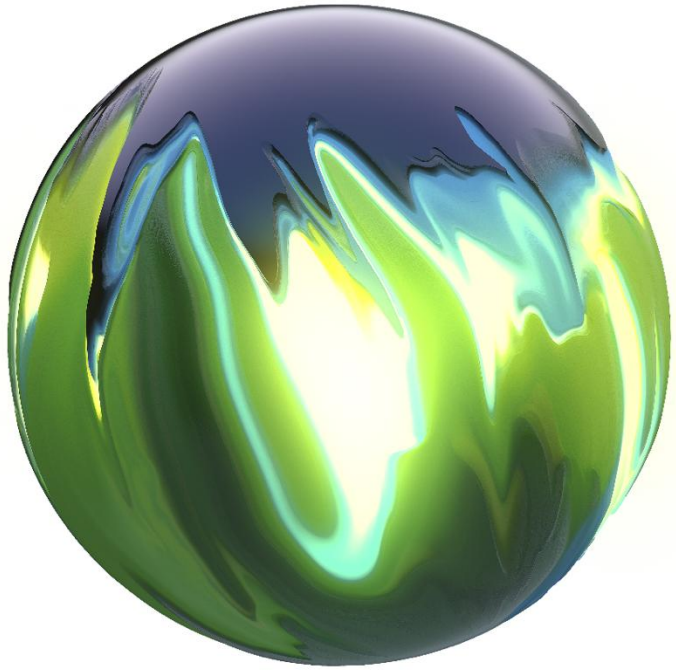
Lørenskog kommune

Deloitte.



# Uavhengig vurdering og forbedringsgjennomgang

Deloitte Cyber Norge September 2026

## OFFENTLIG DEL AV RAPPORTEN

Av hensyn til cybersikkerheten er deler som omhandler tekniske detaljer om det tidligere og det nye tekniske miljøet utelatt i denne delen som omtales som offentlig del av rapporten. Dette da offentliggjøring av slike opplysninger kan øke trusselbildet og risikoen for Lørenskog kommunes cybersikkerhet. En utvidet vurdering er overlevert til kommunen med begrenset tilgang og unntatt offentlighet, ettersom den inneholder konkrete tekniske forbedringsreferanser. Med unntak av disse referansene er rapportenes konklusjoner og rådgivning sammenfallende.

# Innholdsfortegnelse

1 Hendelsesoversikt ..... 6
1.1 Bakgrunn ..... 6
1.2 Tidligere IKT- og sikkerhetshendelser ..... 6
1.3 Umiddelbar respons og eksponering ..... 6
1.4 Positive tiltak og forbedringsambisjoner ..... 7
2 Omfang, metode og vurderingstilnærming ..... 9
2.1 Oppdragets omfang ..... 9
2.2 Vurderingsmetodikk ..... 9
2.2.1 Dokumentgjennomgang ..... 9
2.2.2 Intervjuer ..... 10
2.3 Forutsetninger og begrensninger ..... 10
2.4 Referanseramme for vurderingen ..... 11
3 Hendelsesanalyse, rotårsaker og bidragende faktorer ..... 12
3.1 Hendelsesanalyse ..... 12
3.2 Rotårsaksanalyse ..... 14
3.2.1 Styringsfunn ..... 14
3.2.2 Tekniske funn ..... 18
3.2.3 Utbedring og gjenoppbygging ..... 21
3.3 Konklusjon og oppsummering ..... 22
4 Læringspunkter ..... 26
4.1 Sentrale læringstemaer ..... 26
4.2 Læringspunktmatrise ..... 27
5 Forbedringsprogram ..... 29
5.1 Programstruktur og prioritering ..... 29
Vedlegg B: Intervjuliste ..... 31

# Liste over tabeller

Tabell 1: Tidslinje for mest relevante hendelser under cyberhendelsen. ..... 13
Tabell 2: Kritiske indikatorer for hendelseshåndtering. ..... 13
Tabell 3: Overordnet læringspunktmatrise ..... 28
Tabell 7: Intervjuliste ..... 31

Lørenskog kommune

# Ledelsesoppsummering

## Oppdrag og grunnlag for vurderingen

Deloitte er engasjert av Lørenskog kommune for å gjennomføre en uavhengig, læringsorientert vurdering av cyberhendelsen våren 2026. Formålet har vært å gi kommunen bedre innsikt i hvordan hendelsen kunne oppstå, hvorfor relevante forhold ikke ble identifisert tidligere, hvilke organisatoriske, prosessuelle og tekniske forhold som bidro til risikoen, og hvilke tiltak som bør prioriteres for å styrke kommunens cyberrobusthet fremover.

Vurderingen har ikke hatt som formål å gjenta eller erstatte det tekniske hendelseshåndteringsarbeidet som allerede er gjennomført. Deloitte har gjennomført en avgrenset teknisk og bredere styringsvurdering, med særlig vekt på læring, kontrollsvakheter, datalagring, hendelsesrespons og internkontroll. Arbeidet har vært basert på dokumentasjon fremlagt for Deloitte, samt intervjuer og avklaringsmøter med relevante interne og eksterne aktører.

Som del av oppdraget har Deloitte vurdert seks spørsmål fra kommunen:

| | | |
|---|---|---|
| 1. Hvordan kunne informasjon bli lagret over tid? | 2. Hvorfor ble forholdene ikke identifisert tidligere? | 3. Hvilke forhold bidro til at risikoen utviklet seg? |
| 4. Hvilke kontroller eller tiltak fungerte utilstrekkelig? | 5. Hvilke læringspunkter bør kommunen trekke? | 6. Hvilke konkrete forbedringstiltak anbefales? |

### Innledning og hovedvurdering

Cybersikkerhet i en større virksomhet eller kommune handler om langt mer enn brannmurer og antivirusprogrammer. Det er et helhetlig og kontinuerlig arbeid i et komplekst miljø som omfatter styring og ansvar, kompetanse og sikkerhetskultur, arbeidsprosesser, kompleks teknisk beskyttelse av informasjon og systemer, overvåking, logging, beredskap og evne til å håndtere og gjenopprette etter hendelser. Tiltakene må virke sammen, følges opp og testes, og videreutvikles i takt med endringer i teknologi, digitale tjenester, avhengigheter og trusselbildet. Samtidig er trusselbildet i utvikling, og ny teknologi, lett tilgjengelige angrepsverktøy og kommersielle kriminelle tjenester har senket terskelen for å gjennomføre cyberangrep, også for aktører med begrenset teknisk kompetanse.

Dette er et viktig premiss for forståelsen av hendelsen og for vurderingene som følger: Hva som utgjør et tilstrekkelig sikkerhetsnivå, er ikke statisk, men må vurderes løpende i lys av endringer i teknologi, sårbarheter og trusselbilde. Tiltak som ga tilstrekkelig beskyttelse for seks eller tolv måneder siden, gir derfor ikke nødvendigvis samme beskyttelse i dag. Med dette som bakteppe oppsummere vi nedenfor hva gjennomgangen har vist.

Lørenskog kommune hadde før hendelsen etablert relevante rutiner, sikkerhetsinitiativer, lederarenaer og forbedringsaktiviteter innen informasjonssikkerhet, IKT, internkontroll og beredskap. Hendelsen viser samtidig at disse mekanismene samlet sett ikke ga tilstrekkelig praktisk effekt. Identifiserte risikoer, kontrollmangler og sikkerhetsvarsler ble ikke konsekvent fulgt frem til gjennomført tiltak, dokumentert beslutning, risikoreduserende kontroll eller formell aksept av restrisiko.

Hendelsen bør derfor ikke forstås som en isolert teknisk sikkerhetshendelse. Tekniske svakheter gjorde kompromitteringen mulig, mens svakheter i risikoeierskap, kontrolloppfølging, datalivssyklusstyring, teknisk overvåking og operativ hendelseshåndtering bidro til at risikoen kunne utvikle seg, responsen ble forsinket og skadeomfanget økte.

Rapporten peker ikke på én enkeltstående svikt, men på et kontrollmiljø som ikke ga tilstrekkelig sikkerhet for at risikoer og varsler ble forstått, prioritert, eid og lukket i praksis. Flere risikoforhold var kjent eller identifiserbare, men kunne ikke konsekvent spores til utbedring, formell utsettelse, finansiering, kompenserende tiltak eller eksplisitt aksept av restrisiko. Sikkerhetsvarsler ble heller ikke raskt nok omsatt til undersøkelse, eskalering og begrensningstiltak.

Forbedringsbehovet handler derfor ikke bare om flere tekniske kontroller eller økte ressurser. Den viktigste læringen er styringsmessig: Kommunen bør sikre tydelig eierskap, et godt beslutningsgrunnlag, dokumentert oppfølging og faktisk lukking av risikoer, kontrollmangler og sikkerhetsvarsler. Dette bør være førende for det videre forbedringsarbeidet.

## Svar på kommunens seks spørsmål

1. ***Hvordan kunne informasjon bli lagret over tid?*** Informasjon kunne bli liggende lagret over tid fordi migrering, opprydding og avvikling av eldre lagringsområder ikke hadde tilstrekkelig tydelig eierskap, dokumentert sletting eller formell aksept av restrisiko. Et eldre lagringsområde ble i praksis et vedvarende lagringsområde for informasjon som i hovedsak var eldre eller historisk, men som også omfattet nyere informasjon. Informasjonen burde vært gjennomgått, migrert, slettet eller underlagt bedre beskyttelse.

2. ***Hvorfor ble forholdene ikke identifisert tidligere?*** Forholdene ble ikke i tilstrekkelig grad identifisert, prioritert og håndtert tidligere fordi kontrollmiljøet ikke ga tilstrekkelig praktisk innsikt i status for sentrale risikoer, om avtalte tiltak faktisk var gjennomført, eller om kontrollene fungerte etter hensikten. Flere relevante risikoforhold var kjent, men ble ikke konsekvent omsatt til eide, finansierte, prioriterte og verifiserte utbedringstiltak. Tilgjengelig informasjon indikerer at flere sikkerhetssignaler ble registrert under hendelsesforløpet, uten at disse samlet sett førte til tilstrekkelig rettidig undersøkelse og risikoreduserende tiltak. Dette viser behov for tydeligere ansvar, eskalering og operativ oppfølging av sikkerhetsvarsler.

3. ***Hvilke forhold bidro til at risikoen utviklet seg?*** Risikoen utviklet seg gjennom en kombinasjon av tekniske svakheter og styringsmessige forhold. På teknisk nivå bidro svakheter i sikringen og overvåkingen av deler av IKT-miljøet til at en uautorisert aktør kunne etablere og utvide tilgangen. På styringsnivå bidro uklart eierskap, kapasitets- og budsjettbegrensninger, fragmenterte beslutningsveier og begrenset dokumentasjon på kontrollenes effektivitet til at risikoer ikke konsekvent ble håndtert eller lukket før hendelsen inntraff.

4. ***Hvilke kontroller eller tiltak fungerte utilstrekkelig?*** De mest vesentlige kontrollsvakhetene var knyttet til forvaltning av teknologi og informasjon, tilgangsstyring, teknisk overvåking, nettverkssikring, oppfølging av sikkerhetsvarsler og beskyttelse av sensitiv eller sikkerhetsrelevant informasjon. Hendelsen viser at kommunens sikkerhetsovervåking i praksis var for varslingsorientert og ikke tilstrekkelig utformet som en

operativ responsmodell. Kritiske varsler hadde ikke tilstrekkelig tydelige eiere, responstidskrav, eskaleringsmekanismer eller forhåndsgodkjente begrensningstiltak.

5. ***Hvilke læringspunkter bør kommunen trekke?*** Hendelsen bør forstås som en bred læring om cyberrobusthet, ikke kun som en teknisk kompromittering. Det viktigste læringspunktet er at identifiserte risikoer, sikkerhetsvarsler og kontrollmangler må følges helt frem til dokumentert lukking, formell beslutning om utsettelse eller eksplisitt aksept av restrisiko på riktig ledernivå. Kommunen bør særlig trekke lærdom av at eldre miljøer krever aktiv risikostyring frem til de er migrert eller avviklet, at deteksjon må omsettes til operativ respons, at sensitive data må styres gjennom hele livssyklusen, og at kontrollenes effektivitet må kunne dokumenteres i praksis. Cyberrobusthet avhenger av samspillet mellom styring, mennesker, prosess og teknologi.

6. ***Hvilke konkrete forbedringstiltak anbefales?*** Deloitte anbefaler at kommunen samler og følger opp forbedringstiltakene som et helhetlig forbedringsprogram for cyberrobusthet. Programmet bør prioritere tydeligere risikoeierskap og kontrolloppfølging, videreutvikling av sikkerhetsovervåking og hendelseshåndteringsmodellen, kontrollert migrering og avvikling av eldre miljø, styrket datastyring og innebygd personvern, samt testing av kontinuitet, gjenoppretting og leverandørberedskap. Deloitte anbefaler også at kommunen vurderer om IKT-funksjonens organisering, kapasitet, kompetanse og mandat er tilstrekkelig tilpasset kommunens og tjenesteområdenes digitale avhengighet, sikkerhetskrav og risikobilde. Dette bør inngå som en egen del av forbedringsprogrammet.

## Restrisiko

Kommunen har gjennomført en rekke tiltak, iverksatt sikkerhetstiltak og migrert store deler av tjenestene over til ny infrastruktur. Prosessen med å lukke kjent restrisiko er ikke fullstendig ferdigstilt, men vi forstår at dette arbeidet vil pågå frem til risikoen er bekreftet håndtert.

# 1 Hendelsesoversikt

## 1.1 Bakgrunn

Våren 2026 ble Lørenskog kommune rammet av en cyberhendelse som påvirket kommunens IKT-miljø og tjenestedrift. Basert på vår forståelse av hendelsen skjedde den innledende kompromitteringen 7. april 2026, da en ansatts PC ble kompromittert etter at brukeren åpnet en skadelig fil fra et nettsted som fremsto som legitimt. Den kompromitterte PC'en ga trusselaktøren et innledende fotfeste, som senere ble brukt til å bevege seg videre i miljøet, oppnå utvidede rettigheter, få tilgang til servere, eksfiltrere data og utløse løsepengeviruset.

## 1.2 Tidligere IKT- og sikkerhetshendelser

Som del av arbeidet med denne rapporten har Deloitte mottatt informasjon om tidligere IKT- og sikkerhetshendelser i Lørenskog kommune, herunder hendelser fra 2020 og 2023. Formålet med gjennomgangen har vært å forstå om hendelsen i 2026 kan ses i sammenheng med tidligere erfaringer, identifiserte risikoer og sikkerhetsrelaterte forbedringstiltak.

Informasjonen Deloitte har mottatt viser at kommunen også før 2026 hadde erfaring med hendelser som påvirket IKT-systemer og informasjonssikkerhet. Materialet som er oversendt beskriver blant annet vurderinger av årsaksforhold, gjennomførte analyser og forslag til tekniske og organisatoriske tiltak. Flere av temaene som fremkommer i det historiske materialet er også relevante for vurderingen av hendelsen i 2026. Dette gjelder blant annet identitets- og tilgangsstyring, autentisering, privilegerte kontoer, nettverkssegmentering, beskyttelse av sluttbruker utstyr (PC, Mobil, endepunkter) og servere, beredskap og organisering av hendelseshåndtering.

Informasjonen Deloitte har mottatt viser samtidig at kommunen over tid hadde etablert mekanismer for håndtering av sikkerhetsrelaterte hendelser. Kommunen hadde blant annet prosesser for kritiske IKT-hendelser, avviksbehandling, kriseledelse og rapportering til relevante myndigheter. Historikken vurderes derfor ikke primært som et spørsmål om hvorvidt hendelser ble rapportert eller håndtert, men som et grunnlag for å forstå hvordan identifiserte risikoer, funn og forbedringsforslag ble behandlet og fulgt opp over tid.

De tidligere hendelsene brukes i denne rapporten som kontekst og informasjonsgrunnlag, ikke som dokumentasjon på årsakene til hendelsen i 2026. Basert på det materialet Deloitte har mottatt, er det ikke mulig å fastslå i hvilken grad alle tiltak fra tidligere hendelser ble implementert, verifisert eller opprettholdt gjennom senere organisatoriske og teknologiske endringer. Historikken er likevel relevant fordi den gir innsikt i hvilke risikoer og kontrollområder kommunen tidligere hadde identifisert, og danner et bakteppe for vurderingen av kommunens arbeid med risikostyring, internkontroll, informasjonssikkerhet og beredskap frem mot 2026.

## 1.3 Umiddelbar respons og eksponering

Hendelsen ble identifisert 9. mai 2026, hvorpå Lørenskog kommune etablerte kriseledelse. Det ble også iverksatt begrensningstiltak, herunder nedstenging av berørte systemer og deler av nettverket, frakobling av servere, endring av administratorpassord, krav om passordendring for ansatte og prioritering av gjenoppretting av kritiske systemer og tjenester. Kommunen engasjerte sin leverandør for hendelseshåndtering, Move AS (Move), og varslet relevante myndigheter, herunder Datatilsynet, Nasjonal sikkerhetsmyndighet og Kripos.

Kommunens innledende vurdering, basert på tilgjengelige logger og tidlig teknisk analyse, var at det ikke forelå et bekreftet grunnlag for å konkludere med at betydelige mengder sensitive personopplysninger var eksfiltrert. Denne forståelsen endret seg vesentlig etter at trusselaktøren publiserte, og senere gjorde tilgjengelig, et stort datasett på sitt lekkasjenettsted. Datasettet ble rapportert å være på om lag 1,8 terabyte og inneholde 1,3 millioner filer.

De eksponerte dataene syntes å stamme fra et eldre lagringsområde som blant annet inneholdt informasjon knyttet til sensitive personopplysninger og sårbare grupper. Basert på det opplyste innholdet omfattet materialet også annen sensitiv, beskyttelsesverdig eller annen sikkerhetsrelevant informasjon og informasjon om kritisk infrastruktur.

Kommunen har per i dag ikke fullstendig innsikt i alt innhold som er kommet på avveie. En nærmere vurdering av datakategorier, berørte tjenester og eventuell sikkerhets- eller beredskapsmessig betydning bør derfor inngå i den videre analysen. Slik informasjon kan ha et særskilt beskyttelsesbehov selv om den ikke nødvendigvis utgjør personopplysninger, fordi den kan få betydning for samfunnssikkerhet, beredskap eller kommunens evne til å opprettholde kritiske tjenester dersom den misbrukes eller sammenstilles med annen informasjon.

## 1.4 Positive tiltak og forbedringsambisjoner

Etter at hendelsen ble formelt erkjent, iverksatte Lørenskog kommune flere tiltak for å begrense hendelsen, gjenopprette drift og styrke kontrollmiljøet. Responsen omfattet blant annet etablering av kriseledelse, involvering av Move som leverandør for hendelseshåndtering, varsling av relevante myndigheter og prioritering av gjenoppretting av kritiske tjenester og systemer. Som del av gjenopprettingsarbeidet bygget kommunen opp vesentlige deler av IKT-miljøet på nytt og styrket sentrale sikkerhetsmekanismer.

Deloitte observerer at kommunen mobiliserte roller innen IKT, beredskap, personvern, informasjonssikkerhet, kommunikasjon og sektorledelse for å håndtere konsekvensene for tjenesteleveransen. Intervjuene indikerer at tjenesteområder tok i bruk manuelle rutiner for å opprettholde kritiske tjenester. Dette representerer positive beredskaps- og responskapabiliteter som kommunen bør bygge videre på, samtidig som hendelsen viser behov for å styrke evnen til å håndtere langvarige cyber- og IKT-relaterte avbrudd.

Før hendelsen inntraff, hadde Lørenskog kommune allerede igangsatt flere forbedringer innen sikkerhet og styring. Dette omfattet blant annet modernisering av løsningen for administrasjon og sikring av enheter, forbedring av sikkerhetsrutiner, oppdatering av personverndokumentasjon, bevisstgjøringstiltak og videreutvikling av styringssystemet for informasjonssikkerhet. I tillegg hadde IKT-funksjonen løftet langsiktige behov knyttet til budsjett, kapasitet og modernisering gjennom budsjettinnspillprosessen, herunder behov relatert til teknisk gjeld, ressursbegrensninger og fremtidig IKT-utvikling. Selv om disse initiativene ikke var fullført eller fullt operasjonalisert i tide til å redusere risikoen for hendelsen vesentlig, indikerer de at Lørenskog kommune hadde identifisert flere relevante forbedringsområder og allerede i gang med å styrke sin IKT- og sikkerhetsmodenhet.

Lørenskog kommune har også anerkjent betydningen av å engasjere Deloitte til å gjennomføre en uavhengig vurdering med fokus på læring og forbedring. Gjennom arbeidet har Deloitte observert at Lørenskog kommune har tydelige ambisjoner om å styrke sitt sikkerhetsforbedringsprogram, blant annet gjennom teknologimodernisering og bygge cybersikkerhetskultur i organisasjonen, støtte til styring og kontrolloppfølging, samt sikring av nødvendig finansiering og kapasitet for å redusere

restrisiko fremover. Dette gir et viktig grunnlag for å bruke erfaringene fra hendelseshåndteringen som grunnlag for et strukturert forbedringsprogram.

Lørenskog kommunes initiativ til å invitere Deloitte til å gjennomføre en uavhengig, læringsorientert vurdering representerer i seg selv et positivt steg i forbedringsarbeidet. Gjennomgangen skal bidra til å identifisere konkrete forbedringsområder og gi et styrket grunnlag for å prioritere tiltak som kan videreutvikle kommunens sikkerhetsforbedringsprogram og motstandskraft.

# 2 Omfang, metode og vurderingstilnærming

## 2.1 Oppdragets omfang

Deloitte er engasjert for å gjennomføre en uavhengig og læringsorientert vurdering av hendelsen. Oppdraget er utformet for å støtte Lørenskog kommune i å forstå hvordan hendelsen og den tilhørende dataeksponeringen kunne oppstå, hvorfor relevante forhold ikke ble identifisert tidligere, og hvilke organisatoriske, styringsmessige, prosessuelle, sikkerhetsmessige og tekniske faktorer som bidro til hendelsen.

Vurderingen er basert på informasjon fremlagt av Lørenskog kommune og relevante eksterne parter i oppdragsperioden (Move og Sorasec). Omfanget har vært rettet mot å etablere et faktagrunnlag for observasjoner, årsaksvurderinger, læringspunkter og anbefalte forbedringstiltak.

Gjennomgangen har omfattet både hendelseshåndteringen og bredere forhold av betydning for forebygging, deteksjon, respons, styring, internkontroll, informasjonssikkerhet, personvern og datahåndtering.

## 2.2 Vurderingsmetodikk

Deloitte har gjennomført vurderingen ved å analysere og sammenstille informasjon fra dokumentgjennomgang, intervjuer og statusmøter. For å støtte vurderingen har Deloitte evaluert både organisatoriske og tekniske aspekter ved hendelsen, med særlig fokus på:

| | |
|---|---|
| **1. Datalagring, arbeidsmetodikk og bruk av eldre lagringsområder**<br>Herunder hvordan sensitive opplysninger kunne lagres over tid og hvordan etablerte arbeidsmetoder og kontroller fungerte i praksis. | **2. Oppdagelse, internkontroll og respons**<br>Herunder hvordan risikoen kunne utvikle seg uten å bli identifisert tidligere, og i hvilken grad organisatoriske og tekniske sikkerhetskontrollmekanismer bidro til å forebygge, oppdage og håndtere forholdene. |

Vurderingen er basert på sammenstilling og analyse av informasjon fra dokumentgjennomgangen, intervjuer og statusmøter. Informasjonen er vurdert på tvers av organisatoriske, tekniske og prosessmessige forhold for å identifisere relevante observasjoner, kontrollsvakheter og bidragende faktorer. Det er lagt vekt på hvordan etablerte styringsmekanismer og sikkerhetskontroller var utformet, og hvordan disse fungerte i praksis.

Som del av arbeidet har Deloitte anvendt en strukturert «5-hvorfor»-tilnærming for å identifisere underliggende årsaker og bidragende forhold. Tilnærmingen innebærer å vurdere hvordan styring, internkontroll, prosesser, teknologi og menneskelige faktorer samlet kan ha påvirket hendelsen og kommunens evne til å forebygge, oppdage og håndtere risikoen.

### 2.2.1 Dokumentgjennomgang

For å støtte vurderingen innhentet og gjennomgikk Deloitte dokumentasjon fra Lørenskog kommune og relevante eksterne parter. Dokumentasjonen ble benyttet til å etablere et faktagrunnlag for å forstå hendelsen, kommunens styrings- og kontrollmiljø, samt de organisatoriske og tekniske forholdene som kan ha bidratt til at risikoen utviklet seg over tid.

Gjennomgangen omfattet blant annet hendelsesrelatert dokumentasjon, materiale knyttet til styring og internkontroll, dokumentasjon om informasjonssikkerhet og personvern, risikovurderinger, system- og arkitekturinformasjon, beredskaps- og krisehåndteringsdokumentasjon, leverandøravtaler og annet materiale relevant for datalagring, deteksjon, eskalering, respons og gjenoppretting.

Dokumentasjonen ble vurdert for å identifisere relevante observasjoner, kontrollmangler, læringspunkter og forbedringsmuligheter.

### 2.2.2 Intervjuer

Deloitte gjennomførte en serie strukturerte intervjuer og avklaringsmøter med utvalgte representanter fra Lørenskog kommune og relevante eksterne parter, herunder Move AS og Sorasec. Intervjuene ble benyttet til å supplere dokumentgjennomgangen, validere informasjon, avklare tekniske og organisatoriske forhold og få innsikt i aktiviteter knyttet til hendelseshåndtering, operativ praksis og gjenopprettingsarbeid.

Informasjon innhentet gjennom intervjuene ble vurdert sammen med øvrig tilgjengelig dokumentasjon og informasjon for å identifisere gjentakende observasjoner, bidragende faktorer og forbedringsområder.

## 2.3 Forutsetninger og begrensninger

Denne uavhengige vurderingen er begrenset til de beviskilder, dokumenter, intervjuer, tekniske artefakter og den tiden som har vært tilgjengelig i oppdragsperioden. Vurderingen er ikke en uttømmende etterforskning av alle mulige hendelsesscenarioer eller alternative innfallsvinkler. Deloitte har ikke hatt som mandat å gjennomføre en fullstendig kriminalteknisk granskning, attribusjonsanalyse eller vurdering av alle hypotetiske årsaksforhold, herunder for eksempel innsidehandlinger eller andre scenarier som ikke er særskilt underbygget i materialet som er gjort tilgjengelig. Rapportens vurderinger er basert på dokumentasjon, intervjuer og teknisk informasjon fremlagt for Deloitte, og er rettet mot å identifisere læringspunkter, kontrollsvakheter, bidragende faktorer og forbedringstiltak. Deloitte kan ikke utelukke at ytterligere arbeid, tilleggsdokumentasjon eller utvidet teknisk analyse kunne ha resultert i andre funn, mer presise konklusjoner eller identifisering av ytterligere forhold som Lørenskog kommune bør være oppmerksom på. Med mindre informasjon er bekreftet gjennom flere kilder, har Deloitte lagt til grunn at elektronisk materiale, dokumentasjon og informasjon som er gjort tilgjengelig for oss, er pålitelig, korrekt og fullstendig. Deloitte påtar seg ikke ansvar for deler av rapportens innhold som kan være påvirket av upålitelig, ufullstendig eller uriktig materiale som er gjort tilgjengelig for oss.

Denne rapporten er utarbeidet av Deloitte på oppdrag fra Lørenskog kommune som en offentlig versjon av den uavhengige vurderingen av cyberhendelsen i 2026. Rapporten er utarbeidet på grunnlag av oppdraget som fremgår av arbeidsordren signert 16. juli 2026.

Rapporten er publisert for å bidra til åpenhet om hendelsen, vurderingene som er gjort og de overordnede læringspunktene som er identifisert. Av hensyn til informasjonssikkerhet, personvern og andre beskyttelsesbehov er enkelte opplysninger, vurderinger og detaljer fra den fullstendige rapporten utelatt eller generalisert. Deloitte påtar seg ikke ansvar overfor noen tredjepart for brudd på denne forpliktelsen, for tillit som måtte bli lagt til rapporten, eller for eventuelle vurderinger som er uttrykt eller informasjon som inngår i rapporten.

Tekniske artefakter, datoer og tidspunkter som omtales i rapporten, er angitt som veiledende informasjon. I digitale miljøer kan logger, filer, tidsstempler og andre tekniske verdier endres av

brukere eller systemprosesser. Etter Deloittes beste vurdering foreligger det likevel ikke rimelig grunnlag for å anta at funnene er uriktige som følge av feil eller urettmessig bruk av de aktuelle elektroniske mediene. De datasystemene Deloitte benyttet i analysen, fungerte etter vår vurdering tilfredsstillende på alle relevante tidspunkter. Dersom det har forekommet avvik, er det etter Deloittes vurdering ikke forhold som har påvirket fremstillingen av informasjonen eller nøyaktigheten i innholdet.

Dokumentasjon mottatt fra Lørenskog kommune behandles som konfidensielt prosjektmateriale og skal håndteres i samsvar med avtalte krav til informasjonssikkerhet og konfidensialitet. Med mindre annet er skriftlig avtalt, vil mottatt dokumentasjon bli slettet 60 dager etter godkjenning av rapporten.

## 2.4 Referanseramme for vurderingen

Vurderingene og anbefalingene i denne rapporten er gjennomført som en lærings- og forbedringsgjennomgang.

For å sikre etterprøvbarhet er funn og anbefalinger vurdert opp mot sentrale krav og forventninger til kommunal internkontroll, informasjonssikkerhet, personvern og styring av digitale verdier.

Referanserammen omfatter blant annet:

- Kommuneloven kapittel 25 om internkontroll
- Personopplysningsloven og GDPR
- NSMs grunnprinsipper for IKT-sikkerhet
- Offentlig sektors forventninger til systematisk informasjonssikkerhetsarbeid
- Prinsipper for virksomhetsstyring og kontinuerlig forbedring

# 3 Hendelsesanalyse, rotårsaker og bidragende faktorer

Dette kapittelet oppsummerer Deloittes hendelsesanalyse og vurdering av rotårsaker, herunder de viktigste tekniske, organisatoriske og styringsmessige forholdene som muliggjorde kompromitteringen, påvirket deteksjon og respons, og bidro til gjenværende restrisiko.

Ved bruk av «5-hvorfor»-metodikken vurderer vi ikke bare hva som skjedde, men også hvorfor relevante forhold eksisterte og hvorfor de ikke ble håndtert tidligere. Kapittelet sammenstiller hendelsesforløpet, tidsforsinkelsesindikatorer, styringsmessige og tekniske funn, observasjoner knyttet til utbedring og gjenoppbygging, samt vurderinger av restrisiko. Formålet er å gi en konsis oversikt over de mest vesentlige læringspunktene og prioriterte forbedringsområdene.

## 3.1 Hendelsesanalyse

Deloitte har analysert hendelsesforløpet og kombinasjonen av forhold som gjorde det mulig for trusselaktøren å etablere og videreutvikle tilgang i kommunens IKT-miljø over tid.

Basert på tilgjengelig informasjon og gjennomførte intervjuer kan hendelseskjeden overordnet oppsummeres slik:

- En kompromittert pc ga trusselaktøren videre tilgang til deler av et eldre IKT-miljø.
- Utilstrekkelig segmentering, overvåking og operativ respons gjorde det mulig for trusselaktøren å utvide tilgangen og gjennomføre skadegjørende aktiviteter før effektive begrensningstiltak ble iverksatt.
- Hendelsen fikk konsekvenser for både informasjon og tilgjengeligheten til kommunens systemer og tjenester.
- Forløpet viser at tekniske svakheter og utilstrekkelig oppfølging av sikkerhetsvarsler samlet bidro til hendelsens utvikling og omfang.

Tidslinjen illustrerer de viktigste hendelsene som fant sted under hendelsen. Den gjør det mulig å vurdere tre sentrale forhold: hvor raskt sikkerhetsovervåkingen oppdaget trusselaktøren, når SOC varslet Lørenskog kommune om den ondsinnede aktiviteten, og tidsforløpet for Lørenskog kommunes varsling til interessenter.

Enkelte forsøk på tilgangsutvidelse ble stanset eller ser ikke ut til å ha lyktes, mens senere utnyttelse av tekniske svakheter ga trusselaktøren utvidede administrative rettigheter.

| Dato | Beskrivelse |
|---|---|
| 2026-04-07 | En trusselaktør klarer å kompromittere en PC og bruker den som mellomledd for å kompromittere Lørenskogs IKT-infrastruktur. |
| 2026-04-13 | Første varsel genereres av SOC og eskaleres til Lørenskog. Samme dag forsøkte trusselaktøren å utvide tilgangen gjennom Kerberoasting mot en tjenestekonto. Det ble ikke observert senere mistenkelig bruk av kontoen, og det er derfor rimelig å anta at forsøket ikke lyktes. |
| 2026-04-22 | Trusselaktøren utnyttet en svakhet og oppnådde utvidede administrative rettigheter. Dette gjorde det mulig å utvide tilgangen i kommunens IKT-miljø. |
| | Andre varslingsbølge genereres av SOC og eskaleres til Lørenskog. |
| 2026-04-23 | Trusselaktøren starter omfattende rekognosering for å identifisere relevant informasjon i miljøet. |

| Dato | Beskrivelse |
|---|---|
| | Tredje varslingsbølge genereres av SOC og eskaleres til Lørenskog. |
| 2026-04-26 | Trusselaktøren installerer verktøy for dataeksfiltrering. |
| 2026-05-08 | Trusselaktøren installerer ytterligere verktøy for dataeksfiltrering. |
| | Trusselaktøren begynner å slette spor og kjører løsepengevirus i Lørenskogs IKT-infrastruktur. |
| | Fjerde varslingsbølge genereres av SOC og eskaleres til Lørenskog. |
| 2026-05-09 | Lørenskog kommune kontakter Move AS support for å erklære en cyberhendelse.<br>Melding til Datatilsynet. |
| 2026-05-11 | Tilleggsrapport til Datatilsynet. |
| 2026-07-01 | Tilleggsrapport til Datatilsynet. |
| 2026-07-09 | Tilleggsrapport til Datatilsynet. |

*Tabell 1: Tidslinje for mest relevante hendelser under cyberhendelsen.*

Basert på tidslinjen ovenfor har Deloitte identifisert sentrale forsinkelsesindikatorer for å illustrere hvor lenge trusselaktøren hadde tilgang til miljøet, samt tiden det tok å oppdage, eskalere og respondere på hendelsen:

| Metrikk | Verdi | Beskrivelse |
|---|---|---|
| Deteksjonsforsinkelse | 6 dager | Trusselaktøren etablerte vedvarende tilgang før det ble generert varsel. |
| Responsforsinkelse | 32 dager | Hele angrepsforløpet ble gjennomført før begrensningstiltak ble igangsatt. |
| Varslingsforsinkelse | 32 dager<br>(0 dager) | Varsling ble utløst av driftsstans, ikke av deteksjon. Et positivt funn er at Lørenskog kommune varslet Datatilsynet umiddelbart etter at undersøkelsen ble igangsatt. |

*Tabell 2: Kritiske indikatorer for hendelseshåndtering.*

Analysen viser betydelig forsinkelse mellom første indikasjon på kompromittering, SOC-varsling og iverksettelse av effektive begrensningstiltak. Dette indikerer svakheter både i deteksjonsdekning og i operasjonsmodellen for oppfølging av sikkerhetsvarsler. Forsinkelsen var kritisk fordi den ga trusselaktøren tid til å etablere vedvarende tilgang, eskalere rettigheter, bevege seg lateralt, gjennomføre rekognosering og forberede dataeksfiltrering og skadegjørende handlinger før effektive begrensningstiltak ble iverksatt. Mulige årsaker til forsinkelsene vurderes nærmere i avsnitt

Rotårsaksanalyse, Styringsfunn og Tekniske funn.

Hendelsesforløpet viser at trusselaktøren både fikk teknisk mulighet til å bevege seg videre i miljøet og et tidsvindu til å gjennomføre skadegjørende aktivitet før effektive begrensningstiltak ble iverksatt. De tekniske og organisatoriske forholdene som bidro til dette vurderes nærmere i

Rotårsaksanalyse nedenfor.

## 3.2 Rotårsaksanalyse

Dette kapittelet vurderer de underliggende forholdene som bidro til at risikoen kunne utvikle seg over tid, at trusselaktøren kunne bevege seg videre i miljøet, og at hendelsen ikke ble identifisert og begrenset tidligere. Analysen skiller mellom styringsmessige og tekniske forhold, men disse må forstås samlet. De tekniske svakhetene skapte angrepsmuligheter, mens svakheter i styring, eierskap, kapasitet, kontrolloppfølging og operasjonsmodell bidro til at risikoen ikke ble håndtert eller lukket før hendelsen inntraff.

### 3.2.1 Styringsfunn

**DELOITTE VURDERER**

Materialet indikerer ikke at kommunen manglet mekanismer for å identifisere risiko.

Hovedutfordringen synes i større grad å ligge i internkontrollens evne til å følge identifiserte risikoer, kontrollmangler og sikkerhetsvarsler frem til dokumentert behandling, lukking eller aksept av restrisiko.

Hendelsen bør derfor forstås som en styrings- og internkontrollutfordring like mye som en teknisk sikkerhetshendelse.

#### *3.2.1.1 Svakheter i styring og risikohåndtering*

Den gjennomgåtte dokumentasjonen og intervjuene indikerer at kommunen hadde flere mekanismer for å identifisere, løfte og drøfte risiko knyttet til informasjonssikkerhet og IKT. Dette omfattet blant annet tekniske vurderinger, risiko- og sårbarhetsanalyser, sektorgjennomganger, sikkerhetskoordinatorer, sikkerhetsfora, ledelsesgjennomganger og pågående arbeid med å oppdatere styringssystemet for informasjonssikkerhet. Intervjuene indikerer også at disse mekanismene i flere tilfeller fungerte etter hensikten ved at risikoer ble løftet, diskutert og håndtert i linjen eller gjennom etablerte lederarenaer.

Informasjonen Deloitte har mottatt om hendelsen i 2020 viser at kommunen identifiserte flere områder for videreutvikling av sikkerhetsarbeidet. Dette omfattet blant annet brannmurregler, kontroll med nettverkssoner og dataflyt mellom soner, privilegerte kontoer, autentisering, endepunktbeskyttelse og sporbarhet. Informasjonen Deloitte har mottatt viser samtidig at enkelte etablerte sikkerhetsmekanismer bidro til å begrense konsekvensene av hendelsen.

Materialet Deloitte har mottatt gir imidlertid ikke tilstrekkelig grunnlag for å fastslå i hvilken grad hvert enkelt tiltak ble implementert, verifisert og opprettholdt over tid. Hendelsen er derfor relevant fordi den illustrerer hvordan identifiserte risikoforhold og forbedringstiltak må følges opp gjennom styrte prosesser for gjennomføring, evaluering og senere revurdering. Dette gjelder særlig når teknologi, leverandørforhold eller organisering endres over tid.

Samtidig viser gjennomgangen at prosessen ikke fungerte konsekvent nok på områder hvor risikoer eller kontrollmangler forble uavklarte over tid. Den mest vesentlige svakheten synes å ligge i overgangen fra identifisert risiko til dokumentert beslutning, oppfølging, risikoreduserende tiltak og eventuell aksept av restrisiko. Risiko ble ikke oversatt til et tilstrekkelig tydelig beslutningsgrunnlag med konsekvens, handlingsalternativer, ressursbehov og gjenværende restrisiko. Der risikoer krevde budsjett, kapasitet, involvering fra sektorene eller tverrfunksjonell prioritering, kan Deloitte ikke følge hvem som eide risikoen, hvilken beslutning som ble tatt, hvilke tiltak som ble valgt, eller om gjenværende restrisiko ble akseptert på riktig beslutningsnivå.

Hovedlæringen er derfor ikke at kommunens risikoprosesser generelt var fraværende eller uten effekt, men at identifiserte risikoer, kontrollmangler og sikkerhetsvarsler bør følges mer konsekvent

gjennom en dokumentert livssyklus som viser konsekvens, sannsynlighet, mulige tiltak, valgt håndtering, ansvarlig eier, frist, status, effekt og eventuell restrisiko. Dette er nødvendig for at kommunen skal kunne ta informerte beslutninger og etterprøve om risikoen er redusert, utsatt, finansiert, håndtert med kompenserende kontroller eller akseptert som restrisiko.

#### *3.2.1.2 Mandat, ansvar og beslutningsmyndighet*

Intervjuene indikerer at det forelå formelle mandater, særlig for informasjonssikkerhetsfunksjonen og IKT-funksjonen, herunder mulighet til å rapportere vesentlige forhold til ledelsen. IKT-funksjonen beskrev også et betydelig praktisk ansvar for teknisk sikkerhet og infrastrukturrisiko.

Deloitte har imidlertid ikke identifisert et tydelig og samlet risikoregister som konsekvent omfatter cyber- og informasjonssikkerhetsrisikoer, eiere, beslutninger om risikohåndtering, frister, status, dokumentasjon på lukking og aksept av restrisiko. I fravær av et slikt register synes risikooppfølgingen i større grad å være avhengig av enkeltstående prosesser, dokumenter, fora og eskaleringer, fremfor én autoritativ mekanisme for å følge risikoer gjennom hele livssyklusen.

Formelt ansvar ble ikke alltid omsatt til praktisk myndighet eller kapasitet til å drive frem utbedring på tvers av kommunen. Flere risikoreduserende tiltak var avhengige av budsjett, teknisk kapasitet, prioritering i sektorene eller ledelsesbeslutninger utenfor informasjonssikkerhets- og IKT-funksjonenes direkte kontroll. Dette skapte et gap mellom evnen til å identifisere og eskalere risiko og evnen til å sikre at utbedring faktisk ble gjennomført.

Risiko bør som hovedregel håndteres på lavest mulig effektive nivå, der ansvar, mandat og ressurser er tilstrekkelige til å beslutte og gjennomføre nødvendige tiltak. Når en risiko ikke kan håndteres innenfor operativt mandat, tilgjengelig kapasitet, etablerte budsjettrammer eller akseptert risikonivå, bør den løftes til riktig beslutningsnivå. Eskalering bør derfor ikke forstås som et mål i seg selv, men som en mekanisme for å sikre at risikoer som krever tverrfunksjonell prioritering, finansiering eller formell aksept av restrisiko, får en tydelig beslutning og dokumentert oppfølging.

Deloitte vurderer derfor at kommunen bør tydeliggjøre hvilke roller som er ansvarlige for å identifisere, registrere, finansiere, implementere, verifisere og akseptere restrisiko knyttet til cyber- og informasjonssikkerhet. Dette bør understøttes av et samlet risikoregister og en tydelig modell for eierskap, eskalering og aksept av restrisiko.

#### *3.2.1.3 Begrensninger knyttet til budsjett, kapasitet og operasjonsmodell*

Intervjuene indikerer at begrenset IKT- og sikkerhetskapasitet var en vesentlig bidragende faktor. IKT-funksjonen beskrev en situasjon der et bredt sett av oppgaver måtte håndteres av et begrenset antall ressurser, herunder daglig drift, modernisering, patching, livssyklusstyring, oppfølging av overvåking og forebyggende sikkerhetsarbeid. Sikkerhetsansvar ble delvis ivaretatt av personer med andre primæroppgaver, og IKT-funksjonen hadde begrenset evne til å håndtere ytterligere risikoreduserende arbeid uten dedikert finansiering eller bemanning.

Etter Deloittes erfaring står kommuner og andre offentlige virksomheter i et økende forventningspress knyttet til digitalisering, effektivisering og tjenesteutvikling. Teknologi forventes i økende grad å bidra til bedre brukeropplevelser, mer effektive arbeidsprosesser, bedre datagrunnlag og mer samordnede tjenester. Dette gjør IKT-funksjonen stadig mer virksomhetskritisk. IKT skal ikke bare sikre stabil drift, men også muliggjøre innovasjon, understøtte etterlevelse, håndtere økende teknologisk kompleksitet og beskytte virksomheten mot et mer krevende trusselbilde.

Når digitaliseringsambisjonene øker uten at budsjetter, bemanning og kompetanseutvikling styrkes tilsvarende, oppstår det et gap mellom forventninger og gjennomføringsevne. Nye digitale løsninger, skytjenester, integrasjoner og sikkerhetskrav kan da innføres uten at organisasjonen har tilstrekkelig kapasitet til å forvalte, sikre og videreutvikle dem. Over tid kan dette bidra til økt teknisk gjeld og operasjonell risiko. I praksis kan IKT-funksjonen bli nødt til å prioritere akutte driftsbehov og prosjektleveranser fremfor langsiktig sikkerhetsarbeid, dokumentasjon, kontrolloppfølging, sanering av eldre teknologi og systematisk risikoreduserende arbeid.

Dette reiser også et spørsmål om kommunens organisatoriske organisering er tilstrekkelig tilpasset dagens digitale risikobilde. Dersom IKT er plassert lavt i organisasjonshierarkiet, kan det begrense funksjonens gjennomslagskraft i budsjettprosesser, strategiske prioriteringer og tverrsektorielle beslutninger. Det kan også svekke evnen til å løfte teknologisk risiko som en virksomhetsrisiko, og ikke bare som et operativt eller teknisk forhold. Behov for modernisering, sikkerhetsutbedringer, kompetanseheving og håndtering av teknisk gjeld risikerer dermed å ikke få tilstrekkelig synlighet eller prioritet på riktig beslutningsnivå.

Kompetanseutvikling er særlig viktig i denne sammenhengen. Digitalisering skjer i høyt tempo, og teknologilandskapet endres raskt gjennom økt bruk av skyplattformer, automatisering, identitetsbaserte sikkerhetsmodeller, moderne endepunktbeskyttelse, dataanalyse og kunstig intelligens (KI). Dette stiller høyere krav til kontinuerlig kompetanseutvikling, både i IKT-funksjonen og hos ledelse, systemeiere og tjenesteområder som tar i bruk teknologien. Uten et tilstrekkelig kompetanseløft kan kommunen få utfordringer med å forstå risiko, stille riktige krav, forvalte løsningene sikkert og følge opp leverandører og kontroller på en effektiv måte.

Budsjettmodellen synes i tillegg å ha gitt begrenset fleksibilitet til å håndtere akutte eller mellomstore behov for sikkerhetsutbedringer. Større transformasjonsinitiativer kunne håndteres gjennom porteføljestyring, mens ordinære driftsoppgaver ble håndtert innenfor IKT-funksjonens rammer. Enkelte sikkerhetstiltak falt imidlertid mellom disse kategoriene. De hadde tilstrekkelig risikobetydning til å kreve særskilt prioritering, men var ikke omfattende nok til å bli etablert som egne transformasjonsprosjekter.

Samlet peker dette på et behov for å styrke kommunens evne til å koble digital risiko, prioriteringer og beslutninger tydeligere sammen. Deloittes vurdering er ikke at alle identifiserte sikkerhetsbehov nødvendigvis skulle vært løst umiddelbart, men at beslutninger om håndtering, utsettelse, finansiering, kompenserende tiltak eller aksept av restrisiko bør være tydelig dokumentert og fulgt opp. Etter Deloittes vurdering bør kommunen gjennomføre en egen vurdering av om IKT-funksjonens mandat, kapasitet, kompetanse, beslutningsflater og organisatoriske plassering er tilstrekkelig tilpasset kommunens digitale avhengighet, sikkerhetskrav og risikobilde. Formålet bør ikke være å konkludere med én bestemt organisasjonsmodell, men å sikre at ansvar, beslutningsmyndighet, kapasitet, kompetanse og finansiering står i forhold til kommunens behov for stabil drift, sikkerhet, etterlevelse og trygg digital tjenesteutvikling. Dette bør følges opp som en egen del av forbedringsprogrammet.

#### *3.2.1.4 Styringssystem for informasjonssikkerhet og kontrolloppfølging*

Kommunen hadde etablert flere komponenter i et styringssystem for informasjonssikkerhet, herunder retningslinjer, instrukser, bevisstgjøringsaktiviteter, sikkerhetskoordinatorer i sektorene og mekanismer for ledelsens gjennomgang. Informasjonssikkerhetsansvarlig beskrev også pågående arbeid med å oppdatere og konsolidere styringssystemet ved bruk av anerkjent kommunal veiledning.

Styringssystemet var imidlertid ennå ikke fullt ut operasjonalisert som en praktisk mekanisme for kontrolloppfølging. Eksisterende rutiner var delvis fragmentert på tvers av kommunens dokument- og styringssystem og andre kanaler, og kommunen hadde sterkere dokumentasjon på oppfølging av bevisstgjøring og opplæring enn på systematisk testing av om sentrale tekniske og organisatoriske kontroller var implementert og fungerte effektivt.

Dette er relevant fordi dokumenterte rutiner kun reduserer risiko dersom de er forstått, implementert, overvåket og korrigert når de ikke fungerer som forutsatt.

#### *3.2.1.5 Livssyklusstyring av ressurser*

Lørenskogs tidligere dokumenterte risiko- og sårbarhetsanalyser (ROS) identifiserte flere svakheter knyttet til livssyklusstyring av ressurser. Dette omfattet blant annet ufullstendig oversikt over enheter på kommunens nettverk, manglende plan for håndtering av uautoriserte enheter, ufullstendig oversikt over virtuelle servere og skrivebord, bruk av ikke-godkjent programvare, manglende plan for godkjenning av programvare, utstyr kjøpt inn uten godkjenning fra IKT, og eldre IKT-produkter som ikke var faset ut. Disse funnene indikerer at Lørenskog kommune hadde ressursrelatert informasjon fordelt på flere systemer, herunder flere løsninger for enhets-, identitets- og konfigurasjonsadministrasjon og andre verktøy, men ikke en tilstrekkelig samlet og autoritativ prosess for ressursstyring.

I lys av hendelsen reflekterer den fortsatte tilstedeværelsen av endepunkter som ennå ikke var migrert til moderne endepunktadministrasjon, et bredere gap i livssyklusstyringen av ressurser. Ufullstendig ressursstyring reduserte kommunens evne til å sikre at enheter, programvare og infrastruktur konsekvent var godkjent, støttet, herdet, overvåket og migrert eller avviklet innen definerte tidsrammer. Dette bidro til vedvarende eksponering knyttet til eldre teknologi og reduserte sikkerheten for at sikkerhetskontroller var anvendt konsekvent på tvers av miljøet. Dette understøtter behovet for en kontrollert migrerings- og avviklingsprosess for gjenværende eldre systemer, med tydelige eiere, ønsket sluttstatus og dokumentert lukking.

#### 3.2.1.6 Virksomhetskontinuitet og tjenestekritikalitet

Kommunen hadde etablert flere beredskaps- og kontinuitetselementer før hendelsen, herunder ROS-analyser, kontinuitetsplanlegging på sektornivå, kriseledelsesstrukturer, manuelle rutiner og eksterne ordninger for sikkerhetsovervåking og hendelseshåndtering. Intervjuene indikerer også at enkelte sektorer hadde kommet lenger i dette arbeidet. For eksempel fremkom det at et tjenesteområde med ansvar for kritiske innbyggertjenester hadde gjennomført ROS-analyser og BIA-arbeid, og hadde oversikt over hvilke systemer som var mest kritiske for kritisk tjenesteleveranse.

Deloittes vurdering er likevel at dette arbeidet i begrenset grad fremstod som en helhetlig, konsistent og testet operasjonsmodell på tvers av kommunen for håndtering av omfattende cyber- eller IKT-hendelser. Det gjennomgåtte materialet viste heller ikke at kommunen hadde etablert og øvd scenarioer som spesifikt omfattet løspengeangrep eller langvarig bortfall av sentrale IKT-tjenester.

Selv om det var gjennomført arbeid for å identifisere kritiske tjenester, avhengigheter og akseptabel nedetid, var det i mindre grad dokumentert hvordan informasjonssikkerhetsfunksjonen, IKT-funksjonen, tjenesteeiere, kriseledelsen og eksterne leverandører skulle samhandle under en større cyberhendelse. Dette gjaldt blant annet prioritering av tjenester, bruk av manuelle rutiner, leverandørkoordinering og beslutninger om gjenoppretting.

Hendelsen viser at kontinuitetsplanlegging for ordinære driftsforstyrrelser ikke nødvendigvis gir tilstrekkelig grunnlag for å håndtere langvarige cyberrelaterte avbrudd.

### 3.2.2 Tekniske funn

#### 3.2.2.1 Eksponering knyttet til eldre endepunkter muliggjorde den innledende kompromitteringen

Intervjuer og hendelsesrapporten indikerer at den innledende kompromitteringen skjedde på en enhet i et eldre driftsmiljø som ikke var fullt ut modernisert. Hendelsen illustrerer hvordan gjenværende eldre teknologi kan representere økt risiko dersom den ikke følges opp med tilstrekkelige sikkerhetskontroller og kompenserende tiltak frem til den er modernisert eller avviklet.

#### 3.2.2.2 Utilstrekkelig segmentering økte tilgjengelige angrepsveier

Intervjuer og dokumentasjon indikerer at deler av det berørte miljøet ikke hadde tilstrekkelig grad av logisk separasjon til å begrense konsekvensene av en kompromittering. Dette økte sannsynligheten for at en hendelse kunne få større omfang enn ønskelig.

#### 3.2.2.3 Svakheter knyttet til privilegert tilgang

Gjennomgangen indikerer at enkelte mekanismer for tilgangsstyring og beskyttelse av kritiske ressurser ikke ga tilstrekkelig risikoreduserende effekt. Dette kan ha bidratt til å øke konsekvensene av kompromitteringen.

#### 3.2.2.4 Mangler i serverovervåking og deteksjon

Gjennomgangen indikerer at sikkerhetsovervåkingen ikke hadde tilstrekkelig dekning i hele det berørte servermiljøet før hendelsen. Dette skapte begrenset synlighet i aktivitet på tvers av infrastrukturen og reduserte muligheten for tidlig og pålitelig deteksjon.

Selv om tilgjengelige logger i etterkant bidro til å rekonstruere deler av hendelsesforløpet, var overvåkingsdekningen ikke tilstrekkelig til å understøtte rettidig operativ respons. Hendelsen viser derfor at sentrale mekanismer for overvåking, varsling og oppfølging bør ha tilstrekkelig dekning og evalueres regelmessig, slik at eventuelle svakheter identifiseres og håndteres før en hendelse inntreffer.

#### *3.2.2.5 Begrenset nettverkstelemetri reduserte muligheten til å vurdere dataeksfiltrering*

Gjennomgangen indikerer at det forelå flere tekniske indikatorer på mulig dataeksfiltrering. Det tilgjengelige bevisgrunnlaget gjorde det imidlertid ikke mulig å fastslå presist hvilke filer eller datakategorier som eventuelt var overført.

Dette skapte usikkerhet i vurderingen og kommunikasjonen under hendelsen. Manglende bekreftelse på hvilke konkrete data som var overført, innebar ikke at dataeksfiltrering kunne utelukkes. Tilgjengelig informasjon tilsa at eksfiltrering måtte behandles som en reell risiko, selv om omfanget ikke kunne dokumenteres med tilstrekkelig presisjon.

En sentral årsak til usikkerheten var begrenset tilgang til detaljert informasjon om nettverkstrafikken. Dette reduserte muligheten til å identifisere avvikende utgående trafikk og dokumentere omfanget av mulig dataeksfiltrering.

Vurderingsgrunnlaget endret seg vesentlig etter at trusselaktøren publiserte og senere gjorde tilgjengelig et større datasett. Hendelsen viser behovet for å skille tydelig mellom at eksfiltrering ikke er bekreftet, at det ikke er identifisert hvilke konkrete data som er overført, og at det foreligger grunnlag for å konkludere med at eksfiltrering ikke har skjedd.

Hovedfunnet er at tilstrekkelig nettverkstelemetri understøtter både sikkerhet, personvern og presis kommunikasjon. Uten slik informasjon reduseres kommunens evne til å oppdage mulig dataeksfiltrering, vurdere hvilke opplysninger som kan være berørt og etablere et tilstrekkelig beslutningsgrunnlag for videre håndtering og varsling.

#### *3.2.2.6 Egress-kontroll og veier for dataeksfiltrering var ikke tilstrekkelig begrenset*

Hendelsesanalysen indikerer at servere ga mulighet for kommando- og kontrollaktivitet (C2) og mulig dataeksfiltrering. Hendelsesrapporten fra Move identifiserte verktøy og infrastruktur som kunne brukes til å overføre data ut av miljøet.

Dette forholdet er vesentlig fordi interne servermiljøer normalt ikke bør ha ubegrenset internettilgang. Der utgående tilgang er nødvendig, bør den være eksplisitt autorisert, logget og overvåket. Uten slike kontroller kan kompromitterte servere kommunisere med infrastruktur kontrollert av en trusselaktør, hente verktøy, opprettholde vedvarende tilgang eller eksfiltrere data uten umiddelbar deteksjon.

Hovedfunnet er at egress-kontroll for servere bør følge et «default deny»-prinsipp, støttet av eksplisitte tillatelseslister, håndheving gjennom DNS og proxy, varsling ved avvik og blokkering av kjente høyrisikodestinasjoner som Tor og kommando- og kontrollinfrastruktur (C2) der dette er praktisk mulig. Egress-kontroller bør gjennomgås sammen med SOC for å sikre at forsøk på brudd genererer varsler som kan følges opp operativt.

#### 3.2.2.7 SOC-varsling og responskapasitet

Hendelsesrapporten fra Move viser at det i perioden mellom 13. april og 9. mai ble identifisert flere SOC-varsler som sammenfalt med sentrale faser av angrepet, herunder rekognosering, lateral

bevegelse og aktivitet i forkant av at løsepengeviruset ble aktivert. Intervjuene indikerer samtidig at varslene som i ettertid fremstår som relevante for hendelsesforløpet, inngikk i et større volum av sikkerhetsvarsler som kommunen og leverandørene måtte forholde seg til. Dette gir kontekst for hvorfor enkeltvarsler kan ha vært krevende å identifisere og prioritere i sanntid.

Deloittes vurdering at relevante sikkerhetssignaler ikke ble identifisert, vurdert og prioritert raskt nok, og at deteksjonen ikke ble omsatt til rettidig operativ respons. Varslene førte ikke tidsnok til tilstrekkelig undersøkelse, eskalering og risikoreduserende tiltak før løsepengeviruset ble aktivert. Forbedringspunktet handler derfor både om evnen til å identifisere kritiske signaler i et større varselvolum og om å sikre at slike signaler raskt fører til operativ handling.

Intervjuene med IKT-funksjonen og Move indikerer at prosessen fra deteksjon til videre vurdering, prioritering og oppfølging ikke var tilstrekkelig tydelig definert eller operasjonalisert. Relevante signaler kunne dermed bli fanget opp uten at de raskt nok ble behandlet som del av en samlet og potensielt alvorlig sikkerhetshendelse.

Konsekvensen var at varslene ikke inngikk i en tilstrekkelig robust responsprosess med tydelig eierskap, klare alvorlighetskriterier, definerte responstider og avklarte eskaleringsveier. Dette økte risikoen for at relevante signaler ikke ble undersøkt og fulgt opp med nødvendig hastighet, særlig i et angrepsforløp der tidsvinduet mellom innledende aktivitet, lateral bevegelse og skadegjørende handling kan være kort.

Selv om det ikke er mulig å fastslå årsakene til forsinkelsene med sikkerhet, indikerer vurderingen særlig følgende forhold:

1. **Utilstrekkelig prioritering av kritiske signaler.** Relevante varsler inngikk i et større varselvolum og ble ikke identifisert og vurdert raskt nok som deler av et sammenhengende hendelsesforløp.

2. **Uklart eierskap til videre oppfølging.** Det fremstod ikke som tilstrekkelig tydelig hvem som skulle eie den videre vurderingen, sikre fremdrift og beslutte nødvendige tiltak.

3. **Mangelfull overgang fra deteksjon til respons**. Prosessen for å gå fra observasjon til undersøkelse, eskalering og operativ handling var ikke tilstrekkelig definert og operasjonalisert.

Disse forholdene må ses i sammenheng med de øvrige tekniske svakhetene beskrevet ovenfor. Den tekniske eksponeringen økte behovet for en responsmodell som raskt kunne identifisere og prioritere kritiske signaler og omsette dem til risikoreduserende tiltak.

Samlet viser dette at hendelsen ikke kan forklares med én enkelt svakhet. Den tekniske eksponeringen gjorde miljøet sårbart, mens svakheter i deteksjon, prioritering og operativ oppfølging begrenset evnen til å reagere effektivt da relevante signaler oppstod. Et sentralt forbedringspunkt er derfor å styrke kommunens evne til å omsette deteksjon til rettidig handling.

Hovedfunnet er at kritiske sikkerhetssignaler må identifiseres, vurderes og prioriteres raskere og inngå i en tydelig operativ responsprosess. Prosessen bør ha klare alvorlighetskriterier, definerte eskaleringsveier, forventninger til responstid og navngitte eiere. Dette er nærmere fulgt opp i forbedringsprogrammet gjennom forbedringsområde 2.

### 3.2.3 Utbedring og gjenoppbygging

Som del av vurderingsmetodikken gjennomførte Deloitte en begrenset verifikasjon av utbedrings- og gjenoppbyggingsaktivitetene som ble gjennomført av IKT-funksjonen og samarbeidspartneren Move. Gitt omfanget av kompromitteringen var denne verifikasjonen nødvendig for å vurdere om kjente trusler eller sårbarheter fortsatt var aktive i miljøet.

Basert på intervjuene med Move og IKT-funksjonen forstår vi at det nyetablerte miljøet er bygget opp med styrkede sikkerhetsmekanismer innen segmentering, identitets- og tilgangsstyring, sikkerhetsovervåking og respons på sikkerhetshendelser.

Deloittes avgrensede vurdering indikerer at det nyetablerte miljøet er utformet i tråd med anerkjent praksis for IKT-sikkerhet. For å opprettholde sikkerhetsnivået og dokumentere at kontrollene fungerer som forutsatt, må kommunen etablere en systematisk forvaltningsmodell og gjennomføre regelmessige sårbarhetsvurderinger og sikkerhetsoppdateringer, kontroll med eksterne forbindelser, oppdatert dokumentasjon, erstatning av midlertidige løsninger og periodisk testing av sikkerhetsovervåkingen og hendelseshåndteringsevnen.

#### *3.2.3.1 Restrisiko*

Kommunen har gjennomført en rekke tiltak, iverksatt sikkerhetstiltak og migrert store deler av tjenestene over til ny infrastruktur. Prosessen med å lukke kjent restrisiko er ikke fullstendig ferdigstilt, men vi forstår at dette arbeidet vil pågå frem til risikoen er bekreftet håndtert.

## 3.3 Konklusjon og oppsummering

Analysen i dette kapittelet viser at hendelsen må forstås som resultatet av en kjede av tekniske, organisatoriske og styringsmessige forhold. De tekniske svakhetene skapte angrepsmuligheter, mens svakheter i risikoeierskap, kontrolloppfølging, datalivssyklusstyring, sikkerhetsovervåking og operativ respons bidro til at risikoen kunne utvikle seg over tid, at responsen ble forsinket og at skadeomfanget økte. Cybersikkerhet må i denne sammenhengen forstås som et helhetlig og kontinuerlig arbeid der styring og ansvar, kompetanse og sikkerhetskultur, arbeidsprosesser, teknisk beskyttelse, overvåking, logging, beredskap og gjenoppretting virker sammen. Et tilstrekkelig sikkerhetsnivå er ikke statisk, men må vurderes og videreutvikles i takt med endringer i teknologi, sårbarheter, digitale avhengigheter og trusselbilde. Dette er et sentralt premiss for vurderingen av både hendelsen og kommunens videre forbedringsbehov.

Gjennomgangen viser at kommunen hadde mekanismer for å identifisere risiko og motta sikkerhetsvarsler, men at disse ikke konsekvent ble omsatt til rettidige, eide og dokumenterte tiltak. Flere relevante risikoer og kontrollmangler kunne ikke spores frem til gjennomført utbedring, formell beslutning, kompenserende kontroll eller eksplisitt aksept av restrisiko.

Tilsvarende ble relevante SOC-varsler generert under hendelsesforløpet, uten at modellen for prioritering, eierskap, eskalering og respons raskt nok førte til samlet undersøkelse og effektive begrensningstiltak. Forbedringsbehovet gjelder derfor både den tekniske overvåkingsdekningen og operasjonsmodellen som skal sikre at kritiske signaler blir forstått, prioritert, eid og fulgt opp med nødvendig hastighet.

Hovedutfordringen var dermed ikke et fullstendig fravær av rutiner, kontroller eller sikkerhetsinitiativer, men at den samlede kontrollkjeden ikke ga tilstrekkelig praktisk effekt. Forbedringsarbeidet bør derfor rette seg mot samspillet mellom styring og teknologi, med særlig vekt på tydelig eierskap, et godt beslutningsgrunnlag, dokumentert oppfølging, verifikasjon av gjennomførte tiltak og faktisk lukking av risikoer og sikkerhetsvarsler.

Med dette som utgangspunkt oppsummeres nedenfor svarene på kommunens prosjektspørsmål. Oppsummeringen gir direkte svar på spørsmålene og må ses i sammenheng med de mer detaljerte vurderingene i hendelsesanalysen, styringsfunnene og de tekniske funnene.

**Tekniske forhold**

- Utilstrekkelig beskyttelse av deler av IKT-miljøet
- Svakheter i styring og begrensning av tilganger
- Utilstrekkelig separasjon mellom systemer og miljøer
- Begrenset sikkerhetsovervåking og deteksjonsdekning
- Begrenset synlighet i aktivitet og dataflyt
- Tekniske kontrollsvakheter som økte hendelsens omfang

**Styringsmessige forhold**

- Risikoer ble ikke alltid fulgt til lukking
- Uklart risikoeierskap
- Begrenset kapasitet og budsjettmessig handlingsrom
- Manglende dokumentasjon av restrisiko
- Begrenset oppfølging av sikkerhetsvarsler
- Mangelfull verifikasjon av gjennomførte tiltak

1. ***Hvordan kunne informasjon bli lagret over tid?***

   Informasjon kunne bli liggende lagret over tid fordi migreringen og avviklingen av et eldre lagringsområde ikke hadde tilstrekkelig tydelig eierskap, dokumentasjon på sletting eller formell aksept av risikoen i perioden hvor data fortsatt lå i lagringsområdet. Deloitte har fått opplyst i intervjuer at et eldre lagringsområde historisk var underlagt tilgangsstyring og ikke var åpent tilgjengelig for brukere. Deloitte har imidlertid ikke gjennomført en uavhengig verifikasjon av den historiske tilgangsmodellen eller hvilke rettigheter som faktisk var tildelt

over tid. Vurderingen retter seg derfor primært mot datalivssyklus, eierskap, migrering, sletting og beskyttelse av informasjonen. Vurderingen indikerer at IKT ikke skulle slette data fra et eldre lagringsområde før hele migreringsprosjektet var fullført. Da prosjektet trakk ut i tid, ble informasjon liggende i det lagringsområdet lenger enn planlagt, uten at det forelå en tydelig beslutning om hvilken risiko dette medførte. Majoriteten av informasjonen er eldre. Imidlertid finnes det nyere informasjon, eksempelvis mappenavn og dokumenter fra 2026, som ikke kan spores til etablerte prosesser. Deloitte vurderer derfor at denne informasjonen opprettes ad-hoc.

Intervjuene indikerer også at enkelte ledere oppfattet bortfall av tilgang til et eldre lagringsområde som at informasjonen var slettet. I praksis var informasjonen fortsatt lagret i påvente av endelig sletting fra IKT. Dette skapte et gap mellom opplevd og faktisk kontroll over avdelingenes data. Lederne hadde ansvar for å rydde i dataene, men hadde ikke nødvendigvis dokumentasjon på at dataene faktisk var fjernet. Ansatte synes heller ikke å ha hatt et tydelig nok mandat, eller et praktisk kontrollrammeverk, som hindret videre bruk eller oppbevaring av data i området. Dette gjaldt selv om det forelå en migreringsplan og generell veiledning om hvor sensitiv informasjon skulle lagres, for eksempel i OneDrive eller SharePoint.

Resultatet var at sensitiv informasjon kunne hope seg opp i et lagringsområde som var kjent å være under avvikling, men som ennå ikke var sikkert avviklet. Denne konklusjonen støttes av funnene knyttet til datalivssyklus og personvern i avsnitt Styringsfunn, samt de tekniske funnene om eldre miljøer og angrepsveier i avsnitt Tekniske funn.

Hendelsen illustrerer også en bredere utfordring knyttet til informasjonsforvaltning. Kommunen hadde ikke en tilstrekkelig konsekvent mekanisme for å sikre at informasjon hadde identifiserte eiere, klassifisering, lagringsregler, dokumenterte slettebeslutninger og verifisert etterlevelse gjennom hele livssyklusen.

Risikoen knyttet til det eldre lagringsområdet bør derfor ikke forstås som et isolert migreringsproblem, men som et uttrykk for svakheter i styring av informasjon som virksomhetsressurs.

For å redusere tilsvarende risiko fremover bør kommunen sikre at informasjon forvaltes gjennom tydelige krav til eierskap, klassifisering, lagringstid, migrering, sletting og dokumentasjon av gjennomførte kontroller.

### *2. Hvorfor ble forholdene ikke identifisert tidligere?*

Forholdene ble ikke identifisert tidligere fordi kommunens kontrollmiljø ikke i tilstrekkelig grad ga oversikt over sentrale risikoer, hvordan disse ble fulgt opp, eller om avtalte risikoreduserende tiltak var implementert og fungerte som forutsatt. Flere relevante risikoforhold var kjent, eller burde kunne vært kjent, herunder svakheter i beskyttelsen og overvåkingen av deler av IKT-miljøet, ufullførte moderniserings- og avviklingsaktiviteter, mangelfull oppfølging av sikkerhetsvarsler og informasjon som ble oppbevart over tid. Disse forholdene ble imidlertid ikke konsekvent omsatt til sporbare, prioriterte og verifiserte utbedringstiltak.

Funnene indikerer at flere sikkerhetsvarsler ble generert før den skadegjørende aktiviteten ble gjennomført, men at varslene ikke førte til tilstrekkelig rettidig undersøkelse, eskalering og risikoreduserende tiltak. Utfordringen var derfor ikke nødvendigvis fravær av identifiserte sikkerhetsrisikoer eller varsler. Den sentrale utfordringen var at identifiserte risikoer og

signaler ikke ble håndtert, prioritert og fulgt opp effektivt frem til dokumentert lukking eller aksept av restrisiko.

### 3. *Hvilke forhold bidro til at risikoen utviklet seg?*

Risikoen utviklet seg gjennom en kombinasjon av teknisk eksponering og styringsmessige forhold. På den tekniske siden var det flere svakheter, tilgangskontroller og sluttbrukersikkerhet som sammen skapte mulighet for kompromittering og lateral bevegelse. Disse tekniske forholdene var ikke isolerte svakheter, men reflekterte en bredere utfordring med å opprettholde konsekvent livssykluskontroll over enheter, servere, programvare og infrastruktur i et komplekst og delvis eldre miljø.

Uklart eierskap og uklare mandater, budsjett- og kapasitetsbegrensninger, fragmenterte beslutningsveier og begrenset dokumentasjon på kontrollenes effektivitet bidro til at identifiserte risikoer ikke konsekvent ble omsatt til utbedringsaktiviteter. Tidligere identifiserte risikoer knyttet til ressursstyring og infrastruktur indikerer at kommunen hadde innsikt i flere relevante livssyklusutfordringer, herunder ufullstendig oversikt over enheter og virtuelle servere samt eldre IKT-produkter som ikke var faset ut. I lys av hendelsen reduserte dette sikkerheten for at ressurser var konsekvent godkjent, støttet, herdet, overvåket, migrert eller avviklet innen definerte tidsrammer. Samlet bidro disse forholdene både til muligheten for hendelsen og til forsinkelsen i å erkjenne alvorlighetsgraden.

### 4. *Hvilke kontroller eller tiltak fungerte utilstrekkelig?*

I denne vurderingen anses kontroller som utilstrekkelige dersom de ikke i tilstrekkelig grad bidro til å forebygge eller begrense hendelsesforløpet, avdekke og eskalere relevant aktivitet i tide, muliggjøre rettidige risikoreduserende tiltak eller redusere konsekvensene for informasjon og drift. Som nevnt tidligere peker hendelsen ikke på én isolert kontrollsvikt, men viser at flere administrative, forebyggende, detekterende, responderende og styringsmessige kontroller ikke fungerte samlet med den effektiviteten som scenarioet krevde.

På teknisk nivå bidro svakheter i forebyggende og detekterende kontroller til at den uautoriserte aktiviteten kunne utvikle seg og få større omfang. Begrensninger i overvåking, deteksjon og operativ oppfølging reduserte også kommunens evne til å oppdage, vurdere og stanse aktiviteten før den fikk vesentlige konsekvenser.

Fra et styrings- og operasjonsmodellperspektiv var hovedutfordringen ikke et fullstendig fravær av kontroller, men i hvilken grad kontrollene var implementert, integrert, testet, overvåket og fulgt opp i praksis. Dette var relevant på tvers av risikoeierskap og lukking, aksept av restrisiko, kontrolloppfølging i styringssystemet for informasjonssikkerhet, datalagring, lederansvar, kontinuitets- og gjenopprettingsplanlegging og eksterne sikkerhets- og hendelseshåndteringsordninger. Disse områdene påvirket hvorvidt identifiserte risikoer ble omsatt til gjennomførte utbedringstiltak, varsler ble omsatt til rettidig respons, kontinuitetsforutsetninger kunne legges til grunn under et avbrudd, og sensitiv informasjon ble aktivt styrt gjennom hele livssyklusen.

Samlet bidro kontrollsvakhetene til at hendelsen kunne utvikle seg over tid, få økt omfang og medføre konsekvenser for informasjon og tjenestedrift før effektive begrensningstiltak ble iverksatt. Kontrollmanglene er nærmere oppsummert i avsnittene Styringsfunn og Tekniske

funn. En kobling mellom kontrollmangler og relaterte læringstemaer fremgår også i kapitel 4, Læringspunkter.

5. ***Hvilke læringspunkter bør kommunen trekke?***

   Hendelsen viser at cyberrobusthet ikke kan vurderes ut fra enkeltstående tekniske kontroller alene, men må forstås som summen av styring, risikoeierskap, datahåndtering, teknisk sikkerhet, overvåking, hendelseshåndtering og ledelsesmessig oppfølging.

   Det viktigste læringspunktet er at identifiserte risikoer og sikkerhetsvarsler må følges helt frem til dokumentert lukking, formell beslutning om utsettelse eller eksplisitt aksept av restrisiko på riktig ledernivå. Hendelsen viser også at eldre teknologi, midlertidige løsninger krever aktiv risikostyring frem til de er migrert, avviklet eller underlagt kompenserende kontroller.

   Kommunen bør videre trekke lærdom av at deteksjon alene ikke er tilstrekkelig. Varsler må inngå i en operasjonsmodell med tydelig eierskap, definerte responstider, eskaleringsveier og forhåndsgodkjente begrensningstiltak. I tillegg viser hendelsen at sensitive data må ha tydelig eierskap, klassifisering, lagringsregler, sletting og teknisk beskyttelse gjennom hele livssyklusen. Disse læringspunktene er nærmere beskrevet i kapittel 4, Læringspunkter.

6. ***Hvilke konkrete forbedringstiltak anbefales?***

   Deloitte anbefaler at Lørenskog kommune håndterer forbedringstiltakene som et samlet forbedringsprogram for cyberrobusthet, og ikke som enkeltstående tekniske utbedringer. Programmet bør særlig prioritere tydeligere risikoeierskap og kontrolloppfølging, videreutvikling av SOC- og hendelseshåndteringsmodellen, kontrollert migrering og avvikling av eldre miljø, styrket datastyring og innebygd personvern, forbedret logging, EDR-dekning og nettverkstelemetri, samt testing av kontinuitet, gjenoppretting og leverandørberedskap.

   Deloitte anbefaler også at kommunen vurderer om IKT-funksjonens organisering, kapasitet, kompetanse og mandat er tilstrekkelig tilpasset kommunens digitale avhengighet, sikkerhetskrav og risikobilde. Dette bør ses som en forutsetning for å kunne redusere teknisk gjeld, lukke kjente sikkerhetsrisikoer og understøtte trygg digital tjenesteutvikling over tid. De anbefalte tiltakene er nærmere strukturert i forbedringsprogrammet i kapittel 5, Forbedringsprogram.

# 4 Læringspunkter

Hendelsen gir flere viktige læringspunkter for Lørenskog kommune. Selv om kompromitteringen ble muliggjort av konkrete tekniske svakheter, er den bredere læringen at cyberrobusthet avhenger av den samlede effekten av styring, datahåndtering, tekniske kontroller, overvåking, hendelseshåndtering og ledelsesmessig oppfølging. Kontrollmanglene som ble avdekket i gjennomgangen, viser at flere svakheter var viktige hver for seg, men mer vesentlige når de ses samlet som del av en bredere utfordring i operasjonsmodellen.

Dette er særlig relevant i lys av pågående organisatoriske endringer i kommunen, hvor nye strukturer og roller kan bidra til å styrke eierskap og koordinering, men hvor vurderingen fortsatt indikerer behov for tydeligere ende-til-ende-ansvar, eskaleringsveier og oppfølging av risiko knyttet til cyber- og informasjonssikkerhet. Hendelsen fremhever behovet for å styrke kommunens evne til å omsette identifiserte risikoer til eide, finansierte og verifiserte tiltak. Flere av de mest vesentlige læringspunktene handler ikke bare om hvorvidt kontroller var etablert, men om de var konsekvent implementert, overvåket, eskalert ved svikt og lukket med dokumentasjon.

## 4.1 Sentrale læringstemaer

De viktigste læringstemaene er oppsummert nedenfor:

- **Risiko må håndteres helt frem til lukking**. Hendelsen viser at risikoer som er kjent eller identifiserbare, men ikke eiet, finansiert og lukket, kan bli liggende som reell operasjonell eksponering over tid. Identifiserte sikkerhetsrisikoer bør derfor tildeles tydelige eiere, prioriteres, følges opp og lukkes med dokumentasjon. Der utbedring utsettes som følge av budsjett-, kapasitets- eller driftsmessige begrensninger, bør restrisiko aksepteres eksplisitt på riktig ledernivå og gjennomgås jevnlig.

- **Deteksjon må omsettes til respons.** Hendelsen viser at sikkerhetsvarsler har begrenset verdi dersom de ikke raskt blir triagert, eskalert, eid og fulgt opp med konkrete begrensningstiltak. Overvåking bør derfor ikke vurderes ut fra om varsler genereres alene, men ut fra om varslene fører til rettidig undersøkelse, beslutning og handling innen definerte responstider.

- **Eldre miljøer krever aktiv risikostyring**. Hendelsen viser at eldre miljøer og midlertidige løsninger kan bli stående som varig risiko dersom de ikke styres aktivt frem til migrering eller avvikling. Slike miljøer bør derfor ikke behandles som passiv teknisk gjeld, men følges opp med tydelige eiere, dokumenterte avhengigheter, frister, kompenserende kontroller og ledelsesrapportering frem til de er avviklet eller formelt akseptert som restrisiko.

- **Informasjon må forvaltes som en virksomhetsressurs**. Hendelsen viser at sensitiv informasjon kan akkumulere over tid dersom eierskap, klassifisering, lagringstid, migrering, sletting og dokumentasjon ikke styres som én sammenhengende livssyklus.

  Informasjonsforvaltning bør behandles som et styringsområde på linje med økonomi, kvalitet og risikostyring. Dette blir særlig viktig for sektorer som behandler helse- og omsorgsinformasjon, hvor fremtidige regulatoriske initiativer som EHDS forventes å stille økte krav.

Kommunen bør sikre tydelige dataeiere, dokumenterte lagrings- og sletteregler, klassifisering av informasjon og verifisering av at migrering og sletting faktisk er gjennomført.

- **Digitalisering krever riktig IKT-organisering, kapasitet og kompetanse**. Hendelsen viser at økt digital avhengighet stiller høyere krav til IKT-funksjonens kapasitet, kompetanse, mandat og gjennomslagskraft. Når teknisk gjeld, sikkerhetskrav og digitaliseringsambisjoner øker uten tilsvarende styrking av gjennomføringsevnen, kan kjente risikoer bli liggende uløst over tid. Kommunen bør derfor vurdere IKT- og sikkerhetskapasitet som en forutsetning for trygg digital tjenesteleveranse, ikke bare som et operativt ressursbehov.

- **Sensitive data krever livssyklusstyring og teknisk beskyttelse**. Hendelsen viser at sensitiv informasjon kan hope seg opp dersom eierskap, klassifisering, lagringsregler, migrering og sletting ikke styres som én sammenhengende prosess. Kommunen bør derfor sikre at sensitive data har tydelig eierskap og teknisk beskyttelse gjennom hele livssyklusen, og at migrering eller opprydding ikke anses som fullført før sletting, tilgangsstyring og eventuell restrisiko er dokumentert.

- **Kontrollenes effektivitet må dokumenteres.** Hendelsen viser at dokumenterte rutiner og etablerte initiativer ikke alene gir tilstrekkelig sikkerhet for at kontroller fungerer i praksis. Kommunen bør derfor styrke målingen av kontrollenes faktiske effektivitet, herunder om sentrale tekniske og organisatoriske kontroller er implementert, overvåket, testet og korrigert ved avvik.

- **Operasjonell cyber- og IKT-robusthet må øves ende-til-ende**. Hendelsen viser at cyberhendelser raskt berører både IKT, tjenesteområder, kriseledelse, leverandører, personvern og kommunikasjon. Kontinuitetsplaner, kriseledelsesstrukturer, IKT-rutiner og leverandørordninger bør derfor testes samlet gjennom realistiske scenarioer som validerer prioritering av tjenester, manuelle rutiner, leverandørkoordinering og gjenoppretting av kritiske tjenester under langvarige avbrudd.

## 4.2 Læringspunktmatrise

Matriseoversikten nedenfor kobler sentrale læringspunkter til relaterte kontrollmanglene. Den gir en tydelig fremstilling av hvordan én eller flere kontrollmangler kan knyttes til ett enkelt læringspunkt.

| Læringstema | Hva hendelsen viste | Relaterte kontrollområde |
|---|---|---|
| **Risiko må håndteres til lukking** | Kjente eller identifiserbare risikoer ble ikke konsekvent eiet, finansiert og lukket. | Risikoeierskap, restrisikoaksept, finansiering, handlingsplaner. |
| **Deteksjon må omsettes til respons** | SOC-varsler førte ikke raskt nok til triage, eskalering og begrensning. | SOC-modell, intern triage, responsmandat, playbooks |
| **Eldre miljøer må styres aktivt** | Legacy-miljøer og eldre lagringsområder ble stående med risiko over tid | Livssyklus, migrering, avvikling, segmentering. |

| | | |
|---|---|---|
| **Sensitive data må styres gjennom livssyklusen** | Sensitive personopplysninger og annen beskyttelsesverdig informasjon ble liggende i eldre lagringsområder. | Datalagring, sletting, klassifisering, DLP, DPIA. |
| **Kontrollenes effektivitet må dokumenteres** | Rutiner og tiltak var ikke alltid testet eller verifisert i praksis | ISMS, kontrolltesting, ledelsesrapportering, måleindikatorer |
| **Cyberrobusthet må øves ende-til-ende** | Kontinuitet, IKT, leverandører og kriseledelse må fungere sammen | Beredskap, gjenoppretting, leverandørstyring, øvelser |
| **IKT-kapasitet må samsvare med digital avhengighet** | Kapasitet og kompetanse påvirket evnen til risikoreduksjon | Organisering, bemanning, kompetanse, teknisk gjeld |

*Tabell 3: Overordnet læringspunktmatrise.*

# 5 Forbedringsprogram

Anbefalingene i dette kapittelet kan benyttes som en veiledende ramme for Lørenskog kommunes videre arbeid med et koordinert forbedringsprogram for digital robusthet, internkontroll og informasjonsforvaltning. Anbefalingene bør ses i sammenheng og ikke som et sett med enkeltstående tekniske utbedringstiltak.

Formålet med programmet er å omsette funnene og kontrollmanglene identifisert i rapporten til prioriterte, eide og målbare forbedringsområder som reduserer umiddelbar risiko og styrker kommunens cyberrobusthet over tid.

Detaljerte beskrivelser av enkelte tiltak er utelatt fra den offentlige versjonen fordi de, alene eller sammenstilt med annen informasjon, kan synliggjøre sårbarheter og dermed øke kommunens risikoeksponering. Forbedringsprogrammet dekker likevel konkret styring og eierskap til risiko, håndtering av sikkerhetsvarsler og hendelser, modernisering og avvikling av eldre løsninger, sikker informasjonsforvaltning, kontinuitet og leverandørberedskap samt nødvendig organisering, kapasitet og kompetanse. Den fullstendige tiltaksbeskrivelsen er gjort tilgjengelig for kommunen med begrenset tilgang.

Programmet bør særlig rette oppmerksomheten mot forholdene som i størst grad påvirket kommunens evne til å forebygge, oppdage, respondere på og gjenopprette etter hendelsen. Dette omfatter:

- risikoeierskap, prioritering og dokumentert lukking
- eskalering av sikkerhetsvarsler og rettidig operativ respons
- modernisering, migrering og kontrollert avvikling
- datastyring og informasjonsforvaltning
- teknisk synlighet og sikkerhetsovervåking
- koordinering og oppfølging av leverandører
- verifikasjon av kontrollenes gjennomføring og effekt
- IKT-funksjonens organisering, kapasitet, kompetanse og mandat

For å sikre fremdrift og dokumenterbar effekt bør programmet forankres i et omforent målbilde og understøttes med:

- tydelige program- og tiltakseiere
- risikobasert prioritering
- avklarte beslutninger om finansiering, kapasitet og kompetanse
- definerte leveranser og milepæler
- regelmessig ledelsesrapportering
- evidensbasert verifikasjon og lukking av tiltak

## 5.1 Programstruktur og prioritering

Forbedringsprogrammet bør struktureres som et helhetlig og flerårig initiativ som samler oppfølgingen av læringspunktene, kontrollmanglene og forbedringsbehovene identifisert gjennom denne vurderingen. Programmet bør organiseres rundt konsoliderte forbedringsområder og sikre at identifiserte forhold følges opp gjennom planlegging, gjennomføring, verifikasjon og evaluering av tiltak over tid, samtidig som sporbarheten til rapportens funn og kontrollmangler bevares.

Tiltakene vil ha ulik tidshorisont, forventet effekt og organisatorisk påvirkning. Enkelte områder bør prioriteres på kort sikt for å redusere gjenværende eksponering, sikre rettidig operativ oppfølging av

kritiske sikkerhetsvarsler og etablere tydelig risikoeierskap. Andre områder vil kreve mer langsiktig utvikling og gradvis integrering i kommunens styringsprosesser, arbeidsformer og kontrollmekanismer.

Som en mulig retning for gjennomføringen kan forbedringsprogrammet struktureres i tre overordnede faser:

- **Fase 1 – Stabilisere og redusere kjent risiko:** Prioritere tiltak som reduserer gjenværende eksponering i det eldre miljøet, styrker den operative oppfølgingen av kritiske sikkerhetsvarsler og etablerer tydelig eierskap, beslutninger og dokumentert oppfølging av risiko.
- **Fase 2 – Styrke kontrollmiljøet:** Videreutvikle kommunens internkontroll, informasjonsforvaltning, tekniske synlighet, kontinuitet og leverandørberedskap slik at etablerte krav, rutiner og kontrollmekanismer fungerer mer helhetlig og konsistent i praksis.
- **Fase 3 – Bygge langsiktig cyberrobusthet:** Styrke organisering, kapasitet, kompetanse, rollebasert ansvar og sikkerhetskultur slik at kommunens evne til å håndtere digital risiko utvikles i takt med den digitale avhengigheten og risikobildet.

Fasene angir en overordnet prioriteringsretning og bør ikke forstås som strengt sekvensielle. Flere tiltak vil måtte gjennomføres parallelt, og enkelte forbedringsområder vil kreve kontinuerlig oppfølging gjennom hele programperioden. Faseinndelingen bør derfor videreutvikles og konkretiseres som del av en innledende program- og prosjektdesignfase.

Prioriteringen bør baseres på risiko, avhengigheter, gjennomførbarhet og forventet risikoreduksjon. Effekten av tiltakene bør samtidig vurderes på tvers av dimensjonene styring og strategi, prosess, mennesker og teknologi. Dette vil bidra til at nødvendige endringer ses i sammenheng, og at tiltakene gir dokumenterbar og varig effekt.

# Vedlegg B: Intervjuliste

Følgende personer ble intervjuet som del av prosjektmetodikken for å identifisere og vurdere kontrollmangler, herunder læringspunkter og anbefalinger for videre oppfølging.

| # | Beskrivelse og formål |
|---|---|
| 1 | Formålet var å avklare spørsmål etter gjennomgangen av hendelsesrapporten, herunder den tekniske hendelsesrekken, gjennomførte og planlagte utbedringstiltak samt grunnlaget for kommunens vurdering av mulig dataeksponering. |
| 2 | Formålet med møtet var å få en overordnet forståelse av den tekniske hendelsesrekken, gjenoppbyggingsarbeidet, sikkerhetsovervåkingen og status for videre oppfølging av identifiserte risikoer. |
| 3 | Formålet var å få bedre innsikt i gjenopprettings- og gjenoppbyggingsarbeidet etter hendelsen. Møtet omfattet status, fremdrift og sentrale avhengigheter i arbeidet med å gjenopprette systemer og tjenester, samt overordnede tiltak for å styrke sikkerheten og redusere risikoen for tilsvarende hendelser. |
| 4 | Formålet var å få bedre innsikt i Lørenskog kommunes kritiske prosesser, særlig prosesser med betydning for liv og helse, og de teknologiske avhengighetene knyttet til disse. De viktigste temaene som ble drøftet var kritiske tjenester og systemer, sentrale avhengigheter, konsekvenser ved bortfall eller redusert funksjon, samt eksisterende risiko- og kontinuitetsvurderinger. |
| 5 | Formålet var å få bedre innsikt i Lørenskog kommunes arbeid med personvern, internkontroll og internrevisjon, særlig knyttet til datalagring, etterlevelse av GDPR, risikovurderinger, DPIA-prosesser og oppfølging av identifiserte funn. De viktigste temaene som ble drøftet, var roller og ansvar for personvern og internkontroll, praktisk etterlevelse av lagrings- og slettingsrutiner, bruk og avvikling av et eldre lagringsområde, lederansvar og oppfølging av internkontroll, samt hvordan funn fra revisjoner og ledelsens gjennomgang følges opp i organisasjonen. Det ble også diskutert forbedringsområder knyttet til dataklassifisering, behandlingsprotokoller, lederopplæring, styringskultur og kapasitet til å gjennomføre og lukke tiltak. |
| 6 | Formålet med møtet var å få bedre innsikt i kommunens arbeid med informasjonssikkerhet, herunder organisering, styring, risikoidentifikasjon og risikoreduksjon. De viktigste temaene som ble drøftet, var informasjonssikkerhetsfunksjonens mandat og organisatoriske plassering, samhandling med ledelse, sektorer og øvrige fagfunksjoner, samt prosesser for å identifisere, vurdere og følge opp risikoer. Det ble også diskutert hvordan styringssystemet for informasjonssikkerhet er bygget opp, herunder roller, ansvar, internkontroll, opplæring, etterlevelse og måling av sikkerhetsarbeidet. Videre omhandlet møtet erfaringer knyttet til oppfølging av identifiserte risikoer og sikkerhetstiltak, samt informasjonssikkerhetsfunksjonens rolle i beredskapsarbeid og håndtering av den aktuelle hendelsen. |
| 7 | Formålet var å få bedre innsikt i organiseringen av IKT-funksjonen i Lørenskog kommune, samt ansvar, roller og beslutningsprosesser knyttet til IKT-drift og informasjonssikkerhet. De viktigste temaene som ble drøftet, var IKT-leders rolle og mandat, oppfølging av tidligere identifiserte sikkerhetsfunn, budsjett- og prioriteringsprosesser, kapasitet og bemanning i IKT-avdelingen, samt samhandlingen mellom IT og informasjonssikkerhetsfunksjonen. Det ble også diskutert hvordan sikkerhetsrelaterte behov og tiltak løftes i organisasjonen, hvordan tidligere funn og anbefalinger har blitt fulgt opp, samt hvilke verktøy, prosesser og styringsmekanismer som benyttes for å dokumentere og følge opp IKT- og sikkerhetsarbeidet. |
| 8 | Formålet med møtet var å forstå omfanget og innretningen av sikkerhetsovervåkingen, hvordan relevante sikkerhetssignaler ble håndtert, og hvilke muligheter som finnes for å videreutvikle overvåkings- og responskapabilitetene. |
| 9 | Formålet med møtet var å få en overordnet forståelse av kommunens sikkerhetsovervåking og hvordan tilgjengelig sikkerhetsinformasjon kan benyttes til å identifisere, undersøke og følge opp mulige sikkerhetshendelser. |

*Tabell 4: Intervjuliste*