Sykehuset Innlandet HF
Styremøte 22.04.21

SAK NR 038 – 2021
RIKSREVISJONENS UNDERSØKELSE AV HELSEFORETAKENES FOREBYGGING AV ANGREP MOT SINE IKT-SYSTEMER

Forslag til

VEDTAK:

1. Styret tar informasjonen om Riksrevisjonens rapport til etterretning.

2. Styret ber om at Riksrevisjonens rapport brukes aktivt i det videre arbeidet med informasjonssikkerhet i Sykehuset Innlandet.

Brumunddal, 15. april 2021

Alice Beathe Andersgaard
administrerende direktør

SAKSFREMSTILLING

SAK NR. 038 – 2021

Bakgrunn

Riksrevisjon gjennomførte i perioden 2018 – 2020 en forvaltningsrevisjon om helseforetakenes forebygging av angrep mot sine IKT-systemer. Revisjon var rettet mot Helse- og omsorgsdepartementet, de fire regionale helseforetakene, underliggende helseforetak og de fire IKT-leverandørene.

Riksrevisjonens forvaltningsrevisjon om helseforetakenes forebygging av angrep mot sine IKT-systemer ble lagt fram for Stortinget den 15. desember 2020.

Mer inngående beskrivelser er gitt i «*Riksrevisjonens undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer»* https://www.stortinget.no/globalassets/pdf/dokumentserien/2020-2021/ikt-angrep-mot-hf---rapportvedlegg-til-dok.-3-2-2020-2012.pdf (vedlegg 1). Deler av rapporten er gradert begrenset i henhold til sikkerhetsloven og unntatt offentlighet i henhold til offentlighetsloven.

Denne styresaken redegjør for Riksrevisjonens rapport.

Saksframstilling

Riksrevisjonen har gjennomført dokumentanalyser, innhentet opplysninger gjennom spørrebrev, foretatt intervjuer, gjennomført angrepssimulering og tekniske kontroller, utført phisingtest og foretatt observasjoner, samt gjennomført analyse av avviksmeldinger. Målet med angreps-simuleringen var å ta kontroll over mest mulig av den regionale IKT-infrastrukturen og få tilgang til sensitive opplysninger. Dokumentanalyser og spørrebrev ble benyttet for å belyse hvordan IKT-sikkerheten påvirkes av helseregionenes organisering og styring. Phisingtester[1] og andre observasjoner ble benyttet for å belyse informasjonssikkerhetskulturen.

Riksrevisjon har skrevet følgende om funn og konklusjoner:

- Riksrevisjonens simulerte dataangrep ga høy grad av kontroll over IKT-infrastrukturen i tre av fire helseregioner og tilgang til store mengder pasientopplysninger i alle helseregioner.

[1] Phishing er en form for sosial manipulering hvor en angriper forsøker å lure noen til å utføre en handling, for eksempel åpne et e-postvedlegg, klikke på en lenke eller betale en falsk regning. Via vedlegg kan det installeres skadevare, for eksempel løsepenge-virus («ransomware»), som kan spre seg videre til andre datamaskiner i samme nettverk. Via lenker kan angriperen be om brukernavn og passord til systemløsninger, og videre benytte disse for eksempel til å stjele konfidensielle opplysninger (Datatilsynet).

- I alle fire helseregioner er det vesentlige svakheter i grunnleggende tekniske sikkerhetstiltak som skal forebygge og oppdage dataangrep.
- Helseregionene er på etterskudd i informasjonssikkerhetsarbeidet og mangler oversikt over sikkerheten i IKT-infrastrukturen.
    - Det er økt oppmerksomhet om informasjonssikkerhet i helseregionene, og det er iverksatt flere forbedringstiltak som vil kunne øke IKT-sikkerheten på sikt.
    - Helseregionene har ikke jobbet systematisk nok med opprydding og utfasing av eldre systemer og tilganger.
    - Uklare ansvarsforhold og uklar oppgavefordeling i helseregionene vanskeliggjør forbedringsarbeidet.
    - Ledelsen i både de regionale helseforetakene og de underliggende helseforetakene har mangelfull informasjon om reell sikkerhetstilstand og sikkerhetsrisiko.
    - De regionale helseforetakene har ikke fulgt opp informasjonssikkerhetsarbeidet godt nok.
    - Atferden blant helse- og IKT-personell svekker IKT-sikkerhet.
    - Helse- og omsorgsdepartementet har vært for passive i sin oppfølging av informasjons-sikkerhetsarbeidet i helseregionene.

Arbeidet med informasjonssikkerhet i Helse Sør-Øst

Det har vært jobbet systematisk med tiltak innenfor informasjonssikkerhet i Helse Sør-Øst og underliggende helseforetak før og etter Riksrevisjonens simulerte dataangrep.

Riksrevisjonens simulerte dataangrep fikk ikke kontroll over sentral infrastruktur i Helse Sør-Øst., selv om de fikk fortsette angrepet etter at det var oppdaget og kunne stanses gjennom Sykehuspartner HFs sikkerhetsverktøy.

Videre påpeker Riksrevisjon at store mengder personopplysninger av særlig kategori(sensitive) var tilgjengelig for mange ansatte. Dette gjaldt enkelte typer opplysninger som var lagret på filområder.

Riksrevisjon anbefaler at de regionale helseforetakene:

- Følger opp krav som er stilt til helseforetakene på informasjonssikkerhets-området, slik at det oppnås nødvendig framdrift i forbedringsarbeidet.
- Sørger for at det iverksettes nødvendige tekniske sikkerhetstiltak med utgangspunkt i anerkjente sikkerhetsprinsipper som skal gi et egnet sikkerhets-nivå i tråd med lovkrav.
- Tar større ansvar for å samordne informasjonssikkerhetsarbeidet i egen region, og blant annet gjøre nødvendige avklaringer om ansvar, roller og oppgaver.
- Vurderer egnede tiltak for økt samarbeid mellom helseregionene for å styrke informasjonssikkerheten i sektoren.

Videre anbefaler Riksrevisjonen at de regionale helseforetakene og helseforetakene:

- Sørger for å ha tilstrekkelig kunnskap om sikkerhetstilstanden for å kunne prioritere nødvendige tiltak.
- Iverksetter tiltak som sikrer at:
    - Ansvars og oppgavefordeling blir avklart
    - Nødvendige tekniske sikkerhetstiltak blir gjennomført
    - Det blir systematisk ryddet i gamle løsninger og sensitive helse- og personopplysninger
    - Sikkerhetsatferd hos helse- og IKT-personell blir bedre

Helse Sør-Øst arbeider med informasjonssikkerhet innen følgende områder:

- Avklare roller og ansvar
- Oversikt, rapportering og oppfølging. Helse Sør-Øst har «risiko forbundet med informasjonssikkerhet og personvern» som eget område i risikovurderingen til styret.
- Informasjonssikkerhetskultur og –kompetanse.
- Informasjonssikkerhet i anskaffelser
- Applikasjoner, infrastruktur og teknisk sikkerhet. Infrastrukturmodernisering er et pågående og kontinuerlig arbeid
- Kontinuerlig forbedring

Arbeidet med informasjonssikkerhet i Sykehuset Innlandet

Riksrevisjonens undersøkelse viser at Sykehuset Innlandet i samarbeid med vår tjenesteleverandør Sykehuspartner, må arbeide målrettet med informasjonssikkerhet for å forebygge og oppdage angrep mot våre IKT-systemer. God informasjonssikkerhet skal ivareta konfidensialitet, integritet og tilgjengelighet på en slik måte at pasienten får best mulig behandling. Dette er i samsvar med norm for informasjonssikkerhet fra Direktoratet for ehelse.

Befolkningen må ha tillit til at Sykehuset Innlandet ivaretar deres personvern. Sykehuset Innlandet skal ha etablert god sikkerhetskultur der personell forstår hvordan de skal bidra til digital sikkerhet og hva deres personlige ansvar for dette er. Pasienter og pårørende forventer samtidig at helseopplysninger er tilgjengelig for helsepersonell som behandler dem.

I «Oppdrag og bestilling 2021 for Sykehuset Innlandet HF» (OB) skal Sykehuset Innlandet følge opp Riksrevisjonens hovedfunn, merknader og anbefalinger fra undersøkelsen om helseforetakenes forebygging av angrep mot sine IKT-systemer.

Annen oppgave 2021(OB):

- Helseforetaket skal benytte Sykehuspartner HFs og Norsk helsenett SFs årlige rapport om trusler, trender, sårbarheter og relevante tiltak i sitt arbeid med risiko- og sårbarhetsvurderinger.
- Helseforetaket skal videreføre arbeidet med systematisk innføring av Nasjonal sikkerhetsmyndighets grunnprinsipper for IKT-sikkerhet, og sikre systematisk adressering av arbeidet med informasjonssikkerhet på alle nivåer.
- Helseforetaket skal presentere status fra arbeidet med informasjonssikkerhet, herunder ledelsens årlige gjennomgang, i de etablerte oppfølgingsmøtene med Helse Sør-Øst RHF og i årlig melding.
- Helseforetaket skal ta i bruk regional protokoll over behandlingsaktiviteter og bidra i Sykehuspartner HFs arbeid med å videreutvikle den regionale protokollen slik at den understøtter gode arbeidsprosesser i helseforetakene.
- Helseforetaket skal ha oversikt over informasjonssikkerhetsrisikoen og -tilstanden i helseforetaket, herunder trusselbildet, sårbarheter, tiltak og hendelser. De største risikoområdene skal prioriteres. Etter nærmere spesifisering skal status rapporteres i ordinær tertialrapportering.
- Helseforetaket skal rapportere antall innmeldte avvik innen informasjonssikkerhet og antall brudd på konfidensialitet, integritet og/eller tilgjengelighet.

Riksrevisjonens undersøkelse finner at det gjennomgående er mer begrenset sikkerhet i utstyr og systemer som helseforetakene utvikler og drifter selv. De har svakere tilgangskontroller, oppdateres sjeldnere og er i mindre grad sikret.

Under dataangrepet ved Sykehuset Innlandet i august 2020 var det et egenutviklet system som var «inngangsporten» for angriper og personopplysninger kunne hentes ut fra flere systemer. Sykehuset Innlandet har etter dataangrepet i august 2020 gjort flere tiltak, noen også samordnet med det regionale helseforetaket og tjenesteleverandør for å redusere risikoen for slike angrep fremover. Noen systemer er avviklet, bredding av egenutviklede systemer er satt i bero i påvente av sikkerhetsvurdering av tjenesteleverandør og ingen egenutviklede systemer er eksponert mot internett.

Riksrevisjonens undersøkelse avdekket at store mengder sensitiv informasjon var tilgjengelig for mange ansatte. Dette var opplysninger som ikke var lagret i fagsystemer, men på filområder. Sykehuset Innlandet innførte på nyåret 2021 tjenesten «Sensitiv struktur» levert av tjenesteleverandør. Denne tjenesten er en sikker løsning for lagring av person-opplysninger og personopplysninger av særskilt kategori på filområder. Flytting av filer med sensitivt innhold flyttes til «Sensitiv struktur» og tilgangen til filområdene er strengt regulert slik at kun de som har tjenstlig behov får tilgang.

Infrastrukturmoderniseringen (program STIM) i Helse Sør-Øst er et pågående arbeid i alle foretak i regionen hvor utdatert utstyr skiftes og eksisterende utstyr og systemer oppgraderes for å ivareta nødvendig sikkerhet. Klienter(PC) oppgraderes til Windows10, utskifting av nettverkskomponenter og sanering av utstyr og systemer er pågående arbeid, og vil fortsette i lang tid framover.

IKT-infrastrukturen i Helse Sør-Øst er stor og kompleks. Program STIM, har blant annet et prosjekt med sanering av systemer og utstyr, og innføring av regional protokoll over behandlingsaktiviteter. Dette vil gi Sykehuset Innlandet og de andre foretakene i regionen en god oversikt over IKT-systemene i regionen og muligheter for standardisering på IKT- og informasjons-sikkerhetsområdet.

Informasjonssikkerhetskulturen i alle foretak i Helse Sør-Øst skal måles i løpet av 2021, og eventuelle tiltak skal iverksettes med bakgrunn i målingen.
Terskelen for å melde avvik knyttet til informasjonssikkerhet er høy. Avvik innen informasjonssikkerheten må meldes på lik linje med andre avvik, slik at tiltak kan iverksettes og informasjonssikkerheten forbedres.

God informasjonssikkerhet er et kontinuerlig arbeid. Rapportering, identifisering av avvik og implementering av tiltak er avgjørende for god informasjonssikkerhet.
Alle ledere og medarbeidere i Sykehuset Innlandet må ta del i arbeidet med god informasjonssikkerhet.

Administrerende direktørs vurdering

God informasjonssikkerhet er god pasientsikkerhet og en forutsetning for god pasientbehandling.

Administrerende direktør mener at foretaket har etablert gode systemer for å ivareta informasjonssikkerhet. Det er likevel forbedringsmuligheter som det arbeides aktivt med, både internt og i samarbeid med andre helseforetak og med Helse Sør-Øst RHF.

De regionale helseforetakene er bedt om å følge opp Riksrevisjonens hovedfunn, merknader og anbefalinger i undersøkelsen. Sykehuset Innlandet vil i samarbeid med Helse Sør-Øst RHF og tjenesteleverandør identifisere tiltak og arbeide videre med disse.

Digital informasjonsbehandling er avgjørende for god og sikker pasientbehandling og pasienter og pårørende forventer at informasjon er tilgjengelig på en trygg og sikker måte. Alle ansatte i Sykehuset Innlandet må ta del i informasjonssikkerhetsarbeidet

Administrerende direktør anbefaler at styret tar redegjørelsen til orientering.

Vedlegg : Riksrevisjonens undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer.