KPMG

IKT-sikkerhet i Østre Toten kommune forut for dataangrepet 9. januar 2021

Kartlegging og ekstern vurdering

26. august 2021

www.kpmg.no

Sammendrag

9. januar 2021 ble Østre Toten kommune utsatt for et omfattende løsepengevirusangrep som resulterte i at hele den kommunale tjenesteleveransen, med få unntak ble rammet. I den forbindelse har kommunedirektøren i Østre Toten kommune bestilt en rapport fra KPMG som skal kunne bidra til å belyse forhold rundt årsak og konsekvens for berørte parter, herunder innbyggere, tilsynsorganer og politisk ledelse. Formålet med rapporten skal være å legge til rette for læring og utarbeide innspill til hvordan Østre Toten kommune bør organisere sitt arbeid innenfor digital sikkerhet i fremtiden.

KPMG har innhentet og gjennomgått relevant og tilgjengelig dokumentasjon som ledd i våre undersøkelser. Som følge av den situasjonen Østre Toten kommune har vært i etter dataangrepet, har tilgangen til tilgjengelig dokumentasjon vært svært begrenset. KPMG har som følge av dette i all vesentlighet lagt stor vekt på det som er opplyst oss i samtaler. Opplysningene vi har fått er vurdert opp mot NSM sine grunnprinsipper for IKT-sikkerhet og sikkerhetsstyring.

KPMGs gjennomgang har identifisert en rekke svakheter knyttet til arbeidet med IKT-sikkerheten i kommunen. Selv om en rekke ulike tiltak var implementert innen de fire kategoriene i NSMs grunnprinsipper, herunder «identifisere og kartlegge», «beskytte og opprettholde», «oppdage» og «håndtere og gjenopprette» virker det tilfeldig hva som er på plass, og implementasjonen er i liten grad i tråd med *beste praksis.*

Basert på at implementering av sikkerhetstiltak fremstår som noe tilfeldig, samtidig som enkelte mangler har blitt identifisert, men ikke gjort noe med, vurderer KPMG sikkerhetsstyringen i kommunen som svak eller mangelfull.

Undersøkelser blant norske kommuner gjennomført av blant annet Digitaliseringsdirektoratet, viser generelt store forbedringsområder innen IKT-sikkerhet i sektoren. Det er lite som tilsier at Østre Toten kommune har vært i en særstilling og av den grunn har vært dårligere stilt til å sikre sine digitale verdier enn andre kommuner på tilsvarende størrelse. Vi antar derfor at tilstanden i sammenliknbare kommuner ligger på omtrent samme nivå som Østre Toten kommune forut for hendelsen. Kommuner som har satt litt mer fokus på sikkerhet vil ligge på et litt høyere sikkerhetsnivå. Implementasjon av få, men viktige tiltak kan gjøre stor forskjell på sikkerhetstilstanden i en kommune.

KPMG anbefaler Østre Toten kommune å iverksette titak for å sikre tilstrekkelig internkontroll og sørge for reell etterlevelse. Kommunen må gjennomføre jevnlige risikovurderinger og styrke sin kompetanse innen IKT-sikkerhet og personvern. Som følge av utkontraktering av IKT-tjenestene til IKOMM må kommunen sikre tilgjengelig personell med god bestillerkompetanse, slik at kommunen kan stille funksjonelle og sikkerhetsmessige krav til IKOMMs tjenesteleveranser. Videre anbefaler KPMG at kommunen og deres tjenesteleverandører innfører og styrer etter NSMs grunnprinsipper og samarbeider om ivaretakelsen av de ulike prinsippene.

Innhold

1. Innledning

1.1 Bakgrunn

9. januar ble Østre Toten kommune utsatt for et omfattende løsepengevirusangrep. Hele den kommunale tjenesteleveransen, med få unntak, ble rammet i angrepet. Det ble tidlig klart at IKT-sikkerhetshendelsen var av en svært alvorlig karakter. Ansatte fikk ikke lenger tilgang til IKT-systemer, store deler av kommunens data var blitt kryptert og sikkerhetskopier slettet.

Atea IRT bistod Østre Toten kommune i den innledende håndteringen av hendelsen. Ved involveringstidspunktet var det kjent at tjenester var utilgjengelige og at årsaken skyldtes at kommunens IKT-infrastruktur var rammet av et løsepengevirus.

Østre Toten kommune satt umiddelbart krisestab og det ble utpekt innsatsleder hos Østre Toten kommune. 19. januar 2021 ble KPMG kontaktet av Østre Toten kommune for ytterligere bistand til håndtering og koordinering av hendelsen, og det ble inngått avtale om bistand 22. januar 2021. KPMG sin bistand har dekket flere områder knyttet til hendelseshåndteringen og koordinering, herunder bl.a. teknisk analyse, sikkerhetsmessig rådgivning ved re-etablering av ny infrastruktur, myndighetskontakt og spørsmål knyttet til personvern.

I tillegg til den løpende bistanden i hendelseshåndteringen har kommunedirektøren bestilt en rapport fra KPMG som skal kunne bidra til å kunne gi svar om årsak og konsekvens til berørte parter, herunder innbyggere, tilsynsorganer og politisk ledelse. Formålet med rapporten skal være læring og innspill til hvordan Østre Toten kommune bør organisere sitt arbeid innenfor digital sikkerhet i fremtiden.

1.2 Mandat

Rammene for innhold og gjennomføring av denne undersøkelsen er avklart gjennom bestilling fra kommunedirektøren. Avtalt mandatet ligger til grunn for rapportens innhold og kan oppsummeres i følgende punkter;

- **En kort beskrivelse av hendelsen** (Kap. 2.1)
  Hensikt: En oppsummering av selve hendelsen og konklusjon/resultat av de tekniske undersøkelsene.

- **Kartlegging av IKT-sikkerhetstilstanden i kommunen forut for hendelsen** (Kap. 2.2)
  Hensikt: Basert på samtaler og innhenting av dokumentasjon, gi en beskrivelse av hvordan kommunen og IKT-avdelingen forholdt seg til IKT sikkerhet i den daglige driften, herunder roller og ansvar, kunnskap om tilstand på IKT-sikkerhetsområdet, utfordringer knyttet til IKT-sikkerhet mv.

- **Vurdering av årsakssammenheng mellom hendelsen og resultatet av kartleggingen** (Kap. 3)
  Hensikt: Vurdere om det foreligger noen direkte og åpenbar årsakssammenheg mellom hendelsen og eventuelle funn og observasjoner gjort under kartleggingen. KPMG vil også gi en overordnet beskrivelse av kommunen sin modenhet sett opp mot NSMs grunnprinsipper for IKT-sikkerhet, og eventuelle observasjoner fra de andre kommunene i det regionale samarbeidet

- **Utarbeide lærings- og anbefalingsspunkter for kommunen basert på funn og observasjoner i undersøkelsene** (Kap. 4)
  Hensikt: Erfaringsutveksling og anbefalinger som har til hensikt å bidra til styrking av IKT-sikkerhetsarbeidet i kommunen. Rådene skal bidra til å redusere risikoen for at kommunen kommer i tilsvarende eller likende situasjoner i fremtiden.

1.3 Forbehold og avgrensninger

Rapporten er utarbeidet på bakgrunn av gjeldende mandat. Det har ikke vært en del av KPMGs mandat å vurdere de organisatoriske eller bakenforliggende forholdene ved IKT-avdelingen, eller ta stilling til politiske vedtak knyttet til prioriteringer eller investeringer på IKT-siden. Rapporten skal være på et overordnet nivå og har ikke som formål å rette kritikk mot enkeltpersoner eller funksjoner ved IKT-avdelingen. I den grad organisering og enkeltpersoners roller benevnes, gjøres dette for å beskrive den faktiske situasjonen i IKT-avdelingen ut fra beskrivelser KPMG har fått presentert.

Av hensyn til mandatets rammer og avgrensing har ikke alle oppgitte opplysninger blitt ettergått. Likevel påpekes at det i stor grad har vært samsvar mellom de opplysninger som er innhentet. Faktagrunnlaget regnes derfor som troverdig og korrekt. Rapporten må likevel leses i lys av at den i vesentlig grad baserer seg på muntlig informasjon. Økt ressursbruk og manglende tilgjengelighet på dokumentasjon etter dataangrepet har vært utslagsgivende for valget om å ikke bruke mer ressurser på innhenting og gjennomgang av dokumentasjon.

Siden IKT-sikkerhetshendelsen inntraff har det blitt gjort endringer i organiseringen av IKT i kommunen. Denne rapporten vurderer ikke konsekvensene av omorganiseringen, heller ikke IKT-sikkerhetstilstanden etter omorganiseringene. Rapporten avgrenser seg til å vurdere tilstanden forut for hendelsen og videre sammenhengen mellom denne tilstanden og den aktuelle IKT-sikkerhetshendelsen. Rapporten kan derfor ikke sees på som en modenhetsvurdering, men fungerer som et verktøy for erfaringsutveksling og dokumenterer en rekke læringspunkter.

Rapporten er utarbeidet på bakgrunn av de opplysninger som er gitt og den dokumentasjon som har vært gjort tilgjengelig for KPMG. KPMG fraskriver seg ethvert ansvar for mulige feil eller utelatelser som følge av at KPMG har mottatt uriktige eller ufullstendige opplysninger eller dokumentasjon.

1.4 Metode

1.4.1 Informasjonsinnhenting

KPMG har innhentet og gjennomgått relevant og tilgjengelig dokumentasjon som ledd i våre undersøkelser. Dokumentasjonsinnhentingen er gjort via direkte forespørsler, samt som oppfølging til gjennomførte samtaler.

Som følge av den situasjonen Østre Toten kommune har vært i etter dataangrepet, har det vært svært begrenset med tilgjengelig dokumentasjon. KPMG har som følge av dette i all vesentlighet lagt stor vekt på det som er opplyst oss i samtaler.

1.4.1.1 Gjennomføring av intervjuer

KPMG har gjennomført samtaler/intervjuer med sentrale nøkkelpersoner som ledd i våre undersøkelser. Oppdrasgiver har ikke lagt føringer for hvem KPMG skal gjennomføre samtaler med. Oppdragsgiver har imidlertid ytret ønske om at det gjennomføres samtaler med de øvrige kommunene i det regionale samarbeidet i Gjøvikregionen. Bakgrunnen for dette har vært et ønske om å innhente erfaringer og sammenligningsgrunnlag for hvordan andre har organisert sitt IKT-sikkerhetsarbeid.

Samtalene er gjennomført via Teams med tidligere og nåværende ansatte i Østre Toten kommune , samt ansatte hos Gjøvik kommune, Nordre Land kommune og Vestre Toten kommune.

For samtaler med ansatte og tidligere ansatte i Østre Toten kommune er det i etterkant utarbeidet en oppsummering fra samtalen som er oversendt for gjennomlesning og verifisering. Formålet med oppsummeringene har vært å utarbeide et overordnet referat som gjenspeiler innholdet i samtalen, og derigjennom sikre at KPMG har en korrekt oppfattelse av informasjonen som er gitt under samtalen.

Samtalene med representanter fra andre kommuner er gjennomført uten at det er oversendt referat i etterkant. Formålet har her vært å skaffe seg et inntrykk av hvordan det er jobbet med IKT-sikkerhet generelt, uten at den enkelte kommune skal identifiseres i rapporten. Informasjon fra disse samtalene vil fremkomme som en samlet beskrivelse i rapporten på et overordnet nivå.

1.4.1.2 Avklaringer og statusrapportering

KPMG har underveis og ved behov foretatt nødvendige avklaringer med kommunedirektøren omkring fremdrift og praktiske forhold ved gjennomføringen. KPMG har ved to anledninger oversendt notater med våre foreløpige observasjoner.

Som følge av datalekkasjen som skjedde i april, har det vært en forskyvning av opprinnelig tidslinje for gjennomføring av undersøkelsene. Etter avtale med oppdragsgiver så har KPMG oversendt et foreløpig utkast til rapport før sommeren, og avlevert endelig rapport i august.

1.4.1.3 Kontradiksjon

Berørte og involverte har fått hele eller deler av faktabeskrivelsen til kontradiktorisk gjennomgang. Rapporten er ferdigstilt etter at forslag til rettelser og innspill er vurdert av KPMG

1.4.2 Vurderingskriterier

NSMs grunnprinsipper er benyttet for å vurdere kommunens sikkerhetstilstand forut for hendelsen, samt for gi konkrete anbefalinger basert på norsk annerkjent praksis for sikring av digitale verdier. Rapporten baserer seg på følgende rammeverk:

- NSMs grunnprinsipper for sikkerhetsstyring[1]
- NSMs grunnprinsipper for IKT-sikkerhet[2]

NSMs grunnprinsipper for sikkerhetsstyring er et sett med prinsipper og anbefalte tiltak som beskriver hva virksomheten kan gjøre for å oppnå og opprettholde et akseptabelt sikkerhetsnivå.

NSMs grunnprinsipper for IKT-sikkerhet er et sett med prinsipper og tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. Rammeverket er basert på globalt anerkjente rammeverk og inkluderer de mest relevante tiltakene for norske virksomheter. Ved å ha implementert de anbefalte tiltakene vil virksomheter etablere et godt forsvar mot cybertrusler.

Rammeverkene baserer seg på fire kategorier. I det følgende blir hver kategori kortfattet beskrevet.

1) Identifisere og kartlegge:

- **Grunnprinsipp**: Opparbeide og forvalte forståelse om virksomheten, herunder styringsstrukturer, ledelsesprioriteringer, leveranser, IKT-systemer og brukere. Dette er grunnlaget for en effektiv implementering av de øvrige grunnprinsippene. Hensikten er å forstå virksomhetens leveranser og tjenester, få oversikt over hvilke teknologiske ressurser som må sikres og de roller og brukere virksomheten består av. Dette gjør det mulig å fokusere og prioritere sikkerhetstiltakene i tråd med forretningsbehov og strategi for risikostyring. Kategorien fokuserer også på å etablere prosesser for å forvalte kunnskapen over tid.
- **Styringsprinsipper**: Denne kategorien utgjør grunnlaget for iverksettelse av de andre kategoriene, den vurderer risiko og legger en plan for risikohåndtering. I en risikovurdering gjennomfører virksomheten nødvendige steg for å identifisere, vurdere og evaluere risiko knyttet til virksomhetens identifiserte verdier. Avdekker risikovurderingen en forskjell på ønsket sikkerhetsnivå og reell sikkerhet, lages en plan for å lukke gapet – en plan for risikohåndtering.

2) Beskytte og opprettholde

- **Grunnprinsipp:** Ivareta en forsvarlig sikring av IKT-systemet og opprettholde den sikre tilstanden over tid og ved endringer. Her finnes prinsippene for å etablere en sikker tilstand for IKT-systemet for å motstå eller begrense skaden fra dataangrep. Det innebærer å sikre hvordan IKT-systemet anskaffes, planlegges, bygges og konfigureres slik at ønsket sikkerhet oppnås.
- **Styringsprinsipp:** På bakgrunn av risikovurdering bør virksomheten utforme eller tilpasse virksomhetens sikkerhetsorganisasjon og styringssystem for sikkerhet samt innføre sikkerhetstiltak, slik at den aktuelle risikoen reduseres og opprettholdes til et nivå hvor virksomheten oppnår akseptabel sikkerhet. Akseptabel sikkerhet oppnås når både organisatoriske, elektroniske, fysiske

[1] https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-sikkerhetsstyring/introduksjon/

[2] https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/

og menneskelige tiltak er kombinert og virker sammen, dvs. at det forebyggende sikkerhetsarbeidet er helhetlig.

3) Oppdage:

- **Grunnprinsipp**: Oppdage og fjerne kjente sårbarheter og trusler og etablere sikkerhetsovervåking. Prinsippene i denne kategorien fokuserer på å oppdage og fjerne kjente sårbarheter og trusler gjennom sårbarhetskartlegging og overvåking av IKT-systemet. Kategorien tar også for seg å oppdage avvik fra ønsket, sikker tilstand, gjennom analyse av data fra sikkerhetsovervåkingen.
- **Styringsprinsipp**: Kategorien handler om å kontrollere sikkerhetstilstanden for å oppdage eller avdekke sårbarheter eller forhold av sikkerhetstruende karakter. Dette ivaretas gjennom: (1) Kontroll av sikkerhetstilstanden og (2) ledelsens gjennomgang.

Håndtere og gjenopprette:

- **Grunnprinsipp**: Håndtere sikkerhetshendelser effektivt. Hensikten med disse prinsippene er å få på plass aktiviteter for å håndtere hendelser. Dette innebærer å forberede seg på, vurdere, kontrollere og håndtere hendelser, gjenopprette normaltilstand, samt forbedre sikkerheten basert på erfaringer fra hendelseshåndteringen.
- **Styringsprinsipp** : kategorien omhandler håndtering av hendelser eller avvik fra virksomhetens styringssystem for sikkerhet. Når og hvordan avvik og hendelser skal korrigeres vil avhenge av hvor ressurskrevende og viktig det er å få dette håndtert og korrigert. Formålet med kategorien er at virksomheten skal være rustet til å gjennomføre (umiddelbare) tiltak for å redusere skadeomfanget og gjøre tiltak som gjenoppretter det ønskede sikkerhetsnivået i virksomheten.

2. Faktagrunnlag

KPMG vil i dette kapittelet presentere innhentet faktagrunnalg i våre undersøkelser. Faktagrunnlaget vil dekke i) hendelsen, ii) tilstand på IKT-sikkerhet i kommunen forut for angrepet og iii) informasjon om IKT-sikkerhetsarbeid hos andre kommuner.

2.1 Dataangrepet på Østre Toten kommune

2.1.1 Oppsummering av hendelsen

Natt til 9. januar ble Østre Toten kommune utsatt for et omfattende løsepengevirusangrep. Hele den kommunale tjenesteleveransen, med få unntak, ble rammet i angrepet. Det ble tidlig klart at IKT-sikkerhetshendelsen var av en svært alvorlig karakter. Ansatte fikk ikke lenger tilgang til IKT-systemer, store deler av kommunens data var blitt kryptert og sikkerhetskopier slettet. Spor på systemene og trussel aktørens metodikk, antydet at trusselaktøren bak hendelsen var en aktør/gruppering kjent som «Pysa» eller «Mespinoza» i åpne kilder.

Kommunen satt umiddelbart krisestab og i løpet av innledende fase ble det utpekt innsatsleder hos Østre Toten kommune. Atea IRT bisto innledningsvis i hendelseshåndteringen og KPMG ble etter hvert engasjert i det videre arbeidet med håndtering av hendelsen. KPMG har bistått kommunen med håndtering, koordinering, reetablering av sikker infrastruktur, personvernvurderinger og tekniske undersøkelser.

30. mars ble det kjent at trusselaktør hadde publisert et stort antall filer som trolig stammet fra dataangrepet på det mørke nettet. Hendelseshåndteringen gikk fra dette tidspunktet over i en ny fase der fokuset ble noe endret. Beskrivelsen skiller derfor på tekniske undersøkelser før datalekkasjen 30. mars (fase 1) og tekniske undersøkelser etter datalekkasje 30. mars (fase 2).

2.1.2 Tekniske undersøkelser

Fase 1
Atea IRT bistod IKT-avdelingen i kommunen med innledende undersøkelser av hendelsen. Logger fra brannmur og enkelte domenekontrollere ble sikret og gjennomgått, og avslørte en mengde mistenkelig aktivitet. Ved hjelp av nettverksdata fra Gjøvik kommune, som leverer infrastruktur til kommunen, identifiserte man en unormalt stor opplastingsaktivitet fra kommunen til en IP-adresse i Nederland rundt midnatt, natt til 9. januar.

Gjennom de innledende undersøkelsene ble det avdekket at trusselaktør hadde oversett en lagringsløsning med snapshot av de fleste serverne fra 8. januar 2021. Dataene ble raskt sikret og har dannet grunnlag for den rekonstruksjonen som kommunen har jobbet med.

Da KPMG overtok ansvaret for de tekniske undersøkelsene ble tidligere funn fra Atea verifisert. Kommunens IKT-infrastruktur ble gjennomgått for å indentifisere mulige datakilder for ytterligere analyse. Gjennomgangen av infrastrukturen viste at det ikke fantes sentralisert innsamling av logger, hverken fra servere, klienter eller nettverksutstyr. Kommunen sin brannmur var konfigurert til å sende logg (syslog) til en Solarwinds Orion-server, men lagringsdelen av denne serveren var ikke i drift, sannsynligvis grunnet maskinvarefeil.

Utover dette var brannmuren sparsommelig konfigurert med tanke på logging, og mye interntrafikk ble aldri logget. Dette henger også sammen med en soneinndeling som både gjorde det vanskelig å forsvare og overvåke infrastrukturen. Sonemodellen ble innført i 2016 og er en to-sone modell på infrastrukturen hvor det ble segmentert i forhold til intern og sikker sone. Dette arbeidet ble ledet og gjennomført av en større ekstern leverandør, men uten at det ble utført noen spesifikk risikoanalyse for oppsettet. Oppsettet ble gjort etter hva man mente var beste praksis på det aktuelle tidspunktet.

KPMG påstartet tekniske undersøkelser av kommunens tilgjengelige servere så snart disse ble gjort tilgjengelig for KPMG. De tekniske undersøkelsene var innledningsvis rettet mot å finne ut hvilke data aktøren eventuelt hadde stjålet, samt hvilke data som sannsynligvis ikke var på avveie.

De tekniske undersøkelsene avdekket tidlig interessant aktivitet på e-post serveren til Østre Toten kommune. Det ble gjort funn av en stor mengde eksporterte e-postbokser i PST-format og eksporteringen hadde funnet sted noen timer forut for den mistenkelige nettverkstrafikken man hadde registrert til en IP adresse i Nederland. Aktiviteten var utført av en bruker med administratorrettigheter som var gammel, og som ikke lenger ble brukt av noen i IT-avdelingen. Undersøkelsene har vist at trusselaktøren har hatt administratortilgang til alle datamaskiner, og at alle filer fra serverne KPMG har undersøkt i prinsippet kan ha blitt eksfiltrert.

Totalt utgjorde datavolumet som var eksportert på Exchange serveren ca. 160 GB. Den mistenkelige nettverkstrafikken til IP-adressen i Nederland viste overføring av ca. 31.5 GB. KPMG utarbeidet hypoteser for hva som kunne være eksfiltrert og jobbet med å bekrefte eller avkrefte hvorvidt disse stemte. Usikkerhet knyttet til eksfiltrasjon av data skyldes primært manglende nettverkslogg bakover i tid, ikke kvaliteten på nettverksloggene. Selv om brannmuren har vært dårlig konfigurert mtp. logging, ble trafikk fra interne soner til Internett logget.

KPMG har hatt enkelte hypoteser for hvordan trusselaktøren kan ha fått tilgang. Kommunen benyttet ikke 2-faktor autentisering før hendelsen, og utnyttelse av stjålne innloggingsdetaljer ville derfor vært svært enkelt, forutsatt at kommunen eksponerte fjernaksessløsninger hvor kompromittert innloggingsinformasjon ville gitt tilgang. Alternativt kan trusselaktør ha brukt metoder for sosial manipulasjon, f.eks. via e-post, og lurt en bruker til å installere skadevare som har gitt trusselaktør nødvendig fotfeste. På grunn av manglende loggdatagrunnlag fra hele perioden trusselaktøren har vært aktiv i kommunens IKT-infrastruktur har det ikke lykkes å avdekke angrepsvektoren gjennom de tekniske analysene.

Fase 2
30. mars ble det kjent at trusselaktør hadde publisert et stort antall filer fra dataangrepet hos Østre Toten kommune på det mørke nettet.

Datalekkasjen førte til iverksettelse av ytterligere tiltak (fase 2) med den hensikt å få kontroll over situasjonen og begrense de negative konsekvensene av lekkasjen. KPMG lastet ned og gjennomgikk det lekkede datamaterialet, og kunne konstatere at det med høy sannsynlighet ikke stammet fra e-postboksene som var antatt eksfiltrert. Informasjonen indikerte at trusselaktøren hadde hatt tilgang til kommunen sin infrastruktur tidligere enn først antatt. Informasjon om Voksenopplæring og Flyktningetjeneste blant det lekkede materialet gjorde at IKT-avdelingen raskt identifiserte en server som mesteparten av den lekkede informasjonen med stor sannsynlighet stammet fra. Serveren ble kopiert fra snapshot og overlevert til KPMG for analyse. Analysen viste at de 1 456 av de 1 879 lekkede filene stammet fra den aktuelle serveren. Katalogene som filene stammet fra inneholdt totalt 30 903 filer, totalt rett i overkant av 2 GB data. Det vurderes som sannsynlig at trusselaktøren har eksfiltrert alle disse filene.|

2.1.3 Oppsummering tekniske undersøkelser

KPMGs tekniske rapport ble oversendt kommunen 2. juni 2021. Følgende oppsummerende punkter trekkes frem:

- KPMG vurderer det som sannsynlig at e-postbokser som er eksportert/kopiert på Exchange serveren av trusselaktør, har blitt eksfiltrert. Lekkasjen på det mørke nettet viser også at dokumenter fra minst en annen server har blitt eksfiltrert. Da det ikke er mulig å fastslå eksakt hvilke dokumenter som er eksfiltrert fra denne serveren, anbefalte KPMG at kommunen håndterer saken som om alle kataloger som er pekt på i de tekniske undersøkelsene anses som eksfiltrert. Listen over kataloger er overlevert sammen med KPMGs tekniske rapport.

- De tekniske analysene, samt gjennomgangen av infrastrukturen viste at det ikke fantes sentralisert innsamling av logger, hverken fra servere, klienter eller nettverksutstyr. Den svært begrensede deteksjonskapasiteten som var på plass i kommunen har gjort det mulig for trusselaktøren å operere uoppdaget i kommunens IKT-infrastruktur. Det har samtidig gjort det svært krevende å analysere hva trusselaktøren hadde foretatt seg i infrastrukturen, herunder hvordan trusselaktøren hadde kommet seg inn og hva trusselaktøren hadde eksfiltrert.

- Basert på det tilgjengelige datagrunnlaget har det heller ikke vært mulig å konkludere nøyaktig på hvor lenge trusselaktør har hatt forfeste i infrastrukturen til Østre Toten kommune. De første sporene i logger er fra 3. januar 2021. I forbindelse med publisering av data på lekkasjebloggen til trusselaktør fremkommer datoen 19. desember 2020. Analysene har imidlertid ikke ledet frem til hva denne datoen relaterer seg til.

- Østre Toten kommune hadde ikke aktivert 2-faktor autentisering for pålogging.

De overnevnte observasjonene bidrar til å tegne et bilde av IKT-sikkerheten i kommunen på hendelsestidspunktet. Vi vil i det følgende gi en ytterligere detaljering av IKT-sikkerheten i kommunen forut for hendelsen.

2.2 Arbeid med IKT-sikkerhet i kommunen forut for hendelen

Etter den alvorlige sikkerhetshendelsen i kommunen er det satt spørsmål ved kommunens sikkerhetstilstand og hvorvidt sikkerhetsnivået var forsvarlig gitt dagens trusselbilde. Dette kapittelet har til hensikt å beskrive hvordan kommunen hadde organisert og utøvet sitt arbeid med IKT-sikkerhet før hendelsen inntraff.

Beskrivelsene i dette kapittelet baserer seg på informasjon gitt i samtaler med sentrale personer og noe innhenting av dokumentasjon. KPMG har fokusert på å innhente informasjon om hvordan organiseringen av IKT-avdelingen har vært, herunder roller og ansvar, ressurssituasjonen og fokusområder for personellet ved IKT-avdelingen.

KPMG har ikke gjennomført dybdeanalyser eller systematiske modenhetsvurderinger på sikkerhetsområdet, men formålet har vært å kunne gi en praktisk beskrivelse av hvordan arbeidet med IKT-sikkerhet og informasjonssikkerhet har vært organisert og praktisert som en del av den daglige driften hos IKT-avdelingen i kommunen.

2.2.1 Organisering på IKT-avdelingen

Bemanningen på IKT-avdelingen er beskrevet som stabil over mange år. IKT-sjef har vært ansatt siden 2009 og flesteparten av de øvrige ansatte har lang fartstid. Frem til høsten 2019 så var IKT-avdelingen organisert som en selvstendig enhet og IKTleder rapporterte direkte til kommunaldirektør under rådmannen.

Etter en omorganisering høsten 2019 ble IKT-avdelingen underlagt økonomiavdelingen og IKT-sjef rapporterte deretter til Økonomisjef. Ved inngangen på 2020 hadde IKT-avdelingen seks ansatte i tillegg til IKT-sjef. To personer hadde ansvar for serverdrift, to personer jobbet med prosjektstøtte og porteføljestyring, én person var nettverksansvarlig og én person hadde ansvar for service og helpdesk. IKT-avdelingen har også hatt to lærlingeplasser tilknyttet seg over tid.

Serverdrift har omfattet alt knyttet til datasenter, men ikke nettverk. KPMG har fått beskrevet at en vesentlig del av kapasiteten til driftsressursene de siste årene har vært bundet opp til prosjektarbeid og ikke driftsoppgaver.

Nettverksansvarlig har hatt ansvar for alt på nettverk, brannmur, konfigurasjon, regelsett, logging mv. KPMG har ikke snakket med tidligere nettverksansvarlig, men har fått opplyst fra IKT-sjef at fokus for oppgavene til nettverksansvarlig var rettet mot generell drift og tilgjengeliggjøring av nye systemer, applikasjoner mv. Sikkerhet har ikke vært et fokusområde, utover en jevnlig oppfølging av eksisterende logging som var etablert på infrastrukturen. IKT-sjef har mottatt regelmessige orienteringer om evt. forsøk på ondsinnet aktivitet mv. Man har i ettertid sett at det har vært en del svakheter knyttet til implementering og konfigurasjon av logging.

I februar 2020 ble DigInn, avdelingen for digitalisering og innovasjon opprettet i kommunen. De to ansatte med ansvar for prosjektarbeid og porteføljestyring ble flyttet ut av IKT-avdelingen og over i DigInn. Enheten ble organisatorisk underlagt Samfunnsutvikling med ansvar for å følge opp kommunens prosjektportefølje innenfor digitalisering og innovasjon. KPMG har fått opplyst at samarbeidet mellom DigInn og IKT-avdelingen var godt.

Våren 2020 sa nettverksansvarlig opp sin stilling og vedkommende sluttet i august. Oppgavene ble fordelt på de to gjenværende tekniske ressursene, og en av disse ble gitt opplæring i små endringer i brannmur

etc. Det ble også inngått en midlertidig ordning hvor nettverksansvarlig skulle bistå etter behov på kveldstid med det mest grunnleggende, frem til en erstatter var på plass. Ved behov for større endringer måtte leverandør kontaktes.

Til tross for at stillingen ble utlyst (august 2020) lot det seg ikke gjøre å finne en erstatter før sent på høsten. Erstatteren skulle etter planen tiltre stillingen i mars 2021, og var således ikke på plass da dataangrepet inntraff i januar.

Leder for IKT-avdelingen har over tid hatt flere ulike roller og ansvarsområder mens han samtidig har vært IKT-sjef, blant annet som informasjonssikkerhetsansvarlig fra 2016. Det var en svak struktur på IKT sikkerhetsarbeidet i 2016 og IKT-sjef oppfattet at han fikk rollen fordi ledelsen trengte å peke på noen. Det ble oppfattet som en pro-forma sak og det ble ikke gitt ressurser til å følge opp arbeidet. IKT-sjef har opplyst at han i 2016 påpekte at det var en direkte rollekonflikt mellom det å være både IKT-sjef og informasjonssikkerhetsansvarlig, men uten at dette ble hensyntatt.

IKT-sjef har også i perioden september 2019 og frem til juni 2020 hatt rollen som HR-leder. I en periode på ca. 2 måneder sommeren 2020 var han også konstituert Personalleder Økonomi. Dette var i perioden mellom tidligere rådmann og frem til ny rådmann var på plass i august. I samme periode var Økonomisjef konstituert rådmann.

2.2.2 Ressurssituasjonen i IKT-avdelingen

KPMG har gjennom samtalene fått beskrevet et bilde hvor ressursene på IKT-avdelingen har vært under stort arbeidspress. Kommunen har hatt en digitaliseringsstrategi og IKT-avdelingens ansatte har blitt involvert i prosesser knyttet prosjekter og leveranser til tjenestene «ute». Det har vært en enstemminghet blant de KPMG har snakket med på IKT-avdelingen at det ikke har vært rom for å drive utvikling og tilstrekkelig vedlikehold på systemene, herunder systematisk sikkerhetsarbeid.

IKT-sjef har overfor KPMG pekt på at de største utfordringene har vært mangel på ressurser og det å kunne jobbe systematisk. Internkontrollsystemet hos Østre Toten kommune har ikke vært der det burde være, og man slet med å få på plass en systematikk i både internkontroll og sikkerhetsarbeid, inkludert rapportering.

IKT-sjef har samtidig vært klar på at man ikke har vært tydelig nok i rapporteringen oppover til kommunens ledelse på ressursbehovene. Det er flere årsaker til dette, og det er blant annet pekt på utfordringene med å be om ytterligere ressurser til et område (Stab- og støttefunksjoner) hvor det over tid har vært gitt politiske føringer for å kutte kostnader. Man har derfor forsøkt å løse oppgavene innenfor de angitte økonomiske rammene. I den grad det er gitt signaler om behov for ekstra ressurser så har dette vært knyttet til behov på drifts- og tjenestesiden og ikke sikkerhetsaspektene. KPMG har ikke gått nærmere inn i hvilke føringer som er gitt, eller hva som ligger bak disse.

Også leder for økonomiavdelingen, som fra november 2019 fikk det overordnede ansvaret for IKT-avdelingen, har bekreftet at ressurssituasjonen på IKT-avdelingen var presset. Man hadde ikke mer folk enn nødvendig for å få ting til å gå rundt. Da nettverksansvarlig sluttet i august 2020 bar avdelingens produksjon preg av dette. Økonomisjef har bekreftet at IKT-sjefen formidlet sin bekymring til ham da nettverksansvarlig sluttet, og påpekte at de var enda dårligere rustet til å oppdage uønsket aktivitet i nettverket med denne stillingen ubesatt.

KPMG har fått bekreftet at det ikke er kommunisert konkrete behov til øverste ledelse i kommunen hva gjelder behov for økt bemanning og ressursbruk for å styrke arbeidet på IKT-sikkerhet. Fokusområder har vært på drift- og tjenesteleveranser, herunder prosjektarbeid og støtte til digitaliseringsprosessen i kommunen. Det er opplyst til KPMG at som følge av en forespørsel fra kommunedirektøren høsten 2020 om ressurssituasjonen knyttet til O365 prosjektet, så ble det igangsatt en kartlegging av ressursbehov for å håndtere dette prosjektet. Det er ikke kjent hva som ble formidlet tilbake.

Situasjonen knyttet til korona-pandemien er også opplyst å ha vært en medvirkede årsak til økt belastning på ressursene på IKT-avdelingen. Da pandemien slo til i mars 2020, måtte kommunen forsere den opprinnelige planen for implementering av Microsoft Office 365 (O365). KPMG har fått opplyst at man var i gang med å gjennomføre konseptfasen og at fokus i all vesentlighet var rettet mot funksjonalitet og teknisk oppsett. Sikkerhet knyttet til den nye løsningen hadde ikke vært et tema som ble diskutert, dette var noe man skulle ta tak i under implementeringsfasen. O365 ble tatt i bruk nærmest over natten og dette medførte at det heller ikke ble gjort noen ytterligere vurderinger knyttet til sikkerheten ved bruk av plattformen. Man var heller ikke bevisst nok på hva som var sikkerhetsnivået på en standard O365 implementering.

Konfigurering og oppsett av O365 ble håndtert av driftsressurser ved IKT-avdelingen, sammen med ekstern leverandør. Bruk av den nye løsningen la således ytterligere beslag på kapasiteten til de tekniske ressursene på IKT avdelingen.

2.2.3 Risiko- og sårbarhetsanalyser knyttet til IKT

KPMG har gjennom undersøkelsene fått opplyst at det ikke har vært jobbet systematisk og strukturert med risikovurderinger knyttet til IKT. Det er vist til noe sporadisk arbeid knyttet til risiko- og sårbarhetsanalyser av enkelte IKT-systemer, men disse skal være gjennomført på bestilling fra en prosjektleder/etatsleder og har hatt fokus på tilgjengelighet og drift. Sikkerhet har ikke vært fokus i disse analysene.

Kommunen har mottatt regelmessig sårbarhetsskanning fra Norsk Helsenett, med tilhørende rapportering. Kvalitet og omfang på skanningen er ikke kjent for KPMG.

KPMG har fått oversendt en risikovurdering knyttet til kommunens IKT-infrastruktur i stort, som er datert 2016. Dette indikerer at IKT-risikoer sist ble identifisert og vurdert for 5 år siden.

Risikovurderingen fra 2016 inneholder en oversikt over risiko- og sårbarhetsområdene innenfor IKT. Vurderingen fokuserer i stor grad på konsekvenser og sårbarheter for produksjon av kommunale tjenester og i mindre grad på underliggende infrastruktur. Av rapporten ansees langvarig svikt i strømforsyningen, brudd i kommunikasjonslinjer, klimabaserte hendelser og branner som de viktigste.

Risikovurderingen omfatter i tillegg to scenarioer som knytter seg til ondsinnet aktivitet, i rapporten kalt «Virusangrep/hacking» og «Denial of Service Attack (DOS-angrep)». Virusangrep/hacking ansees for å være mindre sannsynlig, men farlig dersom det skjer, og resulterer således i en den laveste risikokategorien, kalt «En viss risiko, men normalt akseptert. Normalt ingen tiltak», i henhold til rapportens risikovurderingsmetodikk. DOS-angrep blir vurdert til sannsynlig, men ufarlig.

Den lave sannsynligheten for virusangrep/hacking begrunnes med at kommunen historisk sett har hatt et trusselbildet med lavt trusselnivå, samt at diverse sikkerhetstiltak er på plass. Det presiseres at kommunen ikke har erfaring med at hacking forekommer mot egen infrastruktur, men at virusangrep kommer i bølger, og at det alltid er en risiko for at det skjer.

Den aktuelle rapporten oppsummerer analysen med at ingen av risikoene for IKT er slik at de kommer på et gult eller rødt nivå, samt at det tilsynelatende kan se ut som IKT operer innenfor akseptabel risiko. Det legges til at IKT blir stadig mer kritisk for den kommunale tjenesteproduksjonen og at strengere krav til IKT bør vurderes. Det foreslås 3 konkrete risikoreduserende tiltak som i all hovedsak skal bidra til å sikre tilgjengeligheten til kommunens IKT ved ulike type hendelser.

Øvrige vurderinger

KPMG har i forbindelse med samtalene fått tilgang til en SWOT analyse fra 2019 som ser på sterke og svake sider, muligheter og trusler knyttet til Østre Totens IKT-sikkerhet. SWOT analysen ble utført i forbindelse med det regionale IKT-samarbeidet og på bestilling fra RUG (Rådmannsutvalget) hvor formålet var å utrede muligheter for utvidet samarbeide og mulig felles regional drift. KPMG har ikke gått nærmere inn på hvordan SWOT-analysen ble utført, men legger til grunn at den kan bidra til å gi et bilde av hvordan IKT-avdelingen selv vurderte tilstanden på IKT-sikkerhet på det tidspunktet.

STERKE SIDER	SVAKE SIDER
• Høy kompetanse på nettverk • God kompetanse på Windows • Godt skille mellom intern og sikker sone • Godt oppdaterte sikkerhetsløsninger (Netscaler, Palo Alto, ISE, Cisco Prime) •	• Lav serversikkerhet (ingen hardning, ingen antivirus, OK oppdateringsnivå, noen gamle serverOS) • Disaster Recovery er ennå ikke fullt operativt • Backup – Kort retention
MULIGHETER	**TRUSLER**
• Kommune CSIRT	• Cyber trusler • Lav kompetansenivå blant sluttbrukere

Figur 1 – Utdrag fra SWOT Sikkerhet i Østre Toten kommune, datert 2019.

Det vises for øvrig til omtale av SWOT-analysen under kapittel 2.3.2 Regionalt samarbeid.

2.2.4 Sikkerhetstilstand

KPMG har fått beskrevet at kommunen har opplevd seg selv som seriøse i forhold til iformasjonssikkerhet. Det er vist til at kommunen har hatt en informasjonssikkerhetsansvarlig (IKT leder) og at det er stilt krav til eksterne leverandører og samarbeidspartnere hva gjelder databehandleravtaler mv. Personvernet har fått sterkere oppmerksomhet etter hvert. Teknisk sikkerhet har imidlertid ikke blitt viet like mye oppmerksomhet.

KPMG har gjennom samtalene fått beskrevet at man nok har vært litt «lykkelig uvitende» om sikkerhetstilstanden. Kommunen har de siste årene ikke registrert noen alvorlige hendelser, utover sporadiske forsøk på tradisjonelle «phishing-angrep» mot kommunedirektør etc. Man hadde en oppfatning av at man var rimelig godt dekket når det gjaldt den tekniske tilstanden, ved at man faset ut gamle servere og holdt seg oppdatert. Samtidig var det også slik at kommunen hadde teknisk gjeld med eldre utstyr som skulle vært skiftet ut, men som av kapasitetshensyn ikke ble tatt tak i. Det er beskrevet som at sikkerhetsarbeidet har vært ad-hoc basert og en dårlig samvittighet.

Manglende tilgangsstyring har vært et tema, og der ble det foretatt noen innstrammninger for noen år siden. Det er trukket frem manglende kontroll på gamle brukere og tildeling av fulle admin-rettigheter til eksempelvis nye lærlinger. Fravær av segmentering på nettverk er også et forhold som er påpekt som en bekymring.

2.2.5 Ny kommunedirektør

KPMG har gjennomført en samtale med nåværende kommunedirektør som tiltrådte i Øste Toten kommune i august 2020. Formålet med samtalen har vært å få klarlagt hvilket bilde kommunedirektøren dannet seg av tilstanden på IKT-sikkerhetsområdet. I det følgende oppsummeres punktvis de forholdene kommunedirektøren har trukket frem i samtale med KPMG.

- Kommunedirektøren ble gitt en gjennomgang av kvalitetssystemet Compilo. Det var en bred gjennomgang og ikke spesielt knyttet til IKT-sikkerhet. Hovedinntrykket var at internkontrollsystemet var godt. Det var tildelt ansvar til enkeltpersoner og det var definerte rapporteringslinjer. Det forelå bl.a. en rutine for årlig rapportering på IKT-sikkerhet. Det ble påpekt av kvalitetsansvarlig at det var rom for forbedring, blant annet ved at kun deler av organisasjonen brukte systemet.

- Kommunedirektøren observerte at det var manglende driftsstabilitet på systemene, blant annet mye driftsstans. Det fremsto som at det var manglende planlegging eksempelvis ved fornyelse av sikkerhetssertifikater, og tilfeldig tilgangsstyring.

- Det opplevdes vanskelig å få tydelige svar på om kapasiteten ved IKT-avdelingen var god nok. Det ble bl.a. stilt direkte spørsmål om dette som ble referatført i porteføljestyringsmøte, både i forhold til digitaliseringsprosessen og ordinær drift. Driftsstabilitet ble satt øverst på agendaen av kommunedirektøren for 2021.

- Det ble aldri gitt tilbakemeldinger på at det manglet ressurser til å fokusere på sikkerhet. Kommunedirektøren hadde således ikke en oppfatning av at kommunen var i en kritisk situasjon mtp. IKT-sikkerhet.

- Det regionale samarbeidet i Gjøvik-regionen fremsto som uklart for kommunedirektøren. Det eksisterte et samarbeid på operativt nivå mellom IKT-sjefene, men det var uklart hvordan det ble styrt og fungerte i praksis.

- Kommunedirektøren tok initiativ overfor de andre kommunedirektørene for å revitalisere samarbeidet, men et planlagt møte, senhøsten 2020, ble avlyst pga. korona situasjonen.

2.2.6 Atea rapporten

Østre Toten kommune gjennomførte høsten 2020 en sikkerhetsgjennomgang av teknisk miljø med bistand fra Atea. Sikkerhetsgjennomgangen ble utført som et ledd i det regionale IKT samarbeidet mellom Gjøvik, Nordre Land, Søndre Land, Vestre Toten og Østre Toten kommune. Formålet med sikkerhetsgjennomgangen, slik KPMG har forstått det, var å kartlegge nåsituasjonen på sikkerhetssiden hos de fem kommunene som ledd i arbeidet med å se på synergier og samarbeide på tvers av kommunene innenfor IKT området.

Det fremgår av oversendt dokumentasjon at sikkerhetsgjennomgangen ble bestilt i februar 2020 og at den ble planlagt gjennomført over sommeren. Sikkerhetsgjennomgangen hos kommunen ble gjennomført i oktober 2020 og endelig rapport oversendt kommunen er datert 2. desember 2020.

Ved sikkerhetsgjennomgangen benyttet man et anerkjent rammeverk CIS 20, med hovedfokus på punktene 1-16. Østre Toten kommune ble definert som en virksomhet med egen IT-avdeling, men uten dedikerte sikkerhetsressurser.

Rapporten oppsummerte gjennomgangen og ga forslag til tiltak som kommunen kunne implementere med relativt enkle midler for å bedre sikkerheten. Med rapporten fulgte et vedlegg med til sammen 26 anbefalinger fordelt på kategoriene High, Medium, Low og Info, hvorav fire tiltak var under kategorien High (ett High/Medium).

KPMG har fått opplyst at den praktiske gjennomføringen av sikkerhetsgjennomgangen foregikk ved workshop(s) hvor alle ansatte ved IKT avdelingen deltok, og at Atea underveis ga løpende tilbakemeldinger om sikkerhetstiltak som senere også ble tatt inn i rapporten som anbefalinger. Det er opplyst til KPMG at det ikke ble utført noen umiddelbare tiltak som følge av de løpende tilbakemeldingene som ble gitt under sikkerhetsgjennomgangen.

Den endelige rapporten ble oversendt IKT-sjefen i kommunen, som videresendte rapporten til de som hadde deltatt på gjennomgangen. Økonomisjefen mottok også rapporten til orientering.

KPMG har fått opplyst at rapporten ble diskutert mellom IKT-sjefen og økonomisjefen. Man hadde et ønske om å ta tak i rapporten som helhet og ikke sette i gang ad-hoc baserte aktiviteter. På grunn av ressurssituasjonen ble derfor videre oppfølging av rapporten lagt til nyåret 2021.

Det er videre opplyst til KPMG at rapporten og tiltakene ikke ble ikke gjennomgått i detalj. Det er trukket frem at oppsummeringen i rapporten kan ha vært medvirkende til at man ikke så behovet for iverksetting av umiddelbare tiltak. I oppsummeringen fremgikk det at kommunen hadde mye på plass når det gjaldt sikring av IKT-tjenestene, til tross for de forholdene som ble påpekt i rapporten. Det ble påpekt at rapporten kun fremhevet de negative funnene, og ikke alt det positive og gode arbeidet som var lagt ned på sikkerhetssiden.

2.2.7 Internkontroll for sikkerhet og personvern

KPMG har som en del av våre undersøkelser også forsøkt å kartlegge i hvilken grad kommunen hadde implementert IKT sikkerhet som ledd i sin internkontroll. Det er av flere KPMG har snakket med, pekt på kommunens kvalitetsstyringssystem Compilo som en kilde til dokumentasjon for IKT sikkerhetsarbeidet i kommunen. KPMG har fått tilgang til dokumentasjonen som ligger lagret i kvalitetsstyringssystemet, og har også gjennomført samtale med vedkommende som var ansvarlig for for personvernprosjektet i kommunen for å få en beskrivelse av prosessene kommunen har gjennomført.

Kommunen startet arbeidet med personvern høsten 2017 for å være klare til GDPR trådte i kraft sommeren 2018. Kommunen etablerte et GDPR-prosjekt og ansatte personvernombud. Det nytilsatte personvernombudet og et par representanter fra kommunens administrasjon deltok på KINS kurs i grunnleggende personvern.

Kommunen hadde allerede etablert et kvalitetssystem via Compilo, og tok i bruk Compilos modul i GDPR som omfattet kartleggingsverktøy og oppsett av rutiner/prosedyrer. Deler av kommunens retningslinje om informasjonssikkerhet fra 2013 ble implementert i kvalitetssystemet. Det ble utarbeidet overordnede dokumenter som omfattet sikkerhetsstrategi, rutiner og prosedyrer og disse ble godkjent av

rådmannsgruppen. IKT-leder ble utpekt som Sikkerhetsleder og fikk det videre ansvaret med å forvalte dokumentene videre i linjen.

Kvalitetssystemet omfatter en rekke dokumenter som inneholder rutiner og prosedyrer for hvordan kommunens skulle organisere og gjennomføre arbeidet med sikkerhet og personvern. Mye ble publisert på kommunens kvalitetssystem, men en stor del av dokumentene ble ikke publisert eller tatt i bruk.

I prosjektet som arbeidet med å implementere GDPR i kommunen ble systemene til kommunen kartlagt, og det ble utformet en personvernanalyse på overordnet nivå. De enkelte tjenesteeierne fikk ansvar for å utføre tilsvarende analyse på mer detaljert nivå.

2.2.7.1 Kvalitetssystemet

Av rutinene og prosedyrene i kvalitetssystemet fremgår det at kommunens behandlingsansvarlig er kommunedirektøren. GDPR-prosjektet la ansvaret for å sikre at kravene etter GDPR var ivaretatt i de ulike tjenestene til sektoransvarlige. Det ble etablert en arbeidsgruppe under prosjektet bestående av nesten alle sektorene. Målet med arbeidsgruppen var å skape forståelse og kunnskap. De samlet eksempelvis alle tjenesteansvarlige i skole og omsorg for å skape forståelse og kunnskap, samt for å etablere ansvar. Det delegerte ansvaret fra kommunedirektøren til tjenesteansvarlige er ikke gjenspeilet i kvalitetssystemet.

2.2.7.2 Opplæring av ansatte

Kommunen tok i bruk nettkurs i informasjonssikkerhet og personvern utarbeidet av KINS i samarbeid med Bærum kommune fra 2018-2019. Kurspakken omfattet et lederkurs i informasjonssikkerhet og to ulike kurs innen personvern, henholdsvis ett om behandlings av særlige kategorier av personopplysninger og ett om alminnelige personopplysninger. Alle kommunens ansatte ble bedt om å gjennomføre nettkursene, men det har ikke blitt fulgt opp av kommunens ledelse om kursene har blitt gjennomført.

2.2.7.3 Personvernombud

Personvernombudet som ble ansatt i 2017 var en sterk bidragsyter inn i kommunens arbeid med å forberede seg på implementeringen av GDPR i norsk rett. Personvernombudet var bevisst sin rolle etter regelverket og var en rådgivende funksjon for kommunen. Personvernombudet fratrådte sin stilling november 2020. Kommunen forsøkte å finne en erstatter både internt i kommunen og eksternt ved blant annet å foreslå samarbeid med Gjøvik kommune. Dette lykkes ikke. Gjøvik kommune bisto kommunen med personvernombud etter hendelsen og frem til slutten av januar. Deretter ble en nyansatt medarbeider satt inn i rollen som personvernombud, og innehar denne rollen fremdeles.

2.2.7.4 Protokoll over behandlingsaktiviteter

Kommunen har brukt Datatilsynets veileder for protokoll over personopplysninger, samt Excel-arket Datatilsynet har utarbeidet. GDPR-prosjektet bisto tjenesteeierne med innføring og opplæring i hvordan protokollen skal fylles ut, men det har vært utfordrende for brukerne å håndtere protokollen pga. dens kompleksitet. I forbindelse med gjenopprettingen av systemene etter hendelsen har kommunen tatt i bruk protokollen som er tilgjengelig via kvalitetssystemet, og brukerne opplever den som mer brukervennlig. Kommunen har ingen rutiner for oppdatering av protokoll.

Kommunen har ingen rutiner eller praksis for revisjon, kontroll eller oppfølging av informasjonssikkerhet- og personvernområdet.

2.2.7.5 Eksterne leverandører/anskaffelser

KPMG har ikke funnet eller blitt gjort kjent med at det eksisterer rutiner eller prosedyrer for hvordan personvern og informasjonssikkerhet skal ivaretas i anskaffelsesprosesser, med unntak av en overordnet rutine for opprettelse av databehandleravtale. Etter gjennomførte samtaler og arbeidet fra gjenopprettelse av systemene etter angrepet har det fremkommet at kommunen legger til grunn at leverandørene har kontroll på disse områdene og aksepterer deres leveranser uten å ha utført selvstendige vurderinger eller stilt krav.

2.2.7.6 GAP-analyse

Det ble i slutten av januar utarbeidet en GAP-analyse av kommunens håndtering av personvern av KPMG i samarbeid med kommunen. I GAP-analysen fremkommer de observasjoner som er gjort, beskrivelse av

observasjonene og en vurdering av konsekvenser. GAP-analysen tar for seg følgende punkter og er vedlagt kartleggingen:

- Plasseringen av ansvar i organisasjonen
- Prosedyre for innsyn
- Rutine for avvikshåndtering
- Prosedyre for avvikshåndtering
- Rutine for behandling av personopplysninger
- Rutine for innsamling av personopplysninger og informasjon til de registrerte
- Prosedyre for oppretting av databehandleravtale
- Rutine for retting og sletting
- Rutine for gjennomføring av DPIA.
- Rutine for situasjoner hvor personopplysninger blir overført til land utenfor EU/EØS.
- Oppdatering av prosedyrene/dokumentasjonen ihht. nytt personvernregelverk

2.2.7.7 Sikkerhetsorganisering

Som en del av kommunens forberedelse til GDPR, ble det definert et sett med aktiviteter, roller og arenaer som skulle ivareta arbeidet med sikkerhet og personvern i kommunen. Følgende roller gitt et spesialt ansvar for dette:

- Rådmann
- Sikkehetsleder
- Enhetsleder/Avdelingsleder
- Leder IKT
- Rådman
- Sikkerhetsutvalg
- Systemansvarlig
- Personvernombud
- Fagansvarlig arkiv
- Etc.

Organiseringen tok opp i seg viktige ledelses- og internkontrollaktiviteter som skulle ivareta arbeidet med sikkerhet og personvern, herunder, men ikke avgrenset til:

- Utarbeide sikkerhetsmål
- Utarbeide sikkerhetsstrategi
- Årlig eller ved større endringer påse at informasjonssikkerheten ivaretas i.h.t sikkerhetsstrategien. Dokumentere resultat.
- Utarbeide og vedlikeholde oversikt over hvilke personopplysninger som behandles med elektroniske hjelpemidler.
- Gjennomføre risikovurderinger og dokumentere disse

- Vurdere behov for å endre sikkerhetsstrategi og sikkerhetsmål
- Utarbeide og vedlikeholde informasjon om ansvar-, myndighetsforhold og organisasjonskart.
- Konfigurasjonskart med info om tekniske sikkerhetsløsninger
- Godkjenning og informasjon om partnere / leverandører
- Utarbeide oversikt over akseptert nivå for risiko
- Plan for distribusjon og arkivering av dokumenter
- Rutiner for egenkontroll
- Ledelsens gjennomgang en gang pr år.
- Rutiner for konfigurasjonsendringer

Selv om internkontrollsystemet var publisert i kommunens internkontrollsystem, har de fleste av KPMGs intervjuobjekter erkjent at ingen eller få av aktivitetene i praksis ble fulgt opp. Eksempelvis har det har kun vært gjennomført et møte i kommunens Sikkerhetsutvalg som hadde et særskilt ansvar for å ivaretar informasjonssikkerheten for hele kommunen.

2.3 Arbeid med IKT-sikkerhet i norske kommuner

Oppdragsgiver har i forbindelse med oppdraget ytret ønske om at KPMG evt. identifiserer og innhenter relevant sammenligningsgrunnlag fra andre kommuner som kan si noe om hvordan tilstanden på IKT-sikkerhet i kommunen har vært i forhold til sektoren for øvrig. KPMG har i den forbindelse søkt å innhente relevant informasjon fra KS, samt gjennomført samtaler med flere av de andre kommunene i det regionale IKT-samarbeidet. Hensikten og formålet med dette har vært å etablere et grunnlag for en overordnet "benchmarking" slik at kommunen kan trekke erfaringer inn i det videre arbeidet på IKT sikkerhetsområdet.

2.3.1 Sikkerhetstilstanden i norske kommuner – KS

2.3.1.1 Innhentet dokumentasjon fra KS

KPMG har i forbindelse med oppdraget kontaktet KS med forespørsel om det finnes relevante undersøkelser eller øvrig materiale som kan benyttes som sammenligningsgrunnlag ved vurderingen av tilstanden på IKT-sikkerhetsarbeidet i kommunen. KS har som svar på forespørselen vist til følgende informasjonskilder:

1) Arbeidet med informasjonssikkerhet i fylkeskommuner og kommuner[3]
2) Kartlegging av digital modenhet i kommunesektoren[4]
3) Utredning av CSIRT i kommune sektoren[5]
4) Overordnet risiko- og sårbarhetsvurdering for IKT i helse- og omsorgssektoren[6]

KPMG har gjennomgått og vurdert kildene og funnet at «Arbeid med informasjonssikkerhet i fylkeskommuner og kommuner» er den mest relevante publikasjonen i forhold til vårt mandat.

2.3.1.2 Arbeid med informasjonssikkerhet i fylkeskommuner og kommuner, Digitaliseringsdirektoratet 2020

Digitaliseringsdirektoratet (heretter DigDir) har på oppdrag fra Kommunal- og moderniseringsdepartementet (KMD) undersøkt hvordan fylkeskommuner og kommuner arbeider med informasjonssikkerhet (2020)[4]. Dette arbeidet ble utført i samarbeid med KS og må sees i lys av tiltak 5 i «Tiltaksoversikt til Nasjonal strategi for digital sikkerhet» om at Digitaliseringsdirektoratets «arbeid med styring og kontroll på

[3] https://www.digdir.no/media/1102/download

[4] https://www.ks.no/contentassets/3f544fbe44c1404a8b81f7f98737509f/digital-modenhet.pdf

[5] https://norsis.no/wp-content/uploads/2018/05/Utredning-Kommune-CSIRT.pdf

[6] https://www.ehelse.no/publikasjoner/overordnet-risiko-og-sarbarhetsvurdering-for-ikt-i-helse-og-omsorgssektoren

informasjonssikkerhet skal utvides til å omfatte både statsforvaltningen og kommunene fordi utfordringene i statsforvaltningen gjelder også for kommunene».

Rapporten bidrar til en bedre forståelse av hvordan fylkeskommuner og kommuner i Norge arbeider med informasjonssikkerhet. For å vurdere sikkerhetstilstanden i norske kommuner benyttet DigDir og KS utredninger, rapporter og dokumenter fra SSB, DSB, NorSIS, KS, NOU og Datatilsynet fra perioden 2015 – 2020.

DigDirs rapport belyser flere sentrale utfordringer små og mellomstore kommuner har når det kommer til IKT-sikkerhetsdomenet. Rapporten indikerer at kommunestørrelse kan ha betydning for hvordan det arbeides med informasjonssikkerhet, der hvor små og mellomstore kommuner i noe mindre grad lykkes med risiko- og informasjonssikkerhetsarbeidet.

Flere av utfordringene knytter seg til svakheter med sikkerhetsstyring og kontroll. Små og mellomstore kommuner har i mindre grad enn fylkeskommuner og store kommuner en skriftlig informasjonssikkerhetspolicy og en formelt utnevnt person som er fagansvarlig for informasjonssikkerheten. Kommuner har i mindre grad enn fylkeskommuner evaluert, forbedret eller fornyet styringssystemet for informasjonssikkerhet. Og det er særlig de små kommunene som i liten grad gjennomfører risikovurderinger systematisk og periodisk.

Når det kommer til fylkeskommuner og kommuners evne til å øve på håndtering av IKT-sikkerhetshendelser, belyser DigDir og KS at det i for liten grad øves på hendelseshåndtering knyttet til det digitale domenet.

Fylkeskommuner og store kommuner gjennomfører mer kompetansehevende aktiviteter enn små og mellomstore kommuner. Men det poengteres at manglende kompetanse og forståelse hos både medarbeidere og ledere, samt manglende kultur, utgjør hindringer i forbindelse med informasjonssikkerhet, og at det ikke i tilstrekkelig grad arbeides med kompetanseutvikling og sikkerhetskultur i norske kommuner.

Utfordringene som presenteres av DigDir og KS i overnevnte rapport har vært gjeldende i flere år. Riksrevisjonen, Datatilsynet og Digitalt sårbarhetsutvalg har tidligere påpekt en rekke brudd på personvernreglene, alvorlige svakheter i informasjonssikkerheten og kompetansemangel innen IKT-sikkerhet i kommunene i Norge[7]. I perioden 2017 – 2018 kartla KS digital modenhet i kommunesektoren. Kartleggingen viser at kun 15% av kommunene/fylkeskommunene hadde en dedikert funksjon med ansvar for informasjonssikkerhet og ressursmangel oppgis som det absolutt største hinderet for arbeid med informasjonssikkerhet. Selv om andelen som har en dedikert funksjon med ansvar innen IKT-sikkerhet antas å ha økt siden 2018, synliggjør kartleggingen at utfordringene knytte til IKT-sikkerhet ikke bare er en utfordring i dag, men en langsiktig utfordring som ikke lar seg løse over natten.

2.3.2 Regionalt IKT samarbeid

Østre Toten kommune er en del av et regionalt samarbeid mellom Gjøvik, Nordre Land, Søndre Land, Vestre Toten og Østre Toten kommune. Samarbeidet dekker flere områder, herunder IKT området. Kommunene har hatt noe felles drift hos Gjøvik kommune av enkelte løsninger. I forbindelse med det regionale samarbeidet har det også vært en operativ arbeidsgruppe bestående av IKT-lederne for de enkelte kommunene.

KPMG har vært i kontakt med tre av de fire andre samarbeidskommunene, hvor formålet har vært å innhente overordnede erfaringer og læringspunkter for hvordan de tilstøtende kommunene har organisert og praktisert sitt arbeid med IKT-sikkerhet.

Oppdraget KPMG gjennomfører er for Østre Toten kommune, og gitt sensitiviteten som følger med sikkerhetsarbeid så er samtalene gjennomført under forutsetning av at ingen enkelt kommunes tilstand eller svar skal gjengis. KPMG vil derfor i det følgende kort oppsummere de observasjonene vi har gjort oss.

- Det er variasjon i hvordan man har praktisert sikkerhetsarbeidet. Enkelte har gjennomført selvstendige sikkerhetsrevisjoner i tillegg til Atea gjennomgangen. Resultatet er formidlet ut i

[7] https://norsis.no/wp-content/uploads/2018/05/Utredning-Kommune-CSIRT.pdf

enhetene gjennom samtaler med enhetsledere, noe som har bidratt til økt bevissthet omkring sikkerhet.

- Oppfølging av Atea gjennomgangen ble håndtert ulikt. Noen valgte å iverksette umiddelbare tiltak på flere områder, mens andre valgte å utbedre enkelt elementer og utsette de øvrige anbefalingene. KPMG er ikke kjent med detaljene eller funn gjort hos noen av de andre kommunene.

- Gevinsten av det regionale samarbeidet på IKT-området er beskrevet som begrenset. Det har vært lav frekvens på møter og prosesser tar lang tid.

- Det er igangsatt/gjennomført enkelte felles aktiviteter i det regionale samarbeidet. Det er blant annet vist til oppdrag fra RUG (Rådmannsutvalget i Gjøvikregionen) i mars 2019, hvor det ble gjennomført SWOT analyser av alle kommunene innenfor IKT-drift, IKT-sikkerhet og Digitalisering. Formålet var å utrede muligheter for utvidet samarbeid og mulig felles regional drift. Endelig mandat for forprosjekt skulle etter planen vært behandlet av RUG før sommeren 2021, men har blitt utsatt til over sommeren.

- Flere har trukket frem viktigheten av å ha riktig IKT-kompetanse i eget hus. Tilstrekkelig bestillerkompetanse, kompetanse til å stille krav og drive oppfølging av eksterne tilbydere og sikkerhetsstyring er nøkkelord.

- Etter hendelsen har det vært økt interesse for å få til et funksjonelt samarbeid på IKT siden i regionen. Man ser nytten av eksempelvis felles løsninger for monitorering og overvåking som er kostbart.

- Behov for sentralisert logging for bedre synlighet og evne til å detektere uønsket aktivitet. Mangelfull/fravær av monitorering og overvåking på infrastruktur og nettverk bekymrer flere.

- Det er en felles opplevelse av høyt press på IKT-ressursene. Det er ulik størrelse på organisasjonene, noe som også påvirker kapasitet til å kunne drive systematisk og proaktivt sikkerhetsarbeid. Økt digitalisering krever økt fokus og mer ressurser på IKT-sikkerhetssiden.

3. Vurdering

Vurderingene som presenteres i kapittelet baserer seg på faktagrunnlaget presentert i kapittel 2. Kapittelet vil drøfte kommunens tilstand på IKT-sikkerhetsområdet opp mot NSMs grunnprinsipper for IKT-sikkerhet[8] som inneholder tekniske og organisatoriske tiltak for å sikre god IKT-sikkerhet. Vi har også gjort en vurdering opp mot de andre kommunene i det regionale IKT-samarbeidet og offentlig tilgjengelig informasjon om arbeidet med IKT-sikkerhet i Kommune-Norge.

3.1 Vurdering av IKT-sikkerheten ift. NSM grunnprinsipper

3.1.1 Evne til å identifisere og kartlegge

Kommunen har etablert et ledelses- og internkontrollsystem for arbeidet med sikkerhet og personvern som bygger på Datatilsynets veiledere og inneholder enkelte sentrale elementer et slikt system bør inneholde. Ledelsessystemet bærer preg av å være rettet mot personvern og har hatt hovedfokus på elementer i NSM sine grunnprinsipper for å «beskytte og opprettholde», men inneholder få krav til hvordan kommunen skal jobbe med å «Identifisere og kartlegge», «Oppdage» og «Håndtere og gjenopprette», noe som er nødvendig for å imøtekomme dagens trusselbilde.

Kommunen har stilt krav til seg selv at det skal gjennomføres risikovurderinger. Kommunen har gjennomført risikovurderinger på enkelte områder, da i hovedsak knyttet til enkeltsystemer på bestilling fra «systemeier». Etter hva KPMG forstår har det ikke vært gjennomført en risikovurdering på den grunnleggende IKT-infrastukturen, men det ble i 2016 gjennomført en svært overordnet risikovurderingen på IKT-området. Denne risikovurderingen fremstår for KPMG som overordnet og ikke oppdatert i forhold til dagens trusselbilde. KPMG utelukker ikke at manglende risikovurderinger kan ha vært en medvirkende årsak til at kommunen ikke hadde tilstrekkelige tekniske og organisatoriske tiltak på plass da hendelsen inntraff.

Det har eksistert enkelte tekniske tiltak for å sikre oversikt over enheter tilknyttet kommunens IKT-infrastruktur og eksisterende brukertilganger, men som det fremgår av rapporten til Atea har ikke kommunen hatt fullstendig kontroll. KPMG vurderer risikoen som høy for at de etablerte tekniske løsningene og rutinene ikke har vært tilstrekkelige for å følge opp ansattes brukertilganger og rettigheter på IKT-infrastrukturen. En konsekvens av dette kan ha vært at ansatte over tid, har kunnet opparbeide seg utvidede rettigheter etter flere rollebytter i kommunen, som de ikke skulle hatt. Det har heller ikke vært etablert gode nok rutiner til å fange opp brukertilganger til ansatte som slutter, slik at disse har ligget aktive til tross for at arbeidsforholdet har vært avsluttet. Et konkret eksempel på manglende oppfølging knyttet til brukertilganger er administrator-brukeren som ble benyttet av trusselaktør ved datainnbruddet.

Kommunens internkontrollsystem stiller krav til å føre oversikt over alle behandlinger av personopplysninger med tilhørende systemstøtte. Rutiner og maler var fastsatt sentralt, men ansvar for kartlegging og dokumentering var tillagt de respektive tjenesteområdene. Det har imidlertid ikke vært noen som har hatt et sentralt ansvar for å følge opp at arbeidet i praksis ble gjennomført, hvilket har medført at kommunen i praksis ikke har hatt tilstrekkelig oversikt over personopplysninger og programvare som har vært i bruk. Det

[8] Introduksjon - Nasjonal sikkerhetsmyndighet (nsm.no)

er KPMGs forståelse at kun ett område har fulgt opp rutinene og kravene til dokumentasjon, for øvrig har oppfølging i stor grad vært fraværende hos de andre tjenesteområdene.

Det er KPMGS vurdering at manglende i internkontrollsystemet og den svake etterlevelsen skyldes at kommunen ikke har hatt tilstrekkelig kapasitet og allokert rett kompetanse for å gjennomføre fastsatte internkontrollaktiviteter.

3.1.2 Evne til å beskytte og opprettholde

Kommunens IKT avdeling vært liten og driften har vært avhengig av en håndfull nøkkelpersoner med hver sine kompetanseområder, spesielt på området drift, nettverk og systemadministrasjon. KPMG er blitt opplyst at kommunen hadde utfordringer med varierende driftsstabilitet på IKT-området. Fokus har vært på drift og opprettholdelse av tjenester, ikke sikkerhet. Det er KPMGs forståelse at det har vært få dokumenterte driftsrutiner og at man i stor grad har vært avhengig av den enkeltes egne arbeidsrutiner. Disse manglende kan ha medført at vesentlige sikkerhetsaktiviteter ikke har blitt tilstrekkelig gjennomført.

I august 2020 sluttet nettverksansvarlig i jobben. Det ble inngått en avtale med nettverksansvarlig hvor formålet var å få bistand til utførelse av de mest prekære oppgavene på kveldstid. Oppgavene til nettverksansvarlig ble, slik KPMG har forstår det, fordelt på de øvrige ansatte i IKT-avdelingen men uten at disse hadde inngående kjennskap til fagområdet. Det er KPMGs vurdering at konsekvensen av dette kan ha vært at nødvendige og kritiske sikkerhetsaktiviteter ikke har blitt fulgt opp i tilstrekkelig grad.

Kommunen hadde etablert en «sonemodell» som skulle beskytte systemer med særskilt beskyttelsesbehov, for eksempel for systemer innenfor helse og sosial. KPMGs tekniske undersøkelser og samtaler med nøkkelpersonell har gitt indikasjoner på at kommunen ikke hadde etablert en tilstrekkelig sikkerhetsarkitektur, og at det var vesentlige svakheter i den arkitekturen som var valgt. Blant annet har interne tjenester blitt eksponert på internett og kan potensielt ha blitt benyttet til å få tilgang til kommunens interne soner. Kommunens IKT-administrative nettverk har hatt tilgang på tvers av alle kommunens soner, både administrativ sone, sikker sone etc.

Det er pekt på at bruk av utvidede administrator rettigheter har vært et tema og bekymring, og at kommunen i liten grad tilpasset brukerkontoer etter prinsippet «need to have». Videre har kommunen hatt svake rutiner for å regelmessig følge opp kontroll med kontoene, herunder rutiner for regelmessig revisjon av tilganger og stenging av kontoer som ikke lenger var i bruk.

Kommunen har etablert en portefølje over digitaliseringsprosjektet som skulle bidra til å løfte kommunen digitalt. Kommunen har hatt en ambisjon om at sikkerhet og personvern skulle være en integrert del av digitaliseringen i kommunen. KPMGs vurdering er at kommunen i liten grad har hatt et bevist forhold til hvordan økt digitalisering og digital eksponering kunne påvirke risikobildet og hvilke tiltak som var nødvendig for å ivareta digital sikkerhet. Eksempelvis har man hatt for liten fokus på hvilke sikkerhetskrav man skulle stille til teknologien og det har i liten grad vært gjennomført risikovurderinger eller at disse har vært av for dårlig kvalitet. Risikovurderinger er både en plikt og et viktig verktøy for å kunne identifisere, vurdere og definere risiko og behov for tiltak. Kontroll med cyber- og informasjonssikkerhet er en forutsetning for en vellykket digitalisering, økt digitalisering og innføring av ny teknologi uten å tilstrekkelig vurdere risiko og etablere tiltak kan ha medført at tekniske løsninger har blitt innført uten tilstrekkelig sikkerhet.

Det er KPMGs forståelse at det i liten grad har blitt gjennomført risikovurderinger knyttet til sikkerhet i forbindelse med innføring av nye systemer og løsninger. Basert på opplysninger gitt KPMG, fremstår det som at det i mange tilfeller har vært opp til den enkelte IKT-konsulent å vurdere risiko før en endring gjennomføres. Det har vært vist til tilfeller der IKT-avdelingen har gjennomført endringer på anmodning fra systemeier og pålegg fra ledelse, til tross for at endringen har vært i motstrid med deres egne sikkerhetsmessige anbefalinger. KPMG vurderer det som at kommunen kan ha hatt mangelfulle rutiner og prosesser for innføring av nye systemer og løsninger, slik at disse ikke har blitt tilstrekkelig risikovurdert og IKT-avdelingens faglige råd ikke alltid har blitt hensyntatt.

Med utgangspunkt i kommunens digitaliseringsarbeid, varierende driftsstabilitet og IKT-avdelingens størrelse, er det KPMGs vurdering at det er risiko for at oppgavene til IKT-avdelingen og spesielt nettverksansvarlig, herunder vedlikehold og overvåkning, ikke har blitt tilstrekkelig ivaretatt. Dette kan ha medført at kommunen ikke i tilstrekkelig grad har evnet å gjennomføre tiltak for å beskytte og opprettholde et tilstrekkelig sikkerhetsnivå.

3.1.3 Evne til å oppdage

Kommunen hadde etablert grunnleggende tiltak som antivirus og endepunktssikkerhet, samt enkelte loggfunksjoner i sine IKT systemer for å kunne oppdage og respondere på sikkerhetsbrudd. Undersøkelser etter hendelsen viser at mye ikke ble logget og det fremstår for KPMG som at det var noe tilfeldig hvilke logger som var aktivert og ikke. Videre har logger, etter hva KPMG forstår i hovedsak blitt benyttet til feilsøking og enkel overvåkning, og i mindre grad til å kunne avdekke forsøk på og misbruk av kommunens IKT-systemer. Kapasitetsutfordringer i IKT-avdelingen kan også ha medført at logger som faktisk var aktivert, heller ikke ble tilstrekkelig gjennomgått på regelmessig basis.

Kommunen har hatt få verktøy for å oppdage kjente sårbarheter og ingen praksis for å gjennomføre inntrengningstester for å avdekke og utbedre kjente sårbarheter i infrastrukturen.

Kommunen har heller ikke gjennomført sikkerhetsrevisjoner for å forsikre seg om at fastsatte sikkerhetstiltak ble gjennomført og fungerte etter hensikten. Det foreligger ikke dokumentasjon på ledelsesinvolvering hva gjelder personvern og informasjonssikkerhet, utover et møtereferat ved lansering av nytt internkontrollsystem og den overordnede risikovurderingen fra 2016.

Det er KPMGs vurdering at kommunen har hatt svært få tiltak på plass for å kunne oppdage kjente sårbarheter og uønskede hendelser. Ledelsesinformering og involvering har også vært svak.

3.1.4 Even til å håndtere og gjenopprette

Kommunen hadde etablert en Beredskapsplan sist oppdatert i 2014. Beredskapsplanen inneholdt et avsnitt for IKT som primært beskrev planer ved midlertidig bortfall av IKT, som eksempelvis bortfall av strøm, brann etc. Beredskapsplanen inneholdt også beskrivelser for håndtering av «virus» og hvordan dette skulle håndteres. Planen tok ikke opp i seg målrettede angrep slik som kommunen ble utsatt for. Selve planen underbygger dog til dels risikoer avdekket i kommunens overordnede risikovurdering, noe som er metodisk riktig, selv om risikovurderingen etter vår vurdering har vært mangelfull i forhold til dagens trusselbilde.

Det er KPMGs vurdering at kommunen ikke hadde etablert tilstrekkelige tiltak for å kunne fange opp og vurdere og klassifisere hendelser. Det var heller ikke etablert tilstrekkelige tiltak eller prosedyrer for å kunne håndtere og kontrollere en hendelse. Selv om kriseplanen hadde en verdi under hendelsen, så var nytteeffekten svært begrenset på IKT-området. Det er også KPMGs vurdering at kommunen ikke har hatt tilstrekkelige prosedyrer og rutiner for å kunne evaluere og lære av hendelser.

KPMG har ikke vurdert selve krisehåndteringen da KPMG har gitt bistand til håndteringen.

3.1.5 Konklusjon

Det er KPMGs konklusjon at det forelå en rekke svakheter knyttet til IKT-sikkerheten forut for den alvorlige IKT-sikkerhetshendelsen i Østre Toten kommune. Selv om en rekke ulike tiltak har vært implementert innen å «Identifisere og kartlegge», «Beskytte og opprettholde», «Oppdage» og «Håndtere og gjenopprette», virker det tilfeldig hva som er på plass og tilnærmingen er i liten grad i tråd med «god praksis».

Den tilfeldige tilnærmingen til implementering av sikkerhetstiltak, og det faktum at enkelte svakheter har blitt identifisert, men ikke gjort noe med, trekker i retning av mangler ved sikkerhetsstyringen i kommunen. Fraværende sikkerhet- og risikostyring gjør også at helt sentrale sikkerhetstiltak verken er blitt identifisert eller implementert.

Vår konklusjon er at kommunen på hendelsestidspunktet, og i tiden før hendelsen, hadde lav modenhet innen NSMs grunnprinsipper IKT-sikkerhet og Sikkerhetsstyring.

3.2 Årsakssammenheng

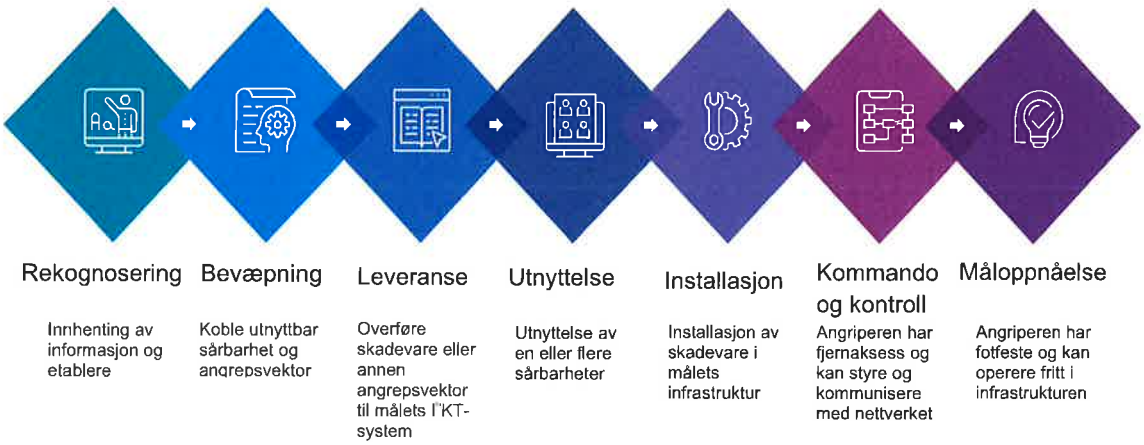
KPMG er bedt om å vurdere om det foreligger noen direkte og åpenbar årsakssammenheg mellom hendelsen og eventuelle funn og observasjoner gjort under kartleggingen.

KPMGs tekniske undersøkelser har ikke konkludert på noen direkte årsak til hvordan trusselaktør fikk tilgang på infrastrukturen hos Østre Toten kommune. Det har heller ikke vært mulig å fastslå med sikkerhet omfanget av informasjon som har kommet på avveie. På dette grunnlaget er det således ikke mulig å

konkludere på noen direkte årsakssammenheng mellom angrepet og den tilstanden på sikkerhet som er fremkommet gjennom denne undersøkelsen.

KPMG mener likevel det kan være en læringseffekt i å beskrive noen kjente forutsetninger for gjennomføring av et dataangrep, og knytte disse opp til det man vet om denne konkrete hendelsen.

På generelt grunnlag er et fellestrekk for de fleste cyberangrep, uavhengig av type, at de gjennomgår de samme angrepsfasene. Dette kan sorteres på eksterne aktiviteter i forkant av en kompromittering og interne aktiviteter i etterkant av en kompromittering, eller beskrives ved hjelp av cyber kill-chain modellen som vist i figuren under. Så snart en trusselaktør har oppnådd tilgang til et målnettverk vil aktøren forsøke å sikre fotfeste, skjule sin aktivitet, utvide tilganger og etablere persistens. Deretter vil aktøren benytte tilgangen til egen vinning, for eksempel til å hente ut data og kryptere filer, slik som ble gjort i kommunen.



Figur 2 – Elementer/steg i et digitalt angrep

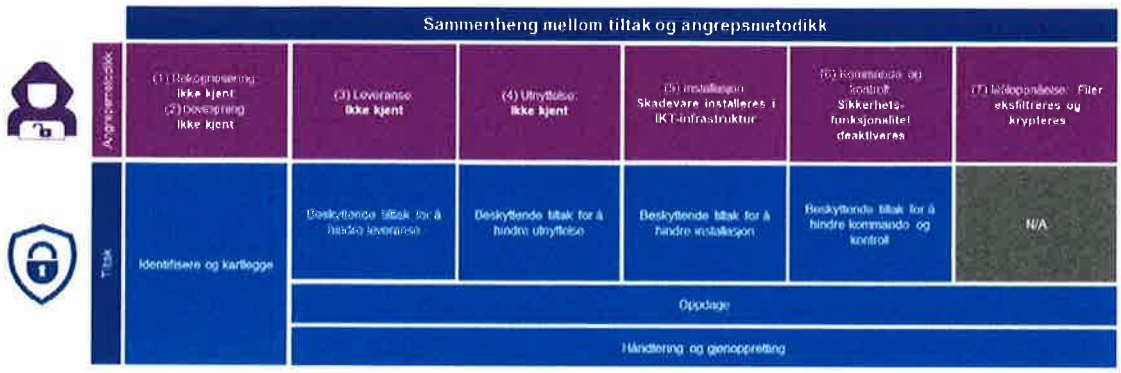
Manglende loggdatagrunnlag har bidratt til at det ikke har vært mulig å avdekke angrepsvektoren som trusselaktøren benyttet for å etablere fotfeste i kommunens IKT-infrastruktur. Trusselaktørens initielle aktiviteter er således ikke avdekket og man kan derfor ikke med sikkerhet fastslå hva trusselaktøren gjorde for å komme seg i posisjon til å kjøre løsepengeviruset (se figur 4).

Figur 3 – Angrepsmetodikken i henhold til kjent metodikk. De innledende aktivitetene er ikke avdekket.

Siden man ikke med sikkerhet kan si hvordan hendelsen oppstod og hva aktøren foretok seg før løsepengeviruset ble aktivert, må man ta utgangspunkt i mulige aktiviteter som kan ha funnet sted.

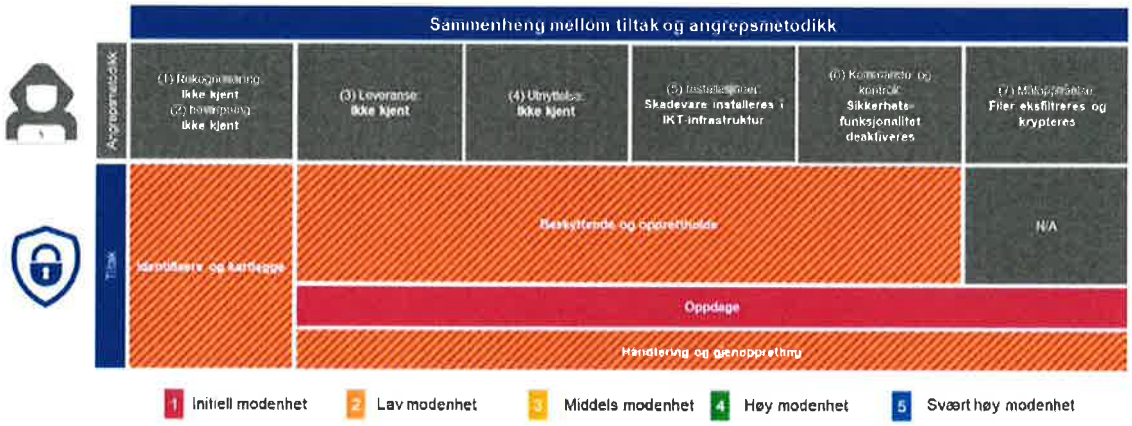
Dersom man hadde kjent trusselaktørens handlinger og aktiviteter i kommunens infrastruktur kunne man vurdert aktivitetene opp mot sikkerhetstiltak som ville ha stoppet trusselaktøren fra å komme seg videre i sin angrepsmetodikk. Prinsippet om sikkerhet i dybden har blitt et etablert prinsipp i sikkerhetsmiljøet. Tiltak

som tar sikte på å stoppe trusselaktøren i ulike steg i kill-chain begrenser aktørens evne til å skade systemer eller stjele informasjon.



Figur 4 – Mapping mellom angrepsmetodikk og sikkerhetstiltak

Fravær av sikre holdepunkter for trusselaktørs aktiviteter gjør at vi heller ikke kan vurdere konkrete sikkerhetstiltak som ville stoppet trusselaktøren i hvert steg. Vi blir i stedet nødt til å se på kommunens IKT-sikkerhet basert på etterlevelse av NSMs grunnprinsipper forut for hendelsen(vurdert i kap. 3.1) opp mot det vi faktisk vet trusselaktøren foretok seg. Av vurderingen i kap. 3.1 fremgår det at kommunens evne til å identifisere og kartlegge, beskytte, oppdage og håndtere og håndtere og gjenopprette var på et lavt nivå. Med dette utgangspunktet så mener vi at en illustrasjon over angrepet sett opp mot kommunens IKT-sikkerhet kan illustreres på følgende måte:



Figur 5 – Vurdering av årsakssammenheng

Vår vurdering er at kommunen på hendelsestidspunktet hadde en svært begrenset evne til å klare å oppdage og hindre en aktør fra å gjennomføre et angrep av typen løsepengevirus. Svakheter knyttet til sonemodellen, administrasjon av brukertilganger, begrenset kontroll over åpne porter og dataflyt, samt administrasjon og konfigurasjon av nettverkskomponenter mm. kan ha bidratt til å gjøre det enklere for trusselaktøren å etablere fotfeste i infrastrukturen. Den begrensede synligheten og overvåkingen i infrastrukturen bidro trolig til at trusselaktøren kunne operere uoppdaget helt til selve krypteringen fant sted.

3.3 Sammenlikning mot andre kommuner

Østre Toten kommune har bedt KPMG besvare om tilstanden i kommunen har vært bedre eller dårligere enn hos øvrige kommuner i Norge. Dette er svært vanskelig å sammenligne uten å gå mer metodisk til verks og gjøre tilsvarende undersøkelser i andre kommuner. Basert på tilgjengelig informasjon og de samtaler vi har hatt med kommunene i IKT samarbeidet, er det vår vurdering at arbeidet med personvern

og IKT-sikkerhet i norske kommuner generelt har stort forbedringspotensial, og at tilstanden i kommunen i stor grad gjenspeiler flere av de utfordringene som bl.a. DigDir trekker frem i sin rapport:

- Manglende kompetanse og personell for å utøve fagansvar for informasjonssikkerheten og de oppgraver dette medfører.
- At manglende kompetanse og forståelse hos både medarbeidere og ledere, samt manglende kultur, utgjør hindringer i forbindelse med informasjonssikkerhet, og at det ikke i tilstrekkelig grad arbeides med kompetanseutvikling og sikkerhetskultur i kommunen Norge.
- Det gjennomføres i liten grad risikovurderinger.
- Det i for liten grad øves på hendelseshåndtering knyttet til det digitale domenet.

Dette understøttes også i våre samtaler med de andre kommunene i det regionale IKT-samarbeidet. Selv om flere påpeker at de har gjennomført sentrale sikkerhetsaktiviteter som:

- Innleie av ekstern hjelp der de selv ikke har hatt kompetanse
- Sikkerhetsrevisjoner
- Risikovurderinger
- Tettere løpende oppfølging av råd og anbefalinger

Utover disse sikkerhetsaktivitetene er det er lite som tilsier at kommunen har stått overfor noen særskilte forhold som har satt kommunen mye dårligere stilt til å sikre sine digitale verdier enn andre kommuner på tilsvarende størrelse. Vi antar derfor at tilstanden i sammenliknbare kommuner ligger på omtrent samme nivå som kommunen var på forut for hendelsen, men at kommuner som har satt litt mer fokus på sikkerhet vil ligge på et litt høyere sikkerhetsnivå. Implementering av få, men viktige tiltak kan gjøre stor forskjell på sikkerhetstilstanden i en kommune.

3.4 Oppsummert vurdering

Det er KPMGs vurdering av IKT-sikkerhetstilstanden i kommunen forut for hendelsen bar preg av mangelfull sikkerhetsstyring. Sikkerhetsstyring danner grunnlaget for det forbyggende sikkerhetsarbeidet i kommunen og uten en velfungerende sikkerhetsstyring vil sikkerhetstiltakene verken være effektive eller tilstrekkelige for å oppnå et forsvarlig sikkerhetsnivå. Sikkerhetsstyringen skal sørge for at kommunen og dens ledelse har informasjonsgrunnlaget som trengs for langsiktig sikring av verdier på en god nok måte.

Det er KPMGs inntrykk at sikkerhetsstyringen i kommunen har vært mangelfull over tid. Sikkerhetstiltak har blitt implementert, men prosessen synes å være lite styrt og relativt tilfeldig. Det har resultert i betydelige svakheter i etterlevelsen av NSMs grunnprinsipper. Evnen til å «Identifisere og kartlegge», «Beskytte og opprettholde», «Oppdage» og «Håndtere og gjenopprette» vurderes som svak. Dette kan ha vært en medvirkende årsak til at konsekvensene av dataangrepet ble så omfattende.

Å implementere sikkerhetstiltak, enten de er organisatoriske, administrative eller tekniske er ingen garanti for at en trusselaktør ikke vil lykkes med sin måloppnåelse, men det vanskeliggjør trusselaktørens arbeid og bidrar samtidig til å oppdage angrepet slik at hendelsen raskt kan bli håndtert og redusere konsekvensene.

Da den faktiske angrepsvektoren ikke er kjent, er det ikke mulig å konkludere eksakt hvilke sårbarheter som ble utnyttet i angrepet og hvilke tiltak som burde ha vært på plass for å stoppe aktøren i den aktuelle IKT-sikkerhetshendelsen. KPMG mener likevel det er dekning for å anta at flere svakheter i kommunens sikkerhetsarbeid i sum har vært en medvirkende årsak til at hendelsen inntraff.

Det er grunn til å tro at IKT-sikkerhetstilstanden i flere norske kommuner er på linje med IKT-sikkerhetstilstanden i Østre Toten kommune forut for den alvorlige IKT-sikkerhetshendelsen. DigDir trekker frem flere sentrale IKT-sikkerhetsutfordringer når de beskriver IKT-sikkerheten i Kommune-Norge. De fleste utfordringene var i stor grad gjeldende for kommunen og det er lite som tilsier at kommunen har stått overfor noen særskilte forhold som har satt kommunen mye dårligere stilt til å sikre sine digitale verdier enn andre kommuner på tilsvarende størrelse. Mange av de vurderingene som er gjort i denne rapporten er således trolig av interesse for flere kommuner i Norge.

4. Anbefalinger

Et forsvarlig sikkerhetsnivå for informasjon og IKT-systemer oppnås ved å redusere risiko for uønskede hendelser til et akseptabelt nivå. For å lykkes er det nødvendig at kommunen har en velfungerende helhetlig sikkerhetsstyring som er en integrert del av virksomhetsstyringen og samtidig må det gjøres kontinuerlige vurderinger av risiko knyttet til egne verdier og håndtering av tilhørende risiko. Risikovurderingene må omfatte vurdering av verdier, identifisering av trusler og avdekking av sårbarheter. Risikovurderingene vil definere hva som er forsvarlig sikkerhetsnivå for kommunen og danner grunnlag for videre risikohåndteringsarbeid. En viktig del av risikohåndteringen er valg av sikkerhetstiltak. Tiltakene må tilpasses verdiene kommunen forvalter, for å redusere sårbarhetene i nødvendig omfang slik at risikoen havner innenfor rammen av hva kommunen kan akseptere. Beskyttelse av verdier ved hjelp av sikkerhetstiltak er dermed viktig for å kunne oppnå et forsvarlig sikkerhetsnivå. Under følger våre klareste anbefalinger for kommunen i deres videre arbeid med IKT sikkerhet:

- Kommunen bør ***oppdatere kommunedirektørens internkontroll*** på IKT-sikkerhet, i samsvar med anerkjente standarder. Videre må kommunen sikre at internkontrollen etterleves i praksis og ikke bare blir en papirøvelse.

- Kommunen må ***gjennomføre jevnlige risikovurderinger***, både overordnet, i IKT-avdelingen og i tjenesteområdene. Essensen i de risikovurderingene som gjøres bør tas med i en overordnet risikovurdering som presenteres for ledelsen slik at kommunedirektøren og hans ledelse er tilstrekkelig informert om tilstand på IKT-området og kan ta stilling til IKT-relatert risiko.

- Kommunen bør ***styrke sin kompetansen innen IKT-sikkerhet og personvern*** i kommunen. Uten tilstrekkelig forståelse og kompetanse vil det være svært utfordrende å oppnå et forsvarlig sikkerhetsnivå i kommunen. For å kunne vurdere risiko tilknyttet bruken av IKT, må kommunen ha oppdatert kunnskap om verdier, sårbarheter og trusler. Vår kartlegging synliggjør behovet for å styrke denne kunnskapen i kommunen, spesielt når det gjelder kunnskap om sårbarheter og trusler. Videre vil også kvalitet i internkontroll og internrevisjon innen IKT-sikkerhetsdomenet fordre en viss IKT-sikkerhetskompetanse hos de som utfører kontroll og revisjonsaktivitetene.

- Som følge av utkontraktering til IKOMM må kommunen ***ivareta god bestillerkompetanse,*** slik at kommunen kan stille riktige funksjonelle og sikkerhetsmessige krav til IKOMMs tjenesteleveranser. Kommunen må også kunne følge opp IKOMM og påse at de utøver sine forpliktelser, også når det kommer til sikring av kommunens digitale verdier. Det anbefales at kommunen bygger opp en viss egenevne og kapasitet for å ivareta sikkerhet og personvern i eget hus. Kompetansen kan leies inn ved behov, men det bør da etableres en tydelig plan for kompetanseoverføring.

- Kommunen og deres tjenesteleverandører bør ***innføre og styre etter NSMs grunnprinsipper*** og samarbeide om ivaretakelsen av de ulike prinsippene. Det blir viktig å sikre klart definerte ansvar, roller og grensesnitt for alle områder av NSMs grunnprinsipper for IKT-sikkerhet. Selv med tjenesteutsatt IKT-drift vil det være enkelte sikkerhetsfunksjoner som kommunen selv må ivareta, deriblant sikkerhetsstyring.

KPMG har basert på opparbeidet kjennskap til kommunens verdier, trusler og sårbarheter, utarbeidet en detaljert liste over forbedringsmuligheter innen IKT-sikkerhet (se appendix 1). Listen inkluderer både anbefalinger innen sikkerhetsstyring og konkrete tiltak relatert til etterlevelse av NSMs grunnprinsipper for IKT-sikkerhet.

Det er viktig å understreke at nivået på forebyggende sikkerhetsarbeid, risikohåndtering og sikkerhetstiltak må være realistisk og sett i forhold til kommunens rammer. Eksempelvis oppnås et forsvarlig sikkerhetsnivå lettere med realistisk gjennomførbare sikkerhetstiltak enn tiltak som i teorien er bedre, men som er i grenseland for hva kommunen klarer å gjennomføre. Rammebetingelser knyttet til økonomi, personell- og

kompetanse, er blant de vanligste begrensende faktorene. Det er derfor viktig at forebyggende sikkerhetsarbeid, risikohåndtering og sikkerhetstiltak sees i et helhetlig perspektiv. Sikkerhetsstyring må derfor være en integrert del av den øvrige styringen i kommunen og tiltakene må sees i sammenheng med risiko- og sikkerhetsstyring, samt øvrige sikkerhetstiltak.

5. Appendix

Rapporten inkluderer følgende vedlegg:

Appendix 1: Konkrete forbedringsmuligheter

Appendix 2: GAP analyse KPMG

Appendix 1 Konkrete forbedringsmuligheter

Basert på rapportens vurderinger er det utarbeidet en liste over forbedringsmuligheter som tar sikte på å heve Østre Toten kommunes modenhet innen IKT-sikkerhet.

#	Pri.	Kompleksitet	Tiltak ID (NSM)	Forbedringsmulighet
Anbefalinger innen sikkerhetsstyring				
1	1	MID	SP 1.2	Identifiser kommunens viktigste funksjoner og hvilke verdier som understøtter disse funksjonene
2	1	MID	SP 1.4	Gjennomfør sårbarhetsvurderinger med mål om å beskrive i hvilken grad eksisterende sikkerhetstiltak vil kunne hindre en trusselaktør i å kunne påvirke kommunens verdier
3	1	MID	SP 1.7	Gjennomfør konsekvensvurdering for å vurdere skadefølger eller konsekvenser det kan få for kommunen om verdiene blir utsatt for skadeverk eller ødeleggelse, og dermed faller helt eller delvis bort.
4	1	LAV	SP 2.2	Etabler sikkerhetsorganisasjon med definerte roller, ansvar, myndighet og oppgaver innen IKT-sikkerhet. Gå opp grensesnittet mellom ØTK og IKOMM og påse at ingenting faller mellom to stoler. Sørg for relevant opplæring.
5	1	MID	SP 2.3	Etabler styringssystem for IKT-sikkerhet for å sikre god sikkerhetsstyring i kommunen. Sikkerhetsstyringen danner grunnlaget for det forebyggende sikkerhetsarbeidet og etterlevelse av grunnprinsippene for IKT-sikkerhet. NSMs grunnprinsipper bør benyttes.
6	2	MID	SP 2.1	Identifiser aktuelle tiltak (organisatoriske, menneskelige, fysiske og elektroniske) basert på risikovurderinger. Prioriter og beslutt de aktuelle tiltakene, for deretter å implementere disse. NSMs grunnprinsipper bør benyttes.
7	2	HØY	SP 3.1	Sikre at det er nødvendig kompetanse i kommunen til å gjennomføre revisjoner som er rettet mot å kontrollere sikkerhetstilstanden. Revisjonene må inkludere IKOMMs tjenesteleveranser og ansvar innen IKT-sikkerhet.

8	2	LAV	SP 3.2	Kommuneledelsen må være tilstrekkelig informert om status på arbeidet med personvern og informasjonssikkerhet. Det må planlegges og gjennomføres kommuneledelsens årlige gjennomgåelse av styringssystemet for IKT-sikkerhet.
9	2	LAV	SP 4.1	Kommunen bør sikre at nødvendig dokumentasjon, det være seg styrende, utførende og kontrollerende dokumenter som ivaretar håndtering av hendelser er integrert i styringssystemet for sikkerhet. Grensesnittet opp mot IKOMM må gås opp som en del av dette arbeidet.
Anbefalinger innen IKT-sikkerhetstiltak				
10	1	LAV	IKT 1.2.3	Etabler rutine for å identifisere, følge opp eller luke ut uidentifisert utstyr i IKT-infrastrukturen.
11	1	LAV	IKT 1.2.4	Implementer verktøy og rutine for skanning av alle maskiner i nettverket regelmessig for å inneha oppdatert oversikt over applikasjoner, versjonsnummer og på hvilke enheter disse applikasjonene er installert.
12	1	HØY	IKT 2.1.9	Ta ansvar for kommunens sikkerhet også ved tjenesteutsetting til IKOMM. Etabler tilstrekkelig bestillerkompetanse gjennom hele livsløpet til tjenesteutsettingen.
13	11	HØY	IKT 2.2.3	Del opp kommunens nettverk etter virksomhetens risikoprofil og etabler sikkerhetsbarrierer mellom sonene for å hindre en aktør fra bevegelse mellom sonene.
14	1	LAV	IKT 2.3.1	Etabler et sentralt styrt regime for sikkerhetsoppdatering / patching.
15	1	LAV	IKT 2.3.2	Konfigurer klienter slik at kun kjent programvare kjører på dem
16	1	LAV	IKT 2.3.3	Deaktiver unødvendig funksjonalitet. Etabler en «security baseline» som sier noe om minimum sikkerhetsnivå på de forskjellige enhetsgruppene.
17	1	MID	IKT 2.6.4	Minimer rettigheter til sluttbrukere og spesialbrukere. Spesielt viktig da enkelte sluttbrukere i kommunen har utvidede rettigheter på sin klient. Brukere med administrator-rettigheter utgjør en større

				sikkerhetsrisiko enn ordinære brukere og man bør gjennomføre jevnlige revisjoner og kontinuerlig jobbe for å redusere antall «admin-brukere».
18	1	MID	IKT 2.6.5	Minimer rettigheter på driftskontoer
19	1	MID	IKT 2.9.1	Legg en plan for regelmessig sikkerhetskopiering av alle virksomhetsdata. Planen bør inkludere offline backup slik at backup ikke er tilgjengelig på nettverket dersom et angrep finner sted.
20	1	MID	IKT 3.2.3	Avgjør hvilke deler av IKT-systemet som skal overvåkes
21	1	MID	IKT 3.2.4	Beslutt hvilke data som er sikkerhetsrelevant og bør samles inn
22	1	MID	IKT 4.1.1	Etabler et planverk for hendelseshåndtering

Figur 6 - Anbefalingene henviser til NSMs grunnprinsipper for sikkerhetsstyring (SP) og NSMs grunnprinsipper for IKT-sikkerhet (IKT)

APPENDIX 2

INTERNT DOKUMENT
26.01.2021

GAP-analyse - Østre Toten kommune

Personvern og informasjonssikkerhet

OBSERVASJON	BESKRIVELSE	KONSEKVENS	STATUS
Det er ikke utarbeidet en rutine for gjennomføring av DPIA.	DPIA skal gjennomføres hvor en behandling representerer en høy risiko for de registrerte rettigheter og friheter. Datatilsynet har utarbeidet en egen liste med tilfeller hvor det må gjennomføres en DPIA. Det bør vurderes å utarbeide en egen DPIA-mal.	Det er risiko for at det ikke blir gjennomført DPIA på kommunens behandlingsaktiviteter som krever slike vurderinger.	DPIA mal er utarbeidet, og rutiner er under arbeid.
Det er ikke utarbeidet en rutine for situasjoner hvor personopplysninger blir overført til land utenfor EU/EØS.	Dersom kommunen overfører personopplysninger til land utenfor EU/EØS, må det foreligge et lovlig overføringsgrunnlag iht. GDPR. art. 45 – 49.	Det er risiko for at kommunen overfører personopplysninger i strid med regelverket. Dette kan føre til at både kommunen og den registrerte mister kontrollen over personopplysningene.	Påbegynt
Noen av prosedyrene/dokumentasjonen inneholder henvisninger til den gamle personopplysningloven og personvernforskriften. Se bl.a.: • Ansvarsmatrise. • Definisjoner. • Fastsetting av akseptabel risiko – GDPR.	Personopplysningsloven av 2000 er erstattet med en ny personopplysningslov av 2018.	Det er risiko for at personell gjør oppslag i uriktige paragrafer i lovverket.	Påbegynt
Plasseringen av ansvar i organisasjonen er ikke tilstrekkelig spesifisert.	Flere av rutinene/prosedyrene legger ansvaret på «behandlingsansvarlig»(mao. kommunedirektøren). Iht. personvernregelverket er det den behandlingsansvarlige som besitter det overordnede ansvaret, men det er antakelig ikke hensiktsmessig eller praktisk mulig at kommunedirektøren skal sitte med praktiske ansvaret for å fylle ut protokoller, informere de registrerte, osv.	Det er risiko for at ansvaret for å etterleve sentrale krav i personvernregelverket ikke blir plassert på riktig sted i organisasjonen.	Påbegynt
Prosedyre for innsyn Rutinen krever ikke at den registrerte skal få	Kommunen må ha et lovlig overføringsgrunnlag for å kunne overføre personopplysninger til land utenfor EU/EØS. Disse	Potensielt lovbrudd og risiko for at den registrerte mister kontrollen over sine egne personopplysninger.	Påbegynt

informasjon om hvilke overføringsgrunnlag som kommunen anvender ved overføring til land utenfor EU/EØS.	overføringsgrunnlagene finnes i GDPR. Kap. V. Ifm. med en innsynsbegjøring har den registrerte rett til å få informasjon om hvilket overføringsgrunnlag kommunen hjemler overføringen i, jf. GDPR. art. 15. (2).		
Prosedyre for innsyn Listen over unntak fra innsynsretten inneholder ikke alle unntakstilfellene i personopplysningsloven §§ 16 og 17.	Ytterligere unntakstilfeller listes opp i personopplysningsloven og bør beskrives i rutinen: • det må anses utilrådelig at den registrerte får kjennskap til av hensyn til vedkommendes helse eller forholdet til personer som står vedkommende nær • utelukkende finnes i tekst som er utarbeidet for intern saksforberedelse, og som heller ikke er utlevert til andre, så langt det er nødvendig å nekte innsyn for å sikre forsvarlige interne avgjørelsesprosesser • det vil være i strid med åpenbare og grunnleggende private eller offentlige interesser å informere om. • det vil kreve en uforholdsmessig stor innsats å gi innsyn eller • innsynsrett sannsynligvis vil gjøre det umulig eller i alvorlig grad hindre at målene med behandlingen nås.	Det er risiko for at kommunen gir innsyn i opplysninger som det er ulovlig, utilrådelig eller uforholdsmessig arbeidskrevende å gi innsyn i.	Påbegynt
Prosedyre for avvikshåndtering Rutinen inneholder ingen henvisning til den nyopprettede personvernombudsstilling en.	Personvernombudet bør involveres i alle avvikshåndteringssituasjoner hvor det er en mulighet for at personopplysninger er kommet på avveie. Iht. GDPR. art. 39 skal PVO gi råd om forpliktelser iht. regelverket og være kontaktpunkt for Datatilsynet.	Det er risiko for at PVO ikke blir involvert/involvert til riktig tidspunkt i håndteringen av avvik.	Påbegynt
Rutine for avvikshåndtering Rutinen beskriver ikke når avvik skal rapporteres til Datatilsynet og de registrerte, og innenfor hvilke tidsfrister dette skal skje.	Brudd på personopplysningssikkerheten skal rapporteres uten ugrunnet opphold og senest innen 72 timer etter oppdagelse, med mindre bruddet sannsynligvis ikke vil medføre en risiko for de involvertes rettigheter og friheter. Dersom det er sannsynlig at bruddet vil medføre en høy risiko for de	Det er risiko for at brudd på personopplysningssikkerhete n ikke blir rettidig rapportert til Datatilsynet/de registrerte.	Påbegynt

	involverte, skal de registrerte underrettes om bruddet uten ugrunnet opphold.		
Rutine for behandling av personopplysninger Rutinen inneholder ikke behandlingsgrunnlaget som kan brukes hvor behandlingen er nødvendig for berettigede interesser som forfølges av kommunen.	I utgangspunktet kan kommunen ikke anvende dette behandlingsgrunnlaget fordi det ikke skal brukes av offentlige myndigheter i utøvelsen av deres oppgaver. Det kan imidlertid tenkes situasjoner hvor kommunen kan bruke behandlingsgrunnlaget hvor det ikke er snakk om utførelse av deres oppgaver.	Det er risiko for at kommunen ikke gjennomfører behandlinger som de egentlig har et lovlig behandlingsgrunnlag for.	Påbegynt
Rutine for behandling av personopplysninger Rutinen beskriver ikke aktuelle behandlingsgrunnlag dersom kommunen skal behandle særlige kategorier av personopplysninger.	Dersom kommunen behandler særlige kategorier av personopplysninger, må det etableres et lovlig behandlingsgrunnlag i GDPR. art. 6 og art. 9.	Det er risiko for at kommunen behandler særlige kategorier av personopplysninger uten et lovlig behandlingsgrunnlag.	Påbegynt
Rutine for behandling av personopplysninger Rutinen inneholder ikke en fullstendig beskrivelse av de grunnleggende personvernprinsippene; Lovlighet, rettferdighet, og åpenhet.	Rutinen beskriver lovlighetskravet ved at kravet til behandlingsgrunnlag iht. art. 6 er omtalt. Behandlinger skal i tillegg være rettferdige og åpne. Dette bør beskrives i rutinen.	Det er risiko for at det ikke blir tatt tilstrekkelig hensyn til rettferdighet og åpenhet når personopplysninger behandles.	Påbegynt
Rutine for innsamling av personopplysninger og informasjon til de registrerte Rutinen mangler informasjon om følgende lovpålagte informasjonsposter: • informasjon om de berettigede interessene som forfølges av kommunen ved bruk av behandlingsgrunnlaget i GDPR. art. 6. (1) bokstav f. • Informasjon om overføringer til tredjeland/organisasjon i tredjeland og hvor denne	I tilfeller hvor kommunen behandler personopplysninger som ikke er et ledd i utførelsen av sine oppgaver, kan behandlingen hjemles i GDPR. art. 6. (1). (f). Det kan derfor tenkes tilfeller hvor den registrerte har krav på informasjon om det berettigede interessene som forfølges. Kommunen må ha et lovlig overføringsgrunnlag for å kunne overføre personopplysninger til land utenfor EU/EØS. Den registrerte har rett til motta personopplysninger om seg selv dersom behandlingsgrunnlaget som anvendes er samtykke eller behandlingen skjer automatisk. Det kan tenkes tilfeller hvor kommunen behandler personopplysninger som ikke er nødvendig for å utøve offentlig myndighet basert på samtykke eller avtale som skjer automatisk.	Det er risiko for at den registrerte ikke får lovpålagt informasjon om kommunens behandlinger.	Påbegynt

	overføringen er hjemlet. • Informasjon om retten til dataportabilitet		
Rutine for innsamling av personopplysninger og informasjon til de registrerte Rutinen beskriver ikke unntakene fra retten til informasjon som følger av GDPR. art. 14. (5)	I visse tilfeller er ikke kommunen pålagt å gi den registrerte informasjon om behandlingen. Dette forutsetter at opplysningene er innhentet fra andre kilder enn den registrerte selv. Disse unntakene bør beskrives i rutinen.	Mye unødvendig informasjonsarbeid kan bli gjort.	Påbegynt
Prosedyre for oppretting av databehandleravtale Prosedyren inneholder ikke informasjonsposter må være en del av en databehandleravtale.	Følgende informasjonsposter skal være en del av en databehandleravtale og er ikke beskrevet i prosedyren: • Pliktene og rettighetene til den behandlingsansvarlige (kommunen). • Plikt til å ha tilfredsstillende sikkerhetstiltak. • Databehandleren bistår den behandlingsansvarlige (ved hjelp av egnede tekniske og organisatoriske tiltak) å oppfylle plikten til å svare på anmodninger fra registrerte om utøvelse av deres rettigheter. • Databehandleren har en plikt til å bistå den behandlingsansvarlige med å overholde de forpliktelsene etter GDPR art. 32-36 som er relevante i det konkrete avtaleforholdet (risikovurderinger, avvikshåndtering, DPIA og forhåndsdrøftelser). • Databehandleren skal straks underrette kommunen dersom det oppstår brudd på personopplysningssikkerhet en. • Dersom bruddet medfører en risiko for de registrertes rettigheter og friheter, må varselet til den behandlingsansvarlige inneholde den informasjonen som kreves for at den behandlingsansvarlige skal kunne gi en utførlig	Det er risiko for at databehandleravtaler ikke oppfyller lovpålagte innholdskravene i GDPR og at databehandler ikke er tilstrekkelig ansvarliggjort i avtaleforholdet.	Påbegynt

	beskrivelse av bruddet til tilsynsmyndigheten. • Dersom bruddet medfører at den behandlingsansvarlige må varsle de registrerte, må databehandleren gi den informasjonen som kreves for at den behandlingsansvarlige kan ivareta plikten til å gi slik underretning på en tydelig måte, og i tråd med GDPR. art. 33. • Ved opphør av tjenestene som gjelder behandling av personopplysninger, er databehandleren forpliktet til å slette eller levere tilbake alle personopplysningene til den behandlingsansvarlige, og slette eksisterende kopier (det må fremgå tydelig hvilket alternativ som er valgt). • Databehandleren må gjøre tilgjengelig all informasjon som er nødvendig for å påvise at forpliktelsene i GDPR. art. 28 er oppfylt, for den behandlingsansvarlige. • Databehandleren må muliggjøre og bidra til revisjoner som gjennomføres av den behandlingsansvarlige eller en annen inspektør, på fullmakt fra den behandlingsansvarlige.		
Rutine for retting og sletting Rutinen beskriver ikke at kommunen kan fortsette å behandle personopplysninger dersom behandlingen er nødvendig for å fastsette, gjøre gjeldende eller forsvare rettskrav.	Den behandlingsansvarlige behøver ikke slette personopplysninger på eget initiativ eller etterkomme krav om sletting dersom det nødvendig å beholde personopplysningene i relasjon til et rettskrav.	Det er risiko for at personopplysninger av betydning for et rettskrav blir slettet av kommunen.	Påbegynt

Kontakt oss

Lars Wilberg
Partner
T +47 91 66 00 54
E Lars.wilberg@kpmg.no

Nils Harald Børve
Director
T +47 40 63 97 02
E nils.harald.borve@kpmg.no