NPISK - Foreslåtte kortsiktige tiltak

Proposisjon 78 S 2021-2022 fremmer behovet for å øke motstandsdyktigheten mot digitale angrep i kommunal sektor, med særskilt fokus på små og mellomstore kommuner. Dette handler bl.a. om å motvirke datainnbrudd, unngå løsepengevirus og opprettholde tilgjengeligheten til kommunens datasystemer. I utgangspunktet er dette et virksomhetsansvar, men en del kommuner – spesielt de små og mellomstore – har faglige og økonomiske utfordringer med å ivareta dette ansvaret.

Det foreslås å øke bevilgningen med 40 mill. kroner i 2022 for å legge til rette for at kommunene kan knytte seg til et cybersikkerhetssamarbeid (CERT eller tilsvarende). Målet med tiltaket er å øke kommunenes evne til å oppdage, forebygge og håndtere digitale angrep. Innretningen må avklares nærmere med berørte aktører. Flere alternativer kan være aktuelle, herunder å utvide kapasiteten i en eksisterende CERT, eller etablering av en ny kapasitet (post 22).

Videre foreslås det i proposisjonen en ordning for å styrke kommunenes kompetanse og kapasitet til å forebygge og håndtere digitale hendelser med en ramme på 10 millioner kroner. Målet med bevilgningen er å bidra til en rask økning i kommunenes evne til å oppdage, forebygge og håndtere digitale angrep (post 61).

Tiltakene som foreslås svarer ut post 22 og 61 i proposisjonen. Tiltakene er bygget opp som arbeidspakker til bruk i kommunene. Det legges videre opp at kommunene vil få veiledning og bistand til gjennomføring av arbeidspakkene. Trusselbildet tatt i betraktning legges det opptil at tiltakene iverksettes i parallell så langt det lar seg gjøre.

Tiltakene vil bli gjennomført med en kombinasjon av kommunene selv, deres IT-leverandører, digitaliseringsnettverkene, HelseCert, KommuneCSIRT og ekstern bistand. På enkelt steder er det utførere i parentes, disse har ikke bekreftet deres bidrag tilbake eller innhold i deres bidrag.

KS anbefaler følgende kortsiktige tiltak:

Arbeidspakke	**Begrunnelse**	**Pri**	**Utførende**	**Effektmål og måleparameter**	**Kostnads-overslag**	**NSM grunnprinsipp/ kobling til 78 S**
1. Bevisstgjøre						
Forankring, mottak og kommunikasjon a) Forankring av NPISK i kommunal sektor.	Formålet med arbeidspakken er å ha tilstrekkelig forankring i kommunal sektor for NPISK.	1	1.a,b,c) Program, KS og Diginettverkene.	Effektmål: Sørge for at NPISK og hvilke effekter det skal gi er godt kjent i		Post 22/61

b) Sørge for at NPISK er tilstrekkelig kommunisert i kommunal sektor. c) Sørge for å ha nødvendig innførings- og mottaksstruktur for å gjennomføre NPISK.	Videre sørge for at kommunal sektor har tilstrekkelig innførings- og mottaksapparat for både å innføre og ta imot programmet, samt tilstrekkelig kommunisert hva det inneholder.			kommunal sektor. Måleparameter: Kjennskap og innhold i programmet		
2. Øke motstandsdyktighet						
a) Sårbarhet: 1) Sårbarhetsskanning. 2) Sjekkliste sårbarhetsreduksjon. 3) Bistand sårbarhetsreduksjon. 4) Bistand sikkert oppsett M365. b) Utarbeide felles kommunale sikkerhetskrav c) Digital Due Diligence d) Situasjonsoversikt. e) Felles ROS / M365.	Målet med arbeidspakken er å redusere sårbarhetsflaten og oppnå et minimum sikkerhetstilstand i tråd med beste praksis og et tilstrekkelig kunnskapsgrunnlag for sikkerhetstilstand i kommunal sektor. Videre er målet med arbeidspakken å oppdage og fjerne kjente sårbarheter (både eksterne og interne (i e-postsegment første omgang). Det kan bidra til å verifisere etablerte sikkerhetstiltak, eventuelt peke på mangler og vurdere egen beredskap. Dette vil gi gevinster i form av at tiltak som er målrettede, mer treffsikre og mindre kostnadskrevende.		2.a.1) Program/HelseCert/KommuneCSIRT 2.a.2) HelseCert/KommuneCSIRT 2.a.3) HelseCert/KommuneCSIRT 2.a.4) Program/Microsoft 2.b) Program/KS/(DFØ) 2.c) Program/ekstern part 2.d) Program/HelseCert/KommuneCSIRT (DFØ) 2.e) Program/kommuner	Effektmål: Redusert sårbarhetsflate (nasjonalt)		Beskytte og opprettholde/ post 22/61

	Formålet med å utarbeide felles kommunale sikkerhetskrav vil bidra til økt sikkerhet i anskaffelser og oppfølgning av dem i etterkant. Det er mange store og viktige tjeneste- og driftsleverandører som leverer til kommunal sektor. Formålet med en Digital Due Diligence er sikre at disse tjeneste- og driftsleverandørene leverer tjenester som har tilstrekkelig sikkerhet og beredskap, samt har kapasitet til å håndtere hendelser i de tjeneste som leveres fra dem til kommunal sektor. Situasjonsoversikt innebærer at kommunene har en enkel oversikt over sin sårbarhetssituasjon og en «standardisert» modenhetsskala. Mange kommuner sliter i dag med å gjennomføre gode risiko og sårbarhetsanalyser. Programmet legger opp til gjenbruk og utarbeide felles ROS for kommunal sektor, i første omgang for M365.					

3. Forbedre beredskap og hendelseshåndtering						
a) Sjekkliste for beredskap og hendelseshåndtering. b) Sørge for tilknytning og SLA CERT. c) Sørge for at kommunene har en egenevne for hendelseshåndtering. d) Kommunikasjonsnettverk for å dele informasjon på tvers. e) Regional SOC / M365	Arbeidspakke for beredskap og hendelseshåndtering er tiltenkt for å øke kommunens evne til å håndtere, gjenopprette og begrense skadeomfanget etter et digitalt angrep. Arbeidspakken skal bidra til at kommunene kan forberede, vurdere, kontrollere, håndtere hendelser, og gjenopprette normaltilstand. Arbeidspakken skal i tillegg sørge for at alle er tilknyttet et responsmiljø, samt sikre at kommuner har en nødvendig egenevne til å oppdage og håndtere hendelser. Arbeidspakken vil også sørge for at kommuner får bistand til å opprette beredskaps- og kontinuitetsplaner samt kunne måle sin egenevne til å kunne stå i et hendelsesforløp. Det vil også opprette et kommunikasjonsnettverk i kommunal sektor for å kunne utveksle sikkerhetsinformasjon seg imellom og mellom CERT.		3.a) Program/HelseCert/KommuneCSIRT 3.b) Program/HelseCert /KommuneCSIRT 3.c) Program 3.d) Program/ HelseCert /KommuneCSIRT 3.e) Program/Bergen/MS	Effektmål: At alle kommuner har forbedret sin evne til å forberede, vurdere, kontrollere, håndtere hendelser, og gjenopprette normaltilstand. Alle kommuner er tilknyttet et respons- eller sikkerhetsmiljø At kommuner har egenevne til å oppdage og håndtere hendelser. At kommuner har opprettet beredskaps- og kontinuitetsplaner. At kommuner kan respondere rasker ved		Håndtere og gjenopprette/ post 22

	Det er viktig at kommuner har nødvendig egenevne til å forebygge, oppdage og respondere på hendelser. Regionale Security Operation Center (SOC) vil derfor være sentrale i så hensende da den enkelt kommune ikke har tilstrekkelig kapasitet og kompetanse til å bygge dette alene. Programmet legger opp til at man piloterer en regional SOC, i første omgang direkte rettet mot M365, for å få kunnskap om både hvordan regionale SOC best kan breddes ut samt hvordan dette kan bidra til å gjøre kommunene mer robust.			eventuelle sikkerhets-brudd.		
4. Øke sikkerhets- og risikokompetanse						
Kompetansetiltak ansatte a) Bevisstgjøringskampanje Kompetanseprogram kommunedirektørene og politisk ledelse: b) Nasjonal og global risiko- og trusselforståelse i digital rom for administrativ og politisk ledelse. c) Beredskapsøvelse (for samtlige kommunedirektører, toppledelse og politisk ledelse).	Arbeidspakken skal gi økt forståelse for viktigheten av god risikostyring og digital sikkerhet, samt gi ledelsen gode verktøy for risiko- og sikkerhetsstyring i kommunen. Kompetansetiltak for ansatte skal bidra til å gjøre kommunene mer robust for angrep, f.eks. phishingangrep, og bidra til at alle ansatte i		4.a) Program 4.b) Program 4.c) Program/HelseCert//KommuneCSIRT (DSB) 4.d) Program/(DigDir) 4.e) Program/HelseCert /KommuneCSIRT	Effektmål: Økt forståelse for viktigheten av god risikostyring og digital sikkerhet. Økt robusthet mot digitale angrep.		Identifisere og kartlegge/post 22.

d) Praktisk ledelsesstyring av digital sikkerhet, herunder sjekkliste for status på sikkerhetsområdet og e) Lokal «dashboard» vedrørende sårbarhet og modenhetsnivå for sikkerhet i kommunen for kommunedirektører	kommunen er en del av det forebyggende arbeidet mot angrep. Kompetanseprogram for kommunedirektørene og politisk ledelse har til hensikt å gi god innsikt i utfordringene i det digitale rom, samt gi ledelsen et verktøy for å kunne prioritere og bidra med god risiko- og sikkerhetsstyring av kommunen.			Gi ledelsen et verktøy for å kunne prioritere og bidra med god risiko- og sikkerhets-styring av kommunen.		