Til kommunedirektør

Fra KS

Datasikkerhets- og beredskapstiltak i kommunal sektor

Hva saken gjelder

Med bakgrunn i dataangrepet mot Østre Toten 9. januar 2021 og trusselbildet i det digital rom, er KS vurdering at flere kommuner vil kunne bli rammet av liknende dataangrep. KS velger derfor å komme med råd og anbefalinger som vi ber kommunen vurdere. KS mener det er nødvendig at kommunene vurderer egen sikkerhets- og sårbarhetssituasjon og treffer egnede tiltak for å redusere risikoen for at denne type hendelser skjer. Når en hendelse først skjer må kommunen på forhånd ha etablert nødvendige tiltak som sørger for at konsekvensene blir lavest mulig.

Flere aktører kan være aktuelle å benytte som støtte for kommuner, eksempelvis Nasjonal sikkerhetsmyndighet, Norsk Helsenett med sitt responssenter og Kommune-CSIRT (responssenter under etablering). KS vil gå i dialog med KMD og andre statlige aktører for å få en best mulig sikkerhet- og beredskapsstøtte for kommunene.

Alvorlige konsekvenser

De fleste kommunale tjenester er helt avhengig av en velfungerende IT-infrastruktur og tilhørende støttesystemer. Resultatet av et dataangrep vil i ytterste konsekvens føre til at kommunen blir totalt lammet over en lengre periode. Kostnadene for å få kommunen tilbake i normal drift vil kunne beløpe seg til 10-talls millioner kroner, selv for kommuner av medium størrelse. Større kommuner må påregne mer. Sensitive data på avveie vil kunne innebære en nasjonal risiko og/eller brudd på personvernet og rettsikkerheten til den enkelte borger. Dette vil kunne føre til erstatningskrav og/eller bøter, at sensitive data misbrukes av andre, at andre tilknyttede IT-systemer (samarbeidspartnere/3.part) kan bli kompromittert eller at man mister tillit til data/systemer og må rekonstruere disse.

KS foreslår flere tiltak

Kommunedirektør har det øverste ansvaret for informasjonssikkerhet og personvern i kommunen. For å øke kommunens sikkerhets- og beredskapsevner innen datasikkerhetshendelser og datainnbrudd anbefaler KS etter dialog med medlemmer og nasjonale myndigheter flere tiltak. Tiltakene i denne listen oppfordrer vi kommunedirektør til å gjennomgå med relevant ledelse for å få en vurdering av om de allerede er ivaretatt eller om det finnes en plan for å iverksette de så raskt som mulig.

KS foreslår følgende undersøkelser og vurdering av tiltak dersom punktene besvares negativt;

1) Grunnsikring av systemer og funksjoner, undersøk
    a) om det er gjennomført en sikkerhetsrevisjon av IT-infrastruktur og systemer. Undersøk om kommunen har nødvendig sikkerhetskompetanse for å gjennomføre en slik sikkerhetsrevisjon.
    b) om det er gjennomført sikkerhet- og sårbarhetstest av IT-infrastruktur og systemer. Hvis dette ikke er gjennomført, anbefales det at dette gjennomføres så raskt som mulig. Automatiske sikkerhetstester bør gjennomføres kontinuerlig og svakheter som avdekkes bør rettes snarest.

2) Risiko- og sårbarhetsanalyse - sikring av kritiske funksjoner og tjenester, undersøk
    a) om det er kartlagt hvilke funksjoner/tjenester i kommunen som anses som kritiske.
    b) om det er kartlagt hvilke systemer som støtter de kritiske funksjonene/tjenestene og hvor kritiske disse faktisk anses å være.
    c) om det er kartlagt kritiske systemers avhengigheter, og hvilke konsekvenser det vil ha for kommunens funksjonsevne hvis disse systemene blir utilgjengelige, eller at man mister tillitt til dem fordi data er manipulert eller på avveie.

3) Sikring av systemer, undersøk
    a) om systemer benytter tilstrekkelig sikkerhetsnivå for identifisering av brukere (for eksempel 2-trinns bekreftelse ved pålogging, som passord og kode)
    b) om det finnes gjenopprettelsesrutiner og om backup er plassert slik at denne ikke kan bli kryptert eller manipulert.
    c) om program og maskinvare som ikke lenger mottar oppdateringer er faset ut, eller at det finnes en plan for å fase disse ut så raskt som mulig.
    d) om det finnes overvåkningssystemer som gir varsel ved dataangrep eller forsøk på manipulering av systemer, samt system/prosess for å følge opp varslene.

4) Beredskapsplan og krisehåndtering
    a) Sikre at det finnes beredskapsplan hvis et dataangrep, eller bortfall av IT systemer av annen grunn, rammer kommunen.
    b) Sikre at det finnes navngitte personer (hos underleverandør, kommunen, eksterne sikkerhetsmiljøer og eventuelt andre enheter) med deres tilgjengelighet som skaffer til veie nødvendige ressurser når angrepet/krisen inntreffer. Det vil si hvem skal kommunen ringe, og hvilke ressurspådrag er tilgjengelig når angrepet/krisen inntreffer.
    c) Vurder om kommunen har nødvendig kompetanse til å håndtere dataangrepet/krisen, samt nødvendig kompetanse for gjenoppretting?
    d) Undersøk om kommunene har gjennomført krise- og beredskapsøvelser med utgangspunkt i bortfall eller manipulering av IT-infrastruktur og systemer. Hvis ikke, anbefales det at dette gjennomføres raskest mulig. Se for eksempel ovelse.no som er utarbeidet av DSB.

5) Administrativt
    a) Kommunen anbefales å ta kontakt med sitt forsikringsselskap og få skriftlig svar på hvorvidt de er forsikret mot Cyber-kriminalitet, herunder datainnbrudd mv. Dersom de har slik forsikring anbefales det å få en oversikt over hva som er dekket og en sammenlikning med hva andre selskaper dekker. Hvis man ikke er dekket bør kommunen vurdere å tegne slik forsikring – gitt de betydelige kostnadene et alvorlig dataangrep kan medføre.
    b) Vurder om kommunen har tilknyttet nødvendig sikkerhetskompetanse, herunder personvernkompetanse, til å gjøre løpende sikkerhets- og personvern vurderinger, og rapportere tilstanden til egnet beslutningspunkt i kommunen.

Eget informasjonsskriv med mer teknisk informasjon er sendt IT-ansvarlig/IT-sikkerhetsansvarlig i alle kommuner.

Mvh

Lasse Hansen
Adm Dir KS

Kristin W Wieland
Områdedirektør