TRONDHEIM KOMMUNE
Trondheim kommunerevisjon

Organisasjonsdirektør
Trude Kristin Kjeldstad

Vår saksbehandler	Vår ref.	Deres ref.	Dato
Børge Sundli	21/21084 oppgis ved alle henv.		14.02.2022

Etterlevelseskontroll 2021, Generelle IT-kontroller med særlig fokus på datasikkerhet og beredskapstiltak i Trondheim kommune

1. Innledning

I forbindelse med ny kommunelov har regnskapsrevisor fått en ny oppgave fra 2019, kalt forenklet etterlevelseskontroll med økonomiforvaltningen. Kontrollen skal skje i forlengelsen av revisjonen av regnskapet og skal rette seg mot de delene av økonomiforvaltningen som går ut over å uttale seg om årsregnskapet.

Loven forutsetter at revisor gir en egen uttalelse om kontrollen som er utført. Kontrollen skal gjennomføres med såkalt moderat sikkerhet. Dette innebærer at kravene til denne kontrollen er definert gjennom god kommunal revisjonsskikk[1] og revisjonsstandarden RSK 301 "Forenklet etterlevelseskontroll med økonomiforvaltningen". Dette er en ny standard som beskriver krav til revisors arbeid. Standarden trådte i kraft fra 2020.

Trondheim kommunerevisjon har gjennomført en forenklet etterlevelseskontroll som gjelder generelle IT-kontroller på økonomiområdet i Trondheim kommune. Formålet er å forebygge svakheter og bidra til å sikre at kommunen følger sentrale bestemmelser og vedtak knyttet til bruk av informasjonsteknologi på økonomiområdet.

I denne revisjonen har vi undersøkt om kommunens generelle IT-kontroller er tilfredsstillende og fungerer etter forutsetningene. Generelle IT-kontroller er et av revisjonens årlige fokusområder, og det må utføres relevante og hensiktsmessige revisjonshandlinger. Generelle IT-kontroller er policyer og rutiner som relaterer seg til mange IT-systemer og bidrar til å sikre kontinuerlig og hensiktsmessig drift av IT-systemene. Generelle IT-kontroller må derfor testes årlig. Valget av hva som vurderes og testes samt omfanget av dette vil derfor være en årlig revisjonsfaglig vurdering.

[1] Med god kommunal revisjonsskikk menes at revisjonen skal utføres i samsvar med den oppfatning av etiske og revisjonstekniske prinsipper for revisjon av kommuner som til enhver tid er alminnelig anerkjent og praktisert av dyktige og ansvarsbevisste utøvere av yrket.

Denne rapporten er en oppfølging av revisjonsrapport Generelle IT-kontroller Rapport 2/2020-R. Vi ser også at den senere tids utvikling knyttet til datasikkerhet og beredskap gjør at risikobildet har endret seg, med sannsynligvis økende antall dataangrep utenfra. Ut fra en revisjonsfaglig vurdering er dette et område som må gis særskilt fokus i 2021.

Med bakgrunn i dette har vi valgt ut noen vesentlige områder som vi har undersøkt nærmere.

Etterlevelseskontrollen formaliseres gjennom en uttalelse fra revisor til kontrollutvalget.

2. Problemstilling og revisjonskriterier

Vi har valgt følgende problemstilling og delproblemstillinger:

Har Trondheim kommune tilfredsstillende internkontroll i og rundt IT-systemene som genererer regnskapstall?

1. Har Trondheim kommunen tilfredsstillende tilgangsadministrasjon til IT-systemene?
2. Er det tilfredsstillende endringshåndtering[2] av IT-systemer i Trondheim kommune?
3. Har Trondheim kommune tilfredsstillende datasikkerhet og beredskapstiltak?

Revisjonskriterier er de krav, normer og/eller standarder som revidert enhet skal vurderes opp mot. Kriteriene er utledet fra følgende kilder:

- Nasjonal sikkerhetsmyndighets (NSM)[3] grunnprinsipper for IKT-sikkerhet.
- KS[4] 2021, brev til kommuner og fylkeskommuner "Datasikkerhets- og beredskapstiltak i kommunal sektor".
- ISO 27000-serien[5] og ISO 31000.
- ISAE 3402-uttalelser.
- Lov om kommunal beredskapsplikt § 17.

3. Metode

Gjennomgangen er i hovedsak en oppfølging av revisjonsrapporten "Generelle IT-kontroller Rapport 2/2020-R". Vi ser på eventuelle endringer i rutinene basert på beskrivelsene fra 2019/2020 og hvordan de er dokumentert og praktisert i 2021. Vi har i år tatt med et nytt tema vedrørende datasikkerhet og beredskapstiltak.

Metodisk baserer undersøkelsen seg på dokumentgjennomgang og intervjuer. Vi har gjennomført analyse av dokumenter i forkant av møter med kontaktpersonen, oppnevnt av kommunen. I møtet med kontaktpersonen presenterte vi problemstillinger og revisjonskriterier. Vi informerte også om

[2] En formell prosess for å håndtere, dokumentere og gjennomføre endringer i IT-systemer

[3] Nasjonal sikkerhetsmyndighet (NSM) er fagorgan for forebyggende sikkerhet, og sikkerhetsmyndighet etter lov om nasjonal sikkerhet (sikkerhetsloven).

[4] KS er kommunesektorens interesseorganisasjon.

[5] ISO: International Organization for Standardization, eller på norsk Den internasjonale standardiseringsorganisasjonen, er en internasjonal standardiseringsorganisasjon som utgir standarder.

etterlevelsesrevisjon generelt og denne undersøkelsen spesifikt. Vi har hatt dialog med kontaktpersonen for å avklare spørsmål underveis.

Vi har herunder gjennomført møter og kommunisert med sentrale personer innenfor IT-området i kommunen.

Videre har vi gjennomført tester av rutinene for tildeling, endring og sletting av tilganger til TK-nettet, lønnssystemet og økonomisystemet i kommunen.

4. Gjennomføring

Med bakgrunn i dokumentgjennomgangen, intervjuene og gjennomført testing, oppsummerer vi resultatet i dette kapitlet.

4.1 Har Trondheim kommune tilfredsstillende tilgangsadministrasjon til IT-systemene?

4.1.1 Revisjonskriterier

Med grunnlag i ISO 27000-serien definerer Nasjonal sikkerhetsmyndighets (NSM)[6] grunnprinsipper for IKT-sikkerhet et sett med prinsipper og underliggende tiltak for å beskytte informasjonssystemer. Grunnprinsippene fremhever at en virksomhet må ha kontroll på de ulike brukerne, og hvilke rettigheter de er gitt i IT-systemene de har tilgang til.

Ekstern revisor hos leverandørene for økonomisystemet LIFT og lønnssystemet Bluegarden utarbeider ISAE 3402-uttalelser[7] som gir kommunen en uavhengig erklæring vedrørende leverandørenes kontrollmiljø ved behandling av regnskapsdata for kommunen.

På bakgrunn av dette har vi utledet følgende kriterier:

- Kommunen skal ha tilfredsstillende tildeling, endring og sletting av tilganger til IT-systemer:
    - Tilganger og utmeldinger skal bestilles av autorisert bestiller og meldes inn i felles tilgangssystem.
    - Brukere skal bare gis tilgang til TK-nettet[8] ved tjenstlig behov.
    - Brukere skal bare gis tilgang til IT-systemer ved tjenstlig behov.

4.1.2 Bestilling av tilganger

Trondheim kommune har overordnede rutiner dokumentert i Kvaliteket[9] som beskriver enhetenes ansvar og fremgangsmåte ved bestilling av ny tilgang, endring og sletting av tilgang i TK-nett og

[6] Nasjonal sikkerhetsmyndighet (NSM) er fagorgan for forebyggende sikkerhet, og sikkerhetsmyndighet etter lov om nasjonal sikkerhet (sikkerhetsloven).

[7] ISAE 3402-standarden gir veiledning som gjør det mulig for en uavhengig revisor (tjenesterevisor) å uttale seg om en tjenesteleverandørs beskrivelse av systemet sitt og egnetheten til utformingen av og den driftsmessige effektiviteten til de tilhørende kontrollene, i en revisorrapport for tjenestene.

[8] TK-nett er en felles betegnelse for det interne nettverket til Trondheim kommune. Det er igjen delt opp i flere undernettverk som er beregnet for forskjellige tjenester og enheter i kommunen.

[9] Kvaliteket er kommunens kvalitetssystem og inneholder kommunens rutiner og dokumenter på ulike områder. Det er et IT-basert verktøy integrert i intranettet til kommunen som er tilgjengelig for alle ansatte. Kvaliteket .

Elevnett[10]. Rutinen i Kvaliteket som beskriver enhetens ansvar ved tilgangsadministrasjon, beskriver også hvilke skjema i Selvbetjeningsportalen[11] som skal benyttes for bestilling, endring og sletting av tilganger til IT-systemer.

Formålet med rutinene er å sikre korrekt bestilling av nye og sletting av eksisterende IT-tilganger for ansatte, vikarer, studenter og eksterne konsulenter.

De skriftlige rutinene for tilgangshåndtering beskriver at det er enhetsleder som har ansvar for å gi beskjed om at ansatte meldes inn og ut fra TK-nettet og IT-systemene.

For å gjennomføre test av tilgangskontroller har vi tatt ut en liste fra lønnssystemet Bluegarden over personer som hadde start- og sluttdato i Trondheim kommune i perioden januar til september 2021. I denne kontrollen ønsket vi å få dokumentasjon på at bestillingsskjema for IT-tilganger er kommet fra autorisert bestiller og å se at bestillingen er registrert i AD[12] (Active Directory). AD viser hvilke IT-systemer personen har fått tilgang til.

Revisjonen har testet følgende tilganger[13]:

- ni nyansatte i kommunen
- seks personer som har sluttet
- en person som har skiftet arbeidssted innad i kommunen.

Revisjonens test av de ni nyansatte viser at alle de som er kontrollert er innmeldt i HR-portalen[14] og har fått riktig tilgang i økonomisystemet LIFT og lønnssystemet Bluegarden. Vi ba IT-tjenesten om å ta ut tilgangsskjemaene som var benyttet for de ni nyansatte. Kontrollen viser at alle tilgangsskjemaene som er sendt inn er bestilt av autorisert bestiller. Tre av de ni innmeldte er ledere, og da er det riktig at det er Enhet for kommunikasjon, administrasjon og innbyggerkontakt som har bestilt tilgangene. Vi ser at innregistreringen av de andre seks nyansatte er gjort på bakgrunn av bestillingsskjema fra andre enn enhetsleder. Spesialkonsulent ved IT-tjenesten opplyser at enhetsledere kan delegere rollen autorisert bestiller til annen ansatt ved enheten ved å bestille dette via Selvbetjeningsportalen på et skjema som heter "Autorisert bestiller". Det er ikke mulig for andre enn autoriserte bestillere å bestille tilganger i Selvbetjeningsportalen. Revisjonen har spurt tre av enhetene hva som er bakgrunnen for at enhetsleder har delegert rollen autorisert bestiller til avdelingsledere og merkantilt personale. De beskriver at bakgrunnen er å avlaste enhetsleder.

Tilgangene til de seks kontrollerte personene som har sluttet i Trondheim kommune i perioden er bestilt av autorisert bestiller og alle er sluttmeldt i lønnssystemet Bluegarden og slettet i økononomisystemet LIFT. En av de kontrollerte personene var ikke slettet fra AD. I dette tilfellet hadde ikke enheten fulgt rutinen, og IT-brukeradministrasjon[15] måtte purre på sletteskjema. Den sluttmeldte ble slettet fra AD 27. september 2021. IT-brukeradministrasjon har som rutine/praksis

[10] Elev-nett: Nettverk for skoler, lærere og elever.

[11] Selvbetjeningsportalen: En nettside i Trondheim kommune hvor det blant annet er samlet skjemaer for bestilling av tilganger til IT-systemer.

[12] AD: En forkortelse for Active Directory som er et system for håndtering av tilgangsadministrasjon.

[13] Utvalget er basert på et en skjønnsmessig vurdering

[14] HR-portalen er Trondheim kommunes HR-system.

[15] IT-brukeradministrasjon er en del av IT-tjenesten i kommunen

at de kontakter enhetene hvis de oppdager at sletteskjema ikke er sendt.

Den kontrollerte personen som hadde skiftet arbeidssted innad i kommunen har riktig tilgang til lønnssystemet Bluegarden og økonomisystemet LIFT. Bestillingsskjemaet er sendt inn av merkantil som er autorisert bestiller.

4.1.2 Tilgang til TK-nettet kun ved tjenstlig behov

I forbindelse med kontroll av leverandørenes tilganger[16] i TK-nettet har revisjonen mottatt en liste over tilganger for personer som ikke er ansatt i Trondheim kommune. Liste over IT-leverandørenes tilganger er fra 29. september 2021 og omfatter 351 personer hos 49 leverandører.

Revisjonen har foretatt en gjennomgang av disse tilgangene. Vi valgte ut de tre største leverandørene og ba IT-tjenesten gjøre en vurdering av at så mange enkeltpersoner fra disse virksomhetene har tilgang til TK-nettet. De tre største leverandørene har tilsammen 219 tilganger til TK-nettet. IT-tjenesten opplyser at disse leverandørene har kontinuerlig drift av IT-systemene som krever stor vaktstyrke. I avtalene med leverandørene er det krav til at man skal gå gjennom tildeling og fjerning av tilganger til TK-nettet og IT-systemene hvert kvartal.

Vi har stilt spørsmål til IT-tjenesten om leverandørtilganger som aldri har vært logget på TK-nettet. IT-tjenesten opplyser at det kan være flere årsaker til at enkelte personer ikke har benyttet seg av sin tilgang. IT-tjenesten svarer at personell hos leverandørene inngår i en vaktordning hvor de kun benytter sin tilgang hvis det oppstår hendelser som krever pålogging.

Revisjonen har bedt Trondheim Eiendom og Enhet for service og internkontroll gjøre en vurdering av behovet for mange tilganger for sikkerhets og alarmtjenester. Vi har fått opplyst at antall tilganger gjenspeiler behovet for døgnkontinuerlig drift og vaktordning. Det er i avtalen stilt krav om jevnlig oppfølging av leverandørens tilganger til løsningene og derav også tilgang til TK-nettet. Alle bestillinger av ny tilgang, endring på eksisterende tilgang og terminering av tilgang blir registrert hos leverandøren. Leverandøren oversender rapporter med oversikt over tilganger og annen nødvendig informasjon til kommunen etter avtalte tidsintervaller. I tillegg gjennomfører leverandøren periodiske revisjoner av tilganger etter avtale med kommunen.

4.1.3 Tilgang til IT-systemene ved tjenstlig behov

Det er enhetsleder som er ansvarlig for å definere tjenstlig behov for ansattes tilgang til IT-systemene. Enheten vurderer hvilke brukere som skal ha hvilke roller for å utføre spesifikke oppgaver i systemene. For å sikre god intern kontroll og motvirke risiko for bevisste og ubevisste feil bør det legges sperrer i IT-systemene slik at uheldige rollekombinasjoner unngås.

Vi har bedt om dokumentasjon av ERP-tilgangsskjema[17] for seks personer som har fått tilgang til økonomisystemet LIFT i perioden. På skjemaene som er testet går det frem hvilke tilganger[18] personene skal ha i LIFT. En ansatt ved IT-brukeradministrasjon opplyser at det kun er enhetsledere og de med delegert fullmakt som kan sende inn dette bestillingsskjemaet. Vi fant ingen avvik på dette. Tilganger i LIFT er i samsvar med ansettelsesforholdet for de kontrollerte

[16] Personer hos leverandøren som har tilgang til IT-systemer i Trondheim kommune

[17] ERP-tilgangsskjema: Skjema som benyttes for å gi tilgang til ERP fagsystemer (LIFT og Bluegarden).

[18] Ulike tilganger/roller i LIFT; fakturabehandling, attestant, bestiller, utgående faktura, sentral regnskapsrolle, enhetsledertilgang

ansatte.

For kommunens økonomisystem LIFT har revisjonen gjort en vurdering av personer og identer med utvidede roller. Per juni 2021 er det 43 brukere som har rollen som Superbruker og Systembruker[19] i IT-systemet LIFT. Det er fire ansatte i Trondheim kommune som har begge disse to rollene. Resten av de utvidede tilgangene gjelder personer som er ansatt hos leverandøren av kommunens økonomisystem. Tjenesteforvalter i LIFT har forklart at oppgradering av økonomisystemet er årsaken til at så mange hos TietoEVRY har tilgang. Det opplyses at det foretas regelmessige gjennomganger med leder for support- og konsulentavdelingen for å vurdere behovet for utvidete tilganger.

IT-tjenesten uttaler at det er gjort en klassifisering av identer hos leverandøren - gjort etter sommeren 2020. På grunn av sammenslåingen av Evry og Tieto til TietoEVRY er det satt flere personer på support hos leverandøren. LIFT har mange prosesser som er knyttet mot ulike prosesseiere hos leverandøren. Kommunen vil sammen med leverandøren av LIFT undersøke nøye før de sletter identer som kan medføre at prosesser stopper.

I avtalen mellom kommunen og leverandøren av LIFT er det avtalt at det skal foretas en årlig vurdering av den interne kontrollen hos leverandøren. Denne vurderingen skal utføres av en ekstern tredjepart og det skal avgis en ISAE 3402-uttalelse. Revisjonen gjennomgår uttalelsene som blant annet omtaler leverandørens tilgangshåndtering til systemet.

I sin vurdering av roller i LIFT sier Regnskapstjenesten i kommunen at de har lagt vekt på å tildele roller i forhold til arbeidsoppgaver, effektiv drift og risiko for at feil oppstår. Revisjonen har foretatt en gjennomgang av uheldige rollekombinasjoner i LIFT i 2021, og kommunen har med bakgrunn i revisjonens funn gjort endringer for å begrense rollekombinasjoner i LIFT. Et viktig tiltak som er satt inn er at de som har remitteringsadgang[20] ikke skal kunne endre bankkontonummer.

Ved ansettelse i kommunen tildeles alle rollen "ansatt" automatisk i Bluegarden HR-portalen[21]. Rollen gir basis tilgang for alle ansatte. Enhetsleder og avdelingsleder får tildelt rollen "leder" gjennom en sentral rutine som administreres av kommunedirektørens fagstab. Enhetsleder bestiller roller i HR-portalen til ansatte via "ERP-tilgangsskjema". Enhetsleder kan også delegere stedfortrederrolle via skjema i Bluegarden. Revisjonen har innhentet dokumentasjon, i form av ERP-skjema, for utvalgte personer som har fått tilgang til HR-portalen i 2021. På de ERP-skjemaene som vi har testet går det frem hvilken tilgang disse personene skal ha i HR-portalen. ERP support[22] opplyser at det kun er enhetsledere og de med delegert fullmakt (autoriserte bestillere) som kan sende inn bestillingsskjemaet "ERP-tilgangsskjema". Revisjonens test av systemet viser at det kun er autoriserte bestillere som har tilgang til dette skjemaet.

4.1.4 Revisjonens vurdering av tilgangsadministrasjon:

For de testene vi har utført fungerte tilgangsadministrasjonen tilfredsstillende. Alle de endringer i brukere som er testet i 2021 er bestilt av autorisert bestiller. Det er også jevnlig gjennomgang av brukere med utvidede roller i TK-nettet og i IT-systemene LIFT og Bluegarden.

---

[19] Superbrukere og Systembrukere er brukere med utvidede brukerrettigheter til IT-systemer

[20] Remittering vil si at bedrifter betaler regninger fra regnskapsprogram ved å overføre en liste med fakturaer til et venteregister i banken.

[21] HR-portalen: En nytilsatt i kommunen blir registrert av egen enhet i HR-Portalen i lønnssystemet.

[22] ERP-support er et team i kommunen som har ansvar for drift og forvaltning av kommunens administrative systemer

Revisjonen anbefaler at kommunen vurderer risikoen ved at ansvaret for sletting av brukere er delegert til enhetene uten en sentral oppfølging fra IT-tjenesten.

4.2 Er det tilfredsstillende endringshåndtering av IT-systemer i Trondheim kommune?

4.2.1 Revisjonskriterier

Gode rutiner for endringer av IT-systemer er viktig for å sikre at kommunen bare tar i bruk endringer som er tilstrekkelig testet og godkjent av de rette ansvarlige. NSMs grunnprinsipper for IKT-sikkerhet anbefaler tiltak for å sørge for god endringshåndtering. Det anbefales at det etableres en formell prosess for å håndtere og dokumentere alle forslag til endringer i virksomheten (kommunen). Prosessen for endringshåndtering bør ifølge NSM inneholde gjennomgang av forslag, risikovurdering, beslutning og planlegging av implementering.

Ekstern revisor hos leverandørene for økonomisystemet LIFT, lønnssystemet Bluegarden og Sopra Steria[23] utarbeider ISAE 3402-uttalelse som gir kommunen en uavhengig erklæring vedrørende leverandørenes kontrollmiljø ved behandling av regnskapsdata for kommunen.

På bakgrunn av dette har vi utledet følgende kriterier:

Kommunen skal ha tilfredsstillende endringshåndtering for IT-systemer. Trondheim kommune skal:

- ha etablert en formell prosess[24] for å håndtere, dokumentere og gjennomføre endringer
- foreta teknisk gjennomgang[25] av forslag til endringer
- beslutte[26] om endringer skal gjennomføres
- planlegge implementering av godkjente endringer (herunder testing).

4.2.2 En formell prosess for å håndtere, dokumentere og gjennomføre endringer i IT-systemer

Ny temaplan for IT ble vedtatt i Bystyret 3.3.2021. I samme bystyrevedtak, pkt 7, opphever Bystyret tidligere vedtak om arkitekturprinsipper[27] av 22. mai 2014. Bystyret erstatter dette med et generelt vedtak om at Trondheim kommune skal følge minimumskravene til Digitaliseringsdirektoratets til enhver tid gjeldende arkitekturprinsipper. Prinsippene skal legges til grunn ved etablering av nye IT-løsninger[28] eller ved vesentlige ombygging av eksisterende IT-løsninger. Prinsippene gjelder både ved egenutvikling og ved anskaffelser. Dermed vil Digitaliseringsdirektoratets arkitekturprinsipper være en rettesnor ved endringer i eksisterende IT-systemer i Trondheim kommune.

4.2.3 Teknisk gjennomgang av forslag til endringer av IT-tjenestene

[23] Sopra Steria drifter IT-systemer for Trondheim kommune.

[24] En prosess for å vurdere og godkenne endringer som skal gjennomføres

[25] En teknisk gjennomgang av en endring i forhold til kommunens eksisterende IT-løsninger

[26] Dokumentert beslutningen skriftlig, feks i et møtereferat, bestilling eller lignende.

[27] Arkitekturprinsipper - design, utvikling og forvaltning av IT-løsninger

[28] IT-løsninger kan omfatte alt fra trådløst nettverk, lagringstjenester, adgang- og innloggingsløsninger, nettverksservere og programvarer.

Kvaliteket inneholder en rutine kalt "Tjenestestyring av IT-løsninger i Trondheim"[29]. Hensikten med rutinen er å beskrive hvilke overordnede oppgaver som inngår i begrepet tjenestestyring, roller som utøver ansvaret og hvordan beslutning om endringer av IT-løsninger skal ivaretas overfor dataeier og prosesseier.

Med tjenestestyring menes summen av aktiviteter som må gjennomføres for å forvalte en IT-tjeneste på en forsvarlig måte. Tjenestestyringen består i å sikre at prosessene rundt IT-løsningene er ivaretatt. Rutinen beskriver blant annet hvordan endringer og nye behov skal håndteres. Rutinen viser til at det er utarbeidet retningslinjer som beskriver hvordan en endring skal behandles, herunder hvilke parter som skal samvirke. Det foreligger en egen beskrivelse av endringer som skal behandles særskilt ved at de eksempelvis er omfattende, berører mange brukere og lignende.

Rutinen beskriver en slik fremgangsmåte for endringer som involverer IT-tjenesten:

1. Ved etablering eller endring av integrasjoner på løsninger meldes dette til IT tjenesten v/arkitektur og utvikling for å vurdere aktuelle integrasjonsmuligheter og for informasjon om pågående initiativ.
2. Endringer som berører tilstøtende løsninger meldes inn til IT tjenesten – som vurderer evt utfordringer med endringsforslaget
3. Ved tjenestebrudd[30] – sikre at dette følges opp iht til avtalen og informasjon om tjenestebruddet varsles IT tjenesten. Ved større brudd etableres kontakt med IT tjenesten for bistand til å håndtere hendelsen.
4. Ved avtalemessige uklarheter – etablere kontakt med Innkjøpstjenesten og/eller IT-tjenesten for å få bistand i arbeidet opp mot leverandøren.

4.2.4 Beslutninger om endringer

Vi har fått opplyst at det ikke skal være de samme rutinene for endringshåndtering for alle IT-systemene, da systemene er forskjellige i omfang og har ulik betydning for driften (kritikalitet). Tjenesteeier[31] skal ha ansvaret for sine fagområder og må velge hvilke rutiner for endringshåndtering som skal praktiseres. Endringshåndtering skal derfor håndteres av fagområdene i kommunen som benytter de forskjellige IT-systemene, og rutinene trenger derfor ikke å være felles. Valg av fremgangsmåte vil derfor være opp til tjenesteeier i samhandling med IT-tjenesten. Generelt vil avtalen med leverandørene (SLA[32] og avtale med skyleverandør[33]) være førende for hvordan endringene skal gjennomføres. Kommunen opplyser også at det finnes maler som omtaler endringshåndtering for de store systemleverandørene.

Kommunedirektøren har vedtatt en rutine kalt "Kvalifisering av IT-prosjekter - investeringsmidler og ressursstøtte - Porteføljeplan". Hovedmålet med rutinen er å sikre at kommunedirektørens ledergruppe får et best mulig grunnlag for å vurdere hvilke IT-tiltak som skal prioriteres, og sikre at de viktigste prosjektene blir startet. Det vil si at disse rutinene er rettet mot prosjekter eller

[29] Dokument-ID: 10233-9. Siste revisjonsdato 14.01.2020.

[30] Avbrutt av leveranse av IT-tjeneste/IT-løsning/IT-system

[31] En tjeneste-eier er en rolle i organisasjonen som har ansvar for tjenester innenfor et definert område.

[32] Service Level Agreement - en avtale mellom en som tilbyr en service og kunden. Avtalen sier noe om hva som omfattes av tjenesten når det gjelder kvalitet, tilgjengelighet og ansvar.

[33] En skyleverandør er et selskap som leverer nettskybaserte tjenester og løsninger til bedrifter og enkeltpersoner.

endringstiltak av vesentlige størrelser og viktighet i kommunen.

Kvaliteket inneholder også en rutine som beskriver "Endringsbehandling av IKT i Trondheim kommune".[34] Rutinen gjelder innføringsprosjekter og tjenesteforvaltere[35]. Det presiseres her at alle endringer i kommunens IT-tjenesteplattform skal være underlagt endringskontroll og skal behandles etter retningslinjene. Rutinen definerer roller og ansvar i endringsprosessen. Et endringsråd skal vurdere endringene. Endringer skal klassifiseres etter type og behandles deretter. Endringstypene er definert til; nødendring, stor normal endring, liten normal endring og standard endring. Revisjonen får opplyst at rutinen følges, men dokumentet er ikke revidert siden det ble opprettet.

Deltakerne i Endringsrådet[36] er endringskoordinator ved IT-tjenesten, prosessansvarlig ved IT-Tjenesten og en endringskoordinator hos den enkelte leverandør. IT-tjenesten opplyser at ved behov stiller teknisk kompetanse fra både IT-tjenesten og den enkelte leverandør opp i formøte før møtet i Endringsrådet for å sikre kvaliteten av endringen, og sikre at all nødvendig informasjon blir presentert.

4.2.5 Planlegging av innføring av godkjente endringer (herunder testing)

Når kommunen tar i bruk nye skyløsninger[37] har vi sett at kommunens rutiner blir tilpasset leverandørenes rutiner for testing, godkjenning og implementering av endringer i IT-systemer. Dette vil utfordre etablerte rutiner for planlegging av implementering av godkjente endringer.

Ved skyløsninger har vi fått opplyst at leverandørene gjør endringer i systemer uten å involvere kunden i prosessen i særlig stor grad. Dette begrunnes ofte med at IT-systemene er såkalte "hyllevarer" som skal passe for flere kunder. Endringer i disse IT-systemene kommer derfor til dels i konflikt med noen av kommunens tidligere retningslinjer på området, men er mer i tråd med føringer i Digitaliseringsdirektoratets arkitekturprinsipper[38], som kommunen har vedtatt å følge. Eksempler på dette er endringer som blir gjort i økonomisystemet LIFT og i HR-portalen.

I avtalene mellom kommunen og leverandørene av de største IT-tjenestene er det avtalt at det skal foretas vurderinger fra en ekstern tredjepart og avgis ISAE 3402-uttalelser. Revisjonen gjennomgår disse uttalelsene når de blir avgitt. Her omtales blant annet leverandørens rutiner for endringshåndtering.

Den seneste ISAE 3402-uttalelsen[39] for LIFT hos TietoEVRY har beskrevet avvik på området endringshåndtering hos leverandøren. Dette avviket omhandler både godkjenning av endringer før implementering, og manglende skriftlig dokumentasjon på avviksrapportering. Leverandøren opplyser at dette i ettertid er håndtert gjennom å oppgradere verktøy for håndtering av slike feil.

---

[34] Denne er datert 6.4.2018.

[35] En tjenesteforvalter er en fagperson som har ansvar for den daglige driften av et IT-system. Herunder å administrere tilganger til IT-systemet. Tjenesteforvalter er et bindeledd mellom leverandør og Trondheim kommune.

[36] Endringsrådet som består av IT-personell hos Trondheim kommune og leverandør, skal være kvalifisert til å vurdere alle konsekvensene av de foreslåtte endringene.

[37] En skyløsning er et IT-system/løsning som blir levert av en skyleverandør (se over).

[38] Overordnede arkitekturprinsipper for offentlig sektor som skal bidra til at digitale tjenester fra offentlige virksomheter blir gode og brukervennlige for innbyggerne, og til bedre samhandling på tvers i hele offentlig sektor.

[39] ISAE 3402, 22. januar 2021

Saken er nå lukket av leverandøren.

Kommunen har også innhentet ISAE 3402-uttalelser for lønnsystemet Bluegarden som blant annet omtaler endringshåndteringen hos leverandøren av systemet. Den forrige uttalelsen fra 2018 fra leverandøren Bluegarden viste god intern kontroll på området og det er derfor ikke innhentet tilsvarende rapporter for 2019 og 2020. Lønnssystemet er nå kjøpt opp av Visma. Det vil derfor bli innhentet en ISAE 3402-uttalelse for lønnssystemet for 2021.

For 2020 ble det innhentet ISAE 3402-uttalelse for Sopra Steria[40]. Kontrollene er utført og rapportert av et revisjonsselskap. Uttalelsen rapporterte mindre avvik både for ordinære endringer og nødendringer. Sopra Steria har opplyst at det er etablert tiltak som skal lukke avvikene.

4.2.6 Revisjonens vurdering av endringshåndtering:

På bakgrunn av undersøkelsen mener vi at Trondheim kommune har etablert formelle prosesser for å håndtere, dokumentere og gjennomføre endringer i IT-systemer. Dette omfatter både teknisk gjennomgang, beslutning om endringer skal gjennomføres og implementering av godkjente endringer. Revisjonen mener imidlertid det er noe uklart hva som er gjeldende rutiner for endringshåndtering av skyløsninger i kommunen.

4.3 Har kommunen tilfredsstillende datasikkerhet og beredskapstiltak

4.3.1 Revisjonskriterier

Ifølge Nasjonal sikkerhetsmyndighet (NSM) står Norge overfor et komplekst risikobilde der fremmede stater og andre aktører forsøker å utnytte sårbarheter i funksjoner, virksomheter og systemer. Covid 19-pandemien har medført raskere digitalisering og har bidratt til å forsterke dette risikobildet. I januar 2021 ble Østre Toten kommune rammet av et løsepengevirus. Dataangrepet satte flere av kommunens systemer ut av drift, og gjorde noen av kommunens tjenester utilgjengelige. Kommunen måtte planlegge analoge løsninger for drift og mange oppgaver måtte håndteres manuelt. Høsten 2020 ble Stortinget rammet av et alvorlig datainnbrudd. Ifølge PST[41] viser etterforskningen at det er hentet ut sensitivt innhold fra en del av de berørte e-postkontiene under dette datainnbruddet i 2020. Stortinget ble også utsatt for dataangrep i 2021.

Dersom et dataangrep mot kommunen lykkes, kan det føre til at kommunen blir lammet over en lengre periode. Det kan medføre store kostnader å få kommunen tilbake til normal drift. Et dataangrep kan også medføre at sensitive data kommer på avveie. Det kan innebære brudd på personvernet og rettsikkerheten til den enkelte borger. Dersom sensitive data misbrukes av andre eller kommer på avveie kan det medføre erstatningskrav og/eller bøter for kommunen.

KS sendte den 8.2.2021 brevet "Datasikkerhets- og beredskapstiltak i kommunal sektor" til kommuner og fylkeskommuner der de gir råd på bakgrunn av dataangrepet mot Østre Toten

[40] Sopra Steria arbeider med strategiutvikling, IT-rådgivning, systemutvikling og digitale løsninger. I tillegg har de en egen avdeling som jobber med drift av systemer og infrastruktur hos sine kunder. Blant annet drifter Sopra Steria Oslo kommune og Trondheim kommune.

[41] PST: Politiets sikkerhetstjeneste

kommune og trusselbildet i det digitale rom. Vi har i denne undersøkelsen innhentet informasjon om Trondheim kommune etterlever de anbefalingene som KS har gitt. Anbefalingene fra KS inneholder følgende elementer: Identifisere og vurdere risiko, etablere tiltak for å håndtere risiko og oppfølging og evaluering av av risikostyringen.

På tross av god risikostyring kan kommunen bli rammet av uønskede hendelser som påvirker IT-driften. I så fall er det viktig at kommunen har etablert planer for å håndtere dette.

På bakgrunn av dette har vi utledet følgende kriterier. Trondheim kommune bør:

- ha identifisert og vurdert risikoen for kommunens IT-funksjon

- ha iverksatt tiltak for å sikre IT-systemer og IT-utstyr
    - etablert tiltak for å håndtere identifisert risikoer slik at risikoen blir akseptabel
    - tiltak for å beskytte kommunens data mot uautorisert tilgang, uautorisert endring/sletting av data eller uautorisert fjerning av kommunens tilgang til egne data
    - overvåkningssystemer som oppdager dataangrep så raskt som mulig
    - sikring av backup av kommunens data slik at data kan rekonstrueres
    - sikring av logger slik at disse ikke kan slettes ved datainnbrudd. Logger kan gi viktig informasjon om hva som har skjedd under et datainnbrudd
    - reserveløsninger dersom kritiske IT-systemer og data ikke er tilgjengelig
    - tiltak for å sikre at gammelt IT-utstyr og programvare, som ikke lenger mottar oppdatering, ikke utgjør en sikkerhetsrisiko
    - forsvarlig kassering av maskinvare slik at data ikke kommer på avveie

- følge opp og evaluere risikostyringen for IT-området
    - oppfølging av risikostyringsprosessen gjennom løpende ledelsesaktiviteter og eller frittstående evalueringer
    - gjennomføre sikkerhets- og sårbarhetstester av IT-infrastruktur og systemer

- ha etablert planer for å håndtere uønskede hendelser[42]
    - etablert en beredskapsplan for IT-sikkerhet
    - beredskapsplanen testes
    - forsikring mot datakriminalitet

4.3.2 Identifisering og vurdering av risikoen for kommunens IT-funksjon

For å kunne sette i verk riktige tiltak for å sikre kommunens IT-systemer og utstyr bør man ha identifisert hvilke uønskede hendelser som kan oppstå. For å vurdere hvilken risiko kommunen har innenfor IT-området kan man gjennomføre en risiko- og sårbarhetsanalyse (ROS-analyse).

Revisjonen har undersøkt om det er foretatt en overordnet ROS-analyse for IT-området. Vi har fått opplyst at det ikke er gjennomført en egen ROS-analyse for IT-området, men det ble gjort en helhetlig ROS-analyse i Trondheim kommune i 2018. Denne analysen handlet om pandemi, leirras og infrastruktur. Vi har innhentet denne ROS-analysen der informasjons- og kommunikasjonsteknologi er definert som kritisk infrastruktur. Strømbrudd og cyberangrep med

[42] For eksempel en beredskapsplan og reserveløsninger

bortfall av elektronisk kommunikasjon er omtalt i denne analysen. En stadig større avhengighet av IKT er påpekt som en åpenbar risiko og sårbarhetsfaktor og denne risikoen vil sannsynligvis øke i takt med den teknologiske utviklingen. Det vurderes at risiko knyttet til IKT må få økt fokus. I ROS-analysen er det anbefalt å se nærmere på risiko og konsekvenser av tap av e-kommunikasjon og utfall av internett og kritiske IT-systemer. Kommunen har benyttet ISO 31000 (internasjonal standard for risikostyring) for å identifisere, analysere og evaluere risiko.

Trondheim kommunes overordnede mål for informasjonssikkerhet er beskrevet i dokumentet "Overordnet styringsdokument for informasjonssikkerhet. Informasjonssikkerhetsstrategi 2021" Kommunen skal ifølge dette dokumentet ha informasjonssikkerhet som sikrer ivaretakelse av konfidensialitet, tilgjengelighet og integritet i samsvar med lov, forskrift og forventninger fra innbyggere, tjenestemottakere og overordnede forvaltningsmyndigheter. Ifølge dette dokumentet er det statistisk sett ansatte, som gjennom uaktsomme eller bevisste handlinger, er den hyppigste trusselutøveren mot informasjonssikkerheten. Kommunen trues også av eksterne trusselaktører som ønsker å skaffe seg ulovlig adgang til informasjon, enten for å stjele eller ødelegge informasjon, eller for å presse enkeltpersoner eller kommunen for penger, eller for å oppnå andre fordeler.

4.3.3. Tiltak for å sikre IT-systemer og IT-utstyr

I henhold til teori om intern kontroll, som for eksempel ISO 31000 som kommunen har benyttet, må man etablere tiltak for å håndtere identifisert risiko slik at denne holdes på et akseptabelt nivå. Basert på kommunens risikovurdering og hendelser som er kjent gjennom media er aktuelle risikoer og tiltak for IT-systemer og utstyr:

- Risiko: Uvedkommende kan få tilgang til sensitiv eller beskyttelsesverdig informasjon som behandles i IT-systemene
  Tiltak: Kommunen sikrer IT-systemer og data mot uautorisert tilgang

- Risiko: Informasjonen som behandles i kommunens IT-systemene er ikke pålitelig, den kan ha blitt endret eller slettet på uautoriserte måter?
  Tiltak: Kommunen sikrer sine data mot uautorisert endring

- Risiko: Informasjonen som behandles i kommunens IT-systemer og data blir utilgjengelig for de som har legitim tilgang til og behov for tilgang til systemene og dataene?
  Tiltak: Kommunen må sikre tilgang til IT-systemer og data for autoriserte brukere

4.3.3.1 Sikring av IT-systemer og data mot uautorisert tilgang

For å beskytte kommunens systemer og data er det viktig å benytte tilstrekkelig sikkerhetsnivå. Trondheim kommune har ifølge IT-tjenesten en god løsning for sikkerhet. Følgende titak er etablert:

- APN (Acdcess Point Name): APN styrer tilgangen til de dataressursene man er autorisert for å ha tilgang til. Dette gjelder primært for mobil aksess.
- To-faktor-autentisering: Med to-faktor/to-trinns bekreftelse logger man seg inn i kommunens systemer med sitt passord i tillegg til en kode man får tilsendt på sin mobiltelefon. To-trinns-bekreftelsen gjør kontoen sikrere fordi den hindrer uvedkommende i å logge seg inn på kontoen selv om de de kjenner passordet.
- Kryptert disk: Data på kommunens PC-er er kryptert. Det vil si at data på PC-ene er

omformet slik at de ikke kan leses eller endres av noen som urettmessig får tilgang til dem. Dette sikrer kommunens data dersom en PC blir stjålet.

Dersom kommunen skulle bli utsatt for er dataangrep er det viktig at man har overvåkningssystemer som oppdager slike angrepet så raskt som mulig. Vi har forespurt om status på kommunens overvåkningssystemer som skal gi varsel om mulig dataangrep/ innbrudd i kommunens IT-systemer.

Vi har fått opplyst at dataangrep overvåkes på ulike steder i kommunens tjenesteplattform[43].

- På ytterkanten av kommunens intranett, det vil si med brannmur[44]
- På endepunkter, som sikkerhetsfunksjoner på for eksempel PC i form av antivirusprogram[45]
- Overvåkning på servernivå[46] og skytjenester[47].

Alle tjenester som kjører på Trondheim Kommunes driftsplattform har overvåkning mot dataangrep i flere lag. De tjenestene som leveres eksternt har tilsvarende krav til overvåkning basert på risikovurdering. Denne overvåkningen involverer også alle kommunens IT-driftsleverandører, IT-tjenesteleverandører og underleverandører som har avtaler gjennom kommunens IT-tjeneste. Dersom det skjer dataangrep om natten er det varsling til IT-brukerhjelp, som er en del av IT-tjenesten i kommunen. De har døgnåpen vakttelefon (24 timer i døgnet, 365 dager i året). De kobler på IT-sjefen i kommunen ved behov. Vi har fått opplyst at driftsleverandører har operativ vakt hele døgnet.

Alle viktige hendelser på IT-området, herunder også sikkerhetsrelaterte, blir dokumentert i en rapport hvor også forbedringer og læringspunkter beskrives. Disse følges opp i etterkant i de jevnlige drift- og sikkerhetsmøtene med de involverte leverandørene.

Kommunen har høsten 2021/ vinter 2022 sendt ut et elektronisk kurs om informasjonssikkerhet til alle ansatte. Det ble på forhånd gjennomført nettfisking (phishing)[48] mot alle ansatte i form av en e-post med en lenke. Dette ble gjort for å teste om ansatte trykket på lenken i en e-post fra en avsender der det kunne være risiko for forsøk på phishing. De ansatte som trykket på lenken ble videresendt til en nettside med en leksjon om nettfisking.

Det elektroniske kurset har bestått av temaene passordsikkerhet, nettfisking, sikkerhet rundt IT-nettverk, virusbeskyttelse på PC og sikkerhet rundt mobiltelefon. Tilsvarende kurs ble også holdt for kommunens ansatte høsten 2019.

[43] Tjenesteplattform inneholder fundamentale funksjonelle og teknologiske deler som gjør det mulig å definere, bygge, eksponere og levere tjenester til brukere/mottakere.

[44] Brannmur, programvare eller maskinvare som skal avvise uønsket kommunikasjon til et program, en datamaskin eller et nettverk. Brannmuren hindrer at utenforstående skal kunne nå tjenester eller informasjon som ikke skal være tilgjengelig.

[45] Antivirusprogram er et program på en datamaskin, som forsøker å identifisere, motarbeide og fjerne datavirus og liknende ondsinnet programvare

[46] Server, datamaskin eller dataprogram som leverer tjenester til klienter i et nettverk.

[47] Skytjenester er en samlebetegnelse på alt fra dataprosessering og datalagring til programvare på servere som er tilgjengelig fra eksterne serverparker tilknyttet internett.

[48] Nettfisking (phishing) forsøk på å få tak i etter sensitiv informasjon, som passord eller kredittkortnummer

Trondheim kommune går nå over til skydrift på sikkerhet. IT-tjenesten opplyser at ansattes PC-er nå blir løpende oppdatert på sikkerhet direkte fra sikkerhetsleverandøren. Det vil ifølge IT-tjenesten styrke sikkerheten.

For å beskytte kommunens e-postsystem mot angrep har kommunen, ifølge det vi har fått opplyst, iverksatt følgende sikkerhetstiltak for epost-løsningen:

- SPF (Sender Policy Framework): En e-postautentiseringsmetode utviklet for å oppdage forfalskede avsenderadresser under levering av e-posten
- DKIM (DomainKeys Identified Mail): En e-postautentiseringsmetode designet for å oppdage forfalskede avsenderadresser i e-post (e-postforfalskning), en teknikk som ofte brukes ved nettfisking og e-postspam (søppelpost).
- DMARC (Domain based Message Authentication, Reporting and Conformance): DMARC er en e-postautentiseringsprotokoll. Den er designet for å gi e-postdomeneeiere muligheten til å beskytte domenet[49] sitt mot uautorisert bruk, ofte kjent som e-postforfalskning. Beskytte et domene fra å bli brukt i e-postangrep, nettfiskings-e-poster, e-postsvindel og andre cybertrusselsaktiviteter

Gammelt IT-utstyr og programvare som ikke lenger mottar oppdatering kan utgjøre en sikkerhetsrisiko da dette utstyret ikke er oppdatert på sikkerhet. Det kan også være en risiko for at det ikke føres tilsyn med dette utstyret slik at det er en risiko for at uautorisert bruk ikke blir oppdaget.

Vi har undersøkt om kommunen har en rutine for å fase ut og sikre programvare og maskinvare som ikke lenger mottar oppdateringer. Installering av programvare i kommunen styres av en programvarekatalog som administreres av IT-tjenesten. Det er et fåtall personer i kommunen (færre enn 20 personer) som har administratorrettigheter til å installere programvare som ikke ligger i programvarekatalogen. Alle PC-klienter overvåkes i tillegg av en løsning som heter Snow. Dette er et lisensovervåkningssystem som gir kommunen et oppdatert bilde til enhver tid over hvilken programvare som er installert. Fjerning av gammel programvare styres av IT-drift i kommunen. All programvare installeres, etter det vi har fått opplyst, fra en firmaportal. Her ligger til enhver tid de siste versjonene av programvaren. I tillegg mottas det i portalen varsler om sikkerhetsproblemer fra leverandører vedrørende feil i programvaren som skal utbedres.

Vi har fått opplyst at kommunen jobber helhetlig med sårbarhetshåndtering når det gjelder programvare. EOL (end of life) programvare som skal fases ut og EOS (end of service/support) programvare som ikke lenger vil motta oppdatering er et viktig moment i sårbarhetsvurderingen. Sårbarhetene til programvaren vektes etter hvor kritisk programvaren er for kommunen. Det vurderes hvor mange installasjoner det er av den sårbare programvaren, hvor ofte programvaren blir brukt og om sårbarheten i programvaren har blitt misbrukt. Vektingen brukes til å prioritere, hvor sårbarheten skal reduseres. Ut ifra opplysninger fra programvareleverandør oppdateres, oppgraderes eller slettes programvaren. Risiko vedrørende EOL/EOS aksepteres unntaksvis, med eventuelle sikkerhetskontroller, i en overgangsfase før det kommer en ny programvare på plass for virksomheten.

[49] Domene er et administrativt delområde i et datasystem eller datanettverk.

Kommunens eksponeringsgrad[50] kalkuleres ut i fra det totale risikobildet av den installerte programvaren. Hendelser, sårbarheter og eksponeringsgrad rapporteres inn til felles sikkerhetsmøte med kommunens driftsleverandører. For sårbarheter som skal reduseres blir det opprettet saker for driftsteamet[51] og dette blir fulgt opp i daglige morgenmøter. I tillegg til dette så jobber sikkerhetsteamet[52] aktivt i sikkerhetsløsningen og får beskjed om nye sårbarheter. I portalene til sikkerhetsløsningen kan man se detaljerte sårbarhetsbeskrivelser og total eksponeringsgrad ved alvorlige sårbarheter.

Når det gjelder maskinvare som skal kasseres er det viktig at dette gjøres på en forsvarlig måte slik at data som eventuelt ligger lagret på disse datamaskinene ikke kommer på avveie. Vi har undersøkt hvilke rutiner kommunen har for kassering av maskinvare.

Kassering av maskinvare gjøres etter det vi har fått opplyst på en sikkerhetsmessig og miljømessig riktig måte av kommunens maskinvareleverandør. Leverandørene er sertifisert innenfor disse områdene. Innlevering (henting) av utstyr bestilles i kommunenes e-handelssystem.

Innføringen av GDPR[53] (personvernforordningen) i 2018 stiller økte krav til beskyttelse av personsensitive data. I brevet fra KS vedrørende datasikkerhet tas det opp spørsmål om kommunen har etablert nødvendig personvernkompetanse til å gjøre løpende vurderinger av sikkerhet og personvern samt rapportere tilstanden til kommunen. Trondheim kommune har en informasjonssikkerhetsansvarlig som også har rollen som personvernombud. Vedkommende har sitt hovedarbeidsområde innen informasjonssikkerhet og personvern, rådgiving og oppfølging. Personvernombudet skal kontrollere at kommunen overholder personvernreglene, drive holdningsskapende arbeid og lære opp personalet som behandler personopplysninger og gi råd om personvernkonsekvenser i ulike saker.

For øvrig er kommunens håndtering av tildeling, endring og sletting av tilganger til IT-systemene omtalt i punkt 4.1 i denne rapporten.

4.3.3.2 Sikring av data mot uautorisert endring

Det er viktig å kunne stole på at kommunens data er riktige og at dataene ikke kan endres på en uautorisert måte. Sikring mot slik endringer av data gjøres blant annet ved å hindre uautorisert tilgang til kommunens IT- systemer og utstyr. Dersom det likevel skulle skje at uautoriserte personer skulle få tilgang til kommunens data og endre, slette eller kryptere disse er det viktig at det finnes gjenopprettelsesrutiner som sikrer at data kan rekonstrueres.

Vi har undersøkt om det tas sikkerhetkopi av av kommunens data, og om dette er sikret slik at de ikke kan bli slettet, kryptert eller manipulert ved et eventuelt datainnbrudd. Vi får opplyst at sikkerhetskopiene for data ved lokal drift (systemer som driftes av Sopra Steria) er skilt fra Windows-domenet[54]. Det vil si at sikkerhetskopien ikke blir tilgjengelig for eksterne hackere som

[50] Eksponeringsgrad i denne sammenheng er samlet sårbarhet knyttet til programvaren

[51] Driftsteamet er ansatte ved avdeling for drift og support ved IT-tjenesten i kommunen

[52] Sikkerhetsteamet er ansatte ved avdeling for drift og support ved IT-tjenesten i kommunen

[53] GDPR er en forordning som skal styrke og harmonisere personvernet ved behandling av personopplysninger i Den europeiske union (EU).

[54] Windows-domener gir nettverksadministratorer en måte å administrere et stort antall PCer og kontrollere dem fra ett sted. En eller flere servere - kjent som domenekontrollere - har kontroll over domenet og datamaskinene på det.

eventuelt bryter seg inn i kommunens systemer.

E-post, arbeidsdokumenter og informasjonssider lagres i Google skylagring[55]. Data som blir slettet blir liggende i en digital papirkurv i 30 dager. Man kan gjenopprette filer fra papirkurven før det har gått 30 dager. Etter 30 dager i papirkurven blir filene permanent slettet. Det er store kostnader forbundet med etablering av en sikkerhetskopi i Google-skyen, og dette er derfor ikke satt opp. Det som er permanent slettet er derfor borte.

Kommunens regnskapssystem LIFT og lønnssystemet Bluegarden er skysystemer. Skytjenester er en samlebetegnelse på alt fra dataprosessering og datalagring til programvare på servere som er tilgjengelig fra eksterne serverparker tilknyttet internett. For disse systemene har skyleverandører speiling av data. Det vil si at datene er lagret i to like versjoner som er adskilt fra hverandre. Dataene er dermed beskyttet med en kopi som er tilgjengelig til enhver tid.

Ved eventuelle datainnbrudd må det foretas en gjennomgang av logger[56] for å kunne avklare hva som har skjedd under innbruddet. Dersom data hentes ut fra kommunens systemer er det en risiko for at taushetsbelagte og personsensitive data blir blir offentliggjort eller solgt. For å få informasjon om hva som har skjedd under datainnbruddet er det viktig at kommunens logger er sikret slik at disse ikke kan slettes ved et eventuelt datainnbrudd.

Kommunes loggsystemer er, etter det vi har fått opplyst, separate løsninger som ikke er koblet til tjenesteplattformen på en slik måte at de potensielt kan ødelegges eller gjøres utilgjengelig dersom kommunens systemer blir utsatt for et dataangrep.

4.3.3.3 Sikring av tilgang til IT-systemer og data for autoriserte brukere

De fleste kommunale tjenester er helt avhengig av velfungerende datamaskiner og programmer (IT-infrastruktur) og tilhørende støttesystemer. Det er derfor viktig at kommunen sikrer at systemer og data er tilgjengelig for de som har legitimt behov for tilgang til systemene og dataene.

Vi har undersøkt om det er kartlagt hvilke IT-systemer som støtter de kritiske funksjonene eller tjenestene i kommunen. Det er viktig at disse systemene er tilgjengelige til enhver tid.

Kommunen har satt opp en oversikt som viser hvordan IT-systemene er vurdert i forhold til betydning for driften (kritikalitet) og krav om tilgjengelighet. Oversikten viser at kommunen har foretatt en vurdering og prioritering av de kritiske IT- systemene.

I driftsavtalen med Sopra Steria[57] er IT-systemene klassifisert i henhold til kritikalitet og krav om tilgjengelighet. Det er vurdert hvor kritiske IT-systemene og tjenestene er i forhold til deres:

[55] Skylagring er en modell for datalagring der digitale data lagres på flere servere og ofte på flere steder. Det fysiske miljøet (maskiner og utstyr) er vanligvis driftet og eid av et «hosting»-firma. Disse skylagringsleverandørene er ansvarlig for å holde dataene tilgjengelig til alle tider, mens det fysiske miljøet skal beskytte det en har lagret fra å havne i uvedkommendes hender.

[56] Logging betyr å skrive til et varig og beskyttet lager. Data som skrives kan være: Hvilken del av programmet som er brukt, når det ble brukt og relevante data for situasjonen, for eksempel hvem som bruker programmet og hvilke dataobjekter som er lest eller skrevet.

[57] Sopra Steria er et IT-selskap som drifter IT-systemer for Trondheim kommune

- avhengighet til andre tjenester/systemer
- påvirkning på liv og helse
- påvirkning på økonomi
- påvirkning på Trondheim kommunes tjenestemottakere (innbyggere, næringsliv ol)
- kommunens omdømme

De IT-systemer som er definert som kritiske i Trondheim kommune har krav om tilgjengelighet 24 timer i døgnet, 365 dager året. Vi har etterspurt informasjon om det er etablert reserverutiner i kommunen som blir satt i verk om kritiske IT-systemer er ute av drift over tid.

De kritiske systemene finnes primært innenfor helse- og velferdsområdet. Det er etablert manuelle reserverutiner som skal tas i bruk dersom IT-systemet Gerica[58] er ute av drift over tid. Disse manuelle rutinene har blitt brukt ved noen anledninger og har, etter det vi har fått opplyst, vist seg å fungere som tiltenkt. Disse reserverutinene er papirbaserte og skal være kjent for personene det gjelder. Vi har fått opplyst at det for andre systemer er mer krevende å opprettholde tjenesteproduksjon ved langvarige feilsituasjoner. Dette gjelder blant annet systemer for legevakten, digital trygghetsalarm, trygghetspatruljen og pasientvarsling.

4.3.4 Oppfølging og evaluering av risikostyringen for IT-området

I henhold til teorien (for eksempel ISO 31000) skal risikostyring følges opp, evalueres og endres etter behov. Oppfølgingen kan utføres gjennom løpende ledelsesaktiviteter, frittstående evalueringer eller begge deler.

Brevet fra KS "Datasikkerhets- og beredskapstiltak i kommunal sektor" til kommunedirektørene, datert 8.2.2021, anbefaler flere tiltak for å øke kommunens sikkerhets- og beredskapsevne innen datasikkerhetshendelser og datainnbrudd. Herunder å gjennomføre sikkerhetsrevisjon[59] av IT-infrastruktur og systemer og gjennomføre sikkerhets-[60]-og sårbarhetstester av kommunens IT-infrastruktur og systemer.

Vi har spurt kommunen om det er gjennomført sikkerhetsrevisjon av kommunens IT-infrastruktur og systemer. Bystyret vedtok i mars 2021[61] at kommunens IT-sikkerhet skulle gjennomgås. Bystyret ba kommunedirektøren utarbeide en politisk sak som redegjør for teknologiplanens mulige konsekvenser for kommunens og innbyggernes datasikkerhet og hvilke beredskapstiltak som er, og planlegges, iverksatt. Bystyret ba videre om at kommunedirektøren skal gjennomføre en vurdering av konsekvenser for personvern og informasjonssikkerhet som følge av mer utstrakt bruk av globale skyløsninger fremover. Vurderingen skulle svare ut ulike problemstillinger rundt slike løsninger, og vise hvordan kommunens ansvar for å ivareta informasjons- og personansvaret for den enkelte innbygger blir ivaretatt.

Kommunen inngikk avtale med et konsulentselskap om å foreta denne gjennomgangen.

[58] Gerica er et elektronisk pasientjournalsystem. Gerica produserer også fakturagrunnlag for fakturering av egenandeler for helsetjenester.

[59] IT-sikkerhetsrevisjonen gir en oversikt over dagens situasjon for virksomhetens sikkerhetsnivå. Den beskriver også ulike tiltak som kan gjennomføres for å øke virksomhetens IT-sikkerhet til et ønskelig og anbefalt nivå.

[60] Sikkerhets- og sårbarhetstesting gjøres for å vurdere hvor godt systemer og brukere er i stand til å håndtere sikkerhetshendelser herunder dataangrep, samt for å identifisere tekniske og menneskelig sårbarheter. Testingen gir en oversikt over sikkerhetshull i nettverk, infrastruktur eller IT-systemer.

[61] Bystyresak 5/21. Temaplan for teknologi og modernisering.

Rapporten skal, etter det vi har fått opplyst, belyse funn og analysere dagens situasjon vedrørende informasjonssikkerhet og personvern (inkludert roller og ansvar). Rapporten er forventet å levere et revidert målbilde og styringssystem på informasjonssikkerhet og personvern, basert på tidligere arbeid. Det nye målbildet forventes å belyse mer sammenheng mellom teknologi, mennesker, prosesser og kultur. Det skal også tilpasses den teknologiske- og samfunnsmessige utviklingen. Rapporten skal også omhandle risikovurderinger, sky- og skyggeløsninger[62], håndtering av bestemmelser fra Schrems II[63], kompetanse og håndtering av uønskede hendelser. Basert på dagens situasjon og målbilde skal rapporten sette opp en liste over tiltak og anbefalinger for videre arbeid med informasjonssikkerhet og personvern i kommunen.

Høsten 2021 hadde IT-tjenesten i kommunen en skrivebordsøvelse sammen med Sopra Steria[64] for å trene på en et angrep med et løsepengevirus. Det var Sopra Steria som arrangerte øvelsen og kommunen visste ikke på forhånd hva som var innholdet i øvelsen. Kommunen har tidligere hatt teknisk testing.

Vi har imidlertid på forespørsel fått opplyst at kommunen ikke har en overordnet plan for IT-sikkerhet. Men det foreligger et målbilde for arkitektur på sikkerhetsområdet og en informasjonssikkerhetsstrategi.

4.3.5 Etablering av planer for å håndtere uønskede hendelser

I henhold til lov om kommunal beredskapsplikt §14 har kommunen plikt til å kartlegge hvilke uønskede hendelser som kan inntreffe i kommunen og utarbeide en beredskapsplan.

I brevet om datasikkerhets- og beredskapstiltak fra KS presiseres også betydningen av å ha en beredskapsplan hvis kommunen utsettes for dataangrep eller IT-systemer faller bort av annen grunn. For å undersøke om beredskapsplanen fungerer er det viktig at kommunen har gjennomført krise- og beredskapsøvelser med utgangspunkt i bortfall eller manipulering av IT-infrastruktur og systemer.

Vi har undersøkt om Trondheim kommune har beredskapsplaner som trer i kraft dersom dataangrep, eller bortfall av IT-systemer av annen grunn, rammer kommunen.

Kommunen benytter ITIL[65] som rammeverk for forvaltning av IT-prosesser. Vi har fått opplyst at rammeverk og metoder som benyttes ved utarbeidelse av beredskapsplaner er ROS-analyse, trusselvurdering, beredskapsanalyse og skade og ulykkesstatistikk.

Trondheim kommune har etablert en beredskapsplan for IT-tjenesten. Vi har mottatt denne planen som er påført at den er gyldig til 31.12.2019. I denne planen står det i punkt 0.7 at det er et minimumskrav at enhetens beredskapsplan blir revidert årlig. Denne revideringen skal ifølge

[62] Skygge IT er et samlebegrep for programvare og (sky)tjenester utenfor bedriftens eierskap og kontroll.

[63] Schrems II-dommen: EU-domstolen avsa 16. juli 2020 en prinsipiell dom om overføring av personopplysninger til land utenfor EU/EØS. Dersom personopplysninger skal overføres til land utenfor EU/EØS, må man ha et overføringsgrunnlag i henhold til personvernforordningen.

[64] Sopra Steria er et IT-selskap som drifter IT-systemer for Trondheim kommune.

[65] ITIL er et internasjonalt anerkjent sett med prosedyrer som en organisasjon kan benytte til å styre sine IT-operasjoner. Disse prosedyrene er kan brukes uavhengig av hvilken leverandør man bruker og er relevante for alle aspekter av en IT-infrastruktur.

planen gjennomføres i første kvartal hvert år i etterkant av «ledelsens gjennomgang». Vi har fått opplyst at denne beredskapsplanen er under oppdatering, og at relevante erfaringer fra øvelsen som ble gjennomført høsten 2021 skal legges inn. Det forventes etter det vi har fått opplyst ingen store endringer i planen, men noen justeringer når det gjelder kommunikasjonsroller samt behov for å definere og beskrive noen konkrete understøttende tiltak. Eksempler på dette kan være hvordan man skal etablere nettsiden "trondheim.kommune.no" på en ny plattform[66] ved nedetid, eller hvordan man skal legge over sentralbordet til mobil plattform, dersom primærløsningen er ute av drift.

Vi ser at den beredskapsplanen for IT-tjenesten som ligger i Kvaliteket[67] per januar 2022 fortsatt har utløpsdato 31.12.2019. Vi vil vi anta at den spesielle situasjonen i 2020 og 2021 med pandemi som blant har medført bruk at hjemmekontor og digital undervisning har endret risikobildet for kommunens IT-drift.

I samsvar med anbefalingene fra KS har beredskapsplanen til IT-tjenesten angitt navngitte personer med funksjon og telefonnummer.

Vi har spurt kommunen om det er gjennomført krise- og beredskapsøvelser med utgangspunkt i bortfall eller manipulering av IT-infrastruktur og systemer. Vi har fått opplyst at gjenoppretting (recovery) av kritiske infrastrukturtjenester fra backup er en del av beredskapsplanen der det testes at gjenoppretting av tjenester fungerer som de skal i tilfellet angrep der alt er blitt kryptert. Denne testen gjennomføres en gang i året.

Når det gjelder planlagte øvelser på strategisk nivå for bortfall av IKT har dette, ifølge det vi har fått opplyst, ikke vært tema de siste årene. Det opplyses imidlertid at håndtering av reelle hendelser er god trening. I løpet av de siste 5 årene har kommunedirektørens ledergruppe eller deler av denne vært engasjert i flere hendelser som har berørt IKT.

IT-tjenesten gjennomførte høsten 2021, som nevnt i punkt 4.3.4, en øvelse hvor kommunen blir angrepet utenfra. Under øvelsen ble det testet hvordan IT-tjenestens prosesser fungerer i praksis ved slike tilfeller. Det foreligger en evalueringsrapport for denne øvelsen. De største læringspunktene handler, etter det vi har fått opplyst, om samhandling på ulike nivå med eksterne parter som driftsleverandører, effektiv internkommunikasjon til ansatte og etablering av tiltak som er dokumentert og utprøvd i forkant.

Vi har fått opplyst at det ikke er utarbeidet en plan for hvordan beredskapen på IT-området skal testes. Det er imidlertid en ambisjon om å gjennomføre jevnlige tester av beredskapen.

KS anbefaler kommunene å tegne forsikring mot datakriminalitet, herunder datainnbrudd med videre, da et alvorlig dataangrep kan medføre betydelige kostnader. Revisjonen har undersøkt om Trondheim kommune har tegnet slik forsikring.

Vi har fått opplyst at Trondheim kommune har ansvarsforsikring. Det vil si at kommunen er forsikret mot skade på tredjepart som en følge av en eller annen kommunal virksomhet. Det foreligger imidlertid ikke en egen forsikring på datakriminalitet. Vi har fått opplyst at det ikke

[66] En digital plattform en teknisk løsning optimalisert for å samle, oppbevare og bearbeide data man samler inn.

[67] Kvaliteket er kommunens kvalitetssystem med kommunens rutiner

foreligger en egen vurdering angående dette i kommunen, men det er innhentet informasjon fra dagens forsikringsselskap om de tilbyr slik forsikring. Per i dag er ikke dette noe som forsikringsselskapene som kommunen har avtaler med tilbyr.

4.3.6 Revisjonens vurdering av datasikkerhet og beredskapstiltak

Identifisering og vurdering av risikoen for kommunens IT-funksjon

Revisjonen har fått tilgang til en overordnet ROS-analyse fra 2018 for kommunen som også inkluderer kommunens IT-drift. I denne ROS-analysen er det identifisert behov for å se nærmere på konsekvensene og risiko knyttet til tap av elektronisk kommunikasjon, utfall av internett og kritiske IT- systemer. De fleste kommunale tjenester er helt avhengig av velfungerende IT-infrastruktur og tilhørende støttesystemer. Revisjonen mener derfor kommunen burde utarbeide en egen ROS-analyse for IT-området for å sikre et helhetlig bilde av risikoen for IT-driften i Trondheim kommune.

Vi ber om en tilbakemelding på om kommunen har planer om å utarbeide en egen risikoanalyse som nærmere definerer risikoene for IT-området.

Tiltak for å sikre IT-systemer og IT-utstyr

Vår vurdering er at kommunen har etablert tiltak for å beskytte kommunens IT-systemer og data mot uautorisert tilgang. Det er imidlertid vanskelig å vurdere om disse tiltakene er tilstrekkelige i dagens komplekse risikobilde. Revisjonen ber derfor kommunedirektøren gi en vurdering om de tiltakene som er satt i verk er tilstrekkelige ut fra dagens trusselbilde.

Gammelt IT-utstyr og programvare som ikke lenger mottar oppdatering kan utgjøre en sikkerhetsrisiko da dette utstyret ikke er oppdatert på sikkerhet. Kassering av maskinvare gjøres etter det vi har fått opplyst på en sikkerhetsmessig riktig måte av kommunens maskinvareleverandør som er sertifisert for dette. Fjerning av gammel programvare styres av IT-drift i kommunen. Kommunen jobber helhetlig med sårbarhetshåndtering. Programvare som skal fases ut eller ikke lenger mottar oppdatering er en del av denne sårbarhetsvurderingen.

Vi vurderer det slik at kommunens data er sikret gjennom sikkerhetskopi eller speiling av data for systemer som driftes av Sopra Steria samt regnskapssystemet LIFT og lønnssystemet Bluegarden. Data som lagres i Google-skyen, e-postsystemet, lagring av arbeidsdokumenter samt informasjonssider slettes automatisk permanent etter 30 dager i papirkurven og kan ikke rekonstrueres. Revisjonen ber om en vurdering av om kommunen ser det som en akseptabel risiko at data i Google-skyen ikke er mulig å rekonstruere etter sletting fra papirkurven.

Vi har fått informasjon om at det er etablert manuelle reserveløsninger for pasientjournalsystemet Gerica. Vi har imidlertid fått opplyst at det for andre systemer er mer krevende å opprettholde tjenesteproduksjon ved bortfall av IT-systemer. Revisjonen ber om kommunedirektørens vurdering av om det er etablert tilstrekkelige reserveløsninger som kan tre i kraft dersom kommunens kritiske systemer, med krav om tilgjengelig 24 timer i døgnet hele året, blir utilgjengelig over tid. Vi ber også om en tilbakemelding om eventuelle reserveløsninger er testet.

Oppfølging og evaluering av risikostyring for IT-området

Revisjonen mener det er positivt at kommunen i 2021 har har hatt en gjennomgang av informasjonssikkerhet og personvern. Gjennomgangen er utført av et konsulentfirma.

Det er også positivt at kommunen høsten 2021 trente på dataangrep sammen med tjenesteleverandør Sopra Steria.

Vi har på forespørsel fått opplyst at kommunen ikke har en overordnet plan for IT-sikkerhet, ut over at det foreligger et målbilde for arkitektur på informasjonssikkerhet og en informasjonssikkerhetsstrategi. Revisjonen mener det er vanskelig å få et klart bilde av kommunens planer for IT-sikkerhet. Vi mener kommunedirektøren bør vurdere om kommunen har tilstrekkelige planer for IT-sikkerhet.

Vi mener også det er vanskelig å få oversikt over planer for og gjennomføring av sikkerhets- og sårbarhetstester av kommunens IT-infrastruktur og systemer. Vi mener kommunedirektøren bør vurdere om det er planlagt og gjennomført tilstrekkelige sikkerhets- og sårbarhetstester av kommunens IT-infrastruktur og systemer.

Etablering av planer for å håndtere uønskede hendelse

Beredskapsplanen for IT-tjenesten som ligger i Kvaliteket per januar 2022 fortsatt har utløpsdato 31.12.2019. Vi ber om kommunedirektørens vurdering av årsaken til at beredskapsplanen for IT-tjenesten ikke er oppdatert.

Vi har fått opplyst at det ikke er utarbeidet en plan for hvordan beredskapen på IT-området skal testes. Vi ber om en tilbakemelding fra kommunedirektøren om det vil bli etablert en plan for gjennomføring av krise- og beredskapsøvelser for IT-området.

Trondheim kommune har valgt å ikke tegne egen forsikring for datakriminalitet. Revisjonen ber om tilbakemelding på hvilke vurderinger kommunen har gjort i forhold til behovet for en forsikring mot datakriminalitet.

5. Konklusjon

Har Trondheim kommunen tilfredsstillende tilgangsadministrasjon til IT-systemene?
Gjennomførte tester viser at tilgangsadministrasjon i kommunen fungerer tilfredsstillende og at endringer er bestilt av autorisert bestiller. Vi anbefaler at kommunedirektøren vurderer risikoen ved at ansvaret for sletting av brukere er delegert til enhetene uten en sentral oppfølging fra IT-tjenesten.

Er det tilfredsstillende endringshåndtering av IT-systemer i Trondheim kommune?
På bakgrunn av undersøkelsen mener vi at kommunen har etablert formelle prosesser for å håndtere, dokumentere og gjennomføre endringer i IT-systemer. Revisjonen mener imidlertid det er noe uklart hva som er gjeldende rutiner for endringshåndtering av skyløsninger i kommunen.

Har Trondheim kommune tilfredsstillende datasikkerhet og beredskapstiltak?
Undersøkelsen viser at kommunen jobber aktivt med datasikkerhet og beredskapstiltak. Det er imidlertid vanskelig å vurdere om de tiltakene kommunen har etablert for datasikkerhet og beredskap er tilstrekkelige i dagens komplekse risiko- og trusselbilde.

Vi ber om kommunedirektørens vurdering og tilbakemelding på følgende punkter:

- Det bør utarbeides en egen ROS-analyse for IT-området for å sikre et helhetlig bilde av risikoen for IT-driften i Trondheim kommune.

- Er de tiltakene som er satt i verk for å beskytte kommunens It-systemer og data mot uautorisert tilgang tilstrekkelige ut fra dagens trusselbilde?

- Er det en akseptabel risiko at data i Google-skyen ikke er mulig å rekonstruere etter sletting fra papirkurven?

- Er det etablert tilstrekkelige reserveløsninger dersom kommunens kritiske systemer, blir utilgjengelig over tid og er disse eventuelle reserveløsninger testet?

- Er det utarbeidet tilstrekkelige planer for IT-sikkerhet i kommunen?

- Er det planlagt og gjennomført tilstrekkelige sikkerhets- og sårbarhetstester av kommunens IT-infrastruktur og systemer?

- Hva er årsaken til at beredskapsplanen for IT-tjenesten i Kvaliteket ikke er oppdatert etter 2019?

- Vil det bli etablert en plan for gjennomføring av krise- og beredskapsøvelser for IT-området?

- Hvilke vurderinger er gjort i forhold til behovet for en forsikring mot datakriminalitet?

Vi ber om tilsvar innen 28. februar 2022. Revisoruttalelsen skal til behandling i Kontrollutvalget 21. mars 2022.

Med hilsen

Per Olav Nilsen
revisjonsdirektør

Børge Sundli
revisor/CISA

Elektronisk dokumentert godkjenning uten underskrift

Kopimottaker: Ola Eirik Klingen, Organisasjonsdirektøren

6 Litteraturliste

ISO/IEC[68] 27001– Ledelsessystem for informasjonssikkerhet
https://internkontroll-infosikkerhet.difi.no/hva-sier-isoiec-27001

NSMs grunnprinsipper for IKT-sikkerhet
https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/grunnprinsipper-ikt

ISA 402 Særlige hensyn ved revisjon av en enhet som bruker en serviceorganisasjon
https://www.revisorforeningen.no/globalassets/fag/standarder-og-veiledninger/revisjonsstandardene/isa-402-sarlige-hensyn-ved-revisjon-av-en-enhet-som-bruker-en-serviceorganisasjon.pdf

ISAE3402 Internasjonal standard for attestasjonsoppdrag. Attestasjonsuttalelser om kontroller hos en serviceorganisasjon
https://revisorforeningen.no/globalassets/fag/standarder-og-veiledninger/revisjonsstandardene/isae-3402-attestasjonsuttalelser-om-kontroll-hos-en-serviceorganisasjon-pr-18-12-2017-.pdf

IT-tilganger for ansatte og vikarer i Trondheim kommune. Kvaliteket Dokument-ID: 15741-1. Siste revisjonsdato 12.1.2022

Tilgangsstyring ERP systemer. Kvaliteket Dokument - ID 16462-1. Siste revisjonsdato 11,1,2021

Bestilling av tilgang i LIFT for eksterne konsulenter/ekstern attestant. Kvaliteket Dokument - ID 16052-1. Siste revisjonsdato 25.9.2020

Temaplan for teknologi og modernisering, bystyresak 5/21 møtedato 3.3.2021
https://www.trondheim.kommune.no/globalassets/10-bilder-og-filer/11-politikk-og-planer/planer/temaplaner/hoveddokument-temaplan-for-teknologi-og-modernisering.pdf

Tjenestestyring av IT-løsninger i Trondheim. Kvaliteket dokument-ID: 10233-9. Siste revisjonsdato 14.01.2020.

Lov om behandling av personopplysninger (personopplysningsloven)
https://lovdata.no/dokument/NL/lov/2018-06-15-38

KS brev av 8.2.20212021 sendt til kommuner og fylkeskommuner "Datasikkerhets- og beredskapstiltak i kommunal sektor"
https://www.ks.no/contentassets/e1931a1709e34666b7bafb59c0e8d23b/SikkerhetKommDir.pdf

Dataangrep på Østre Toten kommune
https://norsis.no/dataangrepet-i-ostre-toten-kommune-minst-9000-dokumenter-og-store-e-postmengder-stjalet/

Dataangrep mot Stortinget i 2020
https://www.pst.no/alle-artikler/pressemeldinger/datainnbruddet-mot-stortinget-er-ferdig-etterforsket/

Datangrep mot Stortinget i 2021
https://forsvaretsforum.no/cyber-stortinget/nytt-dataangrep-mot-stortinget/187879

[68] IEC: International Electrotechnical Commission er en ideell, ikke-statlig internasjonal standardiseringsorganisasjon som utformer og publiserer internasjonale standarder for alle typer elektrisk, elektronisk og relatert teknologi.