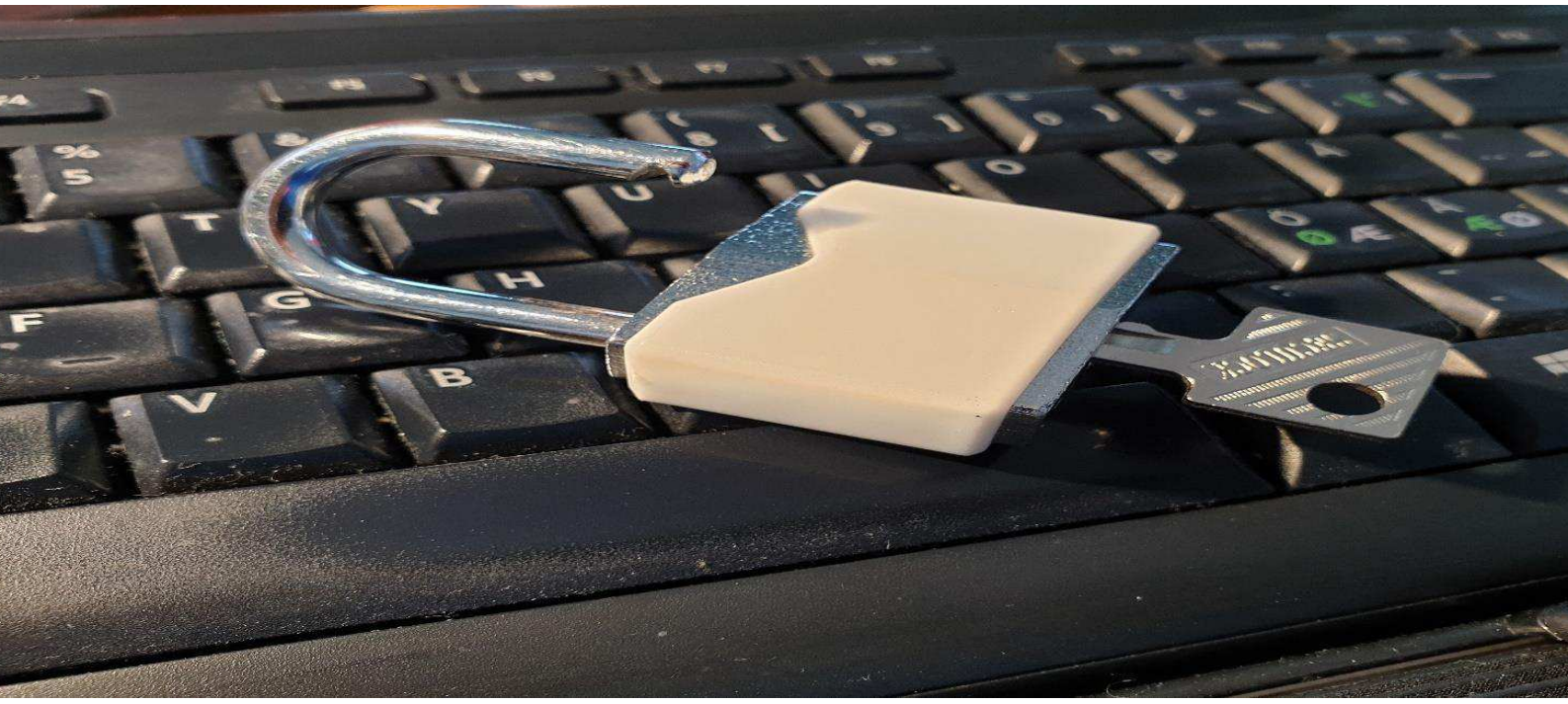
Riksrevisjonen

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

Rapportvedlegg til Dokument 3:2 (2020-2021)



8 Vurderinger

Dagens moderne sykehus digitaliseres i økende grad, og informasjons- og kommunikasjonsteknologi (IKT) benyttes i de fleste sentrale oppgaver på et sykehus. Dette gir grunnlag for økt kvalitet i pasientbehandlingen. Samtidig fører det til at sårbarheten ved bortfall eller feil i IKT-tjenester øker. Pasienter og innbyggere skal kunne ha tillit til at opplysninger ikke kommer på avveie og at uvedkommende ikke får tilgang.

Undersøkelsen viser at det i alle helseregioners IKT-infrastruktur er vesentlige sårbarheter som kan utnyttes med metodene som er benyttet i Riksrevisjonens angrepssimulering. I tre av helseregionene førte vår angrepssimulering til at vi fikk høy grad av kontroll over viktige IKT-systemer, og derigjennom tilganger som kunne utnyttes til å volde stor skade.

Undersøkelsen har avdekket vesentlige svakheter i grunnleggende tekniske sikkerhetstiltak i alle de fire helseregionene. Det varierer mellom regionene på hvilke områder svakhetene ligger, men alle steder kan de utnyttes av angripere. Undersøkelsen viser også at svakheter i tekniske sikkerhetstiltak henger sammen med helseregionenes sikkerhetsorganisering og -styring, og sikkerhetsatferden blant helse- og IKT-personell.

De fleste utfordringene kunne etter vår vurdering vært løst med dagens IKT-løsninger. Det er i alle regioner et etterslep av oppgaver på sikkerhetsområdet. Noen av de viktigste tiltakene krever systematisk arbeid over tid, og gode prioriteringer i den daglige driften.

Alle de fire helseregionene har problemer med å imøtekomme sentrale krav til informasjonssikkerhet stilt i lov og forskrift. Regionenes tekniske og organisatoriske tiltak er etter vår vurdering ikke tilstrekkelige for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen. Videre er sensitive opplysninger ikke tilstrekkelig sikret i henhold til kravene i helseregisterloven, helsepersonelloven og pasientjournalloven. De påviste svakhetene i styringen av området står heller ikke i samsvar med betydningen IKT har for sykehusdriften.

Et dataangrep kan få store konsekvenser for pasientbehandlingen og dermed true pasientsikkerheten. Selv om oppmerksomheten om informasjonssikkerhet har økt i helseregionene, og det er iverksatt flere tiltak de siste årene, er det mye arbeid som gjenstår før IKT-sikkerheten er betryggende.

8.1 De simulerte dataangrepene ga høy grad av kontroll over IKT-infrastrukturen i tre av fire helseregioner, og tilgang til store mengder sensitive pasientopplysninger i alle helseregioner

Helsepersonell som trenger informasjonen må få tilgang til den raskt og enkelt, og kunne stole på at opplysningene er korrekte, oppdaterte og fullstendige. Pasienter og innbyggere skal kunne ha tillit til at opplysninger ikke kommer på avveie og at uvedkommende ikke får tilgang.

Målet i angrepssimuleringen var å ta kontroll over mest mulig av den regionale IKT-infrastrukturen, samt å få tilgang til sensitive opplysninger. I [redacted] fikk vi en høy grad av kontroll over viktige IKT-systemer, og derigjennom tilganger som kunne utnyttes til å volde stor skade. Med de tilganger som vi oppnådde i disse tre helseregionenes systemer, kunne en reell angriper blant annet ha:

- stjålet store mengder sensitive helse- og personopplysninger
- slettet eller utilgjengeliggjort opplysninger som er nødvendige for pasientbehandlingen
- stoppet og utilgjengeliggjort systemer og utstyr som er kritisk for driften av sykehusene
- manipulert opplysninger om pasientene

I [redacted] fikk vi mindre grad av kontroll over IKT-systemene, men kontroll over mange av regionens PCer. Disse kan brukes for videre angrep.

De simulerte angrepene viser også at en angriper kan gjøre betydelig skade selv uten høy grad av kontroll over IKT-systemene. I alle helseregioner fant vi store mengder sensitive opplysninger som var tilgjengelige for alle ansatte.

Ett av formålene med simulering av dataangrep var å undersøke helseregionens evne til å oppdage aktiviteter i dataangrep. Det ble derfor ikke gjort forsøk på å skjule aktivitetene. Riksrevisjonen genererte mye nettverkstrafikk og la igjen kjente tegn på angrep, som burde kunne oppdages i regionenes overvåkning. Aktivitetene i angrepene ble i varierende grad oppdaget av helseregionene. [redacted] oppdaget flere av aktivitetene i angrepssimuleringen, mens de andre tre oppdaget mindre eller ingenting. En profesjonell angriper som går mer forsiktig fram vil redusere sannsynligheten for å bli oppdaget.

I simuleringen ble det brukt velkjente verktøy, som er tilgjengelige for alle på åpne nettsider. Angrepssimuleringen illustrerer dermed hva som er mulig for andre, som for eksempelvis misfornøyde pasienter eller ansatte med visse IKT-kunnskaper, eller enkeltstående hackere som ønsker å vise fram sine kunnskaper. Avanserte aktører - som etterretningstjenester og organiserte kriminelle - vil ha tilgang til et enda større utvalg av verktøy, de kan tillate seg å bruke mer tid på å skjule sine spor og kan ha muligheter til å utnytte sårbarheter som ikke er allment kjent. De kan dermed enklere skaffe seg kontroll med IKT-infrastrukturen med mindre risiko for å bli oppdaget.

[redacted]

[redacted]

Helseregionene har heller ikke gjort nok for å begrense angriperes mulighet til å gjøre skade dersom de først har lyktes med å komme inn, [redacted] «Skallet» som skal sikre mot angrep fra Internett, har blitt hardere de senere årene. Imidlertid har de tekniske sikkerhetstiltakene innenfor dette «skallet» fortsatt vesentlige svakheter.

Etter vår vurdering viser dette at helseregionenes IKT-systemer ikke er beskyttet godt nok mot vesentlige tap av helseopplysninger eller manipulasjon av systemer og utstyr. Dersom helseopplysninger eller IKT-systemer manipuleres eller gjøres utilgjengelige, kan det forårsake pasientskader. Helseopplysninger på avveie kan få alvorlige konsekvenser for helseforetak og pasienter i form av tapt tillit, uønsket eksponering, identitetstyveri, utpressing mm. Dataangrep kan også få betydelige økonomiske konsekvenser.

8.2 I alle fire helseregioner er det vesentlige svakheter i grunnleggende tekniske sikkerhetstiltak som skal forebygge og oppdage dataangrep

Helseregionene skal gjennomføre tekniske sikkerhetstiltak for å oppnå en egnet sikring av sine IKT-systemer og opplysningene lagret i dem. Tekniske sikkerhetstiltak skal primært bidra til å forebygge at dataangrep lykkes, men man må også ha tiltak for å oppdage de angrep man ikke klarer å forebygge.

Resultatene av angrepssimuleringen viser at sentrale sikkerhetstiltak har vært utilstrekkelige for å forebygge og oppdage dataangrep i alle helseregioner. I undersøkelsen er seks sentrale

sikkerhetstiltak basert på blant annet Nasjonal sikkerhetsmyndighets (NSM) grunnprinsipper for IKT-sikkerhet lagt til grunn. Resultatene fra kontrollen av sikkerhetstiltakene er som følger:

1. **Mangelfull kontroll med enheter og programvare**: Helseregionene mangler en fullgod oversikt over maskiner og programvare i egne nettverk, som er en forutsetning for å sikre disse. [redacted] Mangelfull kontroll med enheter og utstyr gjør det mulig for en angriper å kjøre programvare, inkludert angrepsverktøy, i helseregionenes nettverk fra angripers egen PC eller fra helseregionenes maskiner.

2. **Svak kontroll med brukerkontoer og tilgangsrettigheter:** Det brukes mange svake passord både i helseforetakene og hos IKT-leverandørene, som gjør det enkelt for en angriper å knekke passord og få mulighet til å logge inn som ulike brukere. Når mange brukerkontoer i tillegg gis mer rettigheter enn det som følger av tjenstlige behov, er det enklere for en angriper å få kontroll med systemer. Det er videre funnet flere tilfeller der personopplysninger, inkludert sensitiv informasjon om pasienter, er tilgjengelig for alle ansatte i en helseregion. Tofaktor-autentisering er en forbedring for å sikre kontroll med hvem som logger på IKT-infrastrukturen som er tatt i bruk i flere helseregioner, men dette dekker ikke alle situasjoner og den ønskede bedringen i sikkerhet oppnås dermed ikke i mange tilfeller.

3. **Mye utstyr og programvare er ikke sikkert konfigurert:** Mange av helseregionenes maskiner er ikke konfigurert på en sikker måte. Det kan for eksempel bety at usikre metoder for å kommunisere med maskinen ikke er fjernet, unødvendig programvare ikke er fjernet eller at kjente standardpassord ikke er endret. Maskiner med nyere programvare er noe bedre sikret, men størstedelen har vesentlige mangler. [redacted] Svakhetene kan utnyttes til å overta kontroll med maskiner og ulike typer utstyr på sykehusene.

4. **Mangelfull sårbarhetsstyring av IKT-utstyr og programvare:** Rask installasjon av sikkerhetsoppdateringer skal sikre at angripere ikke kan utnytte sårbarheter som oppdages i programvare. Undersøkelsen viser at helseregionene oppdaterer produkter fra [redacted] rimelig raskt i mange tilfeller, men at det går langt tregere for annen programvare. Det finnes også eldre programvare som ikke lenger kan oppdateres, ofte i sammenheng med medisinsk-teknisk utstyr. Kjente sårbarheter i programvare kan utnyttes til å ta kontroll over maskiner i helseregionene, noe vi viste i vår angrepssimulering.

5. [redacted]

6. **Mangelfull logging og overvåkning:** Det er mangler i datagrunnlag for å oppdage angrep ved at det logges mindre enn anbefalt og det mangler sensorer for å innhente supplerende data. Videre er det svakheter i analysene av data for å avdekke dataangrep. Dermed ble få av aktivitetene i vår angrepssimulering faktisk oppdaget av helseregionene.

Det er ikke lagt til grunn at helseregionene skal følge anbefalingene fra Nasjonal sikkerhetsmyndighet (NSM) fullt ut. Helseregionene må foreta prioriteringer av sikkerhetstiltak basert på akseptabel risiko og kostnader. Ettersom tiltakene er grunnleggende for å oppnå god IKT-sikkerhet, er det imidlertid viktig at anbefalingene i størst mulig grad følges.

Alle helseregionene har vesentlige svakheter i sikkerhetstiltakene som ble kontrollert. Disse kan utnyttes av en angriper til å få uautorisert tilgang til systemer og informasjon. Det er ulikheter mellom regionene på hvilke områder svakhetene ligger, men i sum er det vesentlige svakheter i alle de grunnleggende sikkerhetstiltakene i alle regioner.

Svakhetene i de forebyggende sikkerhetstiltakene (punkt 1 til 5) kan utnyttes i dataangrep, og gjorde det mulig å få høy grad av kontroll over tre av fire helseregioners IKT-infrastruktur med kun velkjente standardverktøy i angrepssimuleringen.

Noen dataangrep vil lykkes, og det er derfor viktig at virksomheter også har systemer og rutiner som gjør at de kan oppdage angrep (punkt 6). Dette legger igjen grunnlaget for at angrepet kan håndteres. Helse Sør-Øst, som oppdaget flest av aktivitetene i angrepssimuleringen, hadde kommet lenger enn de andre i arbeidet med å samle inn og analysere data for overvåking av nettverk og IKT-systemer. Dette øker sannsynligheten for at regionen vil kunne oppdage og håndtere reelle dataangrep.

Helseregionene fikk umiddelbart etter testingen informasjon om svakhetene i tekniske sikkerhetstiltak som ble oppdaget. Mange av de konkrete svakhetene som ble utnyttet i angrepssimuleringen og som framkom av analyser, er utbedret i etterkant. [redacted].En angriper vil kartlegge og utnytte de svake punkter som kan finnes. Selv om de fleste sårbarheter blir fjernet, kan en gjenværende vesentlig sårbarhet være nok til at en angriper kan få kontroll over IKT-systemene. For å oppnå tilfredsstillende sikkerhet er det derfor viktig med et systematisk arbeid for å fjerne svakheter.

Etter vår vurdering er det for store svakheter i grunnleggende tekniske sikkerhetstiltak. I alle helseregionene vil det ta tid å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen.

8.3 Helseregionene er på etterskudd i informasjonssikkerhetsarbeidet, og mangler oversikt over sikkerheten i IKT-infrastrukturen

8.3.1 Det er økt oppmerksomhet om informasjonssikkerhet i helseregionene, og det er iverksatt flere forbedringstiltak som vil kunne øke IKT-sikkerheten på sikt

Undersøkelsen viser at det er økt oppmerksomhet om IKT- og informasjonssikkerhet i helseforetakene og helseregionene, og at det gjøres mye godt sikkerhetsarbeid.

Undersøkelsen viser at spesielt tre konkrete hendelser («Outsourcingssaken» i Helse Sør-Øst våren 2017, innføring av GDPR og dataangrepet på Helse Sør-Øst i januar 2018) har ført til økt oppmerksomhet om informasjonssikkerhetsområdet i helseregionene. Det er satt i verk tiltak for å forbedre IKT- og informasjonssikkerheten på flere områder. De viktigste tiltakene er:

- styrking av tekniske sikkerhetstiltak:
  - Sykehuspartner HF har styrket overvåkingskapasiteten, mens de tre andre regionale IKT-leverandørene jobber med konkrete tiltak for å styrke overvåkingen.
  - Det stilles krav til sterkere passord for administratorkontoer.
  - Det er igangsatt sårbarhetsskanning i alle helseregioner.
  - Graden av automatiserte sikkerhetsoppdateringer har økt.

- oppdatering av styringssystemene for informasjonssikkerhet og personvern, som fungerer som et rammeverk for styring/ledelse og sikkerhetsorganisering i den enkelte virksomhet.

- styrket arbeid med risiko- og sårbarhetsanalyser (ROS-analyser) ved innføring og endring av IKT-løsninger. Sammenlignet med situasjonen ved Riksrevisjonens tidligere undersøkelser har det skjedd en tydelig forbedring på dette området.

- større fagmiljøer for IKT-sikkerhet ved de regionale IKT-leverandørene. I Helse Sør-Øst er det bygget opp et fagmiljø som jobber spesifikt med overvåking og deteksjon.

- flere stillinger i helseforetakene som er dedikert til informasjonssikkerhetsarbeid, som rapporterer direkte til ledelsen. Samtidig viser undersøkelsen at helseforetakenes oppgaveportefølje på

informasjonssikkerhetsområdet har økt i omfang og kompleksitet, og at helseforetakene har hatt lite ressurser på dette området i forhold til oppgavemengden.

- e-læringskurs i informasjonssikkerhet er blitt obligatorisk i alle regioner. Det er fortsatt ikke slik at alle har gjennomført kursene.

- etablering av nye, regionale samarbeidsfora på informasjonssikkerhetsområdet, og tydeliggjøring av mandatene til eksisterende fora.

Det er også etablert større, regionale forbedringsprosjekter i Helse Nord og Helse Sør-Øst som helt eller delvis har som formål å bedre informasjonssikkerheten. Prosjektene rettes mot særskilte utfordringer i disse regionene og tar også tak i noen av svakhetene som er avdekket i denne undersøkelsen. Noen av prosjektene har som målsetting å redusere porteføljen av systemer og programvare, og å få bedre oversikt over systemer og komponenter/eiendeler. I Helse Sør-Øst er det også et viktig mål å oppgradere regionens IKT-infrastruktur, samt å etablere en felles teknologisk plattform for hele regionen. Helse Vest og Helse Midt-Norge har ikke sett samme behov for større forbedringsprosjekter.

De gjennomførte tiltakene er i hovedsak rettet mot forbedring av organisatoriske og tekniske forhold, og i mindre grad tiltak rettet mot utvikling av sikkerhetskulturen. Svakheter ved sikkerhetsatferden er nevnt av alle de regionale IKT-leverandørene som en av hovedårsakene til de tekniske sikkerhetsavvikene denne undersøkelsen har avdekket.

8.3.2 Helseregionene har ikke jobbet systematisk nok med opprydding og utfasing av eldre systemer og tilganger

For å imøtekomme de lovkrav som stilles til informasjonssikkerhet i helseforetakene, må helseregionene være ajour med sikkerhetstiltak.

Undersøkelsen viser at helseregionene har utfordringer som har sammenheng med ledelse og prioriteringer i den daglige driften. Der det innføres nye løsninger som i utgangspunktet skal heve IKT-sikkerhetsnivået, er det mange eksempler på at man enten ikke greier å fase ut de gamle løsningene, eller at man ikke greier å rydde opp i gamle løsninger som skal videreføres. Dermed får man en situasjon der nye, sikrere løsninger eksisterer parallelt med gamle, mindre sikre løsninger. Undersøkelsen viser at ingen av helseregionene har jobbet systematisk nok med å rydde i gamle løsninger:

- Brukerkontoer som ikke lenger er i bruk står fortsatt åpne
- Tilganger og tilgangsgrupper som ikke lenger er i bruk, fases ikke ut
- Eldre, lokale domener er i bruk i helseforetakene, selv om det er bestemt at de skal fases ut
- Det ryddes ikke fortløpende i sensitive pasientopplysninger, og i noen tilfeller er slike opplysninger tilgjengelige for ansatte uten tjenestlig behov

I angrepssimuleringen ga manglende opprydding på disse områdene oss mange veier videre inn i helseregionenes systemer, samt tilgang til sensitive person- og helseopplysninger.

Flere av de som er intervjuet peker på at endringsbehovet i sektoren generelt er drevet av ønsker om ny funksjonalitet, og at det derfor kan oppstå konflikt mellom innføring og administrering av nye løsninger, og rydding i gamle. Når rydding ikke prioriteres fortløpende, vil det være desto mer ressurskrevende når man går i gang.

I mange tilfeller er det helseforetakene som skal stå for opprydding. Undersøkelsen viser at helseforetakene kan ha mindre vilje til å prioritere ressurskrevende oppryddingsarbeid, blant annet fordi ressurser til slike oppgaver til enhver tid må veies opp mot andre oppgaver nærmere pasientbehandlingen. Kontrollen av de tekniske sikkerhetstiltakene viser at utstyr og systemer som helseforetakene drifter selv har svakere tilgangskontroller, oppdateres sjeldnere, og i mindre grad er sikret.

Ifølge helseregionene tar opprydding lang tid på grunn av det store omfanget av IKT-systemer, IKT-utstyr og programvare, samt begrensinger i eldre tekniske løsninger. Kompleksitet og omfang påvirker helseregionenes evne til å få oversikt over alt utstyr og programvare, og avhengigheter mellom disse. Manglende oversikt gjør det også vanskeligere å identifisere og gjennomføre viktige sikkerhetstiltak som sikkerhetsoppdateringer, sikker konfigurasjon av systemer og styring av tilgangsrettigheter. Helse Sør-Øst har en særlig kompleks og omfattende portefølje av utstyr, systemer og programvare.

Det er fortsatt mye arbeid som gjenstår for at helseregionene skal komme ajour med viktige sikkerhetstiltak. Manglende opprydding er en sentral årsak til tekniske funn i denne undersøkelsen. Etter vår vurdering bidrar dette til å svekke sikkerheten.

8.3.3 Uklare ansvarsforhold og oppgavefordeling i helseregionene vanskeliggjør forbedringsarbeidet

Ledelsen i de regionale helseforetakene, helseforetakene og de regionale IKT-leverandørene skal sørge for at det er tydelig hvem som har ansvar for hva på informasjonssikkerhetsområdet. Alle skal være kjent med hvilke oppgaver de har, i tillegg til å ha tilstrekkelig kunnskap om andres ansvar og oppgaver, og hvem som har myndighet til å ta beslutninger. De regionale helseforetakene må også sørge for samordning innad i helseregionene på IKT-sikkerhetsområdet, slik at hensyn til helheten og fellesskapet blir ivaretatt.

Undersøkelsen viser at det er uklarheter mellom IKT-leverandørene og helseforetakene om hvem som skal gjennomføre konkrete informasjonssikkerhetstiltak:

- Det er i mange tilfeller uklart hvem som skal gjøre nødvendig opprydding og forbedringstiltak.
- Det er uklart hvordan ansvaret for ivaretakelse av sikkerheten i medisinsk-teknisk utstyr skal fordeles

Opprydding og forbedringstiltak blir forsinket eller satt på vent fordi det ikke er avklart hvem som skal utføre oppgaven. I noen tilfeller er ansvaret delt mellom flere parter (helseforetak og regional IKT-leverandør), og arbeidet stopper opp fordi én av partene ikke tar sin del av ansvaret. Både helseforetakene og IKT-leverandørene påpeker at det gjenstår praktiske avklaringer om oppgavefordeling dem imellom.

I Helse Nord, Helse Midt-Norge og Helse Sør-Øst mener de regionale IKT-leverandørene at manglende avklaring av ansvar og oppgaver mellom helseforetakene og dem er en av hovedutfordringene i arbeidet med å forebygge og avdekke dataangrep. De er gitt et ansvar for sikkerheten i den regionale IKT-infrastrukturen, men har ikke kontroll med alt helseforetakene kobler til denne. Lokale sikkerhetsbrudd kan utgjøre en risiko for regionen som helhet, og de regionale IKT-leverandørene mener manglende avklaringer gjør det tidkrevende å rydde opp i kjente svakheter. Blant annet oppleves dette som en utfordring der det må ryddes i det helseforetakene drifter selv, og der det er vanskelig å gjennomføre oppdatering av programvare for eldre utstyr og systemer ute i helseforetakene. I Helse Vest framstår ansvaret for oppgavene som klarere.

I alle de fire regionene er det uklarheter rundt ansvaret for å ivareta sikkerheten i medisinsk-teknisk utstyr, som for eksempel røntgenutstyr eller måleinstrumenter. Medisinsk-teknisk utstyr har blitt stadig mer integrert i IKT-området ved at en større andel av utstyret i praksis er datamaskiner med egne lagringsenheter og oppkobling mot nettverk. Også Riksrevisjonens undersøkelse av informasjonssikkerhet i medisinsk-teknisk utstyr, som ble rapportert i Dokument 3:2 (2015-2016), viste at det var uklare ansvarslinjer for informasjonssikkerheten for slikt utstyr, både internt i helseforetakene og mellom helseforetakene og de regionale IKT-leverandørene.

Hvordan oppgavene er fordelt for slikt utstyr mellom regional IKT-leverandør og helseforetak varierer, både mellom regioner og mellom helseforetak i samme region. Helse Vest skiller seg ut ved at regional IKT-leverandør ikke er involvert i drift av regionens medisinsk-tekniske utstyr, og i liten grad i sikring av utstyret. Medisinsk-teknisk utstyr er plassert i et nettverk som er sikret av Helse Vest IKT, men for øvrig er det helseforetakene i regionen som ivaretar sikkerheten gjennom sikkert oppsett, sikkerhetsoppdateringer, tilgangskontroller og overvåking.

Etter vår vurdering er det ikke godt nok avklart innad i helseregionene hvem som har ansvaret for å gjennomføre nødvendige informasjonssikkerhetstiltak. I noen tilfeller må helseregionene klargjøre ansvar- og myndighetsforholdene i styringssystemene, i andre tilfeller må det gjøres presiseringer i databehandleravtaler, tjenesteavtaler og andre avtaler om hvem som har det formelle ansvaret og hvem skal utføre oppgaver. Konsekvensen av manglende avklaringer er at viktige tiltak for å forebygge dataangrep blir forsinket eller ikke gjennomført.

8.3.4 Ledelsen i både de regionale helseforetakene og underliggende foretakene har mangelfull informasjon om reell sikkerhetstilstand og sikkerhetsrisiko

Tilstrekkelig styringsinformasjon og forsvarlig beslutningsgrunnlag er en forutsetning for god styring og oppfølging. Det er et ledelsesansvar å håndtere risiko på en helhetlig måte og på bakgrunn av dette gjennomføre tilstrekkelige tiltak, styring og kontroll.

Undersøkelsen viser at ledere i helseregionene i varierende grad får informasjon om den reelle sikkerhetstilstanden:

- Ledelsen i både de regionale helseforetakene og helseforetakene mangler en helhetlig oversikt over informasjonssikkerhetsrisikoen, selv om det gjøres mange risiko- og sårbarhetsanalyser ved anskaffelser eller endringer av IKT-systemer eller -utstyr. Det gjennomføres sjeldent risikoanalyser av sikkerheten i selve IKT-infrastrukturen eller av andre informasjonssikkerhetsrelaterte temaer på et mer overordnet nivå. Risikoanalyser som omtaler risiko for tekniske sikkerhetssvakheter som denne undersøkelsen har avdekket, foreligger i liten grad.
- Helseforetakene gjennomfører få revisjoner, sikkerhetsøvelser og kontroller av blant annet IKT-leverandører. Videre har helseregionene i liten grad undersøkt sikkerhetskulturen og om de ansatte opptrer på en måte som ivaretar IKT- sikkerheten.
- Det er etablert systemer for å melde avvik i helseforetakene, men informasjonen som gis til ledelsen, er mangelfull. For det første rapporteres relativt få informasjonssikkerhetsavvik, noe som indikerer en underrapportering på dette området. For det andre analyseres de rapporterte hendelsene i liten grad. Det fratar organisasjonen muligheten for å lære av IKT-sikkerhetshendelser og sette i verk tiltak for å forebygge framtidige hendelser.

Undersøkelsen viser at helseregionene er klar over flere av risikoene. Det er imidlertid viktig at kunnskap om sikkerhetsrisikoen systematiseres, og inngår som en del av styringsgrunnlaget til styre og ledelse i helseregionene. Etter vår vurdering har ikke helseregionene et godt nok informasjonsgrunnlag til å kunne prioritere og iverksette nødvendige tiltak.

8.3.5 De regionale helseforetakene har ikke fulgt opp informasjonssikkerhetsarbeidet godt nok

De regionale helseforetakene har et tilsynsansvar overfor helseforetak de eier, som blant annet innebærer at de skal påse at helseforetakene håndterer helse- og personopplysninger i henhold til lover og regler. Tilsynsansvaret innebærer også å følge opp de krav Helse- og omsorgsdepartementet stiller til informasjonssikkerhetsarbeidet.

Undersøkelsen viser at de regionale helseforetakene har fulgt opp kravene fra departementet ved å videreformidle dem til helseforetakene og de regionale IKT-leverandørene, og ved at disse rapporterer om hvordan kravene er møtt. De regionale helseforetakene har i liten grad operasjonalisert kravene eller stilt ytterligere informasjonssikkerhetskrav ut ifra risikoen i den enkelte helseregionen.

At de regionale helseforetakene i liten grad stiller konkrete krav til informasjonssikkerhet kan ha sammenheng med at informasjonsgrunnlaget deres om tilstand og utfordringer ikke er tilstrekkelig. Undersøkelsen viser at oppfølgingen fra de regionale helseforetakene er blitt mer aktiv i etterkant av at omfattende regelendring, dataangrep og informasjonslekkasjer har kastet lys på brister i helseforetakenes informasjonssikkerhet. Dette tyder på at oppfølgingen på dette området har vært lite systematisk og proaktivt.

Undersøkelsen viser videre at de regionale helseforetakene heller ikke har fulgt godt nok opp at kravene de har stilt, har blitt innfridd av helseforetakene og IKT-leverandørene. Det gjør at

informasjonen de regionale helseforetakene videreformidler til departementet om tilstand og utfordringer på informasjonssikkerhetsområdet blir ufullstendig.

De regionale helseforetakene har ansvar for å samordne regionenes arbeid på IKT-området. Undersøkelsen viser at de regionale helseforetakene har lagt dårlig til rette for å samarbeide på tvers for å styrke informasjonssikkerheten i hele sektoren. Det er etablert få felles fora og organer der informasjonssikkerhetsutfordringer kan drøftes og løses i fellesskap.

Det felleseide selskapet Sykehusinnkjøp HF benyttes i liten grad til samordning for å sikre at det stilles samme informasjonssikkerhetskrav til like systemløsninger. Sykehusinnkjøp HF har begrenset kompetanse om IKT-sikkerhet, og de regionale helseforetakene har i liten grad bidratt til å styrke denne ved enten å stille til rådighet egen kompetanse eller stille krav til at Sykehusinnkjøp HF selv styrker kompetansen.

Nasjonal IKT HF ble opprettet av RHFene i 2014 som en hovedarena for samarbeid og samordning innen informasjons- og kommunikasjonsteknologi. De fikk imidlertid få definerte oppgaver innenfor informasjonssikkerhet og foretaket ble avviklet i 2019. I stedet er forumet regionalt direktørmøte etablert, men det kan stilles spørsmål ved om dette er tilstrekkelig for å styrke samordningen og samarbeidet innen informasjonssikkerhetsområdet.

Undersøkelsen viser at det er betydelige svakheter ved IKT-sikkerheten i helseregionene, og flere av svakhetene er påvist i tidligere undersøkelser. Samtidig har trusselen for dataangrep økt. Etter vår vurdering har ikke de regionale helseforetakene fulgt opp informasjonssikkerhetsarbeidet godt nok. De regionale helseforetakene har ikke innhentet nok informasjon om sikkerhetsnivået i egen region, det er fortsatt områder der ansvar og oppgavefordeling i helseregionene er uavklart, og samordningen på tvers av helseregionene har ikke vært god nok.

8.4 Atferden blant helse- og IKT-personell svekker IKT-sikkerheten

Foretakene har et ansvar for å utvikle en god sikkerhetskultur. Dette innebærer blant annet at ledelsen må sørge for at medarbeiderne har nødvendig kunnskap om informasjonssikkerhetstrusselen på det aktuelle fagfeltet, relevant regelverk, retningslinjer, veiledere og styringssystem, og at det legges til rette for at kravene kan etterleves. Undersøkelsen viser at en viktig årsak til at det har vært mulig å bryte seg inn i IKT-infrastrukturen er manglende etterlevelse av de retningslinjer og anbefalinger som foreligger.

Undersøkelsen viser at både enkelte IKT-personell og helsepersonell opptrer på en måte som svekker sikkerheten, ved for eksempel å sette svake passord, dele tilganger, gi tilgang til mer enn det som er nødvendig for å utføre oppgaver, og ved å slurve og ta snarveier. Selv når det er etablert retningslinjer som skal sørge for god IKT-sikkerhet, gjøres det i mange tilfeller unntak fra disse som svekker sikkerheten. Dette var en sentral årsak til at vi fikk kontroll over systemer og tilganger til sensitive opplysninger i angrepssimuleringen.
[redacted]
.

Mange dataangrep starter med en forfalsket e-post som har til hensikt å lure bruker til å åpne et vedlegg med ondsinnet programvare, eller klikke på en lenke som fører til infeksjon av maskinen. I denne undersøkelsen ble det gjennomført en phishing-test rettet mot ansatte i helseforetakene. Testen viser at en angriper med stor sannsynlighet ville fått ansatte til å trykke på lenker eller forsøke å laste ned filer med ondsinnet kode. Som testen illustrerer, er det vanskelig fullstendig å forhindre at enkelte ansatte klikker på falske e-poster, og det er derfor viktig å ha tekniske tiltak som kompenserer for dette. Undersøkelsen har ikke omfattet kontroll med tekniske tiltak som kan bidra til å stoppe slike e-poster før de kommer fram til de ansatte, eller hindrer at enkelte typer filer lastes ned.

Undersøkelsen viser videre at det meldes få informasjonssikkerhetsavvik i helseregionene, og at det gjøres få analyser av de avvik som meldes. Dette kan tyde på manglende oppmerksomhet rundt informasjonssikkerhet blant de ansatte.

Kompetanseoppbygging skal være kontinuerlig og tilpasset ulike roller og brukergrupper. Undersøkelsen viser at både helseforetakene og IKT- leverandørene har enkelte opplærings- og informasjonstiltak for å styrke kompetanse og sikkerhetsbevissthet. Informasjon til ansatte om informasjonssikkerhet formidles hovedsakelig som oppslag på intranettet. Opplæringstiltakene er for det meste e-læringskurs. Kursene er i liten grad tilpasset den enkeltes arbeidshverdag og utfordringer, og det er ikke alle som tar kursene selv om de nå er blitt obligatoriske. Opplæringen er noe mer differensiert hos de regionale IKT-leverandørene.

Undersøkelsen viser at sikkerhetskulturen i helseregionene ikke er tilfredsstillende, og at dette gir sårbarheter som kan utnyttes av angripere. Å bygge god sikkerhetskultur slik at sikkerhetsatferden bedres, krever etter vår vurdering ledelsens oppmerksomhet og innsats over tid. Informasjonssikkerhetsfeltet er i kontinuerlig endring, noe som gjør at det er behov for jevnlig og variert påfyll og gjenoppfriskning av kunnskap.

8.5 Helse- og omsorgsdepartementet har vært for passive i sin oppfølging av informasjonssikkerhetsarbeidet i helseregionene

Helse- og omsorgsdepartementet har det overordnede ansvaret for spesialisthelsetjenesten. Dette innebærer å sette de regionale helseforetakene i stand til å oppfylle sine plikter til å sørge for spesialisthelsetjeneste til befolkningen innen sine helseregioner. Departementet er videre ansvarlig for å fastsette de overordnede helsepolitiske målsettingene og for gi de regionale helseforetakene rammebetingelser som gjør det mulig for dem å nå disse målsettingene.

Undersøkelsen tyder på at departementets oppmerksomhet om informasjonssikkerhet har vært økende i kontrollperioden 2017-2019, og de har stilt relevante krav på området i denne perioden. Mange av kravene fra departementet tar utgangspunkt i konkrete hendelser, nye lovkrav eller resultater etter revisjoner/evalueringer.

Samtidig viser undersøkelsen at departementet ikke har innhentet tilstrekkelig informasjon om hvordan krav om IKT-sikkerhet til de regionale helseforetakene er ivaretatt og fulgt opp. For eksempel har departementet stilt krav om at det må jobbes med sikkerhetskultur, men det er ikke gitt svar i årlig melding på om dette kravet er møtt, og departementet har heller ikke etterspurt supplerende rapportering. Mange av svakhetene som ble avdekket i Riksrevisjonens revisjoner i 2014[312] og 2015[313], er fortsatt til stede.

Det er også iverksatt tiltak tidligere ved å etablere HelseCert og utvikle Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren. Samtidig er det etter Riksrevisjonens vurdering et potensial for å utnytte virkemiddelapparatet i Direktoratet for e-helse og Norsk Helsenett bedre for å styrke informasjonssikkerheten. Det er behov for å styrke den rollen HelseCert har når det gjelder å overvåke og teste IKT-sikkerheten i helseregionene. Direktoratet for e-helse har ansvar for Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren, men har hatt en lite tydelig rolle på området ut over dette.

Departementet skal holde seg orientert om foretakenes virksomhet, hvorvidt krav følges og iverksette tiltak ved behov. Undersøkelsen viser at departementet ikke i tilstrekkelig grad har sørget for å skaffe seg et godt nok informasjonsgrunnlag. De regionale helseforetakenes rapportering er på et overordnet nivå og gir ikke alltid svar på om stilte krav er innfridd. Utover rapporteringen i årlig melding fra de regionale helseforetakene, har departementet fått informasjon om status gjennom uformell dialog med de regionale helseforetakene og ved å be Direktoratet for eHelse utarbeide rapporter knyttet til

[312] Dokument 3:2 (2014-2015) undersøkelsen om styring og kontroll av tilgang til helseopplysninger i elektroniske pasientjournaler i fire helseforetak og Helseforetakenes beredskap innen IKT, vann og strøm.
[313] Dokument 3:2 (2015-2016) om de regionale helseforetakenes og helseforetakenes ivaretakelse av informasjonssikkerheten i medisinsk teknisk utstyr.

informasjonssikkerhet. I tillegg mottar departementet årlig rapport fra Norsk Helsenett/HelseCert som inneholder informasjon om inntrengingstester i helseregionene.

Arbeidet med IKT-sikkerhet er en forutsetning for å sikre forsvarlig pasientbehandling og for å lykkes med økt digitalisering av helsektoren. Etter vår vurdering viser de påviste svakhetene i undersøkelsen at departementets oppfølging på dette området har vært for passiv. Styringen synes i stor grad å være hendelsesbasert og for lite proaktiv.