Artikkel publisert på KS sin nettside 21.10.2026, hentet den 06.11.2026

Beredskapen må testes før angrepet kommer

Den siste tiden har vist at dataangrep mot norske virksomheter rammer bredere, skjer raskere og får større konsekvenser enn før. Samtidig peker også trusselvurderinger på et mer krevende digitalt risikobilde og økende bruk av KI i cyberangrep.



Foto: Stockphoto

Beredskapen må testes før angrepet kommer.

I dette landskapet blir spørsmålet stadig mer presserende: Er offentlige virksomheter forberedt når neste alvorlige angrep treffer?

Les rapporten her (pdf)

Planverk er ikke det samme som beredskap

I årets utgave av *IT i praksis* 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 44 prosent mener de har nok kompetanse på cybersikkerhet, og bare 42 prosent øver regelmessig. Under halvparten mener at de ansatte etterlever sikkerhetskravene i hverdagen.

– En beredskapsplan som aldri er øvd, er en plan, men ikke faktisk beredskap. Når et angrep inntreffer, er det folkene som avgjør utfallet, ikke dokumentene. Vi må øve langt oftere, bygge kompetanse i organisasjonene og bruke den eksisterende kompetansen i næringslivet mye bedre. Offentlig og privat sektor må stå sammen om dette, sier Øyvind Husby, administrerende direktør i TEK Norge.

Forpliktende krav, men mangelfull støtte

Etter flere år med jevn framgang faller andelen 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 halvparten at de får god støtte fra nasjonale myndigheter til å gjennomføre dem.

– Nå er hjelpen for fragmentert. Vi som gir veiledning og støtte jobber for å samordne dette. Råd, verktøy og veiledning skal være enklere å finne og enklere å bruke. Slik vil vi tilrettelegge for bedre styringsevne og tilstrekkelig digital sikkerhet i offentlige virksomheter. På Sikkert.no, som ble lansert i vår, samles råd, verktøy og kontaktpunkter til myndighetene på ett sted. Her finner man også anbefalinger vi står samlet bak, og gode råd om forebygging og veien til hjelp den dagen noe går galt, sier Frode Danielsen, direktør i Digdir.

Innbyggerne er skeptiske til beskyttelsen

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 vi 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.

Skepsisen som har blitt målt er i forkant av cyberangrep mot offentlige virksomheter som har fått stor oppmerksomhet, blant annet etter dataangrepet mot Lørenskog kommune og flere tjenestenektangrep mot statlige fellestjenester. Når offentlige virksomheter selv rapporterer om manglende kompetanse og få øvelser, er det heller ikke overraskende at innbyggerne stiller spørsmål ved hvor godt samfunnet er forberedt.

– Når et cyberangrep treffer, er det ikke IKT-systemene som går ned – det er selve tjenestene til befolkningen som ofte rammes. Kommunene er samfunnets førstelinje og har ansvar for de fleste offentlige tjenestene. Mange har små fagmiljøer og kan ikke bygge opp alt alene – så vi er helt avhengige av samarbeid på tvers av kommunegrenser. Svaret er delt kompetanse, felles øvelser og støtte som passer hverdagen i kommunene. Det er ikke nok å bygge opp statlig veilederkapasitet – vi trenger rammer som gjør det mulig å bygge robuste fagmiljø og sikkerhetskultur der kommunene selv har eierskapet – og nasjonal infrastruktur og kapabiliteter som støtter opp under arbeidet, sier Kristin Weidemann Wieland, direktør for forskning, innovasjon og digitalisering i KS.

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, slik nevnt i vår første rapport om KI. 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 å styrke beredskapen i praksis.

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.

Les rapporten her (pdf)

Kontaktinformasjon

Iris Maria Makridis, Senior Market Manager, Rambøll Management Consulting
Telefon: +47 92 47 14 81
E-post: irma@ramboll.com

Dette er en felles pressemelding fra Digdir, KS, TEK Norge og NTNU.

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.