår som objektive.

Videre vil jeg argumentere for studiens reliabilitet ved å reflektere over datainnsamlingen, og hvordan relasjonen med deltakerne kan influere informasjonen. Under intervjuene opplevde jeg åpenhet fra deltakerne, selv om noe informasjon er gradert og forståelig nok noe informantene ikke kan gå i dybden på. Deler av informasjonen kan derfor regnes som noe overfladisk, men informantenes erfaringer og synspunkt rundt rutiner knyttet til cybersikkerhet, samt interaksjon med ledelse og ansatte, var preget av åpenhet. På forhånd hadde jeg gjort meg innforstått med hvordan cybersikkerhet er forankret i helsesektoren og hvordan dette organiseres, noe som gjorde at jeg hadde kunnskap på feltet og dermed kunne diskutere temaet med deltakerne.

Under selve intervjusituasjonen forsøkte jeg å skape tillit til deltakerne ved å være åpen, samtidig som jeg hadde et kritisk blikk. Jeg opplevde ikke at min rolle som forsker og intervjuer ble påvirket av relasjonen med deltakerne, og dette skal ikke ha påvirket relasjonen for dataen jeg fikk. Likevel er det vanskelig å vite hvordan jeg nøyaktig har påvirket informantene. Nøytralitet er utfordrende i fortolkende oppgaver, noe jeg har reflektert over og problematisert. Jeg har vært nøye med å gjøre rede for hva som er referat fra intervjusamtaler og dokumenter, og mener at jeg håndterte balansen på en tilfredsstillende måte.

4.4.3 GYLDIGHET

Validitet knyttes til tolkning av data og viser til forskningens gyldighet (Thagaard, 2013, s. 204). Validiteten kan vurderes ut fra om tolkningene og resultatet man kommer frem til er gyldige i forhold til den virkeligheten som er studert. Seale (1999, s. 38-40 i Thagaard, 2013, s. 205) og Jacobsen (2015) skiller mellom *intern validitet* og *ekstern validitet*. Seale knytter intern validitet til hvordan årsakssammenhengen støttes innenfor en studie, og Jacobsen (ibid., s. 228) knytter det til hvorvidt resultatene regnes som riktige.

En styrke for studiens interne validitet (og pålitlighet) er at jeg har brukt metodetriangulering i form av dokumentanalyse og intervju, der jeg har vært kritisk i utvalget. Jeg har intervjuet informanter innen IKT-sikkerhetsledelse som har kompetanse innen IKT-sikkerhet og jobber fulltid med IKT-sikkerhet i sin virksomhet. Samtidig har jeg med et kritisk blikk sett på ulike offentlige dokumenter, som alle kan regnes som legitime. Informasjonen jeg har fått kan derfor med stor sikkerhet regnes som gyldig og pålitelige. Det er imidlertid viktig å påpeke at det kun er mine tolkninger som ligger til grunn i tolkningen av informasjonen. Jeg har forsøkt å begrense denne svakheten gjennom nøye research og diskusjon med veileder.

Ekstern validitet knyttes til hvordan forståelsen utvikles innenfor en studie også kan være gyldig i andre sammenhenger (ibid.). Begrepet overførbarhet brukes i samsvar med denne forståelsen, og dreier seg om hvorvidt studien kan være gyldig andre sammenhenger. Helsesektoren er organisert med ulike styringsnivåer, noe som gir føringer for organisering og styring av RHF-ene. HOD styrer RHF-ene gjennom lover, vedtekter, foretaksmøter og bestillerdokument. RHF-ene eier og styrer de lokale helseforetakene. Styringsformen gjør at cybersikkerhet i helse-sektoren er forankret på relativ lik måte gjennom styringssystemer. Ledelsen ved RHF-ene og de lokale helseforetakene har god informasjonsflyt med sine ansatte og hverandre, gjennom møter i stab, eget intranett, kurs og oppsøkende virksomhet etc. Det vil si at det ligger betydelig grunn til å tro at informantenes synspunkter om ledelsens og ansattes fokus på cybersikkerhet, erfaringer og lærdom etter dataangrepet mot Helse Sør-Øst, kan overføres til å gjelde hele helsesektoren. Jeg har imidlertid intervjuet personer som jobber med informasjonssikkerhet til daglig, og som har spesialkompetanse på dette feltet. Derfor er det både naturlig og sannsynlig at deres holdninger til cybersikkerhet, og hvordan dette i større grad bør inngå i den daglige driften, kan variere fra toppledelse og ansatte. Jeg har likevel fokusert nettopp på IKT-ledelse, og jeg mener derfor at funnene fra denne studien kan overføres til å gjelde andre situasjoner, men også andre sektorer som avhenger av IKT-systemer.

KAPITTEL 5: PRESENTASJON AV EMPIRI

I dette kapittelet presenteres funn fra datainnsamlingen. Kvalitative dybdeintervjuer løfter frem informantenes holdninger og synspunkter, og danner et fyldigere innblikk og sammenlignings-grunnlag. Dette gjengis ved å direkte sitater, merket i kursiv. Funnene fra dokumentanalysene supplerer informantenes svar og setter det inn i kontekst. Alt som presenteres i dette kapittelet er basert på empiri, og er derfor ikke egen drøfting eller egne synspunkter.

For å gi en systematisk og ryddig presentasjon har jeg valgt å presentere datamaterialet gjennom en kategorisk fremstilling, basert på teamene fra intervjuguiden. Kategoriene er utarbeidet for å gi en rik og dyptgående forståelse av avhandlingens tema og problemstilling: *Hvor forberedt er norske helseforetak på cybertruslene?* Kjernekategorien er «cybersikkerhet ved norske helseforetak», som vil si at dette temaet hele tiden er sentralt i drøftingen.

<table>
<tr><td colspan="6">Kjernekategori: «Cybersikkerhet i norske helseforetak»</td></tr>
<tr><td>Hovedkategorier</td><td>Digitalisering</td><td>Dataangrep</td><td>Sikkerhetskultur</td><td>Digital risiko</td></tr>
<tr><td rowspan="4">Underkategorier</td><td>Avhengighet</td><td>Sikkerhetstiltak</td><td>Dagens sikkerhetskultur</td><td>Risikovurdering</td></tr>
<tr><td rowspan="3">Fremtidens digitalisering</td><td>Læringspunkter</td><td>Styringssystem</td><td>Trusselbildet</td></tr>
<tr><td rowspan="2">Fremtidig sikkerhet</td><td>Ledelsens fokus</td><td rowspan="2">Sårbarheter</td></tr>
<tr><td>Bevisstgjøring/opplæring</td></tr>
</table>

5.1 DIGITALISERING

Digitaliseringen skaper nye løsninger, men også avhengigheter og sårbarheter som går på tvers av sektorer, ansvarsområder og landegrenser. Ifølge Meld. St. 10 (2016-2017, s. 6) kan ingen sektorer kontrollere sine digitale sårbarheter alene. Helsesektorens får stadig flere digitale sårbarheter. RHF-ene bruker flere tusen kliniske og administrative digitale systemer som de er avhengige av i daglig drift. Det er mest kritisk dersom kliniske systemer bortfaller, som bl.a. omfatter elektroniske pasientjournaler (epj) og elektroniske legemiddelsløyfer. Epj blir trukket frem av informantene som det viktigste systemet. Uten dette vil sykehusene få store utfordringer med å drifte sykehuset og yte god helsehjelp, selv med gode manuelle rutiner. Samtidig ser man også at utfordringer rundt informasjonssikkerhet og personvern øker med digitaliseringen. Informasjonssikkerhet er en forutsetning for digitalisering (Normen, 2018, s. 4). I Meld. St. 10 (ibid., s. 132) kommer det frem at digitaliseringen har gjort oss fremmedgjort når det gjelder sikkerhet, da vi ikke lenger har den samme oversikten over sårbarhetsbildet. Effekten av denne fremmedheten er ikke unik for Norge og kan beskrives som en «digital sorgløshet» (ibid.).

5.1.1 AVHENGIGHET TIL SYSTEMER

Region Sør-Øst:

Helse Sør-Øst har ca. 80.000 medarbeidere som konsumerer rundt 60.000 arbeidsplater. De bruker ca. 2.500 applikasjoner, understøtt av ca. 10.000 servere. Informantene påpeker at helseforetakenes digitalisering av arbeidsprosesser, som tidligere var manuelle, gir nye og flere digitale sårbarheter. Et eksempel er innføringen av elektronisk kurve- og medikasjonsløsning. Løsningen gir behandlere en samlet oversikt over observasjoner og målinger for enkeltpersoner, samt mulighet for å etablere en lukket legemiddelsløyfe ved hjelp av IKT. Dersom integriteten på dette systemet ryker, kan pasienten få feilmedisinering som kan være alvorlig i begge ender. Nasjonal e-helsestrategi 2017-2022 trekker fram at lukket legemiddelsløyfe setter store krav til integrasjon med IKT-systemer (Direktoratet for e-helse, 2017b, s. 10).

> *«Det betyr at pasientbehandlingen har digitale sårbarheter som man ikke hadde for bare noen få år siden.»* (Jacobsen)

DIPS trekkes frem som den viktigste kliniske applikasjonen i Helse Sør-Øst. DIPS er det største pasientjournalsystemet i Norge, og brukes av Helse Sør-Øst, Helse Nord og Helse Vest. I Helse Sør-Øst logger ca. 20.000 personer inn på DIPS hver dag, fordelt på ulike installasjoner. For eksempel har Sunnaas sykehus sin en egen DIPS-versjon. Sunnaas har imidlertid få akutte hendelser og liten grad av medisinsk behandling, og er derfor i mindre avhengig av digitale systemer. Sunnaas hadde likevel ikke klart seg lenge uten DIPS.

Telekom, nettverk og infrastruktur står tungt i beredskapsperspektiv. Tilbakemeldingen fra Regjeringens digitale sårbarhetsutvalg var at telekom er viktig for sykehus med akuttmottak fordi de er avhengig av fungerende varslings- og pasientovervåkningssystemer. Telekom vil ikke fungere uten fungerende infrastruktur. Nettverk er derfor det viktigste enkeltsystemet for at Sykehuspartner skal kunne levere DIPS, telekom og andre tjenester. Domenekontroll, som monterer det meste av autentisering og tilgangsstyring, er et annet kritisk system.

Region Vest:

Hele Helse Vest konsumerer ca. 1.400 applikasjoner. Informantene omtaler avhengigheten av digitale systemer som høy og voksende. Informantene påpeker likevel at alle pasienter innenfor den akuttmedisinske tjenesten vil få behandling selv om de kommer til et sykehus der alle IKT-systemene har gått ned. Det er derimot gitt at strømnettet ikke har falt ned, da strømnettet regnes som den viktigste faktoren for å drifte sykehuset. Medisinsk teknisk utstyr (MTU) henter ofte informasjon gjennom IKT-systemer, men MTU vil likevel fungere uavhengig av IKT – så lenge de har tilgang til strøm.

Ingen pasienter blir avvist dersom det er en akutt hendelse. Akutte hendelser blir prioritert, men det blir utfordrende å drive pasientbehandling og sykehus uten IKT. Informantene mener likevel at IKT-bortfall sannsynligvis ikke vil føre til dødsfall, men at det blir utfordrende å få tilgang til opplysninger og kritisk informasjon. Risikoen ved bortfall av IKT er likevel høyt prioritert.

> *«Det eskalerer fort og blir fort alvorlig, spesielt når det gjelder planlagte operasjoner.»* (Baugstø-Hartvigsen)

Region Midt-Norge:

Hemit har ca. 1.400 ulike IT-systemer, som driftes for kundene, i tillegg til moduler, operative systemer og tjenester. AMK-sentralen og nettverket blir trukket frem som kritiske systemer, og de er oppført på høyeste nivå i regionens SLA (Service Level Agreement). En SLA bestemmer hva som er akseptable kvalitetsnivåer på systemene. Helse Midt-Norges SLA har fire nivåer, der nivå 1 og 2 er de mest brukte nivåene. Det vil si at det er høyt oppetidskrav til de fleste systemer og at mange av systemene er oppført på samme SLA-nivå. Nyre mener derfor at regionen har lite fokus på hva nivåene betyr. Helseforetakene gjennomfører ulike vurderinger som setter oppetidskrav til stabilitet og driftssikkerhet. Nyre hevder regionen har et forbedringspotensial når det gjelder å gjennomføre en systematisk gjennomgang av SLA-en.

> *«Forutsetningen er at det skal virke, uten å prioritere hvilket nivå det må virke på.»* (Nyre)

Nyre mener at helseforetakene i større grad bør gjennomføre en Business Impact Analysis (BIA), altså konsekvensanalyse, på sine IT-systemer. En BIA brukes for å kartlegge hvilke systemer man kan klare seg uten, og hva man er absolutt avhengig av.

Region Nord:

Informantene hevder avhengigheten av systemene vil vokse raskere enn samfunnets evne til å sikre dem, og at myndighetene må finne en løsning for å møte denne problemstillingen. Utdanning og økt kompetanse blir trukket frem som én løsning. Ny sikkerhetslov fra 2019 blir trukket frem som en annen, da den er har et bredere virkeområdet og der ansvaret for helseforetakene er utvidet til å omfatte objektsikring og IKT-infrastruktur.

> «*I sikkerhetsloven er det spørsmål om IKT-systemene ved helsesektoren skal være komme under sikkerhetsloven. Men det arbeidet er ikke ferdigstilt ennå.»* (Martinussen)

Regionens beredskapsplaner for bortfall av IKT blir trukket frem som et essensielt virkemiddel for å møte sykehusenes avhengighet av IKT. Spørsmålet dreier seg om hvor lenge systemene eventuelt faller bort, da de er svært avhengig av IKT-systemer for en normal og effektiv drift.

5.1.2 FREMTIDENS DIGITALISERING

Digitalisering har endret risikobildet til de fleste virksomheter. Likevel er ikke ytterligere digitalisering et valg. Det er en forutsetning for et moderne samfunn (St. Meld. 10 (2016-2017), s. 59). For å sikre effektivitet ved økt digitalisering må IKT-løsningene være tilstrekkelig sikre og pålitelige (ibid.). God cybersikkerhet er nødvendig for å oppnå den tilliten. I tillegg må man ha tilstrekkelig nasjonal evne til å avdekke og håndtere digitale angrep (ibid.). Direktoratet for e-helse (2019, s. 21) poengterer at digitalisering i helse- og omsorgssektoren forutsetter at personvern og informasjonssikkerhet ivareta i alle faser av e-helseløsningenes livsløp.

Region Sør-Øst:

Dagens helsevesen er robust fordi det består av mange hender. Digitaliseringen har satt strøm på papir, og man følger de samme arbeidsprosessene som før, men med digitale tjenester. Men slutten av digitalisering er ikke bare en skjerm. Digitaliseringen erstatter helsepersonell, og vil føre til at det er færre som jobber med pasienter og flere som jobber med støttetjenester. Jacobsen mener digitaliseringen gjør helsesektoren mer spisskompetent på informasjons-sikkerhet, men at man må bli mer effektive for hvordan informasjonsbehandlingen skal foregå.

> *«Det betyr at sykehuset vil ha mindre kapasitet til å operere manuelt.»* (Jacobsen)

For å understreke poenget sitt viser Jacobsen til at spesialisthelsetjenesten i større grad inngår rammeavtaler der tredjeparter (underleverandører) utvikler kliniske applikasjoner som kan erstatte helsepersonell. Dersom en tredjepart slås ut i flere uker må spesialisthelsetjenesten forberede seg på å ta imot et pasienttilfang som egentlig er digitalisert. Jacobsen mener man må ha aktiv vurdering av risiko for hva som skjer dersom tjenestene blir utilgjengelige som en del av kartleggingsarbeidet i digitaliseringen av arbeidsprosesser. Da er det ikke primært snakk om ondsinnede aktører, men diverse andre teknologiske faktorer, som f. eks driftsfeil.

Helsesektoren må være klok når i gjennomføringen av digitaliseringen, og Jacobsen mener at helsesektoren har potensiale. Man er nødt til å digitalisere for å effektivisere. Likevel fører dette en sårbar sektor, og digitale sårbarheter gir konsekvenser for pasientbehandlingen.

Region Vest:

Helse Vest har i dag 30.000-40.000 brukere. En utfordring som trekkes frem, med økt digitalisering av helsevesenet, er at tjenestene skal bygges rundt pasientene, noe som gjør at pasientene slippes stadig lenger inn i helseforetakenes infrastruktur.

> *«Etterhvert skal kanskje helseutstyr og verktøy plasserer ut hos pasienten, og flere vil ha tilgang til medisinsk utstyr hjemme. Det blir en utfordring.»* (Oppedal)

I forlengelse av dette trekkes lange verdikjeder og informasjonskjeder frem som en ytterligere utfordring. Informantene forklarer at dersom systemene og kanalene åpnes, og informasjonen blir tilgjengelig for pasientene, så forlenges den digitale verdi- og informasjonskjeden som skal beskyttes. I dette resonnementet trekker de inn ny sikkerhetslov, som i større grad skal gjelde helsesektoren. De trekker likevel frem at de fremdeles er usikre på hvordan loven egentlig vil påvirke dem da de foreløpig ikke har fått en endelig avklaring.

Region Midt-Norge:

En betydelig utfordring som føler med digitaliseringen er økt kompleksitet i alle systemene som benyttes i Helse Midt-Norge. Hemits utfordring er vil være å sikre alle systemene.

> *«Å holde alle tjenester oppdatert, følge med på eventuelle sårbarheter, og sikre at alt er konfigurert riktig etterhvert som de utvikler seg, er ikke så lett.»* (Nyre)

Informantene trekker frem at økt digitalisering i helsesektoren må satse på økt IKT- kompetanse, i tillegg til effektivisering av drift. Det vil si at informasjonssikkerheten må tilpasses jobben til hver enkelt ansatt. Dette trekkes frem som en betydelig utfordring, ettersom kompetansen til ansatte ved helseforetakene er ulik. Det vil si at de har behov for ulike opplegg for informasjons-sikkerhet. Kompetansen må strekke seg utover å gjenkjenne phising-kampanjer, og Nyre trekker frem at utvidede opplæringsopplegg må etableres i de ulike avdelingene.

Region Nord:

Informantene trekker frem to utfordringer ved den fremtidige økende digitaliseringen av helsesektoren. Den første utfordringer er at økt digital samhandling mellom helsenivåene vil presse seg frem. Det andre de peker på er økt angrepsflate i forbindelse med økt bruk av digitale systemer og trådløse enheter i sykehusene. Sykehus skal ta i bruk den økte velferdsteknologien, og i helsesektoren dreier dette seg om MTU. Systemene vil i stor grad lagre mer informasjon og være tilkoblet nett, noe som gjør angrepsflaten større.

> *«Noen av systemene vil vi ikke ha full kontroll over, sett fra vår side.»* (Bruvold)

5.2 DATAANGREP

Norge må være forberedt på å bli stilt overfor hybrid krigføring og angrep i det digitale rom (Meld. St. 38. (2017-2018, s. 249)). Det er ikke mulig å garantere 100% oppetid på ekom- eller kraftnett (ibid., s. 250). DSB har laget to konsekvensanalyser for scenarioet «cyberangrep mot ekom-infrastruktur», presentert i *Nasjonalt risikobilde 2014*. Scenarioet beskriver store samfunnsmessige konsekvenser for helsesektoren, bl.a. at liv kan gå tapt (DSB, 2014b, s. 14).

Region Sør-Øst:

Ransomware, e-postsvindel og CEO-fraud har vært svært vanlig i helsesektoren. Informantene forteller at det er en stund siden de har opplevd at slike angrep kommer gjennom sikkerhets-systemene, og de påvirker driften i svært liten grad. Gjengangeren er automatiserte angrep som er opportunistisk i natur, men ikke målrettede opportunistiske. Det betyr at angriperne leter etter en vei inn i systemene for å undersøke hva de eventuelt kan angripe. De gjentagende forsøkene rettet mot Helse Sør-Øst forklares ved at helsesektoren gir fra seg et stort digitalt fotavtrykk som aktører har interesse for å undersøke i leting etter informasjon.

18. januar 2019 var Helse Sør-Øst rammet av nedetid. Da dette kom frem i media ble det registrert en vesentlig økning av DDoS-angrep hos Helse Sør-Øst. Helsesektoren er sårbare for et høyt volum av distribuerte DDoS-angrep, men mindre distribuerte angrep har IT-teamet gode verktøy for å håndtere. Det har vært flere tilfeller av dataangrep i Helse Sør-Øst der formålet til angriperne har vært å stjele nettbankdetaljer. Denne type trusler har regionen i stor grad gode preventive tiltak mot, og det er sjelden det gir utfordringer eller konsekvenser for virksomheten.

> *«Hvis noen kommer forbi sikkerhetslagene våre, er deteksjons- og responsevnen vår mer enn god nok til å hurtig normalisere en slik hendelse.»* (Jacobsen)

Helse Sør-Øst og Sykehuspartner ble derimot rammet av et stort og omfattende dataangrep i januar 2018. Det dreide seg om et avansert, målrettet dataangrep, trolig utøvet at fremmede statlige aktører. Det er ikke kjent hvor lenge angriperne var inne i systemene deres, eller nøyaktig hva de har hentet. Sykehuspartner ble varslet av HelseCERT 8. januar. Varslingen ble verifiserert av Sykehuspartner, som kunne bekrefte kompromittering av en publisert webserver.

> *«Det tok kort tid fra vi ble kjent med angrepet til vi hadde kartlagt det.»* (Jacobsen)

Beredskap og 24/7 innsatsledelse medførte «takedown» 9. januar. Samme kveld ble det kjent at angriperne hadde etablert større tilstedeværelse enn Sykehuspartner først antok. Helse Sør-Øst gikk i full beredskap 13. januar. Hverken før eller etter dette har regionen opplevd angrep som er bekymringsverdige, varslingspliktige eller rapporteringsmateriale. Dataangrepet har i ettertid gitt store konsekvenser, både for fokuset på informasjonssikkerhet, men også enorme økonomiske konsekvenser. Det er ennå ikke regnet ut hvor mye angrepet har kostet.

Region vest:

Helse Vest IKT opplever at cybertrusselen øker. Det er alltid noen som forsøker å bryte gjennom systemene deres, men vanligvis feiler forsøkene. E-postsvindel utsettes de for daglig, men 95% av mistenkelige e-poster kastes. Helse Vest IKT har satt inn flere sikkerhetstiltak, som applikasjonsblokkeringer og brannmurer, noe som har gjort klientplattformen robust.

Denne programvaren er tilgjengelig for alle sluttbrukere, og vil kun kjøre forhåndsgodkjente programmer, noe som betyr at en ukjent programfil fra et virus ikke vil kunne kjøre.

I 2018 var Helse Vest RHF utsatt for flere DDoS-angrep og andre mindre dataangrep, men informantene legger til at de kan ha vært utsatt for dataangrep uten at de har vært klar om det. Det har vært høy grad av e-postsvindel og CEO-fraud, men det gir sjelden store konsekvenser. Årsaken er tilgangsstyring og sikring av systemer som gjør at aktørene sjelden får gjort noe uten lokale rettigheter. Helse Vest IKT varsler internt hvis angrepene er påtrengende eller påfallende mange. Dersom en hendelse er alvorlig nok blir de varslet av HelseCERT.

Det har imidlertid vært for to bemerkelsesverdige og vellykkede angrep de siste årene:

- DDoS-angrep (2015): Helse Bergens nettside ble utsatt for DDoS-angep, som førte til brudd på hovednettsiden. Brukerne opplevde tap av tilgjengelighet til systemet.
- Ransomware-angrep (2016): Helse Vest IKT ble utsatt for et ransomware-angrep. Løsepengeviruset ble håndtert og mislyktes i å nå målet sitt. De berørte tjenestene opplevde tap av tilgang til journaldatabasen.

Disse angrepene hadde små og begrensede operasjonelle konsekvenser for Helse Vest, men et usikkert skadepotensial. Slike situasjoner kan utløse nødsituasjoner, som i tilfellet med ransomware. I nødsituasjoner informeres IKT-ansatte om hendelsen, som skal jobbe frem til problemet er løst. Brukere og kunder blir også informert og oppdatert. Nødsituasjoner er vanlig på sykehus, så foretakene har derfor prosedyrer for å kunne håndtere ulike situasjoner, som f. eks bortfall av IKT. Den største konsekvensen av slike angrep er at tilgjengeligheten av tjenesten faller bort og at helsetjenesten må fungere uten digitale systemer.

I 2018 ble Helse Vest utsatt for den samme trusselaktøren som angrep Helse Sør-Øst, uten at de lyktes med dette så vidt Helse Vest er bekjent. Det er grunn til å tro at angrepet ikke lyktes hos Helse Vest på grunn av etablerte sikkerhetstiltak, noe som viser at tiltak kan ha god verdi.

Region Midt-Norge:

Helse Midt-Norge har ikke vært utsatt for vellykkede dataangrep som har hatt konsekvenser for driften. Det eneste som trekkes frem er at kryptovirus dukker opp med jevne mellomrom, men stadig sjeldnere. Ved slike tilfeller retankes maskinene, og man er klar for videre drift.

Hemit har tidligere blitt varslet av HelseCERT om at det foregikk CEO-fraud i helsevesenet, men ingen av Helse Midt-Norges helseforetak har vært utsatt for dette i det siste. Hemit har

oversikt over alle angrep som rammer datasystemer. Nyre legger imidlertid til at CEO-fraud som foregår i Helse Midt-Norge ikke alltid blir rapportert til Hemit.

> *«Angrep på mennesker kan faktisk skje uten at jeg har full kontroll over det.»* (Nyre)

Region Nord:

Helse Nord ser daglige forsøk på dataangrep. Ransomware og CEO-fraud på e-post ses jevnlig, men de aller fleste forsøkene blir avvist. I enkelte tilfeller der inntrengerne kommer gjennom sikkerhetsmurene, vil det fanges opp av maskinell kontroll.

> *«I andre tilfeller kommer det ut til sluttbrukeren, og da går det på opplæring og bevisstgjøring av brukerne.»* (Bruvold)

Det mest alvorlige dataangrepet Helse Nord RHF har vært utsatt for var da inntrengere krypterte 600.000 filer for noen år tilbake. Inntrengerne krevde løsepenger fra Helse Nord RHF, men backup av filene gjorde at Helse Nord RHF fikk gjenopprettet alt uten å betale løsepengene.

5.2.1 TILTAK OG LÆRINGSPUNKTER

Jeg skal videre presentere hvilke tiltak som ble helseforetakene iverksatte under dataangrepet mot Helse Sør-Øst og Sykehuspartner i januar 2018, samt de viktigste læringspunktene de har tatt med seg videre.

SIKKERHETSTILTAK

Region Sør-Øst:

HOD delegerte oppfølging av beredskapsansvaret til Hdir, som koordinerte det videre arbeidet innen helsesektoren og samarbeidet med andre myndigheter. Helse Sør-Øst RHF koordinerte arbeidet internt i foretaksgruppen med hyppige møter med administrerende direktører og sikkerhetsledere i foretakene. Helseforetakene fulgte egen beredskapsplan, samt sikkerhetstiltak iverksatt av NSM.

Jacobsen trekker frem at regionen hadde et godt operativt samarbeid med HelseCERT, NorCERT og andre relevante miljøer under angrepet. Sykehuspartner besluttet etter en innledende fase med tradisjonell beredskapsledelse å organisere responsen mot angrepet med et lite og beslutningsdyktig kjerneteam. De identifiserte kritiske trusselscenarioer og la planer for respons om det skulle inntreffe. De etablerte to planer:

- *Remediation plan* – tiltak for å redusere risiko fra trusselaktøren.
- *Re-establishment plan* - tiltakene for å bygge opp igjen etter at trusselaktøren er ute.

Enkelte tiltak blir av sikkerhetsmessige årsaker holdt tilbake, da det er tiltak de ønsker å bruke ved en senere anledning. Det kan derfor ikke være kjent for potensielle aktører hva tiltakene er.

Region vest:

Under angrepet gikk Helse Vest gjennom alle publiserte løsninger for å sørge for at de var sikret tilstrekkelig ut mot nettet, da trusselen var ekstern. Det ble etablert flere tekniske overvåkninger av monitorer, samt prosessmonitorering av serverne for å se etter inngangsdører trusselaktørene kunne ha. Helse Vest implementerte flere tiltak i tråd med anbefalinger fra NSM, HelseCERT og Sykehuspartner, samt tiltak inn mot linjer som var åpne mot Sykehuspartner. Helse Vest testet sårbare applikasjoner og applikasjonene trusselaktørene hadde brukt mot Helse Sør-Øst.

Region Midt-Norge:

Under angrepet mot Helse Sør-Øst ble hendelsen og sikkerheten vurdert og observert av sikkerhets- og beredskapssjefene ved helseforetakene i Helse Midt-Norge, i samarbeid med HelseCERT. Vandvik forteller at det ikke var mye de kunne gjøre utover det da de fikk lite informasjon om hendelsen under angrepet. Informasjonen fikk de primært av pressen.

Region Nord:

Da Helse Sør-Øst RHF og Sykehuspartner HF ble utsatt for et dataangrep av statlige aktører i januar 2018 ble det en nasjonal hendelse, og det var Hdir som koordinerte angrepet. Ved slike hendelser orienterer RHF-ene hverandre, slik at de kan sette i gang egne kontroller på om det rammer dem eller ikke. Helse Nord iverksatte dermed anbefalte tiltak.

LÆRINGSPUNKTER

Region Sør-Øst:

Det viktigste Sykehuspartner lærte er at man ikke kan anta at noen sårbarheter er ubetydelige, og viktigheten av å ha kunnskap om egne verdier og digitalt utstyr.

> *«Det kan og vil skje – og det passer aldri å bi angrepet. Derfor må man først og fremst fikse det mest grunnleggende, og her kommer NSMs fire sikkerhetstiltak inn.»* (Jacobsen)

Videre tok Sykehuspartner med seg følgende læringspunkter:

- Deteksjon er nødvendig.
- «Skjerming» av operativ respons er viktig.
- Øv på forhånd.
- Sjekk backup-systemer.
- Gjennomfør trussel-, verdi- og sårbarhetsvurderinger.
- En god sektorCERT i tillegg til god kompetanse og kapabilitet i egen organisasjon.

Læringspunktene ovenfor er delt med de andre regionene og store kommuner, for å gi disse anledning til å identifisere forbedringer hos seg selv. Helsesektoren har god åpenhetskultur, noe som betyr at regionen deler erfaringer og lærdommer fra både positive og negative hendelser.

Region Vest:

Informantene trekker frem læringspunktene til Sykehuspartner og Helse Sør-Øst som nyttige. Vider mener informantene at økt oppmerksomhet fra ledelsen var et sentralt læringspunkt. Angrepet blir omtalt som en stor øyeåpner for hele Helse Vest. Den dagen forsto ledelsen at også helsesektoren er utsatt for denne type trusler og aktører. De beskriver det som før og etter:

> *«Det var den dagen vi virkelig skjønte at også helsesektoren i Norge er et reelt mål for nasjonale aktører.»* (Baugstø-Hartvigsen)

Som en konsekvens har Helse Vest blir mer oppmerksomme og strengere på IKT-sikkerhet. Helse Vest IKT har satt i gang tiltak på ytterligere herding av tjenestene deres, spesielt på innsiden, og tatt bort systemer og tjenester som ikke var godt nok sikret. Ledelsens fokus på IKT-sikkerhet har endret seg betraktelig etter denne hendelsen. Informantene mener derfor at IKT-skandalene har hatt en positiv effekt på ledelsens fokus og arbeid med IKT-sikkerhet.

Region Midt-Norge:

Dataangrepet som rammet Helse Sør-Øst beskrives som en øyeåpner når det gjelder aktuelle aktører og hvilke verdier de er ute etter. Dette gjelder både for ledelsen i Helse Midt-Norge og i de øvrige helseforetakene, samt underansatte.

> *«Jeg tror det er vanskeligere å tenke at vi ikke er et mål lenger, og det er kanskje den største endringen.»* (Nyre)

Angrepet viste at helsesektoren er nødt til å øve og være forberedt på mer enn kun driftsstans. Denne type aktører er ute etter mer enn å lamme systemer, men å være der over tid uten å bli sett og hente ut informasjon.

Informantene mener at PST og NSM sine trusselvurderinger har fått økt relevans for helsesektoren i etterkant. PST har lenge advart mot russiske og kinesiske etterretnings-operasjoner, hvorav HelseCERTs trusselvurdering fra 2016 ikke nevner dette. I den oppdaterte versjonen fra 2018 er imidlertid fremmede stater nevnt som en trusselaktør.

Region Nord:

Helse Nord RHF tok stor lærdom av angrepet mot Helse Sør-Øst, og fokuset på IKT-sikkerheten økte betraktelig. Informantene viser til læringspunktene til Helse Sør-Øst. Læringselementene som passer inn i Helse Nords styring og organisering er tatt inn i regionens styringssystem, slik at de på den måten kan oppdatere rutinene og prosedyrene de allerede har.

> *«Det man ser fra Helse Sør-Øst er jo at deduksjon kanskje vil bli enda viktigere. Det har vært viktig hele tiden, men det får nok høyere fokus fremover.»* (Martinussen)

5.2.2 FREMTIDIG SIKKERHET

Region Sør-Øst:

Helse Sør-Øst RHF har brukt enorme ressurser i forbindelse dataangrepet. I følge Jacobsen regner de fremdeles ut hva angrepet nøyaktig har kostet dem, og legger til at de blant annet har tatt i bruk nye systemer for tilgangsstyring til rundt 200 millioner kroner. Angrepet har hatt mange konsekvenser for virksomheten, og det vil ta lang tid å gå gjennom alle. Blant annet mistet regionen et e-læringssystem. Positive konsekvenser ved angrepet er at regionen som helhet ble mer sikkerhetsbevisste, og at de står sterkere blant de andre regionene.

> *«Vi har fått en region som er bedre til å tenke på verdivurdering. Man er også bedre på trusselvurderinger, men jeg synes det er viktigst å tenke på verdivurdering.»* (Jacobsen)

Helsesektoren har en god beredskapskultur, og ledelsen i Helse Sør-Øst har vært opptatt av å se på resistansen for angrepet. Det betyr at Sykehuspartner har fått større investeringsmidler på informasjonssikkerhetstiltak, og at regionen som helhet har fått mer sikkerhetskompetente ledere. Videre har ledelsen i Helse Sør-Øst og Sykehuspartner et aktivt forhold til risikostyring.

Informantene mener at det er urealistisk å beskytte seg mot et lignende dataangrep som rammet. Den type statlig APT-aktør har store ressurser, høy kompetanse og er verdidrevne. Aktøren er utenfor deres rekkevidde, altså de preventive tiltakene de har for å forhindre støy og volum. Jacobsen tror ikke helseregionene i Norge kan bygge en sikkerhet som holder APT-aktører ute.

> *«Hvis innstillingen som informasjonssikkerhetsleder er å forhindre APT, så har man enten ekstremt god selvtillit eller ikke evne til å forstå hva man jobber mot.»* (Jacobsen)

Han mener helseregionen må jobbe med å oppdage angrep, fremfor å forutse og forhindre det. Det betyr at fokuset må ligge på responsevne og sikkerhetsdeteksjon, noe som ligger til grunn i sikkerhetsstrategien til Helse Sør-Øst. Sykehuspartner har jobbet hardere og mer målrettet med god deteksjon og respons etter angrepet. Dersom et nytt stort angrep rammer dem, håper Jacobsen at de er i stand til å oppdage det raskere enn de gjorde i januar, slik at de kan være raskere på deteksjon, respons og å få inn datagrunnlaget som trengs for å kunne gjøre de beste beslutningene basert på trusselaktøren.

> *«Vi oppdaget angrepet fort og hadde gode verktøy for å samle inn data for å lage et beslutningsgrunnlag. Nå jobber vi med å gjøre det raskere og bedre.»* (Jacobsen)

Region Vest:

Etter angrepet mot Helse Sør-Øst mener informantene at Helse Vest står bedre rustet mot dataangrep, grunnet implementering av flere tiltak og at de selv klarte å stå imot angrepet. Ettersom trusselaktører allerede har forsøkt, og fått til, et angrep i denne skalaen, forventes det

at sektoren kommer til å rammes av flere dataangrep fra store trusselaktører. De fremhever at trusselaktørene ikke lenger er på utsiden, men på innsiden. Spørsmålet om hvorvidt de kan beskytte seg mot trusselaktører og dataangrep avhenger derfor av hvor trusselen kommer fra og på hvilken måte. Informantene tror at Helse Vest, sammen med resten av sektoren og HelseCERT, er bedre rustet til å oppdage og håndtere eksterne trusler i dag.

> *«Et gjensidig APT-angrep tror jeg ikke vi er godt nok rustet for.»* (Baugstø-Hartvigsen)

For at sykehusene i fremtiden skal kunne håndtere og forebygge konsekvenser av dataangrep, hevder informantene at de har behov for mer ressurser, både midler og ansatte, flere systemer for sikkerhet – og bedre organisering. Organiseringen kan bedres uavhengig av ressurser.

> *«Jeg tror vi savner en organisering som er på et nivå som gjør at informasjonsdeling ved angrep er raskere og bedre.»* (Baugstø-Hartvigsen)

Informantene savner bl.a. et formelt apparat eller en formell struktur dersom helseforetakene skulle oppdage noe mistenksomt. I dag benyttes HelseCERT til dette, men informantene hevder at det er en omvei i den generelle informasjonsdelingen. Informantene stiller videre spørsmål rundt læring i etterkant av hendelser, og etterspør bedre organisering når det gjelder debrifing.

<u>*Region Midt-Norge:*</u>

Informantene hevder at sykehusene er relativt godt beskyttet mot dataangrep i dag. Systemene er ikke helt åpne, men det åpne vinduet ved installeringen av patcher kan av tidsmessige årsaker utgjøre en sårbarhet. Hemit har intensivert egen nettverksovervåking, sentralisert logg-overvåkningen og er i ferd med å anskaffe nye verktøy for dette. Nyre mener at dette i større grad gjør det mulig å avdekke mistenksom aktivitet. De har likevel ikke øvd på skarpe hendelser.

Konkret jobber Hemit med leverandørtilgang, spesielt på store uoversiktlige selskaper der tjenestene leveres fra land som er mer ustabile enn Norge. Dette ble et større fokus i Hemit etter Helse Sør-Øst sin skandale med tjenesteutsetting.

Nyre peker på at man kun kan sikre seg mot dataangrep til en viss grad, og at det handler om å kunne håndtere angrep. Han hevder derfor at man trenger bedre og mer integrert risikostyring og hendelseshåndtering, slik at ledelsen forstår risikoen og kan ta gode beslutninger. Dette vil ikke direkte forhindre noen i å komme inn, men kan gjøre det lettere å identifisere tiltak.

> *«Informasjonssikkerhet bør blir en integrert del av hverdagen til alle, men det er på vei opp og fram nå.»* (Nyre)

Vandvik peker på at St. Olavs Hospital vil være i stand til å ivareta pasientene ved et dataangrep som lammer systemene deres, selv om det vil være problematisk. Noen pasientkategorier er mer sårbare, noe som gjør det vanskelig å gi tilfredsstillende helsehjelp ved bortfall av IKT,

strøm og vann. Dette gjelder spesielt pasienter som ligger på overvåkede intensivplasser og som har vært gjennom større operasjoner. Spørsmålet er hvorvidt de vil være i stand til å drifte sykehuset uten internettilkobling, og Vandvik peker på at det er paradoksalt at forskriftskravene for bortfall av strøm er sterkere enn forskriftskravene for bortfall av både IKT og vann, ettersom han anser avhengigheten til vann, strøm og IKT som like stor.

Region Nord:

Hvorvidt Helse Nord kan beskytte seg mot dataangrep kommer an på angrepets art. Helse Nord har tiltak for å avdekke angrep, og tiltak som skal iverksettes dersom hendelser/angrep oppstår for å få organisasjonen raskest mulig tilbake til normal drift. Noen angrep vil de kanskje ikke legge merke til, mens andre angrep kan ha større betydning som gjør at tjenester må reduseres. Informantene peker på Helse Nord at Helse Nord kun har 10% av pasientgrunnlaget av Norges befolkning, og at de derfor har et lavere modenhetsnivå.

> *«Vi har potensiale for forbedringer. Vi har et stort fokus på informasjonssikkerhet, og legger betydelig ressurser i det, men det er et komplisert område.»* (Martinussen)

De hevder at informasjonssikkerhet i helsesektoren er et komplisert område, og at det krever spesialkompetanse som er vanskelig å oppdrive fordi utdanningsinstitusjonene har kommet for sent i gang med denne type opplæring og kompetansetiltak. Det er en betydelig utfordring å ha høy nok kompetanse til å holde seg oppdatert på de truslene som finnes, og informantene hevder at Helse Nord ikke skilles seg ut blant de andre på dette punktet.

Informantene mener at helsesektoren aldri vil kunne sikre seg mot dataangrep, og det er en risiko som alltid vil være der. Konkrete planer i Helse Nord er tilstrekkelig backup av systemer og beredskapsplaner, samt strukturert arbeid med fagfeltene innen beredskap og informasjons-sikkerhet. De hevder at digitaliseringen vil tvinge frem nye og andre typer backup-løsninger.

5.3 SIKKERHETSKULTUR

Målrettede angrep, IoT og sikkerhetshull gjennom velferdsteknologi stiller store krav til både databehandlingsansvarlig og databehandler når det gjelder sikkerhetskultur, risikobevissthet og strategi for digitalisering. (Omerovic & Gjære, 2015, s. 10). Ett av HelseCERTs (2018) tiltak for å redusere risikoen for cyberangrep er nettopp å bygge god sikkerhetskultur, noe som blant annet innebærer opplæring og bevisstgjøring ansatte. Informasjonssikkerhet er en forutsetning for digitaliseringen, noe som betyr at teknologien og behandling av opplysninger kan bli utsatt for tilsiktede og utilsiktede hender. Det digitale risikobildet er komplekst og i stadig endring,

og det kan være krevende å bedømme risiko rett til enhver tid. Derfor påpeker også Normen (2018, s. 4) viktigheten av å bygge en god og robust sikkerhetskultur. Kultur og god ledelse kan imidlertid ikke vedtas. Det er noe som må skapes og videreutvikles. Arbeidet med god kultur og ledelse er et kontinuerlig arbeid som må utvikles over tid (Meld. st. 10 (2016-2017), s. 121).

Hdir hevder at helsesektoren er nødt til å bygge en bedre sikkerhetskultur i arbeidet med å møte det nye trusselbildet (Hdir, 2017, s. 24). God sikkerhetskultur kjennetegnes ved at ansatte er oppmerksomme på problemstillinger knyttet til personvern og informasjonssikkerhet, at de har tilstrekkelig kompetanse om det aktuelle trusselbildet, trusselaktører, teknologi, og at de kjenner sin egen rolle og er klar over virksomhetens styringssystem og rutiner (ibid.). Manglende IKT-kompetanse blant ansatte er et gjennomgående tema i rapporter og trussel-vurderinger. I helse- og omsorgstjenesten er personvernet godt forankret.

«Våre verdier, holdninger, meninger, kunnskaper og handlinger som knyttes til sikkerheten i det digitale rom kan oppsummeres i begrepet *IKT-sikkerhetskultur*» (Meld. st. 10 (2016-2017), s. 70). Vurderingselementer av sikkerhetskultur består av et bredt spekter av temaer (Nieva & Sorra, 2003, s. 18). Instrumentene vurderer ofte verdier, holdninger, bevegelser og normer for organisasjonsmedlemmer, samt oppfatninger av organisatorisk kontekst, som ledelsesmessige prioriteringer, tilstrekkelighet av opplæring og ressurser, eller retningslinjer og prosedyrer. Jeg skal gjennomgå informantenes synspunkt rundt nåværende sikkerhetskultur. Fokuset ligger på ansattes bevissthet og kompetanse, men ettersom ledelsmessige prioriteringer og retningslinjer er en del av den helhetlige sikkerhetskulturen vil også dette inngå i kapittelet.

Region Sør-Øst:

Sikkerhetskulturen og sikkerhetskompetansene til ansatte ved Helse Sør-Øst og Sunnaas Sykehus blir beskrevet som nokså god. Den har blitt bedre, men er varierende. Når det gjelder personvern og den lovpålagte taushetsplikten er de ansatte gode til å forholde seg til dette. Ertenstein legger til at ansatte har blitt mer bevisste på IKT-sikkerhet det siste året. Hun har sett en klar forbedring av sikkerhetsfokuset. Hun opplever samtidig at ansatte ønsker å lære mer.

Informantene påpeker at helsepersonell ikke har forutsetninger til å være kompetente på IKT-sikkerhet, noe som heller ikke er forventet. Sykehuspartner, som en IKT-virksomhet, har et naturlig annet fokus enn helseforetakene når det gjelder informasjonssikkerhet.

En periode opplevde Helse Sør-Øst flere avvik og svært mange ransomware-angrep. Som en konsensus ble det bestemt at det var behov for en betydelig strengere internettpolicy. Av

operative hensyn er Gmail, Facebook og Dropbox sperret i hele regionen. Helse Sør-Øst er strengere på dette enn andre regioner fordi de hadde flere avvik og et sterkt forskningsmiljø.

Med regionens volum av ansatte har ledelsen sett at det ikke hjalp med holdningskampanjer. Helse Sør-Øst har 80.000 ansatte hvorav 4000 er fremmedspråklige, noe som gjør at det ikke finnes ressurser til å sikre at alle har ambisjonsnivå og kompetanse hva det gjelder IKT-Sikkerhet. Sikkerhetskampanjer fra Sykehuspartner blir derfor bygget med tanke på at ansatte ikke har denne kompetansen. Sykehuspartner klarer ikke å nå godt nok ut blant de ansatte for å øke sikkerhetskulturen, og kompenseres derfor med prosesskontroller og tekniske kontroller.

IKT-sikkerhetskompetansen hos Sykehuspartner er forholdvis høy på teknisk side. Sykehuspartner har 1.400 ansatte, noe som gjør at nivået er ulikt og at de på så måte har forbedringspotensial. Jacobsen forteller imidlertid at de fleste er opptatt av operasjonell sikkerhet, og han ser et sterkt operativt sikkerhetsfokus. Sykehuspartners største utfordring handler om prosessuell og organisatorisk sikkerhet, og det å se endringer som en kildre til økt risiko. Utarbeidelse av dokumentasjon er en vedvarende utfordring.

> *«Det er lett for en godt utøvende tekniker å gjøre jobben, men det å huske å oppdatere systemdokumentasjon etter at jobben er gjort er veldig viktig.»* (Jacobsen)

Sikkerhetsfokuset endret seg betraktelig på operativ side etter dataangrepet i januar 2018. Det vil si at oppmerksomheten mot eksterne trusler har økt. Den største risikoen i Helse Sør-Øst er likevel interne avvik, som de har en del av. Avvikene går på dårlig dokumentasjon og at leverandører får tilganger de ikke skulle hatt.

Region Vest:

Ansatte i Helse Vest har ikke god nok kompetanse om IKT-sikkerhet og digital risiko i dag. Oppedal viser til at Intranettet i Helse Bergen har 2000-3000 unike besøk daglig, noe som ikke er dekkende for hele virksomheten. Han vet at flere ansatte ikke leser e-postene sine, og de har en gjennomføring på kun 50% på det obligatoriske e-læringskurset.

Ansatte i Helse Vest har rett oppmerksomhet rettet mot visse digitale trusler, men informantene hevder at kompetansen deres dekker «lettvektinformasjonssikkerhet», som e-postvindel, falske internettsider, falske telefoner og passordsikkerhet. De hevder det er en overflatekompetanse, og at kompetanse om det dyptgående og komplekse trusselbildet er manglende.

Når det gjelder problemstillinger knyttet til personvern stiller informantene seg mindre kritisk til ansatte ved sykehusene. Informantene viser til at den lovpålagte taushetsplikten sitter i

ryggmargen til helsepersonellet, og at de har stort fokus på at helseopplysninger er konfidensielt og skal skjermes og vernes. De hevder helsepersonell ser på dette som et grunnleggende prinsipp for å kunne gi god helsehjelp, fremfor å se på det som et personvern.

> *«Samtidig ser vi at man ikke har nok kompetanse til å forstå at opplysninger er uskyldige nok i én setting. I en større kontekst kan metadata ha en helt annen verdi.»* (Oppedal)

Informantene viderefører resonnementet til sikkerhetssjefenes IKT-hverdag og hevder at helsepersonell ikke har det samme bildet på informasjonssikkerhet når det gjelder å ønske tilgang til ulike systemer. Helsepersonell forstår at pasientinformasjon skal vernes, men ønsker likevel økt tilgang til ulike systemer for å kunne gjøre jobben sin. Med økt tilgjengelighet vil konfidensialiteten forsvinne, mener informantene.

Tilgang til systemer fører oss videre til de regionale prosessene for innføring og forvaltning av systemene i Helse Vest. Informantene hevder at den administrative siden, altså de som skal drive innføring og endring av IKT-systemer, ikke har tilstrekkelig forståelse av personvernet. Informantene mener at personvern som begrep er farlig, og at personvern handler om mer enn personopplysningssikkerhet.

> *«Personvern handler ikke kun om å beskytte informasjon. Det er galt å sette personvern, pasientsikkerhet og tilgjengelighet opp mot hverandre.»* (Baugstø-Hartvigsen)

<u>*Region Midt-Norge:*</u>

IKT-kompetansen i Helse Midt-Norge blir beskrevet som varierende. Nyre forteller at mange ansatte i helsesektoren først og fremst forholder seg til journalsystem eller labsystem, og i liten grad av egen PC. De er derfor i liten grad utsatt for skadevare gjennom e-post.

Vandvik antar at ansatte ved St. Olavs Hospital har lav forståelse for teknisk sikkerhet, men at personvern er relativt godt forankret. Påstanden om lav forståelse for teknisk sikkerhet underbygges av at ansatte ikke kjenner god nok til sykehusets tre strømforsyninger: normalkraft levert fra energiselskapet, reservekraft som er aggregater, samt UPS; avbruddsfri batteri backup.

Med ulik bruk av systemer er det ulik kunnskap og bevissthet om IKT-sikkerhet. I Hemit har de aller fleste et forhold til sikker bruk av PC og informasjonssikkerhet. Hemit er på så måte en mer homogen gruppe, til tross for at de jobber med ulike felt. Arbeidshverdagen er nokså lik, og Nyre mener at forståelsen for sikkerhet sannsynligvis er høyere.

Sikkerhetskulturen i Hemit beskrives som god. Det har blitt økende kultur for å melde om avvik, og å forholde seg til sikkerhetsplanen, driftspolicyer, samt konfigurasjon- og nettverksoppsett med tilhørende prosedyrer og faktaark fra Normen. Ansatte tar i høyere grad kontakt med

ledelsen for å få informasjon om informasjonssikkerhet, for eksempel da GDPR ble innført. Nyre påpeker at noen ansatte har blitt svært bevisste på dataangrep og svindelforsøk på e-post.

Bevisstheten og det å tenke på informasjonssikkerhet har altså økt i alle ledd. Ansatte er i stor grad klar over sikkerhetstiltakene i Hemit, samt hvilke trusler og risiko de står ovenfor ved økende digitalisering. Likevel savner Nyre at de gjentagende oppgavene, som for eksempel risikovurderinger, blir beskrevet mer detaljert og dermed enklere å gjennomføre for flere.

Region Nord:

Helsepersonellet er vant til å forholde seg til den lovpålagte taushetsplikten. Martinussen mener at de ansatte generelt er godt informert om problemstillinger knyttet til IKT-sikkerhet og personvern. Kompetanse om cybersikkerhet er derimot begrenset. Bruvold mener ansatte har nok kompetanse til å forvalte de opplysningene som er innad i sykehuset.

Når det kommer til sikkerhetskulturen i Helse Nord, påpeker informantene at de har noen utfordringer. Det dreier seg blant annet om en utfordrende balansegang når det gjelder eierskapet av pasientjournaler, som har endret seg ettersom pasientene har fått større tilgang og eierskap til egen journal.

> *«Helsepersonellet har en lovfestet plikt til å dokumentere, men man har ikke tatt inn over pasientrettigheten å styre hvem som har tilgang til dine opplysninger.»* (Bruvold)

Informantene forteller at det har skjedd mye dramatisk de siste tre årene, noe som har gjort at sikkerhetskulturen har økt i riktig retning. Helse Nord RHF fikk blant annet MinJournal i 2015. Helse Nord RHF begynte å jobbe med denne løsningen i 2007, og allerede da begynte de prosessen med å bevisstgjøre brukerne om systemet. Samtidig har det skjedd endringer på lovsiden som krever at helseforetakene bevisstgjør ansatte og brukere. Etter at pasienter har fått tilgang til egen journal har bevisstheten rundt informasjonssikkerhet økt kraftig.

5.3.1 BEVISSTGJØRING OG OPPLÆRING

Informantene er enige i at taushetsplikten er godt forankret hos helsepersonell, men kompetanse om digital sikkerhet og god sikkerhetskultur er manglende. RHF-ene har flere tiltak og jobber kontinuerlig med bevisstgjøring og opplæring av sine ansatte gjennom holdningsskapende arbeid og kurs. Alle ansatte skal blant annet gjennomgå et e-læringskurs, som informantene mener er svært nyttig til tross for varierende oppslutning. Mange hendelser inntreffer som følge av manglende opplæring, holdninger og årvåkenhet, noe som gjør at helsesektoren vurderer å styrke bruken av e-læringsprogrammer (Omerovic & Gjære, 2015, s. 14).

Region Sør-Øst:

Det obligatorisk e-læringskurset er det primære tiltaket for å bygge grunnleggende kompetanse om informasjonssikkerhet i Helse Sør-Øst. Kurset har tidligere hatt dårlig oppslutning, men etter aktiv sanksjonering fra Sykehuspartner dette har endret seg. Kurset må bestås, og dersom det ikke gjennomføres kan ansattes rettigheter inndras frem til kurset er bestått.

> *«Hvis man møter opp på jobb uten rettigheter over tid kan du faktisk få en advarsel, eller beskjed om å finne et annet arbeidssted.»* (Jacobsen)

Informasjonssikkerhet er gjennomgående i intranettet til Helse Sør-Øst, og styringssystemet er lett tilgjengelig for alle. Videre blir nyhetsbrevet *Sikkerhetsnytt*, med dagsaktuelle saker, sendt ut hver måned. Sykehuspartner driver med oppsøkende virksomhet i ulike ledergrupper og har etablert Sikkerhetsskolen, et kurs over 13 uker for egne ansatte som vil lære mer om sikkerhet.

> *«Målsettingen er å gjøre de ansatte mer sikkerhetsbevisste og få de til å tenke sikkerhet i alt de gjør.»* (Jacobsen)

Region Vest:

Helse Vest har flere tiltak for å øke ansattes kompetanse og forståelse for IKT-sikkerhet. Det primære er obligatorisk e-læringskurs for alle som ansettes. Helse Bergen har imidlertid en gjennomføring på kun 50%. E-læringskurset skal tas hvert 2-3. år for å holde de ansatte oppdaterte, men informantene stiller seg kritisk til frekvensen fordi IKT-sikkerhet er ferskvare.

> *«Hadde vi derimot hatt nasjonale sikkerhetskampanjer hvert eneste år hadde det kanskje vært tilstrekkelig med kurs hvert 2. eller 3. år.» (Oppedal)*

Helse Vest har en regional IKT-sikkerhetsinstruks for å sikre at ansatte har nok informasjon om personvern, informasjonssikkerhet og trusselbildet. Regionen har sporadiske kampanjer på sikkerhetsområder, f. eks da hele regionen deltok på nasjonal sikkerhetsmåned i 2018. Oppedal påpeker at sikkerhetssjefene skal informere ansatte, men at mengden ansatte er utfordrende. I Helse Bergen er det rundt 13.000 ansatte. I hele Helse Vest RHF er det over 25.000. Sikkerhetssjefene forsøker likevel å nå via intranettet, e-poster og andre opplysningskampanjer. Av og til går de ut til avdelinger og holder foredrag, presentasjoner og annen opplysende virksomhet, men frekvensen er for lav til at det kan trekkes frem som et vesentlig virkemiddel.

Region Midt-Norge:

Hemit har flere tiltak for å øke ansattes kompetanse om cybersikkerhet. Det blir gjennomført interne kurs i Hemit, de har en kompetanseplan for sikkerhet, og alle ansatte skal gjennomføre et grunnkurs i informasjonssikkerhet med varighet på ca. en halv dag. Det er også kurs for både risikovurdering og risikostyring. Nyre jobber med et eget ledelseskurs i informasjonssikkerhet.

Nyre peker på at det er få i Helse Midt-Norge som har informasjonssikkerhet i stillingstittelen. Videre peker han på at kompetansen til ansatte ved helseforetakene er ulik. Det vil si at leger, sykepleiere, forskere og bioingeniører har behov for ulike opplegg for informasjonssikkerhet. Kompetansen må derfor tilpasses hvert arbeidsområde dersom IKT-kompetansen skal dekke områder utover det å kjenne igjen phising-kampanjer og ha sterke passord.

> *«Vi bidrar så langt det lar seg gjøre. Men hvis informasjonssikkerhet skal funke, så må det tilpasses den jobben man gjør.»* (Nyre)

Helseforetakene, inkludert Hemit, har i utgangspunkt ansvar for egen læring. Hemit gjør likevel noen av kursene tilgjengelig for de andre helseforetakene. Helse Midt-Norge har ca. 22.000 ansatte, noe som gjør at Hemit, med to sikkerhetsrådgivere, ikke har mulighet til å gjennomføre sikkerhetskurs for alle. Unntaket er det obligatoriske e-læringskurset. E-læringskurset har tidlige kun vært obligatorisk i Hemit, men det er nå vedtatt at det skal være obligatorisk for hele regionen. Helseforetakenes implementering av det obligatoriske kurset er derimot varierende. I helseforetakene er det avdelingslederen som har ansvar for sin egen enhets kompetanse, og Nyre tror de selv velger om e-læringskurset skal være obligatorisk kompetanse eller ikke.

> *«I henhold til kompetanseplanen må de teknisk sett si at det er obligatorisk. I Hemit er det obligatorisk, og jeg tror det bør repeteres hvert år, eller annet hvert år.»* (Nyre)

<u>*Region Nord:*</u>

Ledelsen ønsker å sikre at ansatte har nok informasjon om det aktuelle trusselbildet i cyberspace. Blant annet publiseres artikler med dagsaktuelle saker på intranettet. Alle ansatte i Helse Nord RHF skal gjennomføre det obligatoriske e-læringskurset, som de startet med for 3 år siden. Ledelsen ønsker nå at kurset skal gjennomføres ved jevne mellomrom, gjerne hvert 3. år eller oftere. Ledelsen og ansatte har god erfaring med kurset, som er en teoretisk gjennomgang som føles opp med praktiske eksempler. Helse Nord RHF følger det opp dersom avdelinger eller helseforetak har lav andel ansatte som har gjennomført kurset.

> *«Vi følger det opp ved å utfordre den enkeltes leder, fordi det er lederens ansvar å se til at de har nødvendig kompetanse.»* (Martinussen)

I tillegg driver Helse Nord med oppsøkende virksomhet ut i avdelingene, som de kaller for «opplæring og bevisstgjøring». Dette tar for seg informasjonssikkerhet og hvordan informasjon forvaltes i Helse Nord, samt diskusjoner rundt aktuelle problemstillinger.

> *«Det siste er kanskje det vi har mest læring ut av. Det er noe de kjenner til hver dag. Så det er en kombinasjon av teori og praksis.»* (Martinussen)

5.3.2 STYRINGSSYSTEM

Offentlige virksomheter er gjennom eforvaltningsforskriften § 15 pålagt å ha internkontroll på informasjonssikkerhetsområdet ((Meld. St. 27. (2015-2016), s. 151). Arbeidet med personvern og informasjonssikkerhet favner styring, gjennomføring og kontroll, og skal dokumenteres i styringssystemet (internkontroll) som dekker personvern og informasjonssikkerhet (Normen, 2018, s. 12). Strengere krav til styring i helsesektoren førte til iverksettelsen av forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten (2017). Forskriften ligger til grunn for helseforetakenes felles regionale styringssystemer, som beskriver roller, ansvar og beslutningsansvar i virksomhetene, risikostyring, policy og beredskap (Normen, 2018, s. 12.).

Styringssystemet er tett knyttet til ISO-standarder og viser til Normen, der Normen påpeker at informasjonssikkerhet og personvern i størst mulig grad bør inngå som en del av det totale styringssystemet i virksomheten, og at styringssystemet skal etterleve forskriftenes krav om personvern og informasjonssikkerhet (ibid.). Det er virksomhetens øverste ledelse som skal etablere styringssystemet og gjøre det kjent i virksomheten (ibid., s. 13). I 2018 ble styrings-systemet revidert og oppgradert i henhold til GDPR (ibid., s. 9).

Alle informantene trekker frem styringssystemet som et godt verktøy i organiseringen av IKT-sikkerheten ved helseforetakene.

Region Sør-Øst:

Informantene mener eier-og styringsmodellen i Helse Sør-Øst gjør styringssystemet komplisert. Hvert foretak er en selvstendig, juridisk enhet, noe som gjør det vanskelig for eieren å definere risikoaksept på vegne av hvert enkelt foretak. Styringsdokumentet er konsensusutarbeidet, som vil si at nye dokumenter, bestemmelser og endringer må behandles i regionale månedlige møter der alle informasjonssikkerhetslederne deltar. Deltakerne er selvstendig dataansvarlige og blir vurdert på at de har gjort en vurdering selv, og det må derfor være enighet ved endringer eller innføringer. De kan ikke ha avstemminger basert på flertall ved endringer eller innføringer.

> *«Det blir mer arbeid å gjennomføre endringer. Det kan være en krevende prosess, særlig hvis noen av foretakene er negativt innstilt til en endring.»* (Jacobsen)

Informantene trekker likevel frem at styringssystemet bidrar positivt på flere måter. For det første gir det en forutsigbarhet, som beskrives som svært viktig. Det gir forutsigbarhet i tjenesteutvikling og kravspesifikasjon, slik at det også kan brukes mot leverandører og andre virksomheter som sykehusinnkjøp og sykehusbygg.

Dokumentet kan også brukes som et benchmarkingverktøy, altså til sammenligning ut fra visse kriterier eller standardverdier. Jacobsen forteller at man kan vurdere risiko i løsninger opp mot styringssystemet og hva bestemmelsene sier: dersom man har et avvik mellom en tjeneste og det styringssystemet vurderer, kan man lettere vurdere risiko.

Sykehuspartner bygger sikkerheten i fire domener: teknologi, organisasjon, prosess og kultur. Jacobsen forteller at styringssystemet er viktig i teknologiaksen, men at det er mest viktig i kultur- og prosessaksen der de har opplevd noen utfordringer med avvik og lignende. Det som trekkes frem som den viktigste egenskapen er derfor at styringssystemet er et normativt verktøy. Det gir Sykehuspartner anledning til å sanksjonere mot kunder, leverandører og ansatte som ikke forholder seg til sikkerhetsbestemmelsene. I 2018 terminerte Sykehuspartner tre arbeidsforhold der informasjonssikkerhet var en vesentlig del av totalvurderingen.

Region Vest:

Styringssystemer i Helse Vest forvaltes av et felles regionalt IKT-sikkerhetsutvalg, som består av sikkerhetslederne i Helse Vest og ledes av en jurist i Helse Vest RHF. Alle virksomhetene i helsevesenet har et felles styringssystem for informasjonssikkerhet og personvern. I Helse Vest inkluderer dette både helseforetakene, i tillegg til eksterne virksomheter som helseforetakene samarbeider tett med. Med eksterne virksomheter menes private ideelle virksomheter som også får IT-tjenester levert av Helse Vest IKT. Styringssystemet er likt i alle virksomhetene. Det er basert på Normen og gir retningslinjer for regionens sikkerhetsarbeid og en overordnet sikkerhetspolicy som gjelder for hele Helse Vest.

> *«Styringssystemet vårt er brukbart, men ikke komplett. Det må operasjonaliseres i detalj i hver enkelt virksomhet.»* (Baugstø-Hartvigsen)

Region Midt-Norge:

Nyre kritiserer at styringssystemet har manglet tilknytning til virksomheten, og legger til grunn at det ikke har vært tydelig at informasjonssikkerhet og personvern er med på å bidra til å oppnå målene i virksomheten, som er å yte helsehjelp. Nyre peker på at styringssystemet for informasjonssikkerhet er et subsett av virksomhetens styringssystem. For at det skal bli en integrert del av virksomheten kan ikke regionen ha et konkurrerende styringssystem, hevder Nyre. I fjor startet Hemit arbeidet med et regionalt *rammeverk* for informasjonssikkerhet, som bygger videre på styringssystemet. Rammeverket skal utarbeide dokumentene og prosedyrene man trenger, og ta det inn i et eget styringssystem. Nyre mener dagens styringssystem skaper

forvirring fordi ansatte skal forholde seg til et styringssystem, samt prosedyrer og policy i en virksomhet, og at informasjonssikkerhet kommet som noe eget.

> *«Jeg hadde ikke lyst til at vi skulle ha noe eget for informasjonssikkerhet. Vi har jo ikke felles regionalt styringssystem for helsehjelp, mannskapsprioritering eller HR.»* (Nyre)

Nyre hevder at likevel at styringssystemet til bidrar til å integrere informasjonssikkerhet som en del av den generelle virksomhetsstyringen. Det forenkler oppgaver, lager prosedyrer, og sørger for dokumentasjon. Ved å dokumentere oppgaver på en konkret og detaljert måte er det enkelt å henvise til styringssystemet dersom noen har spørsmål om handlinger som har blitt gjort. Nyre kritiserer derimot at fokuset på dokumentasjonen varierer, noe som gjør at det blir personavhengig. Et eksempel han trekker frem er at tjenester som ikke skal brukes slås av ved herding av servere. Når dette ikke er godt nok dokumentert er det vanskelig å svare på hvilke tjenester det gjelder. Videre mener at mye blir dokument på et abstrakt nivå.

> *«Det blir utfordrende når noen spør om noe, når vi lurer på noe eller skal sjekke noe. Da er det personavhengig og man få tak i de som gjorde det.»* (Nyre)

<u>*Region Nord:*</u>

Helse Nord RHF har 24 sikkerhetsområder som skal sikres til enhver tid, og informantene henviser til regionens felles styringssystem for informasjonssikkerhet der det er utarbeidet felles regionale sikkerhetsmål og sikkerhetsstrategier. Regionalt styringssystem for informasjons-sikkerhet og handlingsplan for informasjonssikkerhet er styrende dokumenter i Helse Nord. I tillegg har sikkerhetsansvarlige en egen stillingsinstruks som beskriver deres roller og ansvar. Informantene trekker frem at dokumentene sikrer forutsigbarhet i virksomheten i den forstand at Helse Nord må definere en strategi, regler som skal følges, samt rutiner og prosedyrer innenfor enkelte sikkerhetsområder.

> *«At man har et strukturert dokument man kan gå ut i fra for å bevisstgjøre brukerne gjør det lettere for de som skal drive opplæring og bevisstgjøring av ansatte.»* (Bruvold)

Styringssystemet og handlingsplanen har tre fokusområder som regionen jobber med: egen sikkerhetskultur, å holde seg oppdatert på lover og revidering av styringssystemet. Et konkret eksempel på at regionen måtte oppdatere seg på nye lover var innføringen av GDPR, der poenget var å ha en strategisk tilnærming til GDPR, sikkerhetsloven og NIS-direktivitet.

Styringssystemet legger opp til aktiviteter som årlig skal gjennomgås. Et eksempel er årlige meldinger og hva som skal inn i ledelsens gjennomgang. Dokumentene inneholder faste punkter, deriblant hvilke sikkerhetsrevisjoner som er gjennomført og trender fra disse, trender fra avviksrapporteringer, om det har vært offentlige tilsyn og hvilke risikovurderinger som er gjort.

5.3.3 LEDELSEN

Hvordan man forholder seg til risiko og hvor godt forberedt man er på en krise, påvirkes av holdninger og kultur. I offentlig sektor kan kultur og ledelse påvirkes gjennom forvaltning og politikk: «*Vedtak om bevilgninger, organisasjonsstruktur, teknologiske løsninger og tiltak gir rammebetingelser som har betydning for kultur og ledelse*.» (Meld. st. 10 (2016-2017), s. 121). Imidlertid er det ikke mulig å vedta god kultur og ledelse. Det må skapes og videreutvikles. Regjeringen arbeider med å utvikle egnede rammebetingelser for å sikre god ledelse og gjennomføringskraft (ibid.), men det er likevel ledelsens ansvar å lage gode rammebetingelser og skape gode holdninger i den daglige driften – og på så måte sørge for god sikkerhetskultur.

For å oppnå en god kultur for forebygging, må man påvirke og endre kunnskap, motivasjon, holdninger og adferd både, noe som forutsetter forståelse og erkjennelse av at sikkerhet er viktig (ibid., s. 131). Det må gjennomsyre hele organisasjonen, noe som krever lederoppmerksomhet og prioriteringer, og å etablere en felles forståelse av hvorfor forebygging er viktig og hvilke skadefølger manglende forebygging kan få. God ledelse og tilstrekkelig fokus og oppmerksomhet rundt cybersikkerhet er dermed et viktig aspekt ved å bygge sikkerhetskultur.

Region Sør-Øst:

Ledelsen har fått et økt fokus på informasjonssikkerhet. I dag er det kun Ertenstein som jobber med informasjonssikkerhet på Sunnaas sykehus, men de er i en omorganiseringsprosess når det gjelder sikkerhet. De har fått flere ressurser og ledelsen skal ansatte flere innen sikkerhet. Kun i løpet av ett år har Ertenstein sett at fokuset har blitt vesentlig bedre. Informasjonssikkerhet tas jevnlig opp på ledelsens gjennomgang, og Sunnaas har årlige samlinger der det er et tema.

Jacobsen ble ansatt hos Sykehuspartner i 2013. På det tidspunktet jobbet kun tre personer med sikkerhet, nederst i organisasjonen og langt unna beslutningene. Siden den gang har Sykehuspartner jobbet aktivt med å fremme viktigheten av å jobbe med informasjonssikkerhet og å gjøre ledelsen oppmerksomme på hvordan god sikkerhet i design- og konseptfasen i et prosjekt for å spare penger i gjennomføringen av forvaltningsfasen.

Administrerende direktør i Sykehuspartner og Helse Sør-Øst RHF beskrives som svært opptatt informasjonssikkerhet. Påstanden underbygges ved at styret i Sykehuspartner behandler informasjonssikkerhet ved hvert styremøte, der det rapporteres på fremdrift, og at direktørene er aktivt engasjert i å følge opp at Sykehuspartner får gjennomført planene sine.

> *«Administrerende direktør i Helse Sør-Øst og Sykehuspartner er sikkerhetsbevisste, og de tar beslutninger sine med tanke på informasjonssikkerhet.»* (Jacobsen)

Region Vest:

Informantene menter at ledelsen i Helse Bergen HF og Helse Vest IKT har et tett fokus på IKT-sikkerhet. Sikkerhetssjefene i helseforetakene har hyppige møter med administrerende direktør der de rapporterer direkte til vedkommende, som kommer med føringer for det videre arbeidet. Baugstø-Hartvigsen hevder at IKT-sikkerhet er godt forankret i ledelsen og at det er sikkerhet i alt de driver med, men at de mangler ressurser. Oppedal støtter opp uttalelsen og forteller at helseforetakene ikke har øremerkede midler eller budsjettavsetting til sikkerhetsarbeidet.

> *«Det er et problem. Det betyr at hvis jeg trenger et verktøy, et fokus eller en satsing, så må jeg finne det en plass. Det er ikke alltid like lett.»* (Oppedal)

Oppmerksomheten og fokuset på IKT-sikkerhet har likevel endret seg drastisk de siste årene, men Baugstø-Hartvigsen påpeker at Helse Vest IKT skiller seg ut. Han mener Helse Vest IKT har hatt et vedvarende høyere fokus på sikkerhet, og at de andre helseforetakene i for stor grad har hvilt på leverandørene sine og ikke har tilstrekkelig oppmerksomhet, selv om informasjons-sikkerhet er på ledelsens agenda. Det er blant annet økt fokus på leder- og styresamlinger om informasjonssikkerhet, og det hentes inn ekspertise for å bli opplyst om sikkerhet og trusler.

Informantene peker på tre IKT-hendelser som har bidratt til å øke ledelsens fokus på sikkerhet i positiv retning. Den første hendelsen rammet var en nedetid som rammet hele Helse Vest da de oppgraderte DIPS i juni 2016. Informantene har tidligere trukket frem at det er vanskelig å drive sykehus uten IKT, og denne hendelsen blir trukket frem som et eksempel på dette. Helse Vest måtte føre alt på papir, og hendelsen viste hvor sentralt IKT og informasjonssikkerhet er.

> *«Informasjonssikkerhet har andre dimensjoner enn konfidensialitet, så dette var også på en måte med på å starte et eller annet.»* (Oppedal)

De andre hendelsene er knyttet til IKT-skandaler hos Helse Sør-Øst. Den ene hendelsen var en IKT-anskaffelse i Helse Sør-Øst i 2016, der helseforetaket outsourcet IT-driften til IT-selskapet DXC. Det ble senere avslørt at IT-arbeidere i Bulgaria og Malaysia hadde hatt tilgang til sensitiv pasientdata i strid med avtalen, og Helse Sør-Øst skrotet avtalen. Etter dette ble det større skepsis til og fokus på tjenesteutsetting i Helse Vest.

Den andre hendelsen var dataangrepet mot Helse Sør-Øst og Sykehuspartner i januar 2018. Informantene mener dette var en øyeåpner for lederne deres da de forsto at også helsesektoren er utsatt for denne type trusler og aktører.

Helse Vest har som resultat blitt mer oppmerksomme, strengere og innført ekstra tiltak for ytterligere sikre systemene. Informantene mener derfor at IKT-skandalene har hatt en positiv effekt på ledelsens fokus og arbeid med IKT-sikkerhet.

Region Midt-Norge:

Som IT-leverandør har Hemit godt fokus på IKT-sikkerhet, og det er derfor høyt oppe på prioriteringslisten. Både IKT-sikkerhet og risiko er tema i virksomhetens handlingsplaner, strategier og årlige arbeidsplaner. Bevissthet rundt informasjonssikkerhet beskrives som god i alle ledd i hele Helse Midt-Norge, også i ledelsen. Nyre hevder at fokuset på IKT-sikkerhet er svært godt når virksomheten vurderer nye tjenester. Da det f. eks kom spørsmål om bruk av Huawei-utstyr, etterspurte ledelsen en nøye vurdering grunnet faren for kinesisk etterretning.

> «*Vi kjører ikke bare på fordi det er 200.000 kr å spare, og det viser at det er relativt høy bevissthet*.» (Nyre)

Nyre ser et økende fokus på IKT-sikkerhet i Hemit, og underbygger at ansettelsen av han er en del av denne endringen. Stillingen hans ble utlyst før dataangrepet mot Helse Sør-Øst, noe som viser at fokuset var økende allerede før dette. Likevel tror han angrepet påvirket ledelsen til å få enda mer fokus. I følge Nyre har det gjort ledelsen svært redd for å gjøre feil.

> *«Man er redd for å bli tatt for å ikke gjøre vurderinger og være ubevisst. Det har vært en driver, spesielt for å få oversikt og kontroll. Så det har vært et økende fokus.*» (Nyre)

Nyre tror likevel at personvernskandalen i Helse Sør-Øst i forbindelse med tjenesteutsettings-prosjektet i 2016, samt de påfølgende bøtene fra Datatilsynet på tilsammen 7,2 millioner kroner, påvirket ledelsen i større grad. Han mener det traff ledelsen direkte. Dataangrepet mot Helse Sør-Øst i 2018 mener han var en større øyeåpner for fagretsen innenfor IKT-sikkerhet.

På St. Olavs Hospital blir IKT-sikkerhet jevnlig diskutert i ledelsen. Vanvik er likevel usikker på om alle forstår problematikken. Han peker på at driftsavdelingen med ansvar for de tekniske systemene, som nå er koblet til nettet, er klar over risikoen. Likevel er de preget av en usikkerhet om hvorvidt systemene godt nok sikret. Ledelsen er i følge Vandvik dyktige til å håndtere IKT-hendelser fordi det i stor grad klarer å improvisere. Han savner likevel et godt planverk som gjør at stedfortredere og ansatte med lite erfaring kan håndtere de samme hendelsene.

Region Nord:

Ledelsens fokus på cybersikkerhet har økt drastisk de siste årene, og det er større fokus på at sikkerheten skal ivaretas i et helhetsperspektiv i hele regionen. Både Helse Nord IKT og sikkerhetsansvarlige i de øvrige helseforetakene følger med på utviklingen når det gjelder cybersikkerhet. Martinussen påpeker at hun ble ansatt som informasjonssikkerhetsleder i Helse Nord RHF i 2016. Stillingen var nyopprettet, og hun er altså den første med stillingen i Helse

Nord RHF, noe som viser regionens økte fokus på sikkerhet. Informantene legger til at Helse Nord IKT har satt i gang et stort arbeid for å ytterligere sikre regionens infrastruktur.

Sikkerhetslederne ved hvert helseforetak rapporterer til styret 1-2 ganger i året, via direktøren. I rapportene skal sikkerhetslederne fortelle om status når det gjelder sikkerhetsarbeidet, om de har hatt avvik, hvilke risikovurderinger som er gjennomført, i tillegg til status på tiltak, samt hovedtrekk når det gjelder sikkerhetsutfordringer. Bruvold gir i tillegg informasjon om den generelle utviklingen av cyberkriminalitet. Samtidig ser informantene en økning i frekvensen i rapportering til departementene, noe som viser til at det også har fått økt politisk fokus.

> *«Det har vært en enorm endring. Det begynte i 2006, men så har det eskalert. Vi har fått større fokus at sikkerheten skal ivaretas i et helhetsperspektiv i hele regionen.» (Bruvold)*

Selv om ledelsens fokus på informasjonssikkerhet begynte å øke allerede for noen år siden, påpeker de likevel at dataangrepet mot Helse Sør-Øst økte fokuset økte ytterligere, spesielt blant ledelsen fordi det rammet nær krets. De hevder at det ikke endret fokuset til de som jobber fulltid med informasjonssikkerhet, men at de så en helhetlig økning i organisasjonen rundt. Dette er en positiv effekt av angrepet, men det har endret arbeidshverdagen til de som jobber med sikkerhet til daglig. Økt fokus og interesse for et fagfelt som ikke har hatt høyt fokus tidligere, har gjort at arbeidsbelastningen til denne gruppen har økt.

> *«Det er likevel positivt at ledelsen er interessert i dette.»* (Martinussen)

5.4 DIGITAL RISIKO

Den digitale verden blir stadig mer kompleks. Både nye og gamle systemer, basert på ulik teknologi, skal fungere sammen, verdikjeder blir lengre og uoversiktlige, tjenester settes ut som øker avhengigheten til underleverandører, virksomhetens systemer eksponeres på nett, og ny teknologi introduseres raskt (NSM, 2018c, s. 5). Endringer skjer hurtigere, og kompleksiteten kommer ikke uten sikkerhetsutfordringer (ibid). I følge NSM (ibid) øker den digitale risikoen. Flere verdier skal passes på, og man utsettes for profesjonelle, målrettede aktører. Samtidig øker antall sårbarheter i både samfunnet og hos norske virksomheter (ibid). NSM mener likevel at digitaliseringen kan gjennomføres med akseptabel risiko dersom virksomheter arbeider systematisk og godt med sikkerheten (ibid.) Sikkerhetsarbeidet krever større innsats, men NSM skisserer at en enkel løsning er å prioritere sikkerhet og gjennomføre risikovurderinger for å kartlegge sårbarheter og risiko man står ovenfor (ibid.)

5.4.1 RISIKOVURDERING

Det nasjonale trussel- og risikobildet viser at utfordringene ved å ivareta informasjonssikkerhet er tverrsektorielle, og at det krever en helhetlig tilnærming. NSM har derfor utarbeidet et nasjonalt IKT-risikobilde, som er et verktøy for å utarbeide risikovurderinger (Meld. St. 27. (2015-2016), s, 151). NSM (2018b, s. 5) mener at ledelsen må prioritere sikkerhet og sørge for at virksomheten gjennomfører risikovurderinger.

Informasjonssikkerheten skal ivaretas med en risikobasert tilnærming (Meld. St. 27. (2015-2016), s. 12). Det vil si at alle sikkerhetstiltak som skal iverksettes skal være basert på en risikovurdering, og at virksomhetsledelsen gjør nødvendige tiltak for å sikre at risikoen er begrenset (ibid., s. 50). Personvern og informasjonssikkerhet skal være en integrert del av utviklingen og bruken av IKT i helsesektoren (Direktoratet for e-helse, 2017, s. 9). Informasjonssikkerhet skal ivaretas med utgangspunkt i risikovurderinger basert på oppdaterte trussel- og sårbarhetsinformasjon og følges opp gjennom god internkontroll (ibid.)

Ved endring eller innføring av en tjeneste eller et system, gjennomfører helseforetakene risikovurderinger for å kartlegge risiko og sårbarheter. Dette er særlig kritisk hvis en tjeneste behandler personvernopplysninger. Risikovurderingen danner et beslutningsgrunnlag for å vurdere endringen eller innføringen, og eventuelt sette inn forebyggende tiltak. Forebygging handler om å unngå at noe uønsket skjer, eller redusere skadepotensialet til de hendelsene som inntreffer (Meld. st. 10 (2016-2017), s. 131).

Region Sør-Øst:

Jacobsen mener Helse Sør-Øst gjennomfører for mange tunge risikovurderinger. Prosessen kan ta opp mot 200 timer, inkludert dokumentasjon rundt løsningssystem, konfigurasjon og risikovurderingen. Jacobsen er kritisk til at tiltak som er risikoreduserende i natur likevel må gjennom en tung og tidkrevende prosess, og at risikovurderingene ofte er negativt ladet.

> *«Jeg synes kravene om risikovurderinger ofte er et hinder mot å gjøre ting bedre. Det vurderes sjelden hva en positiv gevinst er.»* (Jacobsen)

Man får altså ikke en risikovurdering som balanserer fordeler og ulemper, men en vurdering som er ensidig negativt. Det er dermed en tendens til å fokusere på risikoreduserende tiltak for å oppnå en nøytral tilstand. Jacobsen kaller det en «tiltakssyke» der man setter i gang tiltak etter tiltak med fire egenskaper som i ulik grad er fremtredende: det blir mer komplisert, det blir forsinket, det blir dyrere og det blir vanskeligere å bruke. Jacobsen mener at Helse Sør-Øst har en risikosituasjon som medfører at risikovurderinger blir en negativ øvelse. Det skaper et

system og en kultur for risikovurderinger som hovedsakelig er negative – uavhengig av hvor positive endringene er.

> *«Det betyr at ting som skulle gjort ting bedre ikke blir gjort, fordi man sitter og løser tiltak på det som allerede er dårlig.»* (Jacobsen)

Region Vest:

Helse Vest IKT har et driftssenter som driver overvåkning av infrastrukturen døgnet rundt, og Helse Vest IKT utfører flere risikovurderinger i uka på vegne av helseforetakene. I tillegg mottar regionen årlig en stor leveranse for deres overordnende infrastruktur. Det blir også gjennomført mindre risikovurderinger lokalt i hver virksomhet. Helse Vest har felles metodikk og verktøy for å drive risikovurdering – og etterhvert også personkonsekvensvurdering.

Alle større IKT-endringer som Helse Vest IKT utfører blir gjenstand for risikovurderinger. Det vil si at hver gang et system skal utvikles, oppdateres eller brukes, blir det gjennomført en risikovurdering. Dersom et system eksponeres, blir det sikret med tofaktorautentisering. Risikovurderingen avdekker omfang, sårbarheter og kritikalitet til det som er knyttet til en konkret anskaffelse, implementering eller endring av systemer. Resultatene bestemmer hvilke tiltak som iverksettes. Eksempler på tiltak er sikkerhetstester, penetrasjonstester og leverandørstyring.

Region Midt-Norge:

Helse Midt-Norges har en helhetlig og operativ risikovurdering som oppdateres kontinuerlig og brukes av kriseledelsen og i beredskapsarbeidet ved innføring eller endring av et system. Driftsavdelingene har et pågående arbeid med å analyse alle driftssystemer for å finne sårbarheter og presentere dette, til slik at helsepersonell og ansvarlige ledere kjenner til digital risiko og risikoen av IKT-bortfall.

Når nye systemer skal utvikles tar Hemit høyde for trusselaktører ved å gå fra implisitt til eksplisitt i risikovurderingene, som vil si at de gjør et bevist valg på hvem man tar med som aktuelle aktører. Hemit har nå rundt 20 aktører og varianter, som inkluderer ansatte og pasienter. Risikovurderingen oppdateres dersom det kommer frem at aktører må utelates eller inkluderes, noe som alltid må begrunnes og beskrives. Dersom en aktør endrer karakter, går Hemit gjennom alle systemer der aktøren er relevant og oppdaterer risikovurdering.

Nyre ønsker at gjennomføring og styring av risikovurderinger skal bli enklere. Hemit jobber med å forbedre metoden for risikovurdering, der målet er reproduserbarhet og forenkling, slik at flere kan gjennomgjøre det. Ved nøyaktig dokumentasjon av metode, utgangspunkt og antagelser, ønsker Nyre å gjøre risikovurderingene mindre personavhengig.

Intern gjennomgang i Hemit viser at risikovurderingene har liten tilknyttingen til virksomheten, da risikovurderingene ofte er preget av et stort lovfokus. Nyre kritiserer at risikovurderingene styres av fare for brudd på lov, sannsynlighet for brudd på lov og hvor alvorlig bruddet er, fremfor å fokusere på effekt på helsehjelp, omdømme, erstatningsansvar og driften av virksomheten. Han mener en risikovurdering kan bli gradert for brudd på konfidensialiteten, uten å systematisk gå til verks for hva risikovurderingen kan bety for liv og helse.

> *«Da får du en utfordring med risikostyring, fordi ledelsen i mindre grad har et forhold til at konsekvensene er brudd på konfidensialiteten for helseopplysningene.»* (Nyre)

Region Nord:

For å sikre de digitale systemene utfører helseforetakene risikovurderinger hver gang det skjer en endring som har betydning for informasjonssikkerheten, eller før et nytt system skal ta i bruk. Å ta høyde for trusler når nye systemer utvikles er en naturlig del av risikovurderingene som gjøres. Risikovurderingene er også en del av beredskapsarbeidet, der hensikten med risikovurderingene vil være å avdekke hvor de har for høy risiko og dermed sette inn tiltak for å møte risikoen. Selve infrastrukturen er bygd slik at den skal takle nedetid.

> *«Hvis en datasentral faller sammen, så skal vi kunne bytte over til en reservedatasentral og være oppe å gå igjen. Den fysiske delen har vi sånn sett god kontroll på.»* (Bruvold)

Virksomhetene i Helse Nord er i tett dialog om utviklingen og utfordringer rundt regionens informasjonssikkerhet, noe som innebærer risikovurderinger. Internt i UNN er det en gruppe som jobber med informasjonssikkerhet, som går ut på forebyggende arbeid og risikovurderinger.

5.4.2 TRUSSELBILDET

Man ser i økende grad at det foregår målrettede angrep, og det blir stadig mer krevende for helsesektoren å holde tritt med trusselbildet (Omerovic & Gjære, 2015, s. 25). Trusselbildet i det digitale rom er raskt og voksende, og etter angrepet mot Helse Sør-Øst så også helsesektoren gevinsten av en helhetlig oversikt over dette. Flere av informantene forteller at de nasjonale trusselvurderingene fikk økt relevans for dem etter angrepet. Det er likevel mangelfullt grunnlag for en helhetlig oversikt, og per i dag benytter helsesektoren flere kilder for å skaffe seg informasjon om trusselbildet. Følgene kilder trekkes fram av informantene:

- Åpne trusselvurderinger fra PST, NSM og E-tjenesten
- HelseCERT – oppdatert trusselvurdering fra 2018
- Normen og Normkonferansen – gir deler av trusselbildet
- Ulike konferanser om cybersikkerhet
- Twitter (Jacobsen, Helse Sør-Øst)

Region Sør-Øst:

Helse Sør-Øst skaffer informasjon om trusselbildet på ulike måter. Informasjon om operative data, som IOC eller annen type operativ angrepsinformasjon, skaffer de særlig gjennom åpne eller lukkede kilder. Lukkede kilder kan være en gjensidig del av en kompetanseutvekslings- og informasjonsutvekslingsgruppe, altså et lukket forum. Dette beskrives som gode nettverk der man kan dele kunnskap om trusselbildet.

Når det gjelder det større strategiske trusselbildet, der de ønsker informasjon om hvem trusselaktørene er, hvorfor de gjør det og hva de vil oppnå, brukes åpne kilder, som åpne trussel- og sårbarhetsvurderinger, i tillegg til Sykehuspartner CERT. Jacobsen bruker også Twitter i stor grad, og hevder at å følge med på trendene i kanalen er en av de beste måtene til å holde seg oppdatert om cybertrusler. Blant annet plukket de opp cyberangrepetet mot SingaHealth i 2018 på Twitter før de fikk offisiell informasjon om hendelsen.

> *«Summen av flinke folk som gir gode analyser gjør at vi kan sette det sammen til noe som er relevant for oss, og vi kan følge med på trender»* (Jacobsen)

Jacobsen forteller at trusselaktørene drives av verdibasert strategisk styring. Det betyr at Helse Sør-Øst har verdier som gjør at noen har en strategisk interesse for å angripe dem. Attribusjon gjør det mulig å si noe om både verktøyene og metoden til en trusselaktør, men også hva som er deres ultimates mål. Aktøren som angrep Helse Sør-Øst var ute etter data. Det var en etterretningsoperasjon, og Jacobsen mener at etterretning for å håndtere dette er en vesentlig mangel i markedet. For å kunne ta de beste beslutningene under et angrep, er det er helt nødvendig å forstå hvem som mest sannsynlig angriper deg før angrepet inntreffer.

Helse Sør-Øst og Sykehuspartner forsøker å bygge en god trusseletterretning for å håndtere kompliserte etterretningsoperasjoner, men per i dag er det ingen norske aktører som tilbyr den type trusseletterretning som Jacobsen sikter til.

Region Vest:

Konferansen HackCon (The Norwegian Cyber Security Convention) blir trukket frem som en spesielt nyttig arena for å få innsikt i trusselbildet.

Informantene påpeker at brudd på integritet, konfidensialitet og tilgjengelighet er de største cybertruslene i Helse Vest. De påpeker likevel at det finnes ulike svar på nettopp dette, og at den desidert farligste og skumleste for helsesektoren er statlige aktører, som trusselaktøren som angrep Helse Sør-Øst. Såkalte APT-aktører som trenger seg inn over tid uten å gi seg til kjenne, med et mål om å hente informasjon. Informantene forteller at de ser mindre av dataangrep som

ransomware, der aktørene forsøker å stenge linjene, systemer eller enkelte nettsider. Dette er de robuste nok til å håndtere og regnes derfor ikke som en aktuell og vesentlig trussel.

Region Midt-Norge:

Nyre peker på at man historisk sett ikke har hatt et godt dokumentert forhold til trusselbildet i helsesektoren, da det har vært uenigheter om hvorvidt trusselbildet ser ut. Helsesektoren har begynt å lage egne trusselvurderinger som tar for seg en vurdering av ulike aktørtyper og deres grunnleggende ressurser, kompetanse, mål og hva de kan gjøre. Åpne trusselvurderinger fra er gode utgangspunkt for å hente informasjon om trusselbildet.

> *«Dessverre er våre trusselvurderinger nesten utelukkende basert på disse trussel-vurderingene. Vi prøver derfor å tolke de inn i vår kontekst og dokumentere det»*. (Nyre)

Vandvik mener de åpne trusselvurderingene samt og de ulike organisasjonene i helsesektoren gir et godt overblikk over trusselbildet helsesektoren står ovenfor. Han hevder at den største trusselen i helsesektoren er ansatte som gjør feil. Han antar at de ikke står ovenfor en spesifikk overhengende trussel, men at de må være forberedt på aktørers vedvarende forsøk på å finne svakheter som kan utnyttes. Derfor mener han driftsavdelingens arbeid med å finne og tette svakheter svært viktig for helseforetakene.

Det er flere potensielle aktører som er interessert i å angripe helsesektoren, og noen er mer fremtredende enn andre. Nyre ser at trusselbildet har endret seg raskt. For tiden er fremmede stater ansett som aktuelle trusler, noe Nyre kaller mener er et overdrevent fokus. Selv om fremmede stater ikke er mest relevant for helsesektoren og sjelden slår til, er det en ekstrem aktør som Nyre mener er viktig å vurdere når det gjelder infrastrukturen.

> *«Man må være klar over at den type aktør finnes, og at de kan være interessert i å angripe oss. Tar vi for oss enkeltsystemer er de ikke ansett som en stor trussel.»* (Nyre)

Følgende aktører trekkes frem som relevante for helsesektoren: (1) økonomisk kriminelle, (2) leverandører, (3) ansatte, (4) kryptovirus (kan skape problemer på infrastruktur og servere).

Både virksomheter, bedrifter og ansatte utgjør en trussel. Etter innføringen av GDPR har ansatte og virksomheter i helsesektoren blitt lagt inn som en aktuell aktør i risikovurderinger av pasienters personvern. Dette begrunnes med at ansatte selv kan skape en trussel mot pasienten personvern, enten med intensjon eller ufrivillig.

Region Nord:

Deltakelse i internasjonale og nasjonale fora er en viktig arene for Helse Nord når de skal skaffe seg kunnskap om det aktuelle trusselbildet. Ellers nevnes FRIS som én av de viktigste kildene,

i tillegg til HelseCERT og Normen. Normen bidrar med kunnskap, forståelse og rammebetingelser for hvordan Helse Nord skal håndtere helse- og personopplysninger.

> *«De ulike driftsorganisasjonene i de ulike regionene har et nært samarbeid og deler informasjon, som også er en god kilde til informasjon om trusselbildet.»* (Martiunssen)

Informantene påpeker at Helse Nord RHF står ovenfor mange cybertrusler. Én av truslene er at utenforstående får tilgang til pasient- og personopplysninger, blant annet gjennom drift- og vedlikeholdsarbeid fra systemleverandører. HelseCERT ivaretar en del av overvåkningen når det gjelder trafikken ut og inn av sykehusenes systemer. HelseCERT bidrar også med inntrengingstesting utenifra, for å se på om helseforetakene har hull i sikkerhetssystemene. Helsesektoren har flere risikoområder, og trekker spesielt frem følgende områder: (1) bevisstgjøring av ansatte og kompetanse, (2) cyberkriminalitet, (3) samhandling med andre virksomheter, (4) økende avhengighet til systemer, (5) beredskap ved nedetid.

Martinussen er bekymret for at avhengigheten til systemene ser ut til å vokse raskere enn man kan klare å sikre dem. God nok kompetanse er derfor er en reell utfordring, både regionalt og nasjonalt. Regjeringens strategi for nasjonal digital kompetanse underbygger påstanden.

> *«De har skissert flere konkrete tiltak på hvordan man skal få økt kompetanse om informasjonssikkerhet, både fra grunnskolen og inn til mot forskning.»* (Martinussen).

5.4.3 SÅRBARHETER

En stor andel uønskede hendelser som rammer IKT-systemer er utilsiktede. Feil og avvik i IKT-systemer kan skje grunnet menneskelige feil, programvarefeil, utstyrsfeil, eller en kombinasjon. Menneskelige feil relateres ofte til mangelfull kompetanse og forståelse av nettverk og systemer, mangelfull sikkerhetskultur eller for dårlig internkontroll (Meld. st. 10 (2016-2017), s. 59).

Videre kan tjenesteutsetting utgjøre en trussel. NSMs (2018, s. 12) anbefalinger for å ivareta IKT-sikkerheten ved tjenesteutsetting er å ta gode risikovurderinger for å kunne ta gode beslutninger, ha god bestillerkompetanse og ha oversikt og kontroll over livsløpet. Underleverandører blir stadig flere, og også de bli mål for målrettede dataangrep. Derfor forventes det at også underleverandører har god sikkerhetskultur og tilsvarende rutiner og opplæring omkring taushetsplikt som helsesektoren for øvrig (Omerovic & Gjære, 2015, s. 21).

Region Sør-Øst:

Mangel på modernisering og manglende dokumentasjon på gamle tjenester trekkes frem som teknologiske sårbarheter. Menneskelige sårbarheter knyttes til manglende kunnskap og nøkkel-

personell, samt kompetansebeslutninger. Organisatoriske sårbarheter er manglende ressurser, behov for bedre ledelsesfokus og manglende risikostyring.

En del av metodeverket er å ta høyde for trusselaktører i utvikling av nye systemer. Jacobsen skiller tjenestene mellom kliniske tjenester og infrastrukturtjenester. Tilgangsstyring sikrer at uvedkommende ikke får tilgang. Infrastrukturtjenester er tilgangsstyrt gjennom katalogtjenester basert på ansvarsforhold og tjenstlig behov. Prosessen begynner med at man bestiller en tilgang, før henvendelsen sendes til nærmeste leder som skal validere om det er et tjenstlig behov. Ved godkjennelse går henvendelsen videre til tjenesteansvarlig, som verifiserer og sikrer tilgangen.

Tilgangsstyringen av kliniske applikasjoner varierer. For eksempel har epj-systemet DIPS en granulert tilgangsstyringsmetode. Det vil si at tjenesteansvarlig ser på medarbeiderens stilling og HPR-nummer i personalsystemet, samt hvor vedkommende jobber. Ut i fra dette og andre variabler får hver ansatt en tilgangsprofil. I enkelte systemer finnes det ikke tilgangsstyring. Det er leverandørenes ansvar å designe god tilgangsstyring i kliniske applikasjoner.

Der Helse Sør-Øst har hendelser som gir nedetid er årsaken ofte manglende standardisering, forvaltning og kontroll. Da foretaket var rammet av nedetid 18. januar 2019, skyldes det en feil på ruteren. Helse Sør-Øst har også hatt hendelser forårsaket av brukerfeil. APT-angrep og fremmede stater er dermed ikke den største trusselen mot Helse Sør-Øst. Den største trusselen er manglende modernisering, som skaper sårbarheter i driften.

> *«Vår trussel mot sikkerhetsstabil drift er en foreldet infrastruktur som blir vanskeligere å forvalte og drifte, der man blir mer sårbare for driftsfortstyrelser.»* (Jacobsen)

Helsesektoren har flere utdaterte applikasjoner, som er laget uten hensyn til personvern eller informasjonssikkerhet og som er vanskelig og kostbart å erstatte. Enkelte systemer har ikke alternativer som oppfattes som helsemessig tilfredsstillende eller forsvarlig av klinikerne. Det gjør at man ender opp i dilemmaer om hva som skal veie tyngst: god sporbarhet og autentisering, eller best mulig helsehjelp. Ved slike tilfeller er det viktig med god ledelsesforankring av informasjonssikkerhet, slik at diskusjonen blir avklart på riktig ledernivå. Jacobsen mener at det må være administrerende direktør som avgjør om en tjeneste er så viktig at det for eksempel går på kompromiss med personvernet. Informasjonssikkerhet må bli organisatorisk plassert.

> *«Dette er risikostyring i praksis. Man må dokumentere og vite hvilken risiko man tar.»* (Jacobsen)

Region Vest:

Lange digitale verdikjeder utgjør en sårbarhet i helsesektoren. Helse Vest sikrer dette ved at leverandørstyring skal foregå gjennom tjenestenivåavtalen og databehandleravtalen, samt verktøy for å styre tilgangene. Ansvarliggjøringen ligger altså i avtalereguleringen. Gjennom funn fra risikovurderinger vurderes bruk av tjenesteutsetting og eventuelle sikkerhetstiltak.

For å sikre tilgangen til systemene bruker Helse Vest tilgangsstyringsmekanismer og andre sikkerhetsfunksjoner for å identifisere brukerne. For eksempel brukes tofaktorautentisering dersom noe i intern infrastruktur skal gjøres tilgjengelig. Helse Vest har et stort IAM-system (Identify Access Managment) som er regionens samlepunkt. Systemet er integrert mot flertallet av regionens store systemer. Informantene forteller at dette er en egenutviklet hjemmeløsning som ivaretar sikkerheten. Systemet ligger ute på hver enkelt avdeling. Helse Vest har altså et sentralt verktøy for tilgangsstyring, og delegeringen styres i forhold til tilgang. Når man først har fått en tilgang betyr det at den fortsatt kan styres avhengig av hvor man befinner seg.

> *«Det er lederen på posten som beslutter hvilke tilganger du skal ha.»* Oppedal)

Menneskelige sårbarheter og aktørers evne til å utnytte ansatte er problemstillinger som sikkerhetssjefene må forholde seg til, og Helse Vest har flere tiltak for å ta høyde for den menneskelige sårbarhetsfaktoren. I Helse Vest settes det inn tekniske tiltak på alt sluttbrukeren bruker for å sikre klientplattformen og sluttbrukerutstyret. De tekniske tiltakene er blant annet ikke-administrative brukere, kryptering av utstyr, applikasjonsblokkeringer og hvitelisting m.m.

> *«Mitt mantra er at det skal være lett å gjøre det rett. Vi forsøker å aldri si at noen har gjort en feil.»* (Baugstø-Hartvigsen)

Ved avvik grunnet menneskelig feil, puttes avviket inn i et synergiverktøy, altså et avviks-håndteringssystem. Avviket håndteres primært på virksomhets-, avdelings- eller gruppenivå og fremstilles som en dårlig praksis alle i regionen kan lære av. Det kalles derfor for øvelsesavvik.

Region Midt-Norge:

Nyre henviser til DSBs definisjon av sårbarhet som evnen til å motstå angrep eller hendelser. Nyre definerer sårbarheter som en svakhet som kan utnyttes. Upatchede systemer utgjør dermed en sårbarhet. Styringssystemet i Helse Midt-Norge fører krav og regimer til å patche systemer. Dette er effektivt og gjøres jevnlig, men enkelte systemer og programvarer bruker servere som ikke lenger lar seg patche. Nyre trekker frem at dette spesielt gjelder MTU. Årsaken til at det ikke finnes patcher skyldes at gamle programvarer ikke fungerer på oppgradert programvare og operativsystem. Det vil si at det ikke finnes en patch dersom man finner sårbarheter.

En sårbarhet Hemit jobber med å styrke er datarom og nettverk. I dag er alle datarom i Trondheim, noe som gjør at et kabelbrudd i Trondheim vil ramme både Nord-Trøndelag og Møre og Romsdal. Det finnes en strømbackup, men Nyre mener det er uhensiktsmessig. Det har blitt vurdert å endre det, men sannsynligheten for kabelbrudd ble vurdert som minimal og kostnaden så stor at saken ble liggende. Nå skal det vurderes på nytt fordi konsekvensene av et kabelbrudd er store. Intern telefon, internnettverk og kommunikasjonstjenester er svært viktig for driften. En løsning som trekkes frem er å etablere geo-redundans på datasentrene.

Helse Midt-Norges volum av systemer gjør det utfordrende å følge med på sårbarheter og sikre at alt er rett konfigurert. Kompleksitet og manglende geo-redundans blir derfor trukket frem som store sårbarheter. I forlengelsen av dette påpekes avhengighet til systemer som en sårbarhet. Mange systemer kommuniserer med hverandre, noe som ved oppgraderinger av ett system kan skape uventete hendelser i et annet system. Konsekvensen kan være at hele tjenesten faller bort.

Menneskelig feil blir likevel trukket frem som den største sårbarheten. Mennesket beskrives som både det sterkeste og svakeste ledd, da mange angrep starter med menneskelige sårbarheter – altså at ansatte lures eller presses. Det påpekes at menneskelige feil kan være så banalt som at en håndverker slår av en bryter eller sikring som gjør at nettverket faller bort. Det kan også være at ansatte bruker systemer feil. Likevel fokuseres det på at ingen ansatte skal kunne gjøre feil som får katastrofale følger, som sikres ved å styre rettigheter, muligheter og tilgang.

> *«Jeg er opptatt av å ikke snakke om folk som idioter. Folk gjør feil, det vil de alltid gjøre. Det er det man kaller tilgivende design.»* (Nyre)

En sentralisert gruppe jobber med elektronisk tilgangsstyring i Helse Midt-Norge, noe som skal sikre at uvedkommende ikke får tilgang til systemer. Hver klinikk har en fagansvarlig som gir tilgang til systemer og delegerer rettigheter nedover i linjen. De er også ansvarlig for å sjekke at ingen har flere rettigheter enn de har behov for i sin stilling. Tilgangen bestilles fra Hemit. Internt i Hemit gjennomføres det systematiske tilgangsvurderinger. Tilgangsstyringen kontrolleres ved at ingen kan ikke delegere flere rettigheter enn de har selv.

Region Nord:

Både organisatoriske, teknologiske og menneskelige sårbarheter blir kartlagt gjennom ROS-analyser. Alle ansatte er ansvarliggjort for egne handlinger, og en del av ansvaret deres er å forvalte informasjon og overholde den lovpålagte taushetsplikten.

> *«Dette ansvaret ivaretar vi med opplæring, bevisstgjøring og kurs, men til syvende og sist påhviler det et ansvar på den enkelte.»* (Bruvold)

Lange digitale verdikjeder utgjør en sårbarhet i hele helsesektoren. Dette reguleres gjennom et avtaleverk der leverandørene forplikter seg til å gjøre de sikkerhetstiltakene som lovverket krever og som dataansvarlige er ansvarlige for. Leverandørene skal i tillegg gjennomføre risikovurderinger, som revideres av de regionale helseforetakene eller en tredjepart. Helse Nord vurderer nøye hvilke systemtilganger leverandørene skal ha.

Faste prosedyrer for tilgangsstyring kontrollerer hvem som har tilgang til systemene. Prosedyrene bestemmer hva den enkelte skal ha tilgang til, og gir føringer om at de enkelte avdelingslederne skal kontrollere tilgangen minst én gang i året. Helse Nord RHF utfører i tillegg loggkontroller for å sikre at uvedkommende ikke har tilgang eller innsyn i journaler. Pasienter kan også selv gå inn å se dette gjennom loggen i Helsenorge.no.

Helse Nord RHF har altså en tredelt strategi for å sikre at ikke uvedkommende har tilgang til journaler og systemer i helseforetaket: (1) pasienten har krav på innsyn i egne opplysninger, (2) interne prosedyrer og kontroller på at prosedyrene blir fulgt og (3) stikkprøvekontroller i loggene.

5.5 OPPSUMMERING AV EMPIRI

Digitalisering: Digitaliseringen har endret risikobildet. Avhengigheten til digitale systemer skaper flere sårbarheter og utfordringer i helsesektoren, som manglende IKT-kompetanse, mindre helsepersonell, lange verdikjeder og informasjonskjeder og en økt angrepsflate. Avhengigheten til systemene vokser raskere enn evnen til å sikre dem. Kritiske systemer svært kritiske mot bortfall av IKT. Kliniske applikasjoner og AMK-sentral svært viktig for drift av sykehusene. Akutte operasjoner vil kunne foregå ved bortfall av IKT, men det blir tidkrevende og tungvint. Bortfall av Telekom, nettverk og infrastruktur viktig i et beredskapsperspektiv.

Cyberangrep: Cybertrusselen er økende. Etter angrepet mot Helse Sør-Øst er APT-angrep er satt på agendaen. Angrepet har hatt store konsekvenser, både økonomisk og fokuset på sikkerhet. Det omtales som en øyeåpner for helsesektoren, og fokuset på viktigheten av god informasjonssikkerhet, verdivurdering og responshåndtering endret seg drastisk. Helsesektoren har god åpenhetskultur, og Helse Sør-Øst delte de viktigste erfaringene og læringspunktene med de andre helseregionene og store kommuner. De viktigste læringspunktene var viktigheten av å ha kunnskap om egne verdier, trusler, sårbarheter og digitalt utstyr, og at deteksjon er nødvendig. Ransomware, CEO-fraud, e-post-svindel og DDoS er fortsatt det vanligste, men det påvirker driften i liten grad grunnet gode mekanismer og sikkerhetslag som kan håndtere dette. Helsesektoren er imidlertid sårbare for et høyt volum av distribuerte DDoS-angrep.

Sikkerhetskultur: Helsepersonell har lav IKT-kompetanse, men høy respekt for taushetsplikt. De har imidlertid ikke forutsetninger for å ha høy IKT-kompetanse, men kurs og oppsøkende virksomhet benyttes for å dekke grunnleggende kompetanse om cybertrusler og cybersikkerhet. Det obligatorisk e-læringskurset trekkes frem som et nyttig verktøy, men kurset burde få strengere gjennomføringskrav og høyere frekvens, ettersom cybersikkerhet er ferskvare. Helsesektoren mangler generelt ansatte med kompetanse innen cybersikkerhet fordi utdanning og opplæring innen feltet har kommet for sent i gang. Helseforetakene har for lite kapasitet til å kunne håndtere informasjonssikkerhet i egen linje, for lite midler til cybersikkerhet og få ansatte med hovedfokus på informasjonssikkerhet.

Styringssystem for informasjonssikkerhet og personvern legger føringer for sikkerhetsarbeidet og sikrer forutsigbarhet. Det forenkler oppgaver, lager prosedyrer og sørger for dokumentasjon, blant annet ved gjennomføring av risikovurderinger. Fokuset på dokumentasjon varierer, noe som gjør det utfordrende å vurdere og forstå endringer som burde vært dokumentert, eller som ikke er tilstrekkelig dokumentert. Styringssystemet gir anledning til å sanksjonere arbeidsforhold dersom noen opptrer utenfor virksomhetens sikkerhetspolicy. Imidlertid mangler styringssystemet likevel tilknytting til helsesektoren og bør operasjonaliseres i detalj, noe som kan bidra til å gjøre sikkerhet til en integrert del av driften. Ledelsen i helseforetakene har fått økt fokus på informasjonssikkerhet, og tar i økende grad beslutninger basert på sikkerhet. Angrepet mot Helse Sør-Øst bidro til å øke ledelsens fokus.

Digital risiko: Risikovurderinger gjennomføres hver gang der skjer en endring eller innføring av en ny tjeneste eller et nytt system, og det gir god oversikt over risiko og sårbarheter, men helseforetak bør i økende grad også fokusere på verdivurderinger. Informantene kritiserer at man generelt er for dårlig til å dokumentere i etterkant av risikovurderinger. Risikovurderingene blir dermed personorienterte. Samtidig er risikovurderingene ofte innstilt på entydig negative konsekvenser, noe som kan hindre de positive gevinstene av sikkerhetstiltak.

Risikovurderingene oppdateres jevnlig for å tilpasses trusselbildet. Informasjon om trusselbildet fås gjennom åpne og lukkede kilder, som nettverksfora og trusselvurderingene til PST, NSM, E-tjenesten og helsesektorens egne vurderinger og kartlegginger. Informantene savner en helhetlig vurdering som fokuserer på helsesektoren. Trussel- og sårbarhetsbildet i sektoren er stort, og omfatter både menneskelig, organisatorisk og teknisks svikt.

KAPITTEL 6: ANALYSE OG DRØFTING

Det følgende kapittelet presenterer oppsummering av empiri, samt analyse og drøfting av empirien i lys av det teoretiske rammeverket. Analysen vil bli delt inn i tre deler. Inndelingen vil følge forskningsspørsmålene presentert i kapittel 1. Det teoretiske rammeverket vil bli brukt gjennomgående for analyse og drøfting.

6.1 KJENNER HELSEFORETAKENE GODT NOK TIL DEN DIGITALE RISIKOEN?

IKT har blitt en stor del av helsesektoren, som er en bærebjelke for befolkningens liv og helse. Digitaliseringen fører til større digital avhengighet i helsesektoren, og implementeringen av nye løsninger øker den digitale risikoen. Helsesektoren får flere sårbarheter og trusselbildet vokser, noe som kommer tydelig frem i empirien. I følge Aven (2015, s. 13) består risiko av faktorene usikkerhet og konsekvenser: en gitt aktivitet leder til usikre konsekvenser, og utgjør dermed en risiko. NSM (2015a, s. 10) definerer risiko som forholdet mellom faktorene verdier, trusler og sårbarheter. Viktigheten av å identifisere og kartlegge egen risiko er det første punktet i NSMs grunnprinsipper for IKT-sikkerhet (NSM, 2018a, s. 6). I følge empirien viste dataangrepet mot Helse Sør-Øst at helsesektoren i større grad må identifisere og kartlegge egen risiko. Det vil si å gjøre seg kjent med egne verdier, avhengigheter, sårbarheter, kompetansebehov og ansatte.

Flere av informantene mener det er utfordrende å ha oversikt over et trusselbilde som er kompleks og som kontinuerlig endres, noe som tydeliggjør at helsesektoren har behov for tilstrekkelig kompetanse på cybersikkerhet. Trusler er mulige årsaker til uønskede hendelser, og empirien viser nødvendigheten av å sammenfatte trusselbildet innen det digitale rom. Kunnskap om trusselaktører og det aktuelle trusselbildet er nødvendig for å kunne kartlegge digital risiko. Helseforetakene får informasjon om trusselbildet gjennom åpne og lukkede kilder, der trusselvurderingene til PST, E-tjenesten og NSM omtales som gode og viktige kilder. Disse trusselvurderinger har fått økt relevans for helsesektoren etter dataangrepet mot Helse Sør-Øst i 2018, fordi det viste hvilke aktører som kan være interessert i å ramme sektoren. Likevel er informasjonen om trusselbildet nokså generell i disse trusselvurderingene, og empirien viser at det fremdeles er mangelfullt grunnlag og forståelse for risikobilde i helsesektoren.

HelseCERTs oppdaterte trusselvurdering fra 2018 beskrives som en god kilde til informasjon om trusselbildet i helsesektoren, samtidig som Normen og Normkonferansen presenterer deler av trusselbildet. Jeg finner det interessant at Twitter nevnes som en god kilde til trusselbildet, og det viser at enkle tiltak som sosiale medier kan bidra i å få et mer helhetlig og oppdatert

bilde på trender og trusler innen cybersikkerhet. Ved å abonnere på internasjonale kanaler innenfor cybersikkerhet kan helsesektoren raskt få et overblikk og sette sammen et eget risikobilde, i kombinasjon med trusselvurderinger fra norske aktører. Samtidig er angrep fra avanserte trusselaktører vanskeligere å oppdage og detektere. Respons og deteksjon har vist seg som et svært viktig læringspunkt etter angrepet mot Helse Sør-Øst, der deteksjons- og respons-evnen blir beskrevet som god, men ikke god nok. Respons og deteksjon må gå fortere ved angrep, som er empirisk bevist etter angrepet mot Helse Sør-Øst.

Empirien viser at flere cybertruslene som nevnes stemmer overens med cybertruslene som presenteres i trusselvurderingene til NSM, PST, E-tjenesten og HelseCERT. Det vil si trusler som DDoS-angrep, CEO-fraud, ransomware og phising. Disse truslene er svært vanlig i helsesektoren og dukker stadig opp, men de påvirker driften i liten grad grunnet gode beskyttelsesmekanismer. Samtidig er også etterretningsoperasjoner og målrettede angrep fra avanserte trusselaktører en økende trussel i helsesektoren. HelseCERT (2018, s. 4) påpeker at det er den største trusselen i helsesektoren, men informantene mener det er urealistisk å holde en aktør som dette ute, grunnet deres ressurser, kompetanse og profesjonalitet. Trusselen beskrives som relativt usannsynlig, og det er ikke en høy prioritet å holde denne type aktør ute ettersom det krever for mer midler enn det helsesektoren har i dag.

NSM (2015a, s. 10) påpeker at trusselbildet ligger utenfor det de fleste har mulighet til å gjøre noe med, fordi man ikke vet når, hvor eller med hvilke metoder en trusselaktør vil slå til med. Derfor anbefales det at sikkerhetsarbeidet må rette fokus mot det man *kan* gjøre noe med. Det er i tråd med ny sikkerhetslov av 2019, som i større grad fokuserer på hva virksomheter kan oppnå (Regjeringen, 2018c). Dette betyr at virksomheter må identifisere verdier og interesser som kan være mål for trusselaktører, og redusere sårbarhetene som kan utnytte. I empirien kommer det frem at verdivurdering har fått mer fokus etter angrepet mot Helse Sør-Øst. Samtidig trekker NSM frem viktigheten av å oppdage angrep, men påpeker også at det stadig blir vanskelige å oppdage cyberangrep (NSM, 2015b, s. 3). Trusselaktørene blir mer avanserte i sine angrepsmetoder, og de tilpasser seg vår evne til å oppdage angrepene. Trusselaktørers evne til å utnytte mennesker, og rette angrepene mot mennesker, er derfor et problem. Det viser at denne trusselen må tas hensyn til, og at kompetansenivået i helseforetakene må økes.

Empirien viser tydelig hvordan kompleksiteten i trusselbildet har endret seg. Helseforetak tar stadig i bruk flere og komplekse systemer, verdikjedene blir stadig lengre og mer uoversiktlige, og helseforetak blir i økende grad avhengige av underleverandører. Med lange og uoversiktlige

digitale verdikjeder blir det vanskeligere å holde oversikt over alle sårbarheter, og det blir vanskelig å sørge for at alle systemer er konfigurert rett. Mange av systemene er også koblet til hverandre, og dermed avhengige av hverandre, noe som gjør at alle systemer kan falle bort ved et IKT-bortfall. Samtidig kan det være vanskelig å oppdage hvor feilen ligger. Informant Nyre fra Hemit poengterer at alle digitale systemer er satt opp på et SLA-nivå fra 1-4 (kvalitetsnivå). De fleste systemer er oppført på nivå 1 og 2, som betyr at de fleste systemer har et høyt oppetidskrav og strenge sikringstiltak. I lys av empirien er det uhensiktsmessig at alle nesten alle systemer har tilsynelatende samme SLA-nivå, da det viser at man ikke har forståelse for betydningen av nivåene og faktiske avhengighet til systemene. BIA, altså en konsekvensanalyse som kartlegger avhengigheten til IT-systemene, foreslås som en løsning. Det er viktig å forstå hva sikkerhetsnivåene innebærer og hvilke systemer som er mest kritisk.

Risiko er forbundet med usikkerhet, og informantene er enig i at risikovurderinger, ROS-analyser og verdivurderinger er gode verktøy for å analysere og kartlegge risiko, sårbarheter og verdier med hensyn til dagens trusselbilde. Verdier har vist seg særlig viktig å gjøre rede for i helsesektoren, fordi omfanget av teknologi, systemer og opplysninger kan være verdier som er interessante for trusselaktører. Nøye gjennomgang av egne verdier var et sentralt læringspunkt etter angrepet mot Helse Sør-Øst, i følge informantene fra region Sør-Øst.

Det mest sentrale som kom frem i empirien, vedrørende risikovurderinger, er at helsesektoren har en tendens til å drive negativt ladede risikovurderinger, noe som betyr at risikovurderinger måler negative konsekvenser – til tross for at nye løsninger kan ha flere positive gevinster. Som Aven (2015) er inne på i sin definisjon av risiko, kan risiko også omfatte positive konsekvenser. Samtidig er man for dårlig til å dokumentere risikovurderingene, og prosessen er ressurs-krevende og vanskelig å gjennomføre. En risikovurdering bør være reproduserbar. Det krever nøye dokumentasjon av metoden. Risikovurderinger og ROS-analyser kan være et godt verktøy når høyrisikoorganisasjoner, som helseforetak, skal kunne håndtere systemer med høy risiko. Fokus på sikkerhetsnivåenes betydning, resultater fra ROS-analyser og risikovurderinger (som blant annet setter tiltak for forebygging) kan kompensere for menneskelige svakheter. Befolkningen kan få økt tillit til helseteknologi dersom helsesektoren har dokumenterte forutsetninger for risiko av IKT-bortfall og hvordan hendelsen skal håndteres. Samtidig er deteksjon og responsevne særdeles viktig når tilsiktede uønskede hendelser først oppstår, da helseforetakene må evne å håndtere hendelsene på rett måte og på rett nivå. Dette viser igjen viktigheten av høyere fokus, rett kompetanse og gode ledelsesbeslutninger.

Når kompleksiteten i IKT-systemene i helsesektoren øker, vil sannsynligvis også sårbarhetene øke dersom man ikke klarer å redusere eller eliminere dem. En stor andel uønskede hendelser som rammer IKT-systemer er utilsiktede. Feil og avvik i IKT- systemer kan skje grunnet menneskelige feil, programvarefeil, utstyrsfeil, eller en kombinasjon. Sårbarheter deles grovt sett inn i tre kategorier: teknologiske, menneskelige og organisatoriske.

Teknologiske sårbarheter som trekkes frem er foreldet infrastruktur og systemer som ikke lar seg oppdatere – altså mangel på modernisering. Informantene fra region Sør-Øst uttrykker at foreldet infrastruktur blir vanskeligere å forvalte og drifte, noe som gjør helseforetakene sårbare for driftsforstyrrelser. Dette er på så måte en trussel mot sikkerhetsstabil drift. Samtidig er et stort antall av gamle IKT-systemer i helsesektoren ikke utviklet til å beskytte seg mot trusler fra nettet, og utgjør dermed en risiko (NOU 2015:13, s. 194). Sikkerhetsoppdateringer skal lukke sårbarheter som finnes i systemene. Ved flere tilfeller har det vist seg at helsesektoren bruker IKT-utstyr og programvarer som ikke er oppdatert, eller at helsepersonell benytter programvarer som er utenfor support, noe som skyldes både manglende IKT-investeringer og avhengighet til eldre IKT-løsninger. Dette kommer også frem i empirien.

Empirien viser at helsesektoren har flere utdaterte applikasjoner, som er laget uten hensyn til personvern eller informasjonssikkerhet, og at flere av systemene ikke lar seg oppdatere. Enkelte applikasjoner er kostbare eller vanskelig å erstatte, da helsepersonell og klinikere kan mene at det ikke finnes et alternativ som er helsemessig tilfredsstillende og forsvarlig. Informantene påpeker en interessant, og svært aktuell problemstilling, da det oppstår et beslutningsdilemma om hva som skal veie tyngst av god sporbarhet og autentisering eller best mulig helsehjelp. For at problemet skal bli løst ut fra et sikkerhetsperspektiv, kreves det at informasjonssikkerhet er organisatorisk plassert og forankret i ledelsen. Slike tilfeller krever god risikostyring, noe som også innebærer å avdekke sårbarheter og dokumentere og vite hvilke risikoer man tar.

I følge empirien fører økt bruk av underleverandører og tjenesteutsetting til lange, svake og uoversiktlige verdikjeder som kriminelle kan utnytte (HelseCERT, 2018, s. 4). Avhengighet til underleverandører og lange digitale verdikjeder er en sårbarhet i helsesektoren fordi trussel-aktører får tilgang til større angrepsflate (NOU 2015:12, s. 289). Det forsterkes av et komplekst aktørbilde der ansvaret for de ulike løsningene, produktene og verdikjedene er uoversiktlig (Hdir, 2017, s. 21). Underleverandører blir stadig flere, og de blir mål for målrettede dataangrep. Bruk av underleverandører og tjenesteutsetting er en klar sårbarhet, og Helse Sør-Øst har allerede bevist at man må være kritisk når man skal bruke eksterne leverandører. For å ivareta

sikkerheten ved tjenesteutsetting krever det at man har bestillerkompetanse og oversikt og kontroll over livsløpet, og at man tar gode risikovurderinger for å kunne ta gode beslutninger (NSM, 2018, s. 12). Samtidig må underleverandørene ha god sikkerhetskultur og samme rutiner som helsesektoren rundt opplæring og taushetsplikt. Empirien viser at helseforetakene har rutiner og krav for at underleverandører skal gjennomføre egne risikovurderinger, og det har generelt blir større skepsis til å bruke underleverandører.

Menneskene i helsesektoren er også en del av sårbarhetene. Dette knyttes både til manglende spesialistkompetanse og generell IKT-kompetanse, manglende sikkerhetsbevissthet, og evnen til å bli utnyttet av trusselaktører. Samtidig er systemenes kompleksitet en sårbarhet fordi man ser at ansatte har problemer med å forstå systemene. Menneskelige sårbarheter er noe alle virksomheter må ta stilling til, for menneskelige feil vil alltid skje – uansett om arbeidsoppgaver og systemer er automatiserte. Til syvende og sist vil det uansett være behov for menneskelig overvåkning for å kunne detektere eventuelle feil eller sårbarheter som kan lede til angrep.

Informantene fra region Midt-Norge påpeker at mennesket er helsesektorens sterkeste og svakeste ledd, og at menneskelige feil er den største sårbarheten de står ovenfor. Mange angrep starter med at mennesker lures og presses. Informantene fra region Midt-Norge og Vest påpeker at menneskelige sårbarheter håndteres ved å gjøre det vanskelig å gjøre feil som får alvorlige konsekvenser. Det vil si å sikre klientplattformen og sluttbrukerutstyret. Tilganger, muligheter og rettigheter er nøye kontrollert og styrt i alle helseforetak. Det er også tekniske tiltak som ikke-administrative brukere, kryptering av utstyr, applikasjonsblokkeringer og hvitelisting.

Informantene fra region Midt-Norge og Vest påpeker at de ikke ønsker å omtale mennesket direkte som en sårbarhet. Det vil si at de ikke ønsker å legge skylden for avvik og feil på mennesket. De er opptatt av tilgivende design, og tar alltid høyde for at menneskelige feil kan skje. Nettopp derfor settes det inn flere tekniske tiltak for å unngå store feil, og det er tilrettelagt for at det skal være så lett som mulig å gjøre rett. I Helse Vest blir avvik grunnet menneskelige feil puttet inn i et avvikshåndteringssystem, og blir fremstilt som dårlig praksis regionen kan lære av. Dette er i tråd med NSMs grunnprinsipper for IKT-sikkerhet, altså at man skal vurdere, kategorisere, kontrollere, håndtere, evaluere og lære av hendelser. I Helse sør-Øst har arbeidsforhold blitt sanksjonert fordi enkelte medarbeidere ikke er gode nok til å forholde seg til regionens sikkerhetspolicy, og enkelte nettsider er sperret. Å sperre nettsider er et enkelt, men kanskje drastisk, tiltak. Kun ved å sperre nettsider som kan eksponere ansatte og informasjon, kan helseforetakene enkelt minimere risikoen for menneskelige feil.

Empirien viser at helseforetakene kjenner til den digitale risikoen som oppstår ved den økte digitaliseringen av helsesektoren, til tross for at trusselbildet er kompleks og utfordrende å ha en fullstendig oversikt over. Risikovurderinger, sårbarhetsvurderinger og verdivurderinger har fått økt fokus i helsesektoren. Informantene understreker viktigheten av å ha oversikt over egen risiko, egne sårbarheter og egne verdier i møtet med trusselaktører som står foran dem, og det er oversikten kan gi grunnlaget for å kunne håndtere cybertruslene.

6.2 HVORDAN HÅNDTERES CYBERTRUSLENE?

Kompleksiteten i trusselbildet har endret seg, blant annet i form av flere avanserte angrep (APT) som tar lang tid å detektere og som utgjør en stor trussel. Trusler mot sikkerhetsstabil drift i helsesektoren er cyberkriminalitet som ransomware, DDoS-angrep og CEO-fraud. Slike angrep har helseforetakene gode mekanismer for å kunne håndtere, og det påvirker derfor driften i liten grad. Andre trusler er feil og avvik grunnet manglende kompetanse, manglende forankring av informasjonssikkerhet i daglig drift, underleverandører og foreldet infrastruktur.

Empirien viser at det ikke har vært en større cyberhendelse i helsesektoren enn dataangrepet som rammet Helse Sør-Øst i 2018. Samtidig var dette en svært alvorlig hendelse med store konsekvenser, der konsekvensene av angrepet ennå ikke er fullstendig gjennomgått. Det har hatt store økonomiske konsekvenser, men også en positiv konsekvens i form av økt sikkerhets-fokus i flere nivåer i sektoren. Helsesektoren har også fått økt nasjonalt fokus fra myndighetene, som ser at det er behov for bedre sikkerhet og høyere IKT-kompetanse. Slik det fremkommer i empirien, blir cybertruslene i helseforetakene håndtert ved risikostyring og risikovurderinger, bevisstgjøring av ansatte, og sikring og tilgangsstyring av systemer og rettigheter.

Alle sikkerhetstiltak må være basert på en risikovurdering, og virksomhetsledelsen må gjøre nødvendige tiltak for å sikre at risikoen er begrenset (Meld. St. 27. (2015-2016), s. 12). Risikovurderinger gjennomføres hver gang en tjeneste skal innføres eller oppdateres, og det danner et beslutningsgrunnlag for å vurdere endringen eller innføringen, og eventuelt sette inn forebyggende tiltak. Informantene er enige i at dette bidrar til å kunne håndtere cybertrusler, da det kartlegger sårbarheter og risiko. Empirien viser at dette er særlig kritisk dersom et system behandler pasientopplysninger. Trusselbildet krever en helhetlig og risikobasert tilnærming, og NSM bidrar ved å utarbeide et nasjonalt IKT-risikobilde, som er et verktøy for å utarbeide risikovurderinger. Samtidig må informasjonssikkerheten i helsevesenet ha en risikobasert tilnærming, fordi personvern og informasjonssikkerhet må være en del av utviklingen og bruken

av IKT. Empirien viser likevel at dette fører til utfordringer knyttet til personvern og sikkerhet av personsensitive opplysninger. Enkelte sikringstiltak kan komme på bekostning av personvernet. Slik det fremkommer i empirien, må informasjonssikkerheten ivaretas med utgangspunkt i oppdaterte risikovurderinger, og deretter følges opp med internkontroll.

Internkontrollen for informasjonssikkerhet og personvern i helsesektoren er beskrevet i Styringssystemet for personvern og informasjonssikkerhet. Som tidligere nevnt mener informantene at styringssystemet i høyere grad må integreres i målet om å yte god helsehjelp, og at det må operasjonaliseres i detalj i hver virksomhet. Styringssystemet bidrar likevel positivt i sikkerhetsarbeidet, blant annet med å legge føringer for prosedyrer, sanksjonering og dokumentasjon. Styringssystemet er dermed et godt verktøy for å håndtere cybertruslene, men det forutsetter at virksomhetene arbeider aktivt med å sette ansatte inn i hva styringssystemet betyr for en sikkerhetsstabil drift, slik at sikkerhet blir en større del av hverdagen i helsevesenet.

I følge empirien utgjør underleverandører en trussel fordi de er et mål for målrettede dataangrep. Dette bunner i at det stadig brukes flere underleverandører, og at digitale verdikjeder blir lengre, mer komplekse, og uoversiktlige, noe som skaper en større angrepsflate for trusselaktører. Tjenesteutsetting blir spesielt brukt i applikasjonsforvaltning og applikasjonsutvikling- og innføring. Motivene er gjerne økonomisk motiverte. Prinsipper som er viktig å ta hensyn til ved tjenesteutsetting er å hindre uvedkommende å få tilgang til informasjonen (konfidensialitet), sikre at det ikke er forfalsket informasjon (integritet) og sikre at den som skal ha informasjonen faktisk har tilgang (tilgjengelighet) (NSM, 2018b, s. 26.).

Styringssystemet bidrar til internkontroll på sikring av konfidensialitet, tilgjengelighet og integritet av ekstern og intern informasjonsbehandling. I følge NSM (ibid.) har hensynet til uautorisert tilgang (konfidensialitet) fått mest oppmerksomhet, noe som stemmer med empirien. Det er likevel viktig å ta like stort hensyn til alle prinsippene, og det må vurderes helhetlig. Tjenesteutsetting av IKT-tjenester krever grundig verdivurdering, samt riktige og gode krav til IKT-tjenesten og leverandøren, riktig beslutninger på rett nivå og gode risikovurderinger for å kunne ta gode beslutninger. Empirien viser at helsesektoren har fått økt fokus på å vurdere egne verdier. Samtidig kommer det frem at leverandører forplikter seg til å gjøre sikkerhetstiltak som lovverket krever, og at leverandørene skal gjennomføre risikovurderinger som revideres av RHF-ene. RHF-ene har prosedyrer for tilgangsstyring som sikrer at uvedkommende ikke får tilgang, og at ingen har tilgang til tjenester de ikke har behov for. Dette kontrolleres jevnlig.

Cybertrusler knyttet til mennesker og menneskelige sårbarheter håndteres ved bevisstgjøring og kurs. Informantene påpeker likevel at mennesker alltid vil gjøre feil, og det håndteres derfor med å tekniske tiltak, som applikasjonsblokkeringer. I Helse Sør-Øst er flere nettsider sperret, da de opplevde avvik. Empirien viser at sikkerhetskampanjer ikke har fungert tilstrekkelig. Helsepersonell har heller ikke forutsetninger for å ha kunnskap om cybersikkerhet. Det ligger til grunn at tilganger sperres, men i ytterste konsekvens kan rettigheter inndras og arbeidsforhold permitteres dersom ansatte ikke forholder seg til sikkerhetspolicyen. Videre jobber sikkerhetslederne kontinuerlig med å holde ansatte oppdatert på trusselbildet, og god sikkerhetskultur er en utfordring som må håndteres.

6.3 HVORDAN ER SIKKERHETSKULTUREN I HELSEFORETAKENE?

Sikkerhetsstyring kan bidra til bedre effekt av sikringstiltak og redusert risiko (St. Meld. 10 (2016-2017), s. 167). Empirien viser at god sikkerhetsstyring forutsetter opplærte og bevisste ansatte, nok ressurser til å gjennomføre arbeidet, og et styringssystem som integrerer sikkerhet i daglig drift. Det krever kompetanse, erfaring og gode verktøy. NSM mener virksomheter bør legge til rette for god sikkerhetskultur, *i tillegg* til å integrere sikkerhetsstyring i virksomhetsstyringen: «Beslutninger om sikringstiltak er ikke bare avhengig av sikkerhets- og risikoforståelse, men vil også påvirkes av den rådende sikkerhetskulturen.» (NSM, 2018b, s. 20).

En gruppes felles sett av verdier, holdninger, meninger, kompetanse og handlinger knyttet til cybersikkerhet, utgjør sikkerhetskulturen. En god og robust sikkerhetskultur preges av at dette «settet» er velutviklet og godt forankret, ved hjelp av ledelse, opplæring og rammeverk. Positiv sikkerhetskultur kjennetegnetes av at kommunikasjonen er grunnlagt på gjensidig tillit, felles oppfatninger av viktigheten av sikkerhet og tillit til effekten av forebyggende tiltak (ACSNI, 1993, sitert i Nieva & Sorra, 2003, s. 18). Nieva og Sorra (ibid.) peker på at man kan vurdere elementer som virksomhetens verdier, holdninger, bevegelser og normer, i tillegg til ledelsesmessige prioriteringer, opplæring, ressurser, retningslinjer og prosedyrer, når man skal vurdere sikkerhetskultur. Jeg skal derfor drøfte helseforetakenes sikkerhetskultur i lys av dette.

I helsesektoren er det høy bevissthet når det gjelder å sikre personvern og forholde seg til den lovpålagte taushetsplikten. Informantene beskriver sikkerhetskulturen i helseforetakene som god/nokså god og varierende. Empirien viser at sikkerhetskulturen ikke er tilstrekkelig ut fra vurderingselementene presentert av Nieva og Sorra (ibid.). For det første er holdningene til cybersikkerhet varierende. Helsepersonell har begrenset kompetanse om cybersikkerhet og

heller ikke tilstrekkelig fokus på sikkerhet, noe som blant annet har blitt bevist ved gjentatte avvik, lav oppslutning på e-læringskurs og økende etterspørsel etter tilganger de ikke har et reelt tjenstlig behov for. Helseforetakene har heller ikke nok ressurser til å kunne gjøre et tilstrekkelig og tilfredsstillende sikkerhetsarbeid, og styringssystemet mangler per i dag tilknytting til virksomhetene og virksomhetenes daglige drift. Styringssystemet er imidlertid et godt verktøy til å forenkle oppgaver og sørger for prosedyrer og forutsigbarhet.

Opplæring og bevisstgjøring om cybersikkerhet baserer seg i dag på e-læringskurs, oppsøkende virksomhet, informasjonskampanjer o.l. Dette kan være med på å styrke sikkerhetskulturen. Flere avvik skjer likevel på grunn av manglende opplæring, holdninger og årvåkenhet. Å styrke bruken av de obligatoriske e- læringskursene kan være en enkel løsning, men det krever at det settes av ressurser og tid til arbeidet. Empirien viser at kursene har hatt dårlig oppslutning, og at de repeteres hvert 2-3 år – noe informantene uttrykker som sjelden. Det digitale trusselbildet er kontinuerlig i endring, og kunnskap om cybersikkerhet er ferskvare. Dette ligger til grunn at e-læringskursene bør få strengere deltakelseskrav og økt fokus fra ledersiden, slik at det faktisk settes av tid og ressurser. Et effektivt tiltak kan også være å repetere e-læringskurset oftere. En løsning kan være sanksjonering og inndragelse av rettigheter derom kurset ikke gjennomføres, noe som har vist seg som et nyttig tiltak i Helse Sør-Øst.

Helseforetakene har per i dag ikke nok ressurser eller folk til å gjennomføre kurs for alle ansatte i helseforetakene. At sikkerhetsledere engasjerer seg i å lage informasjonsvideoer og bruke intranettet til å informere er forholdsvis enkle og lite ressurskrevende tiltak, men det krever likevel at sikkerhetslederne tar seg tid til dette – og deres ledelse gir dem mulighet til å sette av tid til dette. Empirien viser likevel at det er reelt behov for flere med IKT-kompetanse i helsesektoren. Høy IKT- kompetanse blant både ledelse og ansatte er en del av å forbedre sikkerhetskulturen.

Når det gjelder rammeverkets betydning for sikkerhetskultur, er Styringssystem for personvern og informasjonssikkerhet effektiv for å sikre forutsigbarhet i virksomheten, da det forenkler oppgaver, lager prosedyrer og sørger for dokumentasjon. Samtidig viser det til Normen, som fører krav om sikkerhetskultur, personvern og informasjonssikkerhet. Likevel viser empirien at styringssystemet mangler tilknytning til virksomheten, og per i dag er det ikke en fullkommen integrert del av virksomhetens daglige drift. Empirien viser at styringssystemet bør settes i sammenheng med helsesektorens mål om å yte god helsehjelp, spesielt i en tid der helsesektoren digitaliserer og forholdet mellom sikkerhet og personvern stadig blir mer utfordrende. En bedre forankring og forståelse for styringssystemet, både blant ledelsen, dataansvarlige, data-

behandlere og ansatte for øvrig, kan i følge empirien sikre at sikkerhetskulturen blir bedre og mer robust. Det ligger blant annet til grunn at man må operasjonalisere styringssystemet i hver enkelt virksomhet og gjøre styringssystemet til en større del av alles hverdag.

God sikkerhetskultur er lettere å skape hvis alle opplever at det er mulig å utføre arbeidet i tråd med nødvendig sikkerhet og forbyggende tiltak, krav og instrukser (Meld. st. 10 (2016-2017), s. 131). Det handler om tilrettelegging og gjennomførbarhet, opplæring og veiledning. Det bør være åpenhet om utfordringer, rapportering på uønskede hendelser og kontinuerlig læring og forbedringer. Informantene uttrykker at helsesektoren har god åpenhetskultur, og at erfaring og lærdom fra hendelser åpent deles med andre – uansett om de har gjort feil. Dette gjorde Helse Sør-Øst og Sykehuspartner etter at de ble rammet av dataangrepet i januar 2018, og det kan ses som et steg i riktig i retning når det gjelder å utvikle en sikkerhetskultur.

God sikkerhetskultur kan forebygge hendelser, men arbeid for god sikkerhetskultur krever at man øker kunnskapen og motivasjon, og endrer holdninger og atferd når det gjelder cybersikkerhet i helsesektoren. Det krever forståelse og bevissthet av at sikkerhet er viktig, noe som må prege hele virksomheten. I dette ligger det er klart ledelsesansvar, tilstrekkelig oppmerksomhet fra ledelsen, og prioriteringer. Stortinget (Meld. st. 10 (2016-2017), s. 132) fremhever at ledelsen må etablere felles forståelse av hvorfor det er viktig med forebygging og hvilke konsekvenser manglende forebygging kan få. Et virkemiddel som fremheves er å synliggjøre innsatsen i virksomheten, for eksempel ved at spørsmål om sikkerhet inngår i rapportering og resultatmål, eller at brudd og mangler innenfor forebygging inngår i ledersamtaler eller lederkontrakter. Tilsyn, veiledning og oppfølging kan også være avgjørende virkemidler. Forebygging av hendelser kan lykkes hvis det blir en integrert del av daglig drift.

Gode holdninger, nok IKT-kompetanse, høyt fokus, nok ressurser og gode verktøy, prosedyrer og retningslinjer innen cybersikkerheter komponenter som må være tilstede for å bygge en god og robust sikkerhetskultur, da dette arbeidet er tid- og ressurskrevende. Sikkerheten er per i dag ikke tilstrekkelige integrert som del av sykehusenes daglige drift, og heller ikke i den generelle kulturen. Informantene forteller at fokuset på cybersikkerhet har økt, både blant ledelsen og ansatte. Fokuset og interessen økte brått som et resultat av hendelser og fadeser i Helse Sør-Øst.

Helsesektoren er en høyrisikoorganisasjon. Gale beslutninger, feil fokus og dårlige holdninger kan få alvorlige konsekvenser dersom en krise oppstår. Helsesektoren og samfunnet forøvrig digitaliseres og utvikles, og det digitale trusselbildet øker. Før handlet sikkerheten først og fremst om å sikre fysiske komponenter. Det var noe håndfast. Slik er det ikke i dag, da

sikkerheten må ivaretas i nesten alt helsepersonell bruker i det daglige arbeidet. Derfor er sikkerhetskulturen nødt til å være en del av driften, og det burde være til alles interesse å bygge god sikkerhetskultur. Dette krever godt samvirke og samarbeid, men godt samvirke krever at tekniske, organisatoriske og menneskelige forutsetninger er til stede (Meld. st. 10 (2016-2017), s. 121). Derfor er også holdninger, kultur og ledelse viktig, ettersom det er mennesker som samvirker i virksomheter (ibid.). Samarbeid og samvirke krever forståelse og respekt for hverandres roller, ansvar, faglige bidrag, og aksept for at ulike oppgaver og perspektiver må veies opp mot hverandre. Informantene uttrykker at sistnevnte er en utfordring i dagens helsevesen, fordi cybersikkerheten ofte preges av å stå i et dilemma mellom god sikkerhet og personvern. Risikoreduserende tiltak kan stå i veien for godt personvern og beskyttelse av sensitiv informasjon. Bedre risikoforståelse, bedre beslutningsgrunnlag og økt sikkerhets-kompetanse kan være et steg i retningen mot å forbedre sikkerhetskulturen.

KAPITTEL 7: KONKLUSJON

Denne avhandlingen har besvart problemstillingen: *Hvor forberedt er norske helseforetak på cybertruslene?* Hensikten med studien har vært å undersøke cybersikkerhet, som er en stadig økende tematikk i helsesektoren. Studien har undersøkt hvilke organisatoriske kriterier som må iverksettes for å sikre god cybersikkerhet i helsesektoren, og gjennom kvalitativ datainnsamling har denne tematikken blir analysert og drøftet i lys av valgt teori.

Studiens funn viser at helseforetakene har forståelse for egen risiko og egne sårbarheter, og en økende bevissthet rundt eget trusselbilde, selv om det er manglende grunnlag for et helhetlig trusselbilde. Helsesektorens må se på nasjonale trusselvurderinger i sammenheng med egen virksomhet, og trekke ut det som er relevant. Gjennom egne risikovurderinger, basert på trusselvurderingene, oppdager helseforetakene egne sårbarheter og forbedringsområder, og de kan prioritere risikoområder og sette inn tiltak for å forhindre eller redusere risiko.

Funnene viser at helsesektoren har forstått hva som kreves for å ha god cybersikkerhet, noe som ble spesielt tydelig etter angrepet mot Helse Sør-Øst. Dette innebærer å ha kontroll på egne trusler og sårbarheter, kunnskap om egne verdier og digitalt utstyr, og at deteksjon og respons ved hendelser er viktig. Angrep kan og vil skje, og NSMs fire grunnleggende sikkerhetstiltak er det mest grunnleggende som må være på plass. Grunnprinsippene er altså et *minimumskrav*.

Diverse tiltak viser at sektoren er på vei til å få en helhetlig forankring av cybersikkerhet. Likevel er det flere svakheter ved dagens cybersikkerhet. Et sentralt poeng er at helsesektoren

mangler IKT-kompetanse og at sikkerhetskulturen er svak. Cybersikkerhet er et nokså nytt og fremmed område. Digitaliseringens raske utvikling har skapt nye og flere utfordringer knyttet til sikkerhet på nett, spesielt i helsesektoren som er svært avhengig av IKT i den daglige driften. Helsesektoren har ikke tilstrekkelig kompetanse og kunnskap om cybersikkerhet, til tross for økende fokus. Risikovurderinger må oppdateres i tråd med det rådende trusselbildet.

Trusselaktørene arbeider stadig mer målrettet og profesjonelt, noe som er en viktig årsak til å betydelig heve IKT-kompetansen, drive kontinuerlig opplæring av ansatte og utføre risiko-, verdi- og sårbarhetsvurderinger. Helsesektoren kan ikke klare å sikre seg mot dataangrep, i alle fall ikke avanserte, målrettede angrep fra statlige aktører. Det handler imidlertid om å klare å oppdage angrepene raskt nok, og håndtere det på en måte som minimerer konsekvensene.

Denne oppgaven har dermed kommet fram til følgende konklusjon: Helsesektoren er ikke forberedt på store cyberangrep fra avanserte aktører i dag, fordi de ikke har muligheten. De mangler kompetanse, ressurser, fokus og robust sikkerhetskultur. Dataangrepet mot Helse Sør-Øst har vært en viktig påminnelse om at cybersikkerhet må få økt fokus og bedre organisatorisk plassering i helseforetakene. Helsesektoren er på vei til å gi cybersikkerhet en større plassering i den daglige driften, og fokuset per i dag ligger på respons og håndtering av hendelser i det digitale rom – ikke på å stoppe angrep. Risiko-, verdi- og sårbarhetsvurderinger bidrar til at helseforetakene er bedre rustet til å håndtere cyberangrep og møte de økte cybertruslene.

7.1: FORSLAG TIL VIDERE FORSKNING

I denne studien har jeg sett på de organisatoriske forutsetningene for cybersikkerhet, og sett spesielt på sikkerhetsledelsen. Denne studien er en av få kvalitative studier som utelukkende tar for seg cybersikkerhet ved norske helseforetak, og funnene viser at det er behov for mer kvalitativ forskning innen feltet.

Ved å studere cybersikkerhet på et organisatorisk nivå, har jeg naturligvis fokusert på menneskelige og organisatoriske aspekter ved cybersikkerhet. Jeg har blant annet sett på sikkerhetskulturen, og oppdaget at sikkerhetskulturen i helsesektoren er et studiefeilt i seg selv. Et forslag til videre forskning er derfor å grave dypere i årsaken til helseforetakenes utfordringer med å etablere en robust og god sikkerhetskultur – og eventuelt se på mulige løsninger.

INTERVJUGUIDE

Bakgrunn
1. Hvilken stilling har du? (Korrekt stillingstittel)
2. Hva er din rolle og ditt ansvar?
3. Hvor mange er ansatt i denne virksomheten?
4. Hvordan er cybersikkerheten organisert?
Digitalisering
5. Hvilke typer og hvor mange digitale systemer tar dere i bruk i dag?
6. Hva er de viktigste systemene dere bruker?
7. Hvor avhengige er dere av digitale systemer?
Ledelse og cybersikkerhet
8. I hvilken grad fokuserer ledelsen på cybersikkerhet? Hvordan har dette endret seg, evt.: når så dere en markant endring?
9. Hvordan jobber ledelsen med cybersikkerhet?
10. Hvilke retningslinjer har ledelsen for sikkerhetsarbeidet i dag?
11. Hvordan bidrar styringssystemet for cybersikkerheten? Hva burde vært bedre?
12. Hvordan og hvor mye engasjerer ledelsen seg i sikkerhetsarbeidet?
13. Har dataangrepet mot Helse Sør-Øst endret fokuset på cybersikkerhet?
IKT-kompetanse og sikkerhetskultur
14. Hvordan er de ansattes IKT- og sikkerhetskompetanse? (Digitale systemer, trusselbildet, trusselaktører etc.)
15. Hvordan er sikkerhetskulturen? Hvilke utfordringer er knyttet til sikkerhetskulturen?
16. I hvilken grad er ansatte oppmerksomme på problemstillinger knyttet til personvern vs. informasjonssikkerhet?
17. Hvordan sikrer ledelsen at alle har informasjon om trusselbildet og sikkerhetstiltak?
18. Hvor viktig er det å sikre at de ansattes IKT- og sikkerhetskompetanse er god nok? Hva gjør dere med dette?
19. Hvilke tiltak har dere for å øke bevisstheten om dataangrep og digital risiko på sykehusene? Hvilke resultater gir tiltakene?
20. Har bevisstheten endret seg etter angrepet mot Helse Sør-Øst? Hvordan? Evt. når?
cyberangrep og cybertrusler
21. Er dere godt nok beskyttet mot cyberangrep i dag?
22. Har dere tiltak på plass for å agere riktig når det skjet? Hvordan agerte dere under angrep mot Helse Sør-Øst?
23. Hvordan var varslingsrutiner og informasjonsflyt under angrepet?
24. Hvilke sikkerhetstiltak satte dere i gang under angrepet?
25. Hvilke konsekvenser har dette angrepet hatt? (Økt fokus på cybersikkerhet, brukt mer ressurser på cybersikkerhet, trygghet og tillit blant ansatte og pasienter?)

26. Hva lærte dere av denne hendelsen, og hvilken effekt har dette på arbeidet med IKT sikkerhet?
27. I hvilken grad er dere forberedt på et større cyberangrep i dag? Hva er fokuset?
Trusselbildet
28. Hvordan har trusselbildet endret seg de siste årene?
29. Hvordan skaffes informasjon om trusselbildet?
30. Hva anses som den største trusselen nå? Hva ser dere for dere at kan skje?
Sårbarheter – organisatoriske, menneskelige og teknologiske
31. Hvor ofte utfører dere risikovurderinger?
32. Hva er de største sårbarhetene?
33. Hvilke krav har dere til bruk av underleverandører?
34. I hvilken grad tar helseforetaket høyde for trusler fra insidere, sabotasje og spionasje i utvikling av nye systemer? Er det satt i gang noen konkrete tiltak?
35. Hva er de største menneskelige sårbarhetene, og hvordan tar dere høyde for dette?
36. Hva er de organisatoriske sårbarhetene?
37. Hvordan kontrollerer dere hvem som får tilgang til systemer, digital infrastruktur og hvordan sikrer dere at uvedkommende ikke har tilgang?
Fremtiden
38. Hvilke endringer er det forventet at digitaliseringen kommer med, og hvordan påvirker dette trusselbildet?
39. Hva skal til for at sykehusene skal sikre seg mot cyberangrep? Hvilke planer har dere?

Vil du delta i forskningsprosjektet ”Cybersikkerhet i helsesektoren”?

Dette er et spørsmål til deg om å delta i et masterprosjekt hvor formålet er å undersøke de organisatoriske forutsetningene for cybersikkerhet i helsesektoren. I dette skrivet gir jeg deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål
Studien for seg følgende problemstilling: «*Hvor forberedt er norske helseforetak på cybertrusler?»*. Med utgangspunkt i denne problemstillingen vil jeg undersøke hvorvidt helsesektoren kjenner sine egne sårbarheter og under hvilke omstendigheter den kan forvente å bli rammet av cyberangrep.

Formålet med prosjektet er å få et innblikk i cybersikkerheten i helsesektoren, noe som blant annet innebærer å få en oversikt over trusselbildet og hvordan ledelsen ved helseforetakene arbeider med sikkerheten. Jeg skal undersøke hvorvidt helseforetakene er forberedt på å møte dagens cybertrusler, samt hvor motstandsdyktige de er mot cyberangrep.

Hvem er ansvarlig for forskningsprosjektet?
Nord Universitet (Bodø) er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?
Jeg kontakter deg fordi du sitter i ledelsen for informasjons/IKT-sikkerhet i helseforetaket.

Hva innebærer det for deg å delta?

- Hvis du velger å delta i prosjektet innebærer det at du blir intervjuet av meg.
- Intervjuet gjennomføres over telefon eller Skype, med mindre noe annet avtales.
- Intervjuet vil sannsynligvis ta minst 60 minutter.
- Intervjuet blir tatt opp med en opptaker og transkriberes i sin helhetSpørsmålene handler om digitalisering, ledelsens arbeid med IKT-sikkerhet, IKT-kompetanse, dataangrep og cybertrusler, dagens trusselbilde og sårbarheter.
    - *Jeg er innforstått med at noe informasjon rundt helseregionens arbeid med cybersikkerhet kan være konfidensiell informasjon om samfunnskritisk infrastruktur, og at det derfor kan være visse begrensninger i hvilken grad informanter kan gi informasjon om dette temaet.*

Det er frivillig å delta
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykke tilbake uten å oppgi noen grunn. Alle opplysninger om deg vil da bli anonymisert. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

- Ditt personvern – hvordan dine opplysninger blir oppbevart og brukt
- Jeg vil bare bruke opplysningene om deg til formålene jeg har fortalt om i dette skrivet. Jeg behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

- Det er kun jeg, Silje Furulund, og min veileder, Stig Ole Johannesen, ved Nord Universitet, som har tilgang til opplysningene om deg.
- Jeg tar opptak av intervjuet, men bruker en ekstern opptaker for å sikre meg mot hacking.
- Navnet og kontaktopplysningene dine vil jeg erstatte med en kode som lagres på egne navneliste adskilt fra øvrige data.
- Konfidensialitet opprettholdes ved at datamaterialet krypteres slik at ikke informasjonen kan leses av uvedkommende.

Deltakerne i denne studien skal i utgangspunkt gjenkjennes i publikasjonen. Opplysningene jeg ønsker å publisere er navn, stilling og arbeidssted.

- **Ønsker du å være anonym?** Ved behov kan du være anonym i publikasjonen – eventuelt kan enkelte opplysninger om deg anonymiseres. Dette avtales på forhånd (se samtykkeerklæring).

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?
Prosjektet skal etter planen avsluttes 15. mai 2019. Alle personopplysninger, opptak og transkripsjoner slettes ved prosjektslutt.

Dine rettigheter
Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn til sitatene dine som brukes i publikasjonen,
- innsyn i hvilke personopplysninger som er registrert om deg,
- å få rettet personopplysninger om deg,
- få slettet personopplysninger om deg, og
- få utlevert en kopi av dine personopplysninger (dataportabilitet).

Jeg behandler opplysninger om deg basert på ditt samtykke.

Hvordan kan du finne ut mer?
Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:

- Meg, Silje Furulund, på e-post (silje_furulund@hotmail.no) eller telefon: 412 69 884
- Min veileder, professor Stig Ole Johannesen, på e-post (stig.o.johannessen@nord.no) eller telefon: 920 35 007

Med vennlig hilsen

Silje Furulund
Student, Nord Universitet

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet «Cybersikkerhet i helsesektoren» og har fått anledning til å stille spørsmål. Jeg samtykker til:

- □ å delta i kvalitativt intervju
- □ at opplysninger om meg publiseres slik at jeg kan gjenkjennes
- □ at (enkelte) opplysninger om meg er anonyme i publikasjonen (kryss av nedenfor):
- □ *Navn*
- □ *Stilling*
- □ *Arbeidssted*

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet, ca. 15.05.19.

(Signert av prosjektdeltaker, dato)

REFERANSER

Litteratur og forskningsartikler:

- Aven, T. (2015) *Risk analysis.* 2. edition. UK, Wiley and sons.
- Bang, H. (2013) Organisasjonskultur: En begrepsavklaring. *Tidsskrift for norsk psykologiforening,* 50, s. 326-336. Tilgjengelig fra: https://www.traumebevisst.no/program/romforalle/filer/Organisasjonskultur.pdf [Lest 12.04.19].
- Cavelty, M. D. (2016) Cyber-security. I: Alan, C. red. *Contemporary security studies*. 4. utg. UK, Oxford University Press, s. 400-417.
- Choudhry, R. M., et. al. (2007) The nature of safety culture: A survey of the state-of-the-art. *Safety Science*, 45 (10), s. 993-1012. doi:10.1016/j.ssci.2006.09.003 [Lest 11.04.19].
- Clarke, R. & Younstein, T. (2017) Cyberattack on Britain's National Health Service – A Wake-up Call for Modern Medicine. *The New England journal of medicine*, 377 (5), s. 409-411. doi: 10.1056/NEJMp1706754 [Lest 30.10.18].
- DeJoy, D. M. (2005) Behavior change versus culture change: Divergent approaches to managing workplace safety. *Safety Science,* 43 (2), s. 105-129. doi:10.1016/j.ssci.2005.02.001 [Lest 11.04.19].
- Filkins, B. (2014) *SANS Health Care Cyberthreat Report: widespread compromises detected, compliance nightmare on horizon*. US, Norse. Tilgjengelig fra: http://www.redwoodmednet.org/projects/events/20150731/docs/Norse-SANS-Healthcare-Cyberthreat-Report2014.pdf [Lest 30.10.18].
- Fritzvold, E. (2017) *Cybersecurity in organizations.* Masteroppgave, Universitetet i Stavanger. Tilgjengelig fra: https://brage.bibsys.no/xmlui/bitstream/handle/11250/2460083/Fritzvold_Einar.pdf?sequence=1 [Lest 25.10.18].
- Fuentes, M. R & Huq, N. (2018) *Securing Connected Hospitals: A Research on Exposed Medical Systems and Supply Chain Risks*. US, Trend Micro. Tilgjengelig fra: https://documents.trendmicro.com/assets/rpt/rpt-securing-connected-hospitals.pdf?_ga=2.181707303.1240363472.1522828155-2043217583.1518166393 [Lest 25.01.19].

- Halligan, M. & Zecevic, A. (2011) Safety culture in healthcare: a review of concepts, dimensions, measures and progress. *BMJ Quality and safety*, 20 (4), s. 338-343. doi:10.1136/bmjqs.2010.040964 [Lest 04.04.19].
- Hopkins, A. (2006) *Studying Organisational Cultures and their Effects on Safety*. Canberra, Australian National University. Tilgjengelig fra: https://pdfs.semanticscholar.org/a46a/c2aa2977d7cf53871ebb9b4fb446c424f12e.pdf [Lest 12.04.19].
- Jacobsen, D. I. (2015) *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode.* 3. utg. Oslo, Cappelen Damm akademisk.
- Jewkes, Y. & Yar, M. (2010) *Handbook of Internet crime*. UK, Willan Publishing.
- Kruse, S. C. (2017) Cybersecurity in health care: A systematic review of modern threats and trends. *Technology and Health Care*, 25 (1), s. 1-10. doi:10.3233/THC-161263 [Lest 30.10.18].
- Land, T. (2018) Taking Action Against the Growing Threat of Cyberattacks in Healthcare. *Frontiers of Health Services Managment*, 35 (1), s. 1-2. doi:10.1097/HAP.0000000000000043 [Lest 30.10.18].
- Langø, H.-I. & Sandvik K. B (2013) Cyberspace og sikkerhet. *Internasjonal politikk*, 71 (2), s. 221-228. Tilgjengelig fra: https://www.idunn.no/file/pdf/60693172/cyberspace_og_sikkerhet.pdf [Lest 31.10.18].
- Langø, H.-I. (2013). Den akademiske debatten om cybersikkerhet. *Internasjonal politikk*, 71 (2), s. 229-240. Tilgjengelig fra: https://www.idunn.no/file/pdf/60693176/den_akademiske_debatten_omcybersikkerhet.pdf [Lest 31.10.18].
- Murphy, S. (2015) Is cybersecurity possible in health care? *National Cybersecurity Institute Journal*, 1 (3), s. 49-62. Tilgjengelig fra: http://publications.excelsior.edu/publications/NCI_Journal/1-3/offline/download.pdf#page=51 [Lest 29.10.18].
- Nieva, V. F. & Sorra, J. (2003) Safety culture assessment: a tool for improving patient safety in healthcare organizations. *BMJ Quality and safety*, 12 (2), s. 17-23. doi: 10.1136/qhc.12.suppl_2.ii17 [Lest 04.04.19].
- Nigris, D. J. (2014) When hacktivists target your hospital. *The New England journal of medicine*, 371 (5), s. 393-395. doi:10.1056/NEJMp1407326
- Perakslis, E. D. (2014) Cybersecurity in health care. *The New England journal of medicine*, 371 (5), s. 395-397. DOI: 10.1056/NEJMp1404358 [Lest 30.10.18].

- Ponemon Institute (2013) *Cost of data breach study: global analysis.* US, Ponemon Institute. Tilgjengelig fra: https://www.ponemon.org/local/upload/file/2013%20Report%20GLOBAL%20CODB%20FINAL%205-2.pdf [Lest 30.10.18].
- Pronovost, P. & Sexton, B. (2014) Assessing safety culture: guidelines and recommendations. *BMJ Quality and safety*, 14 (4), s. 231-233. doi: 10.1136/qshc.2005.015180 [Lest 04.04.19].
- Schjølberg, S. (2017) *Cyberkriminalitet.* Oslo, Universitetsforlaget.
- Thagaard, T. (2013) *Systematikk og innlevelse: En Innføring i kvalitativ metode.* 4. utg. Bergen, Fagbokforlaget.
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security* [Internett], 38, s. 97-102. DOI: 10.1016/j.cose.2013.04.004 [Lest 08.01.19]

Rapporter og trusselvurderinger:

- Baldwin, A. & Shiu, S. (2010) *Managing digital risk: Trends, issues and implications for business* [PDF]. UK, Lloyd's. [Lest 04.01.19].
- Baller, S., Dutta, S. & Lanvin, B. (2016) *The Global Information Technology Report 2016: Innovating in the Digital Economy.* Geneva, World Economic Forum. Tilgjengelig fra: http://www3.weforum.org/docs/GITR2016/GITR_2016_full%20report_final.pdf [Lest 02.01.19].
- Direktoratet for e-helse (2017a) *IKT-organisering i helse- og omsorgssektoren.* Oslo, Direktoratet for e-helse. Tilgjengelig fra: https://ehelse.no/Lists/Publikasjoner/Attachments/12/Rapport%20-%20IKT-organisering%20i%20helse-%20og%20omsorgssektoren.pdf [Lest 09.02.19].
- Direktoratet for e-helse (2017b) *Nasjonal e-helsestrategi 2017-2022. Oppdatert 2019.* Oslo, Direktoratet for e-helse. Tilgjengelig fra: https://ehelse.no/Documents/Nasjonale%20utvalg/NUFA/Vedlegg%202A-C%20sak%2011-17_Nasjonal%20e-helsestrategi%20og%20handlingsplan_pdf.pdf [Lest 11.11.18].
- Direktoratet for e-helse (2019) *Nasjonal e-helsestrategi 2017-2022. Oppdatert 2019.* Oslo, Direktoratet for e-helse. Tilgjengelig fra: https://ehelse.no/Documents/Nasjonal%20e-helsestrategi%20og%20handlingsplan/Nasjonal%20e-helsestrategi%202017-2022.pdf [Lest 09.02.19].

- DSB (2012) *Nasjonalt risikobilde 2012*. Oslo, Direktoratet for samfunnssikkerhet og beredskap. Tilgjengelig fra: https://www.dsb.no/globalassets/dokumenter/rapporter/nrb_2012.pdf [Lest 04.12.18].
- DSB (2014a) *Nasjonalt risikobilde 2014*. Oslo, Direktoratet for samfunnssikkerhet og beredskap. Tilgjengelig fra: http://www.dsbinfo.no/DSBno/2014/Tema/NRB2014/#/ [Lest 04.12.18].
- DSB (2014b) *Risikoanalyse av «Cyberangrep mot ekom-infrastruktur».* Oslo, Direktoratet for samfunnssikkerhet og beredskap. Tilgjengelig fra: https://www.dsb.no/globalassets/dokumenter/rapporter/risikoanalyse-av-cyberangrep-mot-ekom-infrastruktur.pdf [Lest 04.12.18].
- ENISA (2017) *ENISA Threat Landscape Report 2017: 15 Top Cyber-Threats and Trends* [PDF]. EU, The European Union Agency for Network and Information Security.
- E-tjenesten (2018) *Fokus 2018: Etterretningstjenestenes vurdering av aktuelle sikkerhetsutfordringer*. Oslo, Etterretningstjenesten. Tilgjengelig fra: https://forsvaret.no/fakta_/ForsvaretDocuments/fokus2019_web.pdf [Lest 29.09.18].
- E-tjenesten (2019) *Fokus 2019: Etterretningstjenestenes vurdering av aktuelle sikkerhetsutfordringer*. Oslo, Etterretningstjenesten. Tilgjengelig fra: https://forsvaret.no/fakta_/ForsvaretDocuments/Fokus2018_bokmaal_oppslag_godkjent.pdf [Lest 11.02.19].
- Ganguly, S. et. al. (2017) *Digital risk: Transforming risk management for the 2020.* New York, McKinsey&Company. Tilgjengelig fra: https://www.mckinsey.com/business-functions/risk/our-insights/digital-risk-transforming-risk-management-for-the-2020s [Lest 16.01.19].
- Hdir (2017) *Overordnede risiko- og sårbarhetsvurderinger i helse og omsorgssektoren.* Oslo, Helsedirektoratet. Tilgjengelig fra: https://helsedirektoratet.no/Lists/Publikasjoner/Attachments/1388/IS-2635%20Overordnede%20risiko%20og%20sarbarhetsvurderinger.pdf [Lest 16.01.19].
- HelseCERT (2018) S*ituasjonsbilde.* Trondheim, Norsk Helsenett SF. Tilgjengelig fra: https://www.nhn.no/media/1823/helsecert-situasjonsbilde-2018.pdf [Lest 10.01.19].
- Marinos, L. (2014) *ENISA Threat Landscape 2014: Overview of current and emerging cyber-threats* [PDF]. EU, The European Union Agency for Network and Information Security.
- ISACA/CMMI Institute (2018) *Cybersecurity culture report: Narrowing the culture gap for better business results.* US, ISACA og CMMI Instiute. Tilgjengelig fa: http://www.isaca.org/SiteCollectionDocuments/Cybersecurity-Culture-Report.pdf [Lest 23.03.19].

- Normen (2018) *Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten.* Versjon 5.3. Direktoratet for E-helse, Oslo. Tilgjengelig fra: https://ehelse.no/Documents/Normen/Publisering/Normen%205.3.pdf [Lest 10.01.18].
- Norsk Helsenett (2015) *Årsrapport 2015.* Trondheim, Norsk Helsenett SF. Tilgjengelig fra: https://www.nhn.no/media/1209/nhn-arsrapport-2015.pdf [Lest 09.05.19].
- NSM (2015a) *Sikkerhetsfaglig råd.* Sandvika, Nasjonal sikkerhetsmyndighet. Tilgjengelig fra: https://www.nsm.stat.no/globalassets/rapporter/nsm-sikkerhetsfaglig_raad_2015_web.pdf [Lest 10.01.18].
- NSM (2015b) *1. halvårsrapport 2015*. Sandvika, Nasjonal sikkerhetsmyndighet. Tilgjengelig fra: https://nsm.stat.no/globalassets/rapporter/nsm-rapport-1-halvaar_2015.pdf [Lest 24.01.19].
- NSM (2016) *Helhetlig IKT-risikobilde 2016*. Sandvika, Nasjonal sikkerhetsmyndighet. Tilgjengelig fra: https://nsm.stat.no/globalassets/rapporter/nsm_helhetlig_ikt_risikobilde_2016_web_enkel.pdf [Lest 15.01.19].
- NSM (2017) *Helhetlig IKT-risikobilde 2017*. Sandvika, Nasjonal sikkerhetsmyndighet. Tilgjengelig fra: https://nsm.stat.no/globalassets/helhetlig_ikt-risikobilde_2017_orig_low.pdf [Lest 15.01.19].
- NSM (2018a) *NSMs grunnprinsipper for IKT-sikkerhet*, versjon 1.1. Sandvika, Nasjonal sikkerhetsmyndighet. Tilgjengelig fra: https://nsm.stat.no/globalassets/dokumenter/nsm_grunnprinsipper_for_ikt-2018.pdf [Lest 14.01.19].
- NSM (2018b) *Risiko 2018.* Sandvika, Nasjonal sikkerhetsmyndighet. Tilgjengelig fra: https://nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2018_web.pdf [Lest 13.11.18].
- NSM (2018c) *Et sikkert digitalt samfunn: IKT-risikobilde 2018*. Sandvika, Nasjonal sikkerhetsmyndighet. Tilgjengelig fra: https://nsm.stat.no/globalassets/rapporter/nsm_ikt-risikobilde_2018_web.pdf [Lest 15.01.19].
- Omerovic, A. & Gjære, E. A. (2015) *Digitale sårbarheter i helsesektoren.* Oslo, SINTEF IKT. Tilgjengelig fra: https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/sved/6.pdf [Lest 12.11.18].
- PST (2017) *Trusselvurdering 2017.* Oslo, Politiets sikkerhetstjeneste. Tilgjengelig fra: https://pst.no/trusselvurdering-2017/ [Lest 13.11.18].

- PST (2018a) *Trusselvurdering 2018.* Oslo, Politiets sikkerhetstjeneste. Tilgjengelig fra: https://www.pst.no/globalassets/artikler/trusselvurderinger/psts-trusselvurdering-2018.pdf [Lest 13.11.18].
- PST (2019) *Trusselvurdering 2019.* Oslo, Politiets sikkerhetstjeneste. Tilgjengelig fra: https://pst.no/globalassets/artikler/trusselvurderinger/psts-trusselvurdering-2019.pdf [Lest 04.02.2019].
- Regjeringen (2017) *Internasjonal cyberstrategi for Norge: fastsatt 27. september 2017 av Utenriksdepartementet.* Oslo, Utenriksdepartementet. Tilgjengelig fra: https://www.regjeringen.no/globalassets/departementene/ud/dokumenter/sikpol/cyberstrategi_web.pdf [Lest 10.10.18].
- Regjeringen (2019) *Nasjonal strategi for digital sikkerhetskompetanse.* Oslo, Justis- og beredskapsdepartementet. Tilgjengelig fra: https://www.regjeringen.no/contentassets/8ed748d37e504a469874ce936551b4f8/nasjonal-strategi-for-digital-sikkerhetskompetanse.pdf [Lest 02.01.19].
- Ringard, Å. et. al. (2014) *Det norske helsesystemet 2013.* Rapportnr. 15 (18). Oslo, Folkehelseinstituttet. Tilgjengelig fra: https://www.fhi.no/globalassets/dokumenterfiler/rapporter/2014/hit-det-norske-helsesystemet-2013 [Lest 07.02.19].
- World Economic Forum (2012) *Global Risks 2012.* 7th edt. Sveits, World Economic Forum. Tilgjengelig fra: http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf [Lest 22.11.18].

Melding til Stortinget:

- Meld. St. 9 (2012-2013) (2013) *Én innbygger – én journal*. Oslo, Helse- og omsorgs-departementet. Tilgjengelig fra: https://www.regjeringen.no/contentassets/33a159683925472aa15ad74f27ad04cc/no/pdfs/stm201220130009000dddpdfs.pdf [Lest 18.10.18].
- Meld. St. 10 (2016-2017) (2017) *Risiko i et trygt samfunn: samfunnssikkerhet.* Oslo, Justis- og beredskapdepartementet. Tilgjengelig fra: https://www.regjeringen.no/contentassets/00765f92310a433b8a7fc0d49187476f/no/pdfs/stm201620170010000dddpdfs.pdf [Lest 11.01.19].
- Meld. St. 27 (2015-2016) (2016*) Digital agenda for Norge: IKT for en enklere hverdag og økt produktivitet*. Oslo, Kommunal- og moderniseringsdepartementet. Tilgjengelig fra:

https://www.regjeringen.no/contentassets/fe3e34b866034b82b9c623c5cec39823/no/pdfs/stm201520160027000dddpdfs.pdf [Lest 07.11.18]

- Meld. St. 38 (2016-2017) (2017) *IKT-sikkerhet – Et felles ansvar*. Oslo, Justis- og beredskapsdepartementet. Tilgjengelig fra: https://www.regjeringen.no/no/dokumenter/meld.-st.-38-20162017/id2555996/sec1 [Lest 18.10.18].

Proposisjoner til Stortinget:

- Ot. prp. nr. 66 (2000-2001) *Om lov om helseforetak m.m. (helseforetaksloven)*. Oslo, Sosial- og helsedepartementet. Tilgjengelig fra: https://www.regjeringen.no/contentassets/15a4b853c7be45fb8d432b109b782961/no/pdfa/otp20002000100660000dddpdfa.pdf [Lest 07.02.19].
- Prop. 153 L (2016-2017) *Om lov om nasjonal sikkerhet (sikkerhetsloven)*. Oslo, Forsvarsdepartementet. Tilgjengelig fra: https://www.regjeringen.no/contentassets/0fcee45affd24280896b88b5413a00aa/no/pdfs/prp201620170153000dddpdfs.pdf [Lest 14.02.19].

Offentlige utredninger:

- NOU 2015:13 (2015) *Digital sårbarhet – sikkert samfunn*. Oslo, Departementenes sikkerhets- og serviceorganisasjon, Informasjonsforvaltning. Tilgjengelig fra: https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf [Lest 30.11.18].
- NOU 2016:19 (2016) *Samhandling for sikkerhet.* Oslo, Departementenes sikkerhets- og serviceorganisasjon, Informasjonsforvaltning. Tilgjengelig fra: https://www.regjeringen.no/contentassets/03960058f3f94fbe9d290593bee22c1a/no/pdfs/nou201620160019000dddpdfs.pdf [Lest 14.02.19].
- NOU 2016:26 (2016) *Organisering og styring av spesialhelsetjenesten.* Oslo, Departementenes sikkerhets- og serviceorganisasjon, Informasjonsforvaltning. Tilgjengelig fra:https://www.regjeringen.no/contentassets/6db6ac4fbfde49e6bc5f8bd615c6fa1e/no/pdfs/nou201620160025000dddpdfs.pdf [Lest 07.02.19].
- NOU 2018:14 (2018) *IKT-sikkerhet i alle ledd. Organisering og regulering av nasjonal IKT.* Oslo, Departementenes sikkerhets- og serviceorganisasjon, Informasjonsforvaltning. Tilgjengelig fra:

https://www.regjeringen.no/contentassets/0d408600df2f4738a9bbb85040b02b59/no/pdfs/nou201820180014000dddpdfs.pdf [Lest 14.02.19].

Lover og forskrifter:

- Forskrift om behandling av personopplysninger (2018) *Forskrift om behandling av personopplysninger av 15. juni 2018 nr. 876.* Tilgjengelig fra: https://lovdata.no/dokument/SF/forskrift/2018-06-15-876 [Lest 12.02.19].
- Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten (2017) *Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten av 28. oktober 2017 nr. 1250.* Tilgjengelig fra: https://lovdata.no/dokument/LTI/forskrift/2016-10-28-1250 [Lest 04.04.19].
- Forskrift om IKT-standarder i helse og omsorg (2015) *Forskrift om IKT-standarder i helse- og omsorgs-tjenesten av 9. september 2015 nr. 853*. Tilgjengelig fra: https://lovdata.no/dokument/SF/forskrift/2015-07-01-853 [Lest 12.02.19].
- Helsepersonelloven (1999) *Lov om helsepersonell m.v. av 2. juli 1997 nr. 64.* Tilgjengelig fra: https://lovdata.no/dokument/NL/lov/1999-07-02-64?q=helsepersonelloven [12.02.19].
- Klareringsforskriften (2018) *Forskrift om sikkerhetsklarering og annen klarering av 1. juni 2018 nr. 2054.* Tilgjengelig fra: https://lovdata.no/dokument/SF/forskrift/2018-12-20-2054 [Lest 12.02.19].
- Pasientjournalloven (2014) *Lov om behandling av helseopplysninger ved ytelse av helsehjelp av 20. juni 2014 nr. 42.* Tilgjengelig fra: https://lovdata.no/dokument/NL/lov/2014-06-20-42?q=pasientjournalloven [Lest 12.02.19].
- Personopplysningsloven (2018) *Lov om behandling av personopplysninger av 15. juni 2018 nr. 38.* Tilgjengelig fra: https://lovdata.no/dokument/NL/lov/2018-06-15-38/ [Lest 12.02.19].
- Sikkerhetsloven (2018) *Lov om nasjonal sikkerhet av 1. juni 2018 nr. 24.* Tilgjengelig fra: https://lovdata.no/dokument/NL/lov/2018-06-01-24 [Lest 12.02.19].
- Virksomhetsforskriften (2018) *Forskrift om virksomheters arbeid med forebyggende sikkerhet av 20. desember 2018 nr. 2053.* Tilgjengelig fra: https://lovdata.no/dokument/SF/forskrift/2018-12-20-2053 [Lest 12.02.19].

Internettressurser:

- Bratbergsengen, K. (2017) Digitalisering. I: Store Norske leksikon [Internett]. Tilgjengelig fra: https://snl.no/digitalisering#-Digital_publisering [Lest: 05.11.18].

- Brudvik, M. (2010) *ROS-analyse.* 22. oktober. Oslo, Helsebiblioteket. Tilgjengelig fra: https://www.helsebiblioteket.no/kvalitetsforbedring/metoder-og-verktoy/ros-analyse [Lest 03.03.19].
- Datatilsynet (2018a) *Iverksette styringssystem for informasjonssikkerhet.* 23. juni. Oslo, Datatilsynet. Tilgjengelig fra: https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/internkontroll-og-informasjonssikkerhet/iverksette-styringssystem-for-informasjonssikkerhet/ [Lest 09.04.19].
- Datatilsynet (2018b) *Om personopplysningsloven med forordning og når den gjelder.* 4. september. Tilgjengelig fra: https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/om-personopplysningsloven-og-nar-den-gjelder/ [Lest 12.02.19].
- Difi (u.å.) *Hva er risikovurdering?* Oslo, Direktoratet for forvaltning og IKT. Tilgjengelig fra: https://internkontroll-infosikkerhet.difi.no/risikostyring/risikovurdering [Lest 09.04.19].
- Difi (u.å.) *Helhetlige metoder.* Oslo, Direktoratet for forvaltning og IKT. Tilgjengelig fra: https://internkontroll-infosikkerhet.difi.no/risikovurdering/godt-vite/helhetlige-metoder [Lest 09.04.19].
- Difi (2019) *Internkontroll/styringssystem/ledelsessystem for informasjonssikkerhet.* 30. januar. Oslo, Direktoratet for forvaltning og IKT. Tilgjengelig fra: https://www.difi.no/referansekatalogen/internkontroll-styringssystem-ledelsessystem-informasjonssikkerhet#krav [Lest 09.04.19].
- Direktoratet for e-helse (2018) *Styringssystem for informasjonssikkerhet.* 16. oktober. Oslo, Direktoratet for e-helse. Tilgjengelig fra: https://ehelse.no/Documents/Normen/Faktaark%2002%20-%20Styringssystem%20for%20informasjonssikkerhet.pdf [Lest 09.04.19].
- DSB (2017) *Temaveiledning i risikoanalyse for risikofylte forbrukertjenester.* Oslo, Direktoratet for samfunnssikkerhet og beredskap. Tilgjengelig fra: https://www.dsb.no/lover/produkter-og-forbrukertjenester/veiledning-til-forskrift/temaveiledning-i-risikoanalyse/#risikofylte-forbrukertjenester [Lest 03.03.19].
- Muller, L. P & Strand, S. (2016) *Kampen mot cyberterrorisme*. 18. april. Oslo, NUPI. Tilgjengelig fra: https://www.nupi.no/Nyheter/Kampen-mot-cyberterrorisme [Lest 27.09.18].
- Muller, L. P & Schia, N. N. (2017) *Et usikkert nett av ting.* 24. mars. Oslo, NUPI. Tilgjengelig fra: https://www.nupi.no/Nyheter/Et-usikkert-nett-av-ting [Lest 27.09.18].

- Norsk Helsenett (2015) *Nasjonalt kompetanseforum for IKT-sikkerhet i helse- og omsorgssektoren.* 18. oktober. Trondheim, Norsk Helsenett SF. Tilgjengelig fra: https://www.nhn.no/nasjonalt-kompetanseforum-for-ikt-sikkerhet-i-helse-og-omsorgssektoren/ [Lest 10.01.19].
- Norsk Helsenett (u.å.) *HelseCERT.* Trondheim, Norsk Helsenett SF. Tilgjengelig fra: https://www.nhn.no/helsecert/ [Lest 10.01.19].
- NHO (2018) Digitalisering. I: *Verden og oss. Næringslivets perspektivmelding 2018.* 3. utgave. Oslo, Næringslivets Hovedorganisasjon. Tilgjengelig fra: https://www.nho.no/publikasjoner/p/naringslivets-perspektivmelding/digitalisering/ [Lest 10.01.18].
- NSM (2014) *Sikkerhetskultur.* 15. mai. Sandvika, Nasjonal sikkerhetsmyndighet. Tilgjengelig fra: https://www.nsm.stat.no/om-nsm/tjenester/sikkerhetsstyring/sikkerhetskultur/ [Lest 01.04.19].
- PST (2018b) *PST innstiller etterforskningen av datainnbruddet i Helse Sør-Øst og Sykehuspartner*. 4. desember. Oslo, Politiets sikkerhetstjeneste. Tilgjengelig fra: https://pst.no/alle-artikler/pressemeldinger/pst-innstiller-etterforskningen-av-datainnbruddet-i-helse-sor-ost-rhf-og-sykehuspartner-hf/ [Lest 02.01.2019].
- Regjeringen (2014) *Departementenes eierstyring av de regionale helseforetakene.* 30. oktober. Oslo, Helse- og omsorgsdepartementet. Tilgjengelig fra: https://www.regjeringen.no/no/tema/helse-og-omsorg/sykehus/vurderes/departementets-eierstyring-av-de-regiona/id226148/ [Lest 07.02.19].
- Regjeringen (2014) *Digitalisering i offentlig sektor.* 16. desember. Oslo, Kommunal- og moderniseringsdepartementet. Tilgjengelig fra: https://www.regjeringen.no/no/tema/statlig-forvaltning/ikt-politikk/digitaliseringen-i-offentlig-sektor/id2340245/ [Lest 13.11.18].
- Regjeringen (2018a) *Statsbudsjettet 2019: Tidenes største satsning på digitalisering*. 8. oktober. Oslo, Kommunal- og moderniseringsdepartementet. Tilgjengelig fra: https://www.regjeringen.no/no/aktuelt/tidenes-storste-satsing-pa-digitalisering/id2614074/ [Lest 27.10.18].
- Regjeringen (2018b) *Statsbudsjettet: Bedre IKT-sikkerhet – skjerpet innsats mot hybride trusler og cybertrusler.* 8. oktober. Oslo, Justis- og beredskapsdepartementet. Tilgjengelig fra: https://www.regjeringen.no/no/aktuelt/bedre-ikt-sikkerhet--skjerpet-innsats-mot-hybride-trusler-og-cybertrusler/id2614229/ [Lest 17.02.19].
- Regjeringen (2018c) *Ny sikkerhetslov skal gjøre Norge tryggere.* 20. desember. Oslo, Forsvarsdepartementet. Tilgjengelig fra: https://www.regjeringen.no/no/aktuelt/ny-sikkerhetslov/id2623522/ [Lest 11.02.19].
- Tønseth, S. (2017) *Medisinsk utstyr kan hackes.* 20. januar. Oslo, SINTEF. Tilgjengelig fra: https://www.sintef.no/siste-nytt/medisinsk-utstyr-kan-hackes/ [Lest 04.12.18].

Artikler i nettaviser:

- Didriksen, N. (2018) Pasientsystem fremdeles stengt etter datainnbrudd på sykehus. *NRK*, 22. januar. Tilgjengelig fra: https://www.nrk.no/ostlandssendingen/pasientsystem-fremdeles-stengt-etter-datainnbrudd-pa-sykehus-1.13879494 [Lest 30.10.18].
- Flaarønning, G. (2018) Utelukker ikke at pasientdata har kommet på avveie. *NRK*, 18. januar. Tilgjengelig fra: https://www.nrk.no/norge/listhaug-og-hoie-svarer-pressen-om-dataangrepet-om-helse-sor-ost-1.13873526 [Lest 30.10.18].
- Hotvedt, S. K. (2017*)* Hackere lammer datasystemer på sykehus. *NRK*, 12. mai. Tilgjengelig fra: https://www.nrk.no/urix/dataangrep-lammer-it-systemer-pa-sykehus-1.13514766 [Lest 27.10.18].
- Klungtveit, H. S. (2018) E-tjenesten frykter at Kina hacket pasientinfo om 2,9 millioner nordmenn. *Filternyheter*, 9. mars. Tilgjengelig fra: https://filternyheter.no/kinesere-hacket-helse-sor-ost-e-tjenesten-frykter-at-pasientinfo-om-29-millioner-nordmenn-er-stjalet/ [lest 30.10.18].
- Mordt, H. & Neumann, C. (2018) Innbrudd i datasystemene til Helse Sør-Øst. *NRK*, 18. januar. Tilgjengelig fra: https://www.nrk.no/ostlandssendingen/innbrudd-i-datasystemene-til-helse-sor-ost-1.13866765 [Lest 30.10.18].
- Perlroth, N. & Sanger. D. E. (2017) Hackers hit dozen of countries exploiting stolen N.S.A. tool. *New York Times*, 12. mai. Tilgjengelig fra: https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html [Lest 30.10.18].
- Zetter, K. (2016) Why hospitals are the perfect targets for ransomware. *Wired*, 30. mars. Tilgjengelig fra: https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/ [Lest 17.01.19].