Riksrevisjonen

Riksrevisjonens oppfølging av helseforetakenes forebygging av angrep mot sine IKT-systemer

Rapportert i Dokument 3:2 (2024–2025)

Dette er en offentlig versjon av rapporten. Den opprinnelige rapporten inneholder informasjon som er **unntatt offentlighet** jf. offentleglova § 24 tredje ledd. I denne versjonen er slik informasjon skjermet ved bruk av «sladding».

Revisjonen er gjennomført i henhold til

- **lov om Riksrevisjonen § 9 andre ledd**
- **instruks om Riksrevisjonens virksomhet § 5 andre ledd**
- **INTOSAIs standard for forvaltningsrevisjon (ISSAI 3000)**
- **Riksrevisjonens faglige retningslinjer for selskapskontroll**
- **Riksrevisjonens faglige retningslinjer for forvaltningsrevisjon**

Forsidebilde: Riksrevisjonen
ISBN 978-82-8229-609-0

Innhold

Faktaboksoversikt

Ordliste og forkortelser

Active Directory - Katalogtjeneste som benyttes i et domene hvor det blant annet defineres brukerkontoer, grupper, maskiner og tilgangsrettigheter. Brukeres tilgangsrettigheter defineres ofte ved medlemskap i en gruppe som gis rettigheter i et program

Applikasjon - Programvare som benytter datamaskinens ressurser til en oppgave som brukeren ønsker utført, for eksempel tekstbehandling, regneark eller et pasientjournalsystem. En applikasjon kjøres på en eller flere servere eller PC-er.

Autentisering - Prosessen som gjennomføres for å bekrefte en påstått identitet. Vanligvis oppgir brukeren sin identitet i form av et brukernavn og dette verifiseres ved at det gis et passord og eventuelt en annen faktor (kort, fingeravtrykk, autentiseringsapplikasjon på mobiltelefon etc.). Som oftest brukes begrepet når en brukers identitet skal bekreftes for tilgang til et IKT-system, men autentisering av en maskin er også aktuelt for kontroll med tilgang til for eksempel et nettverk.

Brukerkonto - Representerer en digital identitet og identifiserer hvem en person eller et system er. Brukerkontoer gir tilgang til datamaskiner, nettverk eller tjenester.

Dataangrep - Handlinger med hensikt å skade eller påvirke et IKT-system. Angrepet kan ha som mål å gjøre et system utilgjengelig for brukerne, stjele konfidensielle opplysninger eller endre opplysninger. Dataangrep kan potensielt skade pasienter ved å sette medisinsk utstyr ut av drift eller endre opplysninger som pleiepersonell legger til grunn for behandling. Dataangrep kan utføres av for eksempel fremmede makter, kriminelle grupper, misfornøyde pasienter eller egne ansatte.

Domene - Sammenkobling av flere systemer under én felles kontrollfunksjon, ofte kalt en domenekontroller. Gjennom domenekontrolleren defineres prosesser, tilganger og sikkerhetsnivå, og det er mot domenekontrolleren brukere autentiserer seg. I all hovedsak benyttes Microsoft Active Directory som katalogtjeneste i helseforetakenes domener. Domenet vil understøtte en infrastruktursom tilbyr IKT-tjenestene i et helseforetak, herunder ofte også medisinsk-teknisk og bygningsteknisk utstyr.

Enheter - Alt utstyr som kobles til et nettverk i en virksomhet. På et sykehus vil dette inkludere alt fra servere og PC-er til medisinsk-teknisk og bygnings-teknisk utstyr. Enheter kan være fysiske eller virtuelle.

Herding av maskiner og programvare - Sikker konfigurasjon av maskiner og programvare for å hindre eller redusere konsekvensen av dataangrep eller ubevisste feil.

Inntrengingstest - En metode som etterligner dataangrep hvor vi forsøker å omgå sikkerhetstiltak i applikasjoner, IKT-systemer eller nettverk. Formålet er å kontrollere om tiltakene fungerer etter hensikt og identifisere eventuelle svakheter som kan utnyttes i dataangrep.

Konfigurasjon - Konfigurasjon er en samlebetegnelse for alle innstillinger som er gjort ved oppsett av en datamaskin (eller annet utstyr) og programvare som kjører på den.

Konfigurasjonsfil - Fil som inneholder innstillinger som er gjort ved oppsett av en datamaskin (eller annet utstyr) og programvare som kjører på den.

NAC-løsning - NAC (Network Access Control) er en løsning som brukes for å sikre at kun godkjente enheter (pc-er, telefoner, medisinsk teknisk utstyr, nettbrett osv.) som tilfredsstiller spesifikke krav vil få tilgang til interne nettverk. Dette krever en autentiseringsløsning for enhetene.

PAM - Privileged Access Management (PAM) er en identitetssikkerhetsløsning som bidrar til å beskytte organisasjoner mot cybertrusler ved å overvåke, oppdage og forhindre uautorisert privilegert tilgang til kritiske ressurser.

Passordhash - En enveiskryptert streng av tall og bokstaver som representerer et passord.

Passordspray - Metode som kan benyttes i et dataangrep. Passordspray innebærer forsøk på å logge inn med samme passordet mot mange brukerkontoer i håp om at en eller flere har et enkelt passord.

Server - En server er en datamaskin som leverer tjenester til klienter (for eksempel PC-er) i et nettverk (jfr. klient/tjener-teknologi) slik at data og ressurser kan deles. En klient kan være for eksempel en PC eller smarttelefon. Typiske servere er for eksempel filservere, databaseservere, webservere og applikasjonsservere. Servere kan være virtuelle.

Servicekonto - En brukerkonto som anvendes av et system eller applikasjon som identifikasjon for å få tilgang til tjenester på en server. For eksempel vil et pasientjournalsystem oppgi en servicekonto for å få tilgang til databasen der pasientdata er lagret.

To-faktor-autentisering - Godkjenning med to faktorer (2FA) er en autentiseringsmetode for identitets- og tilgangsstyring som krever to former for identifikasjon for å få tilgang til ressurser og data. Dette betyr ofte bruk av et kort, fingeravtrykk, autentiseringsapplikasjon på mobiltelefon eller lignende ved siden av et passord.

1 Innledning

1.1 Opprinnelig undersøkelse

Den opprinnelige undersøkelsen ble gjennomført i 2019–2020 og ble publisert den 15. desember 2020. Stortinget behandlet saken den 11. mai 2021 og voterte over den 18. mai 2021. Målet med den opprinnelige undersøkelsen var å vurdere hvordan helseforetakenes IKT-systemer sikres mot dataangrep, hvordan de regionale helseforetakene understøtter dette arbeidet, og hvordan Helse- og omsorgsdepartementet følger opp.

Undersøkelsen viste blant annet at:

- Riksrevisjonens simulerte dataangrep ga høy grad av kontroll over IKT-infrastrukturen i tre av fire helseregioner, og tilgang til store mengder sensitive pasientopplysninger i alle helseregioner.
- I alle fire helseregioner var det vesentlige svakheter i grunnleggende tekniske sikkerhetstiltak som skulle forebygge og oppdage dataangrep.
- Helseregionene var på etterskudd i informasjonssikkerhetsarbeidet, og manglet oversikt over sikkerheten i IKT-infrastrukturen
- Uklare ansvarsforhold og uklar oppgavefordeling i helseregionene vanskeliggjorde forbedringsarbeidet.
- Atferden blant helse- og IKT-personell svekket IKT-sikkerheten.
- Helse- og omsorgsdepartementet har vært for passive i sin oppfølging av informasjonssikkerhetsarbeidet i helseregionene.

Under behandlingen i Stortinget uttalte en samlet Kontroll- og konstitusjonskomite blant annet at selv om IKT-sikkerhet er et kontinuerlig forbedringsarbeid, så forventer komiteen at Riksrevisjonens anbefalinger følges opp så raskt som mulig. Komiteen merket seg at Riksrevisjonen her har funnet grunnlag for sin sterkeste form for kritikk, og at det bør medføre rask og kraftfull oppfølging. Den merket seg også at flere av svakhetene var tatt opp allerede i 2014 og 2015.[1] Flertallet i komiteen uttrykte også i behandlingen at de ønsket en ny vurdering fra Riksrevisjonen om departementets oppfølging av IKT-sikkerheten i sektoren.[2]

Komiteen støttet Riksrevisjonens anbefalinger.

1.2 Om denne oppfølgingsundersøkelsen

Riksrevisjonen har på bakgrunn av alvorlighetsgraden til funnene i den opprinnelige undersøkelsen og merknadene fra kontroll og -konstitusjonskomiteen besluttet å gjennomføre en utvidet oppfølging av denne saken.

Helse- og omsorgsdepartementet har informert Stortinget om oppfølgingen av Riksrevisjonens undersøkelse gjennom Prop. 1S i årene etter at undersøkelsen ble publisert, herunder omtale av styrking av HelseCERT, samt henvisning til at helseregionene arbeider systematisk med å styrke informasjonssikkerheten og evnen til å forebygge, oppdage og håndtere dataangrep i samarbeid med Norsk helsenett SF og Direktoratet for e-helse/Helsedirektoratet.[3] Stortinget har imidlertid fått lite informasjon om effekten av tiltakene som er iverksatt.

[1] Innstilling fra kontroll- og konstitusjonskomiteen ble avgitt 4. mai 2021 jf innst 386 S-2021. Stortinget behandlet saken den 11. mai 2021 - Sak 21.
[2] Innst. 386 S-2020-21. Flertallet i komiteen utgjorde Arbeiderpartiet, Senterpartiet og Sosialistisk Venstreparti.
[3] Prop. 1 S (2021–2022) Helse og omsorgsdepartementet; Prop. 1 S (2022–2023) Helse- og omsorgsdepartementet; Prop. 1 S (2023–2024) Helse- og omsorgsdepartementet

Riksrevisjonen ba i et brev av 5. februar 2024 Helse- og omsorgsdepartementet om å redegjøre for hvilke tiltak som er iverksatt for å følge opp Riksrevisjonens anbefalinger og kontroll- og konstitusjonskomiteens merknader, og hvilke resultater som er oppnådd på området. Departementet svarte i brev av 12. mars 2024. Brevet inneholdt også utdypende kommentarer fra de regionale helseforetakene.

1.2.1 Metode og revisjonskriterier i oppfølgingsundersøkelsen

I oppfølgingsundersøkelsen har vi innhentet og analysert data fra Helse og omsorgsdepartementet og alle de fire regionale helseforetakene. Vi har bedt dem om å sende utvalgt dokumentasjon, samt å svare skriftlig på spørsmål om departementets og de regionale helseforetakene (RHF-ene) sitt arbeid med IKT-sikkerhet i tiden etter vi gjennomførte undersøkelsen. I tillegg har vi avholdt møte med Norsk helsenett / HelseCERT. De regionale IKT-leverandørene har også utlevert HelseCERTs rapporter fra inntrengingstester i perioden 2021–2023.

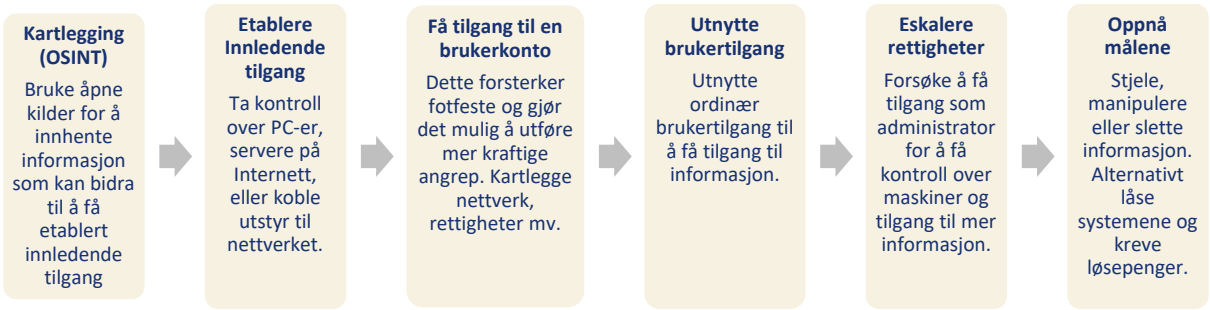
Vi har også gjennomført nye dybdeundersøkelser i to av helseregionene:

- Helse Nord RHF og Universitetssykehuset i Nord-Norge HF (UNN)
- Helse Sør-Øst og Sykehuset Innlandet HF

Vi har anvendt de samme metodene som ved forrige undersøkelse som å gjennomføre inntrengingstester, og gjort analyser av uttrekk fra virksomhetenes IT-systemer. Vi har også bedt det utvalgte helseforetaket og den regionale IKT-leverandøren om å sende dokumentasjon og svare på skriftlige spørsmål, samt avholdt møter med disse.

Formålet med inntrengningstestene var å undersøke om svakheter i informasjonssikkerheten ved de to helseregionene kunne utnyttes til å få tilgang til eller kontroll over pasientopplysninger. Vi har basert oss på allment akseptert metodikk for inntrengingstesting.[4] Kun kjente verktøy som er åpent tilgjengelig på Internett, ble benyttet. Gjennomføring av testene ble avtalt med den enkelte virksomhet før vi startet.

Framgangsmåten vi brukte varierte noe i de to regionene, ettersom vi fulgte «minste motstands vei» mot målet. Hvordan angrepene ble gjennomført og hvilke svakheter som ble forsøkt utnyttet var dermed forskjellig mellom Helse Nord og Helse Sør-Øst. Fasene i inntrengingstestene var imidlertid lik, slik illustrert i figur 1.



Inntrengingstestene skulle også teste regionenes evne til å oppdage aktiviteter i et dataangrep. Vi gjorde ingen forsøk på å skjule angrepene, men produserte mye nettverkstrafikk og andre kjente tegn på angrep. Vi ba om å bli orientert når de regionale IKT-leverandørene oppdaget aktiviteter i testen, men henstilte om at de ikke grep inn. Dette fordi formålet med kontrollene var å teste evnen til å oppdage aktiviteter i et dataangrep, ikke responsevne eller håndtering av hendelser.

[4] Metoden vi anvendte, er satt sammen fra anerkjente kilder i bransjen, som for eksempel grunnlaget for sertifiseringen «Certified Ethical Hacker» fra EC-Council og OSSTMM 3 (The Open Source Security Testing Methodology Manual) utgitt av ISECOM (The Institute for Security and Open Methodologies).

For å vurdere om virksomhetene har etablert tilstrekkelige tekniske sikkerhetstiltak for å forebygge og avdekke angrepsforsøk, har vi også trukket ut og analysert informasjon fra virksomhetenes IT-systemer. Formålet er å få et helhetlig bilde av de tekniske sikkerhetstiltakene i virksomhetene. Disse analysene utfyller dermed bildet fra inntrengingstestene – som viser hvordan konkrete svakheter kan utnyttes for å få kontroll med IT-systemer, men kun involverer et lite antall tekniske sikkerhetstiltak.

Det er umiddelbart etter avslutning av tekniske kontroller gjennomført sluttmøter med den enkelte IKT-leverandør og sykehus som har vært gjenstand for teknisk kontroll. Grunnlagsmateriale for resultatene har blitt overlevert IKT-leverandørene og sykehusene, i form av presentasjoner og dokumentasjon som viser de enkelte avvik. Formålet er å gi mulighet for umiddelbart å starte opprettingsarbeidet knyttet til de sikkerhetshull og sårbarheter som er funnet.

Vi har også gjennomgått dokumenter som kan si noe om hvor systematisk helseregionene har arbeidet med informasjonssikkerhet og personvern siden vår foregående undersøkelse. I dokumentanalysene har vi sett dette i sammenheng med resultatene av inntrengingstester og kartlegging av tekniske sikkerhetstiltak.

1.3 Oppsummering av hovedfunn fra oppfølgingsundersøkelsen

Vi har undersøkt hvordan Helse- og omsorgsdepartementet og de fire RHF-ene overordnet har fulgt opp funn og anbefalinger i vår opprinnelige undersøkelse. Undersøkelsen viser at:

- Helse og omsorgsdepartementet har stilt en rekke konkrete krav om forbedringer til RHF-ene, og hatt en tett oppfølging av forbedringsarbeidet ved å avholde felles, halvårlige oppfølgingsmøter med dem. Departementet har også stilt klare krav til underliggende virksomheter som skal støtte informasjonssikkerhetsarbeidet i sektoren, Norsk helsenett SF og Helsedirektoratet.
- Vår opprinnelige undersøkelse viste at Helse Sør-Øst, Helse Vest og Helse Nord i 2020 hadde utviklet regionale ledelsessystemer for informasjonssikkerhet. I etterkant av dette har også Helse Midt-Norge etablert et regionalt ledelsessystem. Alle regionene har videreutviklet systemene og fortsatt arbeidet med å implementere dem i helseforetakene.
- Alle RHF-ene har utarbeidet regionale planer for informasjonssikkerhetsarbeidet, som de har gjennomgått i de halvårlige oppfølgingsmøtene med departementet. De har også avklart roller og ansvar for informasjonssikkerhet innad i regionene – mellom de regionale helseforetakene, helseforetakene og de regionale IKT-leverandørene. Alle regionene har jobbet særskilt med å avklare ansvarsforhold knyttet til medisinsk-teknisk utstyr.
- Det gjennomføres risikovurderinger av informasjonssikkerhet på flere nivåer i helseregionene. Siden vår foregående undersøkelse har de regionale IKT-leverandørene samarbeidet med Norsk helsenett om årlige trusselvurderinger for spesialisthelsetjenesten for å beskrive trusler og trender i sektoren. Regionene har også vurdert risiko knyttet til skjermingsverdige verdier etter sikkerhetsloven, f.eks. kritiske IT-systemer og -utstyr, som er viktige for å understøtte helseberedskapen.
- Regionene får mer informasjon om egne svakheter nå enn de gjorde da vi gjennomførte den opprinnelige undersøkelsen, gjennom egne sikkerhetsrevisjoner og kontroller og gjennom inntrengingstester fra Norsk helsenett. Norsk helsenett gjennomfører nå årlige inntrengingstester hos alle helseregionene, mot annethvert år tidligere.
- Regionene har satt i verk en rekke tiltak på sentrale områder hvor den opprinnelige undersøkelsen viste svakheter, både i den løpende driften og gjennom større, regionale forbedringsprosjekter. Det er også gjennomført opplæringstiltak for å bedre sikkerhetskulturen. Alle de fire regionene har tatt utgangspunkt i bl.a. NSMs grunnprinsipper for IKT-sikkerhet i forbedringsarbeidet.

For å vurdere om de nye tiltakene har forbedret informasjonssikkerheten har vi foretatt nye dybdeundersøkelser i Helse Nord og Helse Sør-Øst. Undersøkelsene viser at:

- Det er arbeidet målrettet og systematisk med å forbedre informasjonssikkerheten i begge regioner. Tiltakene som er iverksatt har forbedret IT-sikkerheten, men det gjenstår fortsatt vesentlige svakheter. Begge regioner arbeider fortsatt med å få innført sikkerhetstiltak som er vedtatt og påbegynt.
- Nye inntrengingstester viser at gjenstående svakheter kan utnyttes av angripere ut fra ordinære angrepsteknikker med verktøy som kan lastes ned fra Internett. Inntrengingstestene ga full kontroll over databasene hvor pasientopplysninger lagres i [redacted], og tilgang til å administrere flere slike databaser i [redacted].
- I [redacted] var det i inntrengingstesten spesielt enkelt å få tilgang til brukerkontoer for leger og sykepleiere, og med disse brukerkontoene kunne vi lese og endre pasientopplysninger. Årsaken til at det var enkelt å få tilgang til kontoene, var at brukere hadde svake passord og at [redacted]. [redacted] har sterkere sikkerhetstiltak på dette området, noe som gjorde det mer krevende å få tilgang til brukerkontoer for leger og sykepleiere i denne regionen.
- I [redacted] var det i inntrengingstesten enkelt å komme videre inn i kritiske systemer etter å ha fått et fotfeste i nettverket. [redacted]. I [redacted] var det vanskeligere å nå kritiske servere fordi [redacted], men vi fant en svakhet i oppsettet av et verktøy for å administrere systemer som ga mulighet til å administrere en rekke servere og databaser.
- [redacted] oppdaget noen aktiviteter i inntrengingstestene, men her gjenstår arbeid med å få etablert en god overvåkning som kan oppdage og håndtere de fleste angrep. [redacted] har en veletablert overvåkningsenhet som oppdaget mange aktiviteter i inntrengingstesten gjennom oppfølging av alarmer og logganalyser. Regionen kunne dermed på ulike tidspunkt i inntrengingstesten iverksatt tiltak for å hindre videre angrep. Vi greide imidlertid blant annet å få tilgang som lege eller sykepleier i [redacted] uten at det ble oppdaget.
- [redacted] har investert betydelige midler i regionale forbedringsprogrammer, [redacted]. Dette har økt sikkerheten, men:
  - En del av de nye tiltakene er ikke fullt ut innført, og dermed mulig å omgå. Dette gjelder tiltak for økt sikkerhet i autentisering [redacted], og sikring av tilgang til nettverk [redacted]. Det er også arbeidet mye med å bygge opp sikkerhetsovervåking, men det gjenstår en del før overvåkingen kommer opp på ønsket nivå.
  - Noen sikkerhetstiltak undergraves også av at det ikke er ryddet i gamle løsninger. [redacted].
- [redacted] har også investert betydelige midler i regionale forbedringsprogrammer. [redacted]

[redacted]. Den største gjenstående svakheten er svak autentisering av brukere. [redacted]. I våre møter med [redacted] har disse dels lagt vekt på at sterkere passordkrav kan medføre ulemper for helsepersonell, som må logge inn flere ganger daglig på ulike systemer. Videre legges det vekt på at endringer i krav er komplisert pga. [redacted].

- Det er fortsatt sikkerhetsutfordringer knyttet til medisinsk-teknisk utstyr. I vår opprinnelige undersøkelse påpekte vi at slikt utstyr hadde særskilte sårbarheter. Nett for medisinsk-teknisk utstyr ble etter anmodning fra [redacted] unntatt fra inntrengingstesten, fordi utstyret ble ansett som kritisk for pasientsikkerheten og risikoen for at aktiviteter i inntrengingstesten kunne påvirke utstyret for høy.

2 Helse- og omsorgsdepartementets og de regionale helseforetakenes oppfølging

2.1 Helse- og omsorgsdepartementet

2.1.1 Departementets krav og føringer til de regionale helseforetakene

Helse- og omsorgsdepartementet har gjennom foretaksmøtene med de regionale helseforetakene i perioden 2021–2024 stilt en rekke krav som er har til formål å bidra til å understøtte deres ansvar for å øke helseforetakenes evne til å stå imot IKT-angrep. Kravene omfatter blant annet å

- følge opp Riksrevisjonens undersøkelse og lukke sårbarhetene undersøkelsen avdekket[5]
- sikre nødvendig avklaring av roller, ansvar og oppgaver i informasjonssikkerhetsarbeidet i hver helseregion[6]
- videreføre påbegynt arbeid med innføring av NSMs grunnprinsipper[7]
- utarbeide regionale handlingsplaner for informasjonssikkerhetsarbeidet, og fra 2023 oppdatere disse årlig[8]
- presentere status og rapportere fra forbedringsarbeidet bl.a. i felles møter mellom de regionale helseforetakene og departementet, samt i årlig melding[9]
- samarbeide med andre aktører som understøtter informasjonssikkerhetsarbeidet[10]
- delta i utarbeidelsen av årlig rapport om trusler og trender som spesialisthelsetjenesten kan bruke i sitt arbeid med risikovurderinger[11]
- gjennomføre øvelser, revisjoner, sårbarhetsskanning og penetrasjonstesting[12]

Departementet har etter vi publiserte vår undersøkelse fulgt RHF-ene tett opp, blant annet gjennom å avholde halvårlige felles møter med informasjonssikkerhet som hovedtema. I disse møtene har også Helsedirektoratet (tidligere Direktoratet for e-helse), Norsk helsenett SF og Helsetilsynet deltatt. Målet med møtene har vært erfarings- og kompetanseoverføring i det kontinuerlige arbeidet med å styrke informasjonssikkerheten.

I møtene har RHF-ene bl.a. presentert status og videre planer både når det gjelder det systematiske forbedringsarbeidet med å styrke informasjonssikkerheten, og arbeidet med å håndtere de sårbarhetene som ble påpekt av Riksrevisjonen. Departementet skriver at oppfølgingsmøtene vil videreføres for å sikre fortsatt erfarings- og kompetanseoverføring.[13]

[5] I foretaksmøtet i januar 2021 stilte departementet krav om at RHF-ene skulle følge opp hovedfunn, merknader og anbefalinger fra undersøkelsen. I 2022 og 2023 fulgte departementet opp dette kravet med å be RHF-ene fortsette arbeidet med å lukke sårbarhetene som ble avdekket i Riksrevisjonens undersøkelse.
[6] Foretaksmøtet i januar 2021.
[7] Krav om innføring av NSMs grunnprinsipper ble første gang stilt i foretaksmøte 2020. Dette kravet ble fulgt opp i 2021.
[8] I foretaksmøtet i januar 2021 stilte departementene krav om at RHF-ene skulle utarbeide regionale handlingsplaner for informasjonssikkerhetsarbeidet, og at disse skulle presenteres på felles tertialoppfølgingsmøte i oktober. I foretaksmøtet i januar 2022 stilte departementet krav om at RHF-ene skulle rapportere fra arbeidet innen utgangen av året. I foretaksmøtet i januar 2023 stilte departementet krav om at de regionale handlingsplanene skulle oppdateres årlig innen 1. mai, og at det skulle rapporteres fra forbedringsarbeidet.
[9] I foretaksmøtet i januar 2021 ba departementet RHF-ene om å presentere status fra arbeidet med informasjonssikkerhet, herunder ledelsens årlige gjennomgang, i egne felles årlige møter, i de etablerte felles tertialvise oppfølgingsmøtene samt i årlig melding. Videre stilte departementet krav om at RHF-ene skulle presentere de regionale handlingsplanene på felles tertialoppfølgingsmøte i oktober. I foretaksmøtet i januar 2022 ba departementet RHF-ene om å rapportere fra arbeidet med regionale handlingsplaner og med å lukke sårbarhetene som Riksrevisjonens undersøkelse avdekket innen utgangen av året. I 2023 stilte departementet krav om at RHF-ene skulle rapportere fra forbedringsarbeidet årlig i forbindelse med oppdateringen av de regionale handlingsplanene for informasjonssikkerhetsarbeidet.
[10] I foretaksmøtet i januar 2021 ba departementet RHF-ene om å delta i samarbeidsforum med Direktoratet for e-helse og Norsk helsenett SF for å styrke erfaringsoverføring på tvers, og for å identifisere egnede nasjonale og interregionale tiltak for å styrke informasjonssikkerheten i helseforetakene og forebygge angrep mot IKT-systemene. I foretaksmøtet i januar 2022 ba departementet RHF-ene om å samarbeide med HelseCERT om regionale og nasjonale kapabiliteter for å oppdage og håndtere sikkerhetshendelser, og gjennom det styrke egenbeskyttelsen og regionens samlede evne til å oppdage digitale angrep.
[11] I foretaksmøtet i januar 2021 ba departementet RHF-ene om å bruke Norsk helsenett SFs årlige rapport om trusler, trender, sårbarheter og relevante tiltak som sektoren kan bruke i arbeidet med risiko- og sårbarhetsvurderinger, som Norsk helsenett SF første gang fikk i oppdrag av departementet å utarbeide i foretaksmøtet januar 2020. I 2022 og 2023 ba departementet RHF-ene om å delta i utarbeidelsen av den årlige rapporten, og presiserte at erfaringer fra penetrasjonstester, portskanninger og hendelser (fra 2023) ville være relevant.
[12] I foretaksmøtet i januar 2021 viste departementet til øvelser, revisjoner, sårbarhetsskanning og penetrasjonstester var relevante tiltak for å styrke informasjonssikkerheten og forebygge IKT-angrep. I foretaksmøtet i januar 2023 stilte departementet et eget krav til RHF-ene om å øve på håndtering av uønskede kritiske hendelser i samarbeid med Norsk helsenett SF.
[13] Helse- og omsorgsdepartementets svar av 12. mars 2024 på Riksrevisjonens brev av 5. februar 2024

Departementet har også stilt krav knyttet til RHF-ene og helseforetakene (HF-ene) sin ivaretakelse av sikkerhetsloven (se omtale under kapittel 2.1.3).

Det framkommer av kapittel 2.2 hvordan RHF-ene har fulgt opp kravene fra departementet.

2.1.2 Departementets krav og føringer til sentrale aktører som understøtter informasjonssikkerhetsarbeidet i sykehusene

Helse og omsorgsdepartementet har stilt flere krav til sentrale aktører som har et særskilt ansvar for å understøtte informasjonssikkerhetsarbeidet i RHF-ene og HF-ene (se faktaboks for en beskrivelse av aktørene og deres ansvar).

Faktaboks 1 Sentrale aktører som understøtter informasjonssikkerhetsarbeidet i RHF-ene og HF-ene, og deres ansvarsområder

Norsk helsenett SF er et IKT-selskap som leverer digitale tjenester og infrastruktur til helsesektoren. Norsk Helsenett ivaretar informasjonssikkerheten i den nasjonale IKT-infrastrukturen (Helsenettet), ved den interne enheten HelseCERT (Computer Emergency Response Team). HelseCERT er helse- og omsorgssektorens nasjonale senter for informasjonssikkerhet.

Helsedirektoratet har ansvar for den nasjonale beredskapen på IKT-området innen sektoren. Etter sammenslåingen med Direktoratet for e-helse 1.1.2024 er Helsedirektoratet også departementets fag- og myndighetsorgan innen digitalisering.[14] Innen informasjonssikkerhetsområdet omfatter dette blant annet:

- Hovedansvar for å tydeliggjøre rammebetingelsene for arbeidet med informasjonssikkerhet og digitalisering i sektoren.
- Å være sekretariat for Norm for informasjonssikkerhet og personvern i helse og omsorgssektoren (Normen), som er et sett av krav til informasjonssikkerhet basert på lover og regelverk på området.
- Kunnskapsspredning om informasjonssikkerhet (og personvern) i sektoren.

Kilder: *Vedtekter for Norsk Helsenett SF* §3. Sist endret 15. januar 2024; *Riksrevisjonens undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer. Rapportvedlegg til Dokument 3:2 (2020−2021);* Prop. 1 S. (2023–2024) Helse- og omsorgsdepartementet; og Helse- og omsorgsdepartementet (2024) *Treårsoppfølging - helseforetakenes forebygging av angrep mot sine IKT-systemer*. Brev til Riksrevisjonen 12. mars 2024.

Krav til Norsk helsenett SF

Den opprinnelige undersøkelsen viste at det var behov for å styrke rollen til Norsk helsenett SF/HelseCERT når det gjelder å overvåke og teste IKT-sikkerheten i helseregionene, og anbefalte blant annet Helse- og omsorgsdepartementet å vurdere hva slags rolle HelseCERT kan ha i sikkerhetsovervåking av regionale nettverk. Oppfølgingsundersøkelsen viser at Helse- og omsorgsdepartementet har gitt flere krav og føringer til Norsk helsenett SF i årene etter undersøkelsen ble publisert.

I 2021 stilte Helse- og omsorgsdepartementet krav om at Norsk helsenett SF blant annet skulle

- delta i RHF-enes arbeid med å følge opp hovedfunn, merknader og anbefalinger fra Riksrevisjonens undersøkelse, herunder delta i de årlige møtene mellom RHF-ene og Helse- og omsorgsdepartementet for å presentere innsikt fra det operative sikkerhetsarbeidet i sektoren, og et oppdatert trusselbilde.[15]

[14] Direktoratet for e-helse ble etablert i 2016 og var fram til det ble slått sammen med Helsedirektoratet 1.1.2024 departementets fag- og myndighetsorgan innen digitalisering. Ansvarsområdene til Direktoratet for e-helse er fra 1.1.2024 videreført i Helsedirektoratet
[15] Protokoll foretaksmøte Norsk helsenett SF 21. januar 2021

- delta i RHF-enes samarbeidsforum for å styrke erfaringsoverføring på tvers, og for å identifisere egnede nasjonale og interregionale tiltak for å styrke informasjonssikkerheten i helseforetakene[16].
- gjennom HelseCERT bidra til å styrke helse- og omsorgssektorens sikkerhetsarbeid, og videreutvikle nasjonalt beskyttelsesprogram (NBP) og Digital beskyttelse i dybden (DBD) i samarbeid med helseregionenes sikkerhetsmiljøer og andre medlemmer av programmet.[17] Se faktaboks nedenfor for nærmere omtale av Nasjonalt beskyttelsesprogram og Digital beskyttelse i dybden.

Disse kravene har blitt fulgt opp også i årene som fulgte. I 2022 ba departementet Norsk helsenett SF om blant annet å styrke HelseCERTs arbeid med monitorering og overvåking; videreutvikle arbeidet med kommunikasjon og bistand til sektoren; øke kapasiteten til å gjennomføre sikkerhetstesting av aktører i sektoren; samt videreutvikle Digital beskyttelse i dybden (DBD) i samarbeid med de regionale helseforetakene.[18]

Kravene om å styrke HelseCERTs arbeid med overvåkning av sikkerhetssituasjonen i sektoren, og videreutvikle arbeidet med kommunikasjon og bistand til sektoren ble gjentatt i oppdragsbrevene for 2023 og 2024.

Faktaboks 2 Nasjonalt beskyttelsesprogram og Digital beskyttelse i dybden

Nasjonalt beskyttelsesprogram (NBP) er opprettet av HelseCERT som ledd i deres arbeid med å løse sitt oppdrag som sektorvist responsmiljø for helsesektoren. Medlemmene i NBP inkluderer kommuner, hele spesialisthelsetjenesten, leverandører og andre virksomheter som er tilknyttet Helsenettet.

I NBP er det etablert en rekke tjenester som til enhver tid er under videreutvikling for å løse oppdraget fra Helse- og omsorgsdepartementet, og samtidig tilby mest mulig verdi til helsesektoren. Alle tjenestene ligger innenfor spekteret av å forebygge, oppdage og håndtere sikkerhetshendelser. Per april 2024 listet Norsk helsenett SF følgende tjenester i NBP på sine nettsider:

- Anbefaling av sikkerhetstiltak
- Blokkeringslister
- Varsler om brukernavn og passord på avveie
- Hendelseshåndtering
- Automatisert sikkerhetstest («Hurtigtest»)[19]
- Informasjonsdeling og forebygging
- Sikkerhetsskanning[20]
- Rapporter[21]
- Webinarer

Digital beskyttelse i dybden (DBD) er et program som er utviklet de siste årene for å bistå helseregionene i å oppdage cyberangrep på innsiden av regionenes IT-infrastruktur. Tjenestene i DBD er primært rettet mot de regionale IKT-leverandørene i spesialisthelsetjenesten. En sentral leveranse i programmet er bistand til logganalyse med utgangspunkt i regionenes logger. Per mai 2024 var alle helseregionene unntatt Helse Sør-Øst, brukere av DBD.[22]

Kilde: Norsk helsenett SFs årsrapport for 2022, Norsk helsenett SF (u.å.) *HelseCERT og KommuneCERT.* Intervju med Norsk helsenett 21.05.2024

[16] Protokoll foretaksmøte Norsk helsenett SF 21. januar 2021
[17] Oppdragsdokument til Norsk helsenett SF for 2021
[18] Oppdragsdokument til Norsk helsenett SF for 2022.
[19] «Hurtigtest» tar for seg de mest grunnleggende svakhetene HelseCERTs pentestere normalt finner i virksomhetene
[20] Sårbarhetsskanning Internett og Helsenett; portskanning og statusrapport e-postsikkerhet
[21] Rapporten «Situasjonsbilde» gir en situasjonsvurdering for trusler mot helsesektoren, inkludert hvilke angrepsmetoder som typisk benyttes, samt rapporten «HelseCERT tilbakeblikk» som sendes ut tre ganger i året med oversikt over nevneverdige hendelser, sårbarhetsstatistikk generelt, og sårbarhetsstatistikk for den aktuelle virksomheten.
[22] Norsk helsenett SF opplyste i intervju 21.05.24 at Helse Sør-Øst har bygget opp egen kapasitet og følgelig valgt å ikke bruke denne tjenesten.

I november 2023 fikk Norsk helsenett i oppdrag å være sektorvist responsmiljø (SRM)[23] for kommunesektoren, i tillegg til å ha denne funksjonen for helsesektoren. Funksjonen var operativ fra 1. desember 2023.[24]

Tidligere har Helse- og omsorgsdepartementet stilt krav om at Norsk helsenett skulle gjennomføre et visst antall inntrengingstester mot utvalgte helseforetak og kommuner. Det er ikke lenger noe eksplitt krav til omfang av slike tester. Vi registrerer imidlertid at Norsk helsenett siden vår opprinnelige undersøkelse har trappet opp omfanget av slike tester mot helseregionene. Mens de på tidspunktet for den opprinnelige undersøkelsen gjennomførte tester mot den enkelte region annethvert år, gjennomfører de nå tester i alle helseregioner hvert år. Disse testene er nærmere omtalt i kap. 2.2.6, 3.1.3 og 3.2.3.

Krav til Helsedirektoratet og det tidligere Direktoratet for e-helse

Den opprinnelige undersøkelsen viste at Direktoratet for e-helse hadde hatt en lite tydelig rolle på informasjonssikkerhetsområdet, og anbefalte departementet å vurdere direktoratets rolle.

Departementets krav i tildelingsbrevene til Helsedirektoratet i perioden 2021–2024 som berører informasjonssikkerhetsområdet, er i hovedsak knyttet til beredskap[25], samt til oppfølging av ny lov om nasjonal sikkerhet.[26]

Fra 1.1.2024 er Direktoratet for e-helse slått sammen med Helsedirektoratet. Før sammenslåingen stilte departementet krav til Direktoratet for e-helse om å:

- bidra i helseregionenes arbeid med å følge opp Riksrevisjonens rapport i samarbeid med RHF-ene og Norsk helsenett SF.[27]
- utarbeide en strategi for digital sikkerhet i helse- og omsorgssektoren.[28]

Strategien skulle ifølge tildelingsbrevet for 2021 tydeliggjøre roller og ansvar og identifisere relevante strategiske virkemidler og tiltak for å løfte arbeidet med digital sikkerhet i sektoren. Arbeidet skulle gjøres i samarbeid med Helsedirektoratet, Helsetilsynet, Norsk helsenett SF, RHF-ene og kommunesektoren/KS. Oppdraget ble fulgt opp i tildelingsbrevet til Direktoratet for e-helse i januar 2022.[29]

I 2022 ble det imidlertid besluttet å innarbeide strategien i den kommende stortingsmeldingen om helseberedskap.[30] Begrunnelsen for dette var å få mest mulig oppmerksomhet på området og for å minske antall dokumenter å forholde seg til i sektoren.[31] Direktoratet utarbeidet derfor i 2022 et innspill til helseberedskapsmeldingen innenfor temaet Digital sikkerhet.[32] I tildelingsbrev januar 2023 fikk

[23] NSM har etablert et rammeverk for håndtering av IT-sikkerhetshendelser, som i samsvar med Nasjonal strategi for informasjonssikkerhet og handlingsplanen som følger strategien, legger til grunn at det skal etableres sektorvise responsmiljøene (SRM) som skal ha en sentral rolle i hendelseshåndteringen. Kilde: Nasjonal sikkerhetsmyndighet (2017) *Rammeverk for håndtering av IKT-sikkerhetshendelser*.

[24] Norsk helsenett har valgt å legge funksjonen som SRM for kommunesektoren til det opprinnelig sektorvise responsmiljøet for helsesektoren (HelseCERT). Funksjonen heter i dag Helse- og kommuneCERT. Av oppdragsdokumentene fra Helse- og omsorgsdepartementet til Norsk helsenett for henholdsvis 2023 og 2024 framgår det at posten som finansierer bl.a. informasjonssikkerhetsarbeidet økte med 4,3 mill. kroner fra 2023 til 2024. Av protokoll fra foretaksmøtet i Norsk helsenett 24.11.2023 framgikk det at Norsk helsenett ikke skulle stå for deteksjonskapasitet og SOC-leveranser til kommunene.

[25] I tildelingsbrev januar 2021 ba departementet Helsedirektoratet bl.a. om å bidra til å videreutvikle nasjonale helseberedskapsplaner og systemer, bl.a. basert på evaluering av en cyberhendelse og nasjonale risiko- og sårbarhetsvurderinger. Også i tildelingsbrev januar 2022 ga departementet Helsedirektoratet oppdrag knyttet til beredskap, bl.a. skulle direktoratet vurdere hvordan beredskapen i helse- og omsorgstjenestene kan styrkes gjennom endringer i organisering, bruk av teknologi/digitale løsninger, finansiering og/eller regulering av tjenestene. I tildelingsbrevet i januar 2023 ba departementet Helsedirektoratet om å bidra til oppfølging av erfaringene fra koronapandemien og andre hendelser og øvelser, samt gjennomførte nasjonale risiko- og sårbarhetsvurderinger. I tildelingsbrev januar 2024 stilte departementet krav til Helsedirektoratet om å etablere og lede det nyopprettede Utvalg for digital sikkerhet; kartlegge og vurdere eksisterende kompetansetiltak og øvelser som skal danne grunnlaget for en or en kompetanse- og øvelsesplan for sikkerhet og beredskap for sektoren; samt gi tekstbidrag til ny nasjonal helseberedskapsplan som er planlagt ferdigstilt i løpet av 2024.

[26] I tildelingsbrev januar 2021 ba departementet Helsedirektoratet bl.a. om å bidra i koordineringen av arbeidet med å følge opp lov om nasjonal sikkerhet og vurdere truslene helsesektoren kan stå overfor som ved sammensatt virkemiddelbruk kan påvirke tilliten til helsemyndighetene.

[27] Blant annet gjennom å delta i samarbeidsforum mellom aktørene under ledelse av de regionale helseforetakene. Tildelingsbrev januar 2021.

[28] Dette arbeidet ble påbegynt i 2020, da direktoratet i tildelingsbrevet fikk i oppdrag å foreslå innretning på en slik strategi.

[29] «Direktoratet skal, som oppfølging av Strategi for digital sikkerhet i helse- og omsorgssektoren, utarbeide en oversikt over prioriterte nye tiltak for å realisere strategien. Videre skal direktoratet ferdigstille en plan for oppfølging av disse prioriterte tiltakene.»

[30] Oppdraget ble endret gjennom tillegg til tildelingsbrev nr. 5 av 16. mai 2022.

[31] Kilde: Direktoratet for e-helse (2023) *TB2023-9 Digital sikkerhet – anbefaling til prioriterte tiltak. Oppfølging av direktoratets innspill til den kommende helseberedskapsmeldingen s.7.*

[32] Direktoratet for e-helse (2022) *Innspill til kommende stortingsmelding om helseberedskap –Digital sikkerhet*.

direktoratet i oppdrag å følge opp mål og innsatsområder fra innspillet til helseberedskapsmeldingen, og anbefale hvilke tiltak som skulle prioriteres.

Helseberedskapsmeldingen ble overlevert til Stortinget i november 2023.[33] Den definerer digital sikkerhet som ett av seks risikoområder som krever særskilt oppmerksomhet framover. Meldingen skisserer en ny modell for helseberedskapsarbeidet nasjonalt, som inkluderer noen endringer i ledelse og organiseringen av helseberedskapen i stort. Av meldingen går det fram at Nasjonal helseberedskapsplan vil bli revidert i etterkant av Stortingets behandling av meldingen. Det er dermed for tidlig å si om, og i så fall hvordan digital sikkerhet vil tas inn i den nye helseberedskapsplanen.

2.1.3 Departementets oppfølging av ny sikkerhetslov og arbeidet med å identifisere skjermingsverdige IT-systemer og informasjonsverdier

Lov om nasjonal sikkerhet (sikkerhetsloven) trådte i kraft 1. januar 2019, og da vi gjennomførte den opprinnelige undersøkelsen hadde ikke helseregionene påbegynt arbeidet med å tilpasse seg den nye sikkerhetsloven. Vår gjennomgang viser at sektoren nå har oversikt over de viktigste IT-systemene og infrastrukturen som understøtter den grunnleggende nasjonale funksjonen helseberedskap og nasjonale sikkerhetsinteresser.

Helse- og omsorgsdepartementet viser i brev til Riksrevisjonen til at departementet etter loven trådte i kraft har gjennomført en felles prosess med RHF-ene og Norsk helsenett SF for å identifisere potensielle skjermingsverdige objekter og infrastruktur under den grunnleggende nasjonale funksjonen (GNF) helseberedskap. Departementet utpekte skjermingsverdige verdier hos helseregionene i november 2022.[34]

I foretaksmøtet i januar 2023 stilte departementet krav til RHF-ene om å gjennomføre forebyggende sikkerhetstiltak for å beskytte de skjermingsverdige verdiene som er utpekt. Dette kan dreie seg om f.eks. utvalgte IT-systemer og -utstyr som er viktige for å understøtte helseberedskapen. RHF-ene viser i sine svarbrev til at det i etterkant av dette er gjennomført skade- og risikovurderinger, at det er opprettet tiltaksplaner og at arbeidet med risikoreduserende tiltak er i gang. Arbeidet rapporteres løpende til departementet både direkte og gjennom fellesmøter mellom departementet, RHF-ene, Norsk helsenett SF og Helseplattformen.

2.2 De regionale helseforetakene

Oppfølgingsundersøkelsen viser at RHF-ene har arbeidet med en rekke tiltak for å følge opp Riksrevisjonens funn og anbefalinger, samt departementets krav i årene etter undersøkelsen ble publisert.

En gjennomgang av RHF-enes styresaker viser at alle de fire styrene ble orientert om den opprinnelige undersøkelsen enten før eller relativt raskt etter den ble publisert,[35] og at styrene har fulgt opp informasjonssikkerheten i en rekke saker i ettertid.[36] Alle styrene har fått informasjon om status for informasjonssikkerhetsarbeidet årlig, enten gjennom egne styresaker eller som del av styrets orientering om ledelsens gjennomgang av virksomheten.

RHF-ene har orientert departementet jevnlig om framdriften i forbedringsarbeidet i felles møter mellom RHF-ene og departementet (jf. omtale i 2.1.1) og gjennom årlig melding.[37] For 2023 rapporterte RHF-ene også om arbeidet i *Felles plan for IKT-utvikling og digitalisering*[38], som er RHF-enes felles årlige

[33] Meld St. 5 (2023–2024) *En motstandsdyktig helseberedskap. Fra pandemi til krig i Europa.*
[34] Kilde: Svar fra Helse Nord. Helse Vest
[35] Styrene i Helse Nord RHF og Helse Midt-Norge RHF ble orientert om undersøkelsen i november 2020, mens Helse Sør-Øst RHF og Helse Vest RHF hadde egne saker om undersøkelsen i henholdsvis februar og mars 2021.
[36] For eksempel behandlet alle styrene regional handlingsplan i 2021.
[37] Jf. krav i Helse- og omsorgsdepartementets foretaksmøte med helseregionene i januar 2021.
[38] Jf. krav i Helse- og omsorgsdepartementets foretaksmøte med helseregionene i januar 2023 om å rapportere fra forbedringsarbeidet årlig.

rapportering om journal- og samhandlingsløsninger, hjemmeoppfølging og innbyggertjenester, bruk av helsedata, samt informasjonssikkerhet og personvern.

Som ledd i arbeidet med å forbedre informasjonssikkerheten, har RHF-ene etablert samarbeid seg imellom på flere nivåer:

- Det er etablert et interregionalt samarbeidsforum mellom RHF-ene, Helsedirektoratet og Norsk helsenett med formål å dele erfaringer mellom helseregionene. Samarbeidsforumet har cirka 6 møter i året med deltakelse fra blant annet fagressurser og informasjonssikkerhetsledere i hvert RHF og de regionale IKT-leverandørene.
- I tillegg har informasjonssikkerhetslederne i henholdsvis de fire RHF-ene og de fire regionale IKT-leverandørene hver sin møtearena. Begge gruppene møtes månedlig.
- Det er også etablert en møtearena for Nasjonalt sykehusapotekutvalg for informasjonssikkerhet, hvor sykehusapotekenes informasjonssikkerhetsledere og personvernombud møtes.

Nedenfor følger en oppsummering av RHF-enes arbeid innen sentrale områder som ble belyst i den opprinnelige undersøkelsen.

2.2.1 RHF-enes arbeid med regionale styringssystemer

Et styringssystem/ledelsessystem for informasjonssikkerhet fungerer som et rammeverk for styring og sikkerhetsorganisering i den enkelte virksomhet. Det skal sette planlegging, gjennomføring, kontroll/evaluering og oppfølging av informasjonssikkerhetsarbeidet i system.

Istedenfor å la det være opp til den enkelte virksomhet å utarbeide sitt eget ledelsessystem for informasjonssikkerhet, har helseregionene valgt å utarbeide ledelsessystemer for foretaksgruppene som helhet. Det enkelte helseforetak skal så innføre systemet lokalt med nødvendige tilpasninger.

Vår opprinnelige undersøkelse viste at Helse Sør-Øst, Helse Vest og Helse Nord i 2020 hadde utviklet regionale ledelsessystemer for informasjonssikkerhet, med utgangspunkt i standarder som ISO/IEC 27001, samt Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen). Helse Midt-Norge ikke hadde utarbeidet tilsvarende.

Oppfølgingsundersøkelsen viser at også Helse Midt-Norge nå har etablert et regionalt ledelsessystem for informasjonssikkerhet og personvern. I sitt svar skriver Helse Midt-Norge at de har etablert styrende dokumenter som beskriver mål, strategi, overordnede prinsipper, organisering av arbeidet, risikostyring og noen temaspesifikke krav og retningslinjer. Systemet inneholder også prosedyrer, veiledninger og prosessbeskrivelser på utvalgte områder, som f.eks. risikostyring. Helse Midt-Norge oppgir at arbeid med prioriterte temaspesifikke krav og retningslinjer[39] planlegges avsluttet i løpet av andre kvartal 2024.

Svar fra de øvrige tre RHF-ene viser at de har revidert og oppdatert sine felles ledelsessystemer for informasjonssikkerhet og personvern, og fortsatt arbeidet med å implementere systemene i helseforetakene.[40] Disse tre regionene har utarbeidet temaspesifikke policyer som setter krav til tekniske og organisatoriske sikkerhetstiltak som skal gjennomføres. Vi har i denne

[39] Temaspesifikke policyer/retningslinjer pålegger/stiller krav til implementering av sikkerhetstiltak innenfor konkrete områder, som f.eks. opplæring i informasjonssikkerhet, tilgangskontroll, konfigurering av systemer eller sikkerhetsovervåking. Policyene skal sikre at det ikke blir opp til den enkelte ansatte i virksomheten hvordan dette gjøres

[40] **Helse Vest** oppdaterte sitt regionale ledelsessystem gjennom et prosjekt gjennomført i 2022-2023. Målet med prosjektet var å oppdatere malverket for det regionale styringssystemet for informasjonssikkerhet og personvern, på en måte som gjorde det mer brukervennlig og enklere å forholde seg til. Helse Vest sitt direktørmøte ga sin tilslutning til dette i mai 2023. Helse Vest har sendt en oversikt som viser status på innføring av det styringssystemet i hvert enkelt helseforetak i regionen. **Helse Nord** RHF oppdaterte det overordnede policy-dokumentet «Strategiske sikkerhetsmål og strategi for informasjonssikkerhet» i 2021, opplyser at flere av dokumentene på ledelsessystemets nivå 2 (som omfatter til sammen 24 sikkerhetsområder) var under revidering per første kvartal 2024. **Helse Sør-Øst** har videreutviklet det overordnede styrende dokumentet «Mål og strategi for informasjonssikkerhet» i samarbeid med helseforetakene. Gjeldende versjon ble styrebehandlet i april 2021 og ble gjort gjeldende for helseforetakene i tilleggsdokument til oppdrag og bestilling i juni samme år. RHF-et opplyser at de styrende dokumentene «Organisering av personvern- og informasjonssikkerhetsarbeidet» og «Kriterier for vurdering og aksept av risiko innen informasjonssikkerhet» har hatt prioritet. Disse ble sist oppdatert i hhv. 2021 og 2022. Flere av dokumentene i ledelsessystemet som er forvaltet av Sykehuspartner (de såkalte regionale bruksvilkårene for informasjonssikkerhet) har også vært gjenstand for oppdatering de siste årene.

oppfølgingsundersøkelsen ikke undersøkt i hvor stor grad ledelsessystemene er implementert og oppdatert i de enkelte helseforetakene.

2.2.2 Regionale informasjonssikkerhetsplaner

Alle helseregionene har etablert regionale handlingsplaner for informasjonssikkerhet, i tråd med departementets oppdrag fra 2021. I planene definerer hver helseregion 5-6 overordnede tiltaksområder (se faktaboks), som berører de viktigste funnene fra vår opprinnelige undersøkelse. Alle regionene unntatt Helse Vest har oppdatert eller revidert planene i perioden 2021–2023.[41] Status for oppfølging av planene er fra 2021 gjennomgått i felles oppfølgingsmøter mellom RHF-ene og Helse- og omsorgsdepartementet.

Faktaboks 3 Tiltaksområder i regionale handlingsplaner for informasjonssikkerhet

Helse Sør-Øst[42]	Helse Vest[43]	Helse Midt-Norge[44]	Helse Nord[45]
1. Roller og ansvar	1.Roller, ansvar og oppgaver	1. Videreutvikling av Regionalt styringssystem for informasjonssikkerhet og personvern	1. Roller og ansvar
2. Oversikt, rapportering og oppfølging	2. Oversikt, rapportering og oppfølging	2. Kompetanse, holdninger og kultur	2. Oversikt, rapportering og oppfølging
3. Informasjons-sikkerhetskultur og -kompetanse	3. Informasjons-sikkerhetskultur og -kompetanse	3. Tekniske tiltak	3. Informasjons-sikkerhetskultur og -kompetanse
4. Informasjons-sikkerhet i anskaffelser	4. Informasjons-sikkerhet i anskaffelser	4. Medisinsk-teknisk utstyr	4. Infrastruktur og teknisk IKT-sikkerhet
5. Applikasjoner, infra-struktur og teknisk IKT-sikkerhet	5. Applikasjoner, IKT-infrastruktur og teknisk sikkerhet	5. Andre tiltak	5. Kontinuerlig forbedring
6. Kontinuerlig forbedring			6. Beredskap

Kilde: Helseregionenes regionale handlingsplaner

2.2.3 Avklaring av ansvar og roller på informasjonssikkerhetsområdet

Vår opprinnelige undersøkelse viste at uklare ansvarsforhold og uklar oppgavefordeling i regionene gjorde forbedringsarbeidet på informasjonssikkerhetsområdet vanskeligere. Vi pekte på

- uklarheter om hvem som skal gjøre nødvendig opprydding og forbedringstiltak, og
- uklarheter om ansvaret for ivaretakelse av sikkerheten i medisinsk-teknisk utstyr.

Oppfølgingsundersøkelsen viser at alle helseregionene har jobbet med å avklare ansvar og roller på regionalt nivå.

[41] Helse Vest skriver at planen er planlagt revidert i første halvår 2024.
[42] Kilde: Regional handlingsplan for arbeidet med informasjonssikkerhet, versjon 0.99 datert 12.9.2021, Regional handlingsplan for arbeidet med informasjonssikkerhet, versjon 2.0 (utkast)
[43] Kilde: Regional handlingsplan for Informasjonssikkerhet i Helse Vest, mottatt i 2024. Helse Vest RHF skriver i oversendelsesbrevet at de planlegger å revidere planen første halvår 2024.
[44] Kilde: Regional handlingsplan for informasjonssikkerhet og personvern, versjon 1.0, 19.10.2021. Vi har også mottatt versjon 1.6, datert 26.01.2023. Denne inneholder åtte tiltak som skal gjennomføres i planperioden 2023–2024, gruppert under følgende tre hovedtemaer: Videreutvikling av regionalt styringssystem; Kompetanse, holdninger og kultur; og Øvrige tiltak i handlingsplanen
[45] Kilde: Regional handlingsplan for informasjonssikkerhet versjon 1.4, datert 1.3.2023. Vi har også mottatt versjon 2.0, uten dato. Denne inneholder følgende tre innsatsområder som skal gjennomføres i perioden 2024–2027: Organisasjon; teknologi (infrastruktur og teknisk IKT-sikkerhet); og sikkerhetskultur og – kompetanse (mennesket).

Avklaring av ansvar mellom RHF, HF og de regionale IKT-leverandørene

Den opprinnelige undersøkelsen pekte på manglende avklaringer om ansvar og roller på regionalt nivå, mellom RHF, HF og de regionale IKT-leverandørene. Rolle- og ansvarsfordelingen mellom aktørene i den enkelte region var bare i noen grad definert skriftlig i ledelsessystemene for informasjonssikkerhet og personvern.

Tilsendt dokumentasjon viser at alle regioner nå har definert skriftlig hva som er henholdsvis helseregionen, den regionale IKT-leverandøren og helseforetakenes rolle på informasjonssikkerhetsområdet.

I den opprinnelige undersøkelsen så vi særlig utfordringer knyttet til uavklarte ansvarsforhold i Helse Nord, Helse Midt-Norge og Helse Sør-Øst. En større problemstilling i disse tre regionene var hva slags oppgaver og myndighet de regionale IKT-leverandørene hadde og burde ha. Utfordringen for IKT-leverandørene var bl.a. at de var gitt et ansvar for sikkerheten i den regionale infrastrukturen (regionalt nettverk og maskinpark), men ikke hadde kontroll med alt som var koblet til denne. Flere av helseforetakene i disse regionene uttrykte på sin side et behov for eller ønske om en viss grad av lokal kontroll, og pekte på at helseforetakene kan miste kompetanse ved å sentralisere IKT-drift og -sikkerhetsarbeid.

Et fellestrekk i Helse Nord, Helse Midt-Norge og Helse Sør-Øst er at den regionale IKT-leverandøren nå har fått tydeligere ansvar og myndighet knyttet til sikkerheten i den regionale IKT-infrastrukturen.[46]

De reelle endringene i ansvarsforholdene er størst i Helse Nord. På tidspunktet for den opprinnelige undersøkelsen lå eierskapet til sluttbrukerutstyr koblet til IKT-infrastrukturen (inkl. PCer) hos helseforetakene, og det var betydelig innslag av lokal drift av IT-systemer og utstyr. I etterkant av dette har styret i Helse Nord RHF gjort avklaringer gjennom flere styresaker.[47] Helse Nord IKT er nå gitt et tydeligere ansvar for regional IKT-infrastruktur og det som er koblet til denne. Det er også bestemt at all teknisk og merkantil forvaltning av applikasjoner i regionen skal overføres til Helse Nord IKT.

I Helse Sør-Øst er det foretatt en grunnleggende endring i ledelsessystemet for informasjonssikkerhet, ved at *regionale bruksvilkår for informasjonssikkerhet* er skilt ut som en egen del av ledelsessystemet. Denne delen av ledelsessystemet består av dokumenter med krav/vilkår som helseforetak, leverandører og andre må akseptere for å bruke Sykehuspartners tjenester.

Vi observerer at avklaring av roller og ansvar har vært komplisert og tidkrevende i disse regionene, og at en del avklaringer er gjort forholdsvis nylig.[48] Avklaringene som er gjort har ikke nødvendigvis fått «full effekt» – selv om det er avklart hvem som helt overordnet har ansvar for eller myndighet til å gjennomføre opprydding og forbedringstiltak, vil selve gjennomføringen også kunne ta tid.

Da den opprinnelige undersøkelsen ble gjennomført hadde alle de fire helseregionene etablert ett eller flere forum for styring og samarbeid innenfor informasjonssikkerhet og personvern. Disse er videreført og brukes aktivt. Det er også opprettet nye fora.[49]

Det er også gjort endringer i organisering innad i helseforetak og regionale IKT-leverandører. Vi ser f.eks. av svar i dybdeundersøkelsen at både Sykehuspartner HF og Helse Nord IKT HF har opprettet

[46] I **Helse Midt-Norge** har Hemit fått en tydeligere rolle: «Hemit skal ha myndighet til å gjennomføre nødvendige tiltak for å sikre infrastrukturen ved sikkerhetshendelser. (…) Hemit skal ha myndighet til å avvise implementering/oppstart av systemer eller utstyr som medfører uakseptabel risiko for andre virksomheter i foretaksgruppen. Beslutningsprosess for en slik vurdering, skal være beskrevet i tjenesteavtalen.»

[47] Styret har vedtatt et overordnet rammeverk for IKT-styring i regionen mer generelt, en styringsstruktur for IKT-infrastrukturen, og gjort avklaringer av roller og ansvar på informasjonssikkerhetsområdet.

[48] I Helse Nord ble f.eks. retningslinjer som beskriver ansvar og roller (01 Styring av informasjonssikkerhet og 02 Organisering av informasjonssikkerhets-arbeidet i Helse Nord) revidert høsten 2023, og ny versjon ble publisert i februar 2024.

[49] I Helse Nord er det opprettet en ny regional styringsgruppe for informasjonssikkerhet som ledes av eierdirektør i Helse Nord RHF, med deltakelse fra de administrerende direktørene i regionen. Denne gruppen har fått ansvar for å følge opp regional handlingsplan, og har fungert som programstyre i det regionale forbedringsprogrammet HIS2. I Helse Vest er det etablert nye fora for å bedre samarbeid mellom IT og MTU-miljøer (se nærmere omtale nedenfor).

nye styringsgrupper for informasjonssikkerhet internt, for å sikre ledelsesforankring og tettere oppfølging av dette området.[50]

Avklaring av ansvar for medisinsk-teknisk utstyr

Den opprinnelige undersøkelsen viste at hvordan ansvaret skal fordeles for sikkerheten i medisinsk-teknisk utstyr (MTU), var en problemstilling i alle helseregionene.

MTU anskaffes og eies av helseforetakene, og de regionale IKT-leverandørene hadde et begrenset ansvar for sikkerheten i slikt utstyr. De regionale IKT-leverandørene var i mindre grad involvert i drift av enheter (PCer, servere, mm.) og applikasjoner som understøtter MTU, og sikring av dette ble i stor grad ivaretatt av helseforetakene. Samtidig viste undersøkelsen at den praktiske oppgavefordelingen varierte mye, både mellom regioner og mellom helseforetak i samme region.

Svar fra de regionale helseforetakene viser at alle helseregionene har arbeidet med ansvarsfordelingen for slikt utstyr i etterkant av vår undersøkelse.

Helse Sør-Øst har laget en samhandlingsmodell MTU-IKT som skal brukes ved anskaffelse av nytt MTU og ved behov for endringer i eksisterende utstyr. Samhandlingsmodellen ble vedtatt i 2021. Den består av et sett av tjenestemodeller som beskriver ansvars- og oppgavefordelingen mellom helseforetaket og Sykehuspartner HF når det gjelder drift og forvaltning av IKT-komponentene koblet til ulike typer MTU.[51]

I Helse Vest er «Felles tiltak for økt IKT-sikkerhet for MU og TU» ett av seks regionale prosjekter for forbedring av informasjonssikkerheten (se faktaboks om prosjektene nedenfor). Det er etablert to nye fora for samarbeid: Ett mellom fagmiljøene innenfor Medisinsk utstyr (MU) og IKT, og ett mellom fagmiljøene innenfor Teknisk utstyr (TU) og IKT. Disse foraene skal være samarbeidspunktet mellom helseforetakene og Helse Vest IKT AS. Ifølge RHF-et tilbyr Helse Vest IKT nå forskjellige drifts- og samarbeidsmodeller for å møte de forskjellige behovene som hver virksomhet i Helse Vest har. RHF-et viser i svarbrev også til noen andre tiltak for å bedre samhandlingen mellom fagmiljøene.

For de to siste regionene viser svarene at det gjenstår et noe større arbeid:

- Helse Nord RHF har arbeidet med å avklare roller og ansvar knyttet til ivaretakelsen av sikkerheten MTU bl.a. gjennom oppdrag gitt i *Oppdragsdokument (OD)* og *Styringskrav og rammer* over flere år.[52] RHF-et skriver i svarbrev at fremdriften i arbeidet ikke har vært tilfredsstillende. Regionen startet i 2021 et arbeid med en regional strategi for MTU, og et utkast til strategi ligger ifølge RHF-et til grunn for det regionale MTU-forumets forbedringsarbeid.
- Helse Midt-Norge RHF har arbeidet med en tjenestemodell for MTU, med en tilhørende rolle- og ansvarsmatrise (HUKI-modell) som dekker helseforetak, Hemit og Helseplattformen AS. Ifølge RHF-et er det gjennomført et arbeid for å klassifisere og kategorisere MTU med bakgrunn i Normens veileder for MTU og risikovurderinger for de ulike relevante kategorier av MTU. Første utkast til rolle- og ansvarsmatrise ble ifølge RHF-et for krevende å implementere, og deres fagmiljø på IKT og MTU området er i gang med å forenkle modellen.[53]

2.2.4 Risikostyring og -vurderinger

Oppfølgingsundersøkelsen viser at RHF-ene har fulgt opp departementets krav fra 2022 og 2023 om å samarbeide med Norsk helsenett om å utarbeide årlige rapporter om trusler og trender som

[50] **Sykehuspartner** har innført tre beslutningsnivåer for informasjonssikkerhetsstyringen: Et *Security Governance Board* på høyeste ledernivå (LG1) som utgjør den strategiske ledelsen av arbeidet, et *Information Security Management Board* som er en underliggende styringsgruppe bestående av informasjonssikkerhetsleder og representanter for alle virksomhetsområder, og et Team Information Security Management (ISM) som utfører det operative arbeidet med ledelsessystemet.
[51] Samhandlingsmodell for MTU-IKT
[52] Helse Nord RHF viser i brev til Riksrevisjonen til oppdragsdokumentene fra Helse Nord til helseforetakene for 2021, 2022 og 2023.
[53] RHF-et har lagt ved et eksempel på konkret ansvarsmatrise som miljøene har laget for et avgrenset område: Integrasjon av utstyr for radiologi.

spesialisthelsetjenesten kan bruke i sitt arbeid med risiko- og sårbarhetsvurderinger. I 2023 var trusselvurderingen[54] for første gang utarbeidet for å kunne være offentlig tilgjengelig, blant annet for å kunne nå ut til flest mulig ansatte i sektoren.[55]

Den opprinnelige undersøkelsen viste at de tre RHF-ene som hadde etablert ledelsessystemer for informasjonssikkerhet, som del av disse hadde utarbeidet felles regionale krav til handlinger som skulle sikre at man velger de riktige sikkerhetstiltakene og kontinuerlig og forbedrer informasjonssikkerheten. Dette omfattet blant annet krav til risikovurderinger. Etter at også Helse Midt-Norge har etablert et regionalt ledelsessystem, har nå alle helseregionene dokumenter i sine ledelsessystemer som stiller krav til gjennomføring av risikostyring og -vurderinger.[56]

Den opprinnelige undersøkelsen viste også at det ble gjennomført risikovurderinger ved innføring og endring av IKT-systemer. Vi så nærmere på et utvalg av risikovurderinger av systemer, og fant at en del av disse manglet nærmere omtale av tiltakene som skal iverksettes, hvem som har ansvaret for å gjennomføre tiltakene, og/eller frist for når tiltaket skal være gjennomført.

Vi har i denne omgangen ikke bedt RHF-ene om oversikter over risikoanalyser som er gjennomført, eller konkrete vurderinger som er gjennomført av enkeltsystemer. Vi har ikke undersøkt om systematikken i arbeidet med risikovurderinger har blitt bedre.

Som nevnt har alle helseregionene gjort vurderinger av risiko for sentrale deler av IT-infrastrukturen, i forbindelse med arbeid med å utpeke skjermingsverdige objekter og infrastruktur under den grunnleggende nasjonale funksjonen (GNF) helseberedskap. Departementet utpekte skjermingsverdige verdier hos helseregionene i november 2022. RHF-ene viser i sine svarbrev til at det i etterkant av dette er gjennomført skade- og risikovurderinger, at det er opprettet tiltaksplaner og at arbeidet med risikoreduserende tiltak er i gang. Vi har ikke bedt om å få tilsendt disse.

2.2.5 Helseregionenes arbeid med sikkerhetsrevisjoner, evaluering og kontroll

En viktig kilde for å si noe om sikkerhetstilstanden i helseforetakene er sikkerhetsrevisjoner[57] og andre kontroller[58]. Alle RHF-ene stiller krav til at det gjennomføres sikkerhetsrevisjoner i helseforetakene, og har plassert ansvaret for dette hos helseforetakenes informasjonssikkerhetsledere.[59] Helse Vest og Helse Nord har utarbeidet egne regionale retningslinjer for sikkerhetsrevisjoner i sine ledelsessystemer.

I denne oppfølgingsundersøkelsen har vi bedt RHF-ene gjøre rede for hvilke evalueringer og kontroller som er gjennomført i regi av helseregionene i tiden etter den opprinnelige undersøkelsen ble offentliggjort. Vi har ikke bedt om å få tilsendt dokumentasjon på gjennomførte evalueringer og kontroller fra de enkelte helseforetakene. Som nevnt gjennomfører HelseCERT årlige inntrengingstester mot utvalgte sykehus i hver helseregion. Vi har fått tilsendt rapporter fra inntrengingstestene for 2021–2023 fra alle regionene.

[54] Helse Sør-Øst, Helse Nord, Helse Vest, Helse Midt Norge og Norsk helsenett ved HelseCERT (2023) *Trusselvurdering 2023. Det digitale trusselbildet mot spesialisthelsetjenesten.* Alle helseregionene omtaler også ansvar for gjennomføring av risikovurderinger i ledelsessystemenes dokumenter som beskriver roller og ansvar.

[55] Iflg. Helse Nords styresak-37-2024-informasjonssikkerhet---status-for-arbeidet.pdf (helse-nord.no) ble offentliggjøring ansett som viktig for å enklere kunne nå ut til flest mulig ansatte.

[56] Helse Nord: *Risikovurdering og risikostyring*; Helse Midt-Norge: *Risikostyring av informasjonssikkerhet og personvern i Helse Midt-Norge,* samt tilhørende vedlegg; Helse Vest: *Risikostyring* (retningslinje), *Akseptabel risiko* (policy), *Forenklet risikostyring* (prosedyre) samt tilhørende malverk; Helse Sør-Øst: *Kriterier for vurdering og aksept av risiko innen informasjonssikkerhet (*styrende dokument*)* samt dokumentet *ROS-prosess innen informasjonssikkerhet*, som er del av de regionale bruksvilkårene for informasjonssikkerhet som helseforetakene må akseptere, som Sykehuspartner er ansvarlig for.

[57] Dette kan være revisjoner initiert av IKT-avdelingen (innleid bistand), internrevisjonen i foretaket eller konsernrevisjonen i regionen, ekstern revisor eller Riksrevisjonen

[58] Kontroller initiert av ledelsen i helseforetaket (internkontrolltiltak), fra tilsynsmyndigheter som Datatilsynet og Statens helsetilsyn. Det kan også være tester utført av HelseCERT

[59] Kilde: Helseregionenes ledelsessystemer: dokumenter som beskriver organisering av informasjonssikkerhetsarbeidet.

Evalueringer, kontroller og revisjoner i regi av helseregionene

Helse Nord opplyser at de regionale retningslinjene slår fast det skal gjennomføres 1–2 regionale sikkerhetsrevisjoner årlig, i tillegg til de lokale sikkerhetsrevisjonene som gjennomføres i helseforetakene. I 2023 ble gjennomført en regional sikkerhetsrevisjon av Helse Nord IKTs nettverk.[60] I tillegg ble det samme år gjennomført en inntrengingstest av PAM hos Helse Nord IKT.[61]

Helse Midt-Norge viser til internrevisjonens pågående gjennomføring av GAP-analyser av helseforetakenes etterlevelse av NSMs grunnprinsipper (jf. omtale under 2.2.4).

Helse Vest viser til at det etter den opprinnelige undersøkelsen er gjennomført et tiltak som så på Helse Vest IKTs kapabiliteter på operativt sikkerhetsarbeid, som ledd i arbeidet med etterlevelse av NSMs grunnprinsipper.[62]

Helse Sør-Øst viser til at det er gjennomført flere sikkerhetstester, revisjoner og kontroller i tiden etter den opprinnelige undersøkelsen ble publisert. Blant annet har Konsernrevisjonen gjennomført en revisjon av styringen av informasjonssikkerhet hos Sykehuspartner HF. RHF-et viser også til en rekke revisjoner som er gjennomført av sykehuspartner[63], samt penetrasjonstester av alle tjenester i DMZ.[64]

Inntrengingstester gjennomført av HelseCERT

HelseCERT gjennomfører årlige inntrengingstester i hver av de fire helseregionene. Vi har mottatt rapportene fra testene for årene 2021–2023.

Rapportene viser at metodene anvendt av HelseCERT i stor grad samsvarer med de som vi har brukt i våre inntrengingstester. HelseCERT har i tillegg testet om det finnes sårbare tjenester tilgjengelige fra Internett eller Helsenettet. Hvilke elementer som HelseCERT fokuserer på i inntrengingstestene kan variere noe, og helseregionene kan også gi innspill til hva som skal være fokus. Det kan synes som ressursinnsatsen som legges i inntrengingstestene varierer noe, og at ressursbruken per inntrengingstest var noe lavere i 2023 enn tidligere år.

Omfang og type av funn som omtales i rapportene varierer mellom de ulike testene, men flere av de samme svakhetene som vi peker på finnes også i mange av rapportene til HelseCERT. Svake passord, passord tilgjengelig i klartekst og utstyr med standard passord er for eksempel gjengangere. Det kan observeres forbedringer over tid, hvor det for eksempel i flere regioner er færre brukere med svake passord i senere tid.

Vi ser at HelseCERT har gjort mange av de samme funnene som oss i de to regionene hvor vi har gjennomført dybdeundersøkelse. Dette omtales nærmere i kap. 3.1.3 og 3.2.3.

2.2.6 Tiltak på sentrale områder hvor den opprinnelige undersøkelsen viste svakheter

Lukking av svakheter i IT-infrastrukturen

Alle de fire helseregionene har arbeidet med å lukke svakheter som ble avdekket i tiden etter den opprinnelige undersøkelsen ble publisert. Blant annet utarbeidet de regionale IKT-leverandørene tiltakslister basert på de tekniske funnene allerede i 2020. Mens noen av svakhetene var av en slik art

[60] Regional sikkerhetsrevisjon Nettverk utført av eksterne konsulenter fra PwC
[61] Pentest av PAM utført av Transcendent Group
[62] Arbeidet ble ifølge Helse Vest gjennomført med ekstern konsulent som på basis av The European Union Agency for Cybersecurity (ENISA) sitt CSIRT Maturity Framework gjennomførte intervjuer og kartlegging og leverte en rapport til Helse Vest IKT AS. Helse Vest opplyser videre at Helse Vest IKT AS har avtale med ekstern tredjepart på inntrengningstester, som brukes for mer systemspesifikke penetrasjonstester. Dette har ikke vært brukt for infrastrukturtjenester
[63] Blant annet Sikkerhetsrevisjon av DIPS AS, Ettersyn av Sikkerhetsplattformen, og revisjon av brannmurendringer.
[64] En DMZ eller demilitarisert sone i datanettverk er et fysisk eller logisk subnett som offentliggjør en organisasjons offentlige tjenere mot Internett. Hensikten er å sørge for at hackere ikke skal få tilgang til hele bedriftens nettverk dersom han greier å bryte seg inn på maskinen som er tilgjengelig fra Internett.

at de kunne rettes opp relativt raskt, var andre mer omfattende og ville ta lengre tid å rette opp.[65] Oppfølgingsundersøkelsen i de ut to utvalgte helseregionene viser at det fortsatt gjenstår arbeid for å lukke alle svakheter som ble påpekt i forrige undersøkelse, jf. kapittel 3.

Den opprinnelige undersøkelsen viste at helseregionene allerede den gangen hadde iverksatt flere konkrete tiltak for å forbedre IKT- og informasjonssikkerheten på flere områder, og både Helse Nord og Helse Sør-Øst hadde opprettet større, regionale forbedringsprogrammer som helt eller delvis hadde til formål å bedre informasjonssikkerheten. Oppfølgingsundersøkelsen viser at de to regionene har videreført dette arbeidet. Også Helse Vest og Helse Midt-Norge har etablert konkrete regionale prosjekter etter 2021 (se faktaboks).

Faktaboks 4 Regionale forbedringsprogrammer og -prosjekter

Helse Sør-Øst hadde på gjennomføringstidspunktet for den opprinnelige undersøkelsen etablert ett prosjekt og to store programmer for å forbedre infrastrukturen og styrke informasjonssikkerheten:

- Prosjekt for applikasjonssanering, standardisering og konsolidering (ASK) (2017–2020)
- Program for styrket informasjonssikkerhet, personvern og tilgangsstyring (ISOP) (2017–)
- Program for standardisering og IKT-infrastrukturmodernisering (STIM) (2019–)

ISOP-programmet ble avsluttet i juni 2021, og gjenværende prosjekter (privilegerte tilganger og styrket autentisering) ble overført til STIM.[66] STIM ble avsluttet ved utgangen av 2023, mens Sykehuspartner HF fikk ansvar for det videre arbeidet med modernisering av IKT-infrastruktur.[67]

Helse Nord viste i den opprinnelige undersøkelsen til følgende tre prosjekter:

- Felles innføring av kliniske systemer (FIKS) (2011–2016)
- Mobil digital klinisk arbeidsflyt (MODI)
- Prosjekt for helhetlig informasjonssikkerhet (HIS)

MODI-prosjektet pågikk fortsatt ved inngangen til 2024, mens HIS-prosjektet er etterfulgt av prosjektet Helhetlig informasjonssikkerhet, fase 2 (HIS2). HIS2 omfatter blant annet tilgangsstyring (IAM2), sonemodell for nettverk og bedre deteksjonsevne. Prosjektet var opprinnelig planlagt ferdigstilt i løpet av 2024, men enkelte leveranser skyves til 2025.[68]

I tillegg til dette har Helse Nord i 2022-2023 gjennomført prosjektet Sterk autentisering, som hadde som mål å etablere multifaktorautentisering for all tilgang til Helse Nords IT-ressurser.[69]

Helse Vest har som ledd i oppfølgingen av regional handlingsplan for informasjonssikkerhet etablert seks prosjekter etter 2021:[70]

- Felles tilnærming til NSM 2.0
- Revisjon av regionalt styringssystem for informasjonssikkerhet og personvern
- Videreutvikling av sikkerhetskultur
- Digital plattform (forprosjekt Modernisert sikkerheisarkitektur)
- Felles tiltak for økt IKT–sikkerhet for MU og TU
- Tiltak for økt IKT-sikkerhet for Lokal IKT

Helse Midt-Norge har i tillegg til å arbeide med å lukke tekniske funn fra den opprinnelige undersøkelsen, påbegynt et prosjekt for etablering av styringssystem for informasjonssikkerhet og personvern (planlagt ferdigstilt 1. halvår 2024), gjennomført kartlegging av informasjonssikkerhetskultur (jf. omtale nedenfor) og utarbeidet tjenestemodell for ivaretakelse av sikkerhet i MTU. Helse Midt-Norge har også etablert ny identitets- og tilgangsstyring i forbindelse med innføringen av Helseplattformen.

[65] Helse Midt-Norge rapporterte i Årlig melding for 2021 at et eget prosjekt for lukking av tekniske funn ble sluttført i 2021, men at noen restanser fra prosjektet ble overført til linjen. Helse Nord rapporterte i Årlig melding for 2022 at noe av arbeidet måtte videreføres utover 2022 da «da kompleksitet og omfang er betydelig og må håndteres planmessig og strukturert for å oppnå en akseptabel risikotilstand». Helse Sør-Øst rapporterte i Årlig melding 2022 at tiltakene knyttet til Riksrevisjonens undersøkelse i all hovedsak var gjennomført, mens endelig avslutning av den særskilte oppfølgingen ble besluttet i begynnelsen av 2023 (Kilde svarbrev fra Helse Sør-Øst). Av svarbrevet fra Helse Vest til oppfølgingsundersøkelsen framgår det at de til sammen 33 områdene Helse Vest identifiserte for forbedring ble vurdert som gjennomført eller overført til vanlig drift og kontinuerlig forbedring i 2023.

[66] https://www.helse-sorost.no/49a054/siteassets/documents/styret/styremoter/2020/1126/130-2020-status-og-rapportering-2.tertial-2020-for-stim-og-isop-sp.pdf

[67] https://www.sykehuspartner.no/4aee0c/siteassets/documents/styremoter/122023/styresak-102-2023-oppsummering-program-stim-og-videreforing-av-moderniseringsarbeidet.pdf

[68] https://www.helse-nord.no/4ad5da/siteassets/dokumenter-og-blokker/styret/styremoter/styremoter-2023/20231129/styresak-135-2023-helhetlig-informasjonssikkerhet-fase-2-status-pr.-oktober-2023.pdf

[69] Kilde: Sluttrapport for «Sterk autentisering»

[70] Kilde: Årleg melding 2022 for Helse Vest RHF til Helse- og omsorgsdepartementet

I den opprinnelige undersøkelsen tok vi utgangspunkt i anerkjente standarder for tekniske sikkerhetstiltak, herunder **NSMs grunnprinsipper for IKT-sikkerhet** og CIS Controls, og undersøkte sentrale sikkerhetstiltak anbefalt i disse standardene.

Som vist i kapittel 2.1 stilte departementet i 2021 et konkret krav om at helseregionene skulle fortsette innføringen av NSMs grunnprinsipper for IKT-sikkerhet. Tre av RHF-ene videreførte dette kravet til helseforetakene allerede samme år, mens Helse Midt-Norge ikke nevner grunnprinsippene eksplisitt i sine oppdragsdokumenter til helseforetakene før i 2023.

Per inngangen til 2024 hadde alle helseregionene gjennomført eller planlagt å gjennomføre vurderinger av status for innføring av grunnprinsippene (se faktaboks)

Faktaboks 5 Helseregionenes vurderinger av status for innføring av NSMs grunnprinsipper

Helse Sør-Øst vurderte i 2021 grad av implementering av samtlige 118 tiltak i NSMs grunnprinsipper. De konkluderte med at 111 av dem var implementert tilstrekkelig, 5 ble vurdert til ikke å være relevante, mens de to resterende skulle arbeides videre med.[71]

Helse Vest gjennomførte en kartlegging av mulig gap og etablering av relevante tiltak i Helse Vest IKT og i enkelte foretak i 2021, og iverksatte et eget regionalt prosjekt for innføring av grunnprinsippene som tiltak i den regionale handlingsplanen for informasjonssikkerhet.[72]

Helse Nord har gjennomført en første modenhetsvurdering i regionen med utgangspunkt i grunnprinsippene i 2023, basert på egenrapportering fra det enkelte helseforetak. Helse Nord IKT gjennomførte i den forbindelse en modenhetsvurdering av sikkerheten i den regionale infrastrukturen.[73]

Helse Midt-Norge gjennomførte første tertial 2024 GAP-analyser av etterlevelse av NSMs grunnprinsipper i hvert helseforetak. Det regionale helseforetaket opplyste per september 2024 at helseforetakene arbeider med å lukke gapene som ble identifisert.

Opplæring og bevisstgjøring

Den opprinnelige undersøkelsen viste at manglende etterlevelse av retningslinjer og anbefalinger hos enkelte ansatte var en sentral årsak til at vi fikk kontroll over systemer og tilganger til sensitive opplysninger gjennom angrepssimuleringene. På bakgrunn av dette anbefalte Riksrevisjonen helseforetakene å iverksette tiltak for å sikre at sikkerhetsatferden hos helse- og IKT-personell blir bedre.

Oppfølgingsundersøkelsen viser at alle de fire helseregionene har iverksatt tiltak som har som mål å øke kompetansen og bedre sikkerhetskulturen blant de ansatte i sykehusene:

- Alle regionene har angitt informasjonssikkerhetskompetanse og -kultur som ett av de overordnede tiltaksområdene i sine regionale handlingsplaner for informasjonssikkerhet.[74]
- Alle regionene har gjennomført kartlegginger av informasjonssikkerhetskultur blant ansatte i sykehusene som grunnlag for videre arbeid med egnede tiltak.[75]

[71] Årlig melding for Helse Sør-Øst 2021
[72] Jf. Regional handlingsplan for informasjonssikkerhet i Helse Vest. Fram til 2024 ble det også gjennomført 2 runder med samsvarsvurderinger for NSMs grunnprinsipper i Helse Vest IKT. Helse Vest rapporterer at det fant sted en tydelig forbedring i perioden. Kilde: Vedlegg (U.off.) til styresak Helse Vest 015/24.
[73] Styresak 37–2024 Helse Nord RHF - Informasjonssikkerhet – status for arbeidet.
[74] Helse Sør-Øst, Helse Vest og Helse Nord omtaler det under temaområde Informasjons-sikkerhetskultur og -kompetanse, mens Helse Midt-Norge omtaler det under temaområde Kompetanse, holdninger og kultur». I siste versjon av planen omtaler Helse Nord opplæring og kompetanse under innsatsområde «Sikkerhetskultur og –kompetanse (mennesket)». I siste versjon av planen omtaler Helse Midt-Norge opplæring og kompetanse under tre av de åtte tiltakene.
[75] Helse Sør-Øst har gjennomført årlige kartlegginger fra 2021; Helse Nord og Helse Vest har gjennomført målinger i 2021 og 2023, mens Helse Midt-Norge gjennomførte første kartlegging i 2023. Helse Midt-Norge har dermed kommet kortest i arbeidet, men skriver i brev til Riksrevisjonen at «oppfølging og arbeid med tiltak for å forbedre sikkerhetskulturen gjennomføres foretaksvis. Forslag til tiltak som kan gjennomføres i fellesskap er under arbeid og vil bli lagt frem for beslutning i løpet av T1 2024.»

- Helseregionene Nord, Midt-Norge og Vest opplyser i brev til Riksrevisjonen å ha etablert obligatoriske e-læringskurs i informasjonssikkerhet for alle ansatte i regionen.[76]

Helse Sør-Øst har ikke etablert obligatorisk e-læringskurs i informasjonssikkerhet på regionalt nivå. Det er opp til enkelte helseforetak å avgjøre hvordan opplæring skal gis. Flere helseforetak har imidlertid valgt å ha obligatoriske informasjonssikkerhetskurs. I tillegg tilbyr den regionale IKT-leverandøren Sykehuspartner HF et opplæringsverktøy til helseforetakene for at de ansatte skal bli flinkere til å oppdage og rapportere mistenkelige eposter.

[76] I Helse Vest og Helse Midt-Norge skal kurset gjennomføres årlig, i Helse Nord annethvert år. Helse Vest opplyser at regionen i en årrekke har hatt et obligatorisk e-læringskurs i IKT-sikkerhet. Kurset er revidert og omhandler nå informasjonssikkerhet og personvern. Det er i tillegg utarbeidet et nytt og omfattende kurs som er obligatorisk for personell med utvidede rettigheter.

3 Dybdeundersøkelser av oppfølgingen i to utvalgte HF og RHF

3.1 [redacted]

3.1.1 Inntrengingstesten

Oppsummering

I inntrengingstesten testet vi om vi uten noen rettigheter klarte å få tilgang til helseregionens pasientopplysninger.

I løpet av inntrengingstesten fikk vi tilgang til og kontroll på helseregionens pasientopplysninger via to forskjellige fremgangsmåter. Dette førte til at vi kunne hentet ut store mengder pasientopplysninger, endret data i pasientjournaler ol., eller slettet databaser som medisinske systemer bygger på. Maksimal destruktiv bruk av rettighetene som vi oppnådde, kunne bl.a. satt sykehusets systemer for lagring av pasientdata ut av spill i en lengre periode.

Vi fant to veier som gjorde at vi oppnådde målene med inntrengingstesten. Første fremgangsmåte ga oss lesetilgang og delvis kontroll over helseregionens pasientopplysninger. [redacted]. Andre fremgangsmåte ga oss full kontroll over helseregionens pasientopplysninger [redacted].

Inntrengningstesten viste også at [redacted] har fått på plass et miljø som har ansvar for å oppdage og håndtere uønsket aktivitet. Noen av de aktivitetene vi gjennomførte ble oppdaget, men de fleste av våre aktiviteter ble ikke oppdaget. I det følgende gjør vi i korte trekk rede for hva vi gjorde i inntrengingstesten.

Hvordan vi fikk lesetilgang til helseregionens pasientopplysninger samt full kontroll over noen av helseregionens pasientopplysninger

Første steget på denne veien var å få tilgang til [redacted] nettverk. [redacted].

Med tilgang til nettverket kunne vi skanne dette og få oversikt over hvilke maskiner og tjenester[77] som var tilgjengelig. Skanningen viste at det var en god del maskiner og tjenester som var tilgjengelig for alle brukere, [redacted][78], [redacted][79]. [redacted].

Gjennomgang av tilgjengelige tjenester identifisert i skanningen viste at vi uten å autentisere[80] oss hadde tilgang til et filområde med mye informasjon [redacted]. At det var mulig å koble til uten autentisering skyldes trolig at en oppdatering av programvare inneholdt en feil, som resulterte i at alle brukere i sykehusets nettverk fikk

[77] En tjeneste kan for eksempel være tilgang til en webside eller en database.

[78] [redacted]

[80] Autentisering har som mål å bekrefte identitet når en bruker forsøker å koble seg til en maskin eller tjeneste. En vanlig metode for å autentisere seg er å oppgi et brukernavn og et passord.

tilgang til dette filområdet. Det at alle brukere hadde fått mer tilgang enn de skulle, ble ikke oppdaget etter oppdateringen.

[redacted]. Dette ga oss tilgang til en brukerkonto som hadde lesetilgang til mange databaser i helseregionen som inneholder pasientopplysninger. Vi kunne dermed logge oss på databasene for å hente ut pasientopplysninger.

[redacted]. Med disse kontoene logget vi oss på noen servere som administrator, men vi benyttet ikke denne eller de andre kontiene i særlig grad da vi hadde andre brukerkontoer som vi i stedet benyttet i den videre inntrengningstesten, jf. hvordan vi fikk full kontroll over helseregionens pasientopplysninger omtalt nedenfor.

[redacted].

Hvordan vi fikk full kontroll over helseregionens pasientopplysninger

Første del av denne veien var å identifisere brukernavn for en del ansatte. Ved å finne oppbyggingen av vanlige brukernavn produserte vi lister over mulige brukernavn. Listene over mulige brukernavn ble verifisert mot en tjeneste benyttet av [redacted]. På denne måten fant vi gyldige passord for noen få brukerkontoer.

[redacted][83] [84] [redacted][85].

[redacted][86].

[redacted][87].

[redacted][88].

81 [redacted]
82 [redacted]
83 [redacted]
84 [redacted]
85 [redacted]
86 [redacted].
87 [redacted]
88 [redacted]

[redacted] kunne vi ha logget oss på mange ulike databaser som inneholder pasientopplysninger. Dette omfatter blant annet databasene som ligger til grunn for kurvesystemet Metavision som dokumenterer bruk av legemidler og andre viktige data for innlagte pasienter, og Partus som brukes ved svangerskap og fødsler. [redacted]. Vi hadde imidlertid ikke kontroll på alle medisinske data og ønsket å gå videre.

[redacted]. Vi kunne dermed logge på samtlige databaser med muligheter for å lese, slette eller manipulere pasientopplysninger for hele helseregionen.

En ondsinnet aktør kunne med slik tilgang ha hentet ut nærmest samtlige medisinske data i helseregionens IT-systemer. En slik aktør kunne også ha skapt omfattende problemer for drift av sykehuset ved å gjøre medisinske systemer utilgjengelig for helsepersonell eller manipulere data slik at det ikke ville være mulig å stole på informasjon i systemene.

Hva [redacted] oppdaget i inntrengingstesten

[redacted] har etablert en enhet[89] som har som oppgave å oppdage og håndtere uønsket aktivitet. Denne enheten oppdaget noen av de aktivitetene vi gjennomførte.

Aktiviteter som ble oppdaget var:

- [redacted]
- [redacted]
- [redacted]90
- [redacted]91

[redacted].

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

Inntrengingstesten viser at [redacted] kun oppdaget noen av våre aktiviteter, det meste ble ikke oppdaget. [redacted].

3.1.2 Undersøkelser av tekniske sikkerhetstiltak

For å få et bredere bilde av status og forbedringer i tekniske sikkerhetstiltak siden forrige revisjon, gjennomførte vi i tillegg til inntrengingstesten analyser av tekniske sikkerhetstiltak basert på uttrekk fra utvalgte IT-systemer og innhenting av informasjon. Analysene viser at det er iverksatt flere tiltak som har gitt et høyere sikkerhetsnivå, men at det gjenstår vesentlig arbeid både med hensyn til å rydde

89 [redacted]
90 [redacted]
91 [redacted]

opp i gamle løsninger og å få ønsket effekt av implementerte tiltak. Nedenfor omtaler vi tekniske sikkerhetstiltak fordelt på fem undersøkte områder.

Kontroll med brukerkontoer og tilgangsrettigheter

De fleste dataangrep utnytter brukeres rettigheter og det er derfor viktig å ha god kontroll på brukerkontoer og begrense rettigheter til det som er nødvendig. Dette gjelder spesielt privilegerte kontoer for administrasjon av IT-systemer. [redacted] har innført et system for å bedre kontroll med slike brukerkontoer (PAM)[92], som blant annet innebærer at passord endres hver gang en slik konto har blitt benyttet. Både analyser og inntrengingstest indikerer at systemet fungerer etter sin hensikt og gir bedre sikkerhet, [redacted].

[redacted].

[redacted][93], [redacted].

Funksjonsdeling med tilhørende begrensning av rettigheter kan gjøre det vanskeligere for en angriper å komme videre og utvide sine rettigheter. Dette er i hovedsak innført i [redacted] med for eksempel egne kontoer for klient- og serveradministratorer. [redacted].

Autentisering[94]

Når brukere skal logge seg på en virksomhets IT-utstyr, må de identifisere seg. Tradisjonelt skjer dette ved å oppgi et brukernavn og passord. [redacted] har siden forrige revisjon fått en sikrere identifisering ved at kravene til passord har blitt betydelig sterkere, spesielt med hensyn til at det nå kreves lengre passord. I forrige revisjon ble det funnet svært mange brukerkontoer for ansatte med passord som var enkle å gjette. Sterkere krav førte til at det kun ble funnet en håndfull brukerkontoer for ansatte med svake passord i denne revisjonen.

[redacted].

[redacted].

[92] Privileged Access Management (PAM) er en identitetssikkerhetsløsning som bidrar til å beskytte organisasjoner mot cybertrusler ved å overvåke, oppdage og forhindre uautorisert privilegert tilgang til kritiske ressurser

[93] [redacted]

[94] Autentisering er en prosess for å bekrefte en brukers identitet. Vanligvis oppgir brukeren sin identitet i form av et brukernavn og dette verifiseres ved at det gis et passord og eventuelt en annen faktor (kort, fingeravtrykk, autentiseringsapplikasjon på mobiltelefon etc.)

To-faktor-autentisering er innført i regionen siden forrige revisjon. Ved pålogging på en PC benyttes et kort og en PIN-kode. Hvis en angriper identifiserer en brukerkonto med et svakt passord, er det dermed vanskeligere å få anvendt brukerkontoen. Dermed gir løsningen en bedre sikkerhet. Analysen indikerer at alle brukerkontoer er omfattet av denne løsningen. [redacted].

Nettverkssikkerhet og soneinndeling

En angriper vil ofte forsøke å koble sitt eget utstyr til nettverket til virksomheten som angripes, og det er derfor viktig at det er kontroll med hvilke enheter som tillates å bli koblet til virksomhetens nettverk (NAC-løsning)[95]. [redacted] har innført et slikt system.

[redacted][96].

Med tilgang til nettverket er neste ledd for en angriper å kartlegge dette og deretter å koble seg til tilgjengelig utstyr. Inndeling av nettverk i soner og begrensning av kommunikasjon mellom soner er viktige tiltak for å hindre dette. [redacted] har en sonemodell hvor nettverket deles inn i ulike segmenter med regulering av kommunikasjon mellom segmentene. [redacted]

[redacted]

Sårbarhetsstyring

Sikkerhetsoppdatering av programvare er viktig for å hindre at angripere utnytter kjente sårbarheter i programvare. Analyse av uttrekk og mottatt informasjon viser at sikkerhetsoppdatering av programvare på servere og klienter gjøres mer systematisk enn hva som ble funnet ved forrige revisjon. [redacted].

Herding av programvare kan hindre sårbarheter ved å fjerne unødvendige tjenester og konfigurere programvare på en mest mulig sikker måte. I [redacted] brukes nå standarder fra leverandører og anerkjente organisasjoner for å herde maskiner som settes i drift. [redacted].

[95] NAC-løsning: NAC (Network Access Control) er en løsning som brukes for å sikre at kun godkjente enheter (pc-er, telefoner, medisinsk teknisk utstyr, nettbrett osv.) som tilfredsstiller spesifikke krav vil få tilgang til internt nettverk i sykehus. Dette krever en autentiseringsløsning for enhetene.

[96] [redacted]

[redacted] gjennomfører regelmessig intern sårbarhetsskanning for å identifisere sårbarheter, og funn fra skanningen blir fulgt opp av de ulike fagmiljøene. [redacted] Ekstern sårbarhetsskanning gjennomført av HelseCERT avdekker nå få sårbarheter.

Logging og overvåkning

Siden ikke alle dataangrep kan hindres med sikkerhetstiltak, er det viktig at virksomheter har en evne til å oppdage angrep. Grunnlaget for å oppdage angrep ligger ofte i analyse av logger. Logging i [redacted] er mer systematisk enn ved forrige revisjon i 2019 og det er etablert en sentral loggserver for å analysere logger. [redacted].

[redacted] har etablert en døgnbemannet enhet for overvåkning med dedikert personell. [redacted].

Enheten oppdaget noen av aktivitetene i inntrengingstesten, [redacted].

3.1.3 Informasjonssikkerhetsarbeidet i regionen og helseforetaket

For å få et bedre bilde av informasjonssikkerhetsarbeidet i regionen, har vi i dybdeundersøkelsen også innhentet dokumentasjon fra [redacted] og [redacted], og bedt dem om å svare på noen skriftlige spørsmål.

[redacted] har, som vist i kapittel 2.2, arbeidet med å bedre informasjonssikkerheten i etterkant av vår opprinnelige undersøkelse. Vi ser at det på flere nivåer er jobbet målrettet og systematisk med å forbedre informasjonssikkerheten:

- Siden undersøkelsen har regionen fortsatt arbeidet med å implementere det regionale styringssystemet for informasjonssikkerhet, og jobbet ut ifra en regional handlingsplan for informasjonssikkerhet. Styret i RHF-et har blitt holdt løpende oppdatert på framdrift i arbeidet.
- Regional IKT-leverandør og helseforetakene har fått i oppdrag å utarbeide mer detaljerte planer, og følge opp disse. Vi har fått tilsendt dokumentasjon på slike planer fra [redacted].[97] [98] Styrene i disse to virksomhetene har blitt holdt løpende oppdatert om status på informasjonssikkerhetsarbeidet.[99] [100]
- Regionen har jobbet med å avklare roller og ansvar mellom aktørene på regionalt nivå, og gjennomført mange tekniske tiltak og organisatoriske tiltak (herunder opplæring og bevisstgjøring) for å bedre informasjonssikkerheten.

[97] [redacted]
[98] [redacted]
[99] [redacted]
[100] [redacted]

- Det er bevilget betydelige midler til regionale forbedringsprogrammer [redacted].[101]
- [redacted].[102]
- [redacted].[103] [redacted].[104]
- Det gjennomføres risikovurderinger av informasjonssikkerhet på flere nivåer i helseregionen, herunder bl.a. på foretaksnivå/virksomhetsnivå, og av sentral IT-infrastruktur og regionale systemer.[105]
- Det er gjennomført flere tester av sikkerheten på regionalt hold, både inntrengingstester gjennomført av HelseCERT og tester i egen regi. Det er også gjennomført kartlegging av sikkerhetskulturen i alle helseforetak i regionen.

Likevel viser vår undersøkelse at regionen ikke er i mål. Kartleggingen av tekniske sikkerhetstiltak i denne oppfølgingsundersøkelsen viser at helseregionen har forbedret sikkerheten siden den opprinnelige undersøkelsen. Samtidig er det fortsatt betydelige sikkerhetshull, og vi greide som vist å få kontroll på helseregionens pasientopplysninger i inntrengingstesten via to forskjellige fremgangsmåter.

Vi har gjennomgått skriftlige svar og dokumentasjon fra helseregionen, regional IKT-leverandør og det utvalgte helseforetaket [redacted], og sett dette i sammenheng med de tekniske funnene. På bakgrunn av dette, ser vi to overordnede forklaringer på at regionen tross stor innsats og betydelige investeringer ikke har oppnådd sikkerhetsnivået de ønsker:

- **Regionen har på mange av de undersøkte områdene iverksatt nye, relevante sikkerhetstiltak, men som ennå ikke er fullt ut innført.** Dette gjelder tiltak for økt sikkerhet i autentisering [redacted], og sikring av tilgang til nettverk [redacted]. Ettersom disse tiltakene ikke var fullt ut innført greide vi å omgå dem i vår inntrengingstest. Det er også arbeidet mye med å bygge opp **sikkerhetsovervåking**, men det gjenstår en del før overvåkingen kommer opp på ønsket nivå.
- Mange av tiltakene som er del av de regionale forbedringsprogrammene må innføres lokalt, i et samarbeid mellom regional IKT-leverandør og helseforetak. Det framgår av tilsendt dokumentasjon at det har vært **forsinkelser knyttet til innføring av noen sentrale tiltak** ved [redacted] – hvor vi gjennomførte vår inntrengingstest. [redacted].[106]

101 [redacted]
102 [redacted]
103 [redacted]
104 [redacted]
105 [redacted]
106 [redacted]

- Det har også vært forsinkelser i andre leveranser i [redacted]. Dette skyldes, ifølge styresak i RHF-et, bl.a. ressursmangel i sykehusene.[107] [redacted]
- **Noen sikkerhetstiltak undergraves av at det ikke er ryddet i gamle løsninger.** [redacted]

[redacted][108]

[redacted][109]

[redacted][110]

[redacted]

[redacted][111]

[redacted][112]

Regional IKT-leverandør [redacted] peker selv på etterslep og teknisk gjeld som en stor utfordring. De mener at en del av sikkerhetsutfordringene i dag kan tilskrives tidligere uklare roller og ansvar innenfor informasjonssikkerhetsområdet. De skriver i svarbrev til oss at[113]

> «[redacted] er nå gitt et betydelig klarere ansvar på teknologiområdet. En stor utfordring vil være å operasjonalisere de tildelte oppgavene sett opp mot den økonomiske situasjonen [redacted]. Risikobasert tilnærming står sentralt, for å oppnå slik tilnærming må prioriteringene styres dit effektene er størst. Samtidig må det etableres tydelige beslutningsprosesser som ivaretar god beslutningsstøtte og rask håndtering av identifiserte utfordringer.»

[redacted]

107 [redacted]
108 [redacted]
109 [redacted]
110 [redacted]
111 [redacted]
112 [redacted]
113 [redacted]

[redacted].[114]

[redacted] informasjon om egne svakheter og konsekvenser av disse

Skriftlige svar og styresaker i RHF-et og [redacted] viser at regionen har vært klar over mange av de gjenstående svakhetene i sikringen av IT-infrastrukturen.[115]

En gjennomgang av sluttrapportene for 2021, 2022 og 2023 viser at HelseCERT har sett mange av de samme svakhetene som vi har gjort i vår inntrengingstest. Vi observerer imidlertid at HelseCERT i enkelte tilfeller stanser tidligere enn vi har gjort i våre tester. Dette gjelder særlig 2023-testen:

- [redacted]
- [redacted]

Når det gjelder den siste testen, ser det ut til at valg av lokasjon også har spilt inn på resultatene. [redacted]

[redacted] har også gjennomført andre revisjoner med tekniske testaktiviteter. [redacted].[116] [redacted]

- [redacted]
- [redacted].[117]

[redacted].

[redacted]

114 [redacted]
115 [redacted]
116 [redacted]
117 [redacted]

[redacted].[118]
[redacted].

[redacted] arbeid med andre sikkerhetstiltak, inkl. tiltak som gjennomføres lokalt i helseforetakene

Våre inntrengingstester og gjennomgang av tekniske sikkerhetstiltak i denne oppfølgingsundersøkelsen dekker ikke alle sikkerhetstiltak som regionen har gjennomført siden vår opprinnelige undersøkelse.

Sikkerhetsnivået vil også bl.a. avhenge av en rekke organisatoriske tiltak, herunder opplæring og kompetanseheving innen informasjonssikkerhet. Noen slike regionale tiltak er omtalt tidligere under kapittel 2.2.

Det er også gjennomført tiltak i det enkelte helseforetak. Som nevnt over har [redacted] utarbeidet en egen lokal handlingsplan for informasjonssikkerhet for [redacted].[119]

Områdene omfatter en rekke tiltak som implementering av regionale retningslinjer, utarbeidelse og implementering av lokale retningslinjer eller rutiner, samt innføring av konkrete tekniske sikkerhetstiltak. [redacted] opplyser i brev at planen er til revidering i 2024, og at den nye planen vil disponeres etter/knyttes opp mot NSMs grunnprinsipper.

3.2 [redacted]

3.2.1 Inntrengingstesten

Oppsummering

I inntrengingstesten testet vi om vi uten noen rettigheter klarte å få tilgang til helseregionens pasientopplysninger.

I løpet av inntrengingstesten fikk vi tilgang til helseregionens pasientopplysninger gjennom vanlig brukertilgang. Det viste seg å være enkelt å få tilgang til mange brukernavn og passord. [redacted] få tilgang til et passord som gjorde at vi kunne logge på som en bruker i journalsystemet og legge inn eller endre data om pasienter som sykepleiere eller leger. Da vi gjennomførte denne delen av inntrengingstesten ved å bevisst gå forsiktig fram, ble dette ikke oppdaget av [redacted].

Vi fikk også tilgang til å administrere kritiske servere og databaser på linje med [redacted] ansatte i løpet av inntrengingstesten. [redacted][120] [redacted].

[118] [redacted]
[119] [redacted]
[120] [redacted]

[redacted], ville det ha gitt oss mulighet til å hente ut, lagre, slette eller manipulere pasientopplysninger i journalsystemet.

Hele nettverket hvor medisinsk-teknisk utstyr (MTU) er tilkoblet, var unntatt fra inntrengningstesten. Dette har bakgrunn i at utstyret er kritisk for pasientsikkerheten og risikoen for at aktiviteter i inntrengingstesten kunne påvirke utstyret. Testen vil derfor ikke si noe om sikkerheten til MTU og tilhørende IT-utstyr. I vår opprinnelige rapport omtalte vi særskilt sikkerhetsrisiko knyttet til MTU ved at utstyret har lang levetid og at leverandørene av utstyret ofte har hatt mindre oppmerksomhet på IT-sikkerhet, for eksempel sikkerhetsoppdateringer.

Inntrengningstesten viste også at [redacted] med god kapasitet og kompetanse til å oppdage og håndtere sikkerhetshendelser. Dette ble vist under inntrengningstesten da de var i stand til å stoppe flere av våre angrep gjennom oppfølging av alarmer og analyse av hendelser.

I det følgende gjør vi i korte trekk rede for hva vi gjorde i inntrengingstesten.

Hvordan vi fikk tilgang til pasientopplysninger som følge av svake passord

For å legge et grunnlag for å kunne få tilgang til helseregionens systemer identifiserte vi i forkant av inntrengingstesten en rekke brukernavn for ansatte. Ved å finne oppbyggingen av vanlige brukernavn produserte vi lister over mulige brukernavn. Listene over mulige brukernavn ble verifisert mot tjenester benyttet av [redacted]. [redacted] Vi hadde dermed gyldig brukernavn til en stor andel av ansatte på [redacted].

Vi trengte deretter tilgang til nettverket [redacted]. [redacted].

Da vi hadde tilgang til nettverket kunne vi skanne dette og få oversikt over hvilke maskiner og tjenester[121] som var tilgjengelig. [redacted][122], [redacted][123]. [redacted]. Vi valgte her å skanne alle IP-adresser med unntak av nettverket med MTU-utstyr, og mot flere porter. Dette er en aggressiv måte å skanne på. [redacted].

[redacted] Vi logget på med en av de kompromitterte brukerne og tilhørende passord. Vi hadde dermed tilgang til journalsystemet som leger eller sykepleiere. [redacted].

[redacted]

[121] En tjeneste kan for eksempel være tilgang til en webside eller en database.
[122] [redacted]
[123] [redacted]

[redacted]

[redacted]

[redacted]

Hvordan vi fikk tilgang til kritiske servere og databaser

[redacted]

[redacted]

[redacted]

[redacted]. Dette ga oss tilgang til kritiske databaser. Vi hadde dermed mulighet til å lese, skrive og slette data i en rekke databaser med pasientopplysninger. Denne aktiviteten ble ikke alarmert eller oppdaget av [redacted].

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Hva [redacted] oppdaget i inntrengingstesten

Våre inntrengingstester gjennomføres på begrenset tid, hvor vi i løpet av denne tiden forsøker å finne flest mulig svakheter. Aktivitetene i testene skaper en del «støy» som kan oppdages i sikkerhetsovervåkningen i en virksomhet.

[redacted] har høy kompetanse til å oppdage og håndtere sikkerhetshendelser. Således oppdaget og alarmerte [redacted] en rekke aktiviteter i inntrengingstesten. I en reell situasjon ville [redacted] ha gjennomført tiltak for å hindre videre angrep, for eksempel låse brukerkontoer, blokkere arbeidsstasjoner og eskalere situasjonen for å få flere ressurser. Enkelte av disse tiltakene ville ha stoppet angrep. Andre tiltak hadde det vært mulig å omgå, men ville ha forsinket oss. [redacted].

Noe aktivitet ble tatt raskt av alarmer, mens flere aktiviteter ble oppdaget gjennom analyse på bakgrunn av alarmene. Dette viser at [redacted] gjør gode analyser med utgangspunkt i alarmer og kan rekonstruere hvordan angrep er gjennomført i etterkant. Responstid vil naturligvis være lenger for aktiviteter hvor [redacted] er avhengig av analyser for å oppdage aktiviteter.

[redacted]. Det er dog viktig å understreke at ikke alle aktivitetene vi gjorde skal være mulig å alarmere eller oppdage, da noen av aktivitetene som gjøres i en inntrengingstest er nær normal brukeradferd og forventes ikke å bli oppdaget.

3.2.2 Undersøkelser av tekniske sikkerhetstiltak

For å få et bredere bilde av status og forbedringer i tekniske sikkerhetstiltak siden forrige revisjon, gjennomførte vi i tillegg til inntrengingstesten analyser av tekniske sikkerhetstiltak basert på uttrekk fra utvalgte IT-systemer og innhenting av informasjon. Analysene viser at det er iverksatt flere tiltak som har gitt et høyere sikkerhetsnivå, men at det fortsatt er svakheter på noen områder som med enkle midler kan utnyttes av en angriper. Nedenfor omtaler vi tekniske sikkerhetstiltak fordelt på fem undersøkte områder.

Kontroll med brukerkontoer og tilgangsrettigheter

De fleste dataangrep utnytter brukeres rettigheter og det er derfor viktig å ha god kontroll på brukerkontoer og begrense rettigheter til det som er nødvendig.

[redacted][128],
[redacted].

[redacted].

[128] [redacted]

Privilegerte kontoer for administrasjon av IT-systemer er særskilt viktig å beskytte. [redacted] har innført et system for å styre, dokumentere og kontrollere bruk av slike brukerkontoer (PAM).[129] [redacted].

Jo flere brukerkontoer som gis rettigheter til å administrere IT-systemer, jo høyere blir risikoen for at en angriper kan utnytte en av disse. Samtidig må administratorer av IT-systemer få tildelt tilstrekkelige rettigheter til å utføre sine oppgaver. [redacted].

Funksjonsdeling med tilhørende begrensning av rettigheter kan gjøre det vanskeligere for en angriper å komme videre og utvide sine rettigheter. [redacted].

Autentisering[130]

Når brukere skal logge seg på en virksomhets IT-utstyr, må de identifisere seg. Dette skjer ofte ved å oppgi et brukernavn og passord. [redacted]. Mange brukere har dermed valgt passord som er enkle å gjette. Som en konsekvens var det i inntrengingstesten enkelt å finne passord for brukerkontoer for leger, sykepleiere mv. og derigjennom få tilgang til pasientopplysninger. [redacted]

[redacted].

Servicekontoer og privilegerte kontoer for administratorer har strengere krav til autentisering. Mange av passordene til slike kontoer synes heller ikke å bestå av ord, men av tilfeldig genererte tegn. Det er derfor svært vanskelig å gjette eller knekke slike passord. [redacted].

Nettverkssikkerhet og soneinndeling

Det er viktig med systemer som sikrer at kun godkjente enheter tillates å bli koblet til virksomhetens nettverk (NAC-løsning)[131]. [redacted]

[129] Privileged Access Management (PAM) er en identitetssikkerhetsløsning som bidrar til å beskytte organisasjoner mot cybertrusler ved å overvåke, oppdage og forhindre uautorisert privilegert tilgang til kritiske ressurser

[130] Autentisering er en prosess for å bekrefte en brukers identitet. Vanligvis oppgir brukeren sin identitet i form av et brukernavn og dette verifiseres ved at det gis et passord og eventuelt en annen faktor (kort, fingeravtrykk, autentiseringsapplikasjon på mobiltelefon etc.)

[131] NAC-løsning: NAC (Network Access Control) er en løsning som brukes for å sikre at kun godkjente enheter (pc-er, telefoner, medisinsk teknisk utstyr, nettbrett osv.) som tilfredsstiller spesifikke krav vil få tilgang til internt nettverk i sykehus. Dette krever en autentiseringsløsning for enhetene.

[redacted][132].

Når en angriper har fått tilgang til nettverket, er neste ledd å kartlegge nettverket og deretter å koble seg til tilgjengelig utstyr. Inndeling av nettverk i soner og begrensning av kommunikasjon mellom soner er viktige tiltak for å hindre dette.

[redacted] har en sonemodell hvor nettverket deles inn i ulike segmenter med regulering av kommunikasjon mellom segmentene. Skanning av nettverk i inntrengingstesten og analyse av mottatt informasjon, viser at det har blitt gjennomført forbedringer i implementeringen av sonemodellen siden forrige revisjon. Det var i inntrengingstesten vanskelig å nå kritiske servere på grunn av denne segmenteringen. [redacted].

Sårbarhetsstyring

Sikkerhetsoppdatering av programvare er viktig for å hindre at angripere utnytter kjente sårbarheter i programvare. Analyse av uttrekk og mottatt informasjon viser at sikkerhetsoppdatering av programvare på servere i relativt stor grad er automatisert og skjer regelmessig. [redacted].

[redacted]

Herding av programvare kan hindre sårbarheter ved å fjerne unødvendige tjenester og konfigurere programvare på en mest mulig sikker måte. [redacted] brukes standarder fra leverandører og anerkjente organisasjoner for å herde maskiner som settes i drift. Denne herdingen er i stor grad automatisert.

[redacted] har forbedret sårbarhetsskanning siden den opprinnelige revisjonen og gjennomfører regelmessig intern sårbarhetsskanning for å identifisere sårbarheter. [redacted].

Logging og overvåkning

Siden ikke alle dataangrep kan hindres med sikkerhetstiltak, er det viktig at virksomheter har evne til å oppdage angrep. Grunnlaget for å oppdage angrep ligger ofte i analyse av logger. Det gjennomføres omfattende sikkerhetslogging [redacted], og det er etablert en sentral loggserver for å analysere logger. Grunnlaget for å finne ut av hva som har skjedd ved en sikkerhetshendelse er dermed godt.

[redacted] har over lenger tid utviklet [redacted] med høy kompetanse til å oppdage og håndtere sikkerhetshendelser. [redacted]

[redacted]

[132] [redacted]

[redacted].

3.2.3 Informasjonssikkerhetsarbeidet i regionen og helseforetaket

For å få et bedre bilde av informasjonssikkerhetsarbeidet i regionen, har vi i dybdeundersøkelsen innhentet dokumentasjon fra [redacted], og bedt dem om å svare på noen skriftlige spørsmål.

[redacted] har, som vist i kapittel 2.2, arbeidet med å bedre informasjonssikkerheten i etterkant av vår opprinnelige undersøkelse. Vi registrerer at:

- Siden undersøkelsen har regionen fortsatt arbeidet med å implementere det regionale styringssystemet for informasjonssikkerhet, og jobbet ut ifra en regional handlingsplan for informasjonssikkerhet. Styret i RHF-et har blitt holdt løpende oppdatert på framdrift i arbeidet.
- Regionen har jobbet med å avklare roller og ansvar mellom aktørene på regionalt nivå. [redacted].
- Det er også gjennomført mange tekniske tiltak og organisatoriske tiltak (herunder opplæring og bevisstgjøring) for å bedre informasjonssikkerheten. [redacted] har jobbet ut ifra en egen handlingsplan (med mål innenfor kultur, prosess, organisasjon, teknologi), [redacted].

  Styret i [redacted] fikk regelmessige oppdateringer om arbeidet med de tekniske tiltakene fram til slutten av 2021. Etter dette har styret blitt orientert overordnet om informasjonssikkerhetsrisiko hvert tertial i virksomhetsrapportene.
- Det er bevilget betydelige midler til regionale forbedringsprogrammer [redacted]. Disse inneholdt bl.a. tiltak for modernisering og sikring av nettverk, tiltak for sikring av privilegerte tilganger, standardisering samt utfasing av eldre systemer.
- [redacted] gjennomførte et arbeid med innføring av og rapportering på NSMs grunnprinsipper i [redacted].
- Det gjennomføres risikovurderinger av informasjonssikkerhet på flere nivåer i helseregionen, herunder bl.a. på foretaksnivå/virksomhetsnivå, og av sentral IT-infrastruktur og regionale systemer.[133]
- Det er gjennomført revisjoner og tester av sikkerheten i [redacted] og regionen. I tillegg har HelseCERT gjennomført inntrengingstester i 2021 og 2023. [redacted] oppgir også å ha tatt i bruk HelseCERTs hurtigtest. Det er også gjennomført kartlegging av sikkerhetskulturen i alle helseforetak i regionen.

Våre tekniske tester viser at dette har gitt resultater, og at [redacted] har forbedret seg på flere av områdene vi undersøkte i 2019. Dette gjelder særlig modernisering og implementering av sonemodell for nettverket, mer systematisk sårbarhetsskanning, bedre sikkerhetsovervåkning, og opprydding f.eks. av gamle domener, felleskontoer og delte filområder.

Samtidig er det fremdeles svakheter på flere områder: Dette gjelder spesielt autentisering av brukere, der undersøkelsen viser at mange brukere har svake passord [redacted]

[133] [redacted]

[redacted]

[redacted]

[redacted]

Som nevnt ovenfor gjennomførte [redacted] et arbeid med NSMs grunnprinsipper for IT-sikkerhet. [redacted][134] [redacted][135] [redacted].

Ut fra dokumentasjonen vi har mottatt kan vi ikke se om implementeringen av grunnprinsippene har blitt systematisk fulgt opp i ettertid. Vi kan heller ikke se at styret er forelagt flere saker om dette.

[redacted].

[redacted] informasjon om egne svakheter og konsekvenser av disse

Skriftlige svar og styresaker i [redacted] viser at regionen har vært klar over mange av de gjenstående svakhetene i sikringen av IT-infrastrukturen. Både HelseCERT og [redacted] har gjennomført tester/revisjoner som har avdekket svakheter.

HelseCERT gjennomførte ikke inntrengingstester i [redacted] i 2022, og i 2021 var testen begrenset til tjenester tilgjengelig fra Internett og kartlegging av sårbarheter på bærbar klientmaskin. I 2023 fant HelseCERT flere svakheter som samsvarer med våre funn i denne revisjonen. [redacted].

[redacted] gjennomfører også jevnlige revisjoner av informasjonssikkerhet. Hovedfokus i disse revisjonene er etterlevelse av rutiner og retningslinjer på utvalgte områder, men det er også gjennomført revisjoner rettet mot sikkerhetskultur og kontroll av underleverandør. Resultatene fra revisjonene blir behandlet i ledermøter i [redacted] og oppfølgingsansvar blir delegert.

134 [redacted].

135 [redacted]

De har også gjennomført flere oppfølgingsrevisjoner for å se på om avvik som ble funnet er utbedret. [redacted].[136] Funn i oppfølgingen av avvik funnet i revisjoner illustrerer at det kan ta tid å få gjennomført forbedringer i [redacted].

[redacted] arbeid med andre sikkerhetstiltak, inkludert tiltak som gjennomføres lokalt i helseforetakene

Våre inntrengingstester og gjennomgang av tekniske sikkerhetstiltak i denne oppfølgingsundersøkelsen dekker ikke alle sikkerhetstiltak som regionen har gjennomført siden vår opprinnelige undersøkelse.

Sikkerhetsnivået vil også bl.a. avhenge av en rekke organisatoriske tiltak, herunder opplæring og kompetanseheving innen informasjonssikkerhet. Noen slike regionale tiltak er omtalt tidligere under kapittel 2.2. [redacted].

[redacted].[137]

[redacted] opplyser videre at informasjonssikkerhet har fått større oppmerksomhet og antall ressurser og kompetansen hos de som har informasjonssikkerhet som sin oppgave, har økt. Dette omfatter også ledelsen hvor informasjonssikkerhet har vært tema i de månedlige ledermøtene for å øke kompetansen og digital modenhet i ledelsen. Andre konkrete tiltak er:

- etablert porteføljestyring for mer helhetlig og systematisk oppfølging av teknologiporteføljen som også inkluderer prioritering og risikovurdering
- etablert et sikkerhetsnettverket i [redacted] som blant annet gjennomfører presentasjon av årets trusselvurderinger
- gjennomført omfattende sanering av eldre systemer
- etablert nye systemer som Microsoft 365 med nye og bedre aktive sikkerhetstiltak
- endret passord-policy i samarbeid med [redacted]

[redacted].

3.3 Noen forskjeller mellom regionenes sikring av IT-infrastrukturen

Vi har gjennomgått tekniske sikkerhetstiltakene innenfor fem områder, for hver av de to utvalgte helseregionene. På bakgrunn av dette har vi gjort en sammenligning av de to regionene. Vi har sammenstilt dette i tabellen nedenfor.

136 [redacted]

137 [redacted].

[redacted]

Tabellen viser at det er noen likheter mellom regionene for eksempel i forbedring av sårbarhetsstyring siden forrige revisjon. [redacted]. Tabellen illustrerer imidlertid også at det er klare forskjeller mellom utfordringene regionene har med hensyn til tekniske sikkerhetstiltak:

- [redacted] har innført to-faktor-autentisering for vanlige brukere, som gjør det vanskeligere for en angriper å få kontroll over en vanlig brukerkonto til for eksempel en lege eller sykepleier. [redacted] svake passord gjør at det er lett å kompromittere vanlige brukerkontoer for en angriper.
- [redacted].
- [redacted] har et veletablert miljø for sikkerhetsovervåkning som gjennom alarmer og logganalyser oppdager mange angrep. [redacted] har etablert sikkerhetsovervåkning, men har fortsatt en vei å gå med hensyn til å profesjonalisere dette slik at flere hendelser oppdages og håndteres på en god måte.

[138] [redacted]

4 Referanseliste

Regelverk

- Normen – Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren versjon 6.1 Vedtatt: 21. november 2022

Rapporter

- Riksrevisjonen (2020) *Riksrevisjonens undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer. Rapportvedlegg til Dokument 3:2 (2020−2021)*
- Helse Midt-Norge RHF, Helse Nord RHF, Helse Vest RHF, Helse Midt-Norge RHF (2023) *Felles plan 2023. IKT-utvikling og digitalisering*
- Helse Sør-Øst, Helse Nord, Helse Vest, Helse Midt Norge og Norsk helsenett ved HelseCERT (2023) *Trusselvurdering 2023. Det digitale trusselbildet mot spesialisthelsetjenesten*

Stortingsdokumenter

- Meld St. 5 (2023–2024) *En motstandsdyktig helseberedskap. Fra pandemi til krig i Europa*.
- Prop. 1 S (2021–2022) Helse- og omsorgsdepartementet
- Prop. 1 S (2022–2023) Helse- og omsorgsdepartementet
- Prop. 1 S (2023–2024) Helse- og omsorgsdepartementet

Styringsdokumenter

- Protokoller fra Helse- og omsorgsdepartementets foretaksmøter med de regionale helseforetakene
- Protokoller fra styremøtene i de regionale helseforetakene, Helseforetakene og IT-leverandørene
- Oppdragsdokument til Norsk helsenett SF
- Protokoller fra Helse- og omsorgsdepartementets foretaksmøter med Norsk helsenett SF

Veiledere

- Nasjonal sikkerhetsmyndighet (2017) *Rammeverk for håndtering av IKT-sikkerhetshendelser.* Veileder publisert på direktoratets nettsider. [Hentedato 28. mai 2024]

Brev, notater og nettkilder

- Direktoratet for e-helse (2022) *Innspill til kommende stortingsmelding om helseberedskap –Digital sikkerhet*.
- Direktoratet for e-helse (2023) *TB2023-9 Digital sikkerhet – anbefaling til prioriterte tiltak. Oppfølging av direktoratets innspill til den kommende helseberedskapsmeldingen.*
- Helse- og omsorgsdepartementet (2024*) Treårsoppfølging - helseforetakenes forebygging av angrep mot sine IKT-systemer.* Brev til Riksrevisjonen 12. mars 2024.
- Norsk helsenett (u.å.) *HelseCERT og KommuneCERT.* [Hentedato 10.04.2024].