Direktoratet for e-helse

Overordnet risiko- og sårbarhetsvurdering for IKT i helse- og omsorgssektoren

Rapport fra Direktoratet for e-helse

Publikasjonens tittel:
Overordnet IKT-ROS for helse- og omsorgssektoren

Rapportnummer
IE-1047

Utgitt:
25.06.2019

Utgitt av:
Direktoratet for e-helse

Kontakt:
postmottak@ehelse.no

Besøksadresse:
Verkstedveien 1, 0277 Oslo
Tlf.: 21 49 50 70

Publikasjonen kan lastes ned på:

WWW.EHELSE.NO

Innhold

Forord

Denne rapporten er utarbeidet av Direktoratet for e-helse i samarbeid med Helsedirektoratet og Norsk Helsenett SF på oppdrag fra Helse- og omsorgsdepartementet.

Norge er et av de mest digitaliserte landene i verden, og norsk helse- og omsorgssektor er et tydelig eksempel på hvordan digitaliseringen endrer det offentlige tjenestetilbudet. I takt med digitaliseringen øker også avhengighetene mellom IKT, pasientbehandling og pasientsikkerhet. Utilgjengelighet av IKT-systemer er i dag en alvorlig trussel for helse- og omsorgssektoren.

Trusselbildet på IKT-området generelt har endret seg mye de siste årene. Der hvor man tidligere primært så aktivitet som var knyttet til handlinger utført av enkeltindivider, mindre aktivistgrupper og tilsvarende, ser man nå både internasjonalt og nasjonalt et økende antall tilfeller av profesjonelle aktører med knytninger til fremmede stater.

I denne rapporten har vi arbeidet oss igjennom tidligere rapporter og utredninger, gått igjennom nasjonale trusselvurderinger og et utvalg hendelser som har påvirket helsetjenesten i ulik grad. På bakgrunn av trusselbildet, funn fra hendelser og øvelser og allerede foreslåtte tiltak beskrevet i tidligere rapporter og utredninger, foreslår Direktoratet for e-helse fem konkrete tiltak som effektivt vil kunne løfte sikkerhetsnivået i helse- og omsorgssektoren på kort- og mellomlang sikt.

Rapporten konkluderer med at arbeidet med IKT-sikkerhet i helse- og omsorgssektoren må styrkes. Dette er nødvendig fordi økt digitalisering, flere sammenkoblede systemer og mer utveksling av informasjon for å skape bedre tjenester for pasientene og nye gevinster for sektoren, også vil kunne introdusere nye trusler og sårbarheter. Viktigheten understrekes av at det de siste årene har vært en rekke alvorlige IKT-hendelser i helse- og omsorgssektoren både i Norge og internasjonalt.

Oslo, 1. juli 2019

Christine Bergland

Direktør

Sammendrag

Norge er et av de mest digitaliserte landene i verden, og norsk helse- og omsorgssektor er et tydelig eksempel på hvordan digitaliseringen endrer det offentlige tjenestetilbudet. I Norge er vi også i toppen når det gjelder å ta i bruk ny teknologi, og det pågår et stort og langvarig arbeid i sektoren med å digitalisere og effektivisere arbeidsprosessene. Økt digitalisering, flere sammenkoblede systemer og mer utveksling av informasjon vil skape bedre tjenester for pasientene og nye gevinster for sektoren, men introduserer samtidig nye trusler og sårbarheter.

I takt med digitaliseringen øker også avhengighetene mellom IKT, pasientbehandling og pasientsikkerhet. Tilgjengelighet, integritet og konfidensialitet er, og har alltid vært, hjørnesteinene i behandling av pasientinformasjon i sektoren. Journalopplysninger, som før skulle være låst inne i et arkivskap, befinner seg nå i komplekse IKT-systemer med mange avhengigheter. Dette muliggjør rask og effektiv tilgang til og deling av informasjon for helsepersonell som deltar i behandling av pasienten, men åpner samtidig opp for nye sårbarheter og potensielle angrepsflater for ondsinnede aktører. Utilgjengelighet av IKT-systemer er i dag en alvorlig trussel for helse- og omsorgssektoren.

Trusselbildet på IKT-området generelt har endret seg mye de siste årene. Der hvor man tidligere primært så aktivitet som var knyttet til handlinger utført av enkeltindivider, mindre aktivistgrupper og tilsvarende, ser man nå både internasjonalt og nasjonalt et økende antall tilfeller av profesjonelle aktører med knytninger til fremmede stater. Målet for disse aktørene er å bryte seg inn i IKT-systemene til myndigheter, bedrifter og kompetanseinstitusjoner for å stjele data, drive etterretningsvirksomhet og i noen tilfeller gjennomføre sabotasje.

De siste årene har det vært en rekke alvorlige IKT-hendelser i helse- og omsorgssektoren både i Norge og internasjonalt. I mai 2017 rammet viruset "WannaCry" offentlig helsetjeneste i England (NHS) ved å låse brukere ute fra systemene ved flere sykehus og fastlegekontor. Noen måneder senere startet spredningen av viruset "NotPetya" som blant annet stoppet opp deler av legemiddelproduksjonen til Merck, et av verdens største legemiddelfirma. Januar 2018 ble det kjent at en avansert og profesjonell aktør hadde brutt seg inn i datanettverket til Helse Sør-Øst RHF. Og i juli 2018 opplevde helsetjenesten i Singapore at en annen profesjonell aktør brøt seg inn i systemene og hentet ut personlige opplysninger om nesten 1,5 millioner pasienter. Denne aktøren gikk flere ganger spesifikt inn og hentet ut informasjon om landets statsminister.

Eksemplene er mange, og hendelsene over illustrerer hvilke trusler man står ovenfor, hvordan sårbarheter kan utnyttes og ikke minst hvilke konsekvenser dette har for verdiene man ønsker å verne om, både som organisasjon og nasjon.

Direktoratet for e-helse har i sin overordnede ROS-vurdering for helse- og omsorgssektorens IKT-sårbarheter, påpekt de sårbarhetene som er vurdert til å utgjøre størst risiko sett opp mot dagens trusselbilde. Disse er blant annet:

- Lange, komplekse og uoversiktlige verdikjeder
- Manglende IKT-sikkerhetskompetanse
- Mangelfull implementering av tekniske sikkerhetstiltak
- Utdatert programvare og utstyr som ikke oppdateres
- Mangel på og mangelfull etterlevelse av styringssystem for informasjonssikkerhet
- Manglende planverk og trening i håndtering av IKT-hendelser

På bakgrunn av trusselbildet, funn fra hendelser og øvelser og allerede foreslåtte tiltak beskrevet i tidligere rapporter og utredninger, foreslår Direktoratet for e-helse fem konkrete tiltak som effektivt vil kunne løfte sikkerhetsnivået i helse- og omsorgssektoren på kort- og mellomlang sikt. Det vil kreve ressurser, prioritering og lederforankring for å kunne gjennomføre de anbefalte tiltakene på en tilfredsstillende måte.

Tiltak 1: Utarbeidelse av nasjonal IKT-beredskapsplan for helse- og omsorgssektoren som en del av Nasjonal helseberedskapsplan
Planen bør bl.a. omfatte tiltak for å hindre spredning eller avverge ytterligere angrep mot IKT-infrastruktur under en hendelse.
Tiltak 2: Gjennomføre årlig IKT-øvelse
Det bør årlig gjennomføres en øvelse på IKT-scenarier som får konsekvenser for helsesektoren. Øvelsen bør sees i sammenheng med Nasjonal helseøvelse.
Tiltak 3: Styrket operativ IKT-sikkerhet i helse- og omsorgssektoren
HelseCERT bør i kraft av sin rolle som helse- og omsorgssektorens nasjonale senter for informasjonssikkerhet gi ut årlige anbefalinger om basistiltak for økt operativ IKT-sikkerhet i helsesektoren, og ellers kartlegge og informere om den generelle sikkerhetstilstanden i helse- og omsorgssektoren. De foreslåtte tiltakene må være basert på funn av sårbarheter identifisert gjennom sårbarhetsskanning og inntrengningstesting.
Tiltak 4: Styrket myndighetsrolle for IKT-sikkerhet i helse- og omsorgssektoren
Direktoratet for e-helse bør styrke sin rolle som fagorgan for sektoren innen informasjonssikkerhet. Dette bør skje gjennom at direktoratet styrker arbeidet med opplæring og rådgivning knyttet til informasjonssikkerhet og personvern, og ellers kartlegger og informerer om den generelle sikkerhetstilstanden i helse- og omsorgssektoren.
Tiltak 5: Utarbeidelse av helhetlig IKT-sikkerhetsstrategi for helse- og omsorgssektoren
Det bør utarbeides en helhetlig IKT-sikkerhetsstrategi for helse- og omsorgssektoren. IKT-sikkerhetsstrategien bør ses opp mot nasjonal strategi for IKT-sikkerhet og ta høyde for sektorspesifikke utfordringer og utvikling av dagens helsetjeneste.

1 Innledning

1.1 Oppdrag

I juni 2017 leverte Helsedirektoratet sin rapport "Overordnede risiko- og sårbarhetsvurderinger for helse og omsorgssektoren". I konklusjonen for IKT-området ble det løftet frem at det bør gjennomføres en særskilt ROS-analyse for hele helse- og omsorgssektorens IKT-sårbarheter og at Direktoratet for e-helse bør lede dette arbeidet.

I 2018 vurderte Direktoratet for e-helse behovet for og mulig innretning på gjennomføring av risiko- og sårbarhetsanalyse for helse- og omsorgsektorens IKT-sårbarheter. E-helse fremla for departementet et forslag om en stegvis tilnærming (delt i fire deler; A, B, C og D). HOD støttet direktoratets vurdering og anbefaling.

I tildelingsbrev for 2019 fikk Direktoratet for e-helse følgende oppdrag av Helse- og Omsorgsdepartementet:

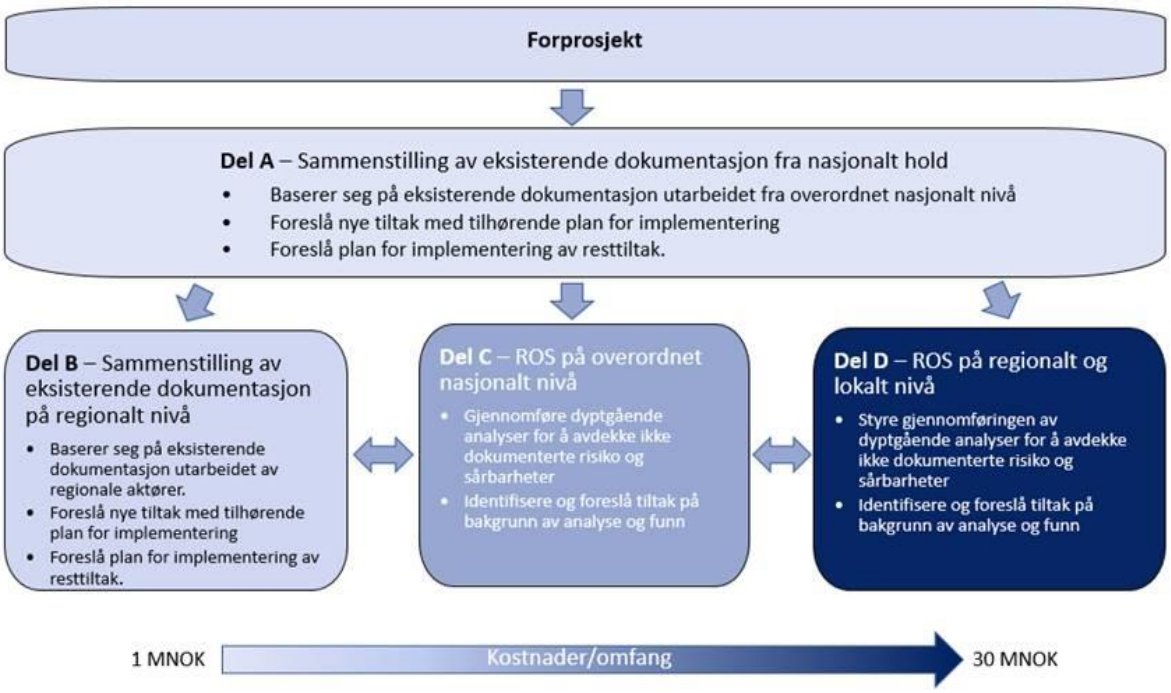
"Gjennomføre en risiko- og sårbarhetsanalyse for helse- og omsorgssektorens IKT-sårbarheter med spesielt fokus på tiltak og oppfølging av disse. Arbeidet må gjøres i samarbeid med Norsk Helsenett SF og andre relevante aktører, i tillegg til Helsedirektoratet, som leder arbeidet i helse- og omsorgssektoren."

1.2 Avgrensing

Direktoratet for e-helse har tidligere[1] anbefalt en stegvis innretning på gjennomføring av en risiko- og sårbarhetsanalyse for helse- og omsorgssektorens IKT-sårbarheter. HOD støttet i brev av 15. august 2018 direktoratets vurdering og anbefaling om en tilnærming med stegvis gjennomføring.

Anbefalingen beskrev fire ulike tilnærminger til å gjennomføre en ROS-analyse (del A, B, C og D). Se figur nedenfor.

[1] I brev av 13.4.2018 som svar på oppdrag i tildelingsbrevet 2018 om vurdering av behovet for og mulig innretning på gjennomføring av risiko- og sårbarhetsanalyse for helse- og omsorgssektorens IKT-sårbarheter.



De ulike delene kan gjennomføres stegvis og i ulike kombinasjoner, men det vil uansett være hensiktsmessig å starte med del A. Denne rapporten vil søke å svare på del A, der tiltak (eksisterende og forslag til nye) vil være det viktigste fokuset.

Oppsummert, handler del A om å skaffe oversikt over hvilke risikoer og sårbarheter helse- og omsorgssektoren har på IKT-området og hvilke risikoreduserende tiltak som fremdeles er utestående. Oversikten vil gi grunnlag for å trekke frem tiltak foreslått i tidligere rapporter og utredninger og legge frem nye tiltak basert på funn fra egen gjennomgang.

Datagrunnlaget vil i del A hovedsakelig bestå av tidligere stortingsmeldinger, høringer, rapporter og utredninger som er produsert fra sentralt hold. I NOU 2015: 13 setter Lysneutvalget spørsmålstegn ved hvorfor ikke flere av tiltakene som er beskrevet i tidligere utredninger er fulgt opp, og om mengden utredninger i seg selv er til hinder for en effektiv iverksetting av tiltakene. I løpet av de tre-fire siste årene er det produsert ytterligere dokumenter som peker på mye av det samme det som allerede er utgitt. I del A benytter man derfor allerede produsert analysemateriale til å identifisere hvilke tiltak som mest effektivt vil redusere risikoene og sårbarhetene.

I det videre kan del B, C og D gjennomføres hver for seg eller stegvis, ut i fra et kost-nytteperspektiv.

Denne rapporten vil være overordnet med et nasjonalt fokus selv om innholdet også vil være relevant for mindre aktører. Tiltakene som foreslås vil også ha et nasjonalt fokus og flere av dem vil ligge på myndighetssiden. I likhet med Helsedirektoratets Overordnede risiko og sårbarhetsvurdering fra 2017 vil også denne rapporten legge vekt på hva risikoene og sårbarhetene består i, uten å gi noen inngående redegjørelser for sannsynlighet, konsekvens og usikkerhet.

2 Metode

2.1 Prosess

I tråd med oppdraget fra HOD, har arbeidet blitt gjennomført i samarbeid med Norsk helsenett (NHN) og Helsedirektoratet (Hdir). Sistnevnte leder det overordnede arbeidet med å holde systematisk oversikt over risiko og sårbarhet i sektoren. Fremdriften for arbeidet med IKT-ROS har inngått i referansegruppemøter ledet av Hdir, og dette har fungert som et forum for å kunne adressere og diskutere relevante problemstillinger.

For å sikre at rapporten skulle resultere i konkrete tiltak, ble arbeidet med å definere forslag til nye tiltak igangsatt tidlig i prosessen. Tiltakene er utformet med bakgrunn i datagrunnlaget presentert under, og det har vært et mål at tiltakene skal treffe så mange av de identifiserte sårbarhetene som mulig, samtidig som de må være tilstrekkelig spisset for enklere gjennomføring. Det har også vært et mål å peke på hvilken aktør som bør være ansvarlig for å utføre tiltaket og å definere en realistisk frist for å legge til rette for at tiltaket blir gjennomført. Det krever ressurser, prioritering og lederforankring for å kunne gjennomføre de anbefalte tiltakene på en tilfredsstillende måte.

2.2 Datagrunnlag

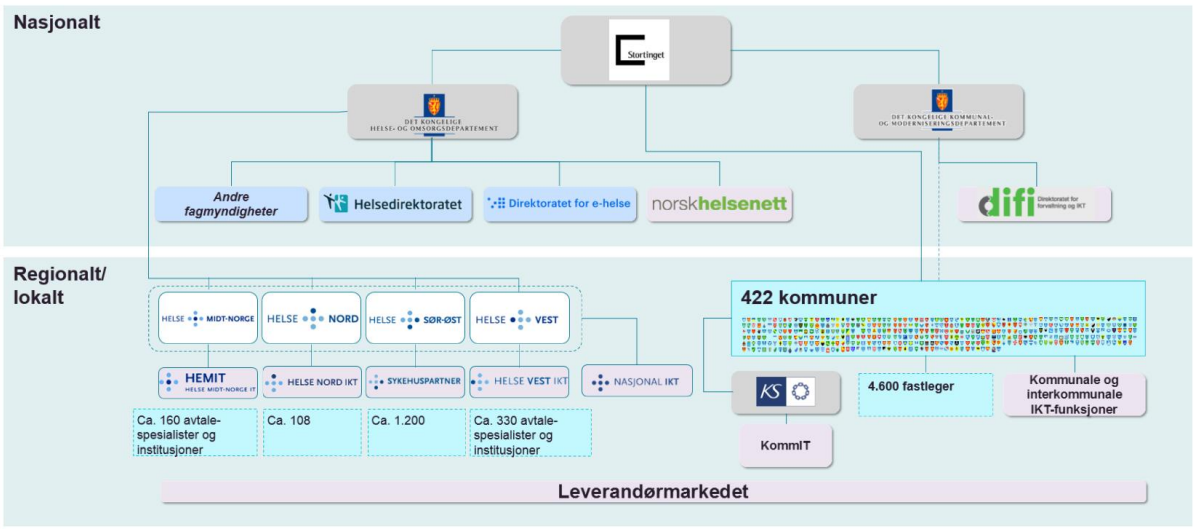
Datagrunnlaget for denne rapporten er både tverrsektorielt og sektorspesifikt. E-helse har således hatt et bredt perspektiv i søket etter relevant dokumentasjon, med både sikkerhet, IKT-sikkerhet, informasjonssikkerhet, sårbarhet, risiko, trusler som sentrale nøkkelord. Dokumentasjonen som er valgt ut, er i hovedsak åpne kilder utgitt i tidsrommet 2015 til vinter 2019, med Lysneutvalgets NOU 2015: 13 som startpunkt. I arbeidet har man trukket ut de momentene som er vurdert som mest relevante i de nedenstående kildene, for å kunne gjøre vurderinger av risiko, sårbarheter og tiltak for helse- og omsorgssektoren.

- NOU 2015: 13 Digital sårbarhet – sikkert samfunn
- NOU 2016: 19 Samhandling for sikkerhet
- Meld. St. 27 (2015–2016) Digital agenda for Norge
- Meld. St. 38 (2016-2017) IKT-sikkerhet – et felles ansvar
- Meld. St. 10 (2016-2017) Risiko i et trygt samfunn
- Risikoanalyse av "Cyberangrep mot ekom-infrastruktur", Direktoratet for samfunnssikkerhet og beredskap (2015)
- Overordnede risiko- og sårbarhetsvurderinger i helse- og omsorgssektoren, Helsedirektoratet (2017)
- Prop. 153 L (2016-2017) Lov om nasjonal sikkerhet (sikkerhetsloven)
- IKT-organisering i helse- og omsorgssektoren, Direktoratet for e-helse (2017)
- Informasjonssikkerhet ved bruk av private leverandører i helse- og omsorgstjenesten, Direktoratet for e-helse (2017)

- Tverrsektoriell evalueringsrapport fra øvelse IKT16, Direktoratet for samfunnssikkerhet og beredskap (2017) (unntatt offentlighet)
- NOU 2018: 14 IKT-sikkerhet i alle ledd
- Lessons learned review of the WannaCry Ransomware Cyber Attack, NHS England (2018)
- Mørketallsundersøkelsen 2018, Næringslivets sikkerhetsråd
- Nasjonal strategi for digital sikkerhet, Departementene (2019)
- Trusselvurdering 2019, Politiets sikkerhetstjeneste
- Fokus 2019, Forsvaret
- IKT-risikobilde 2019, Nasjonal sikkerhetsmyndighet
- IKT-risikobilde 2018, Nasjonal sikkerhetsmyndighet
- Rammeverk for håndtering av IKT-sikkerhetshendelser, Nasjonal sikkerhetsmyndighet
- Situasjonsbilde 2018, HelseCERT
- IKT-sikkerhetskompetanse i arbeidslivet – behov og tilbud, Nordisk institutt for studier av innovasjon, forskning og utdanning (2017)
- Utviklingstrekk 2019, Direktoratet for e-helse

3 Aktørbilde

Helsesektoren kan hovedsakelig deles inn i fag- og myndighetsorganer, spesialisthelsetjenesten og primærhelsetjenesten (inkludert fastleger). I tillegg finnes det både nasjonale leverandører og leverandører fra det private markedet. Figuren under gir et overblikk over aktører i norsk helse- og omsorgssektor og deres styringslinjer.



Et komplekst aktørbilde forsterker sårbarheten, fordi ansvaret for ulike løsninger, produkter og verdikjeder er fragmentert og uoversiktlig. Drifts- og forvaltningsansvaret er plassert hos både offentlige og private leverandører. Dette gjør det utfordrende å skaffe oversikt over og drive god styring av risiko og sårbarhet for IKT i sektoren.

Virksomhetene i sektoren varierer i størrelse, med alt fra store virksomheter med over 1400 ansatte til små IT-avdelinger i de minste kommunene. Siden virksomhetene er av ulik størrelse er også kompetansen og tilgjengelig kapasitet til å følge opp IT-sikkerhet, styringssystemer og systematisk risikoarbeid svært variert.

3.1 Fag- og myndighetsorganer innenfor helse- og omsorgssektoren

Helse- og omsorgsdepartementet
Helse- og omsorgsdepartementet (HOD) har det strategiske ansvaret for IKT-utviklingen i helse- og omsorgssektoren og har et overordnet ansvar for at befolkningen har tilgang til gode og likeverdige helse- og omsorgstjenester. HOD har underliggende etater (Direktoratet for e-helse, Helsedirektoratet, Helsetilsynet, Statens legemiddelverk, Folkehelseinstituttet m.fl.) som blant annet ivaretar rollen som forvalter av IKT-løsninger, registre og sektorens felleskomponenter. Departementet eier også de fire regionale helseforetakene og Norsk Helsenett SF.

Helsedirektoratet
Helsedirektoratet er et fag- og myndighetsorgan underlagt HOD, og har ansvar for å iverksette politikk, samt forvalte lov og regelverk innenfor helse- omsorgssektoren. Helsedirektoratet har også ansvar for den nasjonale beredskapen i sektoren.

Direktoratet for e-helse
Direktoratet for e-helse ble etablert i 2016. Direktoratet har nasjonal myndighet og premissgiverrolle på e-helseområdet og skal være en pådriver i utviklingen av digitale tjenester i helse- og omsorgssektoren. Et av direktoratets faste oppdrag er å ha ansvar for styring, utvikling og forvaltning av nasjonale løsninger på e-helseområdet (eks. e-resept, kjernejournal, helsenorge.no og grunndata). Direktoratet for e-helse har ansvar for sekretariatet for Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten. I tillegg gjennomføres en del andre aktiviteter som omfatter informasjonssikkerhet og personvern, som f.eks. en årlig innbyggerundersøkelse om e-helse[2].

Folkehelseinstituttet (FHI)
Folkehelseinstituttet (FHI) er et forvaltningsorgan underlagt HOD, og en nasjonal kompetanseinstitusjon innen folkehelse. FHI sine virkeområder er i hovedsak helseovervåking, forskning og forebygging, hvor beredskap innen smittevern og miljømedisin, psykisk helse, rusmiddelforskning, helsestatistikk, befolkningsundersøkelser, livsstil og helse, sosiale helseforskjeller og internasjonale helseutfordringer er sentralt.

Statens legemiddelverk (SLV)
Statens legemiddelverk er også et forvaltningsorgan underlagt HOD. SLV forvalter legemiddelloven og apotekloven, som regulerer virksomheten i apotek, grossister og legemiddelprodusenter. SLV har også ansvar for å vurdere og godkjenne nye legemidler, inkludert vaksiner. Legemiddelverket har også en nøkkelrolle i legemiddelberedskap, både ved å overvåke markedssituasjonen og å bistå helsetjenesten med å løse mangelsituasjoner. SLV leverer også Forskrivnings- og ekspedisjonsstøtte (FEST) som forsyner alle deler av reseptkjeden i e-resept med kvalitetssikret og oppdatert legemiddelinformasjon.

Statens helsetilsyn

Statens helsetilsyn er øverste tilsynsmyndighet og har det overordnede faglige tilsynet med helse- og sosialtjenestene. Tilsyn og rådgivning basert på erfaringer fra tilsyn skal medvirke til at befolkningens

[2] https://ehelse.no/aktuelt/tryggere-med-e-helse

behov for sosiale tjenester og helsetjenester ivaretas, at tjenestene drives på en faglig forsvarlig måte, at svikt i tjenesteytingen forebygges og at ressursene brukes på en forsvarlig og effektiv måte.

I tildelingsbrevet for 2019 står det at Helsetilsynet skal bygge opp nødvendig kapasitet og kompetanse for å kunne føre tilsyn med IKT i tjenestene.

3.2 Spesialisthelsetjenesten

De regionale helseforetakene (heretter RHF-ene) har ansvar for spesialisthelsetjenesten, forskning og undervisning. For å ivareta IKT på en best mulig måte har de fire RHF-ene opprettet egne regionale tjenesteleverandører som ivaretar utvikling, drift og forvaltning av løsningene til RHF-et og deres tilhørende HF.

3.3 Primærhelsetjenesten

Hver enkelt kommune har ansvar for den kommunale helse- og omsorgstjenesten. Dette innebærer at kommunene har råderett over lokale anliggender innenfor de formelle styringslinjene gitt av storting, regjering og departement. I Meld. St. 12 (2011-2012) Stat og kommune – styring og samspel, har regjeringen lagt til grunn at rammestyring skal fungere som hovedprinsipp for styring av kommunene. Dette betyr at kommunene og fylkeskommunene i stor grad har mulighet til å organisere sine tjenester og virksomheter ut fra lokale prioriteringer og behov. Statlige pålegg ovenfor kommuner og fylkeskommuner må skje i lovs form eller med hjemmel i lov.

Kommunesektoren skal sikre gode og forsvarlige helse- og sosialtjenester, og har ansvar for mange viktige velferdstjenester slik som primærhelsetjenester, pleie- og omsorgstjenester, barnevern, barnehager og skole. Kommunene har ansvar for å tilby en fastlegeordning, der kommunen inngår individuelle fastlegeavtaler med allmennleger. Fastlegeoppgavene er i hovedsak ivaretatt av selvstendig næringsdrivende, og ifølge HELFO (2014) var 94,5 prosent av fastlegene privatpraktiserende, mens de resterende 4,6 prosent var ansatt i kommunen. Kommunen styrer primært fastlegetjenesten gjennom inngåelse og oppfølging av individuelle fastlegeavtaler med legene, samt via drøfting av aktuelle spørsmål i Lokalt samarbeidsutvalg (LSU).

3.4 Nasjonale leverandører

Norsk Helsenett SF (NHN)
Norsk Helsenett (NHN) ble etablert i 2004 etter initiativ fra de regionale helseforetakene. Norsk Helsenett SF skal påse at det foreligger en sikker og hensiktsmessig infrastruktur som tilrettelegger for effektiv samhandling mellom aktørene i helse- og omsorgssektoren. Norsk Helsenett SF har et ikke-økonomisk formål og skal bidra til forenkling, effektivisering og kvalitetssikring av elektroniske tjenester til det beste for pasienter, helsepersonell og befolkningen for øvrig.

HelseCERT (NHN)

HelseCERT er helse- og omsorgssektorens nasjonale senter for informasjonssikkerhet. HelseCERTs 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.

HelseCERT driver «Nasjonalt beskyttelsesprogram» (NBP). Formålet med tjenesten er å gi IKT-driftspersonell verdifull informasjon om aktuelle trusler, sårbarheter og hendelser. Nasjonalt beskyttelsesprogram inneholder flere komponenter som monitorering, informasjonsdeling og forebygging, hendelseshåndtering, sårbarhetsoversikt og inntrengingstesting. I dag er RHF-enes IKT-driftsorganisasjoner og de fleste kommuner medlemmer av NBP.

HelseCERT gjennomfører også årlig sikkerhetssamtaler med et lite utvalg virksomheter som er tilknyttet Norsk Helsenett. Sikkerhetssamtalen inngår i Norsk Helsenetts rutiner for oppfølging av avtaleforholdet med etablerte kunder.

Helsetjenestens driftsorganisasjon for nødnett HF (HDO)
Helsetjenestens driftsorganisasjon for nødnett HF (HDO) er eid av de fire RHF-ene og er tillagt ansvar for drift, vedlikehold og brukerstøtte til helsetjenestens brukere. Nødnettet er et lukket beredskapsnett for politi, helsetjenesten, brannvesen og andre aktører med et nød- og beredskapsansvar.

Direktoratet for e-helse
Direktoratet for e-helse er i dag leverandør av nasjonale e-helseløsninger som e-resept, nasjonal kjernejournal, helsenorge.no og grunndata. Som det fremgår av tildelingsbrevet til direktoratet for 2019, tar Helse- og omsorgsdepartementet sikte på å overføre dagens leveranseoppgaver til en nasjonal tjenesteleverandør med utgangspunkt i dagens Norsk Helsenett SF, med plan om implementering fra 1. januar 2020.

3.5 Andre relevante aktører

Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten

Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten (Normen) er et omforent sett av krav til informasjonssikkerhet og personvern basert på lovverket. Normen stiller også krav som detaljerer og supplerer gjeldende regelverk. Normens krav er krav som helsetjenesten mener er sentrale for sektorens tekniske og organisatoriske tiltak for informasjonssikkerhet og personvern.

I tillegg til å være et felles kravsett gjennom bransjenormen, bidrar Normen med veiledningsmateriell, kurs og kompetanseheving.

Normen er utarbeidet av representanter for helse-, omsorg- og sosialsektoren og forvaltes av styringsgruppen for Norm for informasjonssikkerhet. Styringsgruppen er sammensatt av representanter fra helse- og omsorgssektoren, og har sitt organisatoriske knutepunkt og sekretariat i Direktoratet for e-helse. Normen er en autonom bransjenorm, og omtales derfor her som en egen aktør. Personvernforordningen oppfordrer til etablering av adferdsnormer. Gjeldende versjon av Normen (5.3) er oversendt Datatilsynet for godkjenning som adferdsnorm etter personvernforordningens bestemmelser.

Normen og veiledningsmateriellet oppdateres jevnlig. Normen er for tiden under oppdatering til versjon 6.0. Her tas det blant inn mer innhold om informasjonssikkerhet ved bruk av private leverandører. NSM grunnprinsipper for IKT-sikkerhet legges til grunn for oppdateringer i Normens kapittel om informasjonssikkerhet.

3.6 Private leverandører

Helse- og omsorgssektoren benytter i utstrakt grad private leverandører på hele tjenestekjeden fra serverdrift til medisinsk utstyr. Sektoren er helt avhengig av private leverandører, både nasjonale og internasjonale, innen IKT-området, for å sikre tilgang til oppdatert teknologi, løsninger og tilstrekkelig kompetanse.

3.7 Fag- og myndighetsorganer utenfor helse- og omsorgssektoren

Justis- og beredskapsdepartementet har samordningsansvaret for IKT-sikkerhet i sivil sektor. **Forsvarsdepartementet** har ansvar for IKT-sikkerhet i forsvarssektoren. De to departementene skal sammen bidra til at sivil-militære utfordringer og behov sees i sammenheng. **Kommunal – og moderniseringsdepartementet** har samordningsansvaret for regjeringens IKT-politikk. **Samferdselsdepartementet** har ansvar for IKT-sikkerheten knyttet til elektronisk kommunikasjonsnett og -tjenester, herunder internett. **Utenriksdepartementet** har overordnet ansvar for å norsk utenriks- og sikkerhetspolitikk, herunder å koordinere Norges innsats og posisjoner på internasjonale arenaer hvor globale utfordringer i det digitale rommet diskuteres.

Organiseringen av tverrsektorielle oppgaver innen IKT-sikkerhet i Norge er fordelt mellom flere etater. Sentrale virksomheter er **Nasjonal sikkerhetsmyndighet** (**NSM)**, **Direktoratet for forvaltning og ikt** (**Difi)**, **Nasjonal kommunikasjonsmyndighet** (**NKom)**, **Direktoratet for samfunnssikkerhet** og **beredskap (DSB)** og **Datatilsynet**.

NSM **NorCERT** er den operative delen av NSM, og håndterer alvorlige dataangrep mot samfunnskritisk infrastruktur og informasjon.

Felles Cyberkoordineringssenter (FCKS) er et permanent, samlokalisert fagmiljø med representanter fra NSM, E-tjenesten, PST og Kripos. FCKS skal bidra til å øke den nasjonale evnen til å motstå alvorlige digitale angrep og understøtte strategisk analyseproduksjon og vedlikeholde et helhetlig trussel- og risikobilde for det digitale rom.

4 Trusselbildet og hendelser

Trusselbildet på IKT-området har endret seg mye de siste årene. Tidligere så man primært aktivitet som var knyttet til handlinger utført av enkeltindivider, mindre aktivistgrupper og tilsvarende. De siste årene har man, både internasjonalt og nasjonalt, sett flere og flere tilfeller hvor såkalte Advanced Persistent Threat (APT)-aktører målrettet bryter seg inn i IT-systemene til myndigheter, bedrifter og kompetanseinstitusjoner.

De senere årene har man også sett større og større kampanjer med løsepengevirus som WannaCry og NotPetya. WannaCry rammet offentlig helsetjeneste (NHS) i England ved å låse brukere ute fra systemene ved enkelte sykehus, mens NotPetya stoppet opp deler av Merck sin produksjon av legemidler.

Utilsiktede hendelser er også en trussel som kan få store konsekvenser for enkelte organisasjoner, men også på tvers av sektorer pga. de digitale verdikjedene. I november 2011 medførte en feil på en sentral lagringsløsning til IT-leverandøren Tieto i Sverige at systemene til over 350 apotek ble utilgjengelig og at befolkningen ikke fikk hentet ut e-resepter på flere dager. I denne enkelthendelsen ble over 50 kunder av Tieto rammet av langvarig utilgjengelighet, og blant disse var det flere kommuner og statlige selskap.

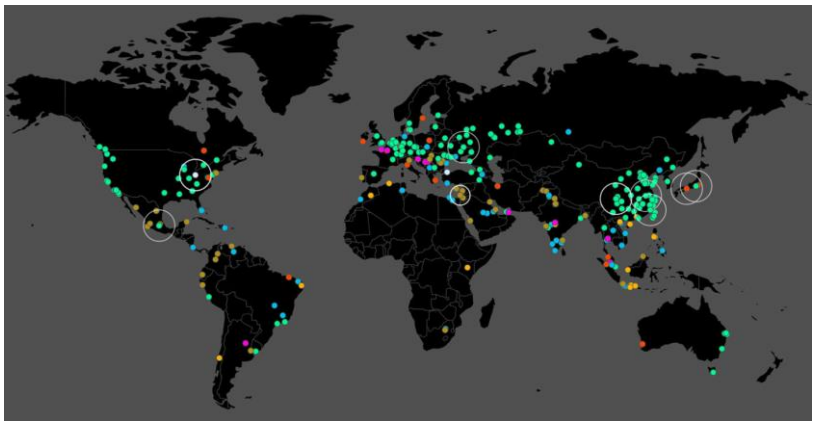
Oppsummert, medfører digitaliseringen, de nye og gamle sårbarhetene og det endrede trusselbildet at helse- og omsorgssektoren i økende grad er utsatt for digitale angrep.

APT

APT er et begrep som benyttes om avanserte trusselaktører som ofte kan være statlig sponsede hackergrupper og fremmede lands etterretning. En APT er en aktør med store kapabiliteter og kapasiteter og som ofte har et langsiktig perspektiv på sine operasjoner og kan jobbe målrettet over flere år

Løsepengevirus

Løsepengevirus eller Ransomware som det blir kalt på engelsk, er en type skadelig programvare (datavirus) som krypterer hele eller deler av innholdet på en infisert datamaskin. Dette medfører at hele systemet eller enkelte filer er utilgjengelig for eieren. For å få tilbake filene eller systemet, skal det betales løsepenger gjerne i form av bitcoin eller annen kryptovaluta til ukjent mottaker.



I løpet av en helg hadde WannaCry-viruset spredd seg til over 200 000 maskiner i over 150 land.

Kilde: MalwareTech

4.1 Nasjonale trusselvurderinger

Hvert år gis det ut fire nasjonale trussel- og risikovurderinger; "IKT-risikobilde" fra Nasjonal Sikkerhetsmyndighet (NSM), "Trusselvurdering" fra Politiets sikkerhetstjeneste (PST), "Fokus" fra Etterretningstjenesten (E-tjenesten) og "Krisescenarier" fra Direktoratet for samfunnssikkerhet og beredskap (DSB). Disse fire rapportene tar for seg samfunnets viktige sårbarheter og trusler, og danner sammen et godt bilde av de truslene man står ovenfor i dag og i tiden som kommer.

Det norske samfunnet og helse- og omsorgssektoren er avhengig av IKT. I sektoren og samfunnet forøvrig blir stadig flere arbeidsprosesser, tjenester og funksjoner digitalisert, og dette skaper større avhengigheter til IKT-systemene. Sårbarhetene øker også i takt med de lange og uoversiktlige digitale verdikjedene som skapes.

Både PST og E-tjenesten peker i sine rapporter på at spionasje og etterretningsoperasjoner fra fremmede land vil være en av de største truslene mot Norge. I sammendraget fra Fokus 2019 oppsummerer E-tjenesten det slik:

> *"Etterretningstrusselen er den mest pågående og omfattende sikkerhetsutfordringen mot Norge og norske interesser. Russiske og kinesiske aktører står for hovedandelen av aktiviteten, og operasjonene blir mer koordinerte. Målene er politiske og militære, så vel som forskningsinstitusjoner og bedrifter med tilgang til høyteknologi. Russiske og kinesiske etterretnings- og sikkerhetstjenester har ressurser til å utføre komplekse, offensive nettverksoperasjoner, og utvikler ferdighetene kontinuerlig. Samtidig har tilgangen til avansert skadelig programvare blitt enklere både for statlige og ikke-statlige aktører."*

E-tjenesten nevner i sin trusselvurdering helsesektoren som et attraktivt mål for spionasje.

> *"Norske kunnskaps- og forskningsinstitusjoner, og aktører innenfor industrisektoren, vil være aktuelle mål for spionasje også i 2019. Utenlandske aktører viser særlig interesse for bedrifter som har unik kompetanse og teknologi, blant annet innenfor våpenindustri, romforskning, maritim sektor og helsesektoren. "*

PST trekker frem både trusselen med rekruttering av innsidere og avanserte operasjoner som har som mål å bryte seg inn i datanettverk:

"I 2019 vil flere lands etterretningstjenester forsøke å rekruttere kilder og kartlegge personer og virksomheter i Norge. De vil også forsøke å skaffe seg urettmessig tilgang til norske virksomheters datanettverk. Formålet vil være å skaffe sensitiv informasjon og å påvirke beslutninger. Operasjonene til disse tjenestene vil rettes mot personer og virksomheter innen norsk statsforvaltning, kritisk infrastruktur, forsvar og beredskap, samt mot forskning og utvikling.

Den vanligste måten å komme seg på innsiden av et nettverk på, vil fremdeles være å sende skadevare via målrettede e-poster. Dette er meldinger som ofte er skreddersydd til mottaker. Ved at de appellerer til en faglig eller personlig interesse og knyttes til kjente avsendere, fremstår meldingene som legitime for mottakerne. Vi har også erfart at trusselaktører har brutt seg inn i datanettverk ved at medarbeidere eller gjester bevisst eller ubevisst har plassert skadevare via for eksempel minnepinner. I tillegg ser vi at trusselaktører bruker servere som er koblet til internett som inngangsport. Disse kan være sårbare for utnyttelse. For eksempel har trusselaktører flere ganger skaffet seg tilgang til et nettverk via systemene som brukes for å publisere informasjon på en virksomhets nettsider.

En god del av forsøkene på å trenge inn i norske nettverk blir gjennomført for å rekognosere og identifisere sårbarheter, og for å hente ut informasjon. I tillegg ser vi avanserte operasjoner mot virksomheter som ikke er mål i seg selv, men som kun fungerer som brohode for videre tilgang til andre mål."

4.2 Eksempler på hendelser i helsevesenet

De siste årene har det vært en rekke alvorlige IKT-hendelser i helse- og omsorgssektoren både i Norge og internasjonalt. Hendelsene synliggjør på en effektiv måte hvordan trusselaktører jobber og hvilke sårbarheter de ofte utnytter. Ved å legge ressurser i å analysere og forstå konkrete hendelser kan man skaffe seg en dypere og mer realitetsorientert forståelse av truslene man står ovenfor. Det gir oss også muligheten til å utvikle avgjørende kunnskap om hvilke tiltak som bør treffes for å være mer motstandsdyktig mot lignende hendelser i fremtiden.

I det følgende presenteres en kort oppsummering av fire utvalgte hendelser fra nyere tid, med fokus på angrepsvektorer, konsekvenser og hendelseshåndtering på overordnet nivå. Tiltak som er foreslått i etterkant av disse hendelsene presenteres i kap. 6.

4.2.1 Hendelsen i Helse Sør-Øst RHF

Den 8. januar 2018 mottok Sykehuspartner varsel fra HelseCERT om mistenkelig aktivitet mot deres datasystemer. Etter nærmere undersøkelser viste det seg at systemene var kompromittert av en profesjonell, avansert aktør. Hendelsen ble etterforsket av PST som ulovlig etterretningsvirksomhet som kan skade grunnleggende nasjonale interesser knyttet til samfunnets infrastruktur. Innbruddet ble gjennomført ved å utnytte en sårbar applikasjon i regionen. I forkant av angrepet viste det seg at trusselaktøren hadde foretatt skanning for å avdekke mulige svakheter som kunne utnyttes til å gjennomføre et innbrudd.

13. januar ble det meldt at saken hadde utviklet seg. Samme dag besluttet Helsedirektøren å varsle relevante aktører og innkalle til møte i Helsedirektoratets kriseutvalg 14. januar. Senere samme dag

fikk Helsedirektoratet formelt i oppdrag fra Helse- og omsorgsdepartementet å koordinere håndteringen av hendelsen. Følgende aktører ble innkalt til Helsedirektoratets kriseutvalgsmøter; Direktoratet for e-Helse, Norsk Helsenett og Helse Sør-Øst med Sykehuspartner HF. På grunn av manglende kommunikasjonskanaler for Begrenset informasjon (iht. sikkerhetsloven) var det behov for fysiske møter.

Nasjonal sikkerhetsmyndighet støttet Helse Sør-Øst og Sykehuspartner med kompetanse og ressurser, og koordinerte innsatsen med Politiets sikkerhetstjeneste, KRIPOS og E-tjenesten. Tiltak for å redusere angrepsflaten og øke deteksjonsevnen ble iverksatt. Et viktig tiltak i håndteringen for strategisk ledelse var å be Direktoratet for e-helse, sammen med andre eksperter, utarbeide scenarier med tilhørende tiltaksplan.

Forholdet ble politianmeldt og Politiets sikkerhetstjeneste iverksatte etterforskning av angrepet. Siste møte i Helsedirektoratets kriseutvalg ble avholdt 12. februar og 16. februar ble Helsedirektoratets koordineringsfullmakt trukket tilbake.

Det er per nå ikke noe som tyder på at innbruddet har hatt direkte konsekvenser for pasientbehandling, pasientsikkerhet eller at pasientdata har kommet på avveie.

WannaCry og NotPetya

WannaCry er et løsepengevirus som krypterer ned alt innholdet på infisert PC. For å spre seg benyttet WannaCry seg av en kjent Windows-sårbarhet igjennom verktøyet "EternalBlue".

EternalBlue ble mest sannsynlig utviklet av det amerikanske sikkerhetsbyrået (NSA), for å kunne infiltrere nettverk på vegene av den amerikanske stat, men EnternalBlue ble stjålet fra NSA sammen med en rekke andre verktøy og sårbarheter av en hackergruppe som kaller seg "The Shadow Brokers".

NotPetya, som er et tilsvarende løsepengevirus, benyttet seg også blant annet av EternalBlue som en spredningsmekanisme.

4.2.2 WannaCry løsepengevirus i NHS England

Fredag 12. mai 2017 startet spredningen av løsepengeviruset WannaCry og innen en dag rapporterte Europol at mer enn 230 000 PC-er i minst 150 land var blitt infisert. Majoriteten av de infiserte PC-ene dukket opp i Russland og Ukraina, men også store selskaper i Europa, Asia og USA ble rammet.

I England ble den offentlige helsetjenesten (NHS) rammet særskilt. Angrepet førte til forstyrrelser i en tredjedel av sykehusforetakene i England. Data fra NHS viser at minst 80 av 236 foretak ble påvirket. 34 av disse var infisert og låst ute av PC-ene (hvorav 27 var sykehus), og 46 var ikke direkte infiserte, men rapporterte forstyrrelser. Videre ble 603 virksomheter i primærhelsetjenesten og andre NHS-organisasjoner infisert av WannaCry, inkludert 8% av fastlegene (595 av totalt 7454).

Selv om WannaCry ikke var rettet spesielt mot NHS, belyste WannaCry en rekke sårbarheter hos NHS. Noen kritiske medisinske enheter/utstyr bruker fortsatt Microsoft XP-programvare levert av tredjeparter og ble berørt av WannaCry. Eksempler på dette er MR-skannere og blodprøveanalyseapparater. Dette innebar at til tross for at utstyret fungerte normalt, var programvaren som brukes til for eksempel å se røntgenbilder eller få tilgang til blodprøveresultater, i noen tilfeller utilgjengelig fordi den var på en infisert PC eller en som var i karantene.

Skjermbilde av en PC infisert med WannaCry.

Merck/MSD

Merck, nå MSD, er et globalt forskningsbasert legemiddelfirma med ca. 69 000 ansatte. Selskapet hadde en omsetning på 42,3 milliarder dollar i 2018.

4.2.3 Petya/NotPetya

I juni 2017 ble det kjent at Merck og mange andre bedrifter ble rammet av et massivt løsepengevirusangrep som til slutt endte med å påvirke organisasjoner over hele verden.

Løsepengeviruset som fikk navn Petya/NotPetya, hadde rammet hele organisasjonen til Merck og spesielt fabrikkene og deres evne til å produsere legemidler. Det tok Merck over seks måneder før de kunne gjenoppta full drift og det økonomiske tapet ble estimert til rundt 870 millioner dollar.

Merck og de andre internasjonale organisasjonene som ble rammet, var mest sannsynlig ikke målet i dette angrepet. Mye peker på at Petya/NotPetya var et virus primært rettet mot Ukrainsk infrastruktur som et ledd i konflikten mellom Ukraina og Russland som har eskalert siden Russlands okkupasjon av Krim-halvøya i 2014.

En hackergruppe som har fått navnet "Sandworm" og som har klare knytninger mot russisk militær og myndigheter, hacket oppdateringsservere til skatteprogramvaren M.E.Doc som alle bedrifter i Ukraina må benytte for innrapportering av skatt. Da bedriftene i Ukraina oppdaterte skatteprogramvaren sin, fulgte viruset med og infiserte nettverkene til bedriftene. Angrepet rammet Ukraina hardt og etter kort tid hadde viruset spredd seg til sykehus, flyplasser, strømleverandører og en rekke banker. Totalt ble over 300 bedrifter i Ukraina rammet og 10% av alle landets PCer ble infisert.

For å spre seg videre i nettverket benyttet også Petya/NotPetya "EternalBlue" og andre kjente sårbarheter som en spredningsmekanisme. Hadde bedriftene oppdatert sine systemer etter WannaCry-hendelsen, ville spredningen og konsekvensene potensielt sett blitt mye mindre.

4.2.4 Angrep mot SingHealth

Den 10. januar 2019 publiserte myndighetene i Singapore en rapport om et større angrep mot deres sentrale helsesystemer.

Mellom 23. august 2017 og 20. juli 2018 ble et sofistikert cyberangrep utført på pasientdatabasen til Singapore Health Services Private Limited ("SingHealth"). Pasientdatabasen ble ulovlig aksessert, og personlige opplysninger om nesten 1,5 millioner pasienter ble hentet ut i perioden 27. juni 2018 til 4. juli 2018. For omtrent 159 000 av disse 1,5 millioner pasientene innebar dette også at deres medisinoversikt ble hentet ut og stjålet. Statsministerens medisininformasjon ble spesifikt oppsøkt og aksessert gjentatte ganger.

Angriperne oppnådde tilgang til SingHealths IT-nettverk august 2017, og infiserte mest sannsynlig PC-er gjennom phishing-angrep. Angriperne lå deretter i hvilemodus i flere måneder, før de begynte å bevege seg innover i nettverket mellom desember 2017 og juni 2018, hvor de kompromitterte en rekke PC-er og servere. Underveis kompromitterte angriperne et stort antall bruker- og administratorkontoer, inkludert domeneadministratorkontoer.

Phishing-angrep

Phishing, på norsk også kalt nettfiske, er en betegnelse på «fisking» etter sensitiv informasjon, som passord eller kredittkortnummer. Ved phishingangrep kontaktes offeret som regel via en e-post, hvor avsenderen fremstår som en reell virksomhet. Offeret lures videre til å åpne et vedlegg eller klikke seg inn på en falsk nettside for å "logge seg inn", eller oppgi annen sensitiv informasjon, som konto- eller kredittkortnummer.

Spear phishing (spydfiske) er en selektiv, avansert og sofistikerte form for phishing. Den retter seg ofte mot bedrifter. Angriperen samler inn informasjon på forhånd, for eksempel om kunde, leverandør, avtaler og samarbeidspartnere. Denne informasjonen brukes så til å bygge kredibilitet i en e-post, ved å referere til interne ting og navn som er kjent for mottageren.

5 Identifiserte risikoer og sårbarheter

Økt digitalisering, flere sammenkoblede systemer og sentralisering introduserer nye gevinster, men også nye sårbarheter. Det har vært skrevet mange utredninger og rapporter som tar for seg IKT-sikkerhet de seneste årene. Lysne-utvalgets NOU 2015:13 "Digital sårbarhet – sikkert samfunn" var en grundig utredning av digitaliseringens påvirkning på samfunnet og hvordan digitaliseringen har innført nye risikoer og sårbarheter. Noe som ble spesielt påpekt var utfordringen med uoversiktlige digitale verdikjeder som kritiske samfunnsfunksjoner er blitt avhengige av. Utvalget beskriver effekten av den digitale utviklingen slik:

> *"En effekt av den digitale utviklingen er en kraftig endring i samfunnets risiko- og sårbarhetsbilde. Vi opplever nye trusler, som for eksempel at maskiner og infrastruktur i Norge kan angripes av anonyme aktører som befinner seg i andre land. Vi har fått nye sårbarheter å forholde oss til, som at programmeringsfeil i én komponent kan få effekter som slår ut store deler av mobilnettet. Samfunnsfunksjonene våre er – gjennom digitale verdikjeder – utsatt for hendelser på nye og tidligere ukjente måter. For eksempel kan svikt i telekommunikasjonsnettene føre til at veitunneler må stenges og at leger ikke får tilgang til pasientjournaler."*

5.1 Tverrsektorielle risikoer og sårbarheter

5.1.1 IKT-sikkerhetskompetanse

Mangel på IKT-sikkerhetskompetanse fremstår som en av de største utfordringene på IKT-sikkerhetsområdet, og mye tyder på at mangelen er økende i fremtiden. I en rapport fra Nordisk institutt for studier av innovasjon, forskning og utdanning (NIFU), laget på oppdrag fra Justis- og beredskapsdepartementet, konkluderte NIFU med at det i 2030 vil være en estimert etterspørsel på 15 000 personer med IKT-sikkerhetskompetanse, mens tilgangen samme år vil være på knapt 11 000. De samme trendene ser man også globalt. I Global Information Security Workforce Study av Frost & Sullivan, slår forfatterne fast at det i 2022 på verdensbasis vil være et underskudd på 1 800 000 personer med IKT-sikkerhetskompetanse.

For å adressere denne utfordringen, kunngjorde regjeringen i januar 2019 Nasjonal strategi for digital sikkerhetskompetanse. Strategien beskriver en rekke ulike tiltak knyttet til blant annet forskning, spesialistkompetanse, digital sikkerhet som del av IKT-relatert utdanning, etter- og videreutdanning, samt bevisstgjøring og sikkerhetskultur. Tiltakene vil over tid kunne imøtekomme den store sårbarheten og de uante ringvirkningene det vil ha, at samfunnet totalt sett er i underskudd på IKT-sikkerhetskompetanse.

Undersøkelser fra Nasjonal sikkerhetsmyndighet (NSM) viser at mange virksomheter har betydelige forbedringsbehov knyttet til sikkerhetsbevissthet og sikkerhetskompetanse. I følge NSM er det mange eksempler på styrer og ledere som tar store, strategiske avgjørelser uten å kjenne til virksomhetens digitale sikkerhetstilstand. Slike feilgrep fører ofte til store og kostbare opprydningsjobber, og de bunner i mange tilfeller i manglende kunnskap og forståelse hos

toppledelsen, så vel som hos fagpersonell. Det er derfor essensielt å komme opp med tiltak som kan sikre god kompetanseheving i flere ledd av virksomheten, med spesielt fokus på toppledelsen.

5.1.2 Lange, komplekse og uoversiktlige verdikjeder

Lysneutvalget påpekte i sin utredning at "en spesielt viktig observasjon er at kritiske samfunnsfunksjoner er blitt avhengige av lange og uoversiktlige digitale verdikjeder, som gjerne spenner over mange sektorer og flere land." Dette forsterkes ytterligere i helse- og omsorgssektoren av et komplekst aktørbilde der ansvaret for de ulike løsningene, produktene og verdikjedene er delvis fragmentert og noe uoversiktlig.

Ansvaret for drift og forvaltning er plassert hos ulike driftsleverandører både på kommunalt nivå, i spesialisthelsetjenesten og i den sentrale helseforvaltningen, samt hos private virksomheter og leverandører. Dette gjør det utfordrende å skaffe en dekkende detaljert oversikt over IKT i helsesektoren, samt sikre effektiv hendelseshåndtering og god styring av risiko og sårbarhet for de ulike nivåene i sektoren.

Direktoratet for samfunnssikkerhet og beredskap ga i 2018 ut "Risikoanalyse av legemiddelmangel" som en del av sine "Krisescenarioer" hvor de beskriver kompleksiteten rundt legemiddelforsyningen og sårbarheter knyttet til dette. En av sårbarhetene de peker på er svikt i IKT-systemer. Litt av denne kompleksiteten beskrives ved å se på hvilke ulike deler av verdikjeden som kan rammes av IKT-svikt:

- IKT-svikt i apotekenes systemer eller sykehusenes elektroniske kurveløsninger
- IKT-svikt hos legemiddelgrossistene slik at de ikke kan ta imot ordre fra apotek og/eller plukke ordre og levere varer til apotek og sykehus.
- IKT-svikt hos internasjonale transportører som gjør at de ikke får håndtert varestrømmen og legemiddelgrossistene får ikke levert varer.
- IKT-svikt i leverandørenes logistikkløsninger. Når de ikke lenger kan forsyne grossistene med varer vil lagrene i Norge fort gå tomme.
- IKT-svikt knyttet til den europeiske databasen som skal verifisere at legemidlene som utleveres i apotekene ikke er falske (EUs "forfalskningsdirektiv").
- IKT-svikt i leverandørenes produksjonssystemer som gir redusert tilgang på varer på lang sikt.
- IKT-svikt i Norsk Helsenett.

5.1.3 Avhengigheter

Med et digitalisert samfunn følger også sterke gjensidige avhengigheter mellom en rekke sentrale systemer og infrastruktur. Eksempelvis er mange digitaliserte tjenestekjeder lagt opp slik at data i ett system, automatisk plukkes opp av andre systemer og spres raskt til andre systemer som benytter samme informasjon. Dette er en av de største gevinstene med digitaliseringen, og sørger for en mer effektiv forvaltning. Samtidig er dette en sentral sårbarhet og stiller store krav til god informasjonssikkerhet. Dette fordi man i større grad får utfordringer med å ha kontroll over hvordan data benyttes, og å sikre at samvirket mellom aktørene fungerer godt (f.eks. at hver enkelt aktør kjenner til hvem som har ansvar for hva). Dersom det oppstår feil i en del av verdikjeden (f.eks. at data blir feilaktig endret, korrupt, eller et virus sprer seg fra en liten aktør), kan konsekvensene bli

svært store, og kreve et omfattende arbeid som involverer mange aktører for å få oversikt og ryddet opp slik at feil blir rettet i alle systemer.

Avhengighetene i helsesektoren gjør seg også særlig gjeldende med tanke på elektronisk kommunikasjon, energi og vannforsyning. Disse funksjonene er i økende grad avhengige av digitaliserte prosesser. Eksempel på slike avhengigheter kan være digitale kjølesystemer og ventilasjonssystemer og andre byggetekniske systemer som er viktige for drift av sykehus. Ved bortfall av IKT vil det derfor ofte være store dominoeffekter og tap av andre funksjoner som følge av en gitt hendelse.

Det er altså essensielt å ivareta sikkerhet gjennom lange, komplekse tjenestekjeder, i tillegg til i det enkelte system. Arbeidet med å kartlegge og følge opp avhengigheter er utfordrende og ressurskrevende, og krever systematisk og målrettet sikkerhetsarbeid i samarbeid med relevante aktører.

5.1.4 Mangelfull implementering av tekniske sikkerhetstiltak

Funn fra hendelser og tilsyn viser at mangelfull implementering av tekniske sikkerhetstiltak er en av de største sårbarhetene og den som oftest blir utnyttet. Nasjonal Sikkerhetsmyndighet (NSM) gir ut Grunnprinsipper for IKT-sikkerhet, som nå er i versjon 1.1, og har som en del av dette fremhevet 4 effektive tiltak mot dataangrep. Tiltakene er: oppgradering av program og maskinvare, installere sikkerhetsoppdateringer så fort som mulig, ikke tildele sluttbrukere administratorrettigheter og blokkering av ikke godkjente programmer. I følge NSM vil disse tiltakene stoppe opp mot 90 prosent av dataangrep. Likevel ser man ofte ved hendelser at det er mangelfull implementering av disse tekniske sikkerhetstiltakene, noe som gjør virksomhetene sårbare mot nye, men også gamle angrep og virus. Implementering og kunnskap rundt nødvendige sikkerhetstiltak må prioriteres i hele virksomheten, da en angriper kun trenger én sårbar pc eller server for å komme seg inn på nettverket.

5.2 Forhold spesielt for helse- og omsorgssektoren

Oppgavene, strukturen og organiseringen av helse- og omsorgssektoren medvirker til at sikkerhetsarbeidet er ekstra krevende. Flere virksomheter i sektoren har komplekse og gamle løsninger, med avhengigheter til andre løsninger igjen. Samtidig består sektoren for en stor del av små virksomheter, med begrenset kapasitet, ressurser og kompetanse til å ivareta andre fagområder enn kjernevirksomheten.

5.2.1 Gammelt utstyr/programvare som ikke kan oppdateres

Helse- og omsorgssektoren har et komplekst miljø med mange tilkoblede systemer og man finner til dels gammelt og utdatert utstyr. Årsakene til dette er blant annet manglende IKT-investeringer og legacy/teknisk arv med avhengigheter til eldre IKT-løsninger.

En del kritisk medisinsk utstyr benytter fortsatt Microsoft XP-programvare. Medisinsk utstyr er ofte dyrt utstyr av eldre årgang som krever avhengigheter til eldre IKT-løsninger og i mange av tilfellene

vil det være vanskelig/umulig å innføre sikkerhetsoppdateringer. I noen tilfeller vil oppdateringene kunne medføre at de eldre løsningene slutter å fungere, og andre tilfeller supporteres ikke programvaren lenger, som f.eks. Microsoft XP, og vil derfor ikke motta sikkerhetsoppdateringer.

Det vil også være utfordrende å holde et oppdatert sikkerhetsnivå på programvaren i store miljøer. Oppdateringer må potensielt bli testet opp mot hundre til tusen ulike applikasjoner (som man finner i de største miljøene) for å verifisere og sikre rett funksjonalitet. Etter WannaCry-hendelsen som rammet offentlig helsetjeneste (NHS) i England mai 2017, rapporterte NHS at majoriteten av infiserte PC-er benyttet seg av supportert programvare i form av Windows 7, men at disse PC-ene ikke var blitt oppdatert, noe som hadde forhindret dette angrepet. Det var kun en minoritet av de rammede PC-ene som kjørte usupportert programvare i form av Windows XP.

Manglende oppdateringer medfører derfor at deler av helsesektoren blir utsatt for kjente sårbarheter som enkelt kan utnyttes.

5.2.2 Fragmentert myndighetsutøvelse

Som beskrevet i kap. 3 Aktørbilde, er helse- og omsorgssektoren en kompleks sektor, der myndighetsutøvelsen er spredd mellom ulike forvaltningsnivåer.

Helsedirektoratet skriver i sin rapport "Risiko- og sårbarhetsvurderinger i helse- og omsorgssektoren" fra 2017 at sektorens myndighetsfunksjoner innen IKT heller ikke er helt samlet, og at det er usikkert om rollefordelingen på myndighetsnivå er slik at den minimerer risiko og sikrer god krisehåndtering. Dette var også et funn i rapporten fra Helse Sør-Øst-hendelsen i 2018.

Helsesektoren har fokusert på å gå opp disse problemstillingene på nasjonalt plan de seneste årene, særlig som en del av planleggingsarbeidet i forkant av større øvelser og gjennom å implementere ny Nasjonal helseberedskapsplan, men stadige omorganiseringer og flytting av ansvarsområder mellom aktører, understreker at dette er et kontinuerlig arbeid som krever fokus.

En fragmentert myndighetsutøvelse mellom forvaltningsnivåene er en utfordring både under hendelser og i det daglige. At sektorens aktører har et selvstendig myndighetsansvar for IKT-sikkerhet har sine fordeler, men det innebærer også at nasjonale aktører har få eller ikke tilstrekkelig effektive virkemidler for å sørge for at IKT-sikkerheten på regionalt og lokalt er på et minimumsnivå, eller at man kan gjennomføre effektive tiltak under store, komplekse hendelser med tidspress, f.eks. et virus som spres raskt i helsesektoren.

5.2.3 Mangelfull etterlevelse av styringssystem for informasjonssikkerhet

Mørketallsundersøkelsen utgis av Næringslivets Sikkerhetsråd. Undersøkelsen baserer seg på intervjudata, gjennomført blant både private og offentlige virksomheter med 5 ansatte eller flere. Rapporten fra 2018 bygger på resultater fra 1500 telefonintervjuer. Funnene kan tyde på at manglende etterlevelse av styringssystem for informasjonssikkerhet henger sammen med forekomsten og håndteringen av sikkerhetsbrudd i virksomheten.

Undersøkelsen viser at en høy prosentandel innen offentlige virksomheter har et rammeverk eller styringssystem for informasjonssikkerhet. Av de som rapporterer at de har rammeverk for sikkerhetssystemer oppgir 82 prosent (offentlig administrasjon) til 88 prosent (helse) av offentlige virksomheter at disse rutinene etterleves.

22 prosent av offentlige helsevirksomheter rapporterer at sikkerhetsbrudd skjer grunnet manglende prioritering av sikkerhetsarbeid. En annen årsak til sikkerhetsbrudd som rapporteres blant de som har rammeverk for informasjonssikkerhet er utilstrekkelige prosesser. Innen offentlig administrasjon sier 25 prosent av respondentene at manglende sikkerhetsprosesser førte til sikkerhetsbrudd. Enda flere respondenter, 40 prosent innen offentlig administrasjon, rapporterer at virksomheten har opplevd sikkerhetsbrudd grunnet manglende oppfølging av prosesser. I helsesektoren rapporterer 33 prosent det samme. Dette er svært interessante funn, med tanke på at svært mange rapporterer høy grad av etterlevelse av sikkerhetsrammeverk, samtidig som at manglende prosesser og rutiner blir oppgitt som en betydelig årsak til sikkerhetsbrudd.

Over en tredjedel av offentlige virksomheter rapporterer også at de oppdager sikkerhetsbrudd ved en tilfeldighet. Det er derfor grunn til å spørre seg hvor effektiv etterlevelsen av rammeverk for informasjonssikkerhet er i praksis, samt hvilken effekt mangel på eksisterende prosesser eller etterlevelse av rutiner har på sikkerhetsarbeidet.

5.3 Særskilte funn etter nylige hendelser og øvelser

5.3.1 Manglende planverk og trening i håndtering av IKT-hendelser

Innbruddet i Sykehuspartners datasystemer januar 2018 (nærmere beskrevet i kap. 4.2.1) er et tydelig eksempel på hvilke trusler vi står ovenfor, og hvordan disse truslene treffer oss i praksis. Som en følge av hendelsens alvorlighetsgrad delegerte HOD ansvaret for å koordinere helsesektorens innsats til Helsedirektoratet, i tråd med Nasjonal helseberedskapsplan. Hendelsen var en viktig test av helsesektorens evne til å håndtere IKT-hendelser av en slik kritikalitet og kompleksitet, og evalueringsrapporten belyste flere forbedringspunkter som må prioriteres i arbeidet videre.

Funnene i evalueringsrapporten er i stor grad knyttet til manglende erfaring, trening og planverk knyttet til IKT-hendelser. Eksempler på dette er at Nasjonal helseberedskapsplan ikke omtaler IKT-kriser spesielt, at det var uklarheter rundt roller og tilhørende ansvar i organiseringen av Kriseutvalget i Helsedirektoratet, at deltakerne opplevde manglende kompetanse i klassifisering og håndtering av gradert informasjon, og at samhandling om kommunikasjon ikke er tydelig avklart i IKT-kriser.

Mange av disse funnene gjenspeiler også den tverrsektorielle evalueringsrapporten etter sivil nasjonal øvelse i 2016, "IKT16", der helsesektoren øvde på et lignende scenario.

5.3.2 Utdatert og ikke oppdatert programvare

Sårbarheten som ble benyttet under WannaCry mai 2017 og NotPetya juni samme år, var en sårbarhet i Windows som Microsoft hadde gitt ut en sikkerhetsoppdatering til i mars 2017. Det vil si at hvis systemene hadde vært oppdatert med de siste sikkerhetsoppdateringene, ville ikke de nevnte

løsepengevirusene ha spredd seg slik de gjorde. Det er også et viktig og interessant funn at organisasjonene som ble truffet av NotPetya ikke hadde sikkerhetsoppdatert sine systemer etter at WannaCry ble kjent.

6 Tiltak etter hendelser og utredninger

Datagrunnlaget som er brukt i denne rapporten inneholder en rekke foreslåtte tiltak. Under følger en kort og overordnet oppsummering av sentrale tiltak som er foreslått etter ulike hendelser og i utredninger og rapporter.

6.1 Foreslåtte tiltak etter hendelser

I kjølvannet av omfattende IKT-hendelser i offentlige helsetjenester de siste årene, er det løftet frem viktige funn i evalueringsarbeidet, og det er foreslått en rekke tiltak for å unngå at lignende hendelser skjer igjen. I det følgende presenteres hovedtrekkene i foreslåtte tiltak fra WannaCry-hendelsen som rammet offentlig helsetjeneste (NHS) i England mai 2017, SingHealth-hendelsen i Singapore august 2017-juli 2018, samt Helse Sør-Øst-hendelsen januar 2018, da disse hendelsene vurderes som spesielt relevante og dermed viktige å ta lærdom av. Hendelsene er nærmere beskrevet i kap. 4.2. Selv om hendelsene varierer i omfang og natur, er det mange fellestrekk ved hva som har "gått galt", og tiltakene tar ofte sikte på å få på plass eller forbedre grunnleggende elementer.

Når det gjelder planverk og prosesser, er et viktig tiltak som går igjen at det må utarbeides spesialiserte planer for IKT-scenarier, da slikt planverk er mangelfullt i dag. Lokale planer må dessuten beskrive rutiner for hva som skjer ved bortfall av IKT-tjenester, og det er avgjørende at nødprosedyrer testes regelmessig. I tillegg er det påpekt som et nødvendig tiltak at planverk og prosesser må beskrive hvordan ekspertise med riktig kompetanse skal kalles inn og delta under hendelseshåndtering.

Et annet gjentakende tiltak er å øke øvingsvirksomhet, og å sikre deltakelse fra alle relevante parter. Øvingsbehovene handler både om å forbedre samhandling og øke rolleforståelse, men også evnen til å mestre tekniske verktøy (for eksempel for håndtering av gradert informasjon). I tillegg kommer det frem i samtlige evalueringsrapporter at spesielt cyberhendelser er et komplekst og ukjent domene for mange, noe som gjør at tematikken krever økt oppmerksomhet i fremtidige øvelser, og det bør øves på IKT-scenarier regelmessig.

Tekniske tiltak som foreslås handler ofte om å "fix the basics", med referanse til eksempelvis NSMs grunnprinsipper og HelseCERTs anbefalinger. Eksempler på slike tiltak er å etablere og vedlikeholde et strengt regime for administratorrettigheter, at domenekontroller må sikres og at organisasjoner må sørge for god forvaltning av regelmessige sårbarhets-/sikkerhetsoppdateringer. I England er det bestemt at det i 2019 skal nedsettes en arbeidsgruppe som skal definere standarder for styring og oppdatering av medisinsk utstyr. Et annet viktig tiltak som kan trekkes frem etter WannaCry-hendelsen, er at CareCERT (tilsvarende HelseCERT) bør få en mer fremtredende rolle i sektoren og sørge for å ha god oversikt over tilstanden i det tekniske landskapet på tvers av organisasjoner. På lengre sikt er det også et mål at NHS Digital skal ha evne til å isolere organisasjoner, deler av landet eller spesifikke tjenester med det formål å hindre spredning av et virus under en hendelse.

Det er også flere organisatoriske tiltak som gjentas. Risikovurderinger og revisjon må gjennomføres regelmessig og implementeres i den kontinuerlige styringen og forvaltningen. På ledernivå er det

også flere tiltak som påpekes som hensiktsmessige å innføre. F.eks. er det viktig at ledergrupper/styrer innehar sikkerhetskompetanse, helst ved at sikkerhetsleder er fast representant i leder/-styremøter. Rapporten etter WannaCry-hendelsen anbefaler at NHS etablerer en overordnet sikkerhetssjef med et bredt mandat og nedslagsfelt og at det dedikeres egne ressurser til å jobbe med nettverksikkerhet på tvers av helse regioner og nivåer.

Når det gjelder foreslåtte kompetansehevingstiltak, viser disse også at man bør gjennomføre øvelser. IKT-scenarioer er ukjent for mange, og ofte er det slik at ressurser som deltar i hendelseshåndtering (spesielt på strategisk nivå), ikke har IKT, sikkerhet og/eller beredskap som sitt daglige fagområde. Kompetanseheving og opplæring av nøkkelressurser (f.eks. ledelse) bør derfor være systematisk, målrettet og obligatorisk, og sikre at ressurser kjenner til relevant planverk, og forstår sin rolle og tilhørende ansvar i IKT-scenarier. I tillegg bør man gjennomføre regelmessige kompetansehevende tiltak for å sikre god sikkerhetskultur i organisasjonen.

6.2 Foreslåtte tiltak fra nasjonale utredninger og andre rapporter

Mange av de utfordringene sektoren møter på dette området er felles for alle samfunnssektorer. Tiltak som er beskrevet for å sette Norge i stand til å møte et endret trusselbilde vil også ha stor effekt for helse- og omsorgssektoren. Dette omfatter f.eks. tiltak i Nasjonal strategi for digital sikkerhet. Denne strategien understøttes av en to-delt tiltaksoversikt. Del 1 beskriver myndighetenes utvalgte sentrale tiltak for prioriterte områder. Del 2 beskriver ti grunnleggende tiltak for å øke virksomheters egenevne til å beskytte seg mot og håndtere digitale hendelser. Virksomheter i helse- og omsorgssektoren bør arbeide aktivt med disse tiltakene.

"NOU 2018:14 IKT-sikkerhet i alle ledd" beskriver også viktige tiltak, bl.a. tydeligere styring og bedre koordinering av nasjonal IKT-sikkerhet.

Lysneutvalget, NSM, HelseCERT, Helsedirektoratet og E-helse har alle pekt på opplæring og kompetanse som noen av de viktigste tiltakene. Det anbefales at kompetanseheving innen IKT-sikkerhet må gjennomføres spesielt på styre- og ledelsesnivå da det er her ansvaret for sikkerheten i organisasjonen ligger. Styre- og ledergruppen må ha et bevisst forhold til sikkerhet for å kunne styre risikoen og gjøre riktige beslutninger. Som en forlengelse av dette trekker man frem viktigheten av å ha et styringssystem for informasjonssikkerhet og sikre systematisk og kvalitativt godt arbeid med sikkerhetskultur i virksomhetene.

Øvelser innen IKT der man øver både på konsekvenser av bortfall av IKT-systemer samt krisehåndteringen, er et annet tiltak flere rapporter belyser. Øvelser er et viktig virkemiddel for å styrke og videreutvikle kompetanse og evne til å håndtere krisesituasjoner. Funn etter øvelsen vil kunne bli brukt til å gjøre planverk og prosesser endre bedre, slik at organisasjonene kan redusere negative konsekvenser av hendelser.

For de tekniske tiltakene er det "fix the basics" som gjentatte ganger anbefales (ref. HelseCERT sine 10 anbefalte tiltak, NSMs grunnprinsipper og Regjeringens 10 anbefalte tiltak for virksomheters egenevne i nasjonal strategi for digital sikkerhet).

Gjennom lovarbeid som er igangsatt foreslås det også bestemmelser og tiltak som vil innebære en styrking av IKT-sikkerheten i sektoren. Helsedirektoratets forslag til revidert helseberedskapslov

adresserer styrket IKT-beredskap. Videre vil gjennomføring av EUs direktiv om sikkerhet i nettverk og informasjonssystemer (NIS-direktivet) omfatte tilbydere av samfunnsviktige tjenester innenfor bl.a. helsesektoren. Virksomheter i vår sektor som kommer innenfor direktivets virkeområde vil i hovedsak få to forpliktelser: Å gjennomføre sikkerhetstiltak som står i et rimelig forhold til den risikoen virksomheten står overfor, og varsle om alvorlige IKT-sikkerhetshendelser. Lov om gjennomføring av NIS-direktivet i norsk rett har vært på høring med høringsfrist. 22.3.2019.

7 Forslag til nye tiltak

På bakgrunn av trusselbildet, funn fra hendelser og øvelser og allerede foreslåtte tiltak presentert i foregående kapitler, foreslås her 5 konkrete tiltak som effektivt vil kunne løfte sikkerhetsnivået i helse- og omsorgssektoren på kort- og mellomlang sikt. Det vil kreve ressurser, prioritering og lederforankring for å gjennomføre de anbefalte tiltakene på en tilfredsstillende måte. I tillegg til foreslåtte tiltak bør arbeid med ROS for IKT-området videreføres i henhold til tidligere anbefaling beskrevet i kapittel 1.2

Lysneutvalget stilte spørsmålstegn ved hvorfor ikke flere av tiltakene er fulgt opp, og om mengden utredninger i seg selv er til hinder for en effektiv iverksetting av tiltakene. Direktoratet for e-helse deler denne bekymringen, og ser at det er en trend at det listes opp et høyt antall tiltak, samtidig som prioriteringene uteblir. Det er også et stort behov for å plassere tydelig ansvar og fastsette en frist for hvert tiltak, for at reell forbedring skal kunne skje. En slik konkretisering gir også et bedre utgangspunkt for å få oversikt over hva som er gjennomført, og hvilke tiltak som gjenstår.

Med dette som grunnlag, anbefaler Direktoratet for e-helse at følgende 5 tiltak gjennomføres. Vi har foreslått hvem som bør være ansvarlig for hvert tiltak og angitt en frist som bør være realistisk gitt nødvendig prioritering og finansiering.

Tiltak 1: Utarbeidelse av nasjonal IKT-beredskapsplan for helse- og omsorgssektoren som en del av Nasjonal helseberedskapsplan

Ansvarlig: Helse- og omsorgsdepartementet som ansvarlig for Nasjonal helseberedskapsplan
Frist: Utkast bør være klart til å testes i den nasjonale øvelsen Digital 2020

- **Det bør utarbeides en nasjonal IKT-beredskapsplan for helse- og omsorgssektoren som en del av Nasjonal helseberedskapsplan**
- **Det bør utredes mulige tiltak for å kunne isolere virksomheter, deler av landet eller spesifikke tjenester i helsenettet med det formål å hindre spredning eller avverge ytterligere angrep mot IKT-infrastruktur under en hendelse**
- **Planen og eventuelle tiltak bør sees i sammenheng med Sivilt beredskapssystem for helse (SBS Helse)**

Tiltak 2: Gjennomføre årlig IKT-øvelse

Ansvarlig: Helsedirektoratet
Frist: Årlig fra og med 2020

- **Det bør årlig gjennomføres en øvelse på IKT-scenarier som får konsekvenser for helsesektoren, enten ved at IKT er et eget scenario eller at IKT inngår som en del av en større øvelse**
- **Øvelsen bør sees i sammenheng med Nasjonal helseøvelse som Helsedirektoratet er ansvarlig for og arrangeres i samarbeid med Direktoratet for e-helse, NHN og de regionale helseforetakene**

Tiltak 3: Styrket operativ IKT-sikkerhet i helse- og omsorgssektoren

Ansvarlig: Norsk helsenett SF
Frist: Løpende fra 2020

- **HelseCERT bør i kraft av sin rolle som helse- og omsorgssektorens nasjonale senter for informasjonssikkerhet gi ut årlige anbefalinger om basistiltak for økt operativ IKT-sikkerhet i helsesektoren.**
    - De foreslåtte tiltakene må være basert på funn av sårbarheter identifisert gjennom sårbarhetsskanning og inntrengningstesting, og være koblet mot anbefalinger fra andre sikkerhetsmyndigheter.
    - Inntrengningstesting er et effektivt virkemiddel for å oppdage sårbarheter i infrastrukturen i sektoren. Sektorens totale kapasitet for å gjennomføre slike tester regelmessig bør styrkes.
- **NHN bør spille inn til Direktoratet for e-helse forslag til tiltak som bør gjøres obligatoriske for sektoren.**
- **NHN bør kartlegge og informere om den generelle sikkerhetstilstanden i helse- og omsorgssektoren, herunder:**
    - Sikkerhetssamtaler bør gjennomføres som grunnlag for å si noe om den generelle sikkerhetstilstanden i helse- og omsorgssektoren
    - Sikkerhetstilstanden og trendene i helse- og omsorgssektoren bør dokumenteres i HelseCERTs årlige situasjonsbilde

Tiltak 4: Styrket myndighetsrolle for IKT-sikkerhet i helse- og omsorgssektoren

Ansvarlig: Direktoratet for e-helse
Frist: Løpende fra 2020

- **Direktoratet for e-helse bør styrke sin rolle som fagorgan for sektoren innen informasjonssikkerhet**

  - Direktoratet bør utrede og foreslå for Helse- og omsorgsdepartementet konkrete tiltak, herunder nye pålegg og forpliktelser til virksomhetene i sektoren, som kan redusere sårbarheter og bedre IKT-sikkerheten
  - Direktoratet bør bistå Helsetilsynet i å bygge opp kompetanse på IKTs betydning i helse- og omsorgssektoren slik at IKT inkluderes i deres tilsyn
- **Direktoratet for e-helse bør styrke arbeidet med opplæring og rådgivning knyttet til informasjonssikkerhet og personvern, herunder:**
  - Styrke arbeidet med Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten
  - Utvikle opplæring og kompetansehevingstiltak for beslutningstakere og ledergrupper i helse- og omsorgstjenesten
  - Tilrettelegge for innføring av styringssystem for informasjonssikkerhet gjennom opplæring og veiledere
- **Direktoratet for e-helse bør kartlegge og informere om den generelle sikkerhetstilstanden i helse- og omsorgssektoren, herunder:**
  - Fortsette arbeidet med å skaffe til veie kunnskapsgrunnlag om IKT-sårbarheter i helse- og omsorgssektoren og sektorens arbeid med informasjonssikkerhet og personvern, f.eks. gjennom videre arbeid med ROS-analyser i sektor se kapitel 1.2
  - Regelmessig gjennomføre innbyggerundersøkelser som måler innbyggernes tillit til sektorens evne til å ivareta informasjonssikkerhet og personvern.

Tiltak 5: Utarbeidelse av helhetlig IKT-sikkerhetsstrategi for helse- og omsorgssektoren

Ansvarlig: Direktoratet for e-helse i samarbeid med sektor og kompetansemiljøer
Frist: 2021

- **Det bør utarbeides en helhetlig IKT-sikkerhetsstrategi for helse- og omsorgssektoren. IKT-sikkerhetsstrategien bør ses opp mot nasjonal strategi for IKT-sikkerhet og ta høyde for sektorspesifikke utfordringer og utvikling av dagens helsetjeneste, herunder:**
  - Hvordan bør arbeidet med IKT-sikkerhet i helse- og omsorgssektoren organiseres og drives for å imøtekomme dagens og morgendagens utfordringer og trusselbilde?
  - Hvordan bør man arbeide for å ivareta IKT-sikkerhet i den nye pasienthverdagen med velferdsteknologi, Internet of Things (IoT) og fremtidens teknologi?
  - Hvordan bør helse- og omsorgssektoren samarbeide med øvrige kompetansemiljø og private leverandører for å sikre hele tjenestekjeden for små og store aktører?
  - Hvordan bør helse- og omsorgssektoren strategisk arbeide med kompetanseheving på IKT-sikkerhet?
  - Hvordan bør tilsyn knyttet til IKT-sikkerhet gjøres på en hensiktsmessig måte for å skape trygghet og tillit til IKT-systemene i helsetjenesten

8 Referanser

Dokumentasjonen som er valgt ut, er i hovedsak åpne kilder utgitt i tidsrommet 2015 til vinter 2019, med Lysneutvalgets NOU 2015: 13 som startpunkt.

Følgende publikasjoner er benytter:

- NOU 2015: 13 Digital sårbarhet – sikkert samfunn
- NOU 2016: 19 Samhandling for sikkerhet
- Meld. St. 27 (2015–2016) Digital agenda for Norge
- Meld. St. 38 (2016-2017) IKT-sikkerhet – et felles ansvar
- Meld. St. 10 (2016-2017) Risiko i et trygt samfunn
- Risikoanalyse av "Cyberangrep mot ekom-infrastruktur", Direktoratet for samfunnssikkerhet og beredskap (2015)
- Overordnede risiko- og sårbarhetsvurderinger i helse- og omsorgssektoren, Helsedirektoratet (2017)
- Prop. 153 L (2016-2017) Lov om nasjonal sikkerhet (sikkerhetsloven)
- IKT-organisering i helse- og omsorgssektoren, Direktoratet for e-helse (2017)
- Informasjonssikkerhet ved bruk av private leverandører i helse- og omsorgstjenesten, Direktoratet for e-helse (2017)
- Tverrsektoriell evalueringsrapport fra øvelse IKT16, Direktoratet for samfunnssikkerhet og beredskap (2017) (unntatt offentlighet)
- NOU 2018: 14 IKT-sikkerhet i alle ledd
- Lessons learned review of the WannaCry Ransomware Cyber Attack, NHS England (2018)
- Mørketallsundersøkelsen 2018, Næringslivets sikkerhetsråd
- Nasjonal strategi for digital sikkerhet, Departementene (2019)
- Trusselvurdering 2019, Politiets sikkerhetstjeneste
- Fokus 2019, Forsvaret
- IKT-risikobilde 2019, Nasjonal sikkerhetsmyndighet
- IKT-risikobilde 2018, Nasjonal sikkerhetsmyndighet
- Rammeverk for håndtering av IKT-sikkerhetshendelser, Nasjonal sikkerhetsmyndighet
- Situasjonsbilde 2018, HelseCERT
- IKT-sikkerhetskompetanse i arbeidslivet – behov og tilbud, Nordisk institutt for studier av innovasjon, forskning og utdanning (2017)
- Utviklingstrekk 2019, Direktoratet for e-helse

I tillegg til datagrunnlaget som er listet ovenfor, er det brukt følgende kilder i arbeidet med rapporten:

1. Center for Cyber Safety and Education: 2017 Global Information Security Workforce Study Benchmarking Workforce Capacity and Response to Cyber Risk, Frost & Sullivan Executive Briefing (2017). https://iamcybersafe.org/wp-content/uploads/2017/06/europe-gisws-report.pdf

2. Trend Micro: Why hackers are increasingly targeting electronic health records https://blog.trendmicro.com/why-hackers-are-increasingly-targeting-electronic-health-records/

3. Financial Times: Cyber security: Attack of the health hackers https://www.ft.com/content/f3cbda3e-a027-11e5-8613-08e211ea5317

4. FiercePharma: Merck has hardened its defenses against cyberattacks like the one last year that cost it nearly $1B https://www.fiercepharma.com/manufacturing/merck-has-hardened-its-defenses-against-cyber-attacks-like-one-last-year-cost-it

Vedlegg 1. Tiltak fra rapporter og utredninger

NOU 2015: 13 Digital sårbarhet – sikkert samfunn

Problembeskrivelse (NOU 2015: 13, punkt 17.7.1)
Flere aktører etterlyser en sterkere styring av IKT-sikkerhet fra Helse- og omsorgsdepartementet. Utvalget stiller spørsmål ved hvorfor styringsmuligheten som departementet har til å samkjøre mellom de regionale helseforetakene, ikke benyttes i større utstrekning. Utvalget mener det er behov for sterkere nasjonal styring for å identifisere og oppfylle felles behov og for å unngå divergerende løsninger i regionene. Utvalget har gjennom sitt arbeid registrert at det er publisert en stor mengde utredninger de siste årene som omhandler IKT i helsesektoren. Flere av disse ser ut til å beskrive dagens utfordringer på en god måte, og det synes å være stor bevissthet i sektoren om hvilke forbedringstiltak som er nødvendige. Utvalget stiller spørsmål ved hvorfor ikke flere av tiltakene er fulgt opp, og om mengden utredninger i seg selv er til hinder for en effektiv iverksetting av tiltakene. Utvalget mener at det er viktig med en tydeligere prioritering av forebyggende tiltak for å redusere de identifiserte sårbarhetene, og at det må sikres gjennomføringskraft for disse. Som en del av dette foreslår utvalget at det nye Direktoratet for e-helse utarbeider en årlig statusrapport om tilstanden for IKT-sikkerhet i helsesektoren. Utvalget mener det bør vurderes forenklinger i Norm for informasjonssikkerhet i helse- og omsorgstjenesten (Normen) for de minste helseforetakene i den grad det er mulig uten at det bidrar til å øke sårbarheten.

Problembeskrivelse (NOU 2015: 13, punkt 17.7.4)
Det er behov for beredskap ved bortfall av kritiske IKT-tjenester som skyldes tilsiktede eller utilsiktede hendelser. Mindre grad av manuelle rutiner å falle tilbake på kan i fremtiden gi nye og økte sårbarheter. Utvalget mener det bør gjennomføres flere IKT-øvelser der kritiske systemer er ute av funksjon.

Tiltak i nasjonal strategi for digital sikkerhet
Nasjonal strategi for digital sikkerhet ble lansert av regjeringen i januar 2019. I strategien utpekes det mål for fem prioriterte områder. Strategien understøttes av en tiltaksoversikt, hvor del 1 beskriver utvalgte sentrale tiltak som støtter opp under strategien, og del 2 lister ti grunnleggende tiltak som virksomheter i offentlig og privat sektor anbefales å gjennomføre. Det enkelte departement er ansvarlig for at strategiens prioriteringer og tiltaksoversikten blir fulgt opp innenfor sin sektor.

Tiltakene favner et bredt spekter, med forebyggende digital sikkerhet, kompetanse, kritiske samfunnsfunksjoner, evne til å avdekke og håndtere angrep og IKT-kriminalitet som prioriterte områder.

Direktoratet for e-helses rapport "Informasjonssikkerhet ved bruk av private leverandører i helse- og omsorgssektoren" fra 2017

Kompetanseheving
Kompetanse innen IKT-sikkerhet og risikovurdering på styre- og ledelsesnivå må heves. Det bør vurderes om Norsk Helsenett i samarbeid med Direktoratet for e-helse, som sektorens kompetansesentre for informasjonssikkerhet, kan lede oppgavene med å:

• Etablere et forum for beste praksis i bransjen for kompetanseheving og sikkerhetskultur.

• Utvikle felles plan for å sikre at opplæringstilbud til ledere og ansvarlige beslutningstakere innen sikkerhetskompetanse er på adekvat nivå.

HelseCERT situasjonsbilde 2018

- **Sikkerhetskultur**: Jobb med å bygge en god sikkerhetskultur i virksomheten. Gjennomfør opplæring og bevisstgjør ansatte.
- **Passord**: Etabler en god passordpolicy og gi opplæring i hvordan å lage gode passord. Unngå gjenbruk.
- **Oppdatering**: Oppgrader program- og maskinvare for å ta i bruk ny sikkerhetsfunksjonalitet og lukke sikkerhetshull.
- **Administratorkontoer**: Beskytt administratorkontoer. Unngå at brukere har administratorrettigheter. Bruk LAPS for lokal admin.
- **To-faktor**: Innfør to-faktor-autentisering for tjenester tilgjengelig på internett for å hindre misbruk av kompromitterte eller dårlige passord.
- **Applikasjonshvitelisting**: Applikasjonshvitelisting vil hindre kjøring av uautorisert programvare. Benytt klientbrannmur for å unngå intern spredning.
- **DMARC**: Beskytt e-post-domener med DMARC, som blokkerer uautorisert e-post og hindrer misbruk av domene.
- **Segmentering**: Segmenter nettverket ditt, ikke glem servere.
- **Sårbarhetsskanning**: Gjennomfør sårbarhetsskanning for å oppdage sårbare maskiner i eget nettverk.

Helsedirektoratets overordnede risiko- og sårbarhetsvurderinger i helse- og omsorgssektoren fra 2017

Ansvar for gjennomføring vil ligge på den enkelte virksomhet og i hele styringslinjen.

- Fortsette etablering og videreutviklinger av arenaer for samordning og samvirke. Det har vært en positiv endring på dette området de siste årene og flere tiltak fra departementet, bl.a. opprettelsen av Direktoratet for e-helse og utviklingen av NHN med HelseCERT.
- Tilrettelegge for innføring av styringssystem for informasjonssikkerhet med fokus på Normen (Norm for informasjonssikkerhet i helse og omsorgstjenesten). Normen, som er basert på «beste praksis», er utviklet og vedlikeholdes av sektoren selv. Virksomheter som knytter seg til Norsk Helsenett er forpliktet til å oppfylle kravene i Normen gjennom et styringssystem. Normen utgjør i seg selv et komplett styringssystem med tilhørende maler og veiledere. Blir dette etterlevd, vil den samlede risikoen i sektoren bli vesentlig redusert. Det må avsettes tilstrekkelig med ressurser for dette arbeidet. Videre bør det settes fokus på å revidere etterlevelse.
- Fortsette arbeidet med å inkludere sikkerhet og personvern i eksisterende modeller og rammeverk. I det offentlige finnes det pr. i dag et antall maler, metoder og rammeverk virksomhetene oppfordres til å benytte. Mye av dette arbeidet er ledet av DIFI. Det er fremdeles et stort potensial ved å få inkludert sikkerhet- og personvernsaktiviteter inn i de enkelte rammeverk, som f.eks. prosjektmodellen.
- Tilgang på andre virksomheters problemstillinger og ROS-analyser. Det er et behov i sektoren for standardisering og gjenbruk. Det ville vært ressursbesparende å få tilgang på andres scenarioer, risikoområder, forslag til tiltak, osv.
- Øke frekvensen på nasjonale IKT-øvelser. Øvelsen IKT-16 viste nytten og nødvendigheten av øvelser på nasjonalt nivå. Det er nye krav til situasjonsforståelse («digital modenhet»), samhandling og koordinering.
- Bygge en bedre sikkerhetskultur. En god sikkerhetskultur kjennetegnes ved at de ansatte er oppmerksomme på problemstillinger knyttet til informasjonssikkerhet og personvern, har tilstrekkelig kompetanse om det aktuelle trusselbildet og omgivelsene (teknologi, trusselaktører, etc.), kjenner sin egen rolle og er klar over hvordan virksomhetens styringssystem og rutiner fungerer. Nasjonal Sikkerhetsmyndighet (NSM) gjør et utmerket opplysende/holdningsskapende arbeid på dette området, og bør i størst mulig grad benyttes.
- Videreutvikle NHN og HelseCERT. NHNs rolle som tjeneste- og driftsleverandør på nettverk og sikkerhetstjenester bidrar til å minske risiko for hendelser i sektoren.
- Avklare skjermingsverdige objekter. Det er viktig at overordnet myndighet avklarer hva av e-helseløsninger og infrastruktur som eventuelt er skjermingsverdige objekter etter sikkerhetsloven, eksempelvis i Nødnett Helse. Dette kan endre seg etter hvert som systemene utvikles.
- Ansvarsavklaring innen krisehåndtering. Under IKT-kriser har det vist seg å være uklart for aktørene hvor ansvaret for håndtering er plassert, hva som er rapporteringslinjene og rutinene for informasjonsflyt. Dette må gås opp og øves.

Vedlegg 2. Tiltak etter hendelser

Datainnbrudd hos Helse Sør-Øst

Beredskapsplaner

- Helsedirektoratet må, i samarbeid med Helse- og omsorgsdepartementet, vurdere behov for en spesialisert beredskapsdel som omhandler IKT-kriser i Helseberedskapsplanen.

Varslingsrutiner- og linjer

- Gå gjennom varslingslinjer, slik at alle relevante miljøer blir varslet, og at flyten i varslingen blir tydelig, f.eks. ved å bruke flytdiagram med spørsmål
- Sette opp IKT/helse-scenarier generelt, men også spesielt hvor tid er kritisk.
    - Hvordan kan man håndtere situasjonen raskt med operative ressurser?
    - Hvor lenge kan de arbeide før man må løfte beslutninger opp i Kriseutvalget?
- Øvelser der god varsling i overenstemmelse med planverket er et tydelig øvingsmål
- Gå gjennom varslingsrutiner (unntatt varslingslinjer som står i eget punkt), som: Hvilke systemer som kan brukes i hvilke situasjoner?

Organisering og krisehåndtering

- Helsedirektoratets beredskapsorganisasjon må kjenne til "Rammeverk for håndtering av IKT-sikkerhetshendelser". Rammeverket kom etter krisehåndteringen, men er relevant for bruk i fremtidige hendelser. Det vil sikre enhetlig begrepsbruk og felles koder for kategorisering av IKT-sikkerhetshendelser.
- Få på plass rutiner som støtter en i arbeidet med å systematisk få på plass et kraftfullt Kriseutvalg (eller Koordineringsmøte) tilpasset den situasjonen som er oppstått. Siden IKT-krise er en ny type krise for Helsedirektoratet, må dette hensynstas spesielt.
- Kommunisere forholdene som danner bakgrunnen for at Helsedirektoratet koordinerer hendelsen, slik at man får en omforent forståelse av dette.
- Være tydeligere på å forklare rollene til de som sitter i (er innkalt til) Kriseutvalget (eller Koordineringsmøtet).
- Beredskapsorganisasjonen må møtes regelmessig til øvelser.
- Tydeligere på at "nå er vi i en slik situasjon, så da er det disse reglene som gjelder" – f.eks. med hensyn til kommunikasjon, roller og forventninger til hver av deltakerne.
- Helsedirektoratet må, på et overordnet nivå, sette seg inn i utviklede IKT-scenarier som kan gi helsekonsekvenser, slik at disse gjenkjennes.
- Straks en delegasjon har funnet sted, må Helsedirektoratet sikre at scenarier blir oppdatert. Scenariene må inkludere verste-falls-scenarier for rapportering til Helse- og

omsorgsdepartementet, og aktører som Helsedirektoratet skal samordne og dele informasjon med.

- Diskutere om det er hensiktsmessig å lage retningslinjer for hvem som skal utvikle scenarier under en krise, slik at man unngår at kompetanse ikke blir brukt, eller at flere arbeider med samme scenariene uten å dra nytte av hverandre.
- Helsedirektoratets kriseutvalg bør på permanent basis ha tilgang på et operativt ekspertråd for informasjonssikkerhet og pasientsikkerhet knyttet til IKT-systemer". Direktoratet for E-helse vil utarbeide et forslag til mandat og sammensetting for et slikt operativt ekspertråd

Rapportering og informasjon

- Være tydelig under kommunikasjon på hva som er verdien av hver "informasjonsdel"
- Oppsummering til slutt i møter om hva som er åpen og hva som er gradert informasjon
- Lage retningslinjer for hvordan man oppbevarer og kommuniserer informasjon med ulik verdi (mellom aktører involvert i kriseberedskapen)
- Sørge for at alle potensielle deltakere i en beredskapssituasjon får opplæring i sikkerhetskultur, herunder verdivurdering av informasjon
- Øvelser rundt håndtering av informasjon med ulik verdi
- Gå gjennom rutiner for sikkerhetsklarering og autorisasjonssamtaler, slik at alle i beredskapsorganisasjonen er klarert for det nivå av informasjon (sannsynligvis nivå *hemmelig*) som det kan bli nødvendig å håndtere til enhver tid
- Alle aktørene bør ha tilgang til rom og kommunikasjons-/videokonferansesystemer for møter med deling av gradert informasjon.
- Utvikle rutiner for kommunikasjon og offentlig informasjon til publikum ved hendelser hvor sikkerhetsloven er relevant
- Bare nødvendige deltakere i møter hvor det kan komme til å bli delt gradert informasjon.

Kommunikasjon og mediehåndtering

- Fortsette arbeidet med strategier for kommunikasjonsberedskap
- Fortsette med gode diskusjoner i forkant av møter med pressen, slik det var i denne krisen
- Utvikle standardbudskap som kan være utgangspunkt for kommunikasjon ved ulike scenarier
- Avklare kommunikasjonsroller

SingHealth

- Recommendation #1:
  An enhanced security structure and readiness must be adopted by IHiS and public health institutions
- Recommendation #2:
  The cyber stack must be reviewed to assess if it is adequate to defend and respond to advanced threats
- Recommendation #3:
  Staff awareness on cybersecurity must be improved to enhance capacity to prevent, detect, and respond to security incidents
- Recommendation #4:
  Enhanced security checks must be performed, especially on CII systems
- Recommendation #5:
  Privileged administrator accounts must be subject to tighter control and greater monitoring
- Recommendation #6:
  Incident response processes must be improved for more effective response to cyber attacks
- Recommendation #7:
  Partnerships between industry and Government to achieve a higher level of collective cybersecurity
- Recommendation #8:
  IT security risk assessments and audit processes must be treated seriously and carried out regularly
- Recommendation #9:
  Enhanced safeguards must be put in place to protect electronic medical records
- Recommendation #10:
  Domain controllers must be better secured against attack
- Recommendation #11:
  A robust patch management process must be implemented to address security vulnerabilities
- Recommendation #12:
  A software upgrade policy with focus on security must be implemented to increase cyber resilience
- Recommendation #13:
  An internet access strategy that minimizes exposure to external threats should be implemented
- Recommendation #14:
  Incident response plans must more clearly state when and how a security incident is to be reported
- Recommendation #15:
  Competence of computer security incident response personnel must be significantly improved
- Recommendation #16:
  A post-breach independent forensic review of the network, all endpoints, and the SCM system should be considered

WannaCry hos NHS

- Recommendation 1:
  All NHS organisations are to develop local action plans to achieve compliance with the Cyber Essentials Plus standard by June 2021, as recommended by the NCSC. These plans will be provided to NHS Digital on behalf of the Chief Information Officer for health and social care by 30 June 2018. NHS Digital should produce a framework to support organisations, drawing on security assessments undertaken to-date.
- Recommendation 2: In the first quarter of 2018/2019 financial year, the CIO for health and social care will convene an expert panel to define and consult on a set of IT infrastructure, application and service management guidelines for organisations hosting clinical systems and patient data.
- Recommendation 3: By 31st March 2019, all health and social care organisations that provide NHS care through the NHS Standard Contract must provide NHS Digital on behalf of the CIO for health and social care details of their position against the DSPT. This will help audit compliance against the NDG's 10 security standards and CQC's well-led KLOE. Position statements are expected to include an action plan setting out how organisations will address any shortfalls in their compliance and plans for the forthcoming GDPR.
- Recommendation 4: Research will be commissioned by the CIO for health and social care to build an evidence base to understand the level of cyber security maturity in social care organisations. This research will be used to identify where additional support to the social care sector can be most effective.
- Recommendation 5: All NHS organisations are to ensure that every board has an executive director as data security lead, cyber security risks are regularly reviewed by the board, appropriate counter-measures are in place to mitigate and response plans are in place to address service restoration in the event of a successful attack. As CCGs are the responsible commissioner for GP IT services for general practice, a board member or equivalent senior manager should fulfil this role for CCGs
- Recommendation 6: Health and social care organisations should ensure that local contracts, processes and controls are in place to manage and monitor third party contracts for local IT systems, and that the provisions for software updates and business continuity are understood. CCGs are responsible for this for GP practices.
- Recommendation 7: During the first quarter of the 2018/19 financial year, a working group will be established by NHS Digital on behalf of the Chief Information Officer for health and social care to define standards around the management and patching of diagnostic equipment.
- Recommendation 8: Local organisations' business continuity and disaster recovery plans should include the necessary detail around response to cyber incidents, and must include a clear assessment of the impact of the loss of these services on other parts of the health and social care system. In addition, these plans must identify critical third party services (provided by other health, social care and private sector organisations), setting out the impact of the loss of these services on their operations and necessary business continuity actions required to address the loss of such services. Plans should be regularly tested across local areas both with the NHS and its partners, and reviewed and updated locally with board level oversight.

- Recommendation 9: It is recommended that NHS Digital appoint a system-wide Chief Information and Security Officer (CISO). In addition, it is recommended that NHS Digital appoints a dedicated Cyber Security Lead working across NHS England, NHS Improvement and other partners such as local government in each of the NHS England regions (North, Midlands and East, London, South East and South West).
- Recommendation 10: We recommend that, where they exist, NHS providers join and collaborate with local Warning Advice and Reporting Point groups to share trusted up-to-date advice on information security, cyber threats, incidents and solutions.
- Recommendation 11: In addition to local boards assuring themselves that they have sufficient quality and capable IT technical resources to manage and support their local IT infrastructure, systems and services, we recommend that pooled resourcing arrangements are formalised and captured in STP or ACS wide continuity plans in relation to system wide cyber-attacks.
- Recommendation 12: Professional community network models should be encouraged for cyber and information security, working in conjunction with organisations such as NHS Digital, The British Computer Society, Health Education England and the NHS Digital Academy.
- Recommendation 13: Boards for NHS organisations should undertake annual cyber awareness training and further consideration should be given to the training needs for social care providers arising from recommendation 4. The standards for training will be established nationally in 2018 by the CIO for health and social care. In addition, whilst we do not formally recommend it, all organisations should consider whether access to IT systems and services should be removed from members of staff who have not successfully completed this mandatory training.
- Recommendation 14: In addition to mandatory and statutory training, organisations should ensure that their staff receive regular and targeted cyber and information security awareness training appropriate to their job role. This may range from internal phishing attacks to test the awareness of staff to the danger of opening spam email, through to specific training associated with the management of cyber incidents
- Recommendation 15: It is recommended that NHS Digital proactively publish guidance about the CareCERT service and maintain a clear and consistent view of the technology landscape across local organisations. In the longer term, NHS Digital should have the ability to isolate organisations, parts of the country or particular services in order to contain the spread of a virus during an incident.
- Recommendation 16: It is recommended that NHS Digital enhance its procedures to support regional EPRR and long running incidents and ensure that it works jointly with NHS England's EPRR process, including developing appropriate back-up processes in the event of a cyber incident.
- Recommendation 17: It is recommended that NHS England, working with its partners, describe the EPRR processes for managing incidents on areas such as diagnostic equipment, NHS suppliers and logistic firms, high street pharmacies, dentists, care homes and private providers in the event of a local cyber attack.
- Recommendation 18: It is recommended that NHS England, working with its partners, develop scenarios to ensure that it can manage a coordinated or multiple attack whereby, for instance, a terrorist bombing attack is combined with a cyber attack.

- Recommendation 19: It is recommended that an annual national cyber rehearsal is undertaken by the DHSC, NHS England, NHS Improvement and NHS Digital, and that regional and local organisations similarly undertake regular tests of their EPRR in the event of a cyber incident.
- Recommendation 20: The DHSC, NHS England, NHS Improvement and NHS Digital should develop joint protocols for clear and consistent communications to local organisations to provide updates, advice and guidance incidents and for local reporting. This should include working with local organisations and relevant networks to identify alternative communicate channels in the event of distribution to standard channels.
- Recommendation 21: NHS Digital should develop their on-call and major operating guidelines to ensure the right expertise and seniority of decision making is available in the event of another cyber attack. NHS Digital's contact centre also needs to be sufficiently resourced to address information requests during an incident.
- Recommendation 22: CSUs must be cyber accredited and responsible for coordinating a cyber response across primary care and CCGs. All parts of the country must be covered by a CSU and all GP practices and CCGs must receive IT support from cyber accredited suppliers. NHS Digital should draw up a national response protocol and all approved IT suppliers must comply with it to ensure 24/7 on call care and linkages to CSUs.

Direktoratet for e-helse

Besøksadresse
Verkstedveien 1
0277 Oslo

Kontakt
postmottak@ehelse.no