Grethe Østby, Stewart James Kowalski

Hendelseshåndtering ved cyber-angrepet mot Østre Toten kommune

Hva kan vi lære fra håndteringen?

Rapport

28.09.2022

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Foto: Totens blad

NTNU
Kunnskap for en bedre verden

Historikk

VERSJON
1.0

FORFATTER(E)
Grethe Østby, Stewart James Kowalski

OPPDRAGSGIVER(E)
Østre Toten kommune

OPPDRAGSGIVER REF.
Kommunedirektør Ole Magnus Stensrud

DATO
28.09.2022

ANTALL SIDER OG VEDLEGG
24 sider, 3 vedlegg

Innholdsfortegnelse

Sammendrag. Det skjedde – hvordan ble det håndtert?

9. januar 2021 ble Østre Toten kommune utsatt for et cyber-angrep, et såkalt løsepengevirus. Omkring 240 virksomhets-systemer i kommunen ble utilgjengelige for bruk.

> «Løsepengevirus er en type skadevare som låser eller krypterer hele eller deler av innholdet på datamaskinen. Målet er å få brukeren til å betale løsepenger til angriperen. For at brukeren skal få tilgang til innholdet på egen datamaskin igjen, krever angriper at man betaler løsepenger, ofte i form av BitCoin.» [1]

Angrepet skjedde samtidig med håndteringen av den pågående covid19 pandemien, så organisasjonen var allerede under en krisehåndteringsdoktrine. Det ble allikevel tidlig lørdag morgen etter angrepet satt krisestab for å håndtere denne hendelsen spesielt, og prioriteringer ble gjort basert på forutsetningene som var til stede. Hendelseshåndteringen ble som kjent svært langvarig, og var en krevende prosess for organisasjonen.

I forbindelse med alle type hendelser som er av betydning, anmoder Statsforvalteren i det gitte området om å evaluere hendelser basert på sin instruks (forskrift) [2]. I Østre Toten sitt tilfelle ble det også tildelt skjønnsmidler fra Statsforvalteren, slik at ansatte skulle kunne frigjøres til å delta i evalueringen. Hovedmålene med evalueringen av cyber-sikkerhetshendelsen i Østre Toten var å både lære internt i kommunen av det som har vært erfart, men også at andre skal kunne lære av hendelsen. Rammene for evalueringen av cybersikkerhetshendelsen skulle utøves i en slik form at erfaringer og tilegnet kunnskap også skal kunne benyttes i undervisning, trening og øvelser. Dermed ble vi ved Norges Tekniskvitenskapelige Universitet (NTNU), Institutt for Informasjonssikkerhet og kommunikasjonsteknologi, som forsker på denne type hendelseshåndtering, plukket ut til å gjennomføre denne evalueringen. Mandatet er i sin helhet gjengitt i vedlegg 1.

Vi tilnærmet oss oppdraget med å gjennomføre en spørreundersøkelse, samt gjennomføre dybdeintervjuer. Av totalt n=38 som aksepterte å delta i forskningsprosjektet, svarte x=28 på hele spørreundersøkelsen og y=9 deltok i dybdeintervjuer. Resultater fra spørreundersøkelsen og dybdeintervjuene er presentert i vedlegg 2.

Arbeidet har gitt oss mye informasjon som kan benyttes til både opplæring, trening og øvelser, men vi vil allikevel trekke frem noen hovedfunn, som er spesielt viktige for kommunen selv, samt andre kommuner og organisasjoner som bør forberede seg på et cyber-angrep:

1) Cyber-angrep krever en egen plass på organisasjonens risiko- og sårbarhetsliste (kan ikke betraktes som strømbrudd eller ekom-feil).
2) Eksterne informasjonskrav er ekstraordinære, annerledes og mer krevende enn i en «normal» hendelse (f.eks. fra nasjonale sikkerhetsorganisasjoner, etterretningsorganisasjoner, CSIRT, databeskyttelsesmyndighet etc.).
3) Beredskapsplaner må inneholde en plan for og kontrakt med et eksternt IKT-hendelseshåndterings- og gjenopprettingsteam (hvis slikt personell ikke er en del av organisasjonen).
4) I tillegg bør også beredskapsplaner inneholde en plan for hvordan man håndterer sensitive personopplysninger på avveie.

5) Intern kommunikasjon omkring prioritering og løpende oppfølging av uløste situasjoner er svært krevende, og over tid kan krisestyringslinjen kortsluttes, og man trenger da en god plan for hvordan man ønsker å håndtere dette.
6) Vi anbefaler at det stilles krav om trening og øving av cyber-angrep på lik linje med andre hendelser, og det bør stilles krav til offentlige beredskapsorganisasjoner om å gjennomføre denne type øvelser i nær framtid.
7) Krysskoordinering (regulert) fra lokal koordinering (Statsforvalter) og nasjonale myndigheter (Nasjonal sikkerhetsmyndighet) i slike angrep skaper til tider forvirring og usikkerhet, og det må under dagens regime planlegges for å kunne håndtere begge deler.

I tillegg har vi funnet sammenhenger mellom de ulike tilnærmingene vi hadde i spørreundersøkelsen, samt gjort nye erfaringer ved bruk av modenhetsanalyse (da i dette tilfellet fordi vi benyttet den i etterkant av hendelsen, samt at den ble distribuert blant alle som deltok i spørreundersøkelsen i motsetning til å bli benyttet for å forberede for øvelser som vi tidligere har gjort). Resultatene fra dette vil bli presentert i vitenskapelige artikler, samt i Østby sin doktorgradsavhandling. Vi kan i denne sammenheng påpeke at det eksempelvis er for få svar på noen av spørsmålene i spørreundersøkelsen, og at disse dermed ikke kan benyttes i vitenskapelig sammenheng. Dette og andre forhold som har påvirkning på resultatene vil bli presisert i det øvrige vitenskapelige arbeidet. Svarene er imidlertid presentert i sin helhet i vedlegget i denne rapporten, for å gi en oversikt over hva undersøkelsen innebar.

En del av titlene i rapporten er ikke titler som eksisterer til vanlig, men er brukt for å gi et bilde av hva ansvaret besto i hendelseshåndteringen. Et slikt eksempel er gjenopprettingsansvarlig. Det var jo også slik at det i svarene i dybdeintervjuene ble benyttet navn, og disse navnene er da erstattet med titlene som er presentert under Vurdering av resultatene.

En kommune er en kompleks organisasjon med mange sektorer, og man skulle nok kanskje ønsket seg å gjøre flere dybdeintervjuer opp mot flere av sektorene, men vi valgte å plukke ut noen fra de ulike nivåene i organisasjonen. Dermed kunne vi vurdere tidligere akademisk arbeid på området, samtidig som vi har gitt noen muligheter til å vurdere hva disse resultatene kan bety for kommunen selv og andre kommuner og organisasjoner. Det bør være mulig å bygge opp gode scenarioer for øvelser ved å lese erfaringene fra deltakerne i dybdeintervjuene. Samtidig vil det altså være noe mangelfullt for enkelte sektorer og organisasjoner, men vi anmoder om å bruke materiellet i form av «hva ville i så tilfellet ha skjedd hos oss».

Introduksjon og bakgrunn

Stadig flere organisasjoner også i Norge blir utsatt for målrettede cyber-angrep [3]–[6], og kunnskap om og forståelse for hvordan man skal håndtere slike hendelser er etterspurt [7], [8]. Tidligere studier har vist at det er behov for sosio-teknisk tilnærming til denne type hendelseshåndtering [9]–[11], og i sin avhandling [9] beskriver Kowalski hvordan man i en håndtering av cyber-sikkerhet kontinuerlig må ha fokus på både sosiale og tekniske forhold i en organisasjon. Dette er presentert i figur 1.

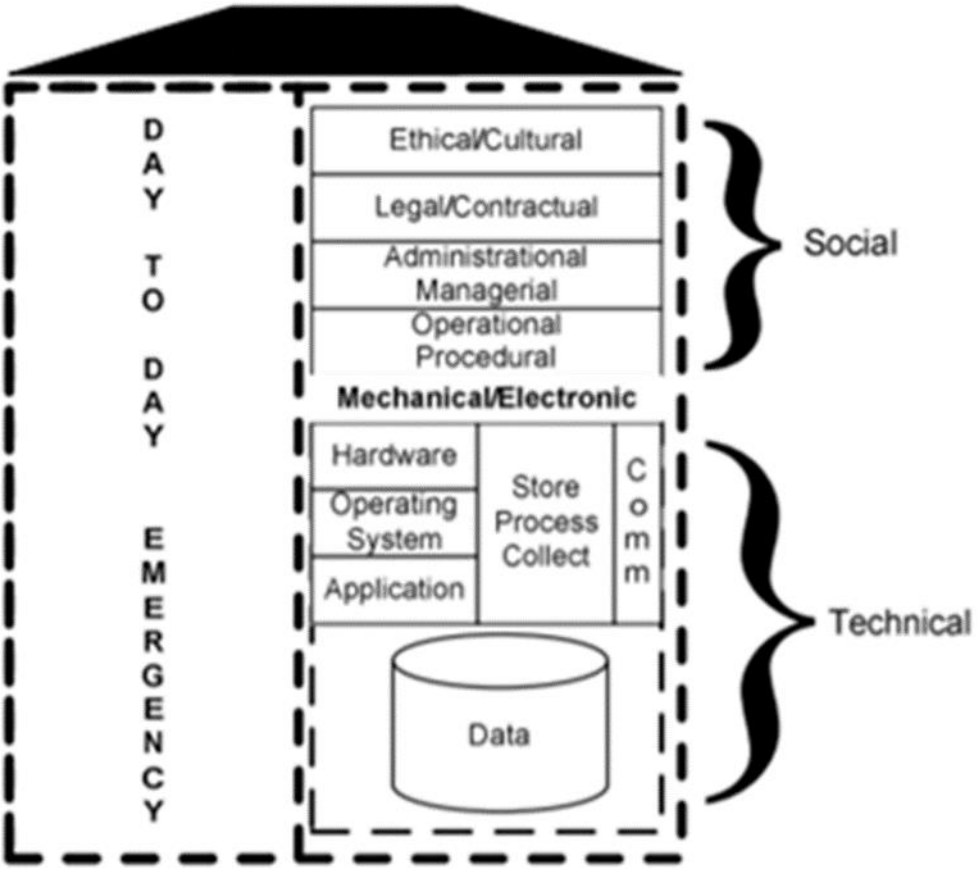


Fig. 1. Sosio-teknisk håndtering av cyber-hendelser [9]

Et nylig studie [10] foreslår også å kombinere denne type sosio-teknisk håndtering med National Institute of Standards and Technology (NIST) sitt rammeverk for hendelseshåndtering [12]. NIST sitt rammeverk er presentert i figur 2.

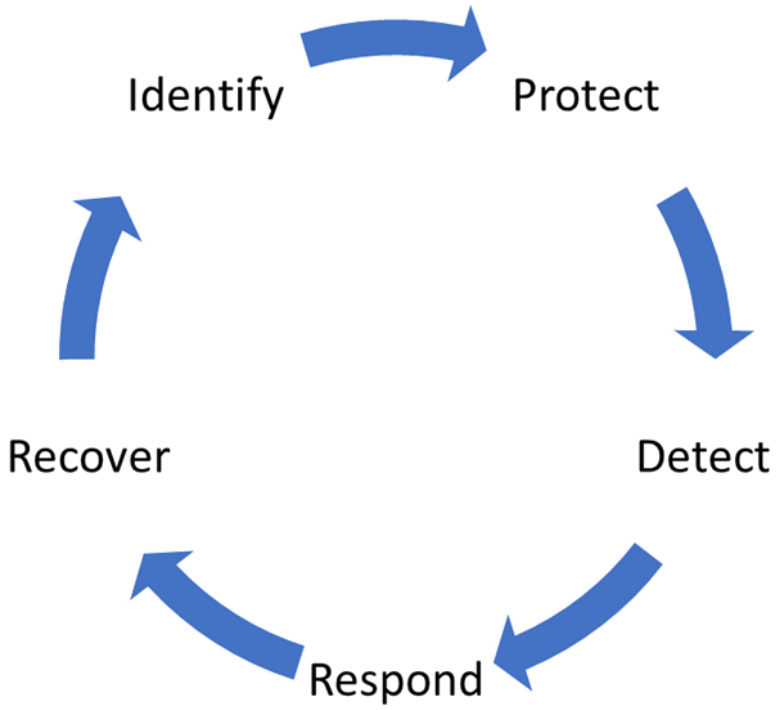


Fig. 2. NIST rammeverk for cyber-sikkerhet [12]

Tilsvarende rammeverk er foreslått i Nasjonal sikkerhetsmyndighet (NSM) sine grunnprinsipper for IKT-sikkerhet, som i stor grad likner NIST sitt rammeverk. Dette er presentert i figur 3.

Fig. 3. NSM sine grunnprinsipper for IKT sikkerhet [13]

Den senere tid har også Nasjonal Sikkerhetsmyndighet (NSM) utarbeidet rammeverk for håndtering av cyberangrep [13], mens Næringslivets sikkerhetsråd (NSR) har gitt ut en Nødplakat for digitale angrep i samarbeid med NSM og Politiet [14]. Som beskrevet i NSM sitt rammeverk, er relevante lover og forskrifter i denne sammenheng blant andre Lov om forebyggende sikkerhet (sikkerhetsloven) med forskrifter, Lov om behandling av personopplysninger (personopplysningsloven) med forskrift, Lov om elektronisk kommunikasjon (ekom-loven), Straffeloven, Politiregisterloven, Lov om helseregistre og behandling av helseopplysninger (helseregisterloven), Lov om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven), Lov om arkiv (arkivloven), Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven), Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) og Forskrift om offentlige arkiv (arkivforskrifta). I tillegg tillegges NSM ansvar for å koordinere IKT-sikkerhetshendelser ved angrep mot kritisk infrastruktur. Allikevel presiseres det i rammeverket til NSM at rammeverket ikke gjelder konsekvenshåndteringen av hendelsen. Det vil med andre ord være organisasjonen selv som må lage planer for håndteringen.

I Norge er det gitt et rammeverk for krisehåndtering for kommuner spesielt gjennom Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret [15] med dertil forskrift [16] og veiledning til forskriften [17]. Samtidig har Statsforvalteren et ansvar for å koordinere større hendelser i sitt geografiske område, og dermed på tross av nasjonal koordinering av IKT-hendelsen, skal altså Statsforvalteren koordinere konsekvensene av hendelsen. Det har derfor vært viktig i arbeidet med denne rapporten å også se på hvordan en kommune (eller en hvilken som helst annen organisasjon) vil måtte forholde seg til dette, og dermed også vurdere sine beredskapsplaner for å både kunne bli koordinert av nasjonale myndigheter samtidig som også av Statsforvalter. I tillegg har det blitt vurdert ulike andre interessenter som kommune-CSIRT, Kommunesektorens interesseorganisasjon (KS), Datatilsynet, og i Østre Toten sitt tilfelle også henvendelse fra Cyber-Forsvaret, som har måttet bli håndtert etter beste evne og etter kommunens besluttede intensjon om åpenhet rundt det som hadde skjedd.

Det å kunne lære fra kriser, eller det vi kan kalle kriseindusert læring, er en sjelden tilstand da en krise er en sjelden tilstand i seg selv [18]. Å lære fra øvelser på samme måte som læring fra hendelser er imidlertid anerkjent [19], og faktorer som støtter læringsaktiviteter i en øvelse kan betraktes som en teknikk som brukes i kunnskapsledelse.

> "Kunnskapsledelse er et sett med teknikker og praksiser som letter flyten av kunnskap inn i og innenfor firmaet." [20]

Overlappingen mellom kunnskapsledelse og organisatorisk læring gjør det imidlertid vanskelig å skille mellom de to [21], men man må anta at den organisatoriske læringen kan foregå uten ledelse. Organisatorisk læring har vært diskutert siden slutten av 1950-tallet [22], men vi vil argumentere for at øvelser også kan etablere grunnlaget for organisasjonslæring, spesielt for å forbedre kunnskap om informasjons- og cybersikkerhet.

> "Organisasjoner er gjenstander designet for menneskelige formål. Organisasjonens effektivitet avhenger av deres kontinuerlige redesign som

> svar på endrede verdier og en skiftende kontekst for handling. Organisatorisk læring vil da referere til denne prosessen med å kontinuerlig redesigne.» [23]

Beslutninger i en krise i beredskapsorganisasjoner tas ofte ved triage-beslutninger. "Selv om de er utviklet for enkeltpersoner, kan konseptene som brukes i et triagevurderingssystem også brukes på organisasjoner i krise" [24]. Innenfor informasjonssikkerhet viser eksempler at triage også kan være en del av hendelsesresponssystemene [25], og vi mener at dette er overførbart til både krisehåndtering og beslutningsteorier, og kan gjøre det lettere å trene sammen og lære av hverandre.

> "Beslutningstaking under usikkerhet handler om å ta valg hvis konsekvenser ikke er helt forutsigbare, fordi hendelser vil skje i fremtiden som vil påvirke konsekvensene av handlinger som tas nå." [26]

Vi mener at øvelser ikke bare kan bidra til teamlæring [27], men også til å legge grunnlaget for organisatoriske beslutninger for endringer for å forbedre modenhet innenfor informasjonssikkerhet og dessuten håndtere fremtidige kriser som har samme mengde usikkerhet.

For å kunne få til en slik læring i øvelser, skal det allikevel til en planlegging av slike øvelser, blant annet med bakgrunn i nettopp tidligere hendelser [11], men også 1) sårbarhetsvurderinger i den gitte organisasjonen, 2) vurdering av historiske trusler og angrep, 3) modenhetsundersøkelser, 4) tilrettelegging for gode leksjoner, og 5) spesifikke sosio-tekniske læringsartifakter i løpet av øvelsene [28]. For å nå målet i mandatet om at både Østre Toten og andre organisasjoner skal lære av hendelsen, ble dermed spørsmål omkring disse forholdene inkorporert i spørreundersøkelsen, men også som åpne spørsmål i dybdeintervjuene.

Siste del av spørreundersøkelsen var en ren modenhetsundersøkelse utviklet av Wahlgren og Kowalski [29], som er rettet mot evnen til å gjennomføre hendelseshåndtering dersom en IKT-sikkerhetshendelse skulle oppstå.

> «En prosess i en modenhetsmodell kan vurderes i mer enn ett prosjekt (dvs. flere forekomster av en prosess). Alle forekomster er samlet for å vurdere prosessen. Økning av antall prosessinstanser i vurdering bør derfor ikke tolkes som en måling av organisatorisk omfang.» [29]

Som vist i figur 4, består Wahlgren og Kowalski modenhetsmodell av en matrise hvis rader representerer ulike modenhetsnivåer og hvis kolonner representerer ulike modenhetsattributter. De brukte ISACAs[1] [30] modenhetsmodell som grunnlag for sin modell. Modenhetsnivåene er de samme som de fem modenhetsnivåene Humphrey et al. benyttet [31], og i likhet med ISACA la Wahlgren og Kowalski til et sjette nivå "Ikke-eksisterende". De brukte ISACAs modenhetsattributter som utgangspunkt, men tilpasset dem rundt eskalering av IT-relaterte sikkerhetshendelser.

[1] ISACA var tidligere kjent som Information Systems Audit and Control Association, men bærer nå kun navnet i form av akronymet ISACA

Attribute / Level	1 Awareness	2 Responsibility	3 Reporting	4 Policies and standards	5 Knowledge and education	6 Procedures and tools
0 Non-existent						
1 Initial						
2 Repeatable						
3 Defined						
4 Managed						
5 Optimized						

Fig. 4. Modenhetsmodell [29]

> «Det er åtte forskjellige modenhetsattributter i Wahlgren & Kowalski sin modell:
> A. Bevissthet omhandler ulike aspekter av hvor bevisste ansatte er på ulike IT-relaterte sikkerhetshendelser.
> B. Ansvar omhandler fordeling av ansvar innen organisasjonen for IT-relaterte sikkerhetshendelser.
> C. Rapportering omhandler rapporteringskanalene og hvordan regelmessig rapportering av IT-relaterte sikkerhetshendelser gjøres.
> D. Retningslinjer omhandler ulike retningslinjer for IT-relaterte sikkerhetshendelser.
> E. Kunnskap omhandler ulike ferdigheter og kunnskaper som trengs for å håndtere IT-relaterte sikkerhetshendelser.
> F. Prosedyrer omhandler ulike prosedyrer for håndtering av IT-relaterte sikkerhetshendelser.
> G. Midler omhandler ulike verktøy for håndtering av IT-relaterte sikkerhetshendelser.
> H. Struktur omhandler ulike forhåndsdefinerte grupper for håndtering av IT-relaterte sikkerhetshendelser.» [29]

Dette er første gang denne modellen er testet hos en organisasjon i etterkant av en hendelse, og må omtales deretter uten sammenlikning med andre undersøkelser. Som nevnt i sammendraget så vil resultatene fra dette arbeidet presenteres i vitenskapelige artikler og Østby sin doktorgradsavhandling.

I det følgende presenteres valgt metode for arbeidet, vurdering av resultatene (diskusjon) og en kort oppsummering med fremtidige vurderinger av nødvendig arbeid. Mandatet og deler av resultatene fra spørreundersøkelsen og dybdeintervjuene presenteres i henholdsvis vedlegg 1 og vedlegg 2.

Metode

I dette arbeidet har vi benyttet oss av forskningsmetodikken «Designvitenskapelig forskning innenfor informasjons systemer» (DSRIS) som har vist seg nyttig når man skal utvikle og teste nye artefakter innenfor informatikk [32]. Designvitenskapelig forskning innenfor informasjons systemer (DSRIS) er en metodikk som kan utføres for å "teste innovasjoner og ideer som kreerer resultater gjennom utviklingsprosessen av artefakter på en effektiv og samtidig nyttig måte" [32].

Hvordan man jobber med DSRIS er presentert i en oppgave skrevet av G. R. Karokola [33]. Han visualiserte denne tilnærmingen som skissert i figur 5. Imidlertid har vi modifisert Karokola sin modell, og da vi allerede tidligere har foreslått løsninger (induktiv tilnærming) slik som beskrevet i mandatet, så har dette altså vært det første steget i prosessen i vårt tidligere arbeid, i stedet for abduktiv tilnærming som Karokola benyttet.

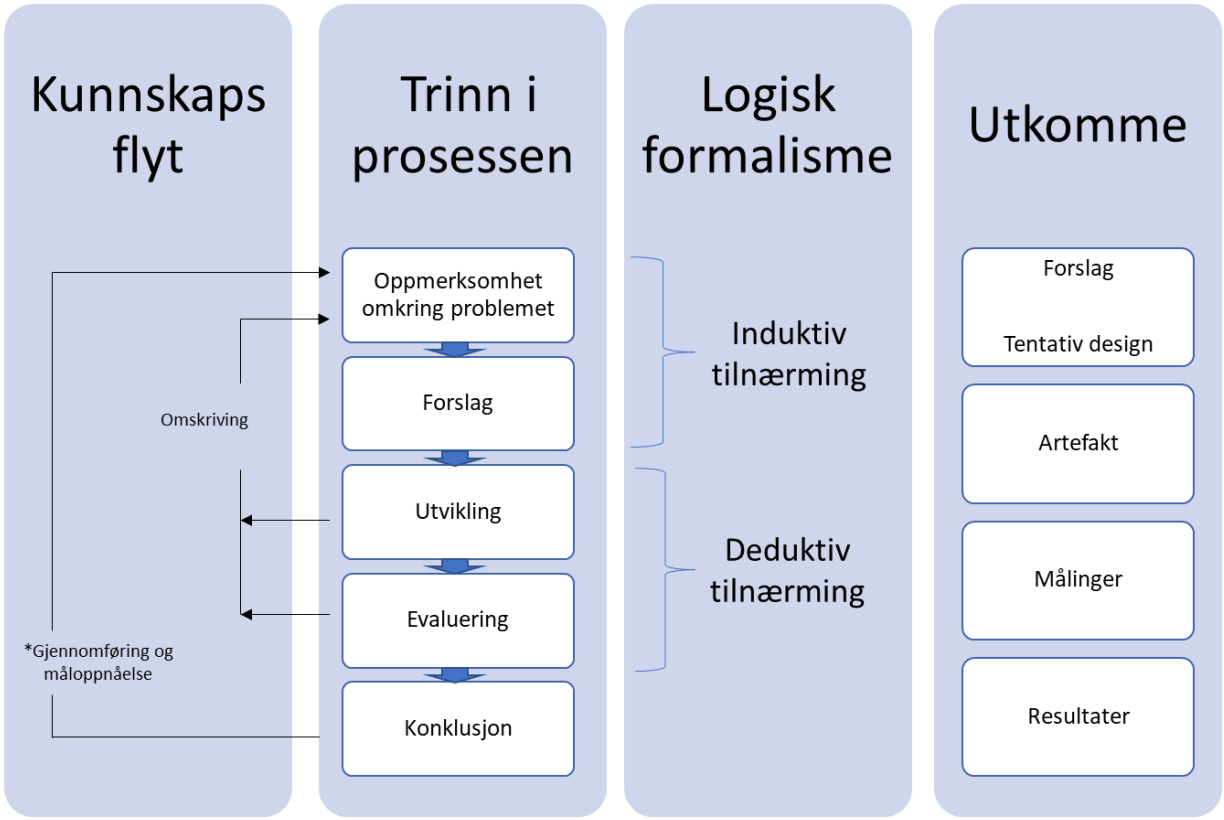


Fig. 5. Designvitenskapelig forskning innenfor informasjons systemer – modifisert [33]

Da forskningsarbeidet i Østre Toten kommune også skal benyttes i Østby sitt totale PhD-arbeid, så ble arbeidet i stor grad lagt opp til å verifisere tidligere arbeid. Som visualisert har Østby tilnærmet seg sitt PhD-arbeid med det som kan omtales som en induktiv tilnærming (i stedet for abduktiv eller deduktiv). Induktiv tilnærmingen starter med å først observere et fenomen og deretter generalisere om fenomenet som fører til teorier som kan falsifiseres eller valideres [9]. Vi presenterte problemstillingen for Østre Toten kommune gjennom en tidligere analyse av en preventiv beslutning i Gjøvik kommune, hvor vi den gang benyttet SBC-modellen i en sosioteknisk kontekst (se figur 1) kombinert med NIST sitt krisehåndteringsrammeverk (se figur 2) for å presentere informasjon og forslag til fremdrift i Østre Toten kommune. Vårt foreslåtte kombinasjonsrammeverk er presentert i figur 6.

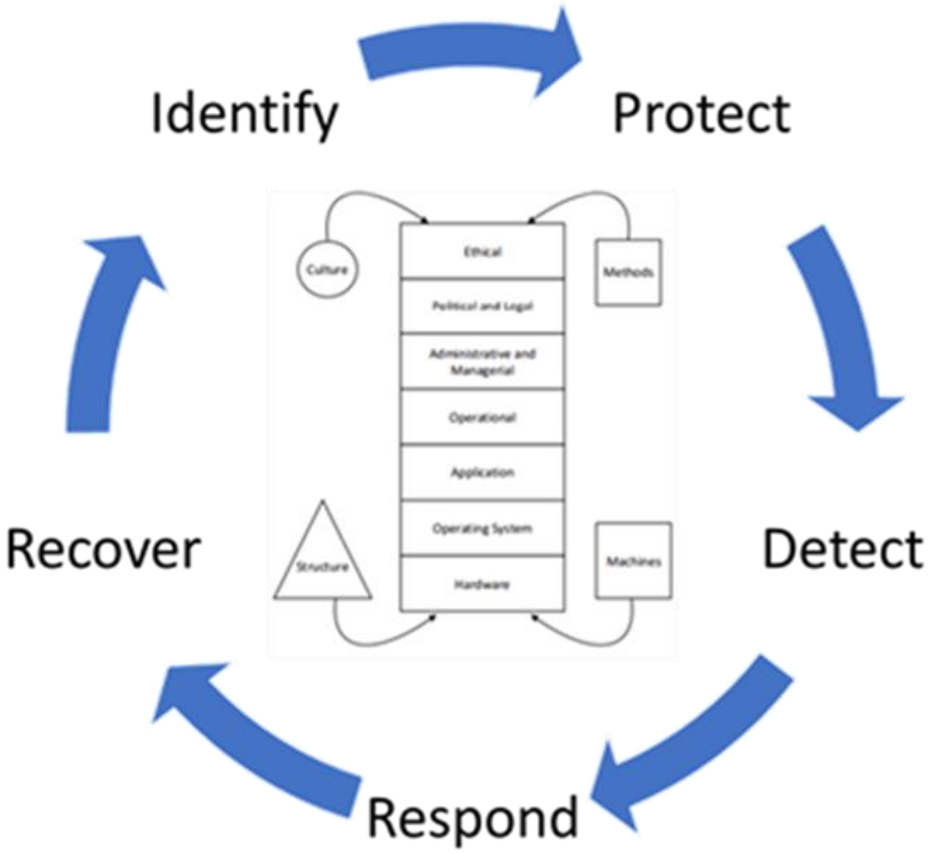


Fig. 6. Et sosio-teknisk og risiko-ledelses rotårsaksanalyse rammeverk [10]

Dette var dermed utgangspunktet for en deduktiv tilnærming i Østre Toten kommune, hvor spørreundersøkelsen var lagt opp til å undersøke hendelseshåndteringen ved å benytte disse rotårsaksmodellene i kombinasjon, samtidig som det ble gjennomført spørsmål knyttet opp mot krav i lovverk og nasjonale forskrifter og veiledere for beredskap [15], [16], [34], og avslutningsvis en modenhetsundersøkelse [29]. Noen av disse spørsmålene er overlappende, og trigget dermed spørsmål fra noen av deltakerne om dette. Fra vårt perspektiv har det vært viktig å nettopp se hvordan man kan kombinere ulike rammeverk (eksempelvis NIST [12], sosio-tekniske rammeverk [9], lovverk [15]), hva som i så tilfelle er overlappende, og hva som mangler i de ulike rammeverkene. De forskningsmessige resultatene fra dette vil som nevnt bli presentert i vitenskapelige artikler, samt i Østby sin doktorgradsavhandling samstemt med tidligere arbeid.

I tillegg til spørreundersøkelsen, så ble det gjennomført 9 dybdeintervjuer. Målsettingen med dybdeintervjuene var å få et bedre innblikk i læring i organisasjonen [18], [20], [21], [22], [23] som også andre kan lære av. Disse ble gjennomført i en semistrukturert form, med temaene 1) type involvering i hendelseshåndteringen, 2) kontaktpersoner i Østre-Toten kommune med fokus på eskalering og de-eskalering, 3) kontaktpersoner utenfor Østre-Toten, 4) hovedoppgaver i hendelseshåndteringen, 5) læring fra hendelsen, 6) anbefalinger til andre kommuner og andre organisasjoner, 7) anbefalinger til arbeidet med trening og øvelser, 8) roller i krisehåndtering av denne type kriser, og avslutningsvis 9) om det var tanker respondenten hadde forberedt og ønsket å formidle.

Utvalget av respondenter ble valgt med bakgrunn i tidligere arbeid i Østby sitt stipendiatprosjekt, for å få en oversikt over krisehåndteringen både på strategisk, taktisk og operativt nivå, og for dermed å kunne møte den deduktive tilnærmingen til dette arbeidet i form av utvikling og evaluering. Østby sitt tidligere arbeid er presentert i figur 7.

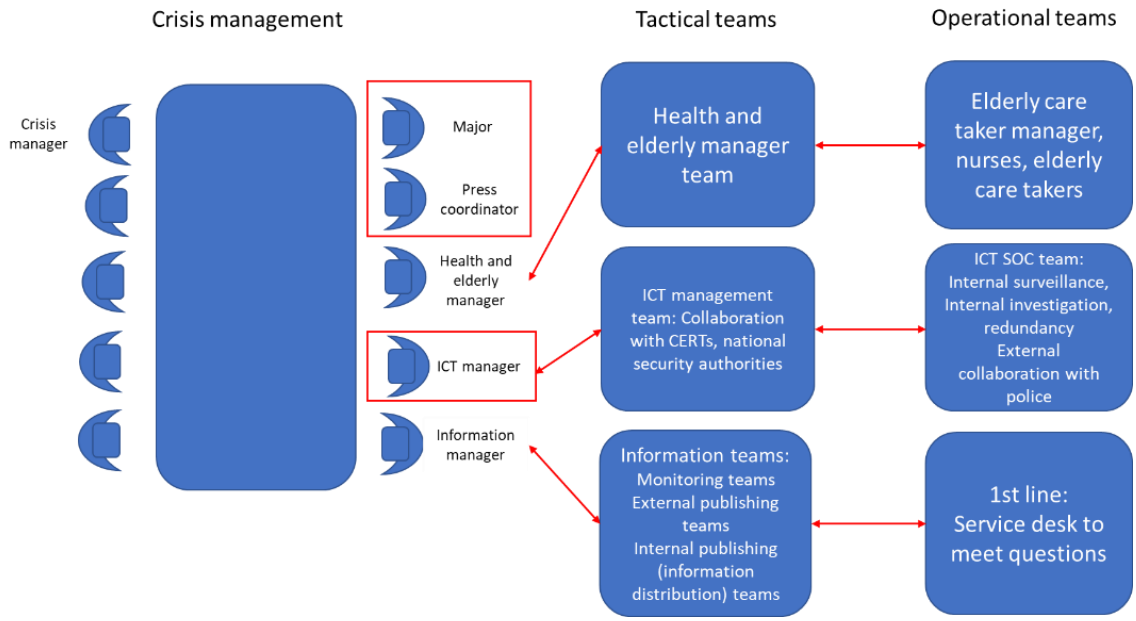


Fig. 7. Roller ved cyber-hendelser [35]

I tillegg ble det valgt respondenter fra utenfor organisasjonen for å vurdere informasjonsbehovet ut og inn av organisasjonen. Dette baserer seg også på Østby sitt arbeid fra samme artikkel [35], som er presentert i figur 8.

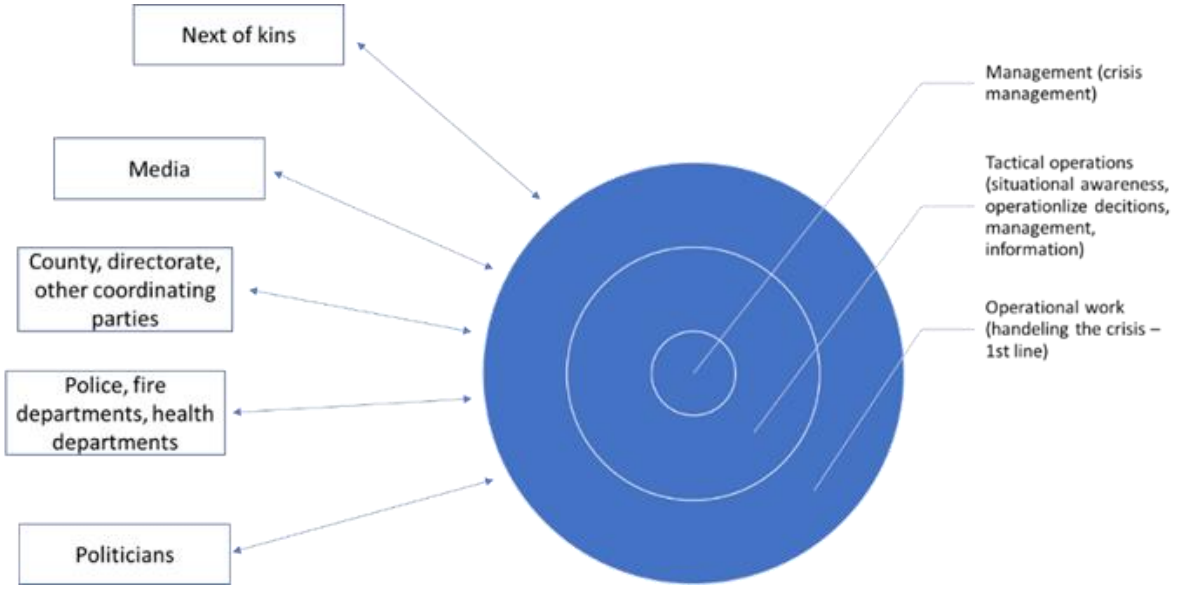


Fig. 8. Behov for informasjon i kriser [35]

Ved overgang fra vurdering av hendelseshåndteringen i seg selv, til dernest å vurdere hvordan man kan lære fra organisasjonen, ble det stilt åpne spørsmål i dybdeintervjuene, men også «naturlige» oppfølgingsspørsmål for å vurdere hvordan man kan bygge opp spillstab for øving [36] av de da endrede forutsetningene vi har sett.

Vurdering av resultatene (diskusjon)

Hovedfunnene i undersøkelsen kan som nevnt i sammendraget deles inn i 7 områder:

1) Cyber-angrep krever en egen plass på organisasjonens risiko- og sårbarhetsliste (kan ikke betraktes som strømbrudd eller ekom-feil).
2) Eksterne informasjonskrav er ekstraordinære, annerledes og mer krevende enn i en «normal» hendelse (f.eks. fra nasjonale sikkerhetsorganisasjoner, etterretningsorganisasjoner, CSIRT, databeskyttelsesmyndighet etc.).
3) Beredskapsplaner må inneholde plan for og kontrakt med et eksternt IKT-hendelseshåndterings- og gjenopprettingsteam (hvis slikt personell ikke er en del av organisasjonen).
4) I tillegg bør også beredskapsplaner ha et kapittel om hvordan man håndterer sensitive personopplysninger på avveie.
5) Intern kommunikasjon omkring prioritering og løpende oppfølging av uløste situasjoner er svært krevende, og over tid kortsluttes krisestyringslinjen.
6) Det bør gjennomføres trening og øving av cyber-angrep på lik linje med andre hendelser, og vi anbefaler at det stilles krav til offentlige beredskapsorganisasjoner om å gjennomføre denne type øvelser i nær framtid.
7) Krysskoordinering (regulert) fra lokal koordinering (Statsforvalter) og nasjonale myndigheter (Nasjonal sikkerhetsmyndighet) i slike angrep skaper til tider forvirring og usikkerhet.

Cyber-angrep som egen risiko og sårbarhetsvurdering

Det ble stilt spørsmål vedrørende gjennomføring av risiko og sårbarhetsvurdering både som en del av tekstbok-delen av undersøkelsen og også som en del av samfunnskravene (lover, forskrifter og veiledere) i undersøkelsen. Fra tekst-bok delen var det kun 4 som kjente til at det var gjort en risikovurdering av cyber-angrep før hendelsen, mens 24 svarte nei på dette. Av de 4 som kjente til at det var gjort en risikovurdering av cyber-angrep, svarte allikevel 1 at dette var utført på strategisk nivå, 1 at det var utført på taktisk nivå, mens 3 svarte at det var utført på operativt nivå. Fra samfunnskravsdelen og deri oppfølgingsspørsmål til de 12 som svarte ja om risiko- og sårbarhetsvurderingen ble gjennomgått ved siste revisjon av kommunedelplaner i henhold til Sivilbeskyttelsesloven §14, svarte 4 ja, 0 nei og 8 vet ikke. På spørsmål om cyber-angrep som hendelse var blitt vurdert i henhold til §14, svarte 1 ja, 4 nei og 7 vet ikke, og på spørsmål om cyber-angrep ble vurdert ved siste revisjon av kommunedelplaner svarte 1 ja, 3 nei, og 14 vet ikke. Det er altså 4 personer i begge delene av undersøkelsen som har hatt et forhold til risikovurderinger, og det kan synes som om at ja, det er gjennomført risikovurdering av cyber-angrep på operativt nivå, men at dette nødvendigvis ikke er knyttet opp mot lovhjemmelen med dertil oppfølging i revisjon av kommunedelplaner.

Hvorvidt en god helhetlig risiko-analyse av cyber-angrep ville medført et større fokus på tiltak og gode beredskapsplaner er jo uansett usikkert, spesielt med tanke på at man ikke før denne hendelsen hadde sett noe liknende med samme type konsekvenser i andre offentlige organisasjoner i Norge. Vi vet jo heller ikke om de 4 som har svart i begge delene av undersøkelsen her refererer til «modenhetsundersøkelsen» ATEA refererer til

(se vedlegg 2, side 44) eller risikovurderingen KPMG refererer til [37]. Sammenliknet med en sosio-teknisk tilnærming til risiko-vurdering, så dekker jo også en slik risikovurdering kun deler av hva som er anbefalt. Dette kan visualiseres som i figur 9.

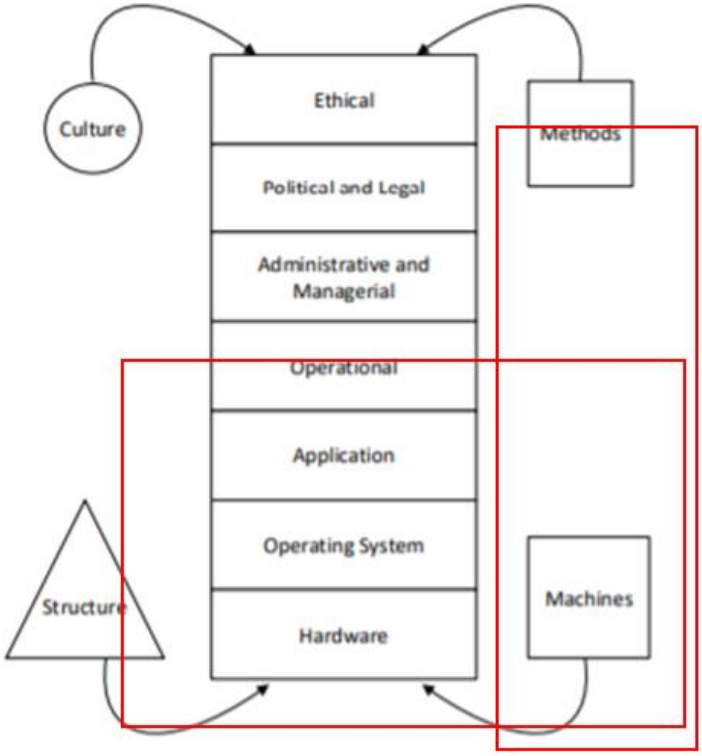


Fig. 9. Delvis risikoanalyse

Uansett så kan man basert på funnene si at det var liten kjennskap til risikovurdering av denne type hendelse. Konsekvensene av å ikke ha gjort en slik risikovurdering som både anbefales i tekstbøker for informasjonssikkerhet og er hjemlet ved nasjonale lover, forskrifter og veiledere har jo vært store, og som ordfører i kommunen peker på, så er det viktig også for folkevalgte å nå etterspørre rapporter på risikoarbeidet rundt cyber-angrep.

Informasjonskrav

Som nevnt i innledning- og bakgrunnskapittelet, så er informasjonsbehovet- og dertil trykk på organisasjonen noe annerledes enn i en vanlig hendelse. Dette kan presenteres ved en modifisert versjon av figur 8, her presentert i figur 10.

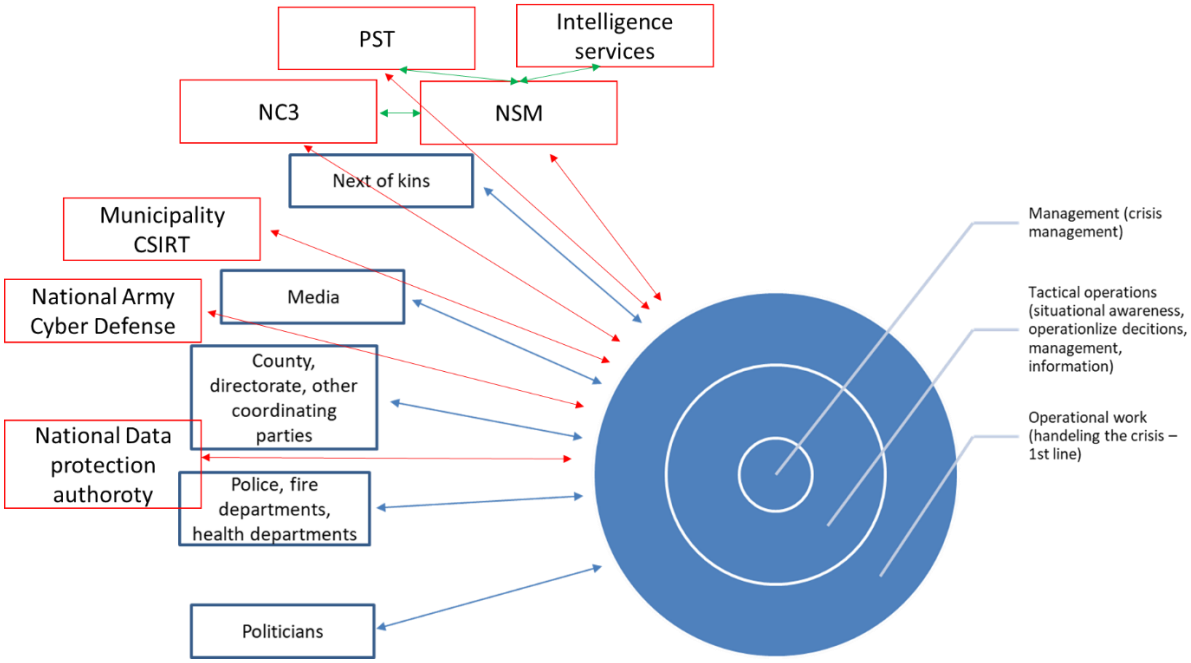


Fig. 10. Behov for informasjonsdeling ved cyber-angrep - modifisert [35]

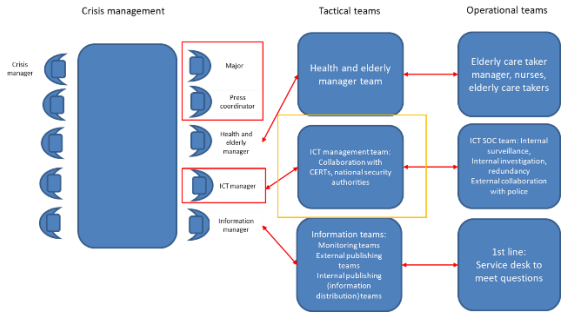
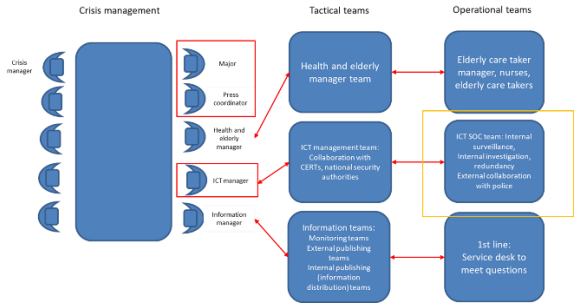
«Felles cyberkoordineringssenter (FCKS) består av NSM, Etterretningstjenesten, PST og Kripos (NC3), og ledes av NSM.» [13] Men selv om NSM har koordineringsansvaret, så var altså innsatsteamet i Østre Toten i dialog med flere av enhetene opptil flere ganger. I stor grad handlet dette om å gi fra seg informasjon, og lite falt tilbake til organisasjonen – før som kommunedirektøren nevner, at det måtte kreves å få innsyn i en rapport som var skrevet.

IKT-hendelseshåndterings- og gjenopprettingsteam

Umiddelbart ble ATEA som er hovedsamarbeidspartner for IKT-sikkerhet i Gjøvik-regionen innhentet for å hjelpe til med gjennopprettingsarbeidet. Prioritering ble gjort basert på liv og helse, og arbeidet ble satt i gang med hjelp av teamet fra ATEA. Prioriteringen ble oppdatert noe i begynnelsen, men det kommer klart frem fra intervjuene at det er denne prioriteringen alle har måttet forholde seg til. Og gjennom tilfeldighetenes spill (?) ble det gjennom en god rådgiver/kontaktperson i KS foreslått navngitte personer i KPMG som også kunne hjelpe til og gi råd om selve ledelsen av hendelseshåndteringen, deri dialog med NC3, NSM og andre, samt det operative arbeidet som gjelder etterforskning og gjenoppretting.

Opp mot den opprinnelige modellen som Østby og Katt [35] har foreslått for organisering av hendelseshåndtering av cyber-sikkerhetshendelser, med et taktisk og et operativt team, er det ikke store avvik i forhold til type arbeid, men noen forhold ble gjort annerledes i hendelseshåndteringen i Østre Toten, samt at opplevelsen av om det var taktisk arbeid eller operativt arbeid var flytende. Selv om IT-sjef i utgangspunktet var alene i kriseledelsen, ble det så snart IKT-innsatsleder kom på plass (onsdag etter hendelsen), også til at vedkommende deltok i kriseledelsen. Det var også slik at både for det første kriseledelse ved kommunedirektør, og for det andre taktisk ledelse ved IKT-innsatsleder, og også de operative teamene var i kontakt med hhv. politi og NC3. IKT-innsatsleder var i starten leder for begge oppgaver, men hadde altså to forskjellige

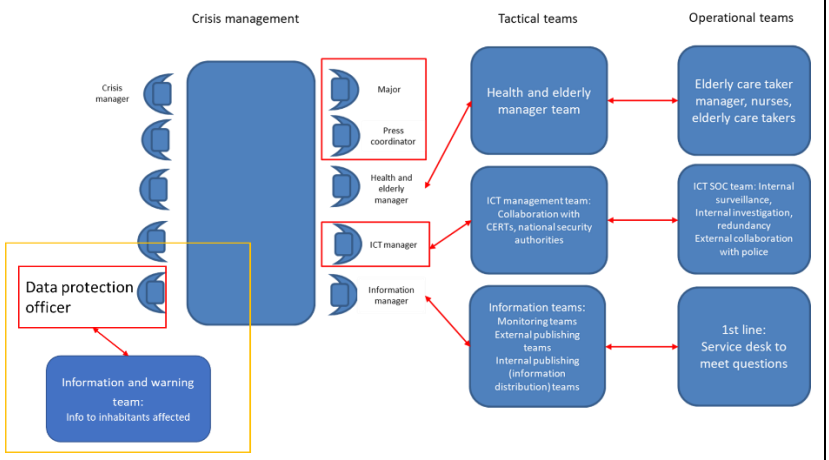
eksperter fra ATEA/KPMG til å støtte seg mot det ulike arbeidet i de to teamene. IKT-innsatsleder sluttet i sin stilling i Østre Toten i løpet av mai 2021.

Taktisk team: IKT-innsatsleder (frem til juni 2021) Innleid ressurs fra Accenture (fra juni 2021) Rådgiver fra KPMG IT-sjef (ble borte fra teamet når han ble flyttet til IKOMM) Økonomisjef	
Operativ team: Også IKT-innsatsleder (frem til juni 2021) Gjenopprettingsansvarlig (fra juni 2021) Sikkerhetseksperter fra først ATEA deretter KPMG ➔ Gjenopprettelseseksperter ➔ Etterretningseksperter	

Det som er viktig å få med seg, er at Østre Toten ikke var rustet med personell for å dekke dette arbeidet, hverken på taktisk eller operativt nivå. For Østre Toten og andre organisasjoner er det dermed viktig å kunne forberede for å få på plass slike team i en tilsvarende krise. Om disse er interne eller eksterne bør være opp til den enkelte organisasjon, men det bør gjøres avtaler og opprettes varslingslister/navnelister for beredskapsplanverket.

Varslingsteam sensitive personopplysninger på avveie

Da hendelsen eskalerte med at sensitive personopplysninger ble lagt ut på det mørke nettet, ble også personvernombud hentet inn i kriseledelsen. For å håndtere informasjonsutveksling med berørte (evt. pårørende) ble det opprettet et varslingsteam:

Varslingsteam Personvernombud En person fra voksenopplæringen En person som tidligere hadde ledet psykososialt kriseteam i Østre Toten med helsefaglig bakgrunn En kommunikasjonsrådgiver Juridisk hjelp fra KPMG	

Man vet jo ikke nødvendigvis om dette er de eksakt rette personene for en annen organisasjon, men det bør allikevel ligge i beredskapsplanen en beskrivelse av oppgaver, samt en varslingsliste med nødvendige ressurser. Oppgavene som ble utført er godt beskrevet i resultatene fra intervju med personvernombud.

Intern kommunikasjon – brudd i kriselinje (?)

Over tid viste det seg at kriselinjen med styring fra kriseledelsen skapte tretthet i organisasjonen. Dette gjaldt spesielt på taktisk nivå, hvor vi erfarer at skolesjef og økonomisjef beskriver dette på en god måte. Når det hadde gått en tid, og trettheten i organisasjonen oppsto fordi man ikke fikk løst oppgavene sine og fortsatt brukte private telefoner og annet for å løse oppdrag, mistet man i noen grad lojaliteten til krislinjene. Det ble derfor da en lettelse for eksempelvis skolen når man kunne ha direkte kontakt med gjenopprettingsansvarlig i det operative innsatsteamet. Den observante leser vil jo da ha sett at her ble det en form for brudd i krisehåndteringslinjen, samtidig som det ble høyere press på det operative IKT-innsatslederteamet (se figur 11). Men, dette ga samtidig en optimisme ute i organisasjonen. Det skal allikevel sies at det operative teamet under ledelse av gjenopprettingsansvarlig hadde klare føringer/prioriteringer fra kriseledelsen.

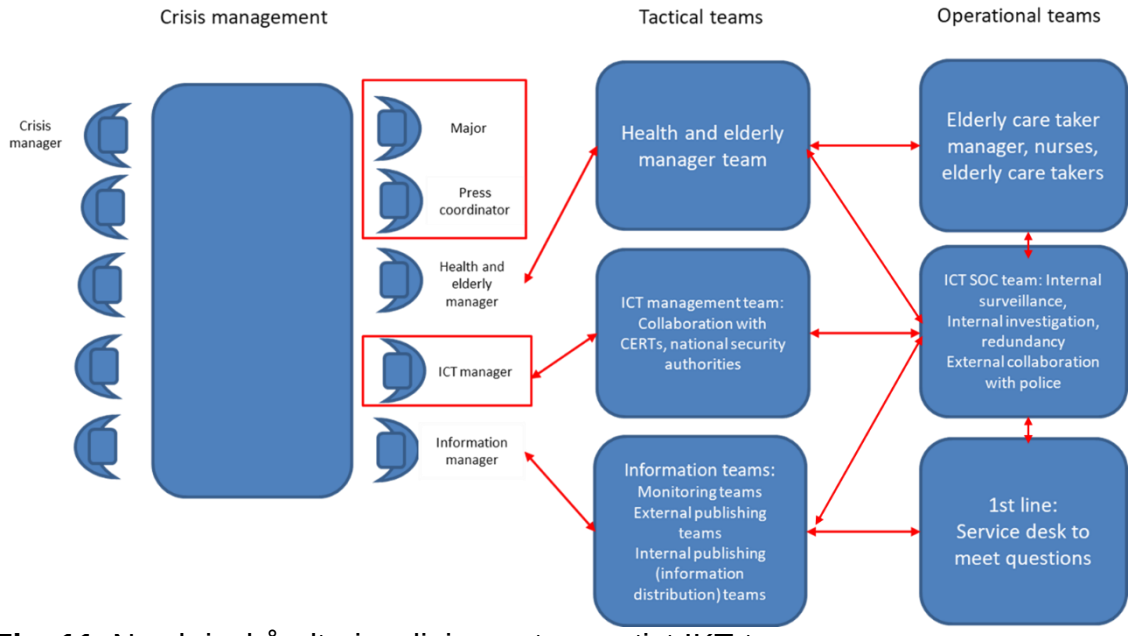


Fig. 11. Nye krisehåndteringslinjer mot operativt IKT-team

Hvorvidt dette er en god løsning må den enkelte organisasjon ta stilling til, og også vurdere ressurser i forhold til, men man bør vurdere presset på det operative IKT-teamet i hendelsesforløpet når dette på et tidspunkt skjer. I tillegg bør det da være enighet og tillit til at dette kan fungere godt for hele organisasjonen. Det som da også er viktig er at kontaktpersonene i gjenopprettingsteamet kjenner prioriteringen til ledelsen.

Trening og øving

I spørreundersøkelsen kom det klart frem at de fleste ikke kjente til om organisasjonen hadde et sikkerhetsprogram. Et sikkerhetsprogram var beskrevet som at «det består av en organisasjonsplan med dertil oppgaver/funksjoner som det er behov for, sertifiseringsprogram, utdanning, trening, øvelser m.m.» Hele 25 svarte negativt på dette, mens 3 svarte positivt.

I intervjuene var det allikevel stor enighet om at slike hendelser må trenes og øves på. Under spørsmål om hva de hadde lært gjennom hendelsen, ble det allikevel gjerne litt stille, og det var ikke like enkelt å analysere hva organisasjonen har lært av hendelsen. Når det ble spurt litt mer konkret om beredskapsplaner, så kom det imidlertid tydeligere frem noen forhold, deri forståelsen av hva et cyber-angrep innebærer med dertil konsekvenser i organisasjonen som må håndteres.

Et eksempel er ved sykehjemmet, hvor de hadde planer for bortfall av strøm, og dermed hadde et døgn gammel liste med oversikt over pasienter og hvilke medisiner de enkelte skulle ha. Men, for å komme seg inn i medisinskapet skulle de egentlig benyttet en kortløsning, som da ikke lenger var aktivt. Andre systemer som var ute av drift var også varsling/alarm hos den enkelte beboer, noe som medførte at beboere måtte ta i bruk bjeller. Denne type eksempler vil være gjeldende også for andre organisasjoner, og kan enkelt skrives inn i scenarioer for øvelser [11].

I tillegg må man etter å ha vurdert hvilket modenhetsnivå den enkelte organisasjon er på sette opp trening og øvelser tilpasset nivået, for deretter å sette inn sosio-tekniske tiltak

for å dekke et skritt av gangen [38]. Dette kan visualiseres som en prosess, slik som presentert i figur 12.

Fig. 12. Modenhets forbedringsprosess [38]

Er modenheten generelt på et lavt nivå, så kan det være aktuelt å starte med enkle seminarer/opplæring eller diskusjonsøvelser, mens man ved et høyt modenhetsnivå gjerne kan arrangere funksjonsøvelser og fullskalaøvelser. Ulike type øvelser for slik trening er presentert i figur 13 [39], og det er også gode veiledere for øvelser hos Direktoratet for samfunnssikkerhet og beredskap (DSB) [40] og hos The European Union Agency for Cybersecurity (ENISA) [41].

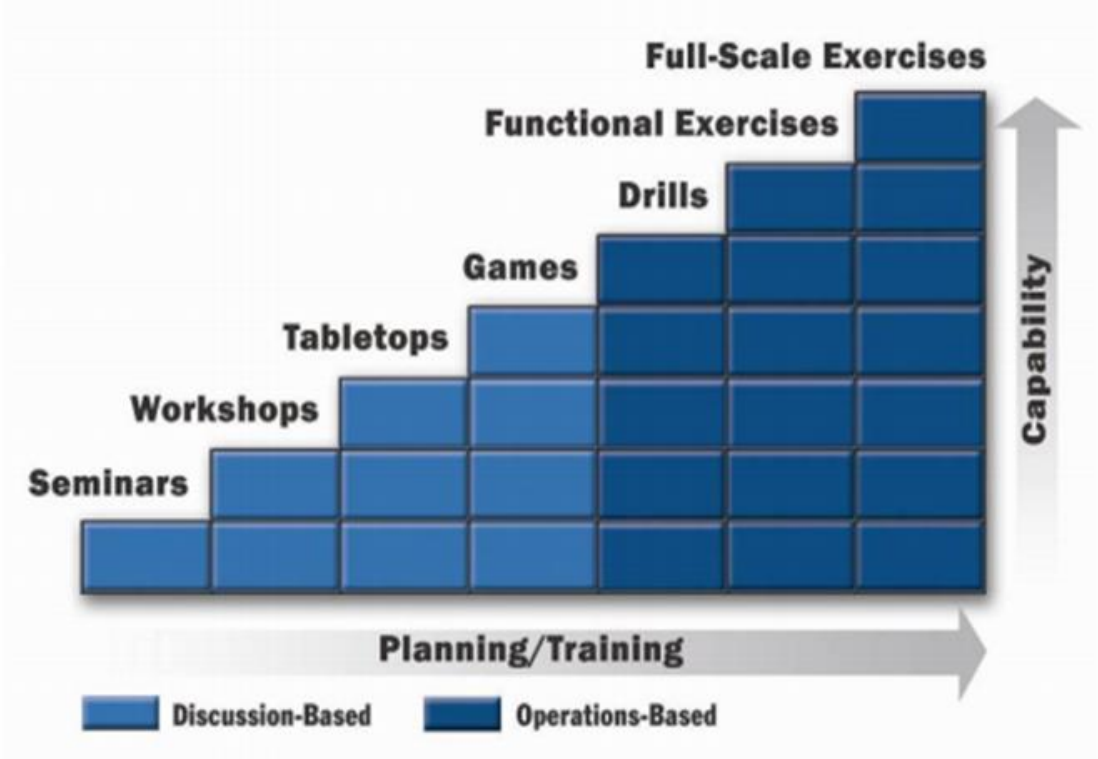


Fig. 13. Ulike type øvelser [39]

Det kan altså være lurt å starte på det laveste nivået dersom modenheten er lav, og vi anbefaler gjerne å starte med diskusjonsøvelser slik som presentert på ovelse.no. Dette er diskusjonsøvelser innenfor kjente temaer av informasjonssikkerhet, med noen gode diskusjonsspørsmål og gode råd. Disse øvelsene er planlagt for å ha en øvingsleder, med dertil egen informasjon til vedkommende, slik at det skal være mulig å forberede seg til øvelsene på en god måte.

Når det gjelder mer avanserte øvelser som funksjonsøvelser og fullskalaøvelser for organisasjoner, så anbefaler vi å forberede øvelser gjennom å skaffe seg god kunnskap om organisasjonen som skal øves [28], for deretter å lage et godt øvingsdirektiv med øvingsmål og scenario nettopp basert på nivået i organisasjonen. For gjennomføring av øvelsen foreslår vi å tilpasse en spillstab til den organisasjonen som skal øves, slik som presentert i figur 14 og figur 15, visualisert med farger i forhold til hvordan teamene bør bygges opp i spillstab.

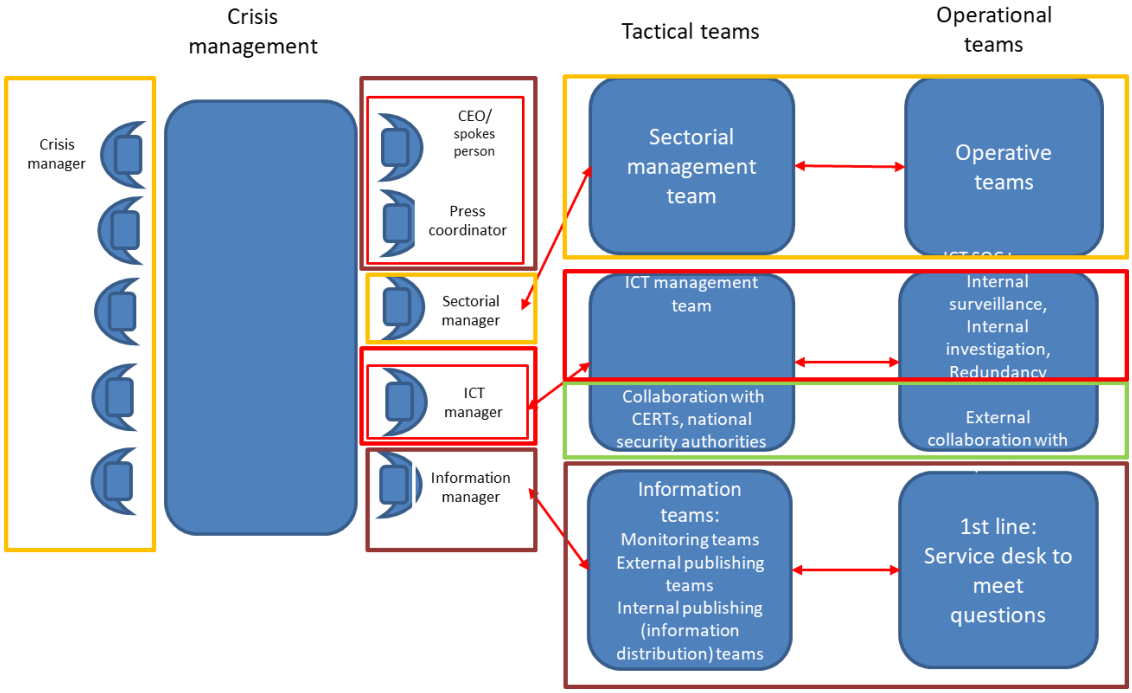


Fig. 14. Hvem skal trenes? [36]

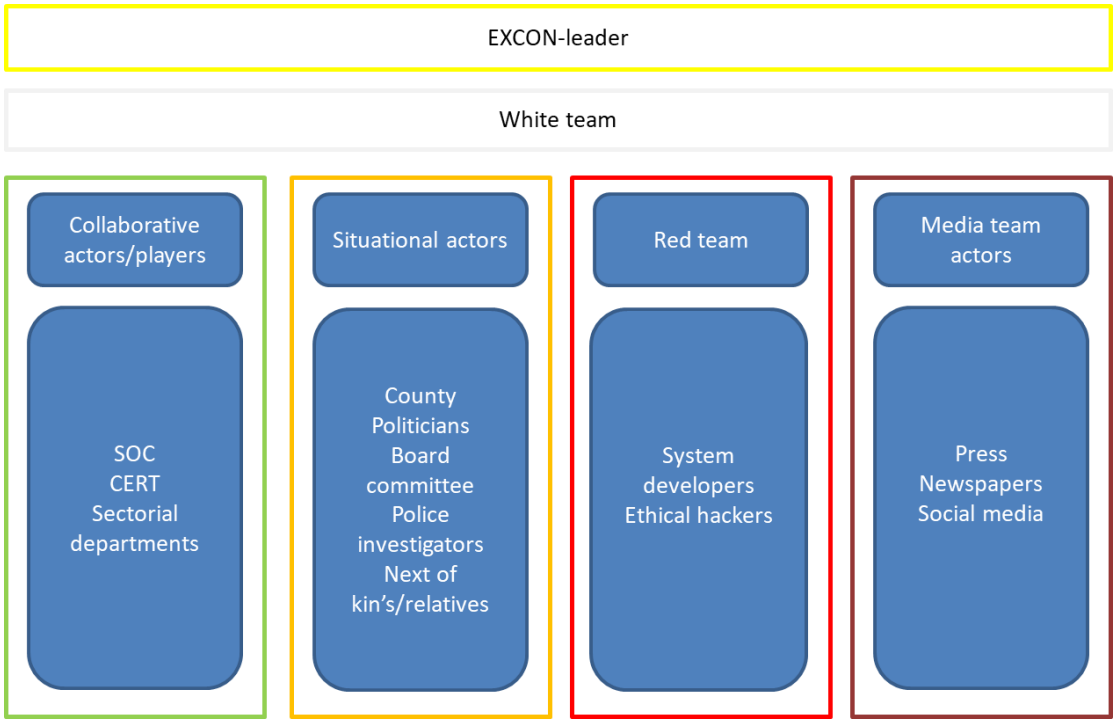


Fig. 15. Spillstab for øving av de som skal trenes [36]

Dette må selvfølgelig bygges opp basert på hva slags organisasjon som skal øves og hva slags øvelse som skal gjennomføres.

Slike øvelser kan koordineres (i henhold til mandater) av Statsforvalter og NSM i samarbeid med ulike cyber-range miljøer, eksempelvis Norwegian Cyber Range/NTNU på Gjøvik.

Krysskoordinering

Krysskoordinering (regulert) fra lokal koordinering (Statsforvalter) og nasjonale myndigheter (Nasjonal sikkerhetsmyndighet) i slike angrep kan til tider skape forvirring og usikkerhet. Som vi ser av intervjuene var Statsforvalter inne i kriseledelsen, men hadde lite å gjøre med de taktiske og operative IKT-teamene. NSM og andre fra Felles cyberkoordineringssenter var i liten grad i dialog med kriseledelsen (noe var det, men ikke mye), men de var ved flere anledninger i kontakt med IKT-teamene både på taktisk og operativt nivå. At NSM sørget for at øvrige aktører ved Felles cyberkoordineringssenter kom i kontakt med «de rette menneskene» i Østre Toten for å få den informasjonen de trengte ble nok gjennomført etter beste evne, men det er mulig NSM burde hatt noe mer dialog med kriseledelsen, slik at kriseledelsen kunne fått muligheten til å delta i prioriteringen av informasjonskravene. I så måte kunne man også sett på muligheter for bedre dialog for prioritering mellom Statsforvalter og NSM. Er det konsekvensene for befolkningen eller informasjonskravene som skal prioriteres? Med andre ord de litt mer overordnede sosio-tekniske faktorene for organisasjonen, 1) Struktur, 2) Kultur, 3) Metoder og 4) Maskiner (se figur 9).

Kort oppsummering og fremtidige vurderinger

Denne rapporten er laget for å gi organisasjonen i seg selv og andre organisasjoner læring. Samtidig vil erfaringene fra hendelsen kunne knyttes opp mot undervisning og øvelser. Rapporten beskriver situasjonen som den er, og hvordan man bør forberede seg dersom tilsvarende skulle skje i egen organisasjon.

Rapporten omfatter imidlertid ikke samfunnsperspektivet, deri den spente situasjonen mellom øst og vest, det at alle systemer er knyttet opp mot alt, teknologisk determinisme med dertil utmattelse i organisasjonene (da også ved sikkerhetshendelser som denne), og ei heller noen form for motstridende tenking når det gjelder å sette seg inn i hvordan en nasjon gjennom hackergrupper kan eksempelvis sette viktige funksjoner i samfunnet ut av spill. Denne gangen var det en kommune som ble angrepet, hva om det samme skulle skje mot flere samfunnskritiske funksjoner samtidig? Å dra nytte av erfaringene fra denne hendelsen og finne synergier inn i scenarioer på regionalt og nasjonalt nivå vil også være en del av det framtidige arbeidet med opplæring, trening og øvelser.

Referanser

[1] nettvett.no, “Løsepengevirus,” *nettvett.no*, 2021. [Online]. Available: https://nettvett.no/losepengevirus/.

[2] Justis og beredskapsdepartementet, *Instruks for statsforvalteren og Sysselmesteren på Svalbard sitt arbeid med samfunnssikkerhet, beredskap og krisehåndtering*. 2015.

[3] J. Gilbrandt and M. Rønning, “Omfattende IT-angrep mot Stortinget,” *dagbladet.no*, 2020.

[4] Nortura, “– Konsekvensene ble mindre enn de kunne blitt,” *Nortura Medlem*, 2022.

[5] N. Rydne, “Slik håndterte Nordic Choice dataangrepet: – Det har vært tøft,” *E24*, 2022.

[6] A. Krantz, M. F. Børresen, T. I. Hagen, and A.-K. Mo, “Dataangrepet: Kan skade korona-beredskapen,” *nrk.no*, 02-Sep-2020.

[7] Cisco, “Annual cyber security report,” 2018.

[8] Næringslivets sikkerhetsråd, “Mørketallsundersøkelsen 2020,” 2020.

[9] S. Kowalski, “IT Insecurity: A Multi-disiplinary Inquiry,” Stockholm University, 1994.

[10] G. Østby and S. J. Kowalski, “A case study of a municipality phishing attack measures - towards a socio-technical incident management framework,” *CEUR*, 2021.

[11] G. ; Østby, L. ; Berg, M. ; Kianpour, B. ; Katt, and S. Kowalski, “A Socio-Technical Framework to Improve cyber security training: A Work in Progress,” 2019.

[12] K. Scarfone, T. Grance, and K. Masone, “Computer Security Incident Handling Guide,” 2008.

[13] Nasjonal Sikkerhetsmyndighet, “Rammeverk for håndtering av IKT-sikkerhetshendelser,” pp. 1–20, 2017.

[14] NSR, *Nødplakat for digitale angrep*. 2022, p. 2022.

[15] Justis- og beredskapsdepartementet, “Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret (sivilbeskyttelsesloven).” Norwegian Government, 2010.

[16] Norwegian government, *FOR-2011-08-22-894*. Norwegian Government, 2011.

[17] DSB, *Municipality guidance, emergency duty*. 2017.

[18] E. Deverell, *Crisis-induced learning in public sector organizations*. 2010.

[19] A. L. Fimreite, P. Lango, P. Lægreid, and L. H. Rykkja, *Organisering, krisehåndtering og samfunnssikkerhet*. NO: Universitetsforlaget, 2014.

[20] J. Birkinshaw, “Making sense of knowledge management,” *Ivey Bus. J.*, vol. 65, no. 4, 2001.

[21] B. Mishra and A. U. Bhaskar, “Knowledge management process in two learning organisations,” *J. Knowl. Manag.*, vol. 15, no. 2, pp. 344–359, 2010.

[22] M. Easterby-Smith, M. Crossan, and D. Nicoliny, “ORGANIZATIONAL LEARNING: DEBATES PAST,PRESENT AND FUTURE,” *J. Manag. Stud.*, vol. 37, no. 6, 2000.

[23] D. A. Schon, “Deutero learning in organizations: Learning for increased effectiveness,” *Organ. Dyn.*, vol. 4, no. 1, pp. 2–16, 1975.

[24] R. A. Myer, C. Conte, and S. E. Peterson, “Human impact issues for crisis management in organizations,” *Disaster Prev. Manag. An Int. J.*, vol. 16, no. 5, pp. 761–770, 2007.

[25] D. West-Brown, Moira J. Stikvoort, G. Killcrece, R. Reufle, and M. Zajicek, *Handbook for Computer Security Incident Response Teams (CSIRTs)*, 2nd ed. Carnegie Mellon Software Engineering Institute, 2003.

[26] G. Parmigiani and L. Inoue, *Decision Theory: Principles and Approaches*. UK: John Wiley & Sons, 2009.

[27] S. Kowalski, T. Grunnan, and M. Maal, *A socio-technical model of a post disaster and crisis management learning process.* 2014.

[28] G. Østby and S. J. Kowalski, “Preparing for Cyber Crisis Management Exercises,” in *n: Schmorrow D., Fidopiastis C. (eds) Augmented Cognition. Human Cognition and Behavior.*

HCII 2020. Lecture Notes in Computer Science, vol 12197., 2020, pp. 279–290.
[29] G. Wahlgren and S. Kowalski, "A Maturity Model for IT-Related Security Incident Management," in *Business information systems*, Springer, Cham, 2019.
[30] G. Wahlgren and S. Kowalski, "IT Security Risk Management Model for Cloud Computing," *Int. J. E-entrepreneursh. Innov.*, vol. 4, no. 4, pp. 1–19, May 2014.
[31] H. W. L. Sweet, R. K. Edwards, G. R. Lacroix, M. F. Owens, and H. P. Schulz, "A Method for Assessing the Software Engineering Capability of Contractors," 1987.
[32] W. Kuechler and V. Vaishnavi, "A Framework for Theory Development in Design Science Research: Multiple Perspectives," 2012.
[33] G. R. Karokola, "A framework for Securing a-Government Services, The case of Tanzania," Stockholm University, 2012.
[34] DSB, *Veileder til forskrift om kommunal beredskapsplikt*. DSB, 2018.
[35] G. Østby and B. Katt, "Cyber Crisis Management Roles – A Municipality Responsibility Case Study," in *Science and Technology in Disaster Risk Reduction in Asia*, 2019, pp. 168–181.
[36] G. Østby, K. N. Lovell, and B. Katt, "EXCON teams in cyber security training," *Proc. - 6th Annu. Conf. Comput. Sci. Comput. Intell. CSCI 2019*, pp. 14–19, 2019.
[37] KPMG, "IKT-sikkerhet i Østre Toten kommune forut for Sammendrag," 2021.
[38] G. Østby, S. J. Kowalski, and B. Katt, "Towards a Maturity Improvement Process – Systemically Closing the Socio-Technical Gap," in *6th International Workshop on Socio-Technical Perspective in IS Development - STPIS*, 2020, pp. 195–205.
[39] HSEEP, "Homeland Security Exercise and Evaluation Program Volume 1: HSEEP Overview and Exercise Program Management," 2006.
[40] DSB, *VEILEDER I PLANLEGGING, GJENNOMFØRING OG EVALUERING AV ØVELSER Metodehefte: Fullskalaøvelse*. 2016.
[41] ENISA, "Good Practice Guide on National Exercises," p. 80, 2009.
[42] M. E. Whitman and H. J. Mattord, *Management of Information Security*. Cengage, 2018.

Vedlegg 1 - Mandat

I forbindelse med alle type hendelser som er av betydning, anmoder Statsforvalteren i det gitte området om å evaluere hendelser basert på sin instruks (forskrift) [2]. I Østre Toten sitt tilfelle ble det også tildelt skjønnsmidler fra Statsforvalteren, slik at ansatte skulle kunne frigjøres til å delta i evalueringen. Mandatet er her gjengitt i sin helhet:

Nylige undersøkelser blant norske organisasjoner viser en økning i antall informasjons- og cybersikkerhetshendeleser, og ingenting tilsier at dette vil avta. Hendelser som cyber-angrepene mot Østre Toten kommune har satt en støkker i mange av oss, og mange sitter nå og lurer på hvordan sin egen organisasjon skal kunne håndtere denne type hendelser. Vi påstår at med hjelp av formidling av kunnskap i form av skolering, trening og øvelser, vil andre organisasjoner kunne dra nytte av det som har skjedd.

Ved NTNU sin Norwegian Cyber Range har de pågående et forskningsprosjekt omkring nettopp håndtering av slike hendelser. Kriselederansvaret i en kommune (og i andre offentlige organisasjoner) er jo fortsatt like klart som det alltid har vært gjennom lover og forskrifter, men de naturlige instansene for hjelp og støtte man finner i en «vanlig» hendelse er ikke nødvendigvis de samme som ved en informasjons- og cybersikkerhetshendelse. For eksempel kommer Politiets sikkerhetstjeneste (PST) og Nasjonal sikkerhetsmyndighet (NSM) raskt på banen, da et cyber-angrep ikke nødvendigvis er lokalisert bare til kommunen det gjelder. I tillegg er det jo ikke bare system-sikkerhetshendelsen som skal håndteres, men også konsekvensene av angrepet - de øvrige hendelsene som oppstår. Eksempelvis i Østre Toten ble det som kjent i tillegg helt egne kriser i både skole, på aldershjem, i forhold til innkreving av avgifter, personopplysninger på avveie, mangel på tilgang til personinformasjon på NAV med mer.

Ved NTNU er det allerede publisert artikler om forskjellen i en slik hendelse sammenliknet med andre hendelser, og om hvilke ansvarlige aktører i samfunnet det er naturlig å knytte til hendelsen. Samtidig er det viktig å analysere hendelser som i Østre Toten for å se om prosjektets antakelser holder mål eller ikke, og for ikke minst å kunne gjøre endringer og forslag til en mest mulig optimal hendelseshåndtering i slike saker.

Målsettingen med evaluering av cyber-sikkerhetshendelsen i Østre Toten er å lære internt i kommunen av det som har oppstått, men også at andre skal kunne lære av hendelsen. Rammene for evalueringen av cybersikkerhetshendelsen skal utøves i en slik form at erfaringer og tilegnet kunnskap skal kunne benyttes i undervisning, trening og øvelser. Forskerne ved Norwegian Cyber Range forsøker nå å få oversikt over hva slags type aktuelle øvelser som eksisterer, og da spesielt innenfor lederansvar ved informasjons- og cybersikkerhetshendelser i offentlige beredskapsorganisasjoner. I et litteratursøk i forskningsdatabaser, alle høyt rangert innenfor informasjonssikkerhet, fant NTNU svært få resultater på øvelser innenfor ledelse av denne type hendelser. Kun 19 relevante akademiske artikler ble funnet, hvor ingen egentlig omfavnet alt i et slikt lederansvar som ligger i offentlige beredskapsorganisasjoner. Det var imidlertid viktige fragmenter i disse nevnte øvelsene som det blir viktig å ta med seg når øvelsene skal utvikles i tiden som kommer. Med andre ord er det skrevet

forskningsartikler basert på evalueringer om tilsvarende hendelser, men svært lite forskningsartikler er skrevet om hvordan man kan tilrettelegge for krisehåndtering fra et samfunnsmessig kriselederperspektiv, samt hvordan man best kan øve på slike hendelser for å være forberedt når de oppstår. Dermed ser kommunen det som viktig at ledelsen for evaluering av krisehåndteringen gis til NTNU Institutt for informasjonssikkerhet og kommunikasjonsteknologi ved forskere som spesialiserer seg innenfor dette feltet.
Evalueringen skal ta for seg hendelseshåndteringen av dataangrepet. KPMG har utarbeidet en rapport om datasikkerheten forut for hendelsen. Rapporten ligger på kommunens hjemmeside, her.

Kriseledelsen gir oppdrag til en evalueringsgruppe

Kommunens kontaktpunkt vil være kommunedirektør, men evalueringen vil i sin helhet bli ledet av NTNU.

Prosjektleder vil være Grethe Østby[2], PhD stipendiat ved NTNU Gjøvik, Institutt for Informasjonssikkerhet og kommunikasjonsteknologi. Grethe er under veiledning av Stewart James Kowalski [3], professor i Informasjonssikkerhet som jobber ved samme institutt.

Statsforvalteren i Innlandet og Statsforvalteren i Nordland vil delta som observatører. Ekstern kompetanse som har et bidrag ved denne type hendelser kan brukes, og de som hadde en rolle i hendelseshåndteringen vil delta i evalueringen (Statsforvalter, Kommune CSIRT, KS, politiet, NSM, PST, ekspertgrupper m.fl.):
Arbeidet skal:

- *Få fram vesentlige læringspunkt fra hendelsen som kan gi grunnlag for å foreslå tiltak som kan styrke kommunens og andre kommuners kompetanse i håndtering av cybersikkerhetshendelser.*
- *Kartlegge håndtering av IKT-sikkerhetshendelsen hos Østre Toten kommune og vurdere hvordan håndteringen ble utført med utgangspunkt i lovverk og forskrifter:*
    - *Krav til risiko- og sårbarhetsanalyse i §3 i forskrift om krav til beredskapsplanlegging og beredskapsarbeid m.v. etter lov om helsemessig og sosial beredskap. Se også krav om forebyggende og skadebegrensende tiltak for å følge opp §4 og §9 i samme forskrift. De omhandler sikring av tilstrekkelig produksjon av tjenester ved mulige hendelser knyttet til avdekket risiko og sårbarhet.*
    - *Forskrift om kommunal beredskapsplikt: https://lovdata.no/dokument/SF/forskrift/2011-08-22-894*
    - *Personvern (GDPR)*
- *Kartlegge hendelsesforløp og involverte aktører*
- *Evalueringen skal omfatte krisehåndteringen, og foreslåtte sosio-tekniske metoder for rotårsaksanalyser av hendelseshåndtering ved informasjons- og cybersikkerhetshendelser skal ligge til grunn for evalueringen.*
- *I og med evalueringsarbeidet skal kunne brukes i forskning, så skal mandatet godkjennes ved Norsk senter for datasikring, og alle som tar del i undersøkelsen*

[2] https://www.ntnu.no/ansatte/grethe.ostby
[3] https://www.ntnu.no/ansatte/stewart.kowalski

i form av spørreundersøkelser og intervjuer vil få et informasjonsskriv om forskningsaktiviteten i evalueringen, samt et samtykkeskjema de må signere på.

- *KPMG har vurdert IKT sikkerheten i Østre Toten kommune forut for hendelsen. En skal vurdere om det er behov for ytterligere vurderinger av hvor godt forberedt kommunen var for å forhindre og oppdage angrep.*

Evalueringsrapporten skal utformes slik at den blir ugradert, med eventuelle graderte vedlegg dersom dette er et behov.

Spørsmål som skal vurderes:

1. *Hvilke aktører ble involvert i krisehåndteringen og hvordan ble den utført.*
2. *Bruk av beredskapsplaner, både generelle beredskapsplaner og spesielle innenfor informasjonssikkerhet (slik som kontinuitetsplaner), må vurderes opp mot faktisk hendelseshåndtering. Dette gjelder da også opp mot hjelpeaktører slik som Statsforvalteren, kommune CSIRT, NSM, PST etc.*

«Hvilke mekanismer som utløses i forbindelse med håndtering av en hendelse kan derfor variere stort, og det kan være utfordrende for alle involverte å arbeide og samvirke optimalt når kompleksiteten og usikkerheten ved en hendelse er betydelig. Av den grunn er evaluering og læring etter større hendelser et nyttig virkemiddel for å bli bedre forberedt på framtidige hendelser (FFI-rapport s. 9)»

Avgrensing

Evalueringsrapporten vil omhandle krisehåndteringen. D.v.s. ikke tekniske innstillinger på servere eller tekniske tiltak underveis. Imidlertid vil det være aktuelt å ta med hvilke beslutninger som ble tatt, hvem som tok disse, og ikke minst i samarbeid med hvem. Håndtering av IKT-sikkerhetshendelser omfatter forhold på ulike nivåer i organisasjonen. Det dreier seg om sikkerhetstekniske undersøkelser, metoder som benyttes i organisasjonen, struktur (kriseledelse, kommunikasjonslinjer etc.) og kultur i organisasjonen.

Metode

Metoden som vil benyttes er en kombinasjon av evaluering av hendelseshåndtering og sosio-teknisk analyse som beskrevet i fotnote[4]. I forkant av evalueringen vil Grethe gjennomføre en innføring i de to nevnte dokumentene som er vedlagt i dette mandatet. Informasjonsinnsamling: Dokumenter, logger, intervjuer og spørreskjema.

Framdrift

Evalueringen vil starte så snart mandatet er gitt, og søknad fra Norsk senter for forskningsdata (NSD) (for å få lov til å oppbevare data fra intervjuer etc. i perioden man analyserer disse). Normalt sett tar det ca. 3 uker for å få en godkjenning fra NSD.

[4] G. Østby and S. J. Kowalski, "A case study of a municipality phishing attack measures - towards a socio-technical incident management framework," *CEUR*, 2021.

I løpet av perioden 13.01.2022 (dato for innsending av materiell til Norsk senter for datasikring (NSD)) – 01.05.2022 ble det gjennomført en større spørreundersøkelse samt 9 dybdeintervjuer for å dekke intensjonen i mandatet. I dialog med NSD hvor rammene for undersøkelsen ble godkjent, ble det i første omgang besluttet å avvente bruk av logger, da dette ville kreve helt andre rammebetingelser for gjennomføringen. Da hovedmålsettingen var at kommunen i seg selv, samt andre kommuner og organisasjoner skulle få læringsutbytte av hendelseshåndteringen med dertil forslag til tiltak for tilrettelegging for hendelseshåndering ved IKT-sikkerhetshendelser, har vi underveis sett at innhentet data i stor grad dekker intensjonen i mandatet.

Vedlegg 2 - Resultater

Som en del av prosessen fikk vi en oversikt over totalt N=63 personer som hadde vært involvert i hendelseshåndteringen i større eller mindre grad. Av disse var N=31 ansatt i kommunen på tidspunktet hendelsen oppsto, mens øvrige var eksterne i form av myndigheter eller eksperter. Av de N=63 personene som sto på listen, aksepterte totalt n=38 å delta i forskningsprosjektet, hvor 25 av disse var ansatt i kommunen på tidspunktet hendelsen oppsto, mens øvrige altså var eksterne.

Av de n=38 som aksepterte å delta i forskningsprosjektet, svarte x=28 på hele spørreundersøkelsen og y=9 deltok i dybdeintervjuer. Av de x=28 som svarte på spørreundersøkelsen, så var 18 ansatt i kommunen på tidspunktet hendelsen skjedde, mens 10 var eksterne. Av de y=9 som deltok på dybdeintervjuer, var 7 internt ansatte, mens 2 var eksterne.

Spørreundersøkelsen

Av de interne respondentene som svarte på spørreundersøkelsen, var det representanter fra politisk, strategisk (kriseledelse/toppledelse), taktisk (informasjonsteam/IT-ledelse/øvrig beredskapsledelse i org.) og operativt (IT-drift/IT-sikkerhet/øvrig drift i org. slik som leder ved sykehjem, leder ved skole etc.) nivå.

Svar	Antall
Politisk	1
Strategisk (kriseledelse/toppledelse)	4
Taktisk (informasjonsteam/IT-ledelse/øvrig beredskapsledelse i org.)	2
Operativt (IT-drift/IT-sikkerhet/øvrig drift i org. slik som leder ved sykehjem, leder ved skole etc.)	11

På spørsmål om hvordan cyber-angrepet påvirket den enkeltes hverdag, rent praktisk, svarte **politisk** respondent at «Epost og nett var borte. Kommuniserte bare med tlf de første dagen. I månedsvis var saksbehandlingskapasitet sterkt redusert», mens respondentene på **strategisk** svarte at «Alle systemer som jeg/vi bruker var nede. Måtte finne nye måter å løse utfordringen på, med å gjøre ting manuelt.», «Tok all fokus. Ansatte som måtte få tilpasset arbeidsforhold. Improvisere for å klare juridiske forpliktelser. Bruke privat epost og også sms i kommunikasjon med omverden. Mye kontakt med eksterne aktører, som var bekymret for at vi skulle sende virus over til deres systemer, og som ville stenge oss ute. Forsinkelser med rapportering og leveranser. Prosjekter som stoppet opp.», «All tid gikk til krisehåndtering både helhetlig i organisasjonen og i sektor, overordnet og operativt. Fokus på å holde driften gående og at innbyggerne i minst mulig grad skulle bli påvirket av angrepet. Mye uvisshet innledningsvis», og «Det er dette jeg har jobbet med det siste året. Veldig mange andre oppgaver har måtte vente.». På **taktisk** nivå svarte respondentene at «Alle fagprogrammer ble utilgjengelige og det førte til at alle arbeidsprosesser måtte foregå med manuelle rutiner. Det påvirket ikke tjenester til liv og helse», «For ordens skyld jobber jeg ikke i ØTK nå, men gjorde det på det aktuelle tidspunktet. Jeg jobbet som leder for digitalisering og innovasjon, en liten enhet med 3 hoder. denne aktiviteten stoppet naturlig nok opp, og jeg ble det vi kalte innsatsleder for arbeidet med

etterforskning, gjenoppretting og annet arbeid som skyldtes dataangrepet.», mens på **operativt** nivå svarte respondentene at «Alle dokumenter var lagret i fagsystem. Mistet tilgang til kritisk informasjon for å kunne utføre saksbehandling. Mistet muligheten til digital saksbehandling. Måtte lage nye rutiner for manuell saksbehandling.», «Ikke tilgang til arkiv, dette gjorde det umulig å behandle klager der en må ha tilgang til arkiv. Vedtak måtte skrives for hånd. Alt som skulle arkiveres, journalføres måtte skrives for hånd og oppbevares nedlåst til systemene var i gang igjen. Alt måtte da skannes inn. Elektronisk sikker kommunikasjon med leger, sykehus osv. måtte tas over telefon og skrives ned med papir og blyant. Dette medførte en betydelig økt tidsbruk. Likeledes ble vi kastet ut av Husbanksystemet, slik at Husbanksøknader ikke kunne behandles. Etterhvert fikk vi her etablert en løsning via NAV sine systemer. Brev måtte sendes ut manuelt.», «Manglende tilgang til oppgaver som skulle følges opp, endring i arbeidsoppgaver med fokus på krisehåndtering og bistå med å rigge sektoren for manuell drift samt driftsetting av systemene igjen i samarbeid med øvrige ansatte. Periodevis manglende tilgang til it systemene endret kommunikasjonsmåter hvor sms var eneste kommunikasjonsmåten med øvrige tjenester/funksjoner utenom fysiske møter.», «Min tjeneste fikk ikke utøvet tjenesten vi er satt til å gjøre. Det krevde mye koordinering i det å holde kontinuitet i tjenesten. Så ble det mye arbeid (koordinering) knyttet til gjennopprettingen.», «Jeg mistet tilgang til alle løsninger jeg brukte i hverdagen min, og derfor ble jeg hindret fra å gjøre jobben min. Ble etter hvert koblet til "dataangrepinnsats", og jobbet derifra med ikke noe annet enn gjenoppretting.», «Lange dager, kriseledelse og gjenopprettingsarbeid Alle dokumenter var borte. Måtte skrive alt på nytt. Måtte skrive referater osv med penn og papir. Ingen tilganger til systemer utover fagsystem som lå i skyen. Måtte kontere alle fakturaer for hele enheten med penn og papir. Ingen tilgang på printer/kopi/scanning. Ingen tilgang på mail første uken.», «Det snudde opp ned på hele arbeidshverdagen, vi måtte ta i bruk manuelle rutiner og det var en stor jobb å sikre at brukere fikk den hjelpen de skulle.», «tilbake til blyant og papir», og «mistet all tilgang til ressurstyringsverktøyet GAT. Var med på på å lage skjemaer for vaktbok, medisinark, legevisittark osv på papir Jeg startet noen få dager etter angrepet så hverdagen før er ukjent. Jeg fikk umiddelbart PC og tilgang til officepakken og e-post, men det var også det.»

Av de eksterne som deltok på undersøkelsen, jobbet 1 ved kommuneCSIRT, 3 i ekspertorganisasjon IKT-sikkerhet og 6 i andre type organisasjoner (man kunne også velge Statsforvalter, Datatilsynet, NSM, PST, men ingen fra disse organisasjonene svarte på undersøkelsen).

På spørsmål om hva bidro du med overfor Østre Toten kommune, rent praktisk, svarte kommuneCSIRT «Koordinering, rådgiving», mens ekspertorganisasjonene responderte med «Jeg jobber som innleid sikkerhetsressurs for KS, særlig som sikkerhetsansvarlig i Fiks-plattformen (bl.a. SvarUt). Jeg var kontakt med Østre Toten for å avklare om det var nødvendig å stenge kommunens tilgang til fellestjenestene på Fiks-plattformen. Dette er et tiltak vi bruker for å sikre at ikke disse fellestjenestene skal kunne misbrukes som angrepsvektor overfor andre brukere av Fiks-plattformens tjenester.
Jeg bistod kommunen i første omgang med å håndtere de personvernrettslige sidene av angrepet via rådgivning og utforming av diverse tekster. Jeg bistod også med gjenoppretting av fagsystemene sett fra et personvernperspektiv.», og «Var i lead fra Atea IRT fra angrepet ble oppdaget og de første dagene etterpå».
Fra «andre» type organisasjoner, ble det respondert med at «Jeg er ansatt som HR rådgiver i Gjøvik kommune, med ansvar for blant annet overordnet internkontroll og delansvar for styringssystem for informasjonssikkerhet. Østre Toten kommune rettet en

henvendelse til Gjøvik for å få bistand i rollen som personvernombud. Jeg ble "utlånt" i en periode som varte ca. 14 dager for primært å bistå med avviksmeldingen til Datatilsynet. Østre Toten opprettet personvernombud som tok over ansvaret på slutten av perioden jeg var utlånt. Det var en litt trå oppstart for PVO rollen: ikke opprettet kontaktperson for meg, dette kom på plass etter hvert. Det var lite fokus på praktiske rutiner og sikkerhet når fagsystemene lå ned: mottak, oppbevaring og avhending av personsensitive opplysninger. Jeg bisto i et oppstartsmøte med ansvarlige personer fra enhetene, hjalp til med pre-definering av ROS analyse som skulle gjennomføres i drift samt vurdering av personvernkonsekvenser. Det var utarbeidet en behandlingsprotokoll, som ikke var tilgjengelig i fasen jeg bisto. Alle enheter måtte derfor svare opp manuelt hvilke personopplysninger og personsensitive opplysninger som var behandlet i fagsystemene som ligger under deres ansvarsområde. Jeg måtte be om å få delta på møte med kriseledelsen for å bli koblet på håndtering av hendelsen. Jeg samarbeidet tettest sammen med Atea og Datatilsynet i forhold til rollen som personvernombud. Avviket ble avdekket 09.01.21, vi hadde tilstrekkelig informasjon til å sende inn avviket til Datatilsynet 13.01.21 (i den fasen vi var i da). Hadde kontakt med Datatilsynet pr. telefon i hele perioden jeg bisto kommunen.», «kommunikasjonsrådgivning», «Jobber ved IKT i Gjøvik kommune. Kommunene i regionen har felles nettverk så jeg var den som kuttet forbindelsen til ØTK den 9. januar, var det vel. I startfasen av hendelsen jobbet vi selv med å få kontroll og oversikt og utover i gjennopprettingsarbeidet koordinerte jeg mye av arbeidet mellom ØTK og Gjøvik av hvilke tjenester de trengte midlertidig tilgang til.», «Salg og prosjektering», «Gjennomgang av mulig infisert data.», og «Bisto innsatsleder med koordinering og håndtering av hendelsen, innleid fra KPMG.».

Lærebokvurderinger av hendelseshåndteringen
Innledende spørsmål baserte seg på hvilke strategier, policyer, daglig vedlikehold, risiko-analyser med dertil håndtering, samt utarbeidelse av beredskapsplaner innenfor informasjonssikkerhetsarbeid, en organisasjon kan utarbeide innenfor informasjonssikkerhet slik som Whitman og Mattord beskriver i sin lærebok innenfor ledelse av informasjonssikkerhet [42].

10 av respondentene hadde tidligere vært med på å utarbeide informasjonssikkerhetsstrategier for en kommune, mens 18 ikke hadde vært borte i slikt arbeid. 6 av respondentene kjente til at Østre Toten hadde informasjonssikkerhetsstrategi når cyber-angrepet oppsto, mens 22 av respondentene var ukjent med dette. Strategi var beskrevet som at det «gjerne er et skriftlig dokument som angir den langsiktige planen for innføring og oppgradering av informasjonssikkerhet i en organisasjon» 11 kjente til at Østre Toten kommune hadde informasjonssikkerhetspolicyer når hendelsen oppsto, mens 17 var ukjent med om dette eksisterte. Policyer var beskrevet at «består av skrevne instrukser på hvordan man gjennomfører spesifikke oppgaver innenfor en organisasjon. Og, at det kan bestå av overordnede føringer fra ledelse, standarder organisasjonen må forholde seg til, veiledninger og prosedyrer.»

De 11 som hadde svart at de kjente til at Østre Toten hadde policyer for informasjonssikkerhet fikk oppfølgingsspørsmål om hvilke typer policyer for informasjonssikkerhet de kjente til at Østre Toten hadde på tidspunktet hendelsen skjedde. Resultatene er presentert i tabell 2 (flere svar mulig).

Tabell 2

Svaralternativ	Antall svar
Overordnede føringer fra ledelse	3
Krav til bruk av standarder innenfor informasjonssikkerhet	3
Veiledere innenfor informasjonssikkerhet (eksempelvis håndtering av GDPR, sikkerhetsklareringer etc.)	8
Prosedyrer for informasjonssikkerhet (med eventuelle retningslinjer for avvikshåndtering)	5

På spørsmål om de kjente til om Østre Toten hadde et utarbeidet sikkerhetsprogram på tidspunktet data-angrepet skjedde, svarte 3 at de kjente til dette, mens 25 svarte negativt. Et sikkerhetsprogram var beskrevet som at «det består av en organisasjonsplan med dertil oppgaver/funksjoner som det er behov for, sertifiseringsprogram, utdanning, trening, øvelser m.m.» De 3 som svarte ja på undersøkelsen fikk oppfølgingsspørsmål om hva slags innhold de kjente til fra Østre Toten sitt sikkerhetsprogram. Disse resultatene er presentert i tabell 3 (flere svar mulig).

Tabell 3

Svaralternativ	Antall svar
Funksjoner og arbeidsoppgaver var definert	1
Stillinger for å dekke funksjoner og arbeidsoppgaver var definert	0
Sertifiseringsprogram var definert	0
Krav til utdanning	0
Fast trening i organisasjonen	0
Øvelser	1

På spørsmål om de hadde deltatt i risikovurdering av cyber-angrep mot kommuner, svarte 8 ja, mens 20 svarte negativt. 4 kjente til at det var gjort en risikovurdering av cyber-angrep før hendelsen, mens 24 svarte nei på dette. Av de 4 som kjente til at det var gjort en risikovurdering av cyber-angrep, svarte allikevel 1 at dette var utført på strategisk nivå, 1 at det var utført på taktisk nivå, mens 3 svarte at det var utført på operativt nivå. Det var derfor viktig å få kartlagt hva som faktisk var gjort i løpet av dybdeintervjuene.

På videre spørsmål om de var kjent med om det var gjort tiltak for å håndtere risikoen for cyber-angrep i Østre Toten kommune, svarte 5 at det var det gjort, mens 23 svarte nei. Tiltakene var beskrevet å kunne «være både organisasjonsmessige, kulturelle, nye metoder for informasjonssikkerhet eller sikkerhetssystemer på applikasjoner, systemer og maskiner.» Blant de 5 som svarte ja, mente 2 at det var gjort tiltak på taktisk nivå, og 3 at det var gjort tiltak på operativt nivå.

De samme 5 ble også spurt om hvilke tiltak som var gjort for å forbedre informasjonssikkerhetsrisikoen i Østre Toten kommune, og resultatene er presentert i tabell 4 (flere svaralternativer mulig).

Tabell 4

Svaralternativ	Antall svar
Organisasjonsmessige tiltak (alt fra tilsetting av rett personell til å utføre rette funksjoner/oppgaver til å outsource systemsikkerhet)	0
Forbedre kultur for informasjonssikkerhet (løpende informasjon, trening, krav (sertifiseringer/klassifisering), øvelser)	0
Forbedre metoder for informasjonssikkerhet (eksempelvis prosedyrer med årlige oppdateringer, avvikshåndtering etc.)	1
Forbedre systemsikkerhet (apper, software, hardware ...)	3

På spørsmål om de kjente til om Østre Toten kommune hadde en vedlikeholdsplan for systemsikkerhet når dataangrepet oppsto, svarte 6 ja, mens 22 svarte nei. En vedlikeholdsplan for systemsikkerhet ble forklart «å bestå av ekstern overvåkning, intern overvåkning (hva slags hendelser kan oppstå internt), plan- og risikovurdering, sårbarhets analyser og utbedring, beredskap og jevnlig gjennomgang av sikkerheten.» Blant de 6 som svarte ja, mente 1 at denne var kjent på strategisk nivå, mens 5 mente at den var kjent på operativt nivå.

Disse som svarte ja ble også spurt om hva slags vedlikeholdsplaner for systemsikkerhet de kjente til når hendelsen oppsto, og disse resultatene er presentert i tabell 5 (flere svaralternativer mulig).

Tabell 5

Svaralternativ	Antall svar
Ekstern overvåkning av trusler	0
Intern overvåkning av trusler	4
Plan- og risikovurdering av systemer (informasjonsverdier, GDPR etc.)	6
Sårbarhetsanalyser og vurderinger (oppfølging av CAPEC, CVE, CWE, CCE, IT assets etc.)	2
Beredskapsplaner (hvem gjør hva når hendelsen oppstår) og jevnlig gjennomgang av systemsikkerheten	3

På spørsmål om de hadde deltatt i utarbeidelse av beredskapsplaner for å håndtere cyber-angrep for kommuner, svarte 4 ja og 24 nei, og på spørsmål om de kjente til om Østre Toten kommune hadde utarbeidet beredskapsplaner for cyber-angrep, svarte 1 ja og 27 nei. Den ene som svarte ja på at det var utarbeidet beredskapsplaner svarte også på hvilke beredskapsplaner for å håndtere cyber-angrep i Østre Toten kommune vedkommende kjente til. Dette er presentert i tabell 5 (flere svaralternativer mulig).

Tabell 5

Svaralternativ	Antall svar
Plan for hendelseshåndtering på operativt nivå (systemteknisk)	0
Plan for hendelseshåndtering på krisehåndterings nivå (som i hendelsen)	1
Eskaleringsplaner (fra operativt, til taktisk, til strategisk nivå)	0
Eskaleringsplaner (anmelde til politiet, melde til Statsforvalter, Datatilsynet etc.)	0
Planer for å innhente eksperthjelp	0
Kontinuitetsplaner (plan for bruk av redundante systemer, back-up, manuelle verktøy)	0
Informasjonsplaner (internt og til media)	1

Lovpålagte krav til samfunnssikkerhet og beredskap i kommunene
De neste spørsmålene omhandlet lovpålagte krav til samfunnssikkerhet og beredskap i kommunene (Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret [15], forskrift til loven [16] og veileder til forskriften [34]).

På spørsmål om Østre Toten kommune har kartlagt hvilke uønskede hendelser som kan inntreffe i kommunen, vurdere sannsynligheten for at disse hendelsene inntreffer og hvordan de i så fall kan påvirke kommunen basert på risiko- og sårbarhetsanalyse ihht. Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret (Sivilbeskyttelsesloven) §14, svarte 12 ja, 2 nei, og 14 vet ikke.

På oppfølgingsspørsmål til de 12 som svarte ja om risiko- og sårbarhetsvurderingen ble gjennomgått ved siste revisjon av kommunedelplaner i henhold til Sivilbeskyttelsesloven §14, svarte 4 ja, 0 nei og 8 vet ikke.

På spørsmål om cyber-angrep som hendelse var blitt vurdert i henhold til §14, svarte 1 ja, 4 nei og 7 vet ikke, og på spørsmål om cyber-angrep ble vurdert ved siste revisjon av kommunedelplaner svaret 1 ja, 3 nei, og 14 vet ikke.

På spørsmål om Østre Toten kommune beredskapsplan i henhold til Sivilbeskyttelsesloven §15, hvor beredskapsplanen skal inneholde en oversikt over hvilke tiltak kommunen har forberedt for å håndtere uønskede hendelser, hvor den som et minimum skal inneholde en plan for kommunens kriseledelse, varslingslister, ressursoversikt, evakueringsplan og plan for informasjon til befolkningen og media, svarte 10 ja, 0 nei og 8 vet ikke.

På oppfølgingsspørsmål blant de som svarte ja, om det var utarbeidet egne roller med definerte oppgaver i kriseledelsen for å håndtere et cyber-angrep, det vil si – om det var definert egne roller i kriseledelsen spesifikt for et cyber-angrep, svarte 2 ja, 4 nei og 0 vet ikke (6 svarte på oppfølgingsspørsmålene). Ytterligere 4 oppfølgingsspørsmål i henhold til veileder for hva en beredskapsplan ble stilt, og svarfordelingen er presentert i tabell 6

Tabell 6

Spørsmål	Ja	Nei	Vet ikke
Er det utarbeidet manuelle varslingslister for bruk ved cyberangrep? Eksempelvis at Statsforvalter, Datatilsynet og Politiet blir varslet.	1	3	2
Er det utarbeidet ressursoversikt til bruk ved cyber-angrep?	1	3	2
Er det utarbeidet en informasjons- og mediahåndteringsplan som kan brukes ved cyber-angrep?	1	3	2
Er det planlagt med hvem som skal uttale seg til media ved et cyber-angrep? Det vil si - vil det bli brukt eksperter (internt eller eksternt) i tillegg til ordfører, som kan uttale seg om type angrep og situasjonsoppdatering omkring dette?	1	0	0

På spørsmål om det det var utarbeidet egne roller med definerte oppgaver på taktisk nivå for å håndtere et cyber-angrep, eksempelvis kontakt med andre kommuner og helseinstitusjoner (gjelder teknisk etat, skoleetat, helse og omsorg og andre), kommuneCERT, politi (og deri evt. PST og NSM) (gjelder IT-ledelse), så var det ingen

som svarte på dette spørsmålet, dermed ble også åpent oppfølgingsspørsmål om hvilke roller og definerte oppgaver på taktisk nivå man kunne kjenne til heller ikke besvart.

På spørsmål om det var utarbeidet egne roller med definerte oppgaver på operativt nivå for å håndtere et cyber-angrep, eksempelvis kontakt med andre tekniske etater, skoler, sykehjem etc. (gjelder samarbeid operativt på tvers av kommunegrenser), eller eksterne SOC, CSIRT's, private ekspertoganisasjoner som Atea etc. (gjelder drift IT), svarte 1 ja, 1 nei og 2 vet ikke. På åpent oppfølgingsspørsmål om hvilke roller og definerte oppgaver for å håndtere cyber-angrep på operativt nivå de kjente til, ble det uttalt «Ingen kjennskap», «det er ikke definerte oppgaver spesielt for cyber-angrep, med for generelle kriseoppgaver», «skal møte opp på angitt sted ved bortfalle av kritisk infrastruktur. Gå over til manuell drift.», «jeg tenker at de som nå skal jobbe i vår IT avdeling (IDI), vil måtte håndtere et cyber-angrep.», «det er ikke utarbeidet eget planverk, varslingslister, tiltakskort eller lignende tilpasset cyberangrep, der har en "all hazards approach" tilnærming» «BCPT, CP, CPMT, CMPT, DRPT, IRPT Alle disse rollene/teamene har ulike oppgaver i en planlegging for kontinuitet i drift.», «Som jeg kjenner til, inneholder ikke kommunens beredskapsplaner noe som har å gjøre med cyberberedskap. Det finnes derfor ikke noen roller og oppgaver som spesifikt angår cyberberedskap.», «IKT avdeling og IKT leder», «vår beredskapsplan omtaler svikt/bortfall av elektronisk kommunikasjon. Kriseledelsen, fagpersonell, nøkkelpersonell, ekstra bemanning, kriseteam, beredskapsråd med frivillige.», «it – avdelingen» og «IKT avdelingen hadde avtale med ekstern leverandør som omhandlet håndtering av slike hendelser.»

Sosio-teknisk tilnærming til hendelseshåndtering
Spørsmål vedrørende hendelseshåndteringen ut ifra et sosio-teknisk tankesett ble presentert på oppstartsmøte og i mail til alle. Det ble også presisert at noen av spørsmålene som allerede er stilt også kommer inn under et slikt tankesett, slik at disse spørsmålene ville være utfyllende spørsmål vedrørende hendelseshånderingen - i en noe større sammenheng. For eksterne bidragsytere og samarbeidspartnere ble det formidlet at dette var de siste spørsmålene, mens det fortsatt ville være noen flere spørsmål til alle som jobber i Østre Toten kommune.

Roller respondentene hadde under krisehåndteringen av cyber-angrepet i Østre Toten kommune var fordelt på kriseledelse (7), taktisk ledelse (1), operativ ledelse (11), ekstern support uten operativmedvirkning (4), og ekstern support med operativ medvirkning (4)

I det følgende er de sosio-tekniske spørsmålene gjengitt i sin helhet, med definerte oppgaver innenfor hvert spørsmål.

I hvilken grad opplever du at det er god struktur for informasjonssikkerhet i Østre Toten kommune (tabell 7)?

Tabell 7

(svar fordelt på antall)	Liten grad	Noen grad	Middels grad	Stor grad	I svært stor grad	Vet ikke
Klart definerte roller og oppgavefordeling i organisasjonen	5	5	3	5	1	4
Gode økonomiske rammer	5	3	4	2	2	7
Klar strategi	6	4	4	3	2	4
Gode policyer med dertil prosedyrer og system for avvikshåndtering	3	6	5	3	2	4
Den enkelte kjenner sitt ansvar innenfor informasjonssikkerhet	4	9	2	1	0	7

I hvilken grad opplever du at det er god struktur for hendelseshåndtering ved cyber-angrep (tabell 8)?

Tabell 8

(svar fordelt på antall)	Liten grad	Noen grad	Middels grad/vet ikke	Stor grad	Svært stor grad	Vet ikke
Klart definerte roller og oppgavefordeling	4	3	3	8	0	5
Bruk av krisehåndteringsplan	5	2	5	2	1	8
Bruk av kontinuitetsplan for informasjonssikkerhet	5	3	2	3	1	9
Bruk av ressurslister	3	3	4	4	0	9
Bruk av informasjonsplan for krisehåndtering	1	2	6	3	1	9

I hvilken grad opplever du at det er god kultur for informasjonssikkerhet i Østre Toten kommune (tabell 9)?

Tabell 9

(svar fordelt på antall)	Liten grad	Noen grad	Middels grad	Stor grad	Svært stor grad	Vet ikke
Det sendes ut jevnlig informasjon om typer av cyber-angrep som kan oppstå	7	2	2	3	5	4
Det gjennomføres jevnlig elektroniske kurs om informasjonssikkerhet (eksempelvis i forbindelse med sikkerhetsmåneded i oktober)	5	6	6	1	0	5
Det gjennomføres jevnlig seminarer om informasjonssikkerhet	11	3	3	0	0	6
Det gjennomføres øvelser innenfor informasjonssikkerhet	10	5	2	0	0	6
Det er tydelig hvor man skal melde fra dersom det er mistanke om brudd på informasjonssikkerhetspolicyer	4	5	6	1	4	3
Saker som blir meldt inn blir raskt tatt hånd om og tilbakemelding blir gitt til varsler	5	4	2	2	2	8

I hvilken grad opplever du at det er god kultur for håndtering av cyber-angrep i Østre Toten kommune (tabell 10)?

Tabell 10

(svar fordelt på antall)	Liten grad	Noen grad	Middels grad	Stor grad	Svært stor grad	Vet ikke
Åpenhet rundt hendelseshåndteringen	0	2	1	9	11	0
Informasjon til ansatte	0	0	5	8	7	3
Involvering av ansatte i håndteringen	0	3	6	5	5	4
Involvering av eksterne i håndteringen	1	0	2	5	13	2
Anmeldelse av hendelsen	0	0	1	5	13	4

I hvilken grad opplever du at det er gode metoder for informasjonssikkerhet i Østre Toten kommune (tabell 11)?
(Totrinnsbekreftelse (autentisering) er et ekstra sikkerhetsnivå for innlogging. Med totrinnsbekreftelse logger du inn med noe du vet (ditt passord) i tillegg til noe du får (en kode på telefon))

Tabell 11

(svar fordelt på antall)	Liten grad	Noen grad	Middels grad	Stor grad	Svært stor grad	Vet ikke
Regelmessig bytte av passord kreves	2	0	1	11	3	6
Det er ikke mulig å benytte gammelt passord ved opprettelse av nytt	1	0	1	9	7	5
PC-er har automatisk skjermlås etter kort tid	1	4	0	4	8	6
PC blir låst etter 3 feil forsøk med pålogging	0	0	0	5	5	13
Kommunen benytter to-trinns autentisering ved pålogging på online-systemer (som email, Transponder o.l.)	5	1	3	0	9	5
Hvis du benytter feil passord, blir du da rutet til to-trinns autentisering	4	0	1	0	4	14
Det er ikke mulig å logge seg inn på systemer med andres passord	3	1	0	0	4	15

I hvilken grad opplever du at det er gode metoder for håndtering av cyber-angrep i Østre Toten kommune (tabel 12)?

Tabell 12

(svar fordelt på antall)	Liten grad	Noen grad	Middels grad	Stor grad	Svært stor grad	Vet ikke
Systemer som er angrepet kan stenges av fra andre systemer	4	0	2	2	1	14
Back-up kunne benyttes etter kort tid	8	5	0	1	1	8
Logger kunne enkelt hentes ut for å gjenopprette data	7	3	1	2	1	9
Alternative systemer kunne benyttes	8	2	1	2	1	9
Alternative metoder (skriftlig, plakat på veggen, jevnlig info per telefon) kunne benyttes	3	3	3	7	3	4
Ble metoder for eskalering av informasjon om hendelsen benyttet	3	0	1	4	3	12

I hvilken grad opplever du at det er god systemsikkerhet i Østre Toten kommune (tabell 13)?

Systemsikkerhet er sikkerhet opp mot både apper (online), software og hardware

Tabell 13

	Liten grad	Noen grad	Middels grad	Stor grad	Svært stor grad	Vet ikke
Mailserver filtrerer bort (sandboxing) infiserte dokumenter	2	2	2	5	2	15
Apper (slik som Transponder) er innenfor brannmurer (DMZ)	2	1	0	2	1	22
Det er egne brannmurer på software (slik som øknomisystemer)	3	0	0	2	1	22
Det finnes en egen brannmur på min personlige PC	2	0	0	4	3	19
Det finnes egne brannmurer på web-sider (url-sikkerhet)	3	1	0	1	0	23
Ved systemoppdateringer så er det sikkerhetsvarsler, slik at du må oppdatere dine passord	3	2	1	1	2	19

I hvilken grad opplever du den system-tekniske håndteringen av cyber-angrepet (tabell 14)?

(svar fordelt på antall)	Liten grad	Noen grad	Middels grad	Stor grad	Svært stor grad	Vet ikke
Krypterte systemer ble sperret av fra andre systemer	1	2	0	1	4	15
Logger fra de avsperrede systemene ble etterforsket	0	0	0	3	8	12
Krypterte PC-er ble isolert og renset	0	1	0	2	13	7
Logger på/fra PC-er ble etterforsket	0	1	0	3	2	17
Ble kryptert hardware koblet fra strøm	0	0	0	2	2	18
Ble logger etterforsket på de isolerte maskinene	1	0	1	2	2	17

Modenhetsundersøkelse (eksalering og de-eskalering av informasjon under hendelseshåndtering)

Spørsmålene i denne delen ble kun gitt til de som jobbet i Østre Toten kommune i forbindelse med hendelseshåndteringen, og omhandlet eskalering og de-eskalering av informasjon under hendelseshåndtering. Disse spørsmålene baserer seg på nylig utviklede modenhetsundersøkelser omkring nevnte [29], og går i noen grad mer i detalj enn tidligere spørsmål for å finne ut hvilket nivå organisasjonen er på. Resultatene fra denne undersøkelsen vil bli presentert i vitenskapelige artikler og Østby sin doktorgradsavhandling.

Dybdeintervjuene

På politisk nivå i organisasjonen, ble det gjennomført intervju med ordfører, mens det på strategisk nivå ble gjennomført intervjuer med kommunedirektør og kommunalsjef for helse og omsorg. På taktisk nivå ble det gjennomført intervju med skolesjef og

økonomisjef, mens det på operativt nivå ble gjennomført intervju med personvernombud og utpekt innsatsleder IKT. Av eksterne ble fylkesberedskapssjef og en ekstern deltakende ekspert på hendelseshåndtering av cyber-hendelser intervjuet.

Ordfører i Østre Toten kommune, som har vært det siden 2019, var en del av kriseledelsen. Som ordfører og øverste politiske leder når data-innbruddet skjedde, så møtte han i kriseledelsen. Det var behov for mye intern og ekstern informasjon, særlig i forbindelse med den eksterne informasjon ut til presse og folket i Østre Toten, men og nasjonalt, som ordfører hadde en ganske stor rolle i. Ordfører fungerte som den folkevalgte representanten i kriseledelsen og hadde et overordnet ansvar for at beslutninger som ble tatt var innenfor «det som folk i Østre Toten kommune synes var greit». Det var viktig for ordfører som øverste politiske leder å fortelle om hendelseshåndteringen, og at det skjedde på en måte som ville være «ok» for folk i Østre Toten kommune, noe det ifølge ordfører var lite debatt rundt.

Kommunedirektør i Østre Toten kommune kom til Østre Toten 15. august 2020, altså et halvt år før cyberangrepet. I funksjonen kommunedirektør ledet han krisestab når den ble satt, da gjennom kriseledelsesmøtene. Første møte i kriseledelsen ble gjennomført lørdagsmorgenen, og det ble gjennomført møter jevnlig utover lørdagen og søndagen. I begynnelsen ble det gjennomført møter veldig ofte, og så ble det så ble det litt mer sjelden utover, men uansett en i gang i uka i over et år. Kommunalsjefene, økonomisjef, HR-sjef, beredskapskoordinatoren, ordfører, og representanter fra IKT var inne i så å si alle møtene. Men det var litt ulike roller de hadde etter hvert som hendelseshåndteringen utviklet seg. Sekretær var også til stede i disse møtene.

Kommunalsjef for helse, omsorg og velferd, var en del av kriseledelsen gjennom hendelseshåndteringen, og hadde det overordnede ledelsesansvaret innenfor sektorfeltet helse og omsorg. Som kommunalsjefen sa

> «I utgangspunktet skulle man jo tro at helse- og omsorgstjenestene er godt vant til å ha fokus på sikkerhet, da alle er vant til å forholde seg til taushetsplikten og har stor forpliktelse til oppfølging av de reguleringene. Og det er jo sånn at vi har bygd et nytt sykehjem for eksempel, som er teknologisk innretta. Vi har forhold i hjemmetjenesten som gjør at den daglige drifta er på digitale arbeidsplasser, og alt dette datt jo ned, så vi var på manuelle rutiner fra minuttet da dette skjedde. Vi var jo på manuelle arbeidsrutiner i lengre tid. Det gjorde jo at vi måtte tilbake til manuelle arbeidsrutiner som de hadde for veldig, veldig mange år siden. Penn og papir og kopimaskin, og telefax. På noen områder har vi hatt pasientsikkerhetsspørsmål, eksempelvis på Labo, som det er så mye teknologi med både pasientvarslingsanlegget, dykkesignalanlegget og dørautomatikk og den slags. Så blir det straks mer alvor ut av det da, og det gjorde det for så vidt i hjemmetjenesten og da, fordi der har vi jo elektroniske, det vil si digitale arbeidslister og når det ikke går an å få inn de lenger så da måtte vi dypdykke i søplekontaineren faktisk, slik at vi fant igjen noen lister som vi visste var kasta, og det er jo forskjell på intervaller på hvor ofte folk skal ha hjelp, hver 14 dag, en dag i uka, og da måtte vi da hente opp igjen de arbeidslistene. Det tok ikke veldig lang tid da, før det ble perm på perm på perm med papir, da alt vi vanligvis dokumenterer i elektronisk pasientjournal nå skal dokumenteres på papir i påvente at vi fikk opp igjen systemene. Jeg sa vel det til pressen en av de første dagene at

> dette er her surrealistisk, og det var det jo også. Jeg veit jo det at vi hadde prata om det helt løst i kommuneorganisasjonen at i framtida måtte vi forberede oss på at det ble flere hendelser, at ikke ustabiliteten ble så stor, og da ble det jo mer alvorlig da, så det så vi jo. Ja, og den dagen telefonen kom, så jobba vi jo hele den lørdagen, så da utpå ettermiddagen sa jeg at det eneste som mangler nå da er vel at strømmen går, og det gjorde den jo og. Det kom jo da melding utpå kvelden at strømmen hadde gått på Fjellvoll. Det var ganske spesielt, men jeg syns jo at det som har vært veldig imponerende er hvordan tjenesten har klart å holde hjula i gang, og vi har ikke fått noen meldinger om at det har vært noen alvorlige pasienthendelser, at det har gått ut over pasientsikkerheten, for ansatte har jobbet hardt for å holde oversikten selv om ikke alle opplysningene har vært tilgjengelig. Det er jo klart at vi har jo også hatt rutiner fra før på noe av det her, blant annet minimumskrav på at hovedkortet i journalen og medisinlistene, at det skal være utskrift av dem. Og det er jo nettopp med tanke på at det skal dette ned, så det har faktisk fungert bra.»

Skolesjefen er nærmeste leder for rektorene og de hadde jevnlig kontakt for å sammen finne løsninger på den enkelte skole i forbindelse med dataangrepet. Rektorene måtte håndtere de ulike utfordringene på sine skoler, med skolekontoret som kontaktpunkt. Skolen i Østre Toten bruker digitale løsninger på det meste av det de gjør, både når det gjelder skolekontoret med forskjellige programvare der og ikke minst ute på skole. Digitale ferdigheter er en av de fem grunnleggende ferdighetene som elevene utvikler gjennom hele skoleløpet. Disse er beskrevet i overordnet del i Kunnskapsløftet (LK-20). Disse ferdighetene er del av den faglige kompetansen og nødvendige redskaper for læring og faglig forståelse.

I tillegg til i undervisningen, benytter skolen i Østre Toten digitale løsninger til kartlegginger, dokumentskriving, skoleadministrativt verktøy, læringsplattform og arkivering. Og, som skolesjefen uttalte:

> «Grunnskolen hadde tatt i bruk Office 365 før 08.01.21, på tross av noe skepsis/ (motstand) fra kommunen for øvrig, da IKT-avdelingen mente at alle burde «gå i takt» her. Det at vi hadde vært såpass «fremme i skoa», ble noe av redningen for oss etter angrepet. Grunnen til at skole var mye lenger fremme enn resten av kommunen her, er at vi så nødvendigheten av å henge med i den digitale utviklingen for å gi best mulig opplæringstilbud til alle grunnskoleelever. En av de ansatte rådgiverne på skolekontoret, som er min stedfortreder, har blant annet arbeidsoppgaven med å være systemansvarlig for dataprogrammer, og han har mye med data å gjøre, så han ble jo veldig viktig i denne situasjonen her. Både for meg og for kommunen for øvrig, og også ute på skolen. Så han var jo en veldig god bidragsyter i denne prosessen her, og helt nødvendig.»

I Østre Toten er ifølge skolesjefen de dataene de har på elever lagret i deres skoleadministrative system som er en skyløsning. I tillegg har de manuelle elevmapper som oppbevares i låste arkivskap på skolene. Individuelle opplæringsplaner lagres i et system som også er en skyløsning, og dataene der var også sikkert lagret. Nevnte data var altså skånet for data-angrepet.

Mye av det den enkelte ansatte hadde lagret på sin egen maskin forsvant allikevel i angrepet. Selv om filene senere ble funnet og gjort tilgjengelig for alle ansatte en periode (slik at disse kunne hentes å lagres på et sikkert sted), var det likevel mange filer som ikke lot seg åpne/var forvunnet. Dette har medført en del merarbeid for lærere, skoleledere og også delvis skolekontoret (selv om de hadde det aller meste i onedrive), da mange dokumenter måtte memoreres så godt som mulig og produseres på nytt.

Økonomisjef er medlem av kommunedirektørens ledergruppe og var også en del av kriseledelsen under data-angrepet. Han ble tidlig kjent med hendelsen gjennom at it-sjefen var hans underordnet, og ble oppringt av ham da han var på vei til på jobb. Økonomisjef tok dermed ansvar for å samle kriseledelsen. Økonomisjef hadde også ansvaret for å melde hendelsen inn til Østre Toten sitt forsikringsselskap. Dette gjaldt blant annet KLP som var bekymret for at det de var utsatt for kunne spre seg igjennom dataflyt mellom Østre Toten og KLP. Gjøvik kommune som er vertskommune for det regionale ikt-arbeidet stengte Østre Toten ute fra gjensidig dataflyt umiddelbart. Husbanken samt flere andre statlige organer stengte Østre Toten ute av frykt for at det virus som kunne spres til deres organisasjoner, og som økonomisjefen uttalte:

> «Det var jo en viss form for kaos, hva var det vi var utsatt for og kunne det spre seg gjennom datatrafikk. Det var nok frykt hos mange.»

Personvernombudet startet i Østre Toten etter angrepet og fikk kort tid etter oppstart beskjed om at hun var ønsket som personvernombud. Før hun begynte i Østre Toten så var det en person som hadde rollen som hadde sluttet, og det var innleid bistand fra Gjøvik kommune frem til nytt personvernombud skulle på plass. Selv om personvernrollen er en liten del av hennes stilling, så ble det jo mye av den rett etter angrepet, og ikke minst når lekkasjen kom i påsken. Så når personopplysninger var delt på det mørke nettet så var hun veldig involvert. Avviket var allerede meldt Datatilsynet innenfor fristen, det ble gjort av økonomisjef, og da i samarbeid med personalsjefen som har ansvar for HR og kommunikasjon. Det som skulle meldes Datatilsynet, og i den grad man visste hva som egentlig hadde skjedd, deri hva som kunne være på avveie, ble håndtert et par dager etter angrepet. Dette ble gjort med bistand fra en person fra Gjøvik kommune. Når da nytt personvernombud startet, så ble det opprettet umiddelbar dialog med vedkommende fra Gjøvik om hvordan dette skulle følges opp.

> «Så satte jeg meg selvfølgelig til å lese igjennom forordningen, GDPR forordningen, og ut fra det spolet jeg meg inn på forskjellige personer i forskjellige nettverk, blant annet KS hvor jeg kunne få rask og effektiv hjelp, og ikke minst Datatilsynet. Jeg hadde veldig kjapt dialog med en fagleder på området i Datatilsynet, sånn at vi gjorde det vi måtte, men at vi ikke brukte mer tid enn vi var nødt for å håndtere det som skulle håndteres i forhold til Datatilsynet og eventuelle innbyggere. Og det var selvfølgelig også så viktig for meg i ombudsrollen å sørge for at vi fikk informasjon ut, altså at innbyggerne skulle bli satt i stand til å gjøre de tingene som er smarte for dem hvis det skulle ha konsekvenser, før vi visste at ting var ute.»

Personvernombudet var først med i kriseledelsen fra påsken når personsensitive data var delt på det mørke nettet. Det ble da opprettet kontakt med Datatilsynet, og det ble rigget for oppfølging umiddelbart. Personvernombudet var da i tett dialog med kommunedirektøren, med informasjonsrådgiverne på rådhuset, tett dialog med

Datatilsynet og med de som håndterte hendelsen (også KPMG). Det ble gjennomført daglige møter når de ble kjent med delingen på det mørke nettet. Det ble rigget en gruppe som skulle varsle innbyggere, under oppfølging av personvernombud.

> «Det viktigste for meg var jo egentlig den rollen min, å få opp en varslingsenhet, ja og jeg behøvde jo strengt tatt ikke å ha deltatt i den, men det er noe med hvem som deltar, hvem gjør dette fysisk, hvilken kompetanse er det lurt å ha på banen når vi skal begynne å varsle innbyggere. Det vi da var litt kjent med, hvor mye sensitiv informasjon, og om hvor mye det kunne være krevende for noen å håndtere, hva som var ute og gikk om dem da, for å si det på den måten. Så da var det da å bistå for å få rigget varslingsenheten, og så fortsatte jeg da å være delaktig i oppdateringsmøter gjennom hele påsken.»

Det var både jurister og ansvarlige fra KPMG som veiledet arbeidet, blant annet en person med solid kompetanse på sikkerhet og på sporing av hendelsesforløp. Kommunen fikk dermed hjelp til maskinelt å avlese det som ble kjent hadde lekket, hva som var lekket, men også hvem det er viktigst å varsle når, og hvor mye som bør varsles.

> «Skal vi varsle konservativt som er den ytterste konsekvensen ved å gå ut i media og si alt kan være ute og så stoppe det der, eller skal vi analysere litt her og lage en modell for hvem vi tar direkte kontakt med? Hvordan rigger vi det, her var det jo snakk om mange personer ikke norsk talende, hvor godt snakker de norsk, må vi rigge et tolke-apparat? Vi visste at det var lekket informasjon fra en 110-logg som egentlig ikke er informasjon unntatt offentlighet, men vi så jo der at det lå informasjon eksempelvis om at det var funnet døde mennesker på en grunneiers eiendom hvor brannvesenet rykker ut og de fører jo det i loggen. Det står jo ikke hvem, men det er klart at Østre Toten er lite så vi gjorde også noen vurderinger av det. Vi hadde med brannsjefen på den biten, og han sitter også i krisestaben. Vi vurderte det jo også sånn at vi i noen tilfeller varslet grunneiere også om at det har vært en hendelse og at det er ute på nett, selv om det kanskje ikke var sånn veldig sensitivt, så er det jo noe med ubehag og konsekvenser. Så vi var ganske romslige der. Vi måtte jo også sjekke, i og med at det var en del helseopplysninger, så måtte vi også bruke noe tid på å ha løsninger for å verifisere at vi snakket med riktig person. Det er sånn når du tror du ringer et damenavn og det er en mann som tar telefonen hver gang, forvisse oss om at vi snakker med riktig person, det var ikke like lett alltid.»

Kulturforskjeller, aldersbestemmelser og vergemål var også forhold som ble vurdert. En i varslingsenheten var i kontakt med NorSIS for å få deres anbefalinger på dette.

> «Men det var vi veldig tidlig, det var vel så fort verden hadde åpnet etter påske. Så hvis jeg kan si litt om det da, så synes jo vi vi gjorde en vanvittig jobb, så vi smilte jo litt i barten når det ukesvis etterpå så ut som om det var NorSIS som hadde kontaktet Østre Toten, og ja så det var litt interessant. Det var nok mange som ville pynte litt på brua si ja, når det gjaldt hvordan man hadde rigget seg. Men vi vi har jo dokumentasjon, jeg har logger fra hvert eneste møte, det skjønte jeg andre dagen i påsken at noen må lage et

konsept her for hvordan vi har håndtert dette her, så det tok jeg ansvar for det, så jeg har jo logger de første 3 - 4 ukene før hvert møte med hvem deltok.»

Varslingsgruppas hovedoppgave var å varsle de som skulle vite at ting som er konfidensielt for den enkelte er ute, og i ytterste konsekvens tapt for alltid. I varslingsgruppa var det en person fra voksenopplæringen, en person som tidligere hadde ledet krisestaben i Østre Toten med helsefaglig bakgrunn, og en kommunikasjonsrådgiver (i tillegg til personvernombud). Det ble utarbeidet en trafikklys-modell hvor de som var røde var de ble varslet en til en, totalt ca. 50 personer. Samtidig var det noen hvor det var en overvekt av gult som ble kontaktet, hvor summen av informasjon på avveie bestemte dette.

«Så var det å få tak i folk, da hadde vi (kommunen) helt tilfeldig bestilt utskrift fra folkeregisteret til et eller annet annet formål. Folkeregisteret er jo stengt i påsken og der er det ingen kriseberedskap. De kan også gjemme seg litt. Men tilfeldigvis var det en person som visste om denne utskriften, det tror jeg var kommunikasjonsrådgiveren som hadde oversikt over det, så den gruppa som ble satt sammen der det var det var kjempesmart.»

Etter at Norge åpnet igjen etter påske fikk de tak i noen ved Folkeregisteret, og fikk aksept for det for det de hadde av adresselister, for derved å kunne sende ut brev til alle innbyggere i Østre Toten kommune som var bosatt der på det tidspunktet. Både på norsk og engelsk, med henvisning til hjemmeside. I tillegg fikk alle de som ble ringt opp et eget brev.

«Vi kjente hverandre ikke, vi har aldri møtt hverandre, så vi begynte med en halvtime på teams hvor vi bare sånn kort dette er jeg flink til og dette er jeg flink til, og så var det en kjempematch. Og så diskuterte vi vanskelig saker. Og vi diskuterte også hvor mye vi kan gå ut med, der jeg for eksempel særlig knyttet til folk med psykisk altså psykisk utviklingshemming og sånn, hvor mye skal de selv vite, så vi hadde noen gode runder på det. Effektive gode runder. Og så loggførte vi selvfølgelig hvem har ringt hvor og når. Og når fikk vi taket i, fikk vi ikke tak i, svarte ikke på telefon, svarte på telefon. Vi kjøpte, det var det altså det er et verktøy som blant annet KPMG bruker til å bistå i sånne situasjoner, hvor du skal altså maskinelt avlese data, ja hvor de gjenkjenner etternavn, gjenkjenner personnummer. Det var et veldig godt verktøy, og der og da kunne vi jo bare bestille kolonner og sånt, for det vi trengte, så de modellerte det for oss.»

Innsatsleder IKT jobbet på daværende tidspunkt i Østre Toten kommune, hadde jobbet der i ca. 3 år, og var leder for det som ble kalt DIGIT, en relativt nyopprettet enhet, hvor det var 3 stykker som jobbet som prosjektledere innenfor de største digitale prosjektene innenfor innovasjon av teknologi/IT. Når hendelsen oppsto, så leste han som skulle bli utpekt som innsatsleder IKT, om hendelsen først i avisa før han fikk høre om det på andre måter. Det var så IT-sjefen som ville at han skulle bli med i et kort møte på søndag, sammen med en representant fra ATEA. Onsdag den påfølgende uken ble han utpekt som innsatsleder, mye på grunn av at det ikke var et prosjekt pågående akkurat da, og for å koordinere innsatsen i den fasen.

Statsforvalteren har ansvar for samordning når det skjer kriser, så det å følge opp kommunene både med øvelser og ved innsatser er vanlig oppfølging for dem. Når det gjelder kriser følger de opp behov for støtte og hjelp med nødvendige ressurser og eventuell samordning mellom kommuner. Fylkesberedskapssjefen, som representant fra Statsforvalteren, deltok i medlytt i møtene i kriseledelsen i Østre Toten kommune.

> «Da det jo er den rollen vi har, vi har jo også tiltakskort eller en strategi om du vil, på eventuelt når kommuner er i kriser, så tilbyr vi oss gjerne til å sitte på medlytt i kriseledelsen for å se om det er noe å bidra med da. Det gjorde vi jo gjennom pandemien når kommunene satte stab og hadde veldig store utbrudd, så hadde vi jo folk som deltok i kriseledelsene, og når Østre Toten ble rammet så var det jeg som satt som liason, eller som støtte, eller på medlytt i møtene i kriseledelsen i Østre Toten kommune.»

Samordningsansvaret handler om å sørge for at ressursene finner hverandre, og at alle som er involvert har den samme situasjonsforståelsen. Dersom det skal være tiltak på tvers av kommuner eller statlige etater så er det også Statsforvalteren som fasiliteter møtestrukturer for å få dette til. I noen hendelser er det veldig mange som skal inn og mene noe for å samordne tiltakene sine, mens i andre situasjoner er det mer isolert, og saken i Østre Toten var for Statsforvalteren mer av det isolerte slaget, da det kun råkte Østre Toten kommune.

> «I hvert fall sånn direkte, så er det jo sånn at for eksempel Østre Toten kommune samarbeider med andre kommuner, og man kunne derfor tro at eksempelvis Gjøvik eller Vestre Toten kunne bli rammet, så det er viktig å få de samtalene på plass og få kartlagt det og få greie på det. Men, det er jo mange andre bidragsytere også og det som ble gjort av samordning her, var nok for det første at vi tipset om kommune CSIRT, at de kanskje kunne være bidragsytere helt i starten, og de ble jo kontaktet, og etter hvert så var jo vår egen organisasjon, altså Statsforvalteren, spesielle spørsmål i denne saken her der vi har tilsynsmyndighet som måtte sørge for at kom inn i bildet blant annet forsvarlig helsetjenester og forsvarlig barnehagedrift da dataene deres var nede ganske lenge. Det var våre egne folk stort sett jeg var i kontakt med i denne hendelsen, det var ikke så mye ressurser som var påkrevd fra utsida som ikke kommunen selv har vanlig kontakt med da. Ja, jeg snakket med kommune CSIRT-en selv og. Ikke noe operativ utveksling, men at det nå skjedde noe som de måtte forholde seg til. Statsforvalteren skal sørge for at kommunene er i stand til å håndtere så mye som mulig selv, og dermed å snakke med dem og høre hva som står på, og om det er noe de trenger. Trenger de hjelp til noe, trenger de ressurser, har de ringt alle de folka man skal ringe når man gir tips om hvem det går an å prate med, og sørge for at de føler at de har noen i ryggen egentlig.»

Med bakgrunn i at Østre Toten en tid forut for hendelsen hadde gjennomført en modenhetsanalyse i samarbeid med ATEA (som en del av et helhetlig arbeid i Gjøvik-regionen), ble ATEA kontaktet når hendelsen oppsto (de hadde ikke en utarbeidet avtale med ATEA på dette, men en slik avtale ble da utarbeidet i løpet av en – to timer etter at de ble kontaktet). En sikkerhetskonsulent fra ATEA ble derfor raskt koblet på hendelsen. Vedkommende er til daglig medlem i ATEA incident responce team (IRT). Han hadde lead da ATEA IRT ble kalt inn på inn på hendelsen. Han satt i rollen som har kontroll på

alle aktivitetene som foregår ved «incident response» og da også informasjon oppover til ledelsen. Kontaktpersonen i kommunen på dette tidspunktet var IT-sjef.

> «Til å begynne med hadde jeg en sånn edderkopp funksjon siden vi jobber slik at vi undersøker saken først, og så finner vi ut hva slags type sak dette her, og så kaller vi inn våre ressurser etter hvilke ekspertområde de har, og så setter vi sammen et team, og til sist hadde jeg den overordnede oppgaven med å koordinere ting, så jeg bisto både med IRT og jeg bisto da også med informasjon og råd oppover.»

I tillegg til kontakt med IT-sjef, hadde ATEA også dialog med kommunaldirektør samt Visma og KS og også med NSM og Datatilsynet. Til å begynne med hadde de jevnlige møter for å finne omfanget av hendelsen, og de så fort at dette kom til å ta tid. De hadde lite å gjøre/lite å jobbe med fordi at det meste var tatt.

> «Det fantes noe brannvegg-logger, så det var vel møter 3 - 4 ganger i løpet av det første døgnet, og så var det det omtrent like mange ganger andre døgnet, men da var det jo også snakk om å briefe i forhold til presse og hva man skulle si og sånn.»

KS ville gjerne vite i detalj hva som hadde skjedd, deri hvor mye ATEA kunne klare å finne ut av angrepet, altså hvor lang tid det tok fra angrepet ble kjørt til systemene var låst. De var også interessert i sårbarheter i systemene, og de kom med noen anbefalinger et par uker i etterkant av angrepet. ATEA hadde imidlertid litt vanskeligheter med å forstå KS sin egentlige rolle, men fikk beskjed fra kommunen om å samarbeide med dem og å gi dem alt de ønsket. Det oppsto deri en usikkerhet omkring rollefordeling, og ATEA uttrykker en skepsis i forhold til om KS egentlig rådga kommunen godt.

> «Jeg tror det var mer til felles beste for alle kommuner, at de prøvde å finne noen felles trekk hvor man kunne gi et felles skriv.»

Underveis i prosessen så fant ATEA ut at på lagringssystemet, altså ikke på back-up-systemet men på lagringssystemet, så var det tatt et snapshot av alle serverne. Dette visste ikke kommunen selv noe om, men de fant dette såpass sent at de kun hadde 2 timer på å kopiere over det de klarte av viktige servere før det ble overskrevet. De hadde ikke mulighet til å stoppe overskrivingen fordi de har ikke nødvendige tilganger. Ergo ble de serverne de fikk beskjed om at det var mest kritiske kopiert, så langt det lot seg gjøre på de nevnte 2 timene. Og det var det de klarte å redde ut av data.

> «Ja bortsett fra «firewall». De hadde tatt back-up serveren. Det ATEA gjorde på den sårbarhetsanalysen, vi gjorde den siste analysen, var jo å påpeke da at de ikke hadde noe slags back-up av systemene, det var satt som veldig høyt kritisk at de ikke hadde det. Det ble laget et regneark med prioriteringer på hva kommunen måtte gjøre, men det rakk de da tydeligvis ikke å få på plass.»

Ifølge ATEA var det heller ikke gjennomført noen «business impact analysis» (BIA) på systemene (basert på at kommunen syntes å kun ha et visst begrep om hvilke systemer som var viktige), eksempelvis var det i kommunen en forståelse av at systemene ble benyttet ved sykehjemmene var viktige, men at systemer som ikke var vurdert var slikt

som låsesystemet og også systemlåser på medisinskapene. Dermed måtte de utstyre alle pasientene med bjeller, og med ekstra bemanning på gangen for å høre bjellene.

> «Det som gjorde at de fikk i gang noe, det var jo at de kunne på en få på plass PC-er og i alle fall bruke office 365 skyen som en som en plattform, men i begynnelsen så fikk de jo ikke kommunisert via email, så da var det private eposter det gikk på. Ja så det var jo det var jo helt nede. Det eneste om ikke var nede var «firewalen» og «switcher». Vi var jo ikke sikre på om de hadde vært inne på disse heller da, så vi anbefalte dem å kjøre clean install på alt sammen, i og med at vi ikke hadde noe logg på om det var kompromittert eller ikke. Angriperne hadde tydeligvis hatt tilgang på administratortilganger, og mot våre anbefalinger da så hadde de jo AD-integrert (Active Directory Integration) på det meste, at du dermed får tilgang til back-up via admin kontoer. Du får da tilgang til VMV-er via admin kontoer, og det er ikke det vi anbefaler alle fall.»

Det var en tidligere ansatt som var hyrt inn for å hjelpe til med brannveggen (hadde fortsatt tilgang selv om vedkommende ikke lenger var ansatt i kommunen). Dette gjorde at de kunne få litt logger fra brannveggen. Det var brukere og passord som hadde ligget der lenge, altså som aldri hadde blitt skiftet på enkelte enheter, dette være seg «appliances» som var «firewall appliances», «switchere», rutere og liknende, samt at det var en del fagsystemer som hadde lokale baser som det ikke var passord policy på.

> «Det var jo 2 hoder da for it avdelingen + IT-sjef, og det var det er jo begrenset hvor mange hatter de kan ha, og hvor mye de klarer å utføre på en måte. Og de hadde jo ikke overvåking av systemene på noen måte, i hvert fall ikke noe SIEMS verktøy eller noe.»

ATEA brifet allikevel ift. hva de så om de mulige angreps-vektorene de fant, også da med hensyn til påvirkning på tjenester hvor de kunne se om de kunne klare å få det opp igjen et nivå. Det ble formidlet at det kunne komme til å vare en stund, gjerne måneder, fordi de var helt på bar bakke. ATEA satte dog opp et system for å vaske data, det vil si at de tok de kompromitterte dataene som de fant fra «snapshoten» på lagringssystemet, for deretter å kopiere data over til en midlertidig løsning som vasket dataene og sjekker dem for ulumskheter, og deretter kopierte videre dataene til et nytt reinstallert system. Den prosedyren ble iverksatt mens sikkerhetskonsulenten fra ATEA var i lead.

ATEA satte altså i gang prosedyrer og fikk i gang et apparat i ATEA så de kunne avhjelpe kunde, hadde en prosjektleder på det, og stilte i utgangspunktet med nødvendige ressurser for å komme fortest mulig i gang igjen med de systemene som var viktigst. Eksempelvis vasking av data ble delt opp i områder hvor ekspert-konsulenter fra ATEA kunne hjelpe Østre Toten med å få på plass data. I tillegg for å få på plass nye maskiner hvis dere trengtes, da man på dette tidspunktet ikke visste om hele serveren kunne være kompromittert, og at det da går det raskere å få tak i nye servere for å gjenopprette arbeidet. Østre Toten hadde en del eldre servere som ikke var koblet mot nett, som man kunne bruke til å reinstallere programvare på. Fokuset var å få systemene opp i drift, med prioritet på de viktigste systemene (kritiske for liv og helse). Kriseledelsen gjorde en prioritering av hvilke systemer som skulle først opp. Dette baserte seg på liste/excel-ark med systemer i prioritert rekkefølge. Listen ble etter kort tid redigert noe for å få på plass eksempelvis nevnte låssystemer. Kriseledelsen var ifølge ATEA mest

opptatt av pasienter og liv og helse. Men også i tillegg, fordi ATEA avdekket i samtaler med VISMA at del-systemet på deres side på den tiden ikke var kryptert godt nok. Der var det kun brukernavn og passord som var kryptert, mens pasientdata/persondata ikke var kryptert i databasen, slik som kommunen trodde. På dette tidspunktet var team fra ATEA inne på det mørke nettet og så sa at det var det var publisert at noe hadde blitt tatt, men det var ikke lagt ut noe ennå. Dette ble kommunisert til kommunedirektør og IT-sjef. For øvrig hadde sikkerhetskonsulenten en eller to samtaler med Kripos hvor vi påpekte hvilken det mørke nettet det lå på. Det var kommunen som anmeldte forholdet og ATEA ga bare noen detaljer til Kripos. Også NSM var i kontakt med sikkerhetskonsulenten for noen detaljer.

Hvem var dine ulike kontaktpersonene i Østre Toten kommune (hvem ble det eskalert eller de-eskalerte informasjon til)? og Var du kontaktperson for noen utenom Østre Toten kommune (eksempelvis for etterforskning eller annet)?

*kommentar: Svar på første og andre spørsmål her overlappet i stor grad, derfor er svarene slått sammen under en felles bolk.

Ordfører var hovedsakelig i kontakt med IKOMM og kommunedirektøren og forskjellige typer media, samt med kommunestyret og formannskapet. I formannskapet var det orienteringspunkter fra ordfører og kommunedirektøren. Hendelseshåndteringen ble gjentatte ganger presentert i kommunestyret for å stadfeste og få aksept på at dette ble håndtert på en «akseptabel» måte, spesielt med bakgrunn i pengebruk. Det ble også tatt noen valg om hvordan IKT-drift og sikkerhet skal organiseres, særlig med tanke på å kjøpe drift av tjenester fra IKOMM, som også ble presentert i kommunestyret. Både kostnadene i seg selv, og også hvordan en endring av struktur for drift av systemene var beslutninger som kommunestyret må ta, i tillegg til å vurdere en del ekstra kostnader som du dukker opp underveis, med tanke på kompetansebehovet.

> «Hva du skal ha på hjemmebane utenom IKOMM for å ivareta sikkerheten våres fremover? Ikke bare sikkerheten, men digitaliseringskapasiteten kan du si da. At du har en slags oversikt over det og hva slags kompetanse på det som er slik at Østre Toten kommune gjør det på en fornuftig måte. Vi kan ikke bare gjøre det slik som andre kommuner gjør, vi må tenke på våre egne behov, og bestille fra IKOMM, og tenke på vår egen utvikling på det området her da. Det går både på digitaliseringskapasitet og sikkerhet, egen sikkerhet da. Så der har vi ansatt en del folk, så jeg tror vi bruker like mye penger på dataavdelingen vår nå, selv om vi har outsourcet. Så vi bruker like mye her hjemme nå som vi gjorde før datainnbruddet. Det er en helt annen situasjon og en helt annen kapasitet på den avdelingen nå da. En helt annen kunnskap. Min oppgave og kommunestyrets oppgave er at de beslutninger som innebærer bruk penger og som involverer på en måte å godkjenne den måten å gjøre det på som kommunedirektøren på en måte egentlig har bestemt, det er jo fagkunnskap ikke sant, og vi har veldig tillit til måten som kommunedirektøren har løst det på, og det gjør at det har vært lite debatt på en måte i kommunestyret fordi på en eller annen måte så har vi fått til det at kommunedirektøren har hatt god tillit og har hatt trua på at vi skal løse dette her.»

Ifølge ordfører var det stor enighet i kommunestyret om måten å gjennomføre arbeidet på.

> «Mye var rundt hvordan vi startet med kommunikasjon eksternt og internt den dagen vi ble rammet av det. Jeg tror at det er en sammenheng med at det er vært ganske troverdig og inngitt tillit tross alt. Derfor har vi fått ganske stor tillit i kommunestyret. For det er jo en ganske stor mulighet til å miste tillit da, når du ikke klarer å passe på dataene dine. At du ikke klarer å unngå at noen bryter seg inn hos deg, så er det en veldig stor mulighet til å miste tillit og det blir veldig, veldig stort behov for å gjenopprette den tilliten, og det er mye lettere å miste sitt gode rykte enn å gjenopprette det da. Men jeg tror det har klart å beholde tillit gjennom intern og ekstern informasjon, det har vært ganske stor ro rundt dette her, ganske tverrpolitisk enighet om gjenopptak, ja gjenopprettelsen.»

Ifølge kommunedirektøren var det ingen plan for å ha IKT-personell i kriseledelsen. IT-sjef ble allikevel innkalt i kriseledelsen når hendelsen skjedde, for å gi status på gjenopprettingsarbeidet. Etter hvert så ble det utpekt en ansvarlig for hendelseshåndteringen på IKT. Da ble møtte han i tillegg i kriseledelsen sammen med IT-sjef.

> «De ga status i forhold til; i begynnelsen så var det jo beskrive hva som hadde skjedd, og så etter hvert så var det jo status i forhold til gjenoppretting og når vi kunne forvente å få systemer oppe da. Og etter hvert som vi etablerte oss og fikk se omfanget så var det jo prioriteringer om hva som skal gjøres først.»

Kriseledelsen hadde da (under ledelse av kommunedirektør) Statsforvalteren i ulike møter, de hadde inne kommune-CSIRT som ga noen opplysninger sånn som de så det, og de hadde inne KS. Kommunedirektøren oppfattet at alle disse hadde en rådgiverfunksjon. Dernest ble det i noen grad delt i to, altså det som handler om IKT, gjenoppretning av systemene, hvordan for det første de skulle håndtere det. Og for det andre samtidig å jobbe med selve driften, hvordan driver man en kommune uten systemer, hvilke konsekvenser får det. Sistnevnte ble håndtert gjennom sektorene.

> «Nødprosedyrer og drift ble satt i gang, spesielt innenfor helse, omsorg og velferd. Det var jo veldig kritisk selvfølgelig. Men detaljene rundt det ble ikke tema i kriseledelsen. Det håndterte kommunalsjefen. Så var det spørsmål som gikk på tvers, for eksempel behov for vakthold, for beredskap og strøm, vi fikk jo også strømstans, så det ble behov for aggregater og sånn. Det var jo da tatt med eiendom og da hadde vi jo eiendom inne sånn som jeg husker det; når det var spørsmål om hvilken kapasitet vi hadde på aggregater, altså aktuelle problemstillinger da. Og så etter hvert som dette utviklet seg så var det jo organisert i forhold til dette med lekking av data, og da ble de jo tatt med inn i kriseledelsen når det var noen spørsmål angående det. Og så har det jo vært en veldig viktig ting og det går på informasjon. Vi har jo en informasjonsmedarbeider - en kommunikasjonsmedarbeider med hele veien selvfølgelig. I den første fasen så var det jo veldig mye informasjon både innad og utad som gikk på konkret på det og hvordan ansatte skulle forholde seg, og da var det vi hadde disse spørsmålene hva trenger vi, hvordan skal vi samle

> dette, og så ble den utførende biten gjort av de kommunale sektorene sammen med kommunikasjon.»

Kommunedirektør innrømmer at han ikke visste hvilke nasjonale ressurser som finnes innenfor informasjonssikkerhet, og at dette var noe han måtte finne ut av selv.

> «Så den jeg var i kontakt med, eller den jeg rådførte meg mye med var den som har et ansvar IKT sikkerhet i KS. Han kunne gi meg råd i forhold til da, hva trenger du av eksperter rundt deg, hvordan bør du organisere arbeidet, så det fikk vi veldig raskt på plass da.»

Spesielt gjaldt dette system-sikkerhet, hva man trenger rundt det, deri ekstern ekspertise. Dette arbeidet ble ikke ledet av kommunedirektør selv, men resultatet av arbeidet ble tatt med inn i kriseledelsen. Ett eksempel i denne forbindelse, var analysene av pågående og kommende gjenopprettingsarbeid, og deri anbefalinger fra eksterne eksperter på å følge et annet spor (outsoursing). Det rent tekniske var aldri kommunedirektør direkte borte i. Kommunen fikk også en ekstern henvendelse fra Cyber Forsvaret hvor disse bare ønsket å bli orientert, så ordfører og kommunedirektør hadde et møte med dem, hvor de informerte om det de visste. Det kom heller ikke noen gode råd eller tilbakemeldinger fra dem.

For øvrig var det kommunedirektør som anmeldte hendelsen til politiet i tråd av den delegerte myndigheten han har til å gjøre dette. Han hadde etter hvert som hendelsen skred frem mye kontakt med politiet. Det kommer her litt an på hvilken fase man er i, fordi da de leverte anmeldelsen, etter hvert som det kom spørsmål om dette med informasjon på avveie og misbruk av data, opplevde kommunedirektør at han hadde god dialog med politiet hele veien.

> «Vi fikk en del henvendelser fra publikum om «kan min bankkonto være misbrukt sånn og sånn» og hadde direkte kontakt med politiet og sendte de sakene over. Og vi fikk tilbakemeldinger om at de ikke hadde funnet noe som kunne knyttes til hendelsen da. Senere sent på høsten så ble jeg også invitert inn i et møte med NC3 altså Kripos NC3, hvor jeg fikk en orientering om etterforskningen rett og slett. Jeg tror kanskje at de som har ansvar for de tekniske undersøkelsene, vi hadde jo det som et eget spor, jeg tror kanskje de ga informasjon til Kripos, men det var ikke sånn som jeg var involvert i. Jeg ble kjent med at Kripos hadde skrevet en rapport om gjenopprettelsen og da vil jeg ha den rapporten, da vi mange runder for om vi skulle få den utlevert rett og slett. For å få vite hva de hva de visste.»

Skolesjef satt ikke i kriseledelsen, det var kommunalsjefen som satt der. Hun sitter i det de i Østre Toten kommune kaller BOO-ledergruppe (barn, oppvekst og opplæring). Denne gruppen hadde ledermøter med sin kommunalsjef, hvor det ble gjennomført beredskapsmøter og referert fra kriseledelsen. Skolesjef hadde jevnlige møter med rektorene der hun videreformidlet informasjon fra kriseledelsen fra kommunalsjef for oppvekst. Dialogen med andre slik som IKT avdelingen, gikk gjennom skolesjefens rådgiver, men det kunne til tider være krevende å «nå frem» med de spesifikke utfordringene som grunnskolen hadde. Det varierte ifølge skolesjefen litt, men det begynte med at skolekontoret hadde noe dialog med IKT avdelingen på rådhuset som hun hadde dialog med, men seinere i prosessen så hadde skolekontoret tett dialog med

gjenopprettingsansvarlig og IKOMM (i den grad de kunne gi de svarene skoleorganisasjonen trengte). Etter hvert ble det kun IKOMM som kontaktpunkt.

Han som ble utnevnt som innsatsleder IKT, koordinere all aktivitet som hadde med hendelseshåndtering IKT å gjøre, altså unntatt det som gikk innenfor den enkelte tjeneste i kommunen, hvor de måtte legge opp til manuelle rutiner. All koordinering rundt kommunikasjon, ekstern bistand, kommunikasjon med Kripos, NC3, NSM, etter hvert da med andre eksterne ressurser som de byttet ut med ATEA IRT (med ressurser fra KPMG) osv. Etter hvert kom det også på koordineringen med personvernsarbeidet, GDPR, rapportering på det, hvor innsatsleder IKT ble noe involvert i arbeidet med dette. I den gruppa var IT-sjef, den tekniske ressursen i kommunen som hadde mer eller mindre styring på gjenoppbyggingen av infrastruktur, og etter hvert kom en ekstern ressurs inn som arbeidet med juss-spørsmål, personvern og litt på GDPR, og også etter hvert eget personvernombud (innleid fra Gjøvik) som gjorde en del rapportering til Datatilsynet. Altså flere eksterne ressurser, men det var hovedsakelig KPMG sine hendelseshåndteringsfolk og etterforskningsfolk som satt i denne gruppen til å begynne med.

> «Vi hadde slike møter i begynnelsen hver morgen, etter hvert så gikk vi over til å ha det mandag, onsdag og fredag, og da skrev vi et levende referat fra hver gang på en måte i tilfeldigvis ei powerpoint-fil, og der er det en boks per område. Rådgiveren fra KPMG var på en måte min assistent, selv om jeg var kanskje like mye hennes assistent, for hun hadde jo erfaring fra faget og feltet. Vi to på en måte koordinerte dette sammen, og hun hadde da dialog med og hjalp meg med å kalle inn til møter og delta i møter med NC3 (Kripos) og NSM og også kommuneCSIRT til dels. Da var det jeg som deltok, det var henne og en rådgiver til fra KPMG som var en av de andre viktige i håndteringa som sto for den tekniske etterforskninga. Så vi fikk på en måte to hovedroller til, pluss at det var vi tre da som deltok i møter med NC3, NSM og ja, representant fra kommuneCSIRT var veldig pågående, så han fikk være med i noen av de møtene der. Han hadde jo ingen rolle i det, han var bare veldig klar og villig til å hjelpe, og veldig nysgjerrig på utviklinga, så han var med i noen av de samme type møtene da. Det som skjedde i de møtene, var jo bare at vi oppdaterte NSM og Kripos.»

Det var kontinuerlig overvåkning av darkweb fra eksterne ressurser (KPMG). Her også en som egentlig driver for seg selv med teknisk etterforskning, og ifølge innsatsleder IKT en av Norges beste eksperter på akkurat det, og i denne hendelseshåndteringen altså innleid fra KPMG. Han var ifølge innsatsleder IKT helt sentral i dette arbeidet, sammen med nevnte rådgiver («assistent») fra KPMG.

> «Litt sånn av historiske årsaker, og organiseringen og sånn, når vi ikke hadde møter i kriseledelsen, det hadde vi ofte for så vidt, da var det veldig naturlig for både meg og IT-sjef å snakke med økonomisjef, som satt i kommunedirektørens ledergruppe og som hadde lang fartstid og for så vidt beslutningsmyndighet ift. økonomi. Så vi drøftet jo veldig mye med ham i de tidlige fasene, for vi måtte jo, dette kostet jo en haug med penger som ikke var behandlet noen plass, så vi måtte bare ha en ryggdekning fra ham. Men ut over det, så var det i kriseledelsen som vi hadde møter i.»

På teknisk etterforskning så handlet det jo om å gi tilgang på data, det var behov for overføring av data (eksempelvis ifra et teknisk miljø til et annet), som ble koordinert og prioritert fra denne gruppen. Samtidig med etterforskningen bygde en i begynnelsen opp ny infrastruktur, så man var dobbelt avhengig av de samme ressursene. Dette innebar koordinering og prioriteringer og selvfølgelig kommunikasjon, hvor de hadde med seg kommunikasjonskonsulent fra kommunen. Vedkommende bidro til ekstern kommunikasjon, blant annet hjemmesider og media.

Sikkerhetskonsulenten fra ATEA hadde i tillegg til kontakt med IT-personell i kommunen, også kontakt med kommuneCSIRT. Dette ble beskrevet som mer en briefing av saken og hvordan og hva de hadde funnet ut underveis egentlig. Kommune-CSIRT-en var veldig interessert og ville gjerne få kjennskap til funn, og prøvde også å gi noe råd underveis, men det ble beskrevet at det var vanskelig å benytte seg av rådene siden alle systemene var nede.

Økonomisjef var i kontakt med Husbanken ved flere anledninger, men vi hadde også flere digitale møter med KLP som viste, ifølge økonomisjefen, en faglig forståelse, men også en kunnskap om hva kommunen var utsatt for. KLP stengte aldri ute kommunen fra sine systemer. Det gjorde imidlertid Husbanken og flere andre statlige organisasjoner. Spesielt i plan og bygningsmyndigheten som kommunen hadde forhold til, det vil blant annet si Kartverket.

> «Internt har jeg jo folka mine i avdelingen, vi måtte jo finne ut hvordan skulle vi kunne utføre det absolutt nødvendige av jobb når alt var borte. Så fant vi ut i fellesskap med Gjøvik kommune at vi kunne teknisk sett få tilgang til våre økonomi systemer og lønnssystemer som ikke var berørt av datainnbruddet fordi at systemene var driftet av Gjøvik kommune. Men vi hadde jo ikke tilgang til Gjøvik kommune, så den tilgangen var borte, men systemet var ikke berørt. Så da etablerte vi en midlertidig tilstedeværelse i Gjøvik rådhus for noen av folkene mine og noen andre folk, og så bygde IKT på Gjøvik en teknisk tilgang for noen av folkene våre slik at de kunne sitte i Gjøvik rådhus og jobbe på vårt økonomi-, personal og lønnssystem i denne her perioden. Og det klarte vi å etablere i løpet av en dag eller 2 eller 3. Det samme gjaldt også for ressursstyringssystemet for omsorgssvikt som ikke var berørt. Altså, de andre systemene som da ble driftet av andre enn Østre Toten kommune som i utgangspunktet var uberørt av datainnbruddet.»

Det var altså tilgangen til systemene som var borte, og det ble kommunisert med personell via telefoni eller privat mail i den første fasen. Økonomisjef sine primæroppgaver var tredelte, den ene var å sørge for at eget personell hadde muligheten for å jobbe. I utgangspunktet så kom de til et tomt Gjøvik rådhus på grunn av at det er var midt i corona-krisen, så det var jo hjemmekontor på stort sett alle ansatte i Gjøvik, mens de fikk lov til å disponere lokaler der. Dermed var det en del praktiske ting som måtte få på plass, så økonomisjef var mye innom på Gjøvik den første tiden. I tillegg var det personell med kompetanse på omsorgssystemet som også fikk jobbe fra Gjøvik. I tillegg deltok økonomisjef i kriseledelsen, og i ledergruppa som også var preget av denne situasjonen.

Hva er det viktigste du lærte under hendelseshåndteringen?

Ordfører:

> «Jeg har jo lært at IKT, jeg har jo kanskje lært det i fra før også, men man tar det for gitt da, at det ligger i bunnen for alle tjenester som kommunen har. Og kommunen har utrolig mange forskjellige virksomheter innenfor sin virksomhet da, selv om det er oppvekst og helse som er hovedoppgaven, så er det jo på plan og bygg og mange andre, altså det en mangslungen virksomhet. IKT er en sånn grunnkapasitet som vi visste vi var avhengig av, men var det litt overraskende at du er så avhengig av det allikevel. Og vi tar det for gitt da, så for 2 år siden kunne vi kanskje tenkt oss at vi skulle bruke mer ressurser på IKT og sikkerhet på IKT, men hvis vi skulle tatt det opp i kommunestyret ikke sant, så blir jo det satt opp mot lærere og sykepleiere og vanskelig å få flertall for å putte enda flere folk inn i rådhuset. For en kjenner seg igjen, når det skjer en sånn hendelse så har det vært mye lettere for oss putte ressurser inn i trygghet til en grunnleggende sikkerhet der, og jeg tror kanskje når vi har fortalt om dette til mange så er det gjort litt inntrykk sånn at noen andre kommuner og putter litt mer ressurser i sikkerhet. Nå var det jo noen manuelle rutiner som fungerte. Hvis du vet om en sykdom som en pasienter så er det jo kanskje en fordel å vite hva slags medisiner den har fått den siste måneden, og det hadde vi altså. De hadde rutiner rundt dette, så sikkerhet ble ivaretatt, men når IKT mangler, så er det jo så utrolig tungvint og det skal journalføres og alt det der, så det føles som å ikke ha det nesten da. Jeg tror at innbyggere i Østre Toten kommune nesten ikke har merket noen ting av det her. Fått regninger for sent og sånn, men dette har vært et problem for organisasjonen, for folk som jobber i Østre Toten kommune. Jeg tror innbyggere merket utrolig lite av det. Den vanlige innbygger som ikke jobber i kommunen. Noen har merket mer av det enn andre, men det har vært relativt lite merkbart og det kunne vært mye verre hvis datakapreren hadde offentliggjort mye mer. Da kunne det blitt en enda større utfordring, og det var en kjempeutfordring det i april, men kunne det vært mye verre. Mye mer ting som kan være mer sensitivt - at personopplysninger kommer ut om en av dem som er på læringssenteret og litte gran om det, og mange andre tjenester som har oppbevart mer sensitiv informasjon om folk. Byggstyring ble råket, og det var jo midt på vinteren og kaldt så det kunne jo vært fare for folk i disse byggene, og verdier i disse byggene hvis vi ikke hadde fått passet på. Så det kunne jo gått ordentlig galt med både folk og verdier.

Kommunedirektør:

> «Jeg vet ikke om du kommer tilbake til det, men når det gjelder lovverket rundt dette, altså kommunal beredskap, lov om kommunal beredskapsplikt sivile beskyttelsestiltak, og Sivilforsvaret, så er det jo sånn at jeg er kjenner jo til loven selvfølgelig, men disse lovkravene der, jeg har skjønt det sånn at det er et lovkrav på rapportering fra kommunens side ved hendelser, og detaljer rundt det har ikke jeg kjent til. Jeg har en beredskapskoordinator, og det er klart at når vi har en hendelse i kommunen så skal vi rapportere til Statsforvalteren og sånn, men detaljene rundt det, hvilke krav som lå til kommunen rundt det har jo blitt bedre kjent med i ettertid da.»

Kommunalsjef helse og omsorg:

> «Jeg sitter jo igjen med at det er ingen krise som er lik. For nå har vi jo hatt både den krisa og coronakrisa, og det er ingen krise som er lik, men det å se hvor ressurskrevende det her har vært det er i hvert fall en erfaring jeg tar med meg. Og så var jeg nok forberedt på at det kom til å ta tid å komme opp igjen og bli gjenoppretta, det så jeg også. Og så ser jeg jo at min egen adferd har endra seg når det kommer til detta her, jeg er jo ekstremt mye mere skeptisk, og mye mere reservert på å trykke på ting, og det gjelder jo både PC-er og telefoner og alt som er. Men så er det jo kanskje slik at du skulle ha trykt på den «greia der», og så blir det sånn så. Så både holdnings- og kompetansearbeid er det jeg har med meg i fortsettelsen, hvor viktig det er. Når det gjelder organisasjonen, så er det vel i enda større grad systemer som fanger opp denna risikoen og sikkerhet, men kanskje også mer automatisert systemovervåkning som går på sikkerhetsmonitorering og driftsmonitorering og ikke minst oversikt over hva vi har av utstyr rundt omkring og risikoen knyttet til det da. Det er jo et kjempestort udekket behov, og et kjempestort område å dekke. Og spesielt nå i et moderne digitalt samfunn, hvor folk jobber alle steder, vi har jo med pc-er, og mobiltelefon er jo med samme hvor vi er. Da handler det jo ikke bare om telefon eller pc-en, men det handler om hvordan håndterer du informasjonen som tilflyter om det så er på papir eller digitale flater da, hva gjør du med det? Det handler jo om grunnkompetanse, og så er det mye holdningsarbeid knyttet til det og.»

Økonomisjef:

> «Det er kanskje det kanskje 2 ting jeg har lært spesielt, og det ene er at det er deler av vår organisasjon som er har godt planverk for alternativ drift, spesielt i omsorg. Det er gjort planer for å kunne drive kommunen manuelt noen steder. Og andre steder var det å finne ut hvordan skal vi kunne drive en virksomhet som er digital, men som nå ikke er det. Hvordan skal vi da fylle våre forpliktelser overfor innbyggere, og også for leverandørene våre, og hvordan skal vi sikre økonomien til våre ansatte? Så vi la vel i utgangspunktet, i avdelingen min, så la vi jo i utgangspunktet alle sånne formelle ting veldig mye til side. Altså så improviserte vi, og jeg fikk jo nødvendige fullmakter. Kommunedirektøren ga meg alle fullmakter på vegne av alle ledere i Østre Toten kommune til å foreta fakturabehandling, for vi har jo en digital fakturabehandling. Det var kanskje 70 stykker som var involvert for at alle fakturaer skal bli kontrollert og attestert og anvist. Jeg fikk den ene fullmakten som jeg fikk lov til å delegere til regnskapssjefen slik at vi kunne utøve denne fullmakten i fellesskap. Så vi behandler jo alle fakturaer manuelt, men vi klarte å oppfylle forpliktelsen juridisk til å betale. Det var relativt mye arbeid. Vi hadde ingen mulighet for å kunne fakturere alle fakturaer ifra alle systemer, vi har jo vel av systemer som genererer grunnlag for det som til slutt blir en faktura. Selve fakturasystemet var operativt fordi at det var en del av dette økonomisystemet vårt som da ble driftet på Gjøvik, men grunnlaget som skulle komme i fra de øvrige systemet var dels borte. Så vi gikk et løp igjennom hele porteføljen for å finne ut hva det er vi klarer å få til og hva er vi da må informere om at vi ikke klarer å få til. Vi fant ut at ja vi kan få (fordi vi hadde

skyløsning på noen systemer som gjorde at etter at vi kom på bane IKT, altså vi fikk etablert epost system og sånn) så fant vi ut at vi kunne fakturere barnehageregninger og SFO-rgninger. Så det gikk ikke så veldig lang tid før vi kunne si at det her fakturerer vi normalt, mens dette her typiske - eiendomsavgiftene som vi kaller det, som da går på vann og avløp og sånn, også eiendomsskatt, det hadde vi ingen mulighet for å sende faktura på. Så da måtte vi forberede våre innbyggere på det, og noen var sikkert veldig glade, mens andre da ble på en måte bekymret for at de ikke fikk betalt regningene sine. Så vi hadde et opplegg for det, vi hadde énsides annonser i lokalaviser, og vi informerte veldig mye på hjemmesiden om det. Og i ettertid så viser det seg at innbyggerne våre var fantastiske til å takle at de i løpet av et halvt år, for vi begynte å fakturere i begynnelsen av juli, og så i løpet av det halve året fakturerte det vi skulle fakturert på et helt år. Og det var fantastisk godt å registrere at innbyggerne våre taklet å få mange fakturaer på kort tid. Vi var jo på tilbudssiden, vi var ute, og vi sa, og vi kommuniserte i alle kanaler, at hvis dette medfører problemer for deg så skal vi finne de løsningene sammen. Det hopet seg opp med papir, fordi der vi normalt har digital dokumentasjon, eller dokumentasjonen i digital form, så ble det papirbunker. Og mange plasser inneholdt de bunkene personsensitive data, og vi var nok ikke de beste i klassen på oss sikre fysisk de dataene. Så det var nok kontorer som ja, kontordøra var låst, men på en pult eller et skap, så var det i en periode personsensitive data tilgjengelig. Det gikk litt tid før vi fikk fokus på det, og den fikk også en dimensjon inn i det gjenoppbyggingsarbeidet vårt som vi kom i gang med forholdsvis tidlig, at av de 6 eller 7 temaer som vi hadde, så var personvernet en del av det. Men det gikk litt tid i starten der vi da ikke hadde gode rutiner for å sikre fysisk til personsensitive data, dette bør endres i et evt. nytt beredskapsplanverk.»

Personvernombud:

«Det er jo litt sånn kanskje man skulle skrive mer om, hva slags kompetanse en slik varslingsgruppe bør ha, altså de som skal være med der. Det er jo ikke sikkert at folk er her. Jeg har ikke spurt kommunedirektøren om akkurat det, for det jeg vet at han orienterer jo meg om når det er noe, og jeg stiller spørsmål, og fokuset har selvfølgelig vært her så langt gjenoppbygging, så jeg tenker at dette oppdraget ditt da vil vel danne grunnlag for hvordan man tar dette inn. Men jeg ser jo at i sånne settinger, så tenker jeg at personvernombudet hvert fall må involveres og ha en viktig rolle. Jeg kan jo spørre så mye jeg vil og er jo sånn sett underlagt taushetsplikt også i alle retninger, men det hender jo det at man kanskje skulle vært observatør da i noen møter for å snappe opp om det er noe som man skulle ta tak i på noe vis. Ombudet kan ikke være «hands-on» og det er de kjempeflinke med her, jeg følger jo mange andre kommuner rundt omkring, og jeg ser at når man lyser ut en stilling hvor man skal både være personvernombud og ansvar for informasjonssikkerhet og personvern da tenker jeg at da har man ikke skjønt ombudsrollen for å være helt ærlig. Nå har vi en databehandleravtale for å se at dette er greit, DPI-er begynner man å bli veldig god på, og der har jeg hatt observatør-rollen for å se om vi gjør dette på en god måte fremover nå. Det jeg mener er å presisere at ombudsrollen må adskilles fra det å ha ansvar for informasjonssikkerhet og personvernsikkerhet. Ombudet skal påse at GDPR

er ivaretatt. Da jeg har nevnt databehandleravtale er det for å gi et eksempel på at jeg noen ganger blir bedt om å lese igjennom databehandleravtaler for å sjekke om de kan aksepteres. Hver gang vi skal ha opp et nytt verktøy, så har jeg tillit til at det fungerer. Så ombudsrollen må folk skjønne hva en måte er, ja også ute i kommune-Norge. Det er ikke å sitte «hands-on» og gjøre ROSen og DPIene. For hvordan skal du skrive en uttalelse på det som du selv har vært med og gjort som ikke går i retning av det du har levert. Altså i forhold til datasikkerheten så er det jo sånn rent personlig så er det jo også min kompetanse fra før av, jeg har også utdanning på dette, men jeg har ikke brukt den til så mye for jeg synes ikke det var så morsomt, men at det er svært nødvendig med å ha fokus og sikkerhet på systemene det er helt klart. En ting er i forhold til rollen min her, at man har en forordning som man må forholde seg til, og det må man gjøre, og om man tenker at den er tilpasset norske forhold eller ikke det tenker jeg også er en greie. Vi gjorde det og må jeg si, vi gjorde jo noen vurderinger også i den gruppa på det. Det var blant annet lekket noen referat fra AMU (arbeidsmiljøutvalget), og der står det hvilke fagforeninger som er representert og med hvem, og vi vurderte eller jeg da at i Norge så er ikke det det har ikke noe med liv og død å gjøre. Hadde det vært i Polen for 30 år siden så hadde jeg nok sett helt annerledes på det, men forordningen er bærer preg av å være skrevet av jurister som ikke har ikke skandinavisk kultur da, så jeg skrev også noen vurderinger på det, at det det vi ser hvilken fagforening man er organisert, at det det har kommet ut, men det jeg tar vi ikke så alvorlig da. Så den det er det som går på den ombudsrollen hvor viktig det det er å ha sikkerhet rundt det, hvor viktig det er å ha altså lukkede systemer, og det er jo også viktig for kommunen, altså i forhold til omdømme og sånn, at man også er nøye med hvordan man håndterer møtereferat og sånn på altså folk som vil etablere seg, altså det er noe med omdømme og det er noen må også til dels en variant av bedriftshemmeligheter, selv om ikke vi har så mye av det. Og jeg tenker jo også beredskapsplaner, det har ikke noe med Østre Toten å gjøre, men jeg fant jo tilfeldig for noen år siden i en nabokommune hjemme hele beredskapsplan, altså hvilke hoteller vi skal evakuere til, hvem som har hvilke roller, hva man gjør her og der, reservevann løsninger og alt mulig sånt, og da ble jeg veldig overrasket. Så jeg mener også sånne ting også, og jeg tror også kommunen skal av beredskapshensyn vurdere veldig strengt i forhold til forvaltningsloven hva man egentlig faktisk skal bør kunne unnta offentlighet. Det er også en greie som jeg tenker på som bør være en del av det hele. Jeg tror at det er lurt å være litt strengere enn det man egentlig er i dag. Nå har jeg også i veldig mange år vært politiker i min hjemkommune, og nå sitter jeg i utvalg for plan og næring og der har vi jo en del av disse, vi har ikke beredskapsplanene men vi behandler jo mye, og det er mye saksdokumenter og som jeg tenker at om er det noen som har litt ugreie hensikter så er det bare å gå inn på møteplanene. Det er noe jeg har tenkt veldig på i etterkant, at hvordan håndterer man det? Så er det jo det at man blir jo lammet da, jeg er jo glad når jeg begynte her at jeg også var på trått i 86, så jeg visste at jeg kan gjøre mye med penn og papir. Men så er det jo da etterpå, å holde orden på dette her, sørge for at ting som kommer inn er lagret, det som er arkivverdig skal ligge her og det skal ligge der.»

Fylkesberedskapssjef:

> «Vi lærte nok mest at dette her kan skje da, og vi hadde jo teoretisert litt rundt det på forhånd, og så videre, men at det faktisk skjedde på den måten var jo en vekker. Statsforvaler eller den gang Fylkesmannen hadde jo selv blitt hacket i 2018, så vi visste jo at det her kunne skje, men at det ble så omfattende i kommunen det var jo en overraskelse egentlig. Det var vel i hvert fall en oppvåkning, og når vi nå forbereder kommunen på noe sånt i ettertid, så er det veldig nyttig å ha Østre Toten hendelsen i bakhånd slik at du vet hva som er realistisk scenario og det er faktisk det her.»

Sikkerhetsekspert ATEA:

> «Man kan lære av hva det er å ikke gi bort for mye detaljer til pressen. Være åpen og ærlig, men heller ikke gi alle detaljer ut fordi det reagerte jeg på da, då jeg plutselig så pressemeldingen som gikk. Det å ikke kunne kontrollere informasjon som gikk ut fra hendelsen, da kommunikasjonsavdelingen ikke kunne håndtere informasjonen, så presse fikk jo fri tilgang til å intervjue sykehjemsleder og andre kommuneansatte og sånt noe, og det er jo ikke sånn IT-sikkerhetsmessig så veldig bra da. Når du gir informasjon så vet du ikke hvilke andre som hører på på en måte. Så det så det var jo en del av saken.»

Hva slags form for beredskapsplaner eller tiltakskort ble benyttet ift. ditt arbeid i krisehåndteringen?

Ifølge ordfører har det tidligere blitt gjennomført arbeid rundt beredskapsplanverk med tidligere rådmann, hvor beredskapsplaner ble vedtatt. Dette var imidlertid noen år tilbake, og etter det har det ikke vært oppe i kommunestyret. De hadde noen planer som de tok frem, men ordfører var usikker på hvor brukbare de var i praksis var for kriseledelsen.

I helse og omsorg er det beredskapsplaner, men det er ikke pekt på spesielt en cyberhendelse, men det kan være strømbortfall eller at systemer faller ned, noe det ifølge helse- og omsorgssjef har vært bevissthet rundt. Og at det da har vært en minimumsløsning for beredskap for det å få tak i opplysninger. Hun beskriver at dette i hovedsak har dreid seg om fagsystemet, da man har hatt en opplevelse av at dette systemet kan være ustabilt. Dermed har dette vært fulgt opp, og man har hatt beredskapsplaner for å håndtere slike situasjoner. Hun mener allikevel at det kan være et stykke ifra det man sier man skal gjøre til etterlevelse, men at det var veldig heldig at de i den fasen hadde tilgang på de aller nødvendigste data.

Ifølge økonomisjef forholdt de seg i utgangspunktet til den overordnede beredskapsplanen, selv om de har en stabsfunksjon, men det var mye de opplevde som ikke var tenkt på. Beredskapsplanen i Østre Toten kommune hadde ikke tatt høyde for at de skulle utsatt for det de ble utsatt for.

> «Vi har litt om flom og flyulykker og kanskje også alvorlige ulykker ellers, streik og sånn, men at vi skulle bli satt tilbake til penn og papir på syttitallet, det har vi jo nok ikke planlagt noe særlig. Ja, så det er jo også et læringspunkt her, at den situasjonen kan oppstå.»

Personvernombud hadde ikke sett på det, men i kvalitetssystemet så ligger det ifølge henne en god del beredskapsinformasjon. Hennes rolle er imidlertid ikke så godt beskrevet, men det er godt lagt til rette for at når man varsler avvik hvor det kan være aktuelt å få en uttalelse fra personvernombudet, så har det ligget der også før, og det er ifølge henne utvidet.

> «Så det avvikssystemet vårt det synes jeg er bra, og jeg opplever at det fungerer når man først melder. Men hvor god man er til å melde, det generelt er nok en diskusjon. Så det å melde avvik det kan man nok med fordel gjøre mer av, men jeg tror at den kulturen er litt å jobbe med. Man melder på store ting, og jeg kan ikke si at jeg har hørt avvik som går i forhold til personvern som ikke er meldt, det har jeg ikke. Informasjonssikkerhetsavvik har jeg ikke sett noe til, men vet at det snakkes om det, det er jo snakk om animasjoner og litt sånn forskjellig. Men det bare hører jeg at det er det snakk om. Og det er også gjennom at jeg har overvært noen arbeidsmiljøutvalgmøter. Og der er det jo også et hierarki, for dette er sorterer jo også under helse, miljø og sikkerhet faktisk. Vi får stadig påminnelser, sånn husk ditten og husk datten, men hvor effektivt det er å bruke dette første skjermbildet som jeg kaller det, litt usikker på det. Så det kan det nok med fordel gjøres noe mer. Men tankene er der, men jeg kan ikke med hånden på hjertet si at det er noe alle har fått med seg og tar inn over seg, for det er å ta det inn over seg som er det viktigste.»

Hos Statsforvalteren har de tiltakskort ved bortfall av ekom og strøm som det går an å benytte seg av, og fokuset er på konsekvensen av denne type hendelser.

Sikkerhetskonsulenten fra ATEA mener man bør i skille på en vanlig hendelse og en sikkerhetshendelse. Det jo mange typer sikkerhetshendelser og det ATEA har gjort er å lage senario-bøker for alle typer hendelser, eller som han sier: «de mest vanlige «incidentene» da, som vi er borte i».

> «Sånn som de har lagt det opp i forsvarssektoren da, så har de først en overordnet sikkerhetsleder, og så har de en datasikkerhetsleder som har hele stemme og så har de da en «incident «manager, sistnevnte gjerne lokalisert sammen med datasikkerhetsleder i IT-avdelingen eller i hvert fall under IT-direktøren, hvor de da har litt forskjellige roller i en «incident» hvor dataleder rapporterer i myndigheter og sånt, noe mens «incident» manager holder i trådene rent IT-messig og «forensics»-messig da. Må prøve å ha den oppgaven jeg hadde da, i Østre Toten, og da med hjelp av eksperter, hjelpe kriseteam med å rapporter på hvor langt vi er kommet i forskjellige saker.»

Hvilke anbefalinger vil du gi til kommuner og andre organisasjoner?

Ordfører:

> «I den rapporten som kom og er skrevet av KPMG i forbindelse med vår hendelse så var det jo sånn at han som hadde ansvaret for sikkerheten i kommunen, altså rapporteringen til kommunedirektøren var det nok så som så med på sikkerhetsområdet. Vi leste det i KPMG-rapporten og at det kanskje ikke var så vits i å rapportere oppover heller for det var ikke politisk vilje til å

dele ut mer ressurser til dette området til sikkerhetsområdet med hensyn på data. Så var det jo sånn at den nye rådmannen bestilte jo informasjon om dette før dataangrepet, så jeg tror kanskje det kunne skjedd noe der, men mitt råd er jo at politikere etterspør sånn rapporter oppover i systemet, altså rapporteringer fra dem som er sikkerhetsansvarlige, at det kommer til kommunedirektøren og videre til kommunestyret sånn at man blir klar over hvordan situasjonen er. Først så må du vite hvordan det står til, og når rapporteringssystemet fungerer, og når du får vite hvordan det står til så får du muligheten til å agere ikke sant. Om du velger å ikke gjøre det da, men da er det på en måte din egen skyld da. Det første som alle bør være interessert i, det er det her å få rapporteringsrutiner til å fungere sånn at kommunestyret er klar over hvordan situasjonen er, hvordan risikoen er og hvordan det blir håndtert i den enkelte kommune. Min klare anbefaling er at man gjør det først og så er det sikkert mange forskjellige ting en kan gjøre for å få vite hvordan det står til. Hvis man ikke vet hvordan det står til så får man i alle fall ikke gjort noe. Det er viktig å ha en leder i kriseledelsen, hvis det er en spesiell situasjon sånn som det her på et på et visst fagfelt, så er det nok viktig å ha en ledelse som forstår problemet da. Det hadde jo vi i dette tilfellet her, og da kan vi følge egentlig den organisasjonsmodellen som vi har. Fra kommunedirektøren og utover i sektorene. Så er det nok viktig når det blir sånn spesielt som dette her, jeg opplever at en liten del av en kommune, som var en veldig viktig del en grunnleggende del ikke sant, så er det viktig å få tak i noen eksterne som kan gi råd da, på et tidlig tidspunkt, og at du klarer å finne ut en 2, 3 forskjellige aktører som du kan få råd ifra, sånn at det blir litt lettere gjøre de riktige tingene. Råd fra han fra KS på det strategiske valget i oppstarten, det tror jeg var viktig for oss da. Ja, de hjalp oss fra KPMG og andre, men på det strategiske gjenopptaket tror jeg han fra KS hadde mye å si for hvordan vi skulle ta oss opp igjen. Og hvilken strategi vi skal velge da. Vi var jo lenge inne på tanken om å ta oss opp sånn som vi på en måte var da, gjøre alt dette på egen kjøl, så det gikk en stund før vi innså at det ble for vanskelig da. Da tror jeg han fra KS var en viktig rådgiver i så måte. Så jeg tror det er lurt at en organisasjon som KS som er kommunen sin egen organisasjon og overordnede paraplyorganisasjon har noen ressurser som kan som kan gå inn i flere lignende organisasjoner og hjelpe til når det er spesifikke sånne kriser og problemer. Når det gjelder strategisk planlegging tror jeg det er lurt. I kriseledelsen så opplever jeg at beslutningene ble tatt i tråd med den organisasjonsplanen vi har, så det fungerte det.»

Kommunedirektør anbefaler først og fremst å følge NSM sine grunnprinsipper med hensyn til sikkerhetsstyring og drift av IKT kommunens IKT systemer. Han anbefaler også å planlegge for bortfall at flere IKT systemer samtidig, og å lage nødprosedyrer for bortfall av IKT systemer og ikke minst lage beredskapsplaner.

Kommunalsjef helse og omsorg:

> «Jeg tror det er viktig å ha beredskapssystemene i orden på det området her og, på lik linje med andre områder. Og det tror jeg har vært felles for mange norske kommuner, man har hatt fokus på skoleterror og sånne ting, som det kanskje er veldig mye lavere sannsynlighet at kommer til å skje, så det å innarbeide det i det ordinære beredskapsarbeidet, og ha orden i sysakene

sine og orden i eget hus, og det er jo det vi driver med nå, det er jo det å få opp rutinebeskrivelser, få opp varslingssystemer, hvem er det som skal ha beskjed, hva betyr dette her, og så må vi gjøre en vurdering og fordi det er jo klart økt sikkerhet gjør jo noe med både tilgjengelighet og funksjonalitet, det kan virke begrensende, og det er jo kvalifiserte valg som kommunen også må gjøre. Hva slags risiko er akseptabel å leve med? For sånn er det jo på alle andre områder også. Sånn sett skiller jo ikke dette seg nevneverdig ut. Men for mange av oss så blir dette her veldig ukjent terreng, ikke sant, mye av dette er jo begrepsbruk og språkbruk som vi og menigmann ikke forstår. Det blir veldig teknisk en del av det. Det er viktig å «tilgjengeliggjøre» det. Språk som gjør at folk forstår hva dette dreier seg om. Noe av dette har jo utviklet seg i en retning, som vi på en måte har akseptert, med mere deling på grunn av digitaliseringen. Og det er jo selvfølgelig noe av gevinsten også, men så må man jo da ta med seg ulempene, og et eksempel er jo det med kjernejournal, før så var det på papir, da måtte man be om å få det oversendt, eller si at det skal sendes hit og dit. Nå ligger det jo tilgjengelig for alle de som har tilgang på kjernejournalen. Det er jo ikke nødvendigvis slik at pasienten ønsker at alt det som står der, at alle skal vite det, men det ligger der det. Framtida vil sikkert også være slik at også pasienten får hånd om sin egen informasjon. Og at man kan gradere det i større grad enn sånn som det er nå. For jeg tenker at om jeg går til øyenlegen så har ikke den øyenlegen brukt for informasjon fra kjernejournalen som angår mitt underliv. Jeg syns egentlig det er gode eksempler. Og det er jo gevinster som alle heier på at vi skal få, men som ikke er nødvendig for alle å få. Og hvis jeg skulle velge å gå å kjøpe meg en privat helsetjeneste, så er det jo ikke sikkert at jeg ønsker at fastlegen min skal vite det. Så jeg har delte synspunkter om det med en journal. Det er ikke bare udelt positivt. Det som er en utfordring når du får en så massiv hendelse som vi hadde da, så er det det å få en god samordning på tvers, vi etablerte ganske raskt en god kriseorganisasjon, og vi har en kommunedirektør som er veldig god på informasjonshåndteringa, og som hadde en veldig bevisst tanke omkring at vi skulle være åpne. Og det tror jeg har vært kjempebra, og viktig, og det tror jeg Østre Toten har stått seg gått på, å være åpne på det som har skjedd. Men sånn vil det alltid være tror jeg, det å gå ut med informasjon, og det å få sikret at det er en god samordning. Det var hyggelige møter og jeg opplevde at det var veldig bra. Kan ikke si nå at det er noe som skulle vært annerledes akkurat i krisehåndteringa. Bortsett fra det jeg sa i sted, vi strevde i starten med å få god nok oversikt og det henger jo sammen med det vi snakker om nå, å ha god nok samordning da. Men sånn tror jeg det ofte er i oppstarten av kriser, sånn var det med corona og, det er litt krevende inntil man finner formen.»

Økonomisjef:

«For det første så håper jeg at ingen opplever det vi opplevde, jeg unner ingen det. En ting er selve hendelsen, det andre er hvordan dette påvirket oss i organisasjon, og tok all fokus. Vi som hadde mange planer og som hadde mange oppdrag i fra folkevalgte i kommunestyret, vi hadde jo nylig vedtatt et budsjett, og i det budsjettet så er det mange ting som vi har fått beskjed om å gjennomføre, og så må du sette mer eller mindre alt til side. Spesielt sett i fra mitt ståsted, som er en del av denne stabsstøtte funksjonen, ikke sant, vi skal

jo på en måte hjelpe alle til å bistå, legge forholdene til rette, vi skal hjelpe til med rapportering, og vi skal søke, og så videre… Den følelsen av å ikke kunne levere samtidig som over tid så jobber du så intenst, du jobber på adrenalin, så ser vi at det sniker seg inn slitasje. Og det er nok en ting som vi må trekke litt lærdom av at må observere hvordan det går med folka i organisasjonen. Er du ansvarlig leder så kan du hende at du takler det, men det er ikke dermed sagt at alle dine folk takler det på samme måten som deg. Det er noe som jeg kjent på litt i ettertid, at vi kunne med fordel ha vært mer observante og fanget opp slitasje. Jeg tror faktisk at det at noen med fordel kunne ha fått litt oppmerksomhet i den situasjonen de satt i, og blitt spurt hvordan det går, ikke bare forvente at det skal gå. Vi levde jo med denne datakrisen i tilnærmet ett år, vi sa jo at vi var i tilbake i tilnærmet normal drift i midten av november, det hadde gått 10 måneder, men vi var det egentlig ikke. Enda så er det en del som er berørt. Men dette her med, vi er i en middels stor norsk kommune, vi har de folka vi har og oftest så er det post type spesialistfunksjoner, veldig få, slik at vi satte jo sammen de beste folkene våre til å jobbe med, på en måte, denne gjenoppbyggingen, og det var på en måte ikke bærende å så gå ut og rullere og hente inn nye folk. Jeg tror at det er 2 ting, det ene er den observasjonen å prøve å fange opp hvor den er den slitasjen, og kanskje også å forebygge ved å sikre at noen får en liten pause. Jeg tror at vi vi hadde, altså helt rett i starten, så var det nesten 24/7 og da hadde vi noen fysiske pauser. Det var på selve hendelseshåndteringen, og når den første helgen var ferdig så måtte folk få lov til å komme opp på jobb på mandag klokka 10.00 i stedet for klokka 06.30. Vi måtte jo bygge en type organisering av alt dette, og alt dette er jo da både å finne ut hva det var som skjedde, hvordan skal vi forklare hva som skjedde, årsaken til at det skjedde, og hvordan skal vi bygge opp igjen punkt 1) den infrastrukturen som var nede og alle fagsystemet som vi fant ut etter hvert måtte bygges opp på nytt. Og, så dels brukte vi de samme folka på begge deler, og så fant vi ut at ja det var kanskje ikke det aller lureste, så vi endrer jo denne prosjektorganisasjonen vår litt underveis, ved å si at ja nå jobber du med infrastruktur, så jobber du med fagsystemer, men så gikk det ei tid, og så fant vi ut at nei nå på dette stadiet så ser vi alt under ett. Så vi endret jo både noe på folk, men også noe på måten vi jobber på. Og så trekker vi inn sånne såkalte perifere, ikke sant, ikke bare de harde tingene, men trekker dette med personvern og informasjonssikkerhet, den dimensjonen, inn i dette arbeidet. Og også kommunikasjonsdelen da. Vi brukte ikke mye tid på å finne ut at kommunikasjonen var viktig, men vi vi brakte kommunikasjon på banen med en gang. Så det jo en strategisk ledelsesbeslutning, at vi skulle være åpne, både internt og eksternt. Så vi var ekstremt åpne om dette hele tiden.»

Personvernombud:

«I hvert fall det å ha tenkt igjennom å ha, for det er jo det er jo særlig det med varsling som er viktig i forhold til forordningen, og at man har tenkt igjennom for det første hvem som kan være aktuelle eller hva slags kompetanse det er lurt å sette sammen. Så tenker jeg det er lurt der man har mulighet for å få vite og få hjelp til å gjennomgå informasjonen som er lekket, at en sånn type maskinell analyse i første runde, med at det er lurt å ha forvisset seg om - hvor kan vi kjapt få tak i det og få nødvendig hjelp til det. Så tenker jeg jo at det er

veldig viktig for hver eneste organisasjon å vite hva slags informasjon har de lagret. For kommune Norge så er det fra før fødsel til du er under oppløsning, så det tenker jeg der er det jo kjempeviktig. Men det betyr jo ikke at jeg tenker at alle organisasjoner er der, men det er klart at hvis vi skal se på mye, altså Mattilsynet har jo enormt med bare for å ta noen sånne ting som jeg kjenner til, informasjon som er superviktig og som kan også berøre noen, og fylkeskommunen har jo også mye på helse. Jeg gikk jo veldig fort telefon fra Nordland, så jeg har jo fått en god venninne der for å si det sånn. Hvor vi har bistått med alt (delt vurderinger og hvordan vi jobbet Østre Toten ble angrepet). De få henvendelser vi har fått, der vet jeg både kommunedirektøren har bistått enormt og jeg har gjort det, bare anonymisert våre vurderinger og stappet det ut, for å si det sånn. Så det å ha kontroll på hva slags type informasjon man har, som er innenfor de gruppene som er dekket av forordningen, det er i hvert fall viktig på personvern. Fordi at hvis du vet at det er en liten del som er stjålet og lekket og den lille biten ikke inneholder noe så er det jo egentlig ikke et stort problem. Så det er jo noe med å maksimere eller minimere her. Så det er et råd jeg ville ha har gitt. Og så har vel jeg opplevelsen av det er nok litt forskjellig da, men det er nok ikke alle ledere som er helt klare på personvernombudet rolle, og det er litt fordi at det har jo vært jeg har jo blitt kontaktet et par som har hatt noen utfordringer, hvor de på en måte ikke får bli med, og ikke blir delaktig fordi at man tenker ikke at det er en greie.»

Innsatsleder IKT:

«Skal jeg være helt kald og konkret, så må jo det være å være forberedt, og du må tenke beredskap også på det her området, ikke bare på de tradisjonelle områdene (der vi har beredskapsplaner). Det du trenger i en sånn setting er gode venner, og hvis du ikke har en plan og ikke har noen tanker om hvem som kan hjelpe deg, så blir det jævla tøft. Det er kanskje feil rekkefølge å bare starte med beredskapsplaner, man burde også begynne med å sikre seg selvfølgelig, mot sånne hendelser. Mine tips vil være å faktisk ha fokus på å sette av midler og bruke penger på riktige sikringstiltak. Og det er jo både tekniske sikringstiltak og alt mulig av teknologi som sikrer deg, men også det å styrke menneska oppi det hele da, som er en stor del av at det skal unngå at det skal skje med å styrke kompetansen der. Men tilbake til det med planer, der må jo tipset være at parallelt med at du sikrer deg teknisk, så du har en plan for hva du gjør når det skjer, og å ha avtaler med partnere som kan hjelpe deg, slik at du har kontaktinformasjon, navn, hoder, ansikter på plass når det smeller, og du må begynne å jobbe.»

Fylkesberedskapssjef:

«Ja det må jo være for det første å ha ting gjennomtenkt rett og slett, beredskaps planer er jo det viktigste man har da, men beredskapsplaner kan jo fort bli litt teoretisk, så man må jo slett tenke gjennom og kartlegge kanskje, hvis nå ting skulle bli borte, hvilke systemer blir borte, hvilke henger sammen som er avhengig av hverandre. Ser sånn som i Østre Toten er går noen systemer på egen kjøl, mens andre er avhengig av hverandre. Noen hadde de felles med Gjøvik, og de fungerte jo. CIM fungerer for eksempel. At man ikke

blir overrasket hvis man får et løsepengevirus, om hva som forsvinner, tror jeg er viktig. Og at man har lite-granne back-up planer og kanskje har beredskapsplaner skrevet ut på papir. Det du ikke har gjort på forhånd får du nå i hvert fall ikke gjort når det skjer tenker jeg. Altså hva er det som er spesielt med cyber-sikkerhetshendelser, en kommunedirektør er fortsatt en kommunedirektør så det er jo ikke noe å lure på. Vi anbefaler at en cyber-hendelse er som en hvilken som helst annen hendelse, så man må bruke de systemene man har. Det som jeg opplevde med Østre Toten, som jeg syns de gjorde bra, var de rigga jo to linjer med en gang. Den ene var en standard beredskapslinje, ikke sant og hvordan håndterer vi konsekvensene av dette her, og det er jo felles for alle beredskapshendelser. Den andre linja var jo den tekniske linja at man begynte å se etter hvordan man kan håndtere det tekniske aspektet da. Rense, bygge opp igjen på nytt osv osv. Som da ble ressurssatt med blant annet ATEA og KPMG og de folka der da etter hvert. Det synes jeg var bra de hadde de hadde et veldig bevisst forhold til hvilke konsekvenser fikk denne hendelsen som man måtte ordne opp i, altså blant annet dette med manglende etter-kriser på hendelsen for eksempel som er en konsekvens av en sånn hendelse. Så jeg tenker jo det at jo mer jo mer likt man klarer å håndtere konsekvensene med andre typer hendelser som man har øvd på, jo bedre er det. Da er man trygg i det man skal gjøre.»

Sikkerhetskonsulent ATEA:

«Så lenge du har en varslingstjeneste som fungerer, de skal jo ikke varsles om alt, men varslingstjeneste er jo at man får veldig mange varsler ikke sant, så det må jo kategoriseres etter kritikalitet, og det som oftest skorter på det da er jo når noen blir ringt opp, hvilke rutiner er det som ligger der, er det å ringe IT-sjefen og gjenoppbyggingsansvarlig og be dem etterforske pent, eller hvilke rutiner liker liksom bak der. Og så er det jo da å få eskalert riktig sånn at man får prioritert sakene riktig og bare når det er noen virkelig faktisk som ikke kan gjøre dette selv ikke sant. Så snart kommunen kan ta en beslutning når ting skjer, altså disse direktørene vil jo ikke bli ringt opp for all verdens ting ikke sant, så det er det er det å få finne den der balansen mellom det som er kritisk og det som ikke er kritisk, og hvor de rutinene som ligger bak der igjen da, hvilke beslutningsprosesser som gjøres snart virkelig er kritisk. Så er det jo det da, har du har vært utsatt for et sånt opplegg, velger man da å stenge ned hele kommunen for den minste ting eller har man et har man et edruelig forhold til det, det er også en greie da. Hvor gode rådgivere har de hos IKOMM eller hos andre, eller internt, for å for å ta de riktige beslutningene. For det første må du jo ha den riktige informasjonen til å ta beslutninger på og det innebærer jo at da de som sitter på den SOC-en klarer å være nok da, til å gi riktig informasjon. Vår egen SOC kontakter jo IRT når de lurer på noe, og vi ser jo at vi er hindrer en del falske meldinger til kunden fordi vi tar en edruelig beslutning på at nei dette ser ut som at det en «VPN som er nede», her må vi undersøke litt nærmere før vi kontakter kunden liksom. Det vi ser er at alle disse sårbarhetene blir utnyttet av kryptominere først, og så når de får tenkt seg litt opp så kommer da randsomware-bølgen eller APT-ene.»

Hvilke anbefalinger vil du gi til arbeidet med roller i krisehåndtering?

Kommunalsjef helse og omsorg:

> «Vi hadde jo etablert en struktur for at det var jo corona samtidig, så vi har nesten gjennom hele coronaen hatt ukentlig beredskapsmøter i sektoren, med alle lederne og ressurspersoner, og det har også vært tilgjengelig personer utenfor sektoren, altså renholdsleder, leder for vaktmesterne, fra bygg og eiendom som har vært med i det beredskapsmøtet. Så vi brukte jo det møtet og vi samla jo alle lederne + lederne i stab i dette møtet den lørdagen, og så fortsatte jo hendelseshåndteringen som en del av det beredskapsarbeidet vi allerede var i gang med. Så det å etablere en egen beredskapshåndtering i sektoren var ikke vanskelig, for den var allerede tilgjengelig. Og ganske tidlig også så dedikerte vi, vi har en stabsressurs, en fagrådgiver som har videreutdanning i beredskap, så han var jo ferdig med det da, og tok en aktiv rolle i å koordinere og håndtere noen av de tingene som måtte sentraliseres. Det er jo andre problemstillinger enn det det er i andre deler av kommuneorganisasjonen med tanke på det som går på digitale arbeidsplater og sånne ting. Det er stort strekk i laget på hvordan den digitale kompetansen er. Og bare det å kunne komme ut med beskjed til alle ansatte, er en kjempegreie, og spesielt når alt er utilgjengelig. Så han tok en veldig aktiv rolle, for å koordinere og følge opp, og det fungerte veldig bra innledningsvis, til vi hadde klart å komme mer over på et driftsspor egentlig. En stor utfordring i starten, det var at dette var relativt uoversiktlig i en tid, det er jo litt vanskelig å huske hvor lang tid, og mange prosesser var jo ikke jeg involvert i. Her er det jo mange fasetter, du har jo etterforskningssporet, du har gjenopprettingssporet, du har krisehåndteringssporet, du har informasjonsbehovet, det er mange fasetter da, som skulle håndteres. Og veldig mange av de var jo ikke vi sektorlederne involvert i, det ble jo håndtert av kommunedirektøren, kanskje alene da, opp imot politi. Opp imot sikkerhetsmyndigheter og den slags, og der var det jo sikkert konfidensielle opplysninger som ikke alle skal vite, og så det var ganske uoversiktlig i starten, og da hadde man fokus på at dette må vi bare få opp igjen. Og da gikk jo det til et punkt hvor det ikke gikk lenger, og da ble det tatt noen beslutninger som ga føringer for den videre oppfølginga. Så det er vel det jeg sitter igjen med litt, at veldig mye har kommunedirektøren håndtert sjøl opp imot de ressursene som har vært både eksternt og internt. Nesten en litt sånn task force gruppe da. Som har jobba med det. Det har vært greit for oss det, og vi har fått den informasjonen vi har hatt behov for, og så ligger det mye mer der, det veit jo jeg og, men av helt åpenbare årsaker så skal ikke det spres på flere enn strengt nødvendig.»

Økonomisjef:

> «Altså kriseledelsen vår er ganske bred bredt sammensatt og vi snevrer ikke den inn fordi at det var data og ulykke eller pandemi. De samme folkene var jo i kriseledelsen, så kommuneoverlegen var jo med når vi hadde kriseledelse om datainnbruddet. Så vi fikk jo med oss de her dimensjonene på hva gjør en krise med en organisasjon og for folk. Så egentlig så ivaretok vi det underveis, og så supplerte vi kriseledelsen med IKT delen, slik at IKT-sjefen kom inn, og

vi hadde vi hadde beredskapslederen hos statsforvalteren med oss i møter i kriseledelsen i starten, vi hadde kommune-CSIRT på banen som også deltok i møter med i kriseledelsen. Vi hadde en kriseledelse som behandlet datainnbruddet i utgangspunktet som en hvilken som helst krise, men som jeg har sagt litt tidligere, det var nok noen sånne elementer i dette som tok litt tid før det sank innover oss at det var viktig å ta på alvor. Og det var da med personvernet spesielt, og den sikringen av det, men også den med slitasje. Vi har vært åpne om det, og sagt det, skrevet rapporter, og i årsrapporten vår nå så vil det stå noe også om dette - at vi har en organisasjon som i løpet av året var preget av, og ikke bare en slitasje, men frustrasjon fordi at folk ikke får gjort jobben sin. Folk ble utålmodige, og så ble det gjort en forholdsvis tidlig prioritering av hvilke datasystemer som skulle prioriteres. Vi laget et såkalt bruttoliste: Den listen innhold i starten 240 systemer og system avhengigheter, for det er integrasjon nesten «all over», ikke sant. Så sa vi at liv og helse har prioritert nummer én, miljø nummer 2 og så får økonomien og alt det andre komme etterpå. Då det er klart at i dette bildet her, så er det noen som jobber med ting som da er viktig for dem og for det området de har et ansvar for, og så er det langt ned på prioriteringslista. Det var ikke utfordrende å informere om det, men det var kanskje utfordrende å registrere den frustrasjonen som det medførte i organisasjonen. Så kombinert med at folk måtte jobbe tungvint og ikke fikk utført jobben sin, og mange identifiserer seg med at de som skal nyte godt av det er den jobben de produserer, enten det er innbyggere, eller brukere, eller hva som helst, så blir de frustrerte på deres vegne. Fordi vi ikke blir i stand til, selv om vi klarte veldig mye i den perioden. Vi doblet i hvert fall kapasiteten med informasjon. Vi hanket jo inn folk som vi mente var gode på informasjon, og sa at nå er det informasjon du skal jobbe med, for det andre får vi tatt igjen en gang. Også på dette feltet her da, kommunikasjon og informasjon, så skulle vi håndtere dette parallelt med at vi hadde en koronasituasjon som også var en krise. … Hjemmesiden vår kom jo opp igjen forholdsvis tidlig og den ble jo også informasjonskanalen internt i organisasjonen. Og når vi skulle informere våre 1300 ansatte, så var det en type informasjon som også var åpent tilgjengelig for alle. For det var jo ikke et intranett vi snakker om nå, vi snakker om at vi brukte kommunens hjemmeside til å informere våre ansatte.»

Personvernombud:

«Nå tenker du Grethe på hvem som er ridder av det runde bord? Personvernet er også uavhengig av om det er informasjonssikkerhet eller ikke, personvern handler også om du er litt uheldig og har pcen din stående, altså det er mange ting, og man kan ha et ulåst kontor og det er papir som flyter. Så jeg tenker at personvernbiten er viktig egentlig uansett, ikke bare ved et cyberangrep da. Jeg har jo, eller personvernombudet har jo, en selvstendig forpliktelse til å stille spørsmål. Men det er klart at da må man jo virkelig sette seg inn i rollen og det skal jeg være ærlig å si, at hvis ikke dette hadde skjedd, så ville jeg nok selvfølgelig ha skummet GDPR og sånn, det ville jeg gjort, men jeg hadde jo aldri brukt (når jeg har 20% stilling), så hadde jeg aldri brukt så mye tid som jeg brukte på å være sikker på rollen min. For jeg sto jo litt alene (det er jo bare et personvernombud), altså du må ha du må jo ha integritet da, til å både stå imot det før du skriver, jo du kan jo også risikere å skrive inn uttalelser her

som er stikk i strid med det du vet at kommuneledelsen ønsker. For det kan ha en kostnadseskalerende side for eksempel. Så jeg tenker at det er viktig hva slags person som får en ombudsrolle, det er viktig. Og at jeg har vel lært at det å skolere seg, det må man faktisk gjøre selv altså. Så man bør ta kontakt med de nettverkene som er og jevnlig stille opp og følge med på det som foregår. Og da har man egentlig i den ombudsrollen, så har man et ansvar for også å stille spørsmål. Jeg vet ikke hvor ofte man har møter i kriseledelsen her, men jeg tipper at det er berammet og så avlyser man hvis det ikke er noe. Så er det klart at det kan hende at man burde fått være med som observatør når det når det er saker som tenderer da mot personvern, uansett om det er cyber eller om det er andre hendelser. Eksempelvis et innbrudd et sted hvor ansvarlig leder ikke er helt sikker på om dokumenter med sensitiv informasjon har ligget innelåst. Det er også noe med at selv om skapet er låst og du har gjort alt du skal og hele skapet er stjålet, da er det informasjon på avveie det må vurderes om det varsles. Jeg er ikke kjent med at vi har gjennomgått kan du si og kategorisert typer av informasjon som kommunen lagrer om noen som er rød, gul eller grønn. Man bør ikke gjøre alt, så det er ikke alt som bør gjøres så innmari stort, altså det er mulig å gjøre mye det er vi kanskje ikke like flink til. Vi skal ha store prosjekter og piloter og oldemora på alt. Det er noen ting som egentlig bare er å gjøre.»

Innsatsleder IKT:

«Når jeg satt der i den settingen, så satt jeg egentlig og drømte om at det skulle komme en slags sånn «cyber-swat-team» og bare komme med to store svarte lastebiler med mett med folk i og bare løse problemet. Det er spøkete sagt, men det er en viss sannhet i det, for det du trenger er folk som kan å navigere dette landskapet. Både på det organisatoriske med å koordinere mot de statlige instansene vi har som bryr seg om dette her, og det fikk vi god hjelp til med henne fra KPMG, som har jobbet i dette miljøet i årevis. Men du trenger jo det samme på teknologi. Dette her har skjedd, hva skal vi nå gjøre? Og det er jo egentlig et stort læringspunkt oppe i dette her, vi brukte jo 3,5 – 4 uker på å bygge opp igjen infrastruktur, som deretter ble skrotet når vi gikk til IKOMM. De 4 ukene var 100% bortkastet ift. den innsatsen som ble gjort på infrastruktur-siden. Og det var en konsekvens av at disse gode hjelperne våre pirket meg på skulderen en fredag og sa at dette vi gjør nå, dette som vi bygger opp igjen – infrastrukturen, det blir ikke bra nok, og dere kommer ikke til å klare å holde det på et nivå som er noe bedre enn det dere hadde før. «Dere mangler teknologien, og dere mangler kompetansen, her bør vi se på alternativer.» Det var rett og slett starten på en annerkjennelse som ikke alle er enig i, men i alle fall gikk den veien at IT-miljøet i kommunen var for dårlig både før, og vi så at vi klarte ikke å få det bra nok, sjøl om vi åpenbart hadde sikkerhet i fokus når vi bygde opp igjen infrastruktur. Og endte da opp med å gå til IKOMM, så den innsatsen over de 4 ukene på teknologi og infrastruktur ble skrotet, og så begynte vi helt på nytt igjen, men da med IKOMM. Alle som jobbet på IT-avdelingen ble overført til IKOMM, det som skjedde etter den verste akuttfasen, og etter at IKOMM hadde begynt å bygge opp igjen infrastrukturen. Selv fortsatte jeg i den her rollen som innsatsleder, men så fikk jeg et annet jobbtilbud som ikke har noe med hverken Østre Toten eller IKOMM å gjøre.»

Hvilke anbefalinger vil du gi til arbeidet med opplæring, trening og øvelser?

Ordfører peker på viktigheten av gjennomføring av øvelser i seg selv og nevnte at det ikke er så ofte de har det på forskjellige områder. Han mener at å sette opp «case» der man får et reellt problem slik man kan se at i den organisasjonen det er satt opp for, så kan det være forskjellig for en hendelse for en del av en sektor, men at du kan få noen øvet noen beslutningslinjer. Samt at man kan og ha en leder og en organisasjon som bruker det og får satt opp sånne øvelser.

> «Jeg tror ikke det er mange ordførere som har hatt flere krisemøter enn meg.»

Han mener derfor at det å ha realistiske øvelser litt oftere er viktig, at man ikke gjør det for vanskelig, og at man har det av og til. Han mener også at det å øve på å rapportere oppover i systemet på forskjellige ting, ikke bare på sikkerhet og på IKT, men også når det gjelder helsetjenester, sørge for at både varslingsrutiner og statusrapporteringer går som de skal, slik at man får vite oppover i systemet hvordan ting står til på en sektor.

> «For vi ser vi jo om du ikke gjør det, så kan det surre og gå i flere år, og når det først blir trøbbel da så, så blir det mye trøbbel, og da tenker jeg kan være lurt å etablere rutiner for å få statusrapporter fra forskjellige deler av den virksomheten som du har. Kanskje det viktigste er at du ikke lurer deg til å tro at det står bra til fordi du ikke hører noe. Man bør kanskje bli flinkere til å ha statusmøter for å få rapporteringer oppover i systemet. Hvis det blir en litt friere flyt av rapportering oppover i organisasjonen, så tror jeg det blir en sunnere organisasjon da.»

Kommunedirektør mener at det å være forberedt på at slike ting kan skje er viktig å øve på. Han kjenner kommunesektoren godt, og har vær med på en del digitalisering, og visste jo det at man kunne få utfallet av enkeltsystemer, men at det kunne få så store konsekvenser, var han ikke klar over.

> «At det var på en måte ikke så usannsynlig da - så man må lære det. Det er vel kanskje noe man tenker seg at det er ting som kan skje ikke sant…»

Kommunalsjef helse og omsorg mente det er viktig å øve på denne type hendelser. Heri stort og smått som å øve på hvordan man responderer på trusler, men også det å øve i og sammen med en sikkerhetsorganisasjon, og erfare hvordan den fungerer. Ergo øve på flere nivåer. Deri øve på phishing-trusler, hvordan systemene responderer på sikkerhetstrusler, det med sikkerhetsmonitorering og annen overvåkning.

> «Og så vil det alltid være utfordring når det kommer til det med varsling og varslingsrutiner. Og spesielt i en så stor organisasjon.»

Skolesjef mente at det er viktig å ta en overordnet vurdering. At alle tjenester er viktige, at eksempelvis skole er et stort volum hvor det er mange pcer, det er mye digital drift, alt fra skolekontor nivå, til administrasjon ute på skolen og til elevene. Hun hadde derfor ønsket en mer direkte link inn i kriseledelsen. I situasjonen som oppsto skulle skolekontoret informere 300 ansatte, og foresatte til 1600 elever. De fikk mange

spørsmål daglig, først og fremst fra de ansatte som sto i mange tekniske dagligdagse ting. Dermed mente hun også informasjon fra kriseledelsen som handlet om data og enhet skole skulle vært mer synlig på grunn av vansker med kommunikasjon som de opplevde og frustrasjonen rundt det. Ett av eksemplene hun trekker frem er dette med feilpålogging, og hvor mange runder man kan ha med det? Kunne det vært et par alternativer som lå beskrevet i en beredskapsplan, slik at når problemet oppsto så ville svaret være «sånn gjør vi det»? I tillegg mente hun at det også handler om hvordan man håndterer stress. Hvordan håndterer man en uforutsett situasjon der man skal prioritere?

I tillegg mener hun at man må øve for å være så godt forberedt som mulig. Og å øve på og å tenke igjennom hva man gjør hvis dette skjer. Hvordan får man informasjon ut til foresatte, hva skal man informere de ansatte om, hvordan kan man drive skole. Er man trygge på hvordan man har lagret data på servere om elevene, spesielt de dataene man har som er sensitive.

Personvernombud foreslår helt konkret oppgaver som man kunne ha gitt, hvilken informasjon kan være lekket eller er lekket, altså løse det og finne ut av det og kategorisere.

> «Det hadde vært en veldig god greie. Det er fra fordi at det er så innmari viktig og det er én ting er å oppfylle lovverket - nå starter man jo den kriminelle løpebanen så fort man egentlig begynner i en kommune sånn i ytterste konsekvens, fordi at ansvarsområdene nesten uansett hvor i næringskjeden man er så er det forpliktelser man har som er veldig lett å bryte, men alvorlighetsgraden av det er jo noe annet. Dersom viktig informasjon lekker her for en person som bor på sperret adresse for eksempel, så kan det ha en fatal konsekvens. Ja det har jeg lært mye om. Nå har jeg jobbet med mye forskjellig og jeg tenker egentlig ofte på at man skal være litt varsom der, men man ser liksom ytterste konsekvenser da når noe sånt skjer.»

Og for eksempel for å øve en type varslingsgruppe, så mener hun at hvordan den bør være sammensatt også er en viktig del av øvelsen. En kommune bør etter hennes oppfatning ikke rigge spesialister på alle disse områdene, men man må ha en plan for hvem man kontakter på samme måte som når man skal man skal evakuere, deri hvilken kompetanse bør denne gruppen bør ha. Og som hun sier «ligger det i planen, så er det jo egentlig å trykke på knappen og få de inn».

Innsatsleder IKT mener at Østre Toten, og dermed andre, burde ha risikoforståelse sånn at man skjønner at dette er en reell risiko og at det er katastrofalt hvis det skjer, eller når det skjer – for det skjer jo.

> «Du veit jo at det skjer, det skjer hele tida. De må ha risikoforståelse for at dette er noe som skjer, og hvor ille det faktisk kan bli i praksis. Og da trenger du jo kompetanse for å jobbe med risiko, du må skjønne trusselen, og hva det betyr når det skjer. Det er i alle fall kompetanse som offentlig sektor trenger. Og det tror jeg egentlig du trenger i alle kommuner. Jeg tror ikke du kan ha ei gruppe i KS eller ei gruppe i et eller annet departement eller noe, du må ha det ute der beslutningene tas. For den andre enden av dette er at vi må investere i ett eller annet, bruke penger og ressurser på noe, og da er vi tilbake til det jeg pratet på. Vi må bygge infrastruktur og teknologi, som i størst mulig grad

> lønner seg, du må bygge sikkerhetskultur, du må lære opp folk til å oppføre seg riktig i cyber-domenet. Og det vet jeg jo, ikke minst etter den her erfaringen, at selv om teknologien stopper så og så mye trusler, så er det alltid noen som kommer igjennom, da truslene utvikler seg hele tiden. Folka er alltid den siste skansen på en måte.»

I tillegg påpekte han beredskap, beredskapsforståelse og beredskapsplaner og å øve på dette.

> «For det gjør man jo ellers i beredskap. Du later som om noe skjer, og så prøver du å håndtere det. Det koster jo og tid og penger. Og da er vi tilbake til det å forstå hva det er viktig å bruke tid og penger på.»

Fylkesberedskapssjef mener at for å begynne med øvelser, så er det jo det å øve på det som kan bli potensialet, at man lager et scenario som her, men kanskje ikke absolutt alt, sette stab og trene ut ifra et kommune-perspektiv. Mot et undervisningsperspektiv mener han at man må være involvert i undervisninga, at man i tillegg til et teknisk aspekt også må se på overgangen til det operative perspektivet.

> «Hva dette har å bety for de som driver med den operative håndteringen, kommunedirektøren da, kommuneperspektivet og hva kommunedirektøren trenger å vite. Hvilke systemer er kompromittert, hvilke kan jeg bruke, kan vi bruke dem allikevel, ikke sant. Hvilke systemer er helt nede som vi ikke kan bruke, hva er konsekvensen av det, hvor lang tid tar det, hvilke deler av min bedrift er ramma, dette er jo sånne ting som kommunedirektøren vil vite om.»

Sikkerhetskonsulenten fra ATEA anbefaler at hvis man klarer å gjøre en øvelse på slike forhold så er det bra. ATEA kjører liknende simuleringer for selskaper, og etter deres erfaring, så klarer man da å finne ut hvem som er best egnet til det ulike roller, da det gjerne kommer opp litt fagkunnskap til de som deltar. Etter deres erfaring er det jo kommunikasjonsavdelingen eller fagenheter, som sammen som tar seg av det med pressen, mens det er kommunedirektøren eller tilsvarende som tar så selve politi/er ansvarlig for politianmeldelse og rapportering til statlige myndigheter. Gjerne med bistand fra IT-sjef.

> «CERT-ene har ikke noe annet enn en rådgivende funksjon slik jeg ser det, og har ikke annen mulighet enn å påvirke dem gjøre de antallet «patcher» og gjøre opp igjen oppmerksom på sårbarheter. … Det blir litt for ja, det blir mange CERT-er som rapporterer akkurat det samme. Det burde jo vært et samarbeid mellom de forskjellige CERT-ene og NSM i større grad synes jeg da, sånn at man kan få litt «intel» og noen prosedyrer rundt dette. Sånn som vi ser det nå så har jeg gjort en del modenhetsanalyser rundt omkring i forskjellige bedrifter og kommuner og det er veldig mange som ikke har en forskjell på en IT hendelse og en vanlig hendelse, slik som en flom eller strømutfall eller sånn, eller annet altså. En IT-sikkerhetshendelse, på en måte innebærer en del andre ting også; isolering, rapportering, kartlegging av hva slags data som kan være. Det er mange det er mange ting som er i tillegg i forhold til en vanlig innsats da.»

ATEA har hittil ved forberedelser til øvelser gjort en simulering på ledelsesnivå, at de har satt seg sammen i et «krisemøte». Som sikkerhetskonsulenten presiserte gir ikke nødvendigvis dette en god nok forståelse av at back-up er nede og utilgjengelig og hva dette faktisk betyr.

Hadde du tenkt på noe før intervjuet som du tenkte det var viktig å fortelle meg for at man skal lære av hendelsen?

Økonomisjef ønsket å formidle at de som er ansatt i kommunen er jo til for dem som bruker dem og som trenger dem.

> «Det er innbyggere i ulike settinger, noen ganger så er de jo da takknemlige, men noen ganger så er det noe krevede.»

Dermed mener økonomisjefen at det er viktig at kommune-samfunnet ikke stopper fordi at man opplever en krise, og det å ha høyde for at selv om man har en krise så må vi ikke glemme hvorfor man er til.

> «For en tid siden så hadde vi en øvelse knyttet opp mot at alle kommunikasjonssystemer var nede, og da hadde vi inn en tur som var god på sånn, som driver med radiokommunikasjon. Ja ulike typer måter å kommunisere på. Og det var lærerikt for meg i den forstand at det ikke bare finnes det noen tekniske løsninger du ikke vet om, men også da hva kan du få til hvis du er flink til å improvisere. Og jeg mener jo at det vi gjorde med å improvisere og få til at vi kunne jobbe for kommunen i en annen kommune, og vi brukte jo NAV i Vestre Toten til å være vårt system for våre NAV-brukere i denne perioden. Så hadde det noen sider i etterkant, for det er jo noe som skal avstemmes, men det var det å se etter muligheter utenfor kommunen da. Men jeg tror et læringspunkt vil jo være at det er noen grunnleggende regler i samfunnet som du ikke kan droppe selv om du er i krise. Det er noen lover som gjelder. Men se folkene dine, følg med folka dine hvordan det går, og særlig når det går jo lang tid. Og være åpen og ærlig. Så langt du kan. Jeg tror vi har tjent på det, jeg tror at våre innbyggere ville ha hatt en annen holdning til oss som organisasjon, men også til selve krisen hvis vi hadde satt lokk på den. Så jeg tror vi har tjent enormt på å ha en åpen og ærlig kommunikasjon underveis. Og ikke prøve å forklare bortforklare at vi ikke var gode nok.»

Han mener også at det er en viktig erfaring å ta med seg i det videre arbeidet at man måtte tenke strategisk fra dag 1, og det var noe av det mest krevende som de hadde vært med på.

> «Det at vi både skulle takle det at IT-folkene våre jobbet døgnet rundt, samtidig som vi da drev og planla for at de skulle slutte å jobbe hos oss. Fordi det tok 6 uker i fra dette her skjedde til vi da hadde fått tatt den strategiske beslutningen at vi ikke skulle gjenoppbygge vår egen dataavdeling. Så det var jo noen heftige timer der vi da drev og vurderte de ulike alternativene, og vi vi hadde jo ikke side opp og side ned med utredninger om dette ikke sant. «Dette er hendelsen, og vi skal bort i fra det, og vi skal forebygge dette». Om vi må da ta en beslutning, skal vi skal vi gjøre sånn, skal vi gjøre sånn, eller skal vi gjøre sånn – det finnes det noen prosedyrer når du har med folk gjøre.

> Og skal du gjøre endringer for folkene så finnes det jo noen etablerte prosedyrer for det, og så skulle vi gjennomføre det parallelt med at de jobber døgnet rundt for at vi skal komme opp igjen å gå. Det var relativt krevende, må si det. Og det var altså krevende å si at, ja i det øyeblikket vi har tatt en beslutning, så er det ingen vei tilbake. Vi jobber jo underveis med tanke på at ja nå skal vi komme opp å gå, og så og så kom det til noen punkter der vi hadde noen som fortalte oss at dette går ikke. «Vi klarer ikke å oppnå det de vil ved å gjøre det på den måten.» Det var krevende å parallelt jobbe i krise og samtidig jobbe strategisk for enhver framtid. I forlengelse av dette, når vi valgte da å legge ned vår egen IKT-drift/avdeling, så sikret vi jo de ansatte, det finnes jo mekanismer som ivaretar deg, men dette skjedde så konsentrert og når den beslutningen var tatt på en torsdag så skulle vi da få den nye samarbeidspartneren vår IKOMM til å planlegge sammen med oss og starte det på fredag. Og når vi da hadde mye oppe i løpet av kort interim drift i mars og over til normal drift i november, men vi brukte da noen få uker til å planlegge den her nye driften der de andre bruker halvannet år. En ting er at det var krevende for oss, men vi har jo pushet andre også i denne situasjonen. Så vi ville hatt en annen et annet tidsforløp hvis vi hadde møtt en type partner som ikke hadde hatt evne eller mulighet eller vilje til å sette oss øverst på prioriteringslisten.»

Kommunen tok denne beslutningen med bakgrunn av den situasjonen de sto i, men økonomisjef påpeker at han vil ikke påstå at de hadde tatt den samme beslutningen dersom de hadde hatt mer tid til å gjennomføre prosessen.

> «Vi sto i den situasjonen vi gjorde, og vi hadde et valg mellom alternativene som fantes, og det valget var nok også litt betinget av og preget av situasjonen vi sto i. Ja for det vi visste var at vi måtte ta et valg på framtida, men samtidig så visste vi at det er kanskje ikke tidspunktet nå for å og ta det mest usikre valget, eller mest spenstige valget, eller det mest uferdige alternativet. Vi mente jo at vi tok dette på alvor, sannsynligvis vil det være like mange folk på IT hos oss som før hendelsen, men det er anna kompetanse.»

Et annet område økonomisjef ønsket å nevne var hvorvidt de har klart å kommunisere godt nok i enhver sammenheng.

> «Fordi denne utålmodigheten i organisasjonen, denne frustrasjon når ting, når vi sier at ja vi er nå er vi 70% opp å gå, da begynner jo å forventningen å komme. Om at ja nå er det vår tur, og da er det ikke bare vår tur til å komme opp å gå, nei da er det også vår tur til å bli prioritert på nye ting, nye prosjekter som vi har på gang. De vil vi gjerne realisere nå. Og vi var så godt i gang i mars, vi hadde god progresjon, og så lekket data på nettet, det mørke nettet, og da fikk det en ny dimensjon. Vi måtte snu oss rundt. Og så særlig etter sommerferien så var disse forventningene til at ja nå skal vi se sånn ut, hvor vi har vi fått klare anbefalinger, så kommunedirektøren og bestilte rapport for å få vite hva det er vi må vi gjøre for å sikre oss, og for at vi er utsatt for ikke skal skje en gang til. Det har vi fått klare anbefalinger på, og i tillegg så har vi jo vi da også laget vår vurdering av sikkerheten eller gjennomgangen hos IKOMM som gjør at vi har mange felles læringspunkter for å bli bedre i tida framover. Så kommer sikkerhetssituasjonen i Europa etter Ukraina ble okkupert /krigen

> startet, med fokus på sikkerhet, så vi jobber jo nå parallelt med å forbedre sikkerheten vår, samtidig som vi skal drive ordinær drift. Og så har vi den ressursen vi har på dette som vi har, og så må vi fremdeles bremse. Nå er vi snart midt i 2022, vi hadde innbrudd i begynnelsen januar i 2021, vi kommer til å bruke hele dette i året og kanskje også mye til neste år for å nå igjennom lista med forbedringspunkter. Som krever tid, ressurser, oppmerksomhet, og som gjør at vi må bremse denne her utviklingstakten.»

Personvernombudet ønsket å påpeke hvilken viktig funksjon for å oppfylle denne forordningen personvernombudet har.

> «Og at det er ikke en ulempe at det er en person som har i hvert fall samfunnet i bakhodet, og som er relativt autonom.»

Innsatsleder IKT ønsket å formidle at selv om han er sikker på at trengs folk ut i kommunene, det trengs folk der beslutningene tas som har en forståelse for dette her, slik det er i dag, så trenger de også hjelp i fra andre. Eksperter på å forberede for dette her, og planlegge for det, og skjønne risikoen. Han mener man trenger ekspert-bistand uansett. Han mener dermed at i offentlig sektor ville det vært naturlig at det ble lagt til rette for et eller annet sted.

> «Det burde vært noen som kan hjelpe kommunene, og de ressurspersonene som sitter ute i kommunene. Oppe i dette her som jeg ikke har sagt så mye om, så fikk vi jo en del hjelp fra KS. Han som var fagansvarlig for personsikkerhet og slikt. Det var jo hjelp det, og jeg hadde dialog med ham. Den ene er at den hjelpa vi fikk av ham var av hans egen interesse i dette her. Den egeninteressen han hadde i det, det var mange grunner til det, han hadde helt åpenbart en agenda, med å gå så hardt inn i dette her og hjelpe oss, både ift KS, men og personlig, men det er for så vidt greit nok og ikke så interessant. Det som er interessant er at han personlig hadde interesse av å hjelpe oss så mye, han hadde ingen rolle, og det var ingen systematikk. Det var han personlig som tiltrådte den rollen. Det er verdt å merke seg, og det er viktig å vite for å se på hvordan man må bygge opp dette for det offentlige. Han kjente folkene fra KPMG og sånne som har jobbet i dette andre miljøet tidligere. Jeg tror du kan telle på ganske få hender de folka som virkelig kan med disse tingene, og som har jobbet med det i praksis i Norge. Poenget, og det viktige med dette er at han hjalp oss som individ, fordi han ville og kunne. Dette var ikke satt i system, og hadde det vært noen andre i hans sted i KS, eller andre omstendigheter så hadde vi gått glipp av masse hjelp, og håndteringen av situasjonen kunne vært helt annerledes.»

I tillegg ville han nevne at det NC3 og NSM gjorde var å tappe oss for informasjon for å kunne komme videre i saken, som ikke hjalp kommunen på noe vis.

> «De dro jo ingen ting inn i å hjelpe oss, annet enn noen støttende ord – de var jo hyggelige folk. Men deres interesse var helt åpenbart kun for sitt eget arbeid og sin egen etterforskning. Og det er jo litt sånn betenkelig. Jeg tenker at hvis man skal gjøre noe for kommunal sektor så burde du hatt det SWAT-teamet som kanskje ikke blir så stort og brutalt som jeg skulle ønske at det var. Det var jo det jeg følte at de tilfeldige ressursene som de fra KPMG var tilfeldigvis

> og heldigvis akkurat de rette folka som hadde akkurat rett kompetanse og erfaring. Og det var det jo han fra KS som visste om – den gruppa med folk. Så det var vel kanskje den mest nyttige hjelpa vi fikk av ham, at «jeg vet at der og der jobber sånn og sånn», og dagen etter satt disse på møterommet på Østre Toten. Og så tok vi sammen kontroll over situasjonen. Og det var det største lettelses sukket jeg har tatt noensinne.»

For øvrig mente han at teknologi og sikkerhet, mennesker og sikkerhet og beredskapsplaner er det viktigste å ha fokus på. «Alt annet vil være å dukke for mye ned i detaljer.»

Fylkesberedskapssjef ville gjerne påpeke at man må evne å ha en situasjonsforståelse på flere nivåer. At det ikke er det samme situasjonsforståelse for teknikerne som det er for kommunedirektøren eller en hvilken som helst direktør.

> «En hvilkens om helst operativ og strategisk ledelse er mest interessert i å vite hva dette betyr for meg og min drift, så ikke veldig sånn, når det er tekniske aspekter så er vi mest interesserte i å vite hvor lang tid ting tar. Hvor lenge vi er «svarte» nå. Så det man er interessert i der, og ikke nødvendigvis de tekniske utfordringene man har da, og det er kanskje litt uheldig fordi det er jo noe tekniske løsninger som man også bør ha kontroll på. Det her med forskjell på online-backup og separat back-up er for eksempel kan jo være en strategisk beslutning, og da finner man kanskje ut at online back-up kanskje ikke er det største trikset i verden. Det at man klarer å kompromittere back-up samtidig som man kompromitterer øvrig system er jo i høyeste grad en reel fare da, som kanskje bør tas tiltak på for å unngå. Nå rammet denne cyber-hendelsen en kommune, som nå kanskje er en sånn noenlunde oversiktlig greie, det er kanskje noen som vil mene at det var vanskelig å få oversikt, men det er utrolig mye mindre komplisert enn om det er et sykehus som hadde blitt satt ut da. Som har ressurser på et helt annet nivå enn en kommune. Det fins jo aktører i staten som gjør at du er nødt til å ressurssette på en helt annen måte når ting er «svart». Derfor er vi så opptatt av at det er en beredskapsplan med tiltak for dette.»

Sikkerhetskonsulenten fra ATEA ville gjerne påpeke at det er under-kommunikasjon på omfanget av IT systemer og særlig i kommuner hvor det er såpass komplekst. Som han nevnte, er det er mange fagsystemer, det er mange divisjoner, det er mange brukere som bruker dette, men det er gjerne lite vilje til å investere i nødvendig sikkerhet.

> «Eksempelvis å sette seg inn i enkle ting sånn som Microsoft har noe som heter LAPS, et gratis system som folk kan installere på 2 timer og så får de unike passord på alle administratorer brukerne på PC-ene. Gratis, tar 2 timer å installere, men folk kjenner ikke til det ikke sant. De har ikke tid til å finne ut av de enkle tingene så er det ofte når vi kommer inn og gjør sånne analyser og modenhetsanalyser, så gir vi noen tips for å for å få dem i hvert fall opp på et visst nivå. Men det er investeringsviljen og eller evne til å se at ting kan over skikkelig galt da så som så svikter ofte. I hvert fall å ha en ordentlig back-up som ikke noen hackere kan komme til. Og så er det veldig mange som ikke har tatt en BIA da for å finne ut av hvilke systemer som er viktige, altså prioritere de systemene, der er det veldig mange som ikke har tatt de

nødvendige analysene da. Og så er det selvfølgelig rutiner ja som ligger i bunnen, opplæring og rutiner av personell rett og slett. De fleste kommuner har jo ikke SIEM løsninger heller. Man må definere noe «use cases» og få lagt inn det, og så når du da har varslingen på plass, hvem skal få de varslingene, for det skjer jo døgnet rundt ikke sant, det må jo være personell som faktisk skjønner dette og hva de blir varslet om.»

NTNU

Kunnskap for en bedre verden

VE