FFI-RAPPORT

20/01560

Håndtering av IKT-sikkerhetshendelsene i Helse Sør-Øst og fylkesmannsembetene

– en vurdering

Janita A. Bruvoll
Aasmund Thuv
Geir Enemo

Håndtering av IKT-sikkerhetshendelsene i Helse Sør-Øst og fylkesmannsembetene – en vurdering

Janita A. Bruvoll
Aasmund Thuv
Geir Enemo

Forsvarets forskningsinstitutt (FFI) 3. juni 2020

Emneord
IKT-sikkerhet
Hendelseshåndtering
Krisehåndtering

FFI-rapport
20/01560

Prosjektnummer
534501

Elektronisk ISBN
978-82-464-3274-8

Engelsk tittel
An assessment of ICT incident management related to the Norwegian Southern and Eastern Health region and County Governor Offices.

Godkjennere
Ann Kristin Elstad, *forskningsleder*
Janet M. Blatny, *forskningsdirektør*

Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur.

Sammendrag

I dag er de aller fleste samfunnsfunksjoner, virksomheter og individer i større eller mindre grad avhengig av digitale tjenester. Anvendelsen av IKT gir oss mulighet til å effektivisere prosesser og tjenester som brukes i hverdagen, men medfører også økt risiko for å bli utsatt for uønskede hendelser i det digitale rom. Slike hendelser kan være alt fra mindre svindelforsøk til omfattende dataangrep gjennomført av avanserte trusselaktører, med hensikt å samle informasjon, sabotere tjenesteproduksjon eller ramme styringsevnen til sentrale virksomheter eller myndigheter.

I 2018 ble både helsesektoren og fylkesmannsembetene rammet av IKT-angrep. Hendelsene var omfattende og krevde at mange aktører bidro i håndteringen. Forsvarets forskningsinstitutt (FFI) har fått i oppdrag av Justis- og beredskapsdepartementet å evaluere håndteringen av hendelsene. Evalueringen skal kartlegge hendelsesforløp og involverte aktører, ta utgangspunkt i samfunnssikkerhetsinstruksen og rammeverk for håndtering av IKT-sikkerhetshendelser, og anbefale videre utvikling av sistnevnte. Til sist skal FFI komme med læringspunkter og anbefalinger til hva som bør øves på i øvelse Digital 2020. For å løse oppdraget har FFI i all hovedsak basert seg på intervjuer med de involverte aktørene i kombinasjon med dokumentstudier og erfaringen forskerne har innenfor krisehåndtering og IKT.

Begge hendelsene framstår som datainnbrudd hvor avanserte trusselaktører har vært ute etter informasjon, og forsøkt å operere skjult. Hendelsene ble oppdaget relativt raskt, og hendelsen som rammet helsesektoren hadde betydelig større omfang når det gjelder både rammede aktører og systemer enn hendelsen som rammet fylkesmannsembetene. Funnene viser at få aktører var forberedt på hendelser av et slikt omfang og hadde i liten grad oversikt over egne verdier, sårbarheter og systemer.

Samfunnssikkerhetsinstruksen retter seg mot departementene, mens rammeverket retter seg mot aktørene NSM NorCERT, sektorvise responsmiljø og virksomheter. FFI finner ingen uoverens-stemmelser mellom dokumentene. Imidlertid gir disse et lite helhetlig bilde av aktørene som er relevante for håndteringen av IKT-sikkerhetshendelser. Særlig sentrale samordningsaktører som Direktoratet for samfunnssikkerhet og beredskap (DSB) savnes. Instruksen og rammeverket gir et godt utgangspunkt for å få en felles forståelse av fagbegreper, enkelte roller og ansvar, men løser ikke det FFI peker på som den største svakheten når det gjelder IKT-sikkerhetshendelser – nemlig forebygging, forberedelser og oversikt over egne verdier, sårbarheter og systemer. Det bør vurderes å utarbeide veiledere på dette punktet for henholdsvis små, mellomstore og større virksomheter.

Øvelse Digital 2020 skal etter planen ikke øve det tekniske personellet. FFI mener likevel at den tekniske dimensjonen bør ivaretas slik at sammenhengen mellom det som skjer på teknisk nivå og videre beslutninger knyttet til håndtering blir belyst og øvd. Deltakerne bør utfordres på informasjonsdeling – både når det gjelder ulike typer informasjon og mottakergrupper. I tillegg bør det legges til rette for at operative konsekvenser for øvingsdeltakerne vurderes og at ressursallokering på sentralt nivå, SRM-nivå og virksomhetsnivå øves.

Summary

Today, most societal functions, enterprises and individuals are to some degree dependent on digital services. The use of ICT enables us to improve much used processes and services, but it also increases the risk of being affected by malicious cyber incidents. Such incidents may range from small fraud attempts to comprehensive cyber attacks by advanced threat actors. The rationale may for instance be to obtain information, sabotage services or impact the governance ability of enterprises or governments.

In 2018, both the health sector and the county governors were hit by ICT incidents. The incidents were extensive, requiring the contributions of many actors in response. The Norwegian Defence Research Establishment (FFI) has been given the task by the Ministry of Justice and Public Security to evaluate the response to both incidents. The evaluation should map the course of events and the response actors involved, make use of the national Instructions for the Ministries' work with Societal Safety and the Framework for management of cyber incidents, and make recommendations for the development of the latter. Finally, FFI shall identify lessons learned and make recommendations for exercise Digital 2020. In order to solve this task, FFI has conducted interviews with involved actors, studied relevant documents and utilized the experience of researchers of crisis management and ICT.

The incidents appear to be data breaches with advanced threat actors covertly seeking information. They were both discovered relatively quickly. The incident in the health sector was considerably larger in terms of the actors and size of the systems hit. Findings from both incidents show that few actors where prepared for events of such magnitude, and had limited overview of their own values, vulnerabilities and systems.

Instructions for the Ministries' work with civil protection and emergency preparedness is directed towards ministries, while the Framework is directed towards NSM NorCERT, sectorwide response entities (SRMs) and enterprises. There are no inconsistencies in these documents, but they do not on their own give the whole picture of the actors involved in national crisis response (including larger ICT incidents). Significant actors like the Directorate for Civil Protection (DSB) and the County Governor are not included in the Framework, which they should be. The Instruction and the Framework give a good starting point for a common understanding of technical terms, roles and responsibilities. They do not solve what FFI considers the greatest weakness in ICT incidents – prevention, preparedness and overview of own values, vulnerabilities and systems. Guidance on this for small and medium-sized, and larger enterprises, respectively, should be considered.

The technical dimension should be taken into account during exercise Digital 2020. This holds true even if technical personnel is not participating. All participants should be challenged on sharing different types of information with different target audiences, ensure that operational consequences for the exercising actors are assessed, and that resource allocation are exercised for the strategic level, the SRM level and the enterprise level.

Innhold

Sammendrag **3**

Summary **4**

Forord **7**

1 Innledning **9**
1.1 Om oppdraget 9
1.2 Forskningsspørsmål 10
1.3 Avgrensning 10
1.4 Begreper og kortformer 11
1.5 Rapportens oppbygning 12

2 Metodiske betraktninger **13**
2.1 Framgangsmåte for å løse oppdraget 13
2.2 Intervjuer og gjennomgang av skriftlige kilder 14
2.3 Vurdering av hendelsene og håndteringen 16
2.4 Valget om å ikke identifisere informantene 17
2.5 Usikkerhetsfaktorer knyttet til framgangsmåten 17
2.6 Utfordringer knyttet til informasjonstilfang 17
2.7 Utfordringer knyttet til gradert informasjon 18
2.8 Troverdighet og pålitelighet i studien 19

3 Krisehåndtering, IKT og organisering **20**
3.1 Rammeverk og instruks 20
3.2 Krisehåndtering 21
3.3 Nasjonal krisehåndtering og relevante roller og aktører 23

4 Hendelse HSØ **29**
4.1 Hendelsesforløpet 29
4.2 Erfaringer knyttet til håndteringen av hendelsen 33

5 Hendelse FM **37**
5.1 Hendelsesforløpet 37
5.2 Erfaringer knyttet til håndteringen av hendelsen 39

6 Krisehåndtering i henhold til rammeverk og instruks 42
6.1 Rammeverk for håndtering av IKT-sikkerhetshendelser 42
6.2 Instruks for departementenes arbeid med samfunnssikkerhet 46

7 Vurdering 47
7.1 Hendelsenes karakter 47
7.2 Håndteringens mangfold 49
7.3 Hendelsenes egenart og overføringspotensial 51
7.4 Spesifikke forhold ved hendelse HSØ 53
7.5 Spesifikke forhold ved hendelse FM 54

8 Betraktninger om rammeverk og instruks 58
8.1 Rammeverk 58
8.2 Instruks 60
8.3 Uoverensstemmelser mellom rammeverk og instruks 61

9 Mulige øvingspunkter til Digital 2020 63
9.1 Generelle vurderinger 63
9.2 Informasjonsdeling 64
9.3 Operative konsekvenser 65
9.4 Sentral ressursallokering 65

10 Konklusjon 67
10.1 Kartlegging og vurdering av håndtering med utgangspunkt i rammeverk og instruks 67
10.2 Kartlegging og dokumentering av eventuelle utfordringer eller motstridende elementer mellom rammeverk og instruks 69
10.3 Vurdering om hvorvidt rammeverk og instruks er tilstrekkelig, og eventuelt anbefale videreutvikling av disse for å bedre samfunnets evne til å håndtere hendelser 69

11 Avsluttende betraktninger 71

Forkortelser 73

Referanser 75

Forord

Forfatterne av denne rapporten ønsker først og fremst å takke Justis- og beredskaps-departementet for muligheten og tilliten til å arbeide med dette oppdraget. Vi vil også rette en stor takk til informantene som har bidratt til informasjon og erfaring fra hendelsene, som har dannet utgangspunktet for vår forståelse og vurderinger.

Kjeller, 28. mai 2020

Janita A. Bruvoll, Aasmund Thuv og Geir Enemo

1 Innledning

De fleste virksomheter i dag anvender IKT[1]-systemer til en rekke ulike formål. Mulighetene som ligger i å bruke IKT, og å kommunisere og samvirke med andre virksomheter digitalt, er mange. En virksomhet vil ofte være både produsent og konsument av digitale tjenester, med eksponering av enkelte systemer mot internett og med internett som en underliggende kommunikasjonsbærer. Med disse mulighetene kommer også en økt risiko for å bli angrepet i det digitale rom. En rekke type aktører benytter internett til å angripe virksomheter eller for å ramme enkeltpersoner, hvor underliggende motivasjon kan spenne fra anerkjennelse gjennom hærverk og ugagn til økonomisk vinning, politisk protest, påvirkning, innsamling av etterretning og understøttelse av militære operasjoner.

Alle virksomheter tilknyttet internett kan rammes av skadevare og annen ondsinnet aktivitet i det digitale rom. Noen ganger er det en grad av tilfeldighet i hvilke virksomheter som rammes, for eksempel ved at en angriper sender ut e-postmeldinger i stort omfang eller gjennomfører automatiserte angrepsforsøk som treffer mange virksomheter. Andre ganger blir en spesifikk virksomhet valgt ut, og angrepet tilpasset deretter. Avhengig av den underliggende motivasjonen vil en angriper kunne søke å oppnå ulike former for virkninger i virksomhetens IKT-systemer, for eksempel tyveri av informasjon, endring av opplysninger eller nedstenging av IKT-tjenester. Enkelte ganger kan følgekonsekvenser for virksomhetens evne til leveranser, som degradering eller stans av vareproduksjon, være målet.

Håndteringen av IKT-angrep kan være en privatsak i de enkleste tilfellene, mens det kan eskalere til å være et nasjonalt anliggende med strategiske konsekvenser som kan ramme både stats- og samfunnssikkerhet. Dette avhenger av en rekke faktorer, blant annet hvilken virksomhet som er rammet, hvilke verdikjeder virksomheten er en del av, målsystemets kompleksitet, angripers evne og vilje samt hvilken aktør som står bak. Hvilke mekanismer som utløses i forbindelse med håndtering av en hendelse kan derfor variere stort, og det kan være utfordrende for alle involverte å arbeide og samvirke optimalt når kompleksiteten og usikkerheten ved en hendelse er betydelig. Av den grunn er evaluering og læring etter større hendelser et nyttig virkemiddel for å bli bedre forberedt på framtidige hendelser.

1.1 Om oppdraget

Justis- og beredskapsdepartementet (JD) har gitt Forsvarets forskningsinstitutt (FFI) i oppdrag å utarbeide en overordnet evaluering av håndteringen av to IKT-sikkerhetshendelser. Den ene hendelsen omfattet et IKT-angrep i 2017–2018 mot systemene til Sykehuspartner helseforetak (HF), som er underlagt Helse Sør Øst regionalt helseforetak (HSØ RHF). Den andre hendelsen omfattet et IKT-angrep mot fylkesmannsembetene (FM) i 2018.

[1] Informasjons- og kommunikasjonsteknologi

Formålet med dette arbeidet er å få kunnskap som kan bedre samfunnets evne til å håndtere IKT-sikkerhetshendelser og konsekvensene av disse. Funn fra arbeidet skal bidra til å videreutvikle rammeverk og gi innspill til Øvelse Digital 2020. Arbeidet skal ta utgangspunkt i *Rammeverket for IKT-sikkerhetshendelser* (NSM, 2017) og *Samfunnssikkerhetsinstruksen* (JD, 2017).

Arbeidet skal:

- Kartlegge IKT-sikkerhetshendelsene hos helseregion Helse Sør-Øst og fylkesmannsembetene og vurdere hvordan håndteringen ble utført med utgangspunkt i Rammeverk for håndtering av IKT-sikkerhetshendelser og del VIII i Samfunnssikkerhetsinstruksen.

- Kartlegge og dokumentere eventuelle utfordringer eller motstridende elementer i Rammeverket for håndtering av IKT-sikkerhetshendelser og Samfunnssikkerhetsinstruksen

- Vurdere hvorvidt Rammeverket for håndtering av IKT-sikkerhetshendelser og Samfunnssikkerhetsinstruksen er tilstrekkelig og eventuelt anbefale videreutvikling av disse for å bedre samfunnets evne til å håndtere IKT-sikkerhetshendelser.

Oppdragsgiver ønsket en ugradert rapport, med mulighet for eventuelle graderte vedlegg.

1.2 Forskningsspørsmål

Et sett forskningsspørsmål ble utarbeidet for å besvare oppdraget:

1. Hva var hendelsesforløpet i de to hendelsene?

2. Hvilke aktører ble involvert i krisehåndteringen, og hvordan ble krisehåndteringen utført?

3. Hva kan vi lære av håndteringen av hendelsene?

4. Hvilken innvirkning hadde rammeverk for håndtering av IKT-sikkerhetshendelser og samfunnssikkerhetsinstruksen i håndteringen av hendelsene?

5. Hva bør øves på i øvelse Digital 2020?

1.3 Avgrensning

Arbeidet inkluderer kun de to IKT-sikkerhetshendelsene definert av JD i oppdragsbeskrivelsen, herunder angrepet mot HSØ RHF og fylkesmannsembetene. Det er håndtering av hendelsene, og ikke etterforskning, som er tema for oppdraget. Videre vil arbeidet ikke søke å karaktersette innsatsen til de individuelle involverte aktørene, men heller beskrive utfordringer og dilemmaer som kan være aktuelle i håndteringen av IKT-sikkerhetshendelser.

FFI har hatt mulighet til å lage et gradert eget vedlegg til rapporten. Mengden gradert informasjon som FFI har hatt tilgang til, har vært meget begrenset. FFI har derfor vurdert at et eget gradert vedlegg ikke har vært hensiktsmessig, selv om enkelte detaljer ikke omtales i den ugraderte rapporten.

1.4 Begreper og kortformer

Begreper

Krisehåndtering: omhandler all respons en virksomhet utøver, planlagt eller *ad-hoc*, for å håndtere en hendelse som har inntruffet (Engen, Kruke, Lindøe, Olsen, Olsen og Pettersen, 2016).

IKT-sikkerhetshendelse: «Tilsiktede uønskede hendelser eller trusler om slike hendelser i det digitale rom som er rettet mot kritisk infrastruktur og /eller kritiske samfunnsfunksjoner» (NSM, 2017:3).

Håndtering av IKT-sikkerhetshendelse: «Defensive prosesser og tiltak for å detektere (avdekke) og stanse alvorlige IKT-sikkerhetshendelser, samt å gjenopprette sikker tilstand for berørte systemer, skadevurdere og skadebegrense» (NSM, 2017:3).

IKT-sikkerhet eller digital sikkerhet: «… at digitale tjenester og produkter er sikre og pålitelige fra starten, og i hele tjenestens eller produktets levetid» (Regjeringen, 2019:13).

Trussel: «Mulig uønsket handling som kan gi negativ konsekvens for en entitets sikkerhet» (NS 5830:2012, s. 4).

Verdi: «Ressurs som hvis den blir utsatt for uønsket påvirkning vil medføre en negativ konsekvens for den som eier, forvalter eller drar fordel av ressursen» (NS 5830:2012, s. 4).

Sårbarhet: «Manglende evne til å motstå en uønsket hendelse eller å opprette ny stabil tilstand dersom en verdi er utsatt for uønsket påvirkning» (NS 5830:2012, s. 5).

Risiko: «Forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifikke trusselen» (NS 5830:2012)

Integritet: «at informasjonen ikke blir endret utilsiktet eller av uvedkommende» (Datatilsynet, 2018).

Tilgjengelighet: «at informasjonen er tilgjengelig for autoriserte ved behov» (Datatilsynet, 2018).

Konfidensialitet: «at informasjonen ikke blir kjent for uvedkommende» (Datatilsynet, 2018).

Avansert trusselaktør: En aktør med betydelige ressurser, kompetanse og vilje til å gjennomføre angrep i det digitale rom. Dette inkluderer «*Advanced Persistent Threats*» (APT-er), som er

trusselaktører som typisk arbeider i det skjulte over lengre tid for å kompromittere utvalgte virksomheter.

Kortformer

Hendelse FM: En kortform for «IKT-sikkerhetshendelsen hos fylkesmannsembetene i 2018 og håndteringen av denne».

Hendelse HSØ: En kortform for «IKT-sikkerhetshendelsen hos Helse Sør Øst RHF og Sykehuspartner Helseforetak (HF) i 2017–2018 og håndteringen av denne».

I tilknytning til hendelsene FM og HSØ, omtales IKT-sikkerhetshendelsene beskrevet i denne rapporten også på kortform som «IKT-angrep». I denne begrepsbruken ligger det ingen vurdering om hva slags aktør som stod bak eller hvilken intensjon denne hadde.

Instruksen: En kortform for «Samfunnssikkerhetsinstruksen».

Rammeverket: En kortform for «Rammeverk for håndtering av IKT-sikkerhetshendelser».

1.5 Rapportens oppbygning

I kapittel 1 beskrives oppdraget, forskningsspørsmål, avgrensning og det redegjøres for sentrale begreper.

I kapittel 2 gis noen metodiske betraktninger om hvordan oppdraget er utført, hvem som har vært involvert og informasjonstilgang.

I kapittel 3 redegjøres det for det faglige utgangspunktet for oppdraget samt sentrale grunnleggende roller og mekanismer for krisehåndtering.

I kapittel 4 og 5 beskrives de to hendelsene hver for seg. Først beskrives hendelsesforløpene og deretter funn som er spesifikke for de enkelte hendelsene.

I kapittel 6 presenteres funn kategorisert etter rammeverk for håndtering av IKT-sikkerhetshendelser, og deretter funn som er relevant i forbindelse med samfunnssikkerhetsinstruksen.

I kapittel 7 presenteres FFIs vurderinger knyttet til håndteringen av hendelsene.

I kapittel 8 presenteres betraktninger om rammeverket, og noen anbefalinger om hvordan dette kan videreutvikles.

I kapittel 9 presenteres noen generelle øvingspunkter og noen konkrete dilemmaer som FFI mener bør øves på under øvelse Digital 2020.

I kapittel 10 og 11 presenteres konklusjon og avsluttende betraktninger.

2 Metodiske betraktninger

Oppdraget fra JD går ut på å utarbeide en *overordnet* evaluering av håndteringen av hendelsene. Denne formuleringen kan tolkes på flere måter. En overordnet evaluering kan på den ene siden omfatte vurderinger av generelle aspekter ved hendelseshåndteringen av disse to hendelsene, som til slutt sammenstilles i en oppsummering med lavere detaljgrad. På den andre siden kan en overordnet evaluering omfatte oppbygging av detaljkunnskap om hendelsesforløpene, herunder hvilke aktører som var involvert, hvilke aktører som gjorde hva og hvilke utfall ulike beslutninger og tiltak fikk, for deretter å trekke ut de store linjene om hendelseshåndteringen og framheve de mest sentrale forholdene. FFI mener sistnevnte tolkning er det eneste alternativet for å sikre at riktige vurderinger blir gjort, med tanke på sammenhenger mellom aspekter i det tekniske hendelsesforløpet og selve håndteringen.

For å løse oppdraget ble det utviklet en metodisk tilnærming. Gjennom denne tilnærmingen søkte FFI å erverve tilstrekkelig kunnskap om hendelsesforløpene, håndteringen og konteksten rundt, som så kunne understøtte relevante vurderinger i lys av oppdragets målsetninger og forsknings-spørsmål. Oppdraget har krevd at to sentrale kompetanseområder måtte spille sammen i vurderingene, herunder krisehåndtering og IKT. FFIs eksisterende kunnskap og erfaring innen disse områdene har vært en forutsetning for å kunne løse oppdraget.

Oppdragets omfang var på ca. 600 timer, noe som la begrensninger på hvilke undersøkelser og analyser som kunne iverksettes og hvor grundig og dypt hendelsesforløpene og håndteringen kunne studeres. FFI anser at det er etablert et tilstrekkelig overordnet bilde av hendelsene som muliggjør læring. Noen usikkerhetsfaktorer er imidlertid til stede i arbeidet, og det var utfordringer knyttet til informasjonstilfang som medførte ytterligere usikkerhet.

I dette kapitlet beskrives først framgangsmåten for å løse oppdraget. Deretter beskrives arbeidet med datainnsamling via intervjuer og gjennomgang av skriftlige kilder. Videre omtales arbeidet med analyse og våre vurderinger av hendelsesforløp og håndtering. Dette følges av en beskrivelse av usikkerhetsfaktorer i arbeidet, og tiltak for å på best mulig måte sørge for gyldighet og pålitelighet i det arbeidet som er gjennomført. Til sist presenteres noen utfordringer knyttet til informasjonstilgang.

2.1 Framgangsmåte for å løse oppdraget

Arbeidet med oppdraget ble delt opp tre hovedsteg:

1. Kartlegging av hendelsesforløpene og hendelseshåndteringen
2. Vurdering av hendelsene og hendelseshåndteringen
3. Forslag til endringer av instruks og rammeverk

Første steg gikk ut på å opparbeide en forståelse for hva hendelsene faktisk gikk ut på og hvordan de ble håndtert. Dette inkluderer det tekniske hendelsesforløpet, vurderinger som de involverte gjorde underveis og beslutninger som ble tatt. Spesielt ble god forståelse for det tekniske hendelsesforløpet, fra FFIs side, ansett som fundamentalt for å kunne gjennomføre de påfølgende stegene i oppdraget. For å oppnå tilstrekkelig forståelse ble det utført intervjuer med flere involverte aktører og en gjennomgang av skriftlige kilder.

I andre steg ble det gjort egne vurderinger av håndteringen, med vekt på hvordan håndteringen fungerte fra et overordnet perspektiv. Både IKT- og krisehåndteringsrelaterte forhold ble vurdert. Enkelte spesifikke forhold som ble ansett som spesielt relevant med tanke på framtidig læring, ble også trukket fram. Videre ble det gjort vurderinger knyttet til i hvilken grad det er mulig å overføre lærdommer fra disse hendelsene, til andre hendelser av samme type og til andre typer hendelser.

I tredje steg ble instruksen og rammeverkets innvirkning på håndteringen vurdert, før forslag til endringer ble konkretisert. Endringene var i hovedsak basert på resultatene fra de forrige stegene, samt FFIs kunnskap innen IKT og krisehåndtering. Her ble også mulige øvingsmomenter for øvelse Digital 2020 konkretisert.

Stegene var i utgangspunktet sekvensielle, men med iterative tilbakekoblinger ved behov. Analysearbeidet startet med datareduksjon hvor rådata ble valgt, forenklet, abstrahert og omformet – her dokumenter og intervjudata (jfr. Miles og Huberman, 1994). Data ble deretter sortert og strukturert, og ledet til en forståelse rundt sammenhenger, likheter og ulikheter. Etter hvert som vi ble mer kjent med hendelsene og håndteringen var det behov for å gå noe fram og tilbake mellom stegene. Prosessen med datareduksjonen, sortering og strukturering ble derfor gjennomført i flere sekvenser.

2.2 Intervjuer og gjennomgang av skriftlige kilder

For å få bedre forståelse for hendelsene, ble det gjennomført søk etter skriftlig materiale på internett. Materialet som ble samlet inn inkluderte blant annet erfarings- og evalueringsrapporter[2], styrereferater[3], pressemeldinger og nyhetsartikler. Etter hvert som intervjuene ble gjennomført, supplerte de involverte aktørene med relevant skriftlig materiale, som ytterligere evalueringsrapporter og tiltakslister. FFI gjennomførte nye søk underveis basert på informasjon som framkom gjennom intervjuene.

Den innledende informasjonsinnsamlingen ga en oversikt over de mest sentrale aktørene som var involvert i håndteringen av hendelsene. Etter vår vurdering ga dette oss et tilstrekkelig utgangspunkt for å identifisere aktører som det ville være fordelaktig å intervjue. Da antall aktører var større enn det som var praktisk gjennomførbart gitt tilgjengelige ressurser, særlig for hendelse HSØ, ble det gjort en foreløpig prioritering av aktørene. Intensjonen var å dekke aktører på ulike

[2] Helsedirektoratet, 2018 og 2019a; Nasjonal sikkerhetsmyndighet, 2018; KMD, NSM, PST, DSB, representanter fra FM, 2019.
[3] Helse Vest IKT, 2018a og b; Helse Sør-Øst RHF, 2018; Sykehuset Innlandet HF, 2019

nivåer og som tilsammen utførte både tekniske, operative og strategiske oppgaver. Denne prioriteringen var basert på vurderinger knyttet til aktørenes nærhet og involvering i hendelseshåndteringen. Prioriteringen ble oppdatert etter hvert som intervjuene ble gjennomført og informasjonsgrunnlaget vokste. I noen tilfeller intervjuet vi aktører på anbefaling fra andre informanter. Det ble gjennomført totalt 14 intervjuer, hvor det fra FFI i de fleste tilfeller deltok tre forskere. Fra de ulike aktørene deltok som oftest to personer etter FFIs forespørsel om å få tilgang til informasjon om tekniske, operative og strategiske forhold. Det ble gjennomført to telefonintervju, mens resterende ble gjennomført hos de ulike aktørene. Hvert av intervjuene hadde en varighet på ca. 1,5 time, og det ble tatt skriftlige notater underveis. Enkelte aktører ble intervjuet flere ganger for kvalitetssikring og for å avklare nye spørsmål som framkom etter at andre aktører var intervjuet. Der hvor vi hadde ytterligere konkrete spørsmål til noen av aktørene ble dette i noen tilfeller gjort via telefonsamtaler i etterkant av intervjuet.

Intervjuguide for hver aktør ble utviklet, med utgangspunkt i FFIs informasjonsgrunnlag på gitt tidspunkt. Intervjuene var delvis strukturerte. Intervjuene med de første informantene var todelt, med én del om virksomheten som ble intervjuet, og én del om selve hendelsene. Første del omhandlet i hovedsak spørsmål om virksomhetens mandat og rolle, IKT-systemer, og trusler, verdi og sårbarhet (risiko). Andre del omhandlet tidslinjen for hendelsen, samarbeid med andre aktører, rammede IKT-systemer, konsekvenser og håndteringen. Etter hvert som informasjons-grunnlaget ble bedre, ble intervjuene spisset mer mot å dekke konkrete mangler i FFIs informasjonsgrunnlag og for å klargjøre eventuelle motstridende oppfatninger og meninger.

De intervjuede aktørene er:

- Justis- og beredskapsdepartementet
- Kommunal- og moderniseringsdepartementet (KMD)
- Helsedirektoratet (Hdir)
- Nasjonal sikkerhetsmyndighet (NSM)
- Direktoratet for samfunnssikkerhet og beredskap (DSB)
- Politiets sikkerhetstjeneste (PST)
- Fylkesmannen Innlandet (FMIN)
- Fylkesmannens fellesadministrasjon (FMFA)
- Helse Sør-Øst Regionalt helseforetak
- Sykehuspartner Helseforetak
- HelseCERT

2.3 Vurdering av hendelsene og håndteringen

Håndtering av større IKT-sikkerhetshendelser omfatter både tekniske, operative og strategiske forhold. Dette inkluderer blant annet:

- teknologiske undersøkelser
- vurderinger og tiltak, helhetlige konsekvensvurderinger, prioritering av verdier, og avveiinger mellom motstridende hensyn
- vurdering av implikasjoner på sektor- og samfunnsnivå

Det finnes ingen altomfattende modell eller teori for håndtering av slike IKT-sikkerhetshendelser som kan benyttes som en fasit eller referansegrunnlag for å karaktersette de ulike delene av hendelseshåndtering i detalj. Hva «god» IKT-hendelseshåndtering er, og hvordan denne målbart og kvantifiserbart skiller seg fra «dårlig» eller «meget god» håndtering er slikt sett ikke tilstrekkelig klarlagt for direkte anvendelse i dette oppdraget.[4] Det finnes imidlertid noe teori og kunnskap som kan anvendes for å vurdere hendelsene. Krisehåndtering er et eget fagfelt, som omhandler hvordan håndtering av ulike kriser kan organiseres for en mest mulig effektiv respons. Bidrag fra krisehåndteringsfeltet ble tilpasset og benyttet for å strukturere og vurdere håndteringen av hendelsene i dette oppdraget. Sentrale temaer innenfor krisehåndtering var blant annet informasjonsdeling, samhandling, planverk og fordeling av roller, ansvar og myndighet.

Det var også behov for kompetanse utover det som krisehåndteringsteori kan veilede med. I vurderingene har vi derfor benyttet FFIs kunnskap og kompetanse om IKT, IKT-sikkerhet, cyberoperasjoner og hendelseshåndtering. Sentralt i hendelsene fra et slikt perspektiv var omfanget på hendelsene, angriperens handlemåte, effekten på tilgjengelighet, integritet og konfidensialitet, reell og potensiell skade på verdier, følgekonsekvenser inn i operativ virksomhet og konsekvenser på sektornivå og nasjonalt nivå. Risikotenking med sårbarhet, trussel og verdi som de sentrale bestanddeler har vært et grunnleggende perspektiv i intervjuer og analysearbeid.

Fasene i rammeverket har blitt brukt som et strukturerende grep på hendelsesforløp og håndtering. Dette er gjort ved at funnene er kategorisert etter fasene rammeverket legger opp til. Basert på eksisterende kunnskap og arbeid ved FFI og de framkomne resultatene i dette oppdraget, ble det gjort vurderinger av rammeverket og instruksen. Øvingsmomenter for Digital 2020 ble også konkretisert, basert på vurderingene og erfaringer fra arbeid med andre øvelser.

[4] Se for eksempel «*Incident Management Capability Assessment*» fra Carnegie Mellon University (Dorofee m.fl., 2018). I en tidligere versjon het rapporten «*Incident Management Capability Metrics*» og dens historie kan spores tilbake til et arbeid utført av Defence Information Systems Agency (DISA) og National Security Agency (NSA) i 2000-2002, kalt «Department of Defence (DoD) Computer Network Defense Service Provider (CNDSP) Evaluator's Scoring Metrics.» Selv med denne historikken ble ambisjonsnivået for arbeidet i denne versjonen redusert: «*This method cannot measure how well a given incident management activity is performed, only that it is performed*» (Dorofee m.fl., 2018).

2.4 Valget om å ikke identifisere informantene

FFI har i rapporten gjort et valg om å ikke identifisere hvilke informanter som har sagt hva, og ivaretar dermed informantenes personvern. Dette samsvarer med at målet med oppdraget er en overordnet evaluering, framfor en undersøkelse av enkeltindividers oppfatninger. Det ble antatt at dette også ville kunne bidra til friere tale under intervjuene.

Informasjon fra intervjuene er ikke direkte gjengitt gjennom sitater. Hvilken aktør som ga informasjonen angis derfor ikke, med mindre dette allerede er offentlig kjent eller øker forståelsen av hendelsene. Hvem FFI har intervjuet identifiseres kun ut ifra hvilken etat eller virksomhet de tilhører. Enkeltpersoner, personopplysninger, hvilken avdeling eller seksjon informantene tilhører er med hensikt ikke identifisert.

Der motstridende oppfatninger eller meninger framkommer, identifiseres etat enkelte ganger for å tydeliggjøre dette. Det har ikke vært en ambisjon å vurdere om beslutningene som ble tatt i håndteringen var riktige eller uriktige, selv om enkelte beslutninger og vurderinger vil bli diskutert.

2.5 Usikkerhetsfaktorer knyttet til framgangsmåten

Det er flere usikkerhetsfaktorer i gjennomføringen av oppdraget. Selv om de mest sentrale aktørene ble intervjuet, så var det flere aktører som kunne ha belyst hendelsene enn vi hadde mulighet til å intervjue. Dette er særlig relevant for hendelse HSØ. Varigheten på intervjuene, vanligvis halvannen time, ga begrensninger på hvor mange spørsmål som kunne stilles og hvor detaljert de kunne diskuteres. Enkelte ganger var det ønskelig å få intervjuet ytterligere personer enn de som hadde mulighet til å stille. Hendelsene inntraff også et par år tilbake i tid, noe som gjorde det vanskelig for enkelte å huske alle detaljene rundt hendelsene.

Flere ganger ble det klart at aktørene hadde motstridende oppfatninger og meninger om hendelsene. Det kan være flere årsaker til dette. Enkelte ganger framstod det som sannsynlig at informasjonsdeling hadde vært mangelfull, særlig i de tilfeller der flere informanter, og skriftlige kilder, bekreftet dette. Andre ganger skyldtes det ulik vektlegging av faktorer i aktørenes vurderinger, og i visse tilfeller var det vanskelig å få klarhet i hvorfor. Generelt har ikke FFI hatt som mål å avdømme hvilken aktør som har rett i slike tilfeller. Dette ville krevd mer ressurser enn tilgjengelig for oppdraget, i den grad det i det hele tatt var mulig å slå fast hva som var korrekt. Der hvor det er betydelige uenigheter eller motstridende oppfatninger er dette forsøkt belyst.

2.6 Utfordringer knyttet til informasjonstilfang

Det var opprinnelig antatt at intervjuer ville være den viktigste informasjonskilden for å oppnå den nødvendige forståelse av hendelsene og håndteringen. De skriftlige kildene var i utgangspunktet tiltenkt som bakgrunnsmateriale for å lage gode intervjuguider og velge ut de rette aktørene for intervju. I utgangspunktet finnes det mer informasjon om hendelse HSØ, enn

hendelse FM. Dette skyldes at hendelsen var mer omfattende, og at flere aktører var involvert. Det viste seg imidlertid å være meget utfordrende for FFI å få informasjon om det tekniske hendelsesforløpet og den operative håndteringen i hendelse HSØ, utover det som allerede var offentlig tilgjengelig. Dette medførte at vi hadde større mangler i vårt informasjonstilfang om hendelse HSØ enn hendelse FM når analyse og vurderinger ble gjennomført.

Fra FFIs perspektiv er denne type informasjon sentral for å kunne gjennomføre de vurderingene som er nødvendig for å løse oppdraget. Det ble derfor gjennomført ytterligere søk etter og gjennomgang av relevante skriftlige kilder som kunne belyse teknisk og operativ håndtering, samtidig som vi i intervjuer med andre aktører forsøkte å redusere informasjonsgapet. Likevel var konsekvensene av manglende informasjon om det tekniske hendelsesforløpet og den operative håndteringen, en betydelig usikkerhet knyttet til hva som faktisk skjedde under hendelsen. Som en følge av dette er det større usikkerhet ved grunnlaget for FFIs vurderinger av denne hendelsen enn det FFI skulle ønske, og det tas forbehold om at det kan være viktige forhold ved hendelse HSØ som fremdeles er ukjent for FFI.

Under siste steg av FFIs prosess for intern kvalitetssikring og rapportgodkjenning, mottok FFI en rapport[5] om hendelse HSØ med informasjon om enkelte tekniske og operative forhold som FFI manglet. Etter å ha gått igjennom rapporten, er FFIs vurdering at rapportens innhold bekreftet enkelte funn samtidig som FFIs konklusjoner ikke endres. Usikkerheten ved enkelte vurderinger ble dermed redusert. Da rapporten kun presenterer én aktørs syn på hendelse HSØ, er FFIs vurdering likevel at det fremdeles er informasjonsmangler ved hendelse HSØ sammenliknet med hendelse FM.

2.7 Utfordringer knyttet til gradert informasjon

Enkelte opplysninger om hendelsene og håndteringen er gradert etter sikkerhetsloven. FFI har hatt noe tilgang til gradert informasjon i arbeidet, men i hovedsak er åpen informasjon benyttet. Målet om å levere en ugradert rapport har ført til at enkelte detaljer ikke kan tas med i rapporten. En konsekvens av dette er at enkelte forhold ved hendelsene potensielt ikke blir belyst i den grad de kunne ha blitt belyst i en gradert rapport.

FFI har blitt informert om at det er enkelte mangler i informasjonsgrunnlaget, som igjen kunne ha påvirket våre vurderinger. Deler av denne informasjonen er gradert. FFI har verken fått innsyn i denne informasjonen, eller fått beskrevet hvilken informasjon dette gjelder. Dette gjør det vanskelig for FFI å vurdere konsekvensene av denne informasjonsmangelen.

FFI har vært nødt til å forholde seg til det informasjonsgrunnlaget som foreligger. Prinsipielt sett kan det ikke utelukkes at ytterligere tilgang på både gradert og ugradert informasjon kunne ha medført justeringer eller på annen måte ha påvirket vurderingene.

[5] Nasjonal sikkerhetsmyndighet (udatert). Hendelsesrapport BLIND BANDICOOT & BLACK BANDICOOT. Unntatt offentlighet.

2.8 Troverdighet og pålitelighet i studien

I dette oppdraget har vi gjort flere tiltak for å sikre troverdighet. For det første har vi der det har vært usikkerhet eller fare for misforståelser gjennomført ytterligere intervjuer eller fått avklaringer via telefonsamtaler. Vi har også tatt skriftlige notater under hvert av intervjuene som har gjort det mulig å gå tilbake til datamaterialet underveis i studien. Videre har det under alle intervjuene vært minst to forskere tilstede – såkalt forskertriangulering – både for å sikre at hensikten med oppdraget ble kommunisert, at spørsmålene ble besvart og at informasjon fra informantene ble oppfattet riktig. Informantene har ikke fått mulighet til å lese våre notater fra intervjuene, men har fått et komplett utkast av rapporten til gjennomlesning og faktasjekk. På denne måten kunne vi på best mulig måte utelukke feilinformasjon og misforståelser.

I tillegg til FFIs interne kvalitetssikring er det for dette oppdraget gjort flere tiltak for å sikre kvaliteten i arbeidet. For å sikre at FFI som forespurt av oppdragsgiver kunne utgi rapporten ugradert, ble deler av rapporten sendt til NSM for graderingssjekk. Dette ble gjort fordi enkelte opplysninger om disse hendelsene er sikkerhetsgraderte etter sikkerhetsloven. FFI har hatt tilgang til noe av denne informasjon underveis i oppdraget.

Da rapporten hadde status som komplett utkast ble dette sendt ut til alle informantene. I denne runden var det i all hovedsak faktafeil og misforståelser aktørene kunne komme med innspill på. Da det gjaldt FFIs vurderinger var dette i mindre grad noe som aktørene kunne påvirke, med unntak av der hvor vurderingen baserte seg på uriktig informasjon.

3 Krisehåndtering, IKT og organisering

I dette kapitlet vil vi først presentere rammeverk for håndtering av IKT-sikkerhetshendelser og instruks for departementenes arbeid med samfunnssikkerhet. Deretter vil vi gjøre rede for hva som inngår i krisehåndtering og IKT-hendelseshåndtering, herunder fasene i «rammeverk for håndtering av IKT-sikkerhetshendelser» (NSM, 2017). Vi vil også redegjøre for nasjonal krisehåndtering, og roller og ansvar tilknyttet dette.

3.1 Rammeverk og instruks

Rammeverk for håndtering av IKT-sikkerhetshendelser

Rammeverk for håndtering av IKT-sikkerhetshendelser har som formål å skape god situasjonsoversikt gjennom aggregering og koordinering av informasjon om alle relevante IKT-sikkerhetshendelser, og å effektivt håndtere alvorlige IKT-sikkerhetshendelser fra virksomhets-nivå til politisk nivå. Dette skal skje gjennom god utnyttelse av samfunnets samlede ressurser, og at Norge framstår koordinert overfor andre land og internasjonale organisasjoner (NSM, 2017:3).

Målgruppen er i utgangspunktet offentlige og private virksomheter som har betydning for kritisk infrastruktur og/eller kritiske samfunnsfunksjoner, sektorvise responsmiljøer (SRM), myndigheter som har en rolle knyttet til håndtering av IKT-sikkerhetshendelser og departementer (NSM, 2017). Det antas også at rammeverket kan ha nytteverdi for andre virksomheter, herunder virksomheter som tilbyr IKT-tjenester og -produkter til tredjepart, samt CERT[6]-, CSIRT[7]- og responsmiljøer som ikke er SRM-er (ibid.).

Rammeverket gir innledningsvis en generisk beskrivelse av enkelte samfunnsaktører og deres overordnede rolle i samfunnet, inkludert en begrenset beskrivelse av deres rolle ved IKT-sikkerhetshendelser. Dette er aktører som regjering, departementer, politi, Etterretningstjenesten og NSM. Rammeverket omfatter ikke beskrivelser av hver sektor.

Selve kjernen i rammeverket er en beskrivelse av et hierarkisk system for håndtering av IKT-sikkerhetshendelser, bestående av NSM, SRM-er og virksomheter. I beskrivelsen av dette systemet framheves forventninger og krav til disse tre aktørtypene, strukturert i henhold til tradisjonelle faser innen IKT-hendelseshåndtering. Fasene er, ifølge rammeverket, i overensstemmelse med ISO 27001: 1 planlegging og forberedelse; 2 deteksjon og vurdering av omfang og alvorlighetsgrad; 3 varsling av relevante parter; 4 iverksetting av prosesser og tiltak for å håndtere hendelsen; 5 situasjonsrapportering; og 6 tilbakeføring og læring av hendelsen.[8]

[6] Computer Emergency Response Team
[7] Computer Security Incident Response Team
[8] Det menes trolig ISO 27035 (ISO, 2016).

I tillegg er det utarbeidet fem vedlegg, herunder prinsippskisser for håndtering av to scenarioer, en mal for aktørkart på sektornivå, en mal for sambandskatalog for en sektor, en begrepsliste og en taksonomi for klassifisering av IKT-sikkerhetshendelser.

Instruks for departementenes arbeid med samfunnssikkerhet

Instruks for departementenes arbeid med samfunnssikkerhet (heretter forkortet samfunnssikkerhetsinstruksen eller instruksen) er utarbeidet av JD og skal presisere kravene til departementenes arbeid med samfunnssikkerhet. Instruksen beskriver blant annet ansvarsforhold, gjøremål og rollebeskrivelser innenfor samfunnssikkerhet og beredskap på departementsnivå. Formålet med samfunnssikkerhetsinstruksen er å styrke samfunnets evne til å forebygge kriser og å håndtere alvorlige hendelser via et helhetlig og koordinert arbeid (JD, 2017:1). Instruksen er gjeldende for sivile sektorer i hele krisespekteret, og inkluderer dermed også planlegging for sivil støtte til Forsvaret.

Instruksen sier noe om hva som forventes at departementene har oversikt over, som risiko og sårbarhet i egen sektor og beredskapsplaner. Instruksen er såpass overordnet at metodikken som legges til grunn for vurderinger, og hvilken kriseorganisasjon hvert enkelt departement legger opp til er opp til departementene selv å avgjøre.

Det er «del VIII Sentral krisehåndtering» av samfunnssikkerhetsinstruksen som nevnes eksplisitt i oppdragsbeskrivelsen når det gjelder sammenheng mellom instruks og rammeverk. Del VIII beskriver ulike roller og ansvarsområder, og tar for seg både oppgaver i normaltilstand og en krisesituasjon. Viktige roller og deres arbeidsoppgaver og ansvar, som lederdepartement, Kriserådet og Regjeringen sikkerhetsutvalg (RSU), blir beskrevet i form av konkrete punkter. JDs koordinerende rolle blir også håndtert. Se kapittel 3.3 for nærmere beskrivelse av disse rollene.

3.2 Krisehåndtering

Krisehåndtering har mange definisjoner, og ulike aktører, teoretikere og praktikere benytter begrepet forskjellig. I stort kan vi si at krisehåndtering omhandler all respons en virksomhet utøver, planlagt eller *ad-hoc*, for å håndtere en hendelse som har inntruffet (Engen, m.fl., 2016).

Boin m.fl. (2005) skiller mellom to ulike analysenivåer ved kriser, hvor det første nivået referer til det operative nivået med de personene og aktørene som er direkte involvert i å håndtere krisen. Det andre nivået refereres til som det strategiske nivået, hvor vi finner de politiske og administrative lederne med et mer overordnet og overgripende ansvar. I dette oppdraget er begge nivåene og samspillet dem imellom relevant.

I tillegg er den tekniske håndteringen som teknisk personell gjør i IKT-systemer når disse rammes, et særskilt tema. Ved større IKT-sikkerhetshendelser vil teknisk personell typisk gjøre flere typer tekniske analyser, som for eksempel diskanalyse, binærkodeanalyse og analyser av

nettverkslogger. Det finnes verktøy, veiledere og beskrivelser av metoder for slike analyser.[9] Videre finnes det «best practice», standarder og annen litteratur om prosesser rundt teknisk hendelseshåndtering samt organisatoriske forhold.[10] Det finnes også standarder og veiledere for responsmiljøer, og for IKT i virksomheter generelt.[11] Som nevnt er imidlertid beskrivelser av «god» hendelseshåndtering på en målbar måte relativt fraværende.[12]

Som utgangspunkt for å strukturere håndteringen av hendelsene har vi benyttet fasene i rammeverket (NSM, 2017:12–19):

1. **Planlegging og forberedelse**

   Rammeverket legger opp til at det skal finnes etablerte prosedyrer for håndtering av hendelser, inkludert rapportering, ansvarslinjer og eskaleringsrutiner og etablering av et IKT-risikobilde. Virksomhetene som omfattes av rammeverket forutsettes å ha implementert grunnsikring basert på egne risiko og sårbarhetsanalyser. Det presiseres i rammeverket at robuste systemer er et viktig premiss for å motstå IKT-sikkerhetshendelser. Det forutsettes at virksomheter mottar, vurderer og formidler informasjon fra og til eget SRM, har systemer for loggføring av nettverkstrafikk, deltar i samhandlingsøvelser og har beredskapsplaner for håndtering av større hendelser og sikkerhetspolitiske kriser i det digitale rom.

2. **Deteksjon og vurdering**

   Det er flere måter rammet part kan detektere hendelser. Det kan oppdages av virksomheten selv, etterretningstjenester, politi, NSM eller andre virksomheter. Den som oppdager at en annen aktør er rammet av en IKT-sikkerhetshendelse skal alltid melde fra om dette til rammet part.

   Når en virksomhet er rammet av en IKT-sikkerhetshendelse handler det om å gjennomføre en kartlegging av situasjonen basert på tilgjengelig informasjon. Rammeverket foreslår at virksomheten bør søke å besvare: i) hvilke systemer som er rammet eller står i fare for å bli rammet, og er det noe som tyder på at andre aktører er rammet? ii) hvor kritiske systemene er, både for virksomheten og for samfunnet og iii) hvilken informasjon virksomheten har om det som har skjedd gjennom logger og sammenstilling av informasjon fra andre.

   Det forutsettes i rammeverket at virksomheten har beredskap for å rettidig kunne avdekke hendelser, ha kompetanse om relevante systemer i virksomheten og kunne vurdere alvorlighetsgrad, omfang og konsekvenser på overordnet nivå, kunne vurdere om kritisk

[9] Se for eksempel «*Reversing*» (Eilam, 2005), «The IDA Pro Book» (Eagle, 2011).
[10] Se for eksempel «*Computer Security Incident Handling Guide*» fra National Institute of Standards and Technology (NIST, 2012), ISO 27035 (ISO, 2016) eller «*Principles of Incident Response and Disaster Recovery*» (Whitman og Mattord, 2007).
[11] Se for eksempel FIRST CSIRT Services Framework (FIRST, 2019), RFC 2350 (Brownlee og Guttman, 1998) og ITIL (Axelos, 2011).
[12] Se kapittel 2.3, fotnote 3.

infrastruktur eller kritiske samfunnsfunksjoner er eller kan bli berørt. Det forutsettes også at virksomheten benytter NSMs system for klassifisering av hendelser, eller et kompatibelt system, og vurderer behov for bistand.

3. **Varsling**

   Utgangspunktet for varsling er at den som er rammet av en hendelse eier informasjonen om sin hendelse. Rammeverket legger opp til at virksomheten skal varsle SRM, NSM (hvis tilknytning til Varslingssystem for digital infrastruktur (VDI) eller at det er inngått bilateral avtale), overordnet myndighet i egen sektor, og eventuelt politi. Virksomheten forventes å ha rutiner for å varsle om IKT-sikkerhetshendelser til SRM og eventuelt samarbeidende parter.

4. **Iverksetting av prosesser og tiltak for å håndtere hendelsen**

   I rammeverket forventes det at virksomheten har etablert eller har tilgang til tilstrekkelig evne og kapasitet til å håndtere IKT-sikkerhetshendelser. Dette kan være gjennom avtale med en kommersiell tredjepart. Rammeverket omtaler håndtering knyttet til å stanse hendelsen, skadevurdere, begrense skadeomfang og gjenopprette sikker tilstand.

5. **Situasjonsrapportering**

   Under en pågående hendelse er rapporteringslinjene like som varslingslinjene. Rapportering skal gå både fra virksomhets- og sektornivå til nasjonalt nivå, samt fra nasjonalt nivå til sektor- og virksomhetsnivå. Virksomheter forutsettes å benytte NSMs system for rapportering av IKT-sikkerhetshendelser, eller et kompatibelt system, og rapportere hendelsene til SRM.

6. **Tilbakeføring og læring av hendelsen**

   Dette innebærer å lukke sårbarheter og øke grunnsikringen om dette anses som nødvendig. Virksomheten forutsettes å varsle og/eller anmelde hendelsen til politiet dersom dette ikke er gjort, delta i evalueringsarbeid i egen sektor, evaluere og forbedre sin egen evne til å håndtere IKT-sikkerhetshendelser og implementere tiltak som kan hindre at lignende hendelser inntreffer igjen.

3.3 Nasjonal krisehåndtering og relevante roller og aktører

I dette delkapitlet gjør vi rede for prinsippene for samfunnssikkerhet og rollene som beskrives som sentrale i samfunnssikkerhetsinstruksen. Deretter beskrives relevante aktører innenfor nasjonal krisehåndtering og andre aktører som har vært sentrale i de to hendelsene FFI har vurdert. Listen over sentrale aktører er ikke uttømmende for nasjonal krisehåndtering, men inkluderer de som har vært involvert i hendelse FM og HSØ.

Krisehåndtering, og arbeidet med samfunnssikkerhet, i Norge bygger på fire grunnleggende prinsipper:

1. Ansvarsprinsippet betyr at virksomheten som har ansvar for et fagområde i normalsituasjon har også ansvaret for nødvendige beredskapsforberedelser og håndtere hendelser på området.

2. Likhetsprinsippet betyr at den organisasjonen man opererer med under kriser skal være mest mulig lik den organisasjonen man har til daglig.

3. Nærhetsprinsippet betyr at kriser skal håndteres på lavest mulig nivå.

4. Samvirkeprinsippet betyr at virksomheter på alle nivå har et selvstendig ansvar for å sikre et best mulig samvirke med aktører og virksomheter i arbeidet med forebygging, beredskap og krisehåndtering (JD, 2017).

Lederdepartement

Lederdepartementet har ansvaret for å koordinere håndteringen av krisen på departementsnivå, men endrer ikke det konstitusjonelle ansvarsforholdet. Dette betyr at hvert departement beholder sitt ansvar og beslutningsmyndighet innenfor sine saksområder. JD er fast lederdepartement hvis ikke annet blir bestemt. Oppgavene til lederdepartementet er blant annet å varsle andre departementer, ta initiativ til møter i Kriserådet, situasjonsrapporter- og analyser, identifisere og vurdere behov for tiltak, sørge for nødvendige fullmakter, distribuere informasjon og utforme beslutningsgrunnlag til regjeringen og informasjon til media og befolkningen (JD, 2017).

Kriserådet

Kriserådet er det øverste koordineringsorganet på departementsnivå. Rådet har seks faste medlemmer, regjeringsråden ved Statsministerens kontor (SMK), utenriksråden i Utenriksdepartementet (UD), og departementsrådene i JD, Forsvarsdepartementet (FD), Helse- og omsorgsdepartementet (HOD) og KMD.[13] Rådet kan utvides med andre departementer og representanter fra underliggende virksomheter ved behov. Det avholdes faste møter i Kriserådet i tillegg til at de samles ved hendelser som krever det. Funksjonene til Kriserådet er å sikre strategiske vurderinger, vurdere spørsmål om lederdepartement, sikre koordinering av tiltak som iverksettes av ulike sektorer, koordinere informasjon til media, befolkningen og andre og påse at spørsmål som krever politisk avklaring raskt legges fram for departementets politiske ledelse eller regjeringen (JD, 2017).

Justis- og beredskapsdepartementets samordningsrolle

Ansvaret som ligger i denne rollen innebærer at JD har ansvar for et helhetlig, systematisk og risikobasert arbeid med samfunnssikkerhet på nasjonalt nivå på tvers av sektorer. I så måte

[13] Under hendelsene var ikke KMD fast medlem av Kriserådet. De ble medlem i 2019, da ansvaret for elektronisk kommunikasjon ble flyttet fra Samferdselsdepartementet til KMD.

innebærer dette planlegging, forberedelser, mekanismer og strategier som legger grunnlaget for en effektiv krisehåndtering. Samordningsrollen til JD som beskrives i instruksen retter seg dermed mot forebygging, ikke krisehåndtering (JD, 2017).

Krisestøtteeneheten

Krisestøtteenheten (KSE) skal ved behov kunne yte støtte til lederdepartementet og Kriserådet i deres håndtering. De understøtter også JDs samordningsrolle og er fast kontaktpunkt for informasjon til og fra JD ved ekstraordinære hendelser og kriser (JD, 2017).

Direktoratet for samfunnssikkerhet og beredskap

DSB skal ifølge samfunnssikkerhetsinstruksen understøtte JDs koordineringsrolle innenfor samfunnssikkerhet og beredskap (JD, 2017). DSB skal også være tilbyder av operativ støtte under kriser innenfor samordning, forsterkninger og faglig rådgivning. DSB er også eier og forvalter av Nødnett (JD, 2016). DSB skal også ha oversikt over risiko og sårbarhet i samfunnet og være pådriver i arbeidet med å forebygge ulykker, kriser og andre uønskede hendelser, samt sørge for god beredskap og effektiv ulykkes- og krisehåndtering (Regjeringen, 2019:23).

Fylkesmannens rolle innen samfunnssikkerhet, beredskap og krisehåndtering

Fylkesmannens rolle innen samfunnssikkerhet er beskrevet i egen instruks (Fylkesmannens samfunnssikkerhetsinstruks, 2015). Denne beskriver blant annet Fylkesmannens regionale samordningsansvar ved håndtering av uønskede hendelser. Dette ansvaret innebærer å samordne den sivile krisehåndteringen, også opp mot Forsvaret, på regionalt nivå. Fylkesmannen skal skaffe oversikt over situasjonen i fylket, kartlegge kommunenes og andre berørte aktørers behov og gi situasjonsrapport til sentrale myndigheter.

Nasjonal sikkerhetsmyndighet

NSM er det nasjonale fagmiljøet for digital sikkerhet, og er nasjonal varslings- og koordineringsinstans for alvorlige dataangrep mot samfunnskritisk infrastruktur og andre viktige samfunnsfunksjoner. NSM driver den nasjonale responsfunksjonen for alvorlige dataangrep mot kritisk infrastruktur og nasjonalt varslingssystem for digital infrastruktur. Nasjonalt cybersikkerhetssenter (NCSC) ble i 2019 etablert som en del av NSM (Regjeringen, 2019:22).[14]

Politiets sikkerhetstjeneste

PST har ansvar for nasjonens indre sikkerhet. PST forebygger og etterforsker lovbrudd som kan true nasjonens sikkerhet, gjennom blant annet innsamling av informasjon om personer og grupper som kan utgjøre en trussel, utarbeidelse av ulike analyser og trusselvurderinger, etterforskning og andre operative mottiltak og rådgivning (Regjeringen, 2019:22). Oppgavene til PST er fastsatt i

[14] Siste setning er oppdatert etter at Nasjonalt cybersikkerhetssenter åpnet. I denne rapporten brukes fremdeles betegnelsen NSM NorCERT om den nasjonale CERT og koordinerende enhet for IKT-sikkerhetshendelser, selv om NorCERT nå er en funksjon ved NCSC i NSM.

politiloven § 17 b. Det framkommer der at PST blant annet skal etterforske (og forebygge) ulovlig etterretningsvirksomhet, sabotasje og overtredelser av straffelovens bestemmelser om terrorhandlinger og terrorrelaterte handlinger. Straffeprosessloven § 224 fastslår at etterforskning foretas "når det som følge av anmeldelse eller andre omstendigheter er rimelig grunn til å undersøke om det foreligger straffbart forhold som forfølges av det offentlige" (PST, 2017).

Etterretningstjenesten

E-tjenesten er ansvarlig for å kartlegge utenlandske trusselaktører, deres motiver, kapasiteter og metoder. Formålet med etterretningsvirksomheten er å bidra til å gi norske myndigheter et solid beslutningsgrunnlag i saker som gjelder utenriks-, sikkerhets- og forsvarspolitikk (Regjeringen, 2019:23).

Kripos

Kripos er den nasjonale enheten for bekjempelse av organisert og annen alvorlig kriminalitet, inkludert datakriminalitet, og er underlagt Politidirektoratet. Enheten har spisskompetanse innen kriminaletterretning og taktisk og teknisk datakrimetterforskning. Kripos har en egen datakrimenhet som driver etterretning, forebygging, avdekking og etterforskning, samt bistår det øvrige politiet og overordnet påtalemyndighet. Enheten for internettrelatert etterforskningsstøtte bistår med sikring av elektroniske spor og bevis på internett, utlevering fra tjenestetilbydere, ransakinger, analyse av beslag, med videre (NSM, 2017:10).

Feller cyberkoordineringssenter

Felles cyberkoordineringssenter (FCKS) består av NSM, Etterretningstjenesten, PST og Kripos, og ledes av NSM. Formålet med FCKS er å styrke nasjonal evne til effektivt forsvar mot og håndtering av alvorlige hendelser og kriminalitet i det digitale rom. FCKS er et permanent og samlokalisert fagmiljø, bestående av faste representanter fra hver av partene. Lederen utnevnes av Sjef NSM, og er sammen med en seniorrepresentant fra hver av de andre partene ansvarlig for daglig drift. Senteret er ikke et selvstendig organ med egen beslutningsmyndighet.

Virkeområdet til FCKS er alvorlige hendelser i det digitale rom. FCKS skal koordinere partenes innsats ved håndtering av hendelser, herunder bidra til mer effektiv bruk av nasjonale ressurser, styrke informasjonsdeling, samt ivareta koordinert varsling til og frembringelse av helhetlige beslutningsgrunnlag til overordnede myndigheter. Senteret er ikke en kapasitet hvor virksomheter kan henvende seg for bistand til håndtering (NSM, 2017:10).

Kommunal- og moderniseringsdepartementet

Kommunal- og moderniseringsdepartementet (KMD) har ansvar for boligpolitikk, plan- og bygningsloven, arbeid med FNs bærekraftsmål, kart- og geodatapolitikken, kommuneøkonomi og lokalforvaltning, IKT- og forvaltningspolitikk, elektronisk kommunikasjon, regional- og distriktspolitikk, det administrative ansvaret for fylkesmenn, valggjennomføring, politikken

overfor samer og nasjonale minoriteter, statlig arbeidsgiverpolitikk og statlig bygg- og eiendomsforvaltning (KMD, 2019).

Helsedirektoratet

Hdir er underlagt HOD, og skal være en faglig rådgiver, iverksette vedtatt politikk og forvalte lov og regelverk innenfor helsesektoren. I tillegg har Hdir et helhetlig ansvar for den nasjonale helseberedskapen. Hdir skal i all beredskapsvirksomhet overfor helse-, omsorgs- og sosialtjeneste og -forvaltning, bidra til at samhandlingen blir ivaretatt i beredskapsplanlegging og ved kriser. Etter delegasjon fra departementet skal Hdir forestå overordnet koordinering av helse- og omsorgssektorens innsats og iverksette nødvendige tiltak når en krisesituasjon truer eller har inntruffet. Hdir leder også Helseberedskapsrådet hvis formål er å sette sivil og militær sektor i stand til å løse viktige helseoppgaver knyttet til sivil-militær planlegging og samhandling under kriser i fred og krig (Hdir, 2019).

Helse Sør-Øst regionalt helseforetak

Helse Sør-Øst RHF er det største av fire regionale helseforetak i Norge og er den strategiske enheten som eier helseforetakene/sykehusene i regionen. Helse Sør-Øst RHF eies av staten ved HOD og sørger for spesialisthelsetjenester til 3 millioner mennesker i Innlandet, Oslo, Vestfold og Telemark, Viken og Agder. Helse Sør-Øst RHF eier 11 helseforetak og har et tett samarbeid med private sykehus og institusjoner. Helseforetakene/ sykehusene i regionen har rundt 80 000 ansatte som utfører om lag 61 000 årsverk. Omsetningen i 2018 var i underkant av 82 milliarder kroner (HSØ RHF, 2020).

Sykehuspartner helseforetak

Sykehuspartner eies av HSØ RHF, og leverer tjenester innen IKT, prosjekt og HR[15] til alle sykehusene i HSØ. De drifter og forvalter livsviktige IKT-systemer for sykehusene, både klinisk og administrative applikasjoner, IKT-infrastruktur, nettverk og arbeidsflater for bortimot 80 000 brukere. I løpet av et døgn sendes det 1 million meldinger mellom deres IKT-systemer og brukere, helseforetak, legekontor og kommuner (Sykehuspartner, 2020-2).

HelseCERT

HelseCERT er helse- og omsorgssektorens nasjonale senter for informasjonssikkerhet. Helse-CERTs oppgave er å øke sektorens evne til å oppdage, forebygge og håndtere ondsinnede inntrengingsforsøk og andre uønskede IKT-hendelser. HelseCERT skal spre kunnskap om IKT-trusler og beskyttelsesmekanismer og kontinuerlig monitorere trafikken i Helsenettet. Helse-CERT er en seksjon i Norsk Helsenett og er lokalisert i Trondheim (Norsk helsenett, udatert).

[15] Human Relations.

Fylkesmannens fellesadministrasjon

FMFA ble etablert 1. januar 2019, og leverer administrative tjenester til alle fylkesmannsembetene. De utvikler og drifter også de digitale tjenestene til innbyggerne i samarbeid med fylkesmennene. FMFA leverer alle IKT-tjenester og IKT-utstyr til embetene (FMFA, 2019).

4 Hendelse HSØ

Hendelsen hos HSØ RHF startet julen 2017 og varte noen måneder inn i 2018. De rammede aktørene var i utgangspunktet Sykehuspartner HF, de andre helseforetakene i regionen som bruker IKT-infrastrukturen og HSØ RHF. Håndteringen involverte Sykehuspartner HF, HSØ RHF, Hdir, NSM, HelseCERT, PST, DSB, KSE, HOD, og to kommersielle aktører.

I dette kapitlet gjennomgås først hendelsesforløpet. Deretter beskrives erfaringer og relevante kommentarer fra de involverte aktørene i håndteringen av hendelsen, slik det har framkommet gjennom dokumentstudier og intervju.

4.1 Hendelsesforløpet

Etter innledende rekognosering før jul, ervervet en aktør tilgang til et IKT-system hos et av helseforetakene i region Helse Sør-Øst tidlig i romjulen 2017.

Tilgangen ble oppnådd gjennom en sårbar applikasjon som ble kjørt på en tjener forvaltet av Sykehuspartner, men driftet av lokalt helsepersonell. Tjeneren sto i en nettverkssone med tjenester eksponert mot internett (såkalt DMZ eller demilitarisert sone). Aktøren benyttet tilgangen til ytterligere å kompromittere og bevege seg inn i Sykehuspartners infrastruktur. Sårbarheter i daværende plattform ble utnyttet som en del av angrepet (Sykehuspartner, 2018).

Sykehuspartner startet hendelseshåndtering etter varsling fra HelseCERT 8. januar 2018 og gikk i rød beredskap dagen etter, tirsdag 9. januar. Det ble satt krisestab, og andre helseforetak i regionen, øvrige regionale IKT-miljøer og HSØ RHF ble varslet. Sistnevnte konkaktet HOD, som varslet Hdir. JD og FD ble varslet av NSM. Fra tirsdag 9. januar 2018 og utover i håndteringen ble det gjennomført hyppige direktørmøter mellom HSØ RHF og helseforetakene i regionen, hvor sikkerhetslederne også deltok. Sykehuspartner fikk allerede fra starten av hendelsen analysestøtte fra HelseCERT.

Et tilsvarende forsøk på datainnbrudd ble gjennomført av samme aktør mot infrastrukturen til Helse Vest IKT i samme periode. Helse Vest IKT samarbeidet fra 8. januar med HelseCERT om å kartlegge og identifisere spor etter trusselaktøren og håndtere mulige svakheter. Angrepet ser ut til å ha mislyktes, og per 22. februar 2018 var det ikke funnet spor etter aktøren i Helse Vest IKT sin infrastruktur (Helse Vest IKT, 2018-2).

På et tidspunkt deaktiverte Helse Vest IKT en såkalt site2site VPN-tunnel[16] til Sykehuspartner på grunn av uklarheter rundt mulige konsekvenser for denne. Dette medførte problemer med utveksling av pasientinformasjon, blant annet radiografibilder (Helse Vest IKT, 2018-1).

[16] En Virtual Private Network-tunnel benyttes for å koble sammen to deler av et nettverk. Tunnelen vil typisk gå over et annet nettverk (som internett), uten at dette er synlig for brukerne.

Forbindelsen ble gjenåpnet etter gjensidig risikovurdering av Sykehuspartner og Helse Vest IKT.[17]

Sykehuspartner tok tirsdag 9. januar 2018 ned kompromitterte tjenere (den såkalte «*takedown*»).[18] Det viste seg i løpet av kvelden samme dag at aktøren hadde fått ytterligere tilgang i infrastrukturen enn først antatt, og at «*takedown*» ikke var tilstrekkelig for å bli kvitt aktøren (Jacobsen, 2018).

Arbeidet med å håndtere situasjonen pågikk utover uken. Onsdag 10. januar 2018 ble NSM kontaktet av KSE, som ba om en brif fra NSM om hendelsen på førstkommende (regulære) møte med de underlagte etatene fredag 12. januar 2018. NSM informerte om hendelsen på møtet, basert på informasjon fra Sykehuspartner. På dette tidspunkt ble situasjonen beskrevet som under kontroll.

Lørdag 13. januar 2018 ble det klart for Sykehuspartner at aktøren hadde penetrert enda dypere inn i deres infrastruktur enn antatt foregående dag – inn i den regionale infrastrukturplattformen SIKT. På dette tidspunkt var det også en bekymring om OUS-nett i tillegg var kompromittert.[19] Sykehuspartner valgte å be om bistand fra NSM NorCERT og ytterligere bistand fra HelseCERT. NSM NorCERT varslet KSE og situasjonssenteret (SITSEN) i FD, og sendte personell til Sykehuspartners lokaliteter sent lørdag kveld. Sykehuspartner informerte HSØ RHF som gikk i beredskap og satte beredskapsledelse. HSØ RHF varslet HOD, som igjen varslet Hdir. Helsedirektøren varslet relevante aktører og kalte inn til kriseutvalg (KU) i Hdir.

På formiddagen søndag 14. januar 2018 ankom personell fra HelseCERT i Trondheim Sykehuspartners lokaliteter. Samme dag ble det gjennomført møte i Hdir KU, og HOD delegerte koordineringsansvar til Hdir. NSM NorCERT satte høy prioritet på hendelsen grunnet alvorligheten og den potensielle risikoen for liv og helse. Sykehuspartner anmeldte hendelsen til politiet, og PST iverksatte etterforskning. I FCKS ble det også startet koordinering av partenes innsats i saken.

Utover i påfølgende uke inngikk Sykehuspartner avtale først med en utenlandsk kommersiell aktør, og kort tid etter en norsk kommersiell aktør, mnemonic (HSØ RHF, 2018-1), om støtte til hendelseshåndteringen. Andre samarbeidspartnere til Sykehuspartner bisto også med støtte. På et tidspunkt ble det også plassert ut en midlertidig VDI-sensor, for å øke deteksjonsevnen i infrastrukturen i helseregion HSØ utover dekningen til den eksisterende VDI-sensoren til NHN.

Mandag 15. januar ble Helsetjenestens driftsorganisasjon for nødnett HF (HDO) gjort kjent med hendelsen i HSØs datasystemer gjennom utsendt informasjon fra Hdir. Senere samme dag mottok

[17] Informasjon fra Sykehuspartner.
[18] En annen skriftlig kilde oppgir torsdag 11. januar som datoen for at tjenere ble tatt ned. Vi har valgt datoen fra Sykehuspartners presentasjon (Jacobsen, 2018).
[19] I region HSØ er det tre regionale infrastrukturplattformer: OUS (Oslo universitetssykehus), SIKT og AHUS (Akershus universitetssykehus) (Sykehuspartner 2020-2).

HDO informasjon fra HelseCERT med anbefalte umiddelbare tiltak. Anbefalte tiltak ble gjennomført uten at det ble avdekket noen funn[20] (HDO HF, 2018).

Onsdag 17. januar 2018 oversendte HSØ RHF til Hdir en samlet oversikt over alle tiltak som helseforetakene i regionen hadde iverksatt og planlagt i forbindelse med hendelsen (HSØ RHF, 2018-2). En ny samlet oversikt ble sendt mandag 22. januar (HSØ RHF, 2018-3). Tiltakene kan grovt sett deles i fem kategorier, der det enkelte helseforetak på selvstendig grunnlag ser ut til å ha gjort vurderinger om passende tiltak basert på den informasjonen de satt med og i hvilken grad de anså seg som direkte berørt av hendelsen. Kategoriene omfattet:

- Tiltak som gikk på årvåkenhet, varsling om unormale hendelser og ustabilitet i systemer.
- Tiltak for å få en oversikt over nettverkskomponenter med tilgang til flere domener og internettilganger.
- Tiltak om å kartlegge brukere med tjenstlig behov for administratortilganger og bytte passord på disse, samt kartlegging, og eventuell fjerning av, AD[21]-grupper med utvidede rettigheter.
- Tiltak som gikk på å forberede seg på at kritiske systemer kunne gå ned eller tas ned, eller at forbindelse med omverdenen ble kuttet. Eksempler på systemer var DIPS og medisinteknisk utstyr.
- Tiltak for å håndtere konsekvensene av allerede iverksatte tiltak og å etablere alternative kommunikasjonskanaler utenfor de (potensielt) kompromitterte systemene.

Det ble gjennomført løpende vurderinger med tanke på mulige operative konsekvenser (HSØ RHF, 2018-4).

På et tidspunkt ble koblingen til Uninett tatt ned (HSØ RHF, 2018-2). Videre ble tilganger fra Forskernett mot SIKT og OUS-nett lukket, og tilganger fra SIKT mot OUS-nett lukket. Brukere og data ble også overført fra Forskernett til OUS-nett (HSØ RHF, 2018-3). FFI antar overføringen skjedde på et tidspunkt da Sykehuspartner ikke lenger jobbet med hypoteser om at OUS-nett var kompromittert, og var relativt sikre på at kun SIKT-domenet var kompromittert.

Konsekvensen av å stenge ovennevnte tilganger var bortfall av flere tjenester. Muligheten for pasientkommunikasjon, forskningseffektivitet og visse kommunikasjonssystemer mellom ambulanse og sykehus (e.g. Lifenet) ble påvirket. Nødrutiner ble etablert (OUS HF, 2018). FFI antar nevnte konsekvenser inkluderer bortfallet av Minjournal.no, og omtalt reduksjon av funksjonalitet i Forskernett som e-post og VPN (HSØ RHF, 2018-3). Sykehuspartner er av den oppfatning at de fleste tjenestene var ikke-essensielle siden nedstengningen etter deres vurdering hadde svært begrensede konsekvenser for pasientbehandlingen. FFI har ikke fått klarhet i når de

[20] FFI antar at dette betyr at det ikke ble funnet spor etter trusselaktøren.
[21] Active directory.

ulike tilgangene ble stengt, fullstendig oversikt over hvilke tjenester som ble påvirket, videre konsekvenser for de andre helseforetakene eller gjort ytterligere vurderinger av tjenestenes kritikalitet.

Onsdag 24. januar 2018 gikk Sykehusparter ned i beredskapsnivå, fra «rød og frys» til «gul og streng endringskontroll» (Sykehuspartner, 2020-1).

På kvelden onsdag 24. januar ble HDO oppringt av Norsk Helsenett (NHN) ved HelseCERT, med spørsmål angående koblingen mellom NHN, HDO og HSØ. Tekniske ressurser fra NHN ved HelseCERT og HDO gjennomgikk den tekniske sammenkoblingen for å sikre felles forståelse for sikkerhetssituasjonen i grensesnittene. NHN meldte status til HOD 25. januar (HDO HF, 2018). FFI kjenner ikke til innholdet i denne rapporten.

Siste møte i Hdir KU var mandag 12. februar 2018. Fire dager senere, fredag 16. februar 2018, trakk HOD tilbake Hdirs fullmakter, og Hdir avsluttet den nasjonale koordineringen av hendelsen. Samme dag HSØ avsluttet sin beredskap.

FFI kjenner ikke til når de enkelte HF-er returnerte til normaltilstand. Omtalelsen av situasjonen i enkelte kilder indikerer at det var ulik situasjonsoversikt hos de ulike helseforetakene (Sykehuset Innlandet HF, 2018).

Fredag 2. mars 2018 avsluttet Sykehusparter sin beredskap (HSØ RHF, 2019).

Per torsdag 7. juni 2018 var fremdeles enkelte tjenester i Forskernett ikke gjenopprettet (UiO, 2018).

PST henla saken 29. november 2018 grunnet manglende opplysninger om gjerningspersonen.

5.desember 2018 kom PST med en pressemelding om hendelsen og henleggelsen (PST, 2018). PST uttalte at det er påvist uthenting av påloggingsinformasjon samt filer knyttet til en læringsapplikasjon. Slik PST så det kan søk i nettverket, sammenholdt med fravær av annen påvist aktivitet, indikere at trusselaktøren var ute etter informasjon om læringsapplikasjonen. PST uttalte videre at trusselaktøren har hatt tilganger til et nettverk med pasientopplysninger, forskningsdata og beredskapsplanverk og at de ikke, basert på den avgrensede etterforskningen, kan fastslå om slike opplysninger er stjålet eller ikke.

Samme dag, 5. desember 2018, kom også HSØ RHF sammen med Sykehuspartner, med en egen pressemelding (Alsén, 2018, HSØ, 2018-5). HSØ og Sykehuspartner pekte på PSTs uttalelse og at aktøren har vært har vært ute etter informasjon knyttet til en e-læringsløsning som ikke inneholder pasientopplysninger, og som ikke er rettet mot pasientbehandlingen. I følge Sykehuspartener inneholdt denne konkrete e-læringsløsningen[22] opplysninger om ansatte i HSØ.

[22] Også omtalt som en e-læringsplattform, Læringsportalen eller et Learning Management System (LMS).

FFI har ikke sett nærmere på denne løsningen og kjenner ikke til dagens status. FFIs forståelse er at identiske løsninger ble benyttet av flere offentlige og private virksomheter i Norge på den tiden.

Videre uttalte HSØ og Sykehuspartner i sin pressemelding at de med stor grad av sikkerhet kunne si at pasientopplysninger ikke var kommet på avveie eller er misbrukt. Dette begrunnes med at et overvåkings- og loggsystem installert før hendelsene, kalt Analyseplattformen, gjorde det mulig for Sykehuspartner å gjenskape detaljer ved angrepet.

PST har i tråd med sitt etterforskningsmandat blant annet utført tekniske undersøkelser av logger og kompromitterte servere. Størrelsen på nettverket gjorde det nødvendig å avgrense undersøkelsene. Sykehuspartner har gitt uttrykk for at deres egne undersøkelser går over en mye lenger tidsperiode og en større del av infrastrukturen enn det PSTs undersøkelser har gjort. FFI sitter ikke på et klart bilde på hvilke tidsperioder som var omfattet av ovennevnte analyser, ei heller hvor omfattende analysene har vært, sett i forhold til nettverkenes totale størrelse, kompleksitet, koblinger mot andre typer nettverk, samt trusselaktørens kompetanse og dyktighet. Trusselaktørens bakenforliggende motivasjon kan være gjenstand for flere konkurrerende hypoteser, uten at FFI har tilstrekkelig informasjon til å bekrefte eller avkrefte disse.

4.2 Erfaringer knyttet til håndteringen av hendelsen

Erfaringer knyttet til håndteringen av hendelse HSØ kan plasseres i følgende kategorier:

- roller
- samvirke og informasjonsdeling mellom involverte aktører
- planverk
- kommunikasjon til berørte internt
- kommunikasjon til befolkning
- rapportering til strategisk nivå

Det var et stort antall aktører som var involvert i håndteringen av hendelse HSØ. I tillegg til aktørene som arbeidet på teknisk nivå, som Sykehuspartner, HelseCERT, NSM NorCERT, Etterretningstjenesten, PST, Kripos og Cyberforsvaret (CYFOR) arbeidet alle HF-er i helseregionen med egne operative vurderinger og tiltaksplaner, med HSØ RHF som det samlende punkt. På direktoratsnivå gjennomførte Hdir kriseutvalg, med blant andre HSØ RHF og Direktoratet for e-helse som medlemmer, og departementene ble holdt orientert.

Funn fra intervjuer og Hdirs (2018) egen evaluering pekte på uklarheter knyttet til hvem som skulle gjøre hva underveis i håndteringen. Ansvarsbeskrivelser ble oppfattet som utydelige, og i den innledende fasen av håndteringen gikk det med mye tid til å klargjøre ansvarsforhold. Hdir

trakk fram at det manglet tydelig rolleavklaring og varlingslinjer mellom IKT-miljøer, og at alle de ordinære varslingslinjene ikke ble fulgt under hendelsen. Primært gjaldt dette aktivitetene som foregikk på utsiden av den tekniske håndteringen til Sykehuspartner.

NSM opplevde et behov for å tydeliggjøre og kommunisere sin rolle i forbindelse med hva de kan og ikke kan bidra med når en IKT-sikkerhetshendelse inntreffer. Deres mandat er å koordinere, rådgi og bidra i håndteringen av IKT-sikkerhetshendelser som potensielt kan få nasjonale konsekvenser. Utover dette er det virksomheten selv som har ansvaret for å håndtere hendelser, og eventuelt ha avtale med kommersielle aktører for å få bistand i håndteringen.

Hvorvidt det var godt samarbeid mellom aktørene under hendelsene synes det å være delte meninger om, særlig på teknisk nivå. Sykehuspartner trakk fram at de verken hadde øvd på slike hendelser, eller hadde tilpasset planverk for hvordan de ulike aktørene skulle samvirke og samarbeide. Sykehuspartner fortalte at på tross av dette ble det utvist en imponerende innsats hvor mange frivillige meldte seg for å bistå dem. Samarbeidet med NSM NorCERT, PST og HelseCERT ble beskrevet som meget bra av både Sykehuspartner HF og HSØ RHF.

NSM NorCERT omtalte på sin side begrensninger i tilgang til data i og om de rammede systemene, som resulterte i at de ikke fikk gjort de analysene de ønsket å gjennomføre eller fikk tilstrekkelig oversikt over situasjonen. Sykehuspartner på sin side mente at NSM NorCERT innledningsvis ba om mer informasjon enn det som var relevant, og at partene kom til enighet etter hvert. Sykehuspartner fortalte videre at enkelte begrensninger var knyttet til at en tredjepart potensielt ville kunne få tilgang til taushetsbelagte personopplysninger. NSM NorCERT, som håndterer mye gradert informasjon etter sikkerhetsloven og dermed har prosesser for å håndtere sensitive data, mente dette kunne ha blitt håndtert på en mer effektiv måte. Sykehuspartner presiserte forskjellen mellom gradert og personsensitive data.

Flere av aktørene involvert i hendelseshåndteringen jobber til vanlig ikke med sikkerhetsgradert informasjon. Enkelte av disse aktørene opplevde at ugradert informasjon om hendelsen ble gradert underveis av andre aktører, noe som gjorde håndteringen av denne informasjonen mer komplisert enn nødvendig.

Det var ytterligere, og til dels store, utfordringer knyttet til håndtering av informasjon blant de som deltok i hendelseshåndteringen. Dette gjaldt blant annet manglende tilgang på systemer som kunne behandle informasjon, kunnskap om verdivurdering av informasjon og personell med nødvendig sikkerhetsklarering. Utfordringene med gradert kommunikasjon førte til at enkelte mente at de ikke fikk tilstrekkelig informasjon, og at de ikke visste hvem informasjonen kunne deles med. I tillegg var det manglende sikkerhetsklarering hos enkelte i Hdirs kriseutvalg, som gjorde at det var vanskelig å få et felles situasjonsbilde da noe av informasjonen bare kunne gis til en del av utvalget. Det ble uttrykt et ønske om egnede fasiliteter for kommunikasjon slik at man kan slipper å bruke unødvendig mye tid på å møtes fysisk.

Enkelte beredskapsaktører etterlyste en villighet hos andre til å informere og involvere dem i større grad i håndteringen av hendelsen. Dersom hendelsen hadde eskalert og medført behov samordning på regionalt nivå, ville de relevante fylkesmannsembetene ha måtte blitt involvert da

dette er oppgaver som ligger hos dem i en beredskapssituasjon. Under håndteringen av hendelse HSØ ble disse fylkesmannsembetene i meget liten grad holdt informert.

HSØ RHFs (2019) evaluering viste til at det gjeldende beredskapsplanverket kun i begrenset grad var dekkende for denne typer hendelser. Det ble pekt på at de spesifikke planene for IKT-beredskap vektla kortvarige bortfall, og inkluderte i mindre grad målrettede, fiendtlige angrep. De generelle planene, som omhandler varsling, beredskapsledelse, kommunikasjon og koordinering med underliggende helseforetak skal ifølge HSØs evaluering ha fungert godt. Sykehuspartner fortalte at de hadde gode beredskapsplaner for håndtering av nedetid, men manglet planer for hendelser som varer over tid. Dette medførte videre at de ikke hadde planlagte mekanismer for prioritering av arbeidsoppgaver. Under håndteringen av hendelsen medførte dette at andre oppgaver tillagt Sykehuspartner ble utsatt.

Det var utfordringer knyttet til kommunikasjon, både internt i berørte virksomheter og ut til befolkningen. Hdir opplevde at det under hendelsen var vanskelig å gjøre kommunikasjons-vurderinger, særlig når det gjaldt kommunikasjon ut mot befolkningen, og hvorvidt de skulle gi mye eller lite informasjon. Hdir (2018:30) pekte på tre forhold som gjorde det vanskelig å avgjøre hva som skulle veie tyngst: i) mye informasjon, eller lite gjennomtenkt informasjon, kunne avdekke sårbarheter før de var håndtert, ii) lite informasjon kunne oppfattes av befolkningen som at informasjon var holdt tilbake, selv om det var gjort for å ikke lekke informasjon til angriperen og iii) at utfordringer kunne kommuniseres, mens informasjon som kunne ha beroliget befolkningen var gradert.

Sykehuspartner manglet en intern kommunikasjonsplan, og fikk erfare at kommunikasjon av IKT-sikkerhetshendelser skilte seg fra hvordan de var vant til å kommunisere helserelatert informasjon. I utgangspunktet er det et ønske om å få ut mest mulig informasjon for å opplyse eventuelle berørte i en helsehendelse, mens det under en IKT-sikkerhetshendelse er et større behov for å holde tilbake deler av informasjon. Begrepsapparatet for IKT er også ukjent for mange, særlig når det kommer til tekniske termer som de ikke bruker til daglig. En intervjuet aktør foreslo at det utvikles en plan for hvordan kommunikasjon skal være forståelig for både befolkningen og andre fagpersoner. De fleste intervjuede aktørene opplevde utfordringer knyttet til å kommunisere faglig informasjon.

NSM NorCERTs bidrag synes å oppleves som større på departements- og direktoratsnivå enn på virksomhetsnivå, og ble av flere trukket fram som en aktør som var nyttig i forbindelse med å formidle hendelsen, konsekvenser og begreper på en forståelig måte.

Hendelsen utløste ikke rapporteringsmekanismene som trer i kraft under større kriser, hvor hvert direktorat rapporterer til sitt departement som igjen rapporterer til lederdepartementet. DSBs retningslinjer for rapportering i samordningskanal ble tilsynelatende ikke benyttet. Under denne hendelsen er vårt inntrykk at rapporteringen i stor grad har skjedd internt i helsesektoren, men at JD/KSE og FD har blitt holdt informert.

Rapporteringen innenfor helsesektoren fikk noe kritikk for å være for lite detaljert knyttet til hva som har skjedd, forventet utvikling og verstefalltenking. HOD har uttrykt at de i framtiden ønsker

et situasjonsbilde som inkluderer hvilke konsekvenser de tekniske forholdene kan ha for evnen til å yte helsetjenester (Hdir, 2018; HSØ RHF, 2019).

5 Hendelse FM

Hendelsen hos fylkesmannsembetene startet sommeren 2018 og varte ut året. De rammede aktørene var i utgangspunktet Fylkesmannen i Aust- og Vest Agder (FMAV), Fylkesmannen i Hedmark (FMHE) og Fylkesmannen i Oslo og Akershus (FMOA). Håndteringen involverte KMD, fylkesmannsembetene, NSM, PST, DSB, og JD/KSE.

Fylkesmannsembetene i Norge har en felles IKT-infrastruktur som leverer en rekke tjenester til embetene. I 2018 var driftsansvaret for IKT-infrastrukturen fordelt på flere utvalgte embeter:

- FMHE var ansvarlig blant annet for fjernaksessløsningen og fylkesmennenes regionale informasjonsnett (FRI), inkludert felles driftstjenester og systemer som katalogtjenesten, utrulling og konfigurasjon av programvare, e-post og andre samhandlingsløsninger (KMD, 2018; KMD, 2014). Enkelte embeter driftet også egne fjernaksessløsninger.

- Fylkesmannen i Sogn og Fjordane (FMSF) var ansvarlig for Trippelnett – løsningen for intranett, internett (nettsider) og ekstranett samt den elektroniske rettshjelpsløsningen (KMD, 2018; KMD 2014; FMSF, 2018).

- Fylkesmannen i Nordland (FMNO) var ansvarlig for drift av arkivløsningen ePhorte, i samarbeid med FMHE (KMD, 2018-2).

I 2017 var det 8 grupper for nettverksdrift, med 28 medlemmer fordelt på 15 embeter. (FMHE, 2017). Ansvaret for drift av IKT-infrastrukturen ble overført til FMFA i 2019.

I dette kapitlet gjennomgås først hendelsesforløpet. Deretter beskrives erfaringer og relevante kommentarer fra de involverte aktørene i håndteringen av hendelsen, slik det har framkommet gjennom dokumentstudier og intervju.

5.1 Hendelsesforløpet

En avansert trusselaktør forsøkte i midten av juli 2018 å få tilgang til infrastrukturen til Fylkesmannsembetene. Første forsøk var iht. logger 17. juli, hvor trusselaktøren prøvde å komme igjennom ulike løsninger for fjernaksess. Brukernavn og passord til enkelte brukere fra FMAV, FMOA, Fylkesmannen i Vestfold (FMVE) og Fylkesmannen i Trøndelag (FMTL) ble forsøkt benyttet. To-faktorautentisering (2FA) stoppet aktøren (Lund, 2019).

Trusselaktøren fortsatte sine forsøk om å få tilgang gjennom fjernaksess den 18. juli, og lyktes til slutt hos FMAV. Det antas at to-faktorautentisering ikke var aktivert for alle mulige inngangsveier.

Gjennom den ervervede tilgangen startet trusselaktøren flere aktiviteter, herunder nettverks- og filrekognosering, tilegnelse av økte adgangsrettigheter, installering av skadevare på tjener hos

FMAV og videre forflytning innover til tjenere hos andre Fylkesmannsembeter. Aktøren skjulte til sine spor, blant annet ved å slette verktøy og filer fra systemene.

Hos FMAV ble skadevare startet den 24. juli, noe som også skjedde hos FMHE og FMOA noen dager senere. I perioden fram til 30. juli fikk trusselaktøren med seg rundt 1,2 gigabyte med data ut av systemene. Dataene ble fraktet ut via internettjenesten Dropbox (Lund, 2019). Skadevaren som ble benyttet var Trochilus.

Skadevaren på systemet var i kommunikasjon med ekstern tjener for kommando og kontroll (K2) fram til 31. august. På daværende tidspunkt ble domenet satt til å peke på en ny IP-adresse, og sluttet å svare på forespørsler fra skadevaren.

22. oktober 2018 ble FMOA kontaktet av NSM NorCERT. De henviste NSM NorCERT videre til FMHE, som hadde driftsansvar for FRI.

Med støtte fra NSM NorCERT, jobbet FMHE med å kartlegge hendelsen. VDI-sensorer ble plassert ut hos flere embeter kort tid etter at trusselaktøren ble oppdaget.

Påtalemyndigheten besluttet på eget initiativ at PST skulle iverksette etterforskning uten anmeldelse, etter en vurdering av angrepets karakter, den rammede virksomheten og verdier.

7. november 2018 ble det etablert en gruppe med flere aktører, herunder KMD, PST, NSM, DSB og fylkesmannsembetene, sistnevnte representert med både IKT- og beredskapsmiljøene. Formålet med gruppen ble oppfattet noe ulikt. Enkelte mente at gruppen i utgangspunktet var en teknisk gruppe, som så fikk et mer operativt fokus – dvs. fokus på konsekvenser – etter påtrykk fra enkelte medlemmer etter hvert. Andre mener at formålet fra start var å se på strategiske konsekvenser av kompromitteringen.

12. november 2018 ble det avholdt et informasjonsmøte i Departementenes fylkesmannsutvalg (DFU).[23] Dagen etter, 13. november, ble det sendt en epost til alle Fylkesmenn på det graderte nettet FISBasis H om hendelsen. Enkelte aktører hos fylkesmannen mener de ikke fikk denne beskjeden.

I midten av november 2018 ble det etablert en oversikt over hva som hadde skjedd i den tekniske infrastrukturen, der dette var mulig.

Blant aktørene var det ulike meninger om hva som burde gjøres. Enkelte miljøer ønsket å kaste trusselaktøren ut og renske systemene så raskt som mulig, mens andre ønsket å monitorere trusselaktørens aktiviteter for å få bedre forutsetninger for den tekniske hendelseshåndteringen. Beslutningen gikk oppover til KMD, som etter råd fra NSM og i samråd med departementene i DFU besluttet å la trusselaktøren være til stede.

[23] KMD, HOD, Landbruk og matdepartementet (LMD), Barne- og likestillingsdepartementet (BLD), Kunnskapsdepartementet (KD), Arbeids- og sosialdepartementet (ASD), Klima- og miljødepartementet (KLD) og JD.

Overvåkingen av trusselaktøren foregikk til 24. desember 2018, hvor skadevaren på ny fikk kontakt med K2-domenet. Den nye aktiviteten til skadevaren ble oppdaget av NSM NorCERT etter 12 timer. Gitt faren for at mer informasjon skulle kunne komme på avveie, varslet NSM NorCERT så FMHE per telefon, som reiste ut til sine lokaler på Hamar for å stenge ned internettforbindelsen. Det viste seg at denne kontakten var en falsk positiv. Skadevaren hadde fått kontakt med en ny tjener på IP-adressen for K2, som ikke var involvert i angrepet. Tjeneren «svarte» på forespørsel fra skadevaren, uten at dette medførte at ytterligere data gikk ut.

Det ble fastslått at det var umulig å vite hvilke faktiske data som ble kopiert ut av systemet, da aktøren hadde fjernet sine spor underveis. En hypotese er at dataene var en blanding av filer med passordinformasjon, samt innholdet i enkelte epostkontoer.

Etterforskningen av hendelse FM er per nå[24] ikke avsluttet.

5.2 Erfaringer knyttet til håndteringen av hendelsen

Erfaringer knyttet til håndteringen av hendelse FM kan plasseres i følgende kategorier:

- varsling og igangsetting av hendelseshåndtering
- samvirke og informasjonsdeling mellom involverte aktører
- beslutningsmyndighet
- kommunikasjon med informasjonseiere

Innledningsvis varslet NSM NorCERT enkelte berørte fylkesmannsembeter og KMD om hendelsen, som så hadde ansvaret for å varsle videre i egne virksomheter. Gitt at oppdagelsen av hendelsen presumptivt var ukjent for trusselaktøren, var det ønskelig å holde spredning av informasjon om angrepet til et minimum. Dette ble begrunnet med at hvis informasjon om hendelsen lakk ut på dette stadiet og trusselaktøren ble klar over at han var detektert, kunne det blitt mer utfordrende å bestemme omfanget på kompromitteringen. Dette vil igjen gjøre det vanskeligere å kaste trusselaktøren ut og å friskmelde systemene.

Restriktiv varsling medførte at flere fylkesmannsembeter opplevde å ikke bli varslet om hendelsen. I ett av embetene fikk fylkesmannen informasjon om at et angrep hadde inntruffet av en sine IKT-medarbeidere, da denne medarbeideren hadde blitt bedt om å bistå i håndteringen. Videre i håndteringen av hendelsen opplevde flere fylkesmannsembeter at informasjon om hendelsen ikke ble formidlet til dem, inklusive varsling om at sentral informasjon kunne være på avveie. Slik disse embetene så det, kunne dette fått konsekvenser for rammede fylkesmannsembeters evne til å forberede og håndtere situasjonen dersom hendelsen viste seg å være større enn antatt.

[24] Februar 2020

Det ble også påpekt under intervjuene at informasjon om hendelsen i første omgang gikk ut til fylkesmennene fra KMD, men uten at fylkesberedskapssjefene ble informert eller involvert. For både DSB og FM opplevdes dette som en uheldig avgrensning, da det er beredskapssjefene som har ansvar for håndtering. Enkelte oppfattet at det ble argumentert for å holde tilbake informasjon i henhold til gradering eller «need to know», men argumentet opplevdes ikke som tilstrekkelig. Både fylkesmennene og fylkesberedskapssjefene har systemer for å motta gradert informasjon og er trent i å behandle slik informasjon.

Gradert kommunikasjonsverktøy var tilgjengelig under hendelsen, men ble ikke benyttet til å kommunisere informasjon enkelte fylkesmannsembeter ønsket seg. Det ble uttrykt, fra fylkesmannsembetenes side, et behov for å få på plass bedre rutiner og kommunikasjon omkring hvilke systemer som kan brukes og ikke, hvilken informasjon som kan være på avveie og hvilken informasjon man kan stole på.

Informasjonen som potensielt kunne vært kompromittert eller blitt ervervet tilgang til i systemene til FM tilhørte flere sektorer, blant annet helse, rettssikkerhet, barnevern og vergemål. Enkelte aktører opplevde det som utfordrende å ikke kunne informere og involvere de sektorer som potensielt kunne være berørt av angrepet. Antall sektorer som var berørt medførte også at godkjenningsprosessen ved å få opphevet taushetsplikt, i forbindelse med etterforskning og tilgang til systemer, måtte via de åtte departementer som DFU inkluderer, og tok derfor lang tid.

Enkelte fylkemannsembeter erfarte tidlig i hendelseshåndteringen at det var behov for en gruppe bestående av flere av aktørene for å kunne koordinere og håndtere hendelsen. Gruppen ble etablert 7. november 2018, noe som opplevdes som for sent av fylkesmannsembetene. Utelukkende teknisk håndtering var heller ikke tilstrekkelig, slik embetene så det. Det ble uttrykt at det var stor avstand mellom de tekniske miljøene som utfører håndteringen og de operative, og at en hendelse tidligere må løftes til et operativt nivå for å vurdere de mulige konsekvensene. I etterkant er det noe uenighet blant deltakerne om gruppens fokus i utgangspunktet var strategiske konsekvenser, eller om gruppen gikk fra et teknisk til operativt fokus.

I hendelsen som rammet FM kan det også synes som rollene og hvem som skal ha ansvaret i slike typer hendelser var (og kanskje fortsatt er) noe uklart. Valget mellom å overvåke trusselaktøren videre for å få bedre oversikt over omfanget, versus å gå i gang med å kaste trusselaktøren ut, framstår som det forholdet som utløste sterkest uenighet i den nedsatte gruppen, bestående av KMD, DSB, NSM, PST og FM. Flere av fylkesmannsembetene har stilt spørsmål både ved om KMD har beslutningsmyndighet over informasjonseier i dette tilfellet, og de mente at feil beslutning ble tatt gitt risikoen for at informasjon kunne komme på avveie.

KMD hadde en aktiv rolle opp mot NSM NorCERT og de rammede fylkesmannsembetene. I beslutningen om å overvåke eller kaste ut aktøren med en gang, opplevde KMD å ha støtte fra PST og NSM NorCERT i sin beslutning, og at denne myndigheten var i tråd med departementets instruksjonsmyndighet over FM. FM opplever imidlertid at det er de som er ansvarlig for å håndtere slike hendelser i tråd med gjeldende lovverk. FM henviser til at både forvaltningsloven, offentleglova og både ny og gammel sikkerhetslov tillegger virksomheten og virksomhetens leder ansvar for å sikre informasjon. FM opplevde å få støtte og forståelse for dette fra PST i ettertid.

PST har uttrykt at de under denne hendelsen formidlet at det er systemeier/verdieier som er ansvarlig og bør ta avgjørelsen, uten at de tok stilling til hvem dette var.

Beslutningen om å overvåke eller kaste ut aktøren med en gang var, slik FFI forstår det, tatt utenfor den nedsatte arbeidsgruppen, av KMD i samarbeid med DFU. Ifølge FM fikk ikke de beskjed før etter at beslutningen var tatt. Dette begrenset FM sin mulighet til å ta – eller bidra i – beslutninger knyttet til egen informasjon, som FM mener de lovmessig har rett til. FM sin opplevelse er at departementet i denne hendelsen ikke hadde rett til å benytte sin instruksjonsmyndighet slik den ble brukt.

6 Krisehåndtering i henhold til rammeverk og instruks

Rammeverket for håndtering av IKT-sikkerhetshendelser og samfunnssikkerhetsinstruksen beskriver relaterte, men i hovedsak ulike deler av apparatet som iverksettes ved håndtering av en hendelse. Rammeverket angir seks steg eller faser ved håndtering av en IKT-hendelse. For hver fase gis det forutsetninger og krav til håndteringen hos virksomheter, SRM og NSM. Samfunnssikkerhetsinstruksen beskriver prinsipper, roller og ansvar innen samfunnssikkerhetsområdet.[25]

I dette kapitlet vurderes håndteringen av hendelsene HSØ og FM med utgangspunkt i rammeverket og samfunnssikkerhetsinstruksen, med særlig vekt på del VIII «Sentral krisehåndtering». Det er FFIs egne vurderinger som ligger til grunn for utvalget av funn og framheving av disse, i motsetning til erfaringsdelen i de to forrige kapitlene hvor aktørenes egne meninger ble beskrevet. Våre vurderinger er basert på informasjon framkommet gjennom intervju og i skriftlige kilder som evalueringsrapporter, presentasjoner, nyhetsartikler og liknende. Det vil naturligvis være en del overlapp med aktørenes meninger, der hvor FFI har samme oppfatning.

6.1 Rammeverk for håndtering av IKT-sikkerhetshendelser

For å systematisere funnene benyttes de seks fasene i rammeverket.

Planlegging og forberedelse

Rammeverket legger til grunn at både virksomheter, SRM og NSM skal ha oversikt over trusler, ha planer for hendelseshåndtering og ha oversikt over samarbeidsaktører. Disse aktørene skal også ha tilstrekkelig kjennskap til systemer og sårbarheter i disse i henholdsvis virksomheten, i sektoren og i et sektorovergripende perspektiv.

Ved hendelsene HSØ og FM hadde de fleste av de involverte aktørene i liten grad oversikt over sine verdier, hva som kunne ramme dem og hvilken aktivitet som forekom i sine systemer. Det var betydelige mangler ved beredskapsplanene for hendelser hvor en avansert trusselaktør har fått tilgang til systemer og infrastruktur. Det at hendelser av en slik karakter ikke var hensynstatt i tilstrekkelig grad har videre innvirkning på håndteringen i de resterende fasene av rammeverket. Hvorvidt virksomhetene har beredskapsplaner, god monitorering av egne systemer, planer for varsling og oversikt over hvilke konsekvenser ulike IKT-angrep kan få internt i virksomheten og for andre som er avhengig av tjenestene de leverer, legger premissene for videre håndtering når en hendelse oppdages.

Funn fra både de aktørene som er rammet og de som skulle bistå i både håndteringen og etterforskningen, viste at det var store mangler i planlegging og forberedelse. Virksomhetene må i større grad enn det som var gjort kartlegge egne verdier, ha oversikt over aktivitet i egne

[25] Stegene i rammeverket er redegjort for i kapittel 3.1. Samfunnssikkerhetsinstruksen er nærmere beskrevet i kapittel 3.3.

systemer, forstå egne IKT-avhengigheter som både produsent og konsument av tjenester, samt avklare roller og ansvar.

Deteksjon og vurdering

Begge hendelsene ble oppdaget og varslet av andre enn rammet virksomhet. Etter at de rammede var varslet kan det tyde på at det har vært, hvert fall innledende, manglende erkjennelse av at virksomhetene var rammet og at problemet var betydelig. Funn fra intervjuene tyder på at det i begge hendelsene var utfordringer knyttet til å vurdere og bestemme omfanget av hendelsene, og derav hvilket skadepotensialet disse hadde eller kunne fått. At de rammede virksomhetene hadde manglende oversikt over egne nett og systemer, gjorde det utfordrende å kartlegge hvor langt inn i systemene trusselaktøren hadde kommet, og hvor mange veier det var inn og ut av systemene.

Rammeverket legger opp til at virksomheten kan vurdere behov for bistand, og i hendelse HSØ ble det hentet inn kommersielle aktører for å bistå i håndteringen.

Rammeverket henviser særlig til vurderinger av hvorvidt kritisk infrastruktur eller kritiske samfunnsfunksjoner (KIKS) står i fare for å bli berørt av en hendelse. Dette vurderingsansvaret er tillagt både virksomheten, SRM-ene og NSM. I hendelse FM ble det nedsatt en tverretatlig gruppe for å vurdere verdier og potensielle konsekvenser på noe lengre sikt. Etter det FFI kjenner til ble det ikke nedsatt en lignende gruppe, hvor tverretatlige konsekvens- og verdivurderinger ble gjort, for hendelse HSØ. Imidlertid er det indikasjoner på at konsekvensvurderinger for helsesektoren ble gjort underveis i håndteringen internt i Sykehuspartner og delvis av HF-ene som benytter Sykehuspartners infrastruktur. Samarbeidet mellom Sykehuspartner og de andre HF-ene på dette området kan se ut til å ha vært begrenset.

Inntrykket til FFI er at det var utfordrende for virksomhetene å gjøre verdivurderinger, og at SRM og NSM har mindre å bidra med i slike vurderinger til spesifikke virksomheter.

Varsling

Varsling ser ut til at har fungert i henhold til rammeverket, hvor både virksomhet, SRM og NSM ble varslet. Det kan imidlertid virke som det var flere relevante aktører som ikke ble varslet i neste steg. Eksempelvis ble sentrale beredskapsaktører som DSB, og relevante miljøer hos fylkesmannsembetene, utelatt innledningsvis i hendelse FM. I hendelse HSØ ble Fylkesmannen ikke varslet. Med tanke på vurdering av konsekvenser for KIKS, og mulighet til å forberede både seg selv og andre aktører på håndtering av hendelser og konsekvenser, burde disse aktørene, som har et viktig samordningsansvar, også ha blitt varslet.

Iverksetting av prosesser og tiltak for å håndtere hendelsen

For å kunne iverksette hensiktsmessige tiltak ved IKT-hendelseshåndtering, har etablering av gode planer i forkant av hendelsen og tilstrekkelig kjennskap til de rammede systemene vist seg å være viktig. Kombinasjonen av de mangler som er påpekt under de foregående fasene, må antas

å være en viktig årsak til at det ikke var åpenbart for aktørene hva som burde være til stede og iverksettes av tiltak og prosesser.

Funn viser at det ved hendelse FM var lite kapasitet og kompetanse tilgjengelig for å håndtere en slik type hendelse, og håndteringen tok lang tid. Det var usikkert om hendelsen hadde rammet alle 16 fylkesmannsembetene, og det var ikke tilstrekkelig oversikt over alle inn- og utganger og aktivitet i nettverket. Dette gjorde det vanskelig å avgrense og bestemme trusselaktørens inngangsveier og aktivitet. Det ble derfor valgt å ikke fjerne den kjente inngangsveien trusselaktøren benyttet, men heller å overvåke systemene. Beslutningen ble tatt av KMD på anbefaling av NSM NorCERT. Sammen med denne anbefalingen ble det også informert om risikoen dette innebar, og at det anbefaltes å iverksette passende sikringstiltak for å håndtere eventuell ny aktivitet fra trusselaktøren. Sistnevnte ble ikke tatt høyde for i tilstrekkelig grad. Dette er synlig gjennom hvor lang tid det tok før internettilkoblingen ble tatt ned av FM etter varsling. Det ser heller ikke ut til at FMHE ga et spesifikt ansvar for å gjennomføre dette sikringstiltaket til en bestemt person eller etablerte en tilstrekkelig vaktordning. NSM NorCERT på sin side gjennomførte forberedelser og planlegging for å overvåke deteksjonsløsningen. På operatørnivå ble dette imidlertid ikke fanget godt nok opp, noe som førte til lang varslingstid fra NSM NorCERT til FM. Mye tydet også på at passord til de ansatte var på avveie, men det ble vurdert at disse ikke skulle byttes da dette kunne gjøre angriperen bevisst på at den var oppdaget.

Ved hendelse HSØ har FFI fått lite innsikt i hvilke tiltak som ble iverksatt som ledd i den tekniske håndteringen. Det er kjent at det ble gjort et forsøk på å ta ned kompromitterte systemer og kaste trusselaktøren ut innledningsvis (takedown). Dette forsøket var ikke tilstrekkelig, noe som indikerte at trusselaktøren hadde penetrert dypere i systemene enn antatt. Det ble satt i gang administrative og organisatoriske tiltak, og både Sykehuspartner, Hdir og HSØ RHF etablerte kriseledelse. For å kunne reagere raskt ved eventuell nyoppdaget skadelig ondsinnet aktivitet, ble det tatt en avgjørelse om å delegere beslutningsmyndighet til lavere nivå for umiddelbar nedstengning av systemer. Denne beslutningsmyndigheten, som ikke ble benyttet, var forbeholdt situasjoner der den normale beslutningslinjen ble vurdert som for treg. Det ble også iverksatt en rekke tiltak ved de ulike helseforetakene i regionen, som primært ser ut til å ha vært rettet mot å kunne fortsette drift uten tilgang på datasystemene. Basert på tiltaksoversikter virker det som at enkelte HF-er savnet informasjon om bakgrunnen for enkelte av tiltakene Sykehuspartner ba disse HF-ene iverksette, samt mer informasjon om angrepet generelt. Sykehuspartner tok også ned enkelte tjenester som et ledd i sin håndtering.

Situasjonsrapportering

Grunnet at oppdraget inkluderer både rammeverk og instruks har vi herunder også involvert en bredere forståelse av situasjonsrapportering enn rammeverket alene legger opp til. I begge hendelsene var et større antall aktører enn rammeverket beskriver involvert, og det er derfor naturlig å inkludere forhold knyttet til dette.

I hendelse FM ser det ut til at NSM i all hovedsak har hatt kontakt med KMD. NSM har også informert JD og FD, i tråd med rammeverket. Fylkesmannsembetene, som må anses som rammet virksomhet, ble ikke informert innledningsvis med unntak av enkelte IKT-medarbeidere. Da

informasjon om hendelsen ble sendt til fylkesmennene, ble ikke denne informasjon videreformidlet til fylkesberedskapssjefene.

I hendelse HSØ ser det ut til at situasjonsrapporteringen i all hovedsak har foregått i helsesektoren, men med kontakt mellom NSM og JD. Situasjonsrapporteringen opplevdes utfordrende for flere av aktørene med utgangspunkt i flere forhold. For det første var det utfordringer knyttet til gradert informasjon. Her var utfordringene både knyttet til å motta, dele og behandle slik informasjon. For det andre var det usikkerhet knyttet til hva man skulle bidra med inn i situasjonsrapportene, særlig når situasjonen var tilsynelatende uforandret. Flere aktører opplevde at det kom rapporter med uendret informasjon. Det tredje forholdet som var utfordrende var manglende vurdering av forventet utvikling i situasjonsrapportering. Vi ser dette i sammenheng med tilsynelatende manglende tverretatlige konsekvensvurderinger.

Enkelte aktører hadde en forventning om å få informasjon tilbake, etter at de selv hadde delt informasjon med NSM. Andre opplevde at NSMs involvering bidro til at informasjonsdeling stanset opp. Noe av forklaringen kan være at NSM selv i enkelte tilfeller ikke satt på mer informasjon, og at det var begrensninger hos andre aktørers videreformidling av informasjon. Enkelte aktører opplevde også at informasjon som var delt med NSM, ble uten aktørenes godkjenning delt videre til andre.

Tilbakeføring og læring av hendelsen

De rammede aktørene har underveis eller i etterkant av hendelsene økt grunnsikringen av egne systemer og nettverk. Det ble for begge hendelsene utarbeidet evalueringsrapporter, med noe ulik innretning. For FM-hendelsen ble det lagd en konsekvensvurdering av den tidligere nevnte nedsatte gruppen, hvor mulig rammede verdier ble kartlagt. Denne ble utarbeidet i samarbeid mellom representanter fra FM, NSM, PST, DSB og KMD. For HSØ-hendelsen har både Hdir og HSØ RHF utarbeidet evalueringsrapporter som i stor grad omhandler krisehåndtering på et overordnet nivå. Det ble også lagd mer tekniske evalueringsrapporter fra Sykehuspartner og kommersielle aktører som har bidratt i hendelseshåndteringen, men disse ble delt med andre aktører i meget begrenset grad.

Begge hendelsene førte til at flere aktører har implementert eller forbedret planverk, eller laget planer om å utvikle og forbedre dette. Blant annet har aktører fra begge hendelsene henvist til at det er utviklet ulike scenarioer, og tiltak tilpasset disse. Samarbeidet og kommunikasjonen mellom enkelte av de sentrale beredskapsaktørene i det nasjonale krisehåndteringsapparatet er også forbedret. FMFA ble opprettet rett etter at hendelsen rammet FM. Dette var en organisasjonsendring som var planlagt før hendelsen inntraff, men beslutningen må antas å ha positiv effekt på det daværende fragmenterte ansvaret for IKT hos fylkesmannsembetene. Det er en fordel at drift av IKT-systemer nå er tillagt én enkelt aktør, framfor at hvert av embetene håndterer dette selv med varierende kompetanse og kapasitet. Det at IKT-driften er gitt til én aktør gjør det sannsynligvis også enklere å varsle riktig instans hvis en lignende hendelse skulle inntreffe.

6.2 Instruks for departementenes arbeid med samfunnssikkerhet

Samfunnssikkerhetsinstruksen stiller en rekke krav til departementene vedrørende systematisk risikostyring og etablering av oversikt over hvem som er ansvarlig for, og hvem som utfører, de ulike oppgavene i egen sektor. Instruksen beskriver også hva som er forventet av sentrale roller i en krise, som lederdepartement, Kriserådet og KSE. Det settes også krav til at departementenes arbeid med samfunnssikkerhet, skal basere seg på fire grunnleggende prinsipper (se kapittel 3.3).

I så måte gir ikke instruksen noen retningslinjer for hvordan departementene skal gjennomføre krisehåndtering, men i større grad hva grunnlaget er og hvilke forutsetninger som skal ligge til grunn. Dermed er det mulig å gjøre antakelser om hvordan instruksen kan ha påvirket håndteringen av hendelsene HSØ og FM, og i hvilken grad det er samspill mellom instruks og rammeverk.

7 Vurdering

Ved hendelsene HSØ og FM er det en rekke forhold som kan være gjenstand for vurdering og evaluering. Dette spenner fra de store linjene i hendelsene og håndteringen, til mer konkrete problemstillinger som oppstod underveis mens aktørene utførte hendelseshåndtering. Avhengig av den faglige forankringen for vurderingene vil ulike forhold være naturlig å belyse. Flere faktorer medvirker imidlertid til en høy kompleksitet i hendelsene og hendelseshåndteringen. Dette gjelder blant annet det nasjonale beredskapsapparatet, antall involverte aktører, de angrepne systemenes rolle i forvaltning og kritisk infrastruktur, systemenes størrelse, usikkerhet knyttet til risiko og konsekvenser, angripernes tekniske evne og i utgangspunktet skjulte agenda.

De ulike aktørene som deltar i håndteringen av IKT-sikkerhetshendelser, som hendelse HSØ og hendelse FM, har på overordnet nivå en sammenfallende intensjon og mål: Å løse hendelsene på en måte som er til det beste for de involverte og nasjonen Norge. Gitt ulike mandater og roller, er det imidlertid ikke uventet at aktørene vil ønske å balansere motstridende interesser og hensyn ulikt og å ha ulike prioriteringer. Dette kan føre til beslutningssituasjoner hvor noen aktører vil argumentere for ett utfall, og andre aktører for et annet. Slike situasjoner er naturlige, og ikke i seg selv et symptom på mangler eller svakheter i håndteringen. Ulike dilemmaer og avveininger som kan oppstå er benyttet som utgangspunkt for våre vurderinger.

I dette kapitlet beskrives og vurderes hendelsene og håndteringen først på et overordnet nivå. Hensikten er å belyse hva slags hendelser som har inntruffet, og hvordan hendelseshåndteringssystemet i stort har fungert. Deretter gjøres noen vurderinger om lærings- og overføringspotensialet fra denne type IKT-sikkerhetshendelser til andre typer IKT-sikkerhetshendelser, og om forskjellen mellom IKT-sikkerhetshendelser og andre typer hendelser. Videre følger noen vurderinger knyttet til mer spesifikke forhold ved de to hendelsene.

7.1 Hendelsenes karakter

Hendelse HSØ og hendelse FM har rammet ulike systemer i henholdsvis helsesektoren og hos fylkesmannsembetene, og er presumptivt gjennomført av ulike aktører. Likevel er det noen klare likhetstrekk mellom hendelsene. Det er tilsynelatende avanserte aktører som har vært ute etter informasjon, og som har forsøkt å operere skjult eller lite synlig. De har kompromittert IKT-nettverk der det blant annet finnes sensitive data om norske borgere, og IKT-systemer som inngår i viktige tjenesteleveranser for samfunnet. Da aktørene først ble oppdaget, gjorde de tilsynelatende ikke aktiv motstand da de ble forsøkt kastet ut. FFI har ikke sett informasjon som tyder på at nedstengning av tjenester (tilgjengelighetsangrep) eller endring av informasjon (integritetsangrep) var en målsetning med angrepene.

Hendelsene framstår i etterkant som enkle å forstå, rent prinsipielt: Det var to datainnbruddshendelser med tapping av informasjon. Størrelsen på systemene som potensielt ble rammet var i det ene tilfellet meget stor, med en infrastruktur som er kompleks og uoversiktlig (hendelse HSØ). I det andre tilfellet var systemene mye mindre relativt sett, men med mye sensitiv

informasjon (hendelse FM). Den tekniske håndteringen hos rammet aktør var i begge tilfeller en oppryddingsoperasjon i etterkant av påvist kompromittering, med enkelte utfordringer knyttet til å bestemme hva som var mest hensiktsmessig framgangsmåte (f.eks. videre overvåking av trusselaktøren). Andre aktører, som de nasjonale sikkerhets- og etterretningstjenestene, gjorde også et teknisk arbeid knyttet til attribusjon og etablering av hendelsesforløp blant annet for etterforskingsøyemed og styrking av nasjonal situasjonsforståelse.

Mulige operative konsekvenser av angrepene, inklusive mulige negative konsekvenser av den tekniske håndteringen, var imidlertid forskjellige. Hovedbekymringen for HF-ene i helseregion HSØ var de umiddelbare implikasjonene for kritisk tjenestetilbud som helseforetakene er avhengig av for å ivareta pasientenes liv og helse. Tilgjengelighet og integritet er sentralt for at helseforetakene skal kunne gjøre sitt arbeid på en tilfredsstillende måte.[26] Hovedbekymringen for fylkesmannsembetene var i mye mindre grad tidskritiske tjenesteleveranser, men heller mengden av sensitive opplysninger om norske borgere som ikke skal komme på avveie.

I hendelse HSØ var det en reell risiko for at eksterne brukere av rammet infrastruktur fikk og måtte håndtere negative konsekvenser av angrepet mens håndteringen pågikk. Hendelsen traff Sykehuspartner som systemeier og driftsansvarlig, og som en større kritisk tjenesteleverandør, til flere helseforetak som igjen tjener en betydelig del av Norges befolkning. Angrepet utløste dermed en sektorbred håndtering, med både systemeier (Sykehuspartner HF), direkte operative «kunder» (helseforetak og HSØ RHF) og koordinerende elementer på direktorats- og departementsnivå.

Selv om konsekvensene for det umiddelbare tjenestetilbudet var hovedbekymringen ved hendelse HSØ, så nyanserer to forhold dette bildet. Det ene er at helsesektoren generelt er godt forberedt på å utøve sitt arbeid under vanskelige forhold. Om frafall av digitale tjenester skyldes flom, brann eller cyberangrep, så er helsepersonell forberedt på å klare seg med de ressursene som er tilgjengelig, og på å måtte prioritere mellom kritiske oppgaver. Det andre er at det finnes mye sensitiv informasjon i Sykehuspartners infrastruktur, som pasientopplysninger og forskningsdata. Dette gjør at selv om tilgjengelighet og integritet er sentralt, så er konfidensialitet også viktig ved denne hendelsen.

I hendelse FM rammes i utgangspunktet kun selve fylkesmannsembetene, mer som en intern hendelse. Det er ingen kritiske operative «kunder» av fylkesmannsembetene som blir berørt, selv om sensitiv informasjon om fylkets befolkning kunne vært på avveie. Håndteringen ble gjort av personell fra IKT-miljøer fra enkelte av embetene, som er mye mindre sammenliknet med IKT-miljøet hos en aktør som Sykehuspartner. NSM NorCERT støttet både den tekniske håndteringen og KMD som ansvarlig departement, men i sum var det likevel et mye mindre håndteringsregime som ble iverksatt i denne hendelsen. Dette gjelder selv om alle 16 fylkesmannsembetene potensielt var berørt.

[26] Dette gjelder planlagte operasjoner og andre helsetilbud der informasjon i datasystemene og IKT-tjenester er nødvendige. I akutte situasjoner der ingen informasjon er tilgjengelig i utgangspunktet er det mye mindre avhengighet av IKT-systemer.

Hendelse HSØ framstår som en kompleks og omfattende hendelse å håndtere for de involverte aktører, gitt antallet aktører som hadde en rolle i eller ble påvirket av håndteringen, kombinert med omfanget av de potensielt rammede systemene. Hendelse FM framstår som mindre kompleks sett fra samme perspektiv, selv om dette ikke betyr at håndteringen av denne hendelsen ikke var utfordrende. Kompleksiteten i begge hendelsene ser imidlertid noe annerledes ut dersom en begrenser seg til å se på trusselaktørene som informasjonsinnsamlere. Hendelsene kan ses på som «enkle» i den forstand at mer ondsinnede handlinger som sletting av data, endring av data og tjenestenekt ikke forekom. En situasjon hvor trusselaktøren aktivt opptrer destruktivt ved oppdagelse, eller med vilje utfører sabotasje etter skjult inntrengning, kan medføre ekstra komplikasjoner fra et håndteringsperspektiv som ikke er tilstede ved en situasjon hvor målet er skjult lekkasje av informasjon. Fraværet av dette betyr imidlertid ikke at hendelsene kan anses som enkle å håndtere.

7.2 Håndteringens mangfold

I særlig hendelse HSØ var det mange aktører som hadde et ansvar i håndtering av hendelsen. Aktørkartet framstår som forholdsvis uoversiktlig og komplisert, og ikke alle ansvarslinjer var klare og tydelige. Noe av denne kompleksiteten skyldes hvilke mandater og roller ulike aktører har blitt tilordnet eller delegert på nasjonalt nivå. En annen årsak er kompleksiteten i verdikjeder, hvor flere aktører integrerer felles IKT-infrastruktur i deres arbeidsflyt. Angrep på infrastruktur kan dermed utløse følgekonsekvenser som det er vanskelig å forutsi på forhånd eller få oversikt over underveis. Dette medfører også at å bestemme ansvarsfordelingen for håndtering blir utfordrende.

Et komplisert aktørkart er i seg selv ikke nødvendigvis et problem for håndteringen av denne typen hendelser. Flere aktører har funnet sammen i klynger, ut i fra konkrete utfordringer og samarbeidsbehov. Med *klynge* menes en gruppe aktører, som i disse tilfellene arbeidet sammen. Rent prinsipielt er klyngene ikke bundet til ett spesifikt nivå, selv om mange av aktørene i en enkelt klynge ofte vil tilhøre samme nivå. I hendelse HSØ har vi identifisert følgende klynger:

- Teknisk håndtering, med Sykehuspartner HF i sentrum. Her bidro også NSM NorCERT, HelseCERT og de kommersielle aktørene som ble leid inn av Sykehuspartner. I FCKS støttet eller avga de andre partene (PST, Etterretningstjenesten og Kripos) samt CYFOR personell til NSM NorCERT. I de andre HF-ene var det også tekniske IKT-miljøer som iverksatte tiltak som følge av hendelsen. Basert på tiltaksoversikter, virker det som om disse miljøene opererte for selv seg etter instruksjon fra Sykehuspartner og egen ledelse. Som omtalt i kapittel 4.1, håndterte Helse Vest IKT et tilsvarende forsøk på datainnbrudd i sin infrastruktur samt nedstengning av en VPN-tunnel. Utover dette har ikke FFI grunnlag for å uttale seg om hvordan Helse Vest IKT AS har deltatt i håndteringen av hendelse HSØ.

- Beredskapsledelse i regionen HSØ, med HSØ RHF som leder. Ledelsen og IKT-sikkerhetssjefene i HF-ene deltok. Her ble det koordinert og delt informasjon mellom HF-er i regionen, både de som var direkte rammet av hendelsen og andre som kunne bli berørt.

HF-ene planla og gjennomførte en rekke tiltak, deriblant preventive tiltak for å være bedre forberedt på å håndtere konsekvensene dersom IKT-angrepet viste seg å være større enn antatt. Tiltakslister fra de ulike HF-ene ble sammenstilt og spredt til alle HF-er og videre oppover.

- Koordinering i helsesektoren, med Hdir i sentrum. Hdir benyttet mest interne ressurser, men hadde også enkelte eksterne medlemmer med i sitt kriseutvalg, deriblant administrerende direktør fra HSØ RHF og Sykehuspartner HF, Direktoratet for e-helse og DSB. Hdir fikk delegert ansvar fra HOD, noe som er vanlig praksis i hendelser som rammer helsesektoren.

- Koordinering på strategisk nivå, med JD som lederdepartement. Her var det løpende dialog med NSM NorCERT som rådgiver samt dialog med andre sentrale departementer og aktører på dette nivået. Det ble avholdt to møter i Kriserådet.

- Avklaringer om Nødnett, bestående av aktører med felles bekymring for koblingen mellom HSØ og Nødnett. Inkludert her var HDO, NHN, HelseCERT og HOD. DSB ser ikke ut til å ha vært involvert i særlig grad, på tross av at de er eier og forvalter av Nødnett.

- Koordinering mellom de nasjonale sikkerhets- og etterretningstjenestene og politiet v/Kripos, gjennom FCKS. Her ble partenes respektive oppfølging av hendelsen i henhold til tjenestenes mandater koordinert. I følge FCKS ble det også produsert et situasjonsbilde til beslutningstakere som var omforent blant partene.

Det har vært tilsynelatende lite samhandling og interaksjon mellom klyngene. Enkelte aktører har ikke kjent til flere av de andre klyngene som har vært virksomme. Et fåtalls aktører har vært til stede i flere klynger.

Vår vurdering er at disse klyngene har interagert lite med hverandre på grunn av hendelse HSØs karakter. Behovet for tettere koordinering mellom klyngene har tilsynelatende ikke vært til stede, i stor grad fordi håndteringen gikk ut på å gjenopprette normal tilstand og dempe eventuelle negative følger av kompromittering og håndtering. Dersom hendelsen hadde gått over til å bli en mer langvarig sabotasjeoperasjon hvor hensikten var å ødelegge, mener vi at for eksempel verdi-vurderinger knyttet til tekniske prioriteringer og operative følgekonsekvenser ville kunne være et element som flere klynger ville følt seg berørt av, og dermed framtvunget en diskusjon på tvers av klyngene. Her ville motstridende interesser og risikovurderinger kunne ha møtt hverandre og flere dilemmaer oppstått, med flere aktører som trekker i forskjellige retninger. Det kan være vanskelig å opprettholde separate klynger i en slik situasjon; i det minste må en kunne regne med at flere aktører vil oppleve å ha en aksje i håndtering som skjer i flere klynger.

En indikasjon på dette kan ses i håndteringen av hendelse FM. Her er det færre separate klynger enn for hendelse HSØ, antakeligvis fordi antall involverte aktører er mindre. Vi har identifisert følgende klynger:

- Teknisk håndteringsklynge, med utvalgte personer fra berørte IKT-miljøer i fylkesmannsembetene i sentrum. Støttet av NSM NorCERT.

- Klynge for operative vurderinger, med KMD, PST, NSM NorCERT og DSB samt representanter for både IKT-miljøene og beredskapsmiljøene hos fylkesmannsembetene. Dette er den tidligere omtalte gruppen som ble nedsatt i midten av november 2018. Den møttes 3– 4 ganger og leverte en rapport som sluttprodukt i februar 2019.

- Strategisk beslutningsklynge, med KMD i sentrum. Støttet av NSM NorCERT. Andre departementer (DFU) og representanter fra enkelte fylkesmannsembeter ble trukket inn ved behov.

- Koordinering mellom de nasjonale sikkerhets- og etterretningstjenestene og politiet v/Kripos, gjennom FCKS. Her ble partenes respektive oppfølging av hendelsen i henhold til tjenestenes mandater koordinert. I følge FCKS ble det også produsert et situasjonsbilde til beslutningstakere som var omforent blant partene.

I håndteringen av hendelse FM tvang tekniske dilemma seg fram som et tema i flere klynger, typisk fra det tekniske til det operative og strategiske, på grunn av mulige operative følge-konsekvenser (dilemmaet overvåking versus gjenoppretning). De andre klyngene ble involvert og diskusjoner gikk mellom aktører på flere nivåer.

Det at hendelsene ble håndtert i disse klyngene, med lite kommunikasjon og samvirke seg imellom, ser ikke ut til å ha ledet til klare eller store konsekvenser. Aktørene har i stor grad arbeidet i henhold til deres ansvar og roller. Det kan også ha vært positive virkninger for enkelte ved arbeid i klynger, ved at personellet ble skjermet for unødig innblanding og kunne arbeidet målrettet med sine oppgaver. Dersom hendelsene hadde utviklet seg annerledes, og medført større eller andre typer konsekvenser, kunne det imidlertid ha vært behov for tettere samvirke mellom klyngene. Dette gjelder både informasjonsdeling og samarbeid, innad i og på tvers av ulike nivåer og sektorer. Basert på den tilsynelatende manglende samhandlingen og interaksjon mellom klyngene under disse hendelsene, vil FFI understreke at dette må tas høyde for i forberedelser av og planlegging for håndtering av framtidige hendelser. Ved en hendelse som skulle kreve at aktører i ulike klynger samarbeider er det av betydning at det finnes mekanismer og rutiner for at disse effektivt finner sammen.

7.3 Hendelsenes egenart og overføringspotensial

Herunder vil vi diskutere i hvilken grad hendelse HSØ og hendelse FM var unike og hvorvidt hendelsene og håndteringen av dem kan overføres som læringspunkter til eventuelle framtidige IKT-angrep.

En IKT-sikkerhetshendelse vil ofte ha enkelte karakteristikker som påvirker hendelseshåndtering sammenliknet med andre typer hendelser. For det første vil det typisk være mye usikkerhet rundt hva som har skjedd, og hva konsekvensene er eller vil kunne bli dersom hendelsen utvikler seg.

Dette skyldes at mye av hendelsesforløpet og de første konsekvensene skjer i det digitale domenet. Sammenliknet med hendelser som brann, flom og terrorangrep vil enkelte typer IKT-hendelser ofte være mer usynlige og vanskelige å avgrense før undersøkelsesarbeid er gjort.

Avhengig av de rammede systemenes kompleksitet, kan svært mye arbeid måtte gjøres for å i det hele tatt forstå og avgrense hendelsen og dens potensielle konsekvenser. Slikt analytisk arbeid og IKT-hendelseshåndtering generelt krever svært mye kompetanse. En kompliserende faktor er at selv om ekspertkompetansen til en fagspesialist er høy og denne har erfaring med relevante analyseteknikker og verktøy, så kreves det ofte spesifikk dybdekunnskap om de faktiske systemene som er rammet. Dette gjør at rask innhenting av relevant støtte utenfra er utfordrende, utover mer generell prosesskompetanse for håndtering eller for delegering av spesifikke tekniske analyseoppgaver. Samtidig er det behov for kunnskap om hvordan avanserte trusselaktører opererer, og hvordan deres operasjoner best kan avdekkes, kartlegges og håndteres.

Gitt en høy grad av usikkerhet som ofte er begrunnet i svært tekniske detaljer knyttet til IKT-systemer, blir kommunikasjon med beslutningstakere og mer operativt personell som må håndtere følgekonsekvenser i det fysiske domenet ofte utfordrende. Enkelte dilemmaer, som overvåking og læring versus hurtig gjenoppretting, framtvinger avveiinger en ikke fullt så ofte ser i mer vanlige krisesituasjoner. Spenningen mellom å informere berørte mest mulig, og å holde tilbake informasjon for å gjøre den tekniske håndteringen best mulig, er også et vedvarende dilemma der håndtering av operative konsekvenser potensielt vil lide til fordel for en god og skadebegrensende teknisk håndtering.

Hendelse HSØ og hendelse FM har begge vist seg å være hendelser som tilsynelatende primært omhandler informasjonslekkasje, i alle fall sett i lys av mulighetene for tilgjengelighetsangrep og integritetsangrep. Enkelte funn knyttet til hendelsene anser vi for å være generelle og kan dermed også potensielt gjelde for andre typer hendelser. Dette inkluderer kjente forhold som behov for og utfordringer knyttet til utveksling av gradert informasjon, manglende planverk, behov for rolleavklaringer og så videre. Andre funn gjelder i større grad kun IKT-sikkerhetshendelser, herunder utfordringer med å kommunisere implikasjonene av et IKT-angrep til personer uten IKT-kompetanse på en forståelig måte, usikkerheten knyttet til hvor godt situasjonen er blitt forstått og så videre.

I tillegg må det stilles spørsmål om i hvilken grad det er mulig å overføre mer detaljert lærdom fra disse spesifikke hendelsene, til andre typer IKT-sikkerhetshendelser. For eksempel, kan vi bestemme om tilnærmingen til hendelseshåndtering ved disse hendelsene, vil være velfungerende for IKT-angrep hvor målet for eksempel er sabotasje og ikke informasjonsuthenting? På generelt grunnlag mener vi dette er vanskelig, primært fordi det er vanskelig å vite om de identifiserte klyngene hadde fungert like godt som de fungerte under disse hendelsene. Som nevnt tidligere antar vi at det i alle fall vil bli behov for tettere interaksjon mellom klynger i slike tilfeller.

7.4 Spesifikke forhold ved hendelse HSØ

Hendelse HSØ peker seg ut – sammenlignet med hendelse FM – ved at det er mange aktører som er involvert i håndteringen. Aktørene kommer fra ulike miljøer, og har ulik kultur for hvordan hendelser håndteres og informasjon om dette deles. Eksempelvis møter miljøer hvor hemmelighold og gradering av informasjon både er korrekt og påkrevd, miljøer hvor en høy grad av intern og offentlig informasjonsdeling er et sentralt element i vanlig hendelseshåndtering. Videre legger miljøene ulike hjemler og sensitivitetsvurderinger til grunn for skjerming av informasjon, utover graderingskravene i sikkerhetsloven. Dette inkluderer taushetsplikt med tanke på personopplysninger, men tilsynelatende også et mer virksomhetsforankret rasjonale om å dele lite om håndteringen som gjøres i egen virksomhet. Utfordringer oppstår når disse miljøene må arbeide sammen, samtidig som de vurderer informasjon forskjellig og dermed ønsker ulik spredning.

Vurderinger om sensitivitet og ønsket om tilbakehold medfører at kommunikasjonen med brukere og ansatte om hva som foregår blir mindre åpen enn for andre typer hendelser. I tillegg er det enkelte aktører som hadde forventet å bli informert og involvert i håndteringen, som ikke blir tatt med. Helt spesifikt gjelder dette Fylkesmannen, som har et generelt samordning- og beredskapsansvar og oppfølgings- og tilsynsansvar gjennom fylkeslegen.

De ulike HF-ene iverksatte og forberedte en rekke tiltak i forberedelse på at sentrale IKT-tjenester kunne gå ned. I en slik kontekst anser FFI det som naturlig at eksempelvis DSB og Fylkesmannen, grunnet deres beredskapsansvar, hadde blitt informert. I lys av de potensielle konsekvensene angrepet kunne fått burde føre-var-prinsippet vært førende for informasjonsdeling. Akkurat hvordan og av hvem beslutningen om å utelate sentrale beredskapsaktører ble tatt, har vi ikke fått klarhet i. Det kan godt være at dette ikke var en bevisst beslutning, men at ingen aktører så det som naturlig, og under sitt ansvar, å kontakte disse.

Begrenset informasjonsdeling kan forstås ut ifra et generelt ønske om å begrense spredning av informasjon om håndtering – mens trusselaktøren fremdeles kan være ukjent med at denne er oppdaget. FFI mener imidlertid at når Norge har valgt å ha en beredskapsordning med en bestemt innretning, så må den også benyttes (forberedes) i de situasjoner hvor anvendelse er et reelt alternativ. Eksempelvis burde Fylkesmannen ha blitt konsultert og informert om muligheten, så lenge usikkerheten knyttet til operative konsekvenser var stor.

Informasjonsdelingen fra Sykehuspartner til enkelte aktører som skulle bidra med teknisk hendelseshåndtering har vært utfordrende. På tross av at Sykehuspartner og HSØ RHF rapporterer om et meget godt samarbeid, har NSM NorCERT vært klare i sine beskrivelser av utfordringene knyttet til å få tilgang til systemene som skulle undersøkes. Tilgang til enkelte typer data tok det ukesvis å få, mens andre typer tilganger aldri ble gitt. Utover det som er allment kjent har FFI fått svært lite innsikt i det tekniske hendelsesforløpet eller den tekniske håndteringen direkte fra Sykehuspartner

Det er naturlig at taushetsplikt og muligheten for å komme over sensitive pasientopplysninger legger begrensninger på hva slags tilganger som kan gis til tredjepart. Samtidig framstår det som et paradoks at dette og andre hensyn skal hindre en nasjonal sikkerhetstjeneste i å undersøke og bidra til håndtering av denne type hendelse, når trusselaktører har tilgang til systemene.

I denne hendelsen er enkelte parter uenige om informasjonstilgangen som ble gitt var tilstrekkelig eller ikke. FFI har ikke fått tilstrekkelig innsikt i detaljene til å kunne avdømme dette i denne saken, men har noen generelle betraktninger om slike forhold. Tjenstlig behov bør styre tilgang til systemer og informasjon. I en fase hvor omfanget på kompromittering er ukjent, bør teknisk personell som leter etter spor få tilgang til de systemer som anses som relevante – gitt deres kunnskap om hvordan slike trusselaktører opererer. Dersom dette inkluderer systemer med sensitive data, bør midlertidig tilgang autoriseres. Etter innledende undersøkelser kan autorisasjon trekkes tilbake, dersom undersøkelser ikke finner spor etter trusselaktøren og videre tilgang ikke er nødvendig. Alternativet er å begrense mulighetene for undersøkelser før omfanget er kjent, noe som kan føre til at spor forblir uoppdaget og omfanget av kompromitteringen feilvurdert.

En generell anbefaling fra FFI, dersom en liknende hendelse skulle oppstå i framtiden, er at relevant teknisk personell fra sikkerhets- og etterretningstjenestene som skal bistå i arbeidet, blir midlertidig autorisert for den type sensitiv informasjon som de kan komme over i sitt tekniske arbeid i tråd med tankegangen over. Dette innebærer at de blir holdt ansvarlig opp imot de retningslinjer og krav som følger en slik type tilgang. Slik autorisasjon bør kunne gis forholdsvis hurtig dersom de formelle linjene gås opp i forkant, da dette personellet allerede vil være sikkerhetsklarert og autorisert til et høyt nasjonalt nivå. Dette gjelder generelt der statlige virksomheter og eiere av kritisk infrastruktur blir rammet, også utover helse- og omsorgssektoren. Samordningsetater som DSB og Fylkesmannen har også sikkerhetsklart personell, som fort kan autoriseres dersom de vil kunne ha en rolle i håndteringen og trenger informasjon. Det påpekes at denne anbefalingen er generell, og uavhengig av det faktiske hendelsesforløpet i hendelse HSØ.

7.5 Spesifikke forhold ved hendelse FM

Dilemmaet om å overvåke aktøren framfor å stenge ned systemene var sentralt under hendelse FM. Dette delkapitlet omhandler diskusjon omkring dette dilemmaet, spesielt med tanke på beslutningsmyndighet. Avslutningsvis diskuteres informasjonsdeling.

Under håndteringen av hendelse FM ble det opprettet en tverretatlig arbeidsgruppe. FFI mener at dette kan være et godt tiltak i håndteringen av slike hendelser. I dette tilfellet ser det imidlertid ut til at formålet med gruppen har vært tolket forskjellig av de ulike aktører. Tidsvinduet mellom oppdagelsen av hendelsen (22. oktober 2018) og etablering av arbeidsgruppen (7. november 2018) framstår også som for stort. Hvis hensikten med gruppen var å bidra i selve håndteringen, er to og en halv uke meget lang tid da hendelsen kan ha utviklet seg betydelig i løpet av denne perioden.

Ved hendelse FM utviklet det seg uenighet blant aktørene om veien videre ved den tekniske håndteringen. På grunn av manglende oversikt over infrastrukturen og omfanget av hendelsen

anbefalte NSM NorCERT å overvåke videre framfor å forsøke å kaste trusselaktøren ut og starte gjenoppretting. NSM NorCERT anbefalte også iverksetting av sikringstiltak for å sikre mot ytterligere skade (se kapittel 6.1, «Iverksetting av prosesser og tiltak for å håndtere hendelsen»). Alle aktørene hadde presumptivt et ønske om å gjennomføre best mulig håndtering, her ensbetydende med gjenoppretting til normal tilstand, men det var uenighet om hva som var mest hensiktsmessig.[27] Slik FFI forstår det tok KMD en beslutning om at systemet skulle forbli oppe og aktøren overvåkes. Dette var i tråd med NSM NorCERTs anbefaling, men imot informasjonseiers – det vil si berørte fylkesmannsembetenes – ønske. FM ble heller ikke, slik FFI forstår det, involvert i beslutningsprosessen, men hadde motforestillinger mot beslutningen som ble tatt når de ble kjent med denne. Innvendingene ble ikke tatt til følge, og beslutningen om at aktøren skulle overvåkes ble opprettholdt.

Hvem som bør ta den endelige avgjørelsen om hvilke tiltak som skal eller ikke skal iverksettes i slike tilfeller, og på hvilket grunnlag den bør bli tatt, er ikke helt opplagt. Problemstillingen omfatter generelt sett både hvem som faktisk har myndighet til å ta beslutningen, hvem som har best innsikt i verdier og risiko ved ulike handlemåter, muligheten for eventuelle skadereduserende tiltak og hvilke hensyn som skal veie tyngst. De som eier verdiene, og som forstår verdikjedene disse er en del av, antas i utgangspunktet å være de som er best skikket til å vurdere mulige skadevirkninger av ytterlige kompromittering. Det kan diskuteres om det faktum at en aktør eier og er ansvarlig for ivaretakelse av verdier, automatisk medfører best innsikt i mulige skadevirkninger og hva som er den mest hensiktsmessige veien videre når verdier ses fra et nasjonalt perspektiv. Likevel kan det anses som en uheldig presedens at eiers ønske om videre håndtering av egne verdier settes til side, spesielt dersom ansvaret både juridisk og mer uformelt oppleves å være plassert hos eieren.

I dette tilfellet var utfordringen å best kunne vurdere hva som var mest hensiktsmessig fra et teknisk perspektiv for å lykkes med å kaste ut aktøren, mens sannsynligheten for ytterligere skade ble minimert. Dette er en diskusjon som i mindre grad handler om motstridende verdivurderinger, men heller om trusselaktørens mulige tilganger til de kompromitterte systemene. Det er svært vanskelig å skulle vurdere hva som er korrekt for en gitt hendelse tilbake i tid, uten ha et betydelig bedre informasjonsgrunnlag enn det aktørene selv satt på. Vår anbefaling er at de involverte aktører ved denne type tekniske uenigheter får anledning til å sette sammen et beslutningsunderlag og gjennom denne prosessen komme til enighet. I en slik prosess må kunnskap og kompetanse stå sentralt.

Det er ulike meninger ved denne hendelsen om KMD faktisk har instruksjonsmyndighet overfor Fylkesmannen i et tilfelle som dette, der de respektive embetene tilsynelatende står rettslig ansvarlig for ivaretakelse av verdiene. Enkelte fylkesmannsembeter argumenterer for at de har forvaltningsloven, offentleglova og både ny og gammel sikkerhetslov på sin side. Ut ifra disse lovene har de en plikt og en rett til å ta beslutninger vedrørende sine verdier og sin informasjon. KMD på sin side har argumentert for at instruksmyndigheten de har over sine underlagte etater gir dem rett til å overstyre slike beslutninger. I dette tilfelle hadde KMD også støtte fra de ulike

[27] Det kan også være andre grunner til å fortsette overvåking av et kompromittert system, som å lære mer generelt om aktørens handlemåte. Det var ikke tilfellet i denne hendelsen.

fagdepartementene i DFU. En ytterligere kompliserende faktor er at det framstår som uklart hvem som faktisk eier de relevante informasjonssystemene i denne hendelsen. FFI har underveis hatt intervjuer med alle vi antar kan være potensielle eiere uten at dette har gitt oss svar på hvem som er informasjonssystemeier. Både hvem som er systemeiere og hva som er styrende av forskrifter og instrukser, bør være mulig å avklare. Hvem som har beslutningsmyndighet bør kunne avklares ved å involvere de rette instanser, slik at aktørene får dette stadfestet før eventuelle framtidige hendelser.

Da NSM NorCERT anbefalte overvåking framfor å stenge ned systemene, kommuniserte de samtidig at det var viktig å iverksette passende sikringstiltak for å unngå ytterligere skade av verdier. Anbefalingen om sikringstiltak ser ikke ut til å ha blitt tatt hensyn til i tilstrekkelig grad. Dette tolker FFI ut ifra at en ansatt ved FMHE måtte fysisk reise ned til FMHEs lokaler for å kunne slå av internettilkoblingen da alarmen gikk 24. desember. Samtidig var det gjort forberedelser og lagt planer hos NSM om overvåking av deteksjonsløsningen, som ikke ble fanget opp godt nok på operatørnivå. Det er store mengder data som kan kopieres ut i løpet av et halvt døgn. Mulige ekstra sikringstiltak kunne ved denne hendelsen eksempelvis være en teknisk eller annen type ordning hos FM slik at internettilkoblingen kunne tas ned eller skadevaren stanses umiddelbart etter ønske. Spesielt i en situasjon hvor informasjonseier er uenig i avgjørelsen, bør ekstra innsats legges ned for å begrense mulig skadeomfang som følger av beslutningen. Dersom eieren har lite ressurser til rådighet, bør denne tilføres økte ressurser for å kunne etablere tilstrekkelig sikringstiltak.

Det var også under hendelse FM utfordringer knyttet til informasjonsdeling. Det at det faktisk hadde skjedd en hendelse, og muligheten til å vurdere konsekvensene denne kunne ha, ble ikke kommunisert tilstrekkelig til fylkesmannsembetene. Innledningsvis er dette forståelig da det potensielt kunne være 16 rammede embeter, hvor ansvaret for IKT var fragmentert og uoversiktlig. Det oppfattes derfor som naturlig at KMD, som driftsansvarlig for embetene, ble et riktig kontaktpunkt. Imidlertid tok det lang tid før embetene ble varslet, og heller ikke når informasjon ble gitt fylkesmennene ble fylkesberedskapssjefene informert. Med tanke på det sentrale ansvaret fylkesberedskapssjefene har for beredskap på regionalt nivå oppfattes dette som uheldig. FM har uttalt at Fylkesmannens samfunnssikkerhetsinstruks ikke ble vurdert tatt i bruk, da FM ikke hadde nok informasjon til å vite om de skulle samordne eller ikke.

Det har underveis i oppdraget vært vanskelig å få tak på årsaken til denne manglende informasjonsdelingen, både til embetene generelt og fylkesberedskapssjefene spesielt. I følge NSM var det en forventning om at KMD skulle varsle embetene, og når KMD varslet fylkesmennene hadde KMD en forventning om at de skulle videreformidle til de som hadde behov for informasjon. Det som derfor synes som mest sannsynlig er at fylkesmennene ikke har delt informasjon videre enten grunnet usikkerhet knyttet til hvorvidt det var greit å dele informasjon, en oppfattelse om at det ikke skulle deles videre, eller at det ble vurdert som hensiktsmessig å vente til ytterligere undersøkelser og avklaringer forelå. FFI anbefaler imidlertid at både kommunikasjon og beredskapsansvar tydeliggjøres på alle nivåer slik at de riktige og nødvendige aktørene kan få den informasjonen de har behov for. Med utgangspunkt i ansvaret FM har for egne verdier og informasjon bør det også være naturlig at de ikke bare informeres, men også får

en reell mulighet til i bidra i håndteringen. Som informasjonseier vil FM kunne ha viktige bidrag i diskusjoner om verdier og hvilke tiltak som bør iverksettes.

8 Betraktninger om rammeverk og instruks

I dette kapitlet vil vi presentere betraktninger om rammeverk og instruks. Betraktningene har tatt utgangspunkt i hendelser i fredstid.

8.1 Rammeverk

Det er gjennom oppdraget framkommet flere ulike meninger om rammeverket fra informantene. Enkelte av deres meninger er basert på erfaringer aktørene har hatt under håndteringen av hendelse HSØ og hendelse FM, mens andre av deres meninger om rammeverket er mer uavhengig av disse to spesifikke hendelsene. FFI har også, basert på egen kunnskap og kompetanse, vurdert rammeverket i lys av hendelsene og på mer generelt grunnlag. Selv om hendelse HSØ og hendelse FM ikke har et stort nedslag på tvers av sektorer, anser FFI at hendelsene er omfattende nok til å belyse rammeverket.

Rammeverket var i varierende grad kjent for aktørene på virksomhetsnivå. Innvirkningen av rammeverket på virksomhetenes hendelseshåndtering ser ut til å har vært begrenset. Enkelte informanter på virksomhetsnivå kjente ikke til rammeverket, mens noen av aktørene som kjente til rammeverket mente at det ikke var relevant. Av aktører på virksomhetsnivå som opplevde rammeverket som nyttig, var særlig etableringen av et felles begrepsapparat og strukturen det gir hendelseshåndteringen framhevet.

Rammeverket ble publisert relativt kort tid før hendelsene. Vi mener dette til dels kan forklare at rammeverket var ukjent for flere virksomheter. Samtidig er det ikke gitt at en virksomhet blir klar over rammeverket før en hendelse inntreffer. En virksomhet kan bli gjort oppmerksom på rammeverket av andre aktører virksomheten kommer i kontakt med i forbindelse med hendeselshåndteringen.

På SRM-nivå oppleves rammeverket å være nyttig for å bygge opp et SRM, gjennom de kravene som stilles. Når en hendelse først inntreffer, har imidlertid ikke rammeverket så stor betydning for håndteringen på dette nivået. Det oppleves også at rapporteringssystemet som rammeverket beskriver i liten grad er operasjonalisert på virksomhetsnivå. Med dette menes rapportering fra virksomhetene til SRM og NSM om hendelser på et standardisert format og etter visse kriterier. Virksomhetene som samarbeidet med SRM under hendelsene opplevde dette som et godt og fruktbart samarbeid.[28]

Rolleforståelsen for NSM NorCERT varierer blant virksomhetene. Ved en IKT-sikkerhetshendelse er det den rammede virksomhetens sitt eget ansvar å håndtere hendelsen. NSM NorCERT sin rolle vil være å koordinere, veilede og rådgi, og hvis mulig bistå med ressurser for å blant annet skape en sektorovergripende situasjonsforståelse. Funnene fra intervjuene tyder på at enkelte aktører antok at NSM kunne bidra mer i selve håndteringen av hendelsen enn det de gjorde. Det er også framkommet et ønske om NSM kan ta en mer aktiv rolle under håndteringen

[28] I praksis kun hendelse HSØ da det ikke finnes et SRM for fylkesmannsembetene.

av en hendelse, inkludert organisering av håndteringen, gjøre prioriteringer og komme med anbefalinger for beslutninger som må tas. En slik rolle går imidlertid utover rollen NSM har. NSM erfarte selv under og i etterkant av hendelsene at de bør tydeliggjøre hva de kan bistå med og ikke, og hva rollen deres er. Dette kan tyde på et behov for å oppdatere rammeverket på dette punktet.

På generelt grunnlag er det viktig å påpeke at NSM er prisgitt at aktørene de skal bistå i hendelseshåndteringen gir NSM tilgang til nødvendig informasjon og systemer som virksomhetene besitter. NSM har ikke myndighet til å kreve tilgang eller legge beslag på virksomhetenes eiendeler, slik som politiet har. Tilgang til nødvendig informasjon og systemer er avgjørende for at NSM skal kunne bistå på en tilfredsstillende måte i hendelseshåndtering av IKT-sikkerhetshendelser. Gitt NSMs andre samfunnsoppgaver, som overvåking med VDI, er den manglende politimyndigheten naturlig. Imidlertid er NSM avhengig av at rammede aktører gir de nødvendige tilganger for å kunne bistå på en god måte. Dette punktet bør tydeliggjøres i rammeverket.

Etter vår vurdering framstår rammeverket på virksomhetsnivå primært som nyttig for virksomheter og miljøer med begrenset kompetanse og kapasitet innen IKT-sikkerhet, og lite kjennskap til NSM NorCERT og SRM-er. Virksomhetene blir eksponert for et begrepsapparat og sentrale forhold ved håndtering av IKT-sikkerhetshendelser. Større virksomheter vil trolig ha mer kunnskap om dette allerede i virksomheten. Imidlertid er det meget krevende, særlig for mindre virksomheter, å leve opp til de forutsetningene som rammeverket legger til grunn. I praksis må forutsetningene ses på som en form for krav til virksomhetene, og de er omfattende. Det er mange ulike vurderinger, som verdivurderinger, skadevurderinger og konsekvensvurderinger, som forutsettes gjennomført både før og under en hendelse. Det er også store krav til oversikt over egne systemer og aktiviteten som pågår i dem.

FFI anser forutsetningene i rammeverket som meget forståelige fra et IKT-faglig perspektiv. En virksomhets evne til å gjøre hendelseshåndtering beror i stor grad på hvor godt forberedt virksomheten er på at IKT-sikkerhetshendelser kan inntreffe. Dette inkluderer å ha god oversikt over egne nettverk og systemer, ha gjennomført verdivurderinger og konsekvensvurderinger, erkjenne at virksomheten vil kunne bli rammet og ha tilstrekkelig med ressurser til rådighet når hendelsen først inntreffer. Risikotenking og risikovurderinger i forkant av en hendelse er sentralt. Grunnlaget for å gjøre et godt arbeid med hendelseshåndtering når en hendelse inntreffer, skjer således i fase 1.

Rammeverket framstår etter FFIs vurdering imidlertid som utilstrekkelig, i den forstand at virksomheter trenger ytterligere hjelp med å forstå og gjennomføre de nødvendige grep både før, under og etter en IKT-sikkerhetshendelse. Dette gjelder både større og mindre virksomheter, som typisk vil ha noe ulike veiledningsbehov avhengig av ressurstilgang og kompetansenivå innen IKT-sikkerhet.

Det bør vurderes om to ulike veiledere skal utvikles, en for små og mellomstore bedrifter, og en for større virksomheter som adresserer de ulike behovene. Det springende punktet er ikke nødvendigvis virksomhetsstørrelsen i seg selv, men tilgjengelige ressurser og kompetanse i

virksomheten samt omfang og kompleksitet på nettverk og IKT-systemer. I hvilken grad utviklingen av veilederne bør medføre endringer i selve rammeverket bør vurderes av NSM under arbeidet.

I tillegg til veiledningsaspektet, er rammeverket også en introduksjon til aktørene som håndterer hendelser på sivil side i Norge. Slik rammeverket er utformet nå, kan helhetsbildet som danner seg være noe misvisende da sentrale aktører er utelatt. Dette skyldes delvis en ikke urimelig avgrensning opp mot håndtering av følgekonsekvenser og den sektorvise responsen til departementer, direktorater og fylkesmannsembetene. På tross av avgrensningen bør rollen til flere av disse aktørene beskrives i de ulike fasene. Fraværet av aktørbeskrivelsene gir en overforenklet framstilling av de ulike mekanismene som settes i sving når en hendelse inntreffer. Hvor mye av aktørenes roller og oppgaver som bør beskrives i rammeverket bør diskuteres med de relevante aktørene. Å opprettholde skillet slik det er i dag, antas å være uhensiktsmessig.

Det kan også argumenteres for at alle departementers og direktoraters rolle bør komme tydeligere fram, slik at ingen relevante aktører blir utelatt. Dette vil i så fall være en betydelig utvidelse av rammeverket, da hver sektors egenart til en viss grad må identifiseres og beskrives. FFI mener imidlertid at en slik beslutning er å gjøre rammeverket for omfattende på det nåværende tidspunkt. Det bør heller legges vekt på å utvikle sektoroversikter i samarbeid med SRM-er og sektormyndigheter, slik vedlegg 2 til rammeverket hentyder til.

Det å avgrense eller avkorte rammeverket ytterligere ses på som en måte å unngå de identifiserte utfordringene. En slik tilnærming vil imidlertid redusere nytteverdien av rammeverket, og kunne gi et falskt og forenklet inntrykk av kompleksiteten ved IKT-hendelseshåndtering. FFI anbefaler derfor ikke dette.

Avslutningsvis omtaler rammeverket at virksomhetenes rolle i verdikjeder på sektornivå og nasjonalt nivå også er et viktig element ved hendelseshåndtering som gjøres på direktorats- og departementsnivå. Gitt aktørmangfoldet som er vokst fram i de fleste sektorer og virksomhetenes økende involvering i digitale verdikjeder, er det meget utfordrende for både virksomheter og myndigheter å forstå og vurdere sammenhengen mellom verdier på tvers av virksomheter. Rammeverket adresserer dette i liten grad, og det er ikke realistisk å forvente at et rammeverk som dette skal kunne løse denne utfordringen.

8.2 Instruks

I oppdraget nevnes eksplisitt del VIII av samfunnssikkerhetsinstruksen, som beskriver roller og ansvar under en krise. Når det gjelder lederdepartement og informasjon til Kriserådet ser dette ut til ha fungert etter instruks. I hendelse HSØ var JD lederdepartement. De har under hendelsen hatt løpende kontakt med NSM, og blitt orientert i henhold til instruks og rammeverk. Det ble også avholdt møte(r) i Kriserådet, hvor medlemmene der ble orientert om hendelse HSØ. Selv om ingen av hendelsene igangsatte rapporteringsmekanismene som fordrer at alle departementer rapporterer til lederdepartementet, ser det ut til at JD har vært involvert og hatt den oversikten som kreves.

I hendelse FM er det uklart om det ble utpekt noe lederdepartement, og antall aktører som var involvert i den løpende håndteringen var langt færre enn hendelse HSØ. I henhold til samfunnssikkerhetsinstruksen er JD lederdepartement inntil noe annet er besluttet, så FFI antar at dette var tilfellet for hendelse FM. Samtidig var en rekke departementer involvert på grunn av at informasjonen i fylkesmannsembetenes systemer kom fra flere sektorer, og det er tilsynelatende ingen unison formening om hvem som hadde ansvaret.

Til tross for at oppdraget skal se på del VIII, vurderer FFI det til å være hensiktsmessig å inkludere en større del av instruksen for å kunne vurdere grunnlaget for håndteringen av IKT-sikkerhetshendelser generelt, og hendelse HSØ og FM spesielt. Som for instruksen er det i rammeverket en forutsetning om at aktører forbereder seg tilstrekkelig på å kunne håndtere fremtidige hendelser, inkludert å skaffe oversikt over risiko og sårbarhet. Generelt sett var mange aktører ikke tilstrekkelig forberedt på IKT-sikkerhetshendelser av et slikt omfang som inntraff. Særlig var det rollebeskrivelser i slike typer kriser som virker som noe uklart. Overordnet kan det se ut som at det har vært greit å avklare hvem som skulle ha hovedansvaret for hendelsene. Imidlertid er det funn som tyder på at ansvaret videre til direktorater og regionalt nivå ikke har vært tydelig nok. Dette tolker FFI ut ifra at en rekke aktører, som DSB og de berørte fylkesmannsembetene, ikke ble inkludert i håndteringen av hendelsene i tilstrekkelig grad. Det er også funn som tyder på at hvilke oppgaver som ligger til de ulike aktørene ikke er avklart. Dette kom til uttrykk både med hensyn til usikkerhet hos aktørene om hvilke oppgaver de skulle gjøre, om oppgavene og rutinene var annerledes i slike type kriser, og også om hvordan samarbeid med aktører de ikke var vant til å samarbeide med skulle foregå.

Samfunnssikkerhetsarbeidet bygger som nevnt på de fire grunnleggende prinsippene ansvar, nærhet, likhet og samvirke (JD, 2017). Den største utfordringen, gjeldende for begge hendelser, synes likevel å være knyttet til samvirkeprinsippet. Som omtalt ytterligere i kapittel 7.2, er det indikasjoner på at håndteringen har vært gjennomført i såkalte klynger, med tilsynelatende tette skott seg imellom. I tillegg er det en rekke aktører som har ment at de var berørt av hendelsene som ikke har blitt informert eller involvert i håndteringen. Dette har ikke fått store konsekvenser for disse hendelsene, men det er likevel viktig å påpeke at samvirket mellom aktørene sannsynligvis ville blitt utfordret hvis hendelsene hadde eskalert eller fått ytterligere operative eller nasjonale konsekvenser. I tillegg viser det vi har beskrevet som klynger en mulig utfordring for likhetsprinsippet. Det er mange av klyngene som består av aktører som ikke er vant til å arbeide sammen, og dermed fraviker fra hvordan oppgaver løses i normalsituasjon. Det er rimelig å forvente at man i krisehåndtering er nødt til samarbeide med ulike, og kanskje ukjente, aktører, men det kan se ut til at dette aktørkartet og nødvendige forberedelser var manglende når det gjelder håndtering av IKT-sikkerhetshendelser.

8.3 Uoverensstemmelser mellom rammeverk og instruks

FFI kan ikke se uoverensstemmelser eller motstridende elementer mellom instruks og rammeverk for håndtering av IKT-sikkerhetshendelser. Imidlertid er ikke beskrivelsene av aktører og beredskapsmekanismer i rammeverk og instruks tilstrekkelige med tanke på større eller sektorovergripende IKT-sikkerhetshendelser. Begge hendelsene viser at det er langt flere

aktører enn de som er inkludert i overnevnte dokumenter, som vil bli involvert. FFI mener at rollene til flere sentrale direktorater og regionale aktører er tynt beskrevet eller mangler i disse dokumentene.

Rammeverket viser et lite helhetlig bilde av hendelseshåndtering, med NSM øverst og med sentrale samordningsaktører som DSB og FM utelatt. Hvilke aktører som bør inkluderes i rammeverket, bør diskuteres med de relevante aktørene. Det bør uansett synliggjøres at aktørbildet er langt mer komplekst enn det som rammeverket legger opp til. Håndteringen av begge hendelsene vi har sett på, og særlig hendelse FM, viser at sentrale aktører ble utelatt på ulike tidspunkt under håndteringen.

9 Mulige øvingspunkter til Digital 2020

Øvelse Digital 2020 skal etter planen gjennomføres høsten 2020 og vil være DSBs sivile nasjonale øvelse (SNØ) for 2020. DSB har ansvaret for å lede planlegging, gjennomføring og evaluering denne øvelsen. Hovedhensikten med øvelsen er å redusere samfunnets sårbarhet for digitale hendelser og å forbedre samfunnets evne til å forebygge, avdekke og håndtere digitale hendelser og øke samfunnets digitale sikkerhetskompetanse. Samlet sett vil arbeidet med øvelsen kunne bli et viktig bidrag i arbeidet med nasjonal IKT-sikkerhet (DSB, 2019).

Øvelsen vil ha et scenario som treffer flere sektorer og nivåer, og som må håndteres gjennom effektiv hendelseshåndtering og samvirke. Ved at øvelsen planlegges og gjennomføres i tett samarbeid med en rekke private og offentlige virksomheter, etater og myndigheter på lokalt, regionalt og sentralt nivå, vil den også kunne bli en viktig del av arbeidet med en økt og felles risikoforståelse knyttet til uønskede digitale hendelser (ibid). Finanssektoren er særlig pekt ut som rammet sektor under øvelsen (Taraldsen, 2019).

FFIs anbefalinger om hva som bør øves under Digital 2020 er basert på:

- Erfaringer opparbeidet som spillere og observatører i ulike øvelser
- Erfaringer opparbeidet som deltagere i øvingsledelsen (både planlegging og gjennomføring) for ulike øvelser
- Vurderinger vi har gjort i oppdraget
- Innspill fra aktørene vi har intervjuet

I dette kapitlet omtales først noen generelle vurderinger knyttet til øving av IKT-angrep og IKT-sikkerhetshendelser. Deretter omtales forhold knyttet til informasjonsdeling, operative konsekvenser og sentral ressursallokering.

9.1 Generelle vurderinger

Vi anser den tekniske dimensjonen for å være kjernen i håndtering av IKT-sikkerhetshendelser. Den tekniske dimensjonen omfatter tekniske tiltak som en virksomhet iverksetter, men også faktorer som nettverksstruktur, oversikt over trusselaktørens bevegelser i nettverket, mulige inn- og utganger i nettverket, koblinger opp mot andre aktører, avhengigheter mellom virksomhetens tjenester og andre aktørers tjenester samt kunnskap og kompetanse om egne verdier. Det er derfor svært viktig at den tekniske dimensjonen er representert på en god måte i alle typer øvelser der IKT-sikkerhetshendelser inngår, selv om teknisk personell ikke er en del av treningspublikum.

En god framgangsmåte for å inkludere den tekniske dimensjonen er å benytte en «cyber range» (et cyberøvingsområde). I praksis er dette en etablert og potensielt instrumentert nettverks-infrastruktur hvor spillere under kontrollerte forhold kan øve på å håndtere ulike typer hendelser

og skadevare. Her øves typisk teknisk personell. Den tekniske håndteringen kan så kobles opp mot andre spillere som vurderer og håndterer følgekonsekvenser utenfor det tekniske domenet.[29] Dette kan for eksempel være konsekvenser for en pågående militær operasjon, konsekvenser for en virksomhets forretningsområder eller konsekvenser for andre aktører, samt tilhørende informasjonsdeling og koordinering. Det tekniske spillet kan i teorien gjennomføres helt frakoblet og i forkant av en ikke-teknisk øvelse, dersom det ikke er behov for å øve på samspillet mellom teknisk og ikke-teknisk nivå. Avhengig av størrelsen på øvelsen, for eksempel antall aktører som deltar, kan bruk av en cyber range imidlertid være svært ressurs- og tidkrevende.

Et alternativ måte for å sikre inkludering av den tekniske dimensjonen, er å sørge for at man i øvelsen har et team med teknisk ekspertise som «simulerer» og erstatter den reelle tekniske håndteringen. En slik gruppe vil på forhånd ha laget en konsistent teknisk beskrivelse som omfatter tidligere nevnte faktorer som nettverksstruktur, trusselaktørens bevegelser i nettverket, type skadevare og koblinger og avhengigheter opp mot andre aktører.[30] Slik vil gruppen under øvelsen være i stand til å bidra med bakgrunnsinformasjon som typisk vil etterspørres av spillere utenfor virksomhetens egen tekniske håndtering. I tillegg vil de under øvelsen kunne besvare oppdukkende og/eller oppfølgende spørsmål som øvingsledelsen ikke hadde mulighet til å lage i forkant, eller som ikke var forutsett var nødvendig. Det er viktig å understreke at en slik gruppe ikke er det samme som det som i det sivile øvingsregimet omtales som lokal øvingsansvarlig. En slik øvingsansvarlig har mer som oppgave å observere og veilede spillere ved behov, mens denne gruppen arbeider mer i tråd med rollen som såkalt LOCON (lower control) i henhold til NATOs øvingsregime (NATO, 2013).

Uten en tilfredsstillende representasjon av den tekniske dimensjonen, er FFI av den oppfatning at øvelsen ikke vil være kostnadseffektiv med tanke på læringsutbytte. I verste fall vil øvelsen kunne gi feil konklusjoner med tanke på fremtidige øvingsmomenter.

9.2 Informasjonsdeling

FFI har sett at det å kommunisere både internt og eksternt under en IKT-sikkerhetshendelse ble opplevd som utfordrende. FFI mener at vurderinger rundt hva som skulle holdes tilbake av informasjon under hendelsene i flere tilfeller synes å ha vært for generelle. Øvelsesdeltagere bør derfor utfordres på å klargjøre og differensiere følgende vurderinger:

- Hva som ikke kan deles på grunn av gradering i henhold til Sikkerhetsloven
- Hva som ikke kan deles grunnet virksomhetens behov for skjerming av virksomhetsinterne opplysninger

[29] Med dette menes konsekvensene av IKT-hendelsene for de øvede aktørenes virke, ikke ytterligere følgekonsekvenser utenfor aktørenes ansvarsområder.
[30] Denne beskrivelsen kan være helt fiktiv, en sammenstilling av reell informasjon eller en blanding.

- Hva som ikke kan deles av hensyn til ikke å gi trusselaktøren ytterligere, unødvendige fordeler ved å offentliggjøre detaljer rundt den tekniske håndteringen

- Hva som ikke kan deles av hensyn til eventuell pågående eller etterfølgende etterforskning

Øvelsesdeltagere bør til enhver tid vurdere om fordelene ved å dele informasjon med andre rammede og potensielt rammede aktører, er større enn ulempene. Aktørenes roller og ansvar, og derigjennom informasjonsbehov, bør vurderes med aktørene tilstede. Ulike grupper i denne sammenheng bør differensieres og behandles individuelt, som brukere av kompromitterte, potensielt kompromitterte eller truede IKT-systemer; driftspersonell av disse IKT-systemene; medier og befolkning.

9.3 Operative konsekvenser

Øvelsen bør legge til rette for at operative konsekvenser vurderes, både for å gjøre øvelses-deltakerne bevisst på at dette er en sentral og krevende oppgave, og for å sikre at alle relevante aktører i håndteringen blir involvert. Øvingsmomenter kan være:

- Prioritering av hva som er viktigst av integritet, tilgjengelighet og konfidensialitet?

- Når skal skadevare fjernes fra et system?

- Hvilken aktør tar beslutningene, og på hvilket grunnlag?

- Hvem har beslutningsmyndighet der flere aktører er uenige?

FFI har påpekt tilfeller i denne evalueringen der enkelte aktører sannsynligvis burde blitt informert og involvert.

Det er særlig tre aktører i krisehåndteringsapparatet som har en sentral samordningsrolle. JD på sentralt nivå, DSB på direktoratsnivå og Fylkesmannen på regionalt nivå. Disse samordnings-rollene bør utfordres og øves på under Digital 2020.

9.4 Sentral ressursallokering

Funn i oppdraget viste at det er manglende kompetanse og kapasitet i virksomhetene ved håndtering av IKT-sikkerhetshendelser. Det er derfor å forvente at det i reelle hendelser blir et stort behov for bistand og rådgivning fra SRM-ene og nasjonale ressurser. Øvelsen bør derfor legge til rette for at man blir utfordret på ressursallokering på nasjonalt nivå og virksomhetsnivå, for eksempel når det gjelder analysekapasitet:

- Det bør legges til rette for vurderinger omkring hvilke virksomheter som skal støttes av nasjonale ressurser, når flere aktører har behov for dette samtidig.

- SRM-ene bør utfordres på hvorvidt de skal sende ut liaisoner til virksomheten, gjøre egne analyser i egne lokaler eller støtte virksomheten direkte på andre måter.

- På virksomhetsnivå bør det være elementer i øvelsen som utfordrer virksomhetene på intern ressursallokering og ansvarsfordeling. Dette inkluderer spørsmål om hvem som skal gjøre og har ansvar for hva, hvilke oppgaver som skal prioriteres og hvilke som eventuelt kan vente, beslutningsmyndighet og så videre.

10 Konklusjon

Konklusjonen er delt i tre, etter punktene i oppdragsavtalen:

1. Kartlegging og vurdering av hvordan håndteringen ble utført med utgangspunkt i rammeverk og instruks

2. Kartlegging og dokumentering av eventuelle utfordringer eller motstridende elementer i rammeverk og instruks

3. Vurdering om hvorvidt rammeverk og instruks er tilstrekkelig, og eventuelt anbefale videreutvikling av disse for å bedre samfunnets evne til å håndtere hendelser

10.1 Kartlegging og vurdering av håndtering med utgangspunkt i rammeverk og instruks

Generelt ble håndtering av hendelsene utført av aktører som arbeidet sammen i klynger. Antall klynger og størrelsen på disse var forskjellig i hendelsene. I hendelse HSØ er det identifisert seks klynger: teknisk håndtering, beredskapsledelse i regionen HSØ, koordinering i helsesektoren, koordinering på strategisk nivå, avklaring mot nødnett og koordinering mellom de nasjonale sikkerhets- og etterretningstjenestene og politiet ved Kripos. I hendelse FM er det fire klynger: teknisk håndtering, operative vurderinger, strategiske beslutninger og koordinering mellom de nasjonale sikkerhets- og etterretningstjenestene og politiet ved Kripos.

Funn viste at det var lite samhandling mellom klyngene, og flere aktører var ikke kjent med flere av de resterende klyngene. Et fåtalls aktører var med i flere klynger. Samlingen av aktører i klynger og manglende kjennskap og samhandling er imidlertid ikke nødvendigvis et problem, da dette vil avhenge av hendelsen som skal håndteres.

To årsaker som delvis kan forklare hvorfor klyngene oppstår er fordelingen av mandater og roller på ulike aktører nasjonalt og i de rammede sektorene, og at hendelsenes karakter har medført at enkelte aktører har hatt lite behov for å samhandle. Begge hendelsene framstår prinsipielt som datainnbruddshendelser med tapping av informasjon. Hadde hendelsene utviklet seg til å være noe annet enn dette, for eksempel sabotasje, ville temaer som blant annet verdivurderinger knyttet til tekniske prioriteringer og operative følgekonsekvenser vært noe som flere klynger ville ha vært berørt av. Dette mener FFI ville ha framtvunget diskusjoner på tvers av flere av klyngene.

For flere av aktørene i de rammede sektorene har forberedelser og planlegging for slike hendelser vært mangelfull. Dette inkluderer manglende verdivurderinger, manglende risiko- og sårbarhets-vurderinger og mangelfull overvåking og logging i egne nett. Planer for å håndtere avanserte trusselaktører i egne nett dersom slike oppdages har manglet. Dette utgangspunktet har naturligvis gitt følgekonsekvenser for håndteringen når en slik aktør så har blitt oppdaget. Manglende oversikt over egne nett og systemer, inkludert verdier, har gjort det utfordrende å fastslå omfanget

av kompromittering og potensiell og reell skade. Det har også vært utfordrende å forstå betydningen av det som har inntruffet.

Varslingen fulgte i utgangspunktet rammeverkets føringer, men i praksis ser det ut til at for få aktører ble varslet og holdt oppdatert om det som har skjedd. FFI antar at dette kan skyldes en for streng tolkning av «need to know» hos mottakerne av varslingen, spesielt med tanke på informering av miljøer som har et ansvar for beredskap og oppfølging av mulige operative følgekonsekvenser.

Dersom oppdagelse av kompromittering ikke er kjent for trusselaktøren, er det naturlig med begrensninger på informasjon om hendelsen. Når hendelsen er blitt kjent og det er sannsynlig at trusselaktøren forstår at han er oppdaget, mener FFI at det bør være færre begrensninger på informasjonsdeling. I hendelse HSØ ser det ut som at informasjonsdeling fra rammet aktør til andre aktører involvert i beredskap og operative vurderinger har vært begrenset, også etter at hendelsen er blitt kjent. Dette kunne ha fått uheldige konsekvenser, særlig dersom hendelsen hadde utviklet seg til mer destruktiv art. I begge hendelsene burde aktører med ansvar for beredskap og operative vurderinger ha blitt varslet og informert før hendelsens karakter var kjent og oppdagelsen potensielt kjent for trusselaktøren. Dette betyr ikke at disse virksomhetene skulle ha varslet bredt internt til alle ansatte på dette tidspunktet, men at flere nøkkelpersoner i virksomhetene med ansvar innen beredskap og operative vurderinger burde ha vært informert. Ved framtidige hendelser, også utenfor helse- og omsorgssektoren, bør relevant teknisk personell fra sikkerhets- og etterretningstjenestene som skal bistå i arbeidet, raskt bli midlertidig autorisert for informasjon de kan komme over i sitt tekniske arbeid. Utgangspunktet bør være at kunnskap om trusselaktørens operasjonsmåter driver informasjonsbehovet og vurderingene om hvilke tilganger som bør gis.

Dilemmaet mellom å overvåke videre eller starte gjenoppretting raskt har vært til stede i håndteringen av begge hendelser. I særs ble dilemmaet et omdiskutert tema med motstridende meninger i hendelse FM. Intensjonen med (eventuell) videre overvåking har i begge hendelser vært å lære tilstrekkelig om omfanget på kompromitteringen slik at gjenoppretting vil ha større sannsynlighet for å lykkes. I hendelse FM ble informasjonseiers ønske om rask gjenoppretting overstyrt til fordel for videre overvåking av KMD, samtidig som tilstrekkelig tiltak rundt overvåkingen ikke ble etablert hos FM. Dette på tross av at NSM NorCERT understreket behovet for passende sikringstiltak. Forberedelser og planlegging ble gjennomført av NSM NorCERT for å overvåke deteksjonsløsningen, selv om dette ikke ble fanget opp på operatørnivå. FFI mener rent prinsipielt at dersom informasjonseiers vurdering og ønske om videre håndtering i en slik situasjon settes til side, bør dette være basert på et grundig beslutningsunderlag hvor fordeler og ulemper belyses samt at tilstrekkelig sikringstiltak etableres. Informasjonseier bør delta i etableringen av beslutningsunderlaget. Dersom motivasjonen for videre overvåking ikke er gjenoppretting, bør forholdet til nasjonal sikkerhet veie tungt. Dersom rammet virksomhet ikke har tilstrekkelig ressurser til å etablere tilstrekkelig sikringstiltak, bør virksomheten støttes i dette. I hendelse FM var det også uenighet om departementet har beslutningsmyndighet i et tilfelle som dette. FFI mener dette bør avklares i de rette instanser for å unngå en tilsvarende diskusjon ved eventuelle framtidige hendelser.

FFI har hatt utfordringer med å få informasjon om den tekniske håndteringen som ble gjort i hendelse HSØ. HF-ene iverksatte tiltak for å håndtere eventuelle operative konsekvenser, da med vekt på tjenestetilgjengelighet. HSØ RHF og Hdir koordinerte på sine nivåer.

For hendelse FM var det mye mindre kapasitet og kompetanse tilgjengelig for hendelseshåndtering i rammet virksomhet enn for hendelse HSØ, og håndteringen tok lengre tid.

Ved situasjonsrapportering i hendelse HSØ var mottakelse og behandling av gradert informasjon en utfordring. Det var manglende vurderinger om forventet utvikling, samt usikkerhet om hva som skulle stå i situasjonsrapporteringen når situasjonen tilsynelatende var uforandret.

For begge hendelsene finnes det evalueringsrapporter, med noe forskjellig innretning. De fleste aktørene har forbedret planverk og scenarioer i etterkant, og enkelte aktører beskriver et forbedret samarbeid etter hendelsene.

10.2 Kartlegging og dokumentering av eventuelle utfordringer eller motstridende elementer mellom rammeverk og instruks

Det er vanskelig å finne motstridende elementer mellom rammeverk og instruks, mest fordi de har fokus på aktører på forskjellig nivå. Det er naturligvis noe overlapp fordi departementene også har en rolle i rammeverket, men beskrivelsen av denne rollen er forholdsvis begrenset. Av den grunn er det lite å hente ved å sammenlikne rammeverk og instruks. På samme måte er det lite som tyder på at de er motstridende.

Det er imidlertid viktig å påpeke at rammeverk og instruks gir et lite helhetlig bilde av aktørene og mekanismene som kan være relevante ved større eller sektorovergripende IKT-sikkerhetshendelser. Rammeverket kan generelt oppleves som noe frakoblet det etablerte systemet som håndterer andre typer nasjonale kriser, hvor særlig sentrale samordningsroller, som rollene til DSB og FM, ikke er inkludert.

10.3 Vurdering om hvorvidt rammeverk og instruks er tilstrekkelig, og eventuelt anbefale videreutvikling av disse for å bedre samfunnets evne til å håndtere hendelser

Rammeverket kan leses på to ulike måter: som en introduksjon til IKT-hendelseshåndtering og sentrale faglige forhold ved dette, og som en introduksjon til aktørene som håndterer hendelser på sivil side i Norge.

For IKT-hendelseshåndtering framsetter rammeverket en rekke forutsetninger eller krav til virksomheter, SRM-er og NSM NorCERT. Sett fra FFIs perspektiv er disse forutsetningene meget forståelige fra et faglig perspektiv. På SRM-nivå er det rapportert at rammeverket på dette nivået er nyttig for å bygge opp et SRM, og i mindre grad anvendelig for selve håndteringen. Etter FFIs vurdering framstår rammeverket som utilstrekkelig på virksomhetsnivå, i den forstand at

virksomheter trenger mer støtte for å forstå og gjennomføre gode tiltak både før, under og etter en IKT-sikkerhetshendelse. FFI legger til grunn at større og mindre virksomheter har ulike veiledningsbehov gitt ulik ressurstilgang og kompetansenivå innen IKT-sikkerhet. Det bør derfor vurderes om to ulike veiledere skal utvikles, en for små og mellomstore bedrifter, og en for større virksomheter tilpasset de ulike behovene. I hvilken grad utviklingen av veilederne bør medføre endringer i rammeverket bør vurderes av NSM.

Som en introduksjon til aktørene som håndterer hendelser på sivil side i Norge, kan helhetsbildet som danner seg være noe misvisende da sentrale aktører ikke er tatt med. Noe av dette skyldes en forståelig avgrensning av rammeverkets omfang opp mot følgekonsekvenser og sektorvis respons hos departementer, direktorater og fylkesmannsembeter. Roller og oppgaver hos flere aktører bør likevel beskrives, da fraværet av dem gir en overforenklet framstilling av de ulike mekanismene som iverksettes ved hendelser. Hvor mye av aktørenes roller og oppgaver som bør beskrives, bør diskuteres med aktørene selv.

11 Avsluttende betraktninger

Som institusjon har FFI et samfunnsoppdrag om å styrke samfunnssikkerheten og å formidle forskningsbasert kunnskap. Gitt FFIs kunnskap og kompetanse innenfor samfunnssikkerhet og cybersikkerhet, var det naturlig for FFI å påta seg oppdraget med å evaluere håndteringen av to IKT-sikkerhetshendelser. FFI har arbeidet med dette oppdraget i ett år.

Ved en evaluering av håndteringen av en IKT-sikkerhetshendelse er et sentralt element å anskaffe tilstrekkelig informasjon om hendelsen. En god oversikt over hendelsesforløpet og hva som faktisk skjedde er sentralt, da det uten denne oversikten er vanskelig å vurdere om håndteringen er passende og på hvilket grunnlag de ulike beslutningene er tatt. Satt på spissen er det vanskelig å vurdere håndteringsmåten hvis vi ikke har innsikt i hva som faktisk er håndtert. For en IKT-sikkerhetshendelse resulterer dette i et behov for ufyllende informasjon om den tekniske infrastrukturen som ble rammet, trusselaktørens handlemåter, vurderinger og beslutninger som ble tatt og informasjonsgrunnlaget som var tilgjengelig på ulike tidspunkter for aktørene som utførte hendelseshåndteringen.

FFIs tilnærming har gått ut på å søke slik informasjon om hendelsene og håndteringen ned til et nødvendig nivå. Det faktum at det var to hendelser og ikke en enkelt hendelse som skulle evalueres, gjorde at mengden informasjon som måtte innsamles og analyseres økte. Det samme gjorde antall aktører som var relevante å intervjue i forbindelse med arbeidet. Tilgjengelige ressurser i oppdraget måtte derfor prioriteres hardere, og det var umulig å gå like bredt ut og dypt nedover i materien som det hadde vært ved analyse av kun én hendelse. På en annen side ble det mulig å gjøre sammenligninger på tvers av hendelsene, og å studere likheter og ulikheter. Det at vi kunne gjøre sammenligninger bidro til et bedre informasjonsgrunnlag og mer nyanserte vurderinger.

Av aktørene vi har snakket med, har mange vært åpne og delt informasjon fritt uten å legge skjul på forhold som kunne sette dem i et dårlig lys. Samtidig har enkelte aktører vært mer tilbakeholdne med informasjon. Dette har ført til et ujevnt informasjonsgrunnlag for de to hendelsene. For hendelse FM, har FFI fått tilgang til deler av informasjonsgrunnlaget fra aktører som har vurdert omfang, alvorlighetsgrad og mulige følgekonsekvenser. I hendelse HSØ har FFI i større grad kun hatt tilgang til konklusjonene fra aktørene, men ikke informasjonsgrunnlaget som ble benyttet for komme fram til konklusjonene. Resultatet av dette er et lite paradoks: det finnes mer informasjon om hendelse HSØ enn hendelse FM, da hendelse HSØ er en større hendelse som involverer flere aktører. Mangelen på bestemt informasjon gjør at vi på visse områder likevel vet mer om hendelse FM.

I tillegg har enkelte aktører kommentert at det finnes annen, potensielt gradert informasjon, som kunne hatt innvirkning på våre vurderinger rundt hendelse HSØ. Da vi ikke har fått tilgang til denne informasjonen er det vanskelig å vurdere hvordan denne informasjonen ville ha endret vurderingene.

En kommentar fra et av de første intervjuene FFI gjennomførte, var at «det gikk jo bra, men vi vet ikke hvorfor». Dette har fulgt oss gjennom hele prosessen, og er nyttig å reflektere over i tilknytning til begge hendelsene. Hva betyr det egentlig at noe går *bra* ved slike hendelser? Var det håndteringen som gjorde at det gikk bra, eller var det at intensjonen til trusselaktøren aldri var å skape store operative konsekvenser? Og gikk det egentlig bra hvis det var fare for at sensitiv informasjon kunne være på avveie? Når så mange aktører er involvert i hendelseshåndteringen – hvem avgjør da om det gikk bra og på hvilket grunnlag? FFI har pekt på en rekke problemstillinger og utfordringer underveis i rapporten, som kan antyde at hvis trusselaktøren hadde hatt andre intensjoner ville aktørene som skulle håndtere hendelsene fått langt større utfordringer. Dette er særlig knyttet til samvirke, informasjonsdeling og oversikt over egne systemer, verdier og sårbarheter. Det er naturlig å spørre seg i hvilken grad utfall av håndtering er prisgitt trusselaktørens motivasjon.

Slik vi ser det, må begge hendelsene studert i dette oppdraget ansees som alvorlige og omfattende. Dette skyldes antallet involverte aktører, størrelsen på rammede systemer og potensialet for skade. Informasjon om eksfiltrering av data i hendelse FM er det mest konkrete FFI har fått, og omfanget av dette har derfor blitt beskrevet i rapporten. Her finnes det også gradert informasjon som inkluderer vurderinger rundt mulig informasjonstap. For hendelse HSØ er detaljene mer uklare. Det er ulike meninger om omfang, usikkerhet og potensiell skade. Grunnet mangelen på informasjon, avstår FFI fra å gjøre ytterligere vurderinger rundt dette og viser til uttalelser fra Sykehuspartner HF og PST.

Det er naturligvis sammenheng mellom det som skjer under en hendelse og hva som gjøres for å håndtere den. Dette gjelder både under øvelser og ved regulær virksomhet. FFI opplever ikke å ha oppnådd forståelse for denne sammenhengen hos enkelte av aktørene. I beste fall er dette noe som bare vanskeliggjør evaluering i etterkant av en hendelse. I verste fall er dette et symptom på manglende forståelse for sammenhengen mellom teknisk hendelsesforløp og mulighetene for å håndtere dette. Hvis sistnevnte er tilfellet, vil dette potensielt kunne føre til at beredskapsplaner og håndteringsmekanismer ikke er tilpasset og tilstrekkelige til å kunne bidra til å håndtere framtidige hendelser.

Forkortelser

2FA	Tofaktorautorisasjon
APT	Advanced Persistent Threat
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
DFU	Departementenes fylkesmannsutvalg
DSB	Direktoratet for samfunnssikkerhet og beredskap
FCKS	Felles cyber- og koordineringssenter
FD	Forsvarsdepartementet
FFI	Forsvarets forskningsinstitutt
FM	Fylkesmannsembetene
FMAV	Fylkesmannen i Aust- og Vest Agder
FMFA	Fylkesmannens fellesadministrasjon
FMFS	Fylkesmannen i Sogn og Fjordane
FMHE	Fylkesmannen i Hedmark
FMIN	Fylkesmannen i Innlandet
FMOA	Fylkesmannen i Oslo og Akershus
FMNO	Fylkesmannen i Nordland
FMTL	Fylkesmannen i Telemark
FRI	Fylkesmennenes regionale informasjonsnett
Hdir	Helsedirektoratet
HF	Helseforetak
HDO	Helsetjenestens driftsorganisasjonen for nødnett
HOD	Helse- og omsorgsdepartementet
HSØ	Helse Sør-Øst
IKT	Informasjons- og kommunikasjonsteknologi
ISO	International Organization for Standardization
JD	Justis- og beredskapsdepartementet
K2	Kommando og kontroll
KIKS	Kritisk infrastruktur og kritiske samfunnsfunksjoner
KMD	Kommunal- og moderniseringsdepartementet
KSE	Krisestøtteenheten
KU	Kriseutvalg
LMS	Learning Management System
LOCON	Lower Control
NCSC	Nasjonalt cybersikkerhetssenter
NHN	Norsk helsenett
NSM	Nasjonal sikkerhetsmyndighet
OUS	Oslo Universitetssykehus
PST	Politiets sikkerhetstjeneste
RHF	Regionalt helseforetak
RSU	Regjeringens sikkerhetsutvalg
SITSEN	Situasjonssenteret

SMK	Statsministerens kontor
SRM	Sektorvise responsmiljøer
UD	Utenriksdepartementet
VDI	Varslingsystem for digital infrastruktur
VPN	Virtual private network

Referanser

Alsén, S. (2018). *Informasjonssikkerhet og personvern er styrket etter datainnbruddet*. Hentet 10. mai 2018 fra: https://sykehuspartner.no/nyheter/informasjonssikkerhet-og-personvern-er-styrket-etter-datainnbruddet

Axelos (2011). ITIL *Lifecycle Publication Suite*. 20 July 2011. https://www.axelos.com/store/book/itil-lifecycle-publication-suite

Boin, A., t'Hart, P, Stern, E og Sundelius, B. (2005). *The Politics of Crises Management. Public Leadership under Pressure*. United Kingdom: Cambridge University Press.

Brownlee, N. og Guttman, E. (1998). *Expectations for Computer Security Incident Response.* BCP 21. RFC 2350. Juni 1998. Hentet 10. mars 2020 fra: https://www.ietf.org/rfc/rfc2350.txt.

Datatilsynet (2018). *Iverksette styringssystem for informasjonssikkerhet*. Hentet 20. januar 2020 fra: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/iverksette-styringssystem-for-informasjonssikkerhet/

Dorofee, A., Ruefle, R., Zajicek, M., McIntire, D., Alberts, A., Perl, S., Huth, C.L. og Walters, P. (2018). *Incident Management Capability Assessment*. (CMU/SEI-2018-TR-007). Carnegie Mellon University. Software Engineering Institute. Hentet 07. Februar 2020 fra: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2018_005_001_538866.pdf

DSB (2019). *Høring - NOU 2018:14 IKT-sikkerhet i alle ledd og utkast til lov som gjennomfører NIS-direktivet*. Hentet 15. februar 2020 fra: https://www.regjeringen.no/contentassets/53124f4f93514d0eae3969076c3ca7bc/direktoratet-for-samfunnssikkerhet-og-beredskap.pdf?uid=Direktoratet_for_samfunnssikkerhet_og_beredskap

DSB (udatert). *Ansvarsområder og roller*. Hentet 25. januar 2020 fra https://www.dsb.no/menyartikler/om-dsb/ansvarsomrader-og-roller/

Eagle, C. (2011). The Ida Pro Book. 2nd ed. No Starch Press. Juli, 2011.

Eilam, E. (2005). Reversing: Secrets of Reverse Engineering. John Wiley & Sons, 2005.

Engen, O.A.H., Kurke, B.I., Lindøe, P.H., Olsen, K.H, Olsen, O.E og Pettersen, K.A. (2016). *Perspektiver på samfunnssikkerhet*. Cappelen Damm AS.

Forum of Incident Response and Security Teams (2019). *FIRST CSIRT Services Framework versjon 2.1.* November 2019. Hentet 10. mars 2020 fra:

https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.1.0.pdf

Fylkesmannens fellesadministrasjon (2019). *Om oss*. Hentet 15. februar 2020 fra : https://www.fylkesmannen.no/nb/fmfa/om-oss/

Fylkesmannen i Sogn og Fjordane (2018). *Årsrapport for Sogn og Fjordane*. Styringsportalen for fylkesmannen 2018. Hentet 17. februar 2020 fra: https://styringsportalen.fylkesmannen.no/2018/arsrapporter/fmsf/

Fylkesmannen i Hedmark (2017). *Årsrapport for Hedmark*. Styringsportalen for fylkesmannen 2017. Hentet 17. februar 2020 fra: https://styringsportalen.fylkesmannen.no/globalassets/arkiv/2017/arsrapporter/arsrapport-for-hedmark.pdf

Fylkesmannens samfunnssikkerhetsinstruks (2015). *Instruks 19. juni 2015 nr. 703 for fylkesmannens og Sysselmannen på Svalbards arbeid med samfunnssikkerhet, beredskap og krisehåndtering*.

Helse Sør-Øst (2019a). Evaluering av dataangrepet mot Helse Sør-Øst I 2018. Helse Sør-Øst RHF versjon nr. 1.0

Helse Sør-Øst RHF (2018-1). «Informasjonssikkerhet og personvern er styrket etter datainnbruddet». Hentet 7. mars 2020 fra: https://www.helse-sorost.no/nyheter/informasjonssikkerhet-og-personvern-er-styrket-etter-datainnbruddet

Helse Sør-Øst RHF (2018-2). - Sammenstilling situasjonsrapport Nr. 6 - Datainnbrudd i Helse-Sør-Øst, januar 2018 (17.01.2018 - 16:00)

Helse Sør-Øst RHF (2018-3) - Sammenstilling situasjonsrapport Nr. 10 - Datainnbrudd i Helse-Sør-Øst, januar 2018 (22.01.2018 - 18:25)

Helse Sør-Øst RHF (2018-4) Saksframlegg til Styret Helse Sør-Øst RHF, Styremøte 1.februar 2018, SAK NR 017-2018, Orienteringssak: Driftsorienteringer fra administrerende direktør, datert 25.januar 2018. https://www.helse-sorost.no/Documents/Styret/Styremøter/2018/20180102/017-2018%20Orienteringssak%20-%20Driftsorienteringer%20fra%20administrende%20direktør.pdf

Helse Sør-Øst RHF (2018-5). Informasjonssikkerhet og personvern er styrket etter datainnbruddet. Hentet 10.mai 2020: https://www.helse-sorost.no/nyheter/informasjonssikkerhet-og-personvern-er-styrket-etter-datainnbruddet

Helse Vest IKT AS (2018-1), Styremøte Helse Vest IKT AS 01.03.2018, Sak 004/18: Rapport frå verksemda per januar 2018, datert 20.02.2018, VEDLEGG 1 til SAK 004/18, Verksemdsrapport for Helse Vest IKT AS per januar 2018. Hentet 26. mai fra: https://helse-

vest-ikt.no/Documents/Styredokumenter/Innkalling%20og%20opne%20saker%20til%20styremøte%2001-03-18.pdf

Helse Vest IKT AS (2018-2), Styremøte Helse Vest IKT AS 01.03.2018, Sak 010/18: Informasjonssikkerhet i Helse Vest, datert 22.02.2018, punkt 7: Om datainnbrudd i Helse Sør-Øst RHF/Sykehuspartner. Hentet 26. mai fra: https://helse-vest-ikt.no/Documents/Styredokumenter/Innkalling%20og%20opne%20saker%20til%20styremøte%2001-03-18.pdf

Helsedirektoratet (2018). Helsedirektoratets håndtering av kompromitteringen av Helse Sør-Øst sin infrastruktur januar 2018. Helsedirektoratet: Oslo

Helsedirektoratet (2019). *Ansvar og oppgaver helseberedskapen i Norge*. Hentet 15. januar 2020 fra: https://www.helsedirektoratet.no/tema/beredskap-og-krisehandtering/ansvar-og-oppgaver-helseberedskapen-i-norge

Helse Sør-Øst RHF (2020). *Om Helse Sør-Øst RHF*. Hentet 10. mars 2020 fra: https://www.helse-sorost.no/om-oss#om-helse-sor-ost-rhf

Helsetjenestens driftsorganisasjon for nødnett HF (2018), Saksfremlegg for Styret datert 26.januar 2018, Sak nr 04-2018 ADs orientering, punkt 3: Sikkerhetssituasjonen i HSØ. Hentet 17. februar 2020 fra: https://www.hdo.no/Documents/Styrem%C3%B8te/Styrem%C3%B8te%202.%20februar%2018/Sak%2004-2018%20ADs%20orienteringer.pdf

International Organization for Standardization (2016). *ISO/IEC 27035:2016 Information Technology – Security Techniques – Information Security Incident Management – Part 1: Principles of Incident Management*. November 2016.

Jacobsen, C. (2018). Lærdommer etter angrepet mot Helse Sør-Øst, Presentasjon datert 28.11.2018. Hentet 11. mars 2020 fra: https://ehelse.no/normen/presentasjoner/_/attachment/download/873e1a33-b003-43df-950e-14c6b014b7cd:a878183a24f43fefc54138e61dbeb4d0946d977b/1300_jacobsen_angrep_mot_HSO.pdf

Justis- og beredskapsdepartementet (2016). *Regjeringen samler mer ansvar for samfunnssikkerhet i DSB*. Hentet 26. mai 2020 fra: https://www.regjeringen.no/no/aktuelt/regjeringen-samler-mer-ansvar-for-samfunnssikkerhet-i-dsb/id2516159/

Justis- og beredskapsdepartementet (2017). *Instruks for departementenes arbeid med samfunnssikkerhet (samfunnssikkerhetsinstruksen)*. (FOR-2017-09.01-1349) Fastsatt av JD, 1. september 2017.

KMD, NSM, PST, DSB, representanter fra FM (2019). *Konsekvensvurdering av kompromitteringen av fylkesmannsembetenes informasjonssystemer.* (Begrenset)

Kommunal- og moderniseringsdepartementet (2019). *Kommunal- og moderniseringsdepartementet.* Hentet 10. mars 2020 fra: https://www.regjeringen.no/no/dep/kmd/id504/

KMD (2018). *Tildelingsbrev til fylkesmannsembetene 2018, vedlegg 2 – Budsjettfordeling 2018.* Hentet 7. mars fra: https://www.regjeringen.no/contentassets/254619ee580b401cb358fa5dab884628/vedlegg_2.pdf

KMD (2018-2). *Virksomhets- og økonomiinstruks.* Styringsportalen for fylkesmannen 2018. Filter: Nordland fylkesmannsembete. Hentet 17. februar 2020 fra: https://styringsportalen.fylkesmannen.no/2018/styringsdokumenter/

KMD (2014). *Styringsdokument fra kommunal- og moderniseringsdepartementet 2014*. Styringsportalen for fylkesmannen 2014. Hentet 17. februar 2020 fra: https://styringsportalen.fylkesmannen.no/contentassets/543d52851ad247718101f62bc1a14a55/kommunal--og-moderniseringsdepartementet2014.pdf

Lund, A. (2019). Pure Penguin - Kompromittering av fylkesmannsembetene sommeren og høsten 2018, Presentasjon av Asbjørn Lund på Planleggingskonferanse 1 for "Øvelse Digital 2020" 26-27.august 2019 - Tønsberg, udatert

Miles, M. B. & Huberman, A. M. (1994). *Qualitative data analysis: an expanded sourcebook*. Thousand Oaks, Calif.: Sage.

Nasjonal sikkerhetsmyndighet (2017). Rammeverk for håndtering av IKT-sikkerhetshendelser. Hentet 20. januar 2020 fra: https://www.nsm.stat.no/globalassets/dokumenter/vedlegg-til-rammeverk-for-handtering-av-ikt-hendelser/rammeverk-for-handtering-av-ikt-sikkerhetshendelser.pdf

Nasjonal sikkerhetsmyndighet (2018). *NSM NorCERT erfaringer fra HSØ-saken*. (Begrenset)

Nasjonal sikkerhetsmyndighet (udatert). Hendelsesrapport BLIND BANDICOOT & BLACK BANDICOOT. Unntatt offentlighet.

National Institute of Standards and Technology (2012). *Computer Security Incident Handling Guide SP 800-61 rev 2.* August 2012. Hentet 10. mars 2020 fra: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

NATO (2013). *Bi-Strategic Command Collective Training and Exercise Directive (CT&ED) 075-003.* 2 oktober 2013. NATO UNCLASSIFIED.

Norsk helsenett (udatert). *HelseCERT.* Hentet 10. mars 2020 fra*:* https://www.nhn.no/helsecert/

Norsk Standard 5830, (2012): Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Terminologi. Norsk Standard NS 5830:2012.

Oslo universitetssykehus HF (2018) Styremøte 16.februar 2018, Sak 13/2018, ADMINISTRERENDE DIREKTØRS ORIENTERINGER, Sak 2: Status IKT, datert 8.februar 2018. Hentet 26. mai fra: https://oslo-universitetssykehus.no/seksjon/styremoter-i-ous/Documents/Styremøter%202018/Styremøte%202018-02-16%20Samlefil.pdf

PST (2018). *PST innstiller etterforskingen av datainnbruddet i Helse Sør-Øst RHF og Sykehuspartner HF*. Hentet 7. mars 2020 fra: https://www.pst.no/alle-artikler/pressemeldinger/pst-innstiller-etterforskningen-av-datainnbruddet-i-helse-sor-ost-rhf-og-sykehuspartner-hf/

PST (2017). Oppgaver. Hentet 12. mai 2020 fra: https://www.pst.no/temasider/oppgaver/

Regjeringen (2019). Nasjonal strategi for digital sikkerhet. Departementene. Hentet 25. januar 2020 fra: https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/nasjonal-strategi-for-digital-sikkerhet.pdf

Sykehuset Innlandet HF (2018) Notat til Styret i Sykehuset Innlandet fra Administrerende direktør, Styremøte 22.februar 2018, Sak: Status og utvikling dataangrep januar 2018, Sak 018-2018 Vedlegg 02f, datert 15.februar 2018. Hentet 26. mai fra: https://sykehuset-innlandet.no/seksjon/styret/Documents/2018-02/018-2018%20Vedlegg%2002f%20Status%20og%20utvikling%20dataangrep.pdf

Sykehuspartner HF (2020-1). Dataangrepet mot Helse Sør-Øst. Overordnet rapport fra intern gjennomgang av Sykehuspartner HFs håndtering av datainnbruddet oppdaget 8.januar 2018-Versjon 1.1. datert 6.januar 2020.

Sykehuspartner HF (2020-2). *Om oss.* Hentet 15. februar 2020 fra: https://sykehuspartner.no/om-oss

Sykehuspartner HF (2018) Saksframlegg til Styret Sykehuspartner HF, Styremøte 2.mai 2018, SAK NR 034-2018, Status og forbedring informasjonssikkerhet, personvern og tilgangsstyring, datert 25.april 2018. Hentet 26. mai fra: https://sykehuspartner.no/Styremter/052018/034-2018%20-%20Status%20og%20forbedring%20informasjonssikkerhet%20personvern%20og%20tilgangsstyring.pdf

Taraldsen, G. (2019). *Beredskapsøvelser*. Presentasjon. Hentet 10. mars 2020 fra: https://www.fylkesmannen.no/globalassets/fm-innlandet/10-samfunnssikkerhet-og-beredskap/beredskap-bilder/fmin---ovelse-evaluering-og-kommunikasjon---kontaktmote-13.september.pdf

UiO Institutt for klinisk medisin Det medisinske fakultet, Oslo universitetssykehus (2018), Referat fra Forskningslederforum 7.juni 2018, Sak 37/2018. Hentet 26. mai fra: https://www.med.uio.no/klinmed/om/organisasjon/forskningslederforum/moter/2018/protokoller/20180607-protokoll.pdf

Virksomhetsikkerhetsforskriften (2019). *Forskrift om virksomheters arbeid med forebyggende sikkerhet* (FOR-2019-05-03-560). Hentet 27. januar 2020 fra: https://lovdata.no/dokument/SF/forskrift/2018-12-20-2053

Whitman, M.E. og Mattord, H.J. (2007). *Principles of Incident Response and Disaster Recovery*, Course Technology, Boston, 2007.

About FFI

The Norwegian Defence Research Establishment (FFI) was founded 11th of April 1946. It is organised as an administrative agency subordinate to the Ministry of Defence.

FFI's MISSION

FFI is the prime institution responsible for defence related research in Norway. Its principal mission is to carry out research and development to meet the requirements of the Armed Forces. FFI has the role of chief adviser to the political and military leadership. In particular, the institute shall focus on aspects of the development in science and technology that can influence our security policy or defence planning.

FFI's VISION

FFI turns knowledge and ideas into an efficient defence.

FFI's CHARACTERISTICS

Creative, daring, broad-minded and responsible.

Om FFI

Forsvarets forskningsinstitutt ble etablert 11. april 1946. Instituttet er organisert som et forvaltningsorgan med særskilte fullmakter underlagt Forsvarsdepartementet.

FFIs FORMÅL

Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som kan påvirke forutsetningene for sikkerhetspolitikken eller forsvarsplanleggingen.

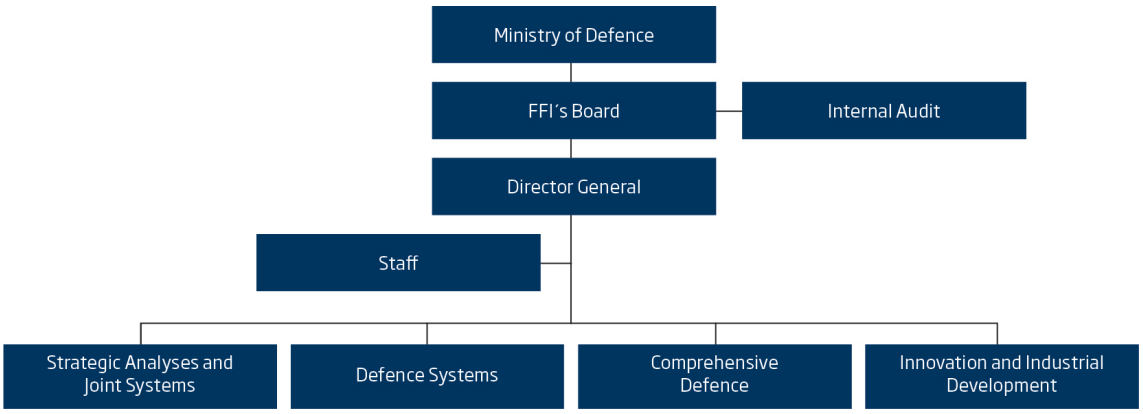
FFIs VISJON

FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs VERDIER

Skapende, drivende, vidsynt og ansvarlig.

FFI's organisation



Forsvarets forskningsinstitutt
Postboks 25
2027 Kjeller

Besøksadresse:
Instituttveien 20
2007 Kjeller

Telefon: 63 80 70 00
Telefaks: 63 80 71 15
Epost: ffi@ffi.no

Norwegian Defence Research Establishment (FFI)
P.O. Box 25
NO-2027 Kjeller

Office address:
Instituttveien 20
N-2007 Kjeller

Telephone: +47 63 80 70 00
Telefax: +47 63 80 71 15
Email: ffi@ffi.no

FFI Forsvarets forskningsinstitutt