Vedlegg B – Utfordringsbildet i kommunal sektor

Innhold

Varierende grad av styringsevne innen informasjonssikkerhetsområdet

Evne til styring og prioritering innenfor digitalisering krever kompetanse og kapasitet også innen informasjonssikkerhet og personvern. Det er gjennomgående enighet blant kommunene om at det er ressurs- og kompetansemangel innen disse fagområdene[1].

De underliggende årsakene til den opplevde ressurs- og kompetansemangelen er sammensatte. Særlig for små kommuner vil det være utfordrende å prioritere dedikerte ressurser på informasjonssikkerhet og personvern, og i tillegg er arbeidsmarkedet på disse fagområdene presset. Det har også vist seg å være utfordrende å rekruttere spesialistkompetanse til distriktene, selv om unntak finnes. Små som store kommuner skal levere de samme lovpålagte tjenestene, der kommunene vil stå overfor de samme problemstillingene innen informasjonssikkerhet og personvern uavhengig av størrelse. De små og mellomstore kommunene har imidlertid mindre ressurser og kapasitet til å ivareta sitt ansvar og utføre oppgavene.

En annen stor utfordring for den enkelte kommune, er omfanget av kompetansen nødvendig for å digitalisere og hente ut gevinster fra dette arbeidet. Digitaliseringsprosjekter- og arbeid krever tverrfaglige team, sammensatt av ulike fag-, forvaltning-, og kompetanseområder. Som tidligere beskrevet har små og store kommuner de samme behovene, men ulik tilgang og mulighet til å allokere tilstrekkelig ressurser og kapasitet i digitaliseringsarbeidet.

I dag er det en lang rekke IKT-samarbeidsformer i sektoren, men det eksisterer fortsatt et potensiale for deling av ressurser, kompetanse og kapasitet mellom ulike aktører i kommunal sektor. Ulikt modenhetsnivå medfører også at det er ulik erfaringsdeling og nyttiggjørelse av kompetanse og kapasitet i digitaliseringsnettverkene.

Veiledere og retningslinjer som tilgjengeliggjøres av aktører med veiledningsansvar er i liten grad samkjørte, og det kan argumenteres for at disse ikke i tilstrekkelig grad tar høyde for hurtig teknologisk utvikling- og endring.

De fleste kommuner har tilpasset seg veiledere ved å etablere et styringssystem for informasjonssikkerhet, men det er ofte ikke innlemmet med kommunens øvrige virksomhet- og styring[2]. På lik linje som at styringssystemet for informasjonssikkerhet er etablert som en isolert prosess, som regel utenfor eksisterende kommunale styringsaktiviteter, er også beslutninger som

[1] Vedlegg E, «Styringsevne (herunder kontrollfunksjon) innen informasjonssikkerhetsområdet».
[2] Vedlegg E, «Styringsevne (herunder kontrollfunksjon) innen informasjonssikkerhetsområdet».

gjelder informasjonssikkerhet og personvern ofte ikke tilstrekkelig forankret og etablert i beslutningsprosesser og strukturer i kommunene og fylkeskommunene. Dette påvirker beslutninger, prosjekter, og til slutt digital robusthet i tjenestene på en negativ måte.

God styring fordrer at hele spektret av digital transformasjon innlemmes i kommunenes etablerte virksomsomhetsstyring og internkontroll. Alternativet blir svak styring av hele digitaliseringskjeden hvis kommunene ikke har en helhetlig tilnærming.

Har varierende grad av nødvendig sikring av teknisk infrastruktur

Kommunene og fylkeskommunene har, på samme måte som alle andre virksomheter i Norge, etablert digitale løsninger over tid. For de aller fleste kommunene er investeringer i digitale tjenester langsiktig. Utfordringene er at maskinvaren og digitale tjenestene har en kort levetid, typisk mellom 5 og 10 år.

Det finnes systemer i bruk i kommuner i dag som har vært i bruk over 20 år. Det finnes også eksempler på svært gamle maskinvareløsninger. Hovedutfordringen med gamle og utdaterte løsninger er vedlikehold. Slike systemer støttes ikke i lengden av leverandørene («end of life»-produkter), og eventuelle sårbarheter som blir avdekket vil ikke bli lukket. Over tid vil infrastrukturen til en vanlig kommune inneholde flere slike gamle løsninger, og sårbarhetsflaten øker.

Samtidig innføres det nye løsninger gjennom digitaliseringsløft, som ofte bygger oppå de gamle løsningene, og det innføres nye leverandører som også krever oppfølging dersom man skal ha kontroll med hele verdikjeden.

Selv for en liten kommune vil infrastrukturen inneholde hundrevis av systemer og løsninger for integrasjoner. Dette gjør at det er svært ressurskrevende å forsøke å vedlikeholde alle løsningene og å følge opp leverandørene, noe som igjen gjør det utfordrende å ivareta sikkerheten[3]. Det er en kjensgjerning at kommunal sektor har teknisk gjeld. Det gir bekymring for ytterligere manglende sikring av teknisk infrastruktur.

Drift av teknisk infrastruktur innebærer også oppdatering av sikringsmekanismene for infrastrukturen. Dette er en krevende oppgave både i form av kompetanse og kapasitet når det skal skje i en omfattende infrastruktur i stadig endring.

For å ha mulighet til å oppnå tilfredsstillende sikring av teknisk infrastruktur, må det gjøres løpende vurdering av risiko, vurdering av tiltak som ofte krever investeringer, prioritering og implementering er aktiviteter. Alle disse aktivitetene krever ulik kompetanse og en betydelig ressursinnsats selv for små kommuner.

Har varierende grad av nødvendig evne til å forebygge og oppdage hendelser

Informasjonsinnhentingen gir indikasjon på at kommunenes evne til å oppdage mulige og faktiske hendelser er begrenset[4]. Alle kommuner har enten gjennom etablering av egen organisasjon, samarbeid med andre kommuner eller innkjøp, sikret seg at de rent driftsoperative oppgavene blir løst. I tillegg er det mange kommuner som er i stand til å oppdage og håndtere avvik fra god praksis.

[3] Vedlegg E, «Løpende sikring av all IT-infrastruktur, inkludert skytjenester, overvåking, analyse- og hendelseshåndtering og beredskaps- og gjenopprettingsevne».

[4] Vedlegg E, «Styringsevne (herunder kontrollfunksjon) innen informasjonssikkerhetsområdet» og «Løpende sikring av all IT-infrastruktur, inkludert skytjenester, overvåking, analyse- og hendelseshåndtering og beredskaps- og gjenopprettingsevne».

Det er likevel bare et fåtall kommuner som har etablert organisasjon og verktøy for å overvåke sikkerheten i egen infrastruktur, for eksempel gjennom et overvåkingssenter (Security Operations Center, SOC)[5], og dermed har etablert en evne til å oppdage og håndtere sikkerhetshendelser.

Mangelen på overvåking av hendelser i egen teknisk infrastruktur gjør det svært krevende å avdekke hendelser på et tidlig stadium, og gjør at trusselaktører får operere i kommunen tekniske infrastruktur uten å bli oppdaget. Eksempler fra tidligere hendelser har vist at enkelte trusselaktører har hatt tilgang til systemene i måneder før de slår til med utpressing eller andre handlinger.

Evne til å avdekke og håndtere en sofistikert angriper i sanntid krever svært mye av en virksomhet. Det er i dag en utfordring i kommunal sektor at det ikke i tilstrekkelig grad er etablert organisasjon og verktøy for å oppdage hendelser. Manglende tilgang på kompetanse svekker styringsevnen og gjør også at problemstillingen med manglende evne til å oppdage hendelser aldri kommer til beslutning i kommuneledelsen.

Har varierende grad av nødvendig evne til å håndtere hendelser

Det er få kommuner som har innarbeidet digitale hendelser i beredskapsplanverket, og det er enda færre som har trent eller øvet på slike hendelser[6].

Det er også svært få kommuner som har etablert eller anskaffet en hendelseshåndteringsenhet (Incident Response Team (IRT)). I bakkant av en hendelse vil det også kunne være aktuelt med å gjenopprette til normal drift, en oppgave som også kan være krevende. Østre Toten kommune og andre virksomheter som har blitt rammet av digital utpressing har brukt lang tid på å komme i normal drift. Å planlegge for, og ha tilgjengelig kompetanse over tid, blir derfor også helt sentralt i evnen til å håndtere hendelser og tiden etter.

Årsaksforhold

Det er som nevnt store forskjeller på kommunene når det gjelder hvilke og i hvilken grad de har utfordringer på disse områdene, men generelt for kommunene er det utfordringer på ett eller flere av de ovennevnte områdene. Årsaken til den varierende modenheten kan i stor grad forklares ut fra:

- Ressurstilgang (personell og økonomi).
- Kompetanse og informasjonstilgang.
- Evne til drift, vedlikehold, utvikling og innføring av teknologi og digitalisering.
- Forvaltningsmodeller.
- Strategisk styringskompetanse (politisk og administrativt nivå).

[5] Vedlegg E, «Løpende sikring av all IT-infrastruktur, inkludert skytjenester, overvåking, analyse- og hendelseshåndtering og beredskaps- og gjenopprettingsevne».

[6] Vedlegg E, «Styringsevne (herunder kontrollfunksjon) innen informasjonssikkerhetsområdet» og «Løpende sikring av all IT-infrastruktur, inkludert skytjenester, overvåking, analyse- og hendelseshåndtering og beredskaps- og gjenopprettingsevne».