Svak kompetanse på cybersikkerhet – Behov for å styrke kommunene

Kommunal Rapport 30.10.2026

En undersøkelse av offentlige virksomheter, fylkeskommuner og kommuner viser et sammensatt bilde av sektorens kompetanse.

Kristin Weidemann Wieland, direktør for forskning innovasjon og digitalisering i KS, mener kommuner ikke lenger kan arbeide med cybersikkerheten alene.
Kortversjon

- En ny rapport sier at kommunene har svakere cyberkompetanse enn staten.
- Nærmere åtte av ti offentlige virksomheter har planer og prosedyrer for å håndtere cyberangrep.
- Bare 43 prosent oppgir at de øver regelmessig.
- KS ønsker sterkere IKT-samarbeid mellom kommuner.

Oppsummeringen er generert av Labrador AI, og kvalitetssikret av en journalist.

Rambøll har publisert sin årlige undersøkelse IT i praksis. Resultatene viser at 76 prosent av offentlige virksomheter oppgir at de har klare prosedyrer for å rapportere og håndtere cyberangrep.

Fakta «Undersøkelsen IT i praksis»
IT i praksis er en undersøkelse av digitalisering i offentlig sektor og gjennomføres av Rambøll i samarbeid med Digdir, KS, TEK Norge og NTNU.

Årets undersøkelse bygger på svar fra 269 statlige virksomheter, kommuner og fylkeskommuner, om lag 1 000 innbyggere og rundt 160 små og mellomstore private virksomheter.

Undersøkelsen har fulgt digitaliseringen i offentlig sektor i 20 år.

To av tre har planer for å gjenopprette systemer og data. Likevel mener bare 44 prosent at de har nok kompetanse på cybersikkerhet, og bare 42 prosent sier de øver regelmessig.

Det er den operative kapasiteten, ikke planverket, som avgjør om virksomhetene klarer å håndtere et angrep når det oppstår, står det i rapporten.

Under halvparten av offentlige virksomheter mener de ansatte forstår, etterlever og tar ansvar for informasjonssikkerhet i det daglige arbeidet.

Dårlige kommuneresultater
Resultatene viser at kommunene gjør det dårligere enn staten på visse områder.
56 prosent av statlige virksomhet er enige i påstanden «Vi har tilstrekkelig kompetanse innen cybersikkerhet i vår virksomhet», mot 39 prosent i kommunene.

Bare 40 prosent av kommunene oppgir at de gjennomfører regelmessige øvelser for å håndtere cyberangrep, mot 48 prosent i staten.

Etablert sikkerhetsarbeid
Rapporten konkluderer med at sikkerhetsarbeidet i offentlig sektor er i stor grad etablert.
De fleste virksomheter har dedikerte sikkerhetsfunksjoner, gjennomfører risikovurderinger og oppgir god oversikt over egne verdier og systemer.

Likevel er det her også stor forskjell på stat og kommune. 70 prosent av de statlige virksomhetene oppgir at de har tilstrekkelig kompetanse på informasjonssikkerhet, mot 56 prosent i kommunesektoren.

Samlet oppgir 60 prosent offentlige virksomheter i 2026 at de har tilstrekkelig kompetanse og ressurser på informasjonssikkerhet. Dette en nedgang på fem prosentpoeng fra fjoråret. I 2021 sa 37 prosent av virksomhetene at de hadde nok kompetanse.

Fallet det siste året kan ses i sammenheng med digitalsikkerhetsloven som trådte i kraft 1. oktober 2025. Loven innebærer skjerpede krav til blant annet styringssystemer, risikovurderinger, beredskap og hendelseshåndtering, står det i rapporten.

Behov for å vurdere IKT-samarbeid
Kristin Weidemann Wieland, direktør for forskning, innovasjon og digitalisering i KS, mener det er et behov for å styrke kommunenes robusthet mot cyberangrep.

Når angrepene treffer handler det ikke først og fremst om at IT-systemene går ned, men at alle tjenestene som er avhengig av teknologien blir satt ut av spill, skriver Weidemann Wieland.

Hun mener at mange kommuner ikke lenger kan arbeide med cybersikkerheten alene. Weidemann Wieland svarer til Kommunal Rapport at det nå kan være behov for å vurdere om samarbeid om IKT kan gjøres sterkere og mer robuste.

Weidemann Wieland mener det så raskt som mulig må komme felles infrastrukturer for deling og forvaltning av data på tvers av stat og kommunal sektor.

Selv for relativt store kommuner krever dette ofte samarbeid for tilgang til tilstrekkelig kompetanse og kapasitet.

Hun er tydelig på at det må øves på cybersikkerhet. Dessuten ønsker hun seg flere felles tiltak for å bygge motstandskraft i kommunal sektor.

Vi må i fellesskap på tvers av stat og kommunal sektor, så raskt som mulig, få etablert en felles infrastruktur for deling og forvaltning av data, skriver hun og fortsetter:
Dette er avgjørende både for sammenhengende digitale tjenester og mulighetene for å ta ut potensialet i KI, men også for å kunne ivareta suverenitet og digitalt handlingsrom når krisen treffer.

Ekspert: – Bekymringsfullt
Mohsen Toorani er førsteamanuensis i cybersikkerhet ved Universitetet i Sørøst-Norge. Han mener det er bekymringsfullt at 76 prosent oppgir å ha prosedyrer for håndtering av cyberangrep, mens bare 42 prosent oppgir at de øver regelmessig.

Prosedyrer gir ingen garanti for at virksomheten vil kunne håndtere et reelt angrep, skriver han.

Mohsen Toorani mener noen av resultatene gir grunn til bekymring.
Toorani kaller det «et alvorlig signal» på spørsmål om hvor sårbart det er at under halvparten vurderer egen kompetanse på cybersikkerhet som tilstrekkelig.

– Tilstrekkelig kompetanse er viktig både for å forebygge og oppdage angrep og for å håndtere hendelser når de oppstår, skriver han.

Likevel understreker han at svarene er virksomhetenes egne vurderinger, og ikke en objektiv måling av sikkerhetskompetansen.

Toorani er tydelig på at undersøkelsen ikke er tilstrekkelig til å konkludere med at offentlig sektor er generelt dårlig beskyttet mot cyberangrep.

Jeg mener det er behov for større oppmerksomhet rundt praktisk beredskap og systematisk evaluering av sikkerhetstiltak. Et sentralt spørsmål er ikke bare hvor ofte virksomhetene øver, men om øvelsene faktisk bidrar til bedre evne til å håndtere cyberangrep, avslutter han.

Flere cyberangrep
Flere kommuner har opplevd omfattende cyberangrep. I mai opplevde Lørenskog kommune et løsepengevirus-angrep. Hackerne fikk tak i 1,34 millioner filer.
Blant dokumentene var det journalnotater og henvendelser til psykisk helsevern i kommunen.

I april ble det kjent at hackere hadde fått tak i flere av Bergen kommunes beredskapsplaner i et cyberangrep i fjor. Ifølge daværende byrådsleder Christine Meyer (H) fikk hackerne bare tak i utdaterte beredskapsplaner.

Andre kommuner har blitt utsatt for såkalte tjenestenektangrep, også kjent som DDOS. I 2025 opplevde både Ringerike og Trondheim at hackere sendte kunstig høy aktivitet til nettsidene med mål om å stenge reelle brukere ute.

Skjerpede krav
I rapporten står det at digitalsikkerhetsloven, som trådte i kraft 1. oktober 2025, har skjerpet kravene til styringssystemer, risikovurderinger, beredskap og hendelseshåndtering.

Virksomhetene vurderer seg derfor både mot en strengere målestokk og et mer krevende sikkerhetspolitisk bakteppe, står det.

Rambøll skriver i sin rapport at totalforsvaret er avhengige av at digitale tjenester, kommunikasjonsløsninger og styringssystemer tåler press.

I rapporten understrekes det at noen av resultatene i rapporten kan ses i sammenheng med den nye loven, med skjerpede krav.

Her er rapporten: IT i praksis 2026