DRAMMEN KOMMUNE
– et godt sted å leve

Spørsmål 176 (2023) fra Herman Ekle Lund (Venstre): Spørsmål om kommunens IT Policy

Til:	Kommunedirektøren	Dato:	12.12.2023
Fra:	Herman Ekle Lund (V)	Saksnr:	23/00858-177
		Deres ref:	

Stemmer det at kommunen har vedtatt en ny IT-Policy som utestenger Mac-brukere fra kommunens digitale grensesnitt?

Jeg ble kjent med denne begrensningen etter at jeg som Mac-bruker nylig ble kastet ut av tilgangen på Framsikt, og etter dette ikke lenger får lov til å autorisere maskinen som arbeidsverktøy lenger.

Hvis ja: denne beslutningen er ikke tatt politisk. På hvilket nivå ble den tatt, og hva var begrunnelsen?

Hvordan kan det tilrettelegges for en politisk omgjøring av dette vedtaket?

Jeg vil minne om at det er over 100 millioner Mac-brukere på verdensbasis. Andelen Mac-brukere i Norge er kjent for å være svært høy i forhold til andre land. Det er med andre trolig en stor andel innbyggere som nå effektivt utestenges fra sentrale tjenester i Drammen kommunes IT-univers, og tvinges over på Microsoft-plattform, skulle de ha behov for dette. Jeg kan ikke se at kommunen har hjemmel til å opprette slike effektive monopol blant kommersielle leverandører, og jeg kan i hvert fall ikke se at det harmonerer med målene i samfunnsdelen om å være verken en serviceinnstilt og næringsvennlig kommune.

Svar

Kommunen administrerer i dag ca. 21.200 enheter, hvorav ca. 13.000 pc-er og 8200 iPader. Disse enhetene har programvare som ivaretar sikkerheten. For å kostnadsoptimalisere har kommunen standardisert på Windows-pc-er, iPader og Microsofts sikkerhetsprodukter.

Februar 2022 ble strategien for teknologi og arkitektur på IKT-plattformen vedtatt etter en høringsrunde i kommunens administrasjon. Denne strategien bygger videre på Nasjonal sikkerhetsmyndighets (NSM) grunnprinsipper for IKT-sikkerhet og prinsippet om «Zero Trust» (tillitsløs sikkerhetsmodell).

Drammen til sky-prosjektet ble initiert våren 2022, blant annet for å realisere teknologi- og arkitekturstrategien. Dette prosjektet ble presentert i formannskapet i 9. mai 2023. Hovedtemaene i denne presentasjonen var hvordan kommunen kunne møte utfordringene med Microsoft som leverandør, Schrems II dommen og det digitale trusselbildet.

7. desember 2023 ble Lov om digital sikkerhet vedtatt i Stortinget. Dette vil på sikt øke kravene til sikkerhet, også i kommunal sektor.

Ansvaret for kommunens sikkerhet er underlagt kommunedirektøren som virksomhetens øverste leder (KS: Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet s. 14). Det er kommunedirektøren som har det øverste ansvaret for at kravene i personopplysningsloven, sikkerhetsloven og eForvaltningsforskriften etterleves i hele kommunen. Videre står det i kommuneloven §22-1 «Kommunestyret og fylkestinget har det øverste ansvaret for å kontrollere kommunens og fylkeskommunens virksomhet.»

Trusselbilde i endring

Ny teknologi gir nye muligheter for tjenesteproduksjonen, men også for ondsinnede aktører som ønsker å utnytte sårbarhetene som teknologien fører med seg. Best kjent av hendelser i kommunesektoren er dataangrepet på Østre Toten kommune i 2021, som medførte flere måneder uten tilgjengelige data og over 30 millioner i kostnader for å bygge opp kommunens systemer. Vi har også sett andre mer eller mindre vellykkede angrep på kommuner, bedrifter og institusjoner som fort kunne fått like katastrofalt resultat. De ondsinnede aktørene er organiserte kriminelle som stadig finner nye måter å nå målet sitt på, og det er bare et tidsspørsmål før vi står ovenfor en ny hendelse som på Østre Toten. Norske kommuner er attraktive mål for angripere.

I vår egen kommune hadde vi et angrep på Vann og avløp vinteren 2021 som hemmet produksjonen til tjenesteområdet og fikk betydelige økonomiske konsekvenser. Vi har også sett lignende saker hos både Departementenes sikkerhets- og serviceorganisasjon og på Stortinget.

Bruk av private enheter

Enheter som ikke administreres av Drammen kommune - enten de administreres av en annen arbeidsgiver eller tilhører privatpersoner, betegnes i denne sammenheng som *private enheter*. Private enheter kan både være Mac, PC, nettbrett og telefoner.

Private enheter som ikke administreres av Drammen kommune kan være en sikkerhetsrisiko. Når kommunen ikke administrerer enheten vil vi ikke ha kontroll på programvare som ivaretar sikkerheten (antivirus), operativsystemoppdateringer, sikkerhetslogger, eventuell skadevare som kan være installert eller hvilke brukerkontoer som har tilgang til enheten. Dersom en enhet administrert av kommunen kommer på avveie, kan virksomhet IKT stenge tilgangen til enheten for å hindre misbruk. Denne muligheten har man ikke for private enheter.

Enkelte av kommunens applikasjoner inneholder data kategorisert som sensitive. Dette inkluderer Framsikt, som er et verktøy for kommunens virksomhetsplanlegging og -oppfølging, inkludert økonomisk styring. Tilgang til denne type applikasjoner må begrenses for å sikre at data ikke kommer på avveie. Derfor er tilgangen til slike applikasjoner begrenset til enheter administrert av Drammen kommune.

Tilrettelegging for private enheter

Det finnes løsninger for å tilrettelegge for bruk av private enheter. Dette kalles *Bring your own device (BYOD).*

Å tilrettelegge for private enheter innebærer at kommunen må ha et kompetanse- og utviklingsmiljø for dette, i tillegg må det investeres i supplerende teknologi. Dagens løsning følger vedtatt strategi.

Brukerstøtte og tilgjengelighet vil kreve større og bredere kompetanse når enhetene ikke er standardiserte. Kommunen vil da måtte bygge kompetanse innenfor områdene utvikling og brukerstøtte..

Bring your own device er ikke anbefalt i henhold til NSMs grunnprinsipper på grunn av kompleksiteten rundt håndheving av dette.

BYOD vil ikke fungere for private enheter som allerede er administrert av andre virksomheter/arbeidsgivere.

Risikoreduserende tiltak

Med utviklingen i trusselbildet blir systematisk arbeid med risikoreduserende tiltak stadig like viktig. Det består i hovedsak i å ha lavest mulig risiko på systemsiden og at brukerne er kjent og oppdatert på det til enhver tid gjeldende trusselbildet. Hvis noe skjer, må organisasjonen også være i stand til å oppdage og håndtere uautorisert inntrenging i kommunens infrastruktur. En komplisert og sammensatt systemportefølje gjør slik oppfølging mer krevende.