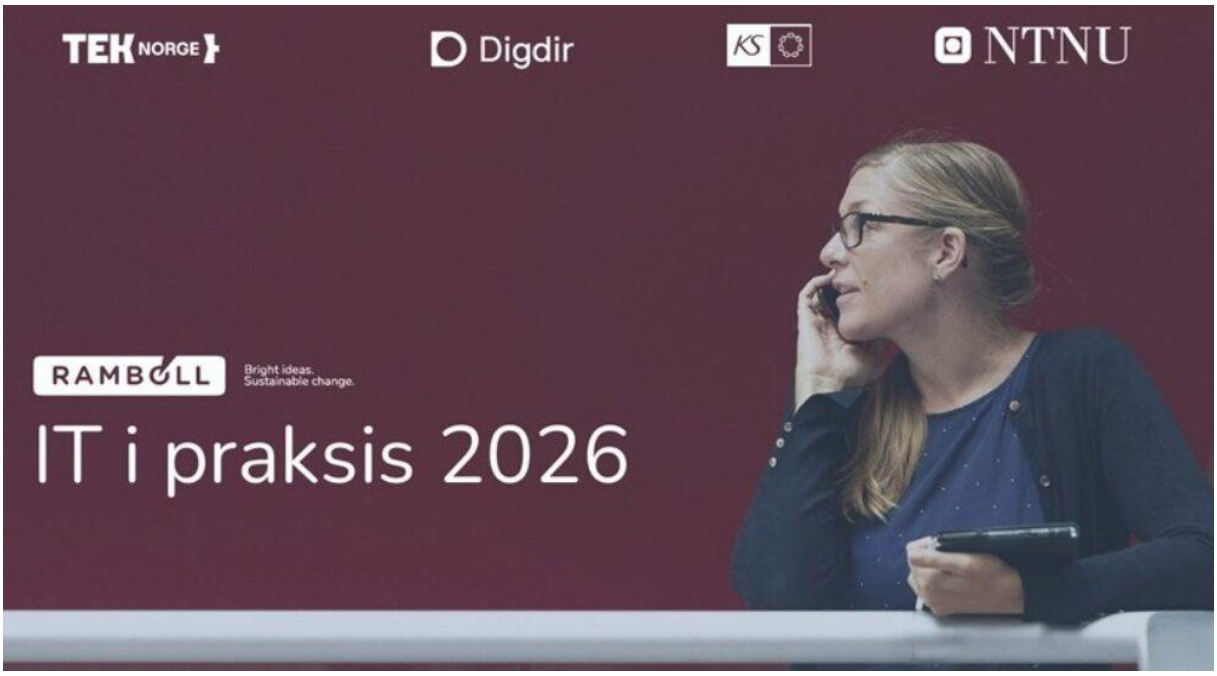

Utsnitt av forsiden til IT i praksis 2026

Beredskapen må testes før angrepet kommer

Publisert 22.10.2026

Den siste tiden har vist at dataangrep mot norske virksomheter rammer bredere, skjer raskere og får større konsekvenser enn før.

Samtidig peker også myndighetenes trusselvurderinger på et mer krevende digitalt risikobilde og økende bruk av kunstig intelligens i cyberangrep. I dette landskapet blir spørsmålet stadig mer presserende: Er offentlige virksomheter forberedt når neste alvorlige angrep treffer?

I årets utgave av ***IT i praksis*** (pdf) har det blitt målt hvor godt rustet offentlige virksomheter er til å håndtere cyberangrep. 76 prosent oppgir at de har klare prosedyrer for å rapportere og håndtere angrep, og to av tre har planer for å gjenopprette systemer og data.

Planverket virker å være på plass, men tallene for utøvelsen viser en annen historie. Bare 39 prosent av kommunene/fylkeskommunene mener de har nok kompetanse på cybersikkerhet, og bare 40 prosent øver regelmessig. Under halvparten mener at de ansatte etterlever sikkerhetskravene i hverdagen.

Etter flere år med jevn framgang faller andelen offentlige virksomheter som opplever å ha nok kompetanse og ressurser på informasjonssikkerhet, fra 65 til 60 prosent.

Virksomhetene oppgir i stor grad at de opplever styringssignalene som forpliktende og tydelige, men likevel mener bare rundt halvparten av kommunene/fylkeskommunene at de får god støtte fra nasjonale myndigheter til å gjennomføre dem (hhv. 54 prosent innen informasjonssikkerhet, 55 prosent innen personvern og 51 prosent innen cybersikkerhet). Tilsvarende tall for statlige virksomheter ligger rundt 10 prosentpoeng lavere.

Bare halvparten av innbyggerne stoler på at det offentlige tar godt vare på personopplysningene deres, og den tilliten har vært stabilt lav i flere år. Bildet blir verre når man undersøker tilliten til

beskyttelsen av offentlig digital infrastruktur. Bare 4 prosent er helt enige i at det offentlige er godt beskyttet mot cyberangrep, mens 18 prosent er helt uenige.

Årets andre temarapport i *IT i praksis* peker på at løsningen ikke først og fremst er flere krav eller planer, men sterkere gjennomføringsevne.

Årets andre temarapport i *IT i praksis* peker på at løsningen ikke først og fremst er flere krav eller planer, men sterkere gjennomføringsevne. Dette gjelder spesielt i en tid hvor kunstig intelligens bidrar til et mer krevende trusselbilde.

Mer kompetanse, hyppigere øvelser, bedre etterlevelse i virksomhetene og mer konkret støtte til å omsette nasjonale krav til praktiske tiltak kan være løsningen. Det er et behov for flere felles øvelser, mer deling av kompetanse og lavterskel veiledning, som vil gjøre det enklere for både statlige virksomheter og kommuner/fylkeskommuner å styrke beredskapen i praksis.

Rapportene viser at digitalisering og sikkerhet ikke er to uavhengige størrelser.

Utfordringen blir ikke mindre i årene som kommer. Den første temarapporten om KI fra *IT i praksis* viste at bruken av kunstig intelligens øker raskt i offentlig sektor. Den samme teknologien som gir store muligheter for effektivisering og innovasjon, bidrar også til et mer krevende trusselbilde, der cyberangrep kan gjennomføres raskere, mer målrettet og i større skala enn tidligere. Rapportene viser at digitalisering og sikkerhet ikke er to uavhengige størrelser. Jo mer av samfunnet som blir digitalt, desto viktigere blir evnen til å beskytte tjenestene, dataene og tilliten de bygger på.

Om IT i praksis

IT i praksis er den mest omfattende undersøkelsen 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.

Kilde: KS

https://www.ks.no/pressemeldinger/beredskapen-ma-testes-for-angrepet-kommer/

Publisert: 22.10.2026