Til kommunenes IT ansvarlig/IT-Sikkerhetsansvarlig

Fra KS

Datasikkerhets- og beredskapstiltak i kommunal sektor – vurderinger og tiltak for IT-ansvarlig/IT sikkerhetsansvarlig

Hva saken gjelder

Med bakgrunn i dataangrepet mot Østre Toten 9. januar 2021 og trusselbildet i det digital rom, er KS vurdering i likhet med nasjonale myndigheter at flere kommuner er utsatt for å kunne rammes av liknende dataangrep i tiden som kommer. KS kommer derfor med en rekke råd og anbefalinger vi ber kommunen vurdere, og i den grad dette ikke allerede er ivaretatt at kommunen 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.

Et eget skriv om dette er sendt alle kommunedirektører/rådmenn. (vedlagt)

Alvorlig konsekvenser

Resultatet av et dataangrep vil i ytterst konsekvens føre til at kommunen vil bli totalt lammet over en lengre periode. Kostnadene for å få kommunen tilbake i normal drift vil selv for kommuner av median-størrelse kunne beløpe seg til 10-talls millioner kroner, enda mer for større kommuner. 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 tillitt til data/systemer og må rekonstruere disse.

KS foreslår flere tiltak

Kommunaldirektør/Rådmann har det øverste ansvaret for informasjonssikkerhet og personvern i kommunen. For å øke kommunens sikkerhets- og beredskapsevner innen datasikkerhetshendelser og datainnbrudd anbefaler KS flere punkter som kommunedirektøren bør vurdere, med iverksettelse av tiltak dersom de ikke alt er ivaretatt. Samtidig anbefaler vi at IT-ansvarlig, alternativt sikkerhetsansvarlig vurderer en rekke tiltak beskrevet nedenfor. Vi er klar over at flere kommuner allerede driver et godt sikkerhetsarbeid og trolig har iverksatt mye av dette allerede, for andre kommuner kan det være mer som bør vurderes gjennomført. Flere tiltak kan bli aktuelle i tiden som kommer, så langt foreslås følgende med bakgrunn i løsepengevirus:

1) Grunnsikring av systemer
    a) Installer sikkerhetsoppdateringer så raskt som mulig etter lansering.
    b) Sikre at det finnes prosess for å oppdatere programvaren jevnlig og om dette gjøres i tråd med retningslinjene fra leverandør. Hvis ikke, vurder konsekvens av at dette ikke gjøres.
    c) Følge NSMs grunnprinsipper.

2) Sikring av passord
    a) Sørg for at det benyttes lange, sikre og unike passord over alt i tråd med nasjonale anbefalinger.

3) For ytterligere herding av systemer
    a) Herde alle løsninger som er eksponert mot internett ekstra godt/nøye, og gjennomgå oppsettet regelmessig for å sikre at det er "up to date".
    b) Vurdere, evt. påse at det er kartlagt «Single point of failure» i IT-infrastruktur eller systemer (altså et punkt eller komponent som medfører fatale konsekvenser for kommunens funksjoner/tjenester ved bortfall eller feil).
    c) Ikke åpne for flere porter/tjenester/host/destinasjon enn det som er absolutt nødvendig i brannmurer.
    d) Ikke tillatt RDP fra internett mot virksomhetens ressurser dersom det er mulig.
    e) Aldri tillatt RDP fra virksomhetens internetteksponerte resurser (DMZ) til andre sikkerhetssoner (slik som DMZ 2, servernett 1 og klientnett 1).
    f) Blokker all trafikk mot TOR-nettverket dersom dette ikke er strengt nødvendig.
    g) Ikke tildel sluttbrukere administrator-rettigheter.
    h) Blokker kjøring av ikke-autorisert programvare.

4) For ytterligere sikring av Microsoft operativsystem
    a) Benytt Local Administrator Password Solution (LAPS) på klienter og servere der det er mulig/aktuelt (eller tilsvarende løsninger for å hindre at det samme lokale administratorpassord benyttes på flere enheter).
    b) For Microsoft operativsystem: Opprett GPO der det er mulig/aktuelt som setter "Interactive logon: Number of previous logons to cache (in case domain controller is not available)" på klienter og servere så lav som mulig. Dette gjør det vanskeligere for angriper å få tak i brukernavn og passord.

5) Overvåkning, logging og filtrering
    a) Logg og overvåk aktivitet på kontoer med utvidede rettigheter (som administrator/service-kontoer).
    b) Påse at det finnes sikkerhetslogger og at disse er plassert slik at de ikke kan manipuleres. At sikkerhetslogger lagres i minst tre måneder, helst enda lenger hvis mulig.
    c) Benytt IP-filter/IPS/GEO-blokkering i FW/proxy for å beskytte internett-eksponerte tjenester. Tillatt kommunikasjon kun til/fra aktuelle IPer eller områder/land (f.eks. Norge dersom ansatte kun skal nå tjenesten fra Norge).
    d) Benytt Web/DNS-filter som hindrer servere og klienter i å kontakte uønskede nettsider på internett (dersom denne internett-tilgangen er nødvendig).
    e) Ha kontroll på og overvåkning av hvilke tjenester som er internetteksponert, deriblant åpne RDP-tjenester og andre fjernaksessløsninger.
    f) Ha kontroll på og overvåkning av datatrafikk mellom ulike soner.
    g) Ha tilstrekkelig logging av tjenester man benytter og bevar disse loggene i tilstrekkelig tid, f.eks. tre måneder. Lagre disse loggene slik at de ikke kan manipuleres.

6) Automatisk sårbarhetskartlegging (Allvis NOR)

Vi oppfordrer at kommunen har en automatisert sårbarhetskartleggingstjeneste som kontrollerer alle internetteksponerte ressurser/tjenester regelmessig (ukentlig). KS har dialog med NSM og ber om at kommunen som minimum slutter seg til NSMs automatiserte sårbarhetskartlegger (Allvis NOR). Hvis kommunen allerede er tilknyttet tjenesten, oppfordrer vi til at man går gjennom innsendte opplysninger og påser at disse er oppdatert/korrekt.

For mer informasjon om automatisk sårbarhetskartlegger se: https://nsm.no/tjenester/allvis-nor/

For mer informasjon om hvordan man knytter seg til tjenestene se: https://doc.allvis.no/

For øvrig henvises det til denne artikkelen hos NSM om løsepengeviruset: Løsepengevirus - Nasjonal sikkerhetsmyndighet (nsm.no)

Det kan bli aktuelt med flere tiltak i tiden som kommer. KS følger situasjoner tett. Ta kontakt med Suhail.mushtaq@ks.no ved spørsmål.

Mvh

Asbjørn Finstad
Avdelingsdirektør Strategisk IKT og digitalisering

Suhail Mushtaq
Fagsjef informasjonssikkerhet