skema 1

Budget 2025 – Nye tiltag/aktivitetsændringer
med kompenserende finansiering

NATURENS RIGE

Cybersikkerhed og NIS2 Direktivet

Forslag nr. _____

Udvalg: Økonomiudvalget

Funktion: 06.45.52

Forslaget er fra udvalget prioriteret som (sæt x)

1 ___x___ udvalget er enigt
2 _____ udvalget er uenigt
3 _____ forslaget kan ikke anbefales af udvalget
4 _____ forslaget har ikke været udvalgsbehandlet

1. Projektbeskrivelse: (herunder hvordan forslaget harmoniserer med de vedtagne politikker)

Da Ringkøbing-Skjern Kommune ønsker at handle med rettidig omhu, gennemførte staben Personale og Digitalisering i august 2023 en GAB-analyse af kommunen IT-sikkerhedsniveau. Analysen er blevet til i samarbejde med sikkerhedsfirmaet Dediko, og på baggrund af den internationale standard, CIS (*Center for Internet Security, version 8*).

Formålet med analysen har været 1) at synliggøre det aktuelle sikkerhedsniveau, 2) at klarlægge hvilket sikkerhedsniveau, der er hensigtsmæssigt med afsæt i kommunens behov for sikkerhed, samt 3) at afdække hvilke tiltag, der er nødvendige for at nå det ønskede sikkerhedsniveau.

Konklusionen er, at Ringkøbing-Skjern Kommune på nuværende tidspunkt har et for lavt sikkerhedsniveau i forhold til det fremadrettede trusselsbillede. Hvis kommunen skal op på det nødvendige sikkerhedsniveau, skal der gennemføres en række større tiltag.

Det aktuelle trusselsbillede
Center for Cybersikkerhed (CFCS) vurderer årligt cybertruslen mod Danmark. I rapporten for 2023 fremhæves det særligt, at krigen i Ukraine har betydning for det aktuelle trusselsbillede. Ringkøbing-Skjern Kommune oplever selv, at der er større aktivitet fra hackere med russiske IP-adresser, og seneste eksempel på et russisk hackerangreb mod en offentlig sektor er fra januar 2024, hvor et offentligt lønsystem i Sverige blev hacket.

Ifølge CFCS, er truslen fra cyberaktivisme *høj,* mens truslen fra cyberkriminalitet er *meget høj.* Cyberkriminalitet ses primært i form af ransomware-angreb, hvor organiserede kriminelle grupper får adgang til data, krypterer dem og kræver løsesum for at dekryptere dem. For Ringkøbing-Skjern Kommune vil ransomware-angreb kunne betyde, at organisationen ikke har adgang til kritiske IT-systemer, og derfor ikke kan løse en lang række opgaver. Ofte vil data efterfølgende blive lækket. Et eksempel på dette er *Härjedalen Kommune* i Sverige, som den 23. december 2023 blev ramt af ransomware. Angrebet har særligt været alvorligt for ældreområdet, og det forventes, at tage flere måneder førend kommunens drift er tilbage på et normalt niveau. Andre eksempler på ransomware-angreb er Vestas, som blev ramt af et angreb i november 2019, Energisektoren, som blev ramt af et angreb i maj 2023, og EUD Syd og IT-Center Syd som på baggrund af et hackerangreb havde et større datalæk i august 2023.

Ringkøbing-Skjern Kommunes situation er på linje med andre sammenlignelige kommuner, som forventelig også står overfor investeringer i forhold til cybersikkerhed. I en baseline-undersøgelse af

KL fremgår det, at kommunens IT-sikkerhedsniveau, der er tilsvarende gennemsnittet af øvrige kommuner.

NIS2-direktivet
Vigtigheden af at der tages hånd om cybersikkerheden underbygges af Net- og Informationssikkerhedsdirektivet (NIS2-direktivet), som træder i kraft 17. oktober 2024.

EU opdaterede i 2023 NIS2-direktivet på baggrund af den stigende trussel mod europæiske informationssystemer og -netværk. Direktivet medfører skærpede krav til håndtering af cyber- og informationssikkerhed, herunder også en skærpelse af ansvarsbestemmelserne i forhold til, at øverste ledelse har et personligt ansvar for cybersikkerhed.

NIS2 har til formål at sikre infrastrukturen og samfundskritiske tjenester mod nedbrud, ved at stille krav om et ensartet niveau af cyber- og informationssikkerhed på tværs af EU. Heriblandt et formaliseret cybersikkerhedsprogram og en Incidens Response aftale (øjeblikkelig hjælp i forbindelse med cyberangreb).

Som en del af det nødvendige sikkerhedsniveau i Ringkøbing-Skjern Kommune implementeres der, hvis indsatsen besluttes med budget 2025, et formaliseret cybersikkerhedsprogram, som forankres hos øverste kommunale ledelse, jævnfør NIS2.

2. Beskrivelse af den faglige og økonomiske effekt/konsekvens, der forventes opnået af budgetforøgelsen (uddybende og dokumenteret beskrivelse)**:**
For at kunne opnå det cybersikkerhedsniveau, som er nødvendigt i forhold til NIS2, trusselsbilledet samt sensitiviteten af de data kommunen håndterer og opbevarer, er der behov for tilførsel af budgetmidler på 6,5 millioner kr. årligt.

Omkostningerne til det øgede sikkerhedsniveau fordeler sig på systemlicenser og -aftaler samt øget behov for personaleressourcer svarende til tre stillinger, hvoraf IT-afdelingen finansierer den ene af eget budget.

I oktober og november 2023 gennemførte IT Optima en IT-benchmarkanalyse af kommunen, som blandt andet sammenligner kommunens udgift til IT-omkostninger med øvrige kommuner. Af analysen fremgår det, at kommunens omkostninger til IT gennemsnitligt ligger 6,7 procentpoint lavere end sammenlignelige kommuner.

Personale og Digitalisering vurderer, at en række sikkerhedstiltag har været kritiske at få på plads, hvorfor der inden for IT-budgettet er fundet ressourcer til cybersikkerhedsprogrammet i 2024. Det er blandt andet sket ved at udskyde udskiftning af servere samt centrale routere, hvor det har været muligt at forlænge servicen. Dertil har det undtagelsesvist været muligt at udskyde nogle af de investeringer, der sædvanligvis kører i en tre-årig kadence, så kommunens grundlæggende IT-infrastruktur kan leve op til fællesoffentlige standarder samt krav fra leverandører af fagsystemer.

Fælles for tiltagene er, at det er nødvendige investeringer, hvorfor der kun er fundet ressourcer til indsatsen for 2024. Sagen blev behandlet på Økonomiudvalgets møde den 27. februar 2024, hvor det blev besluttet at udgifterne fra 2025 og fremad skal indgå i Økonomiudvalgets budgetdrøftelser.

3. Opfølgningsplan på tiltaget:

Med cybersikkerhedstiltagene vil IT-afdelingen kvartalsvis afrapportere det aktuelle sikkerhedsniveau, samt planlagte tiltag for at løfte/vedligeholde sikkerhedsniveauet, så øverste

kommunale ledelse er orienteret om den aktuelle status, og løbende kan vurdere, om sikkerheden er på et tilstrækkeligt niveau.

Cybersikkerhedsprogrammet vil sikre struktur og styring af, hvilket sikkerhedsniveau kommunen har, både i forhold til køb og integrering af nødvendige systemer, samt hvordan systemerne fungerer ind i den eksisterende IT-arkitektur.

Da cybertruslen løbende ændres og udvikles, har IT-afdelingen et kontinuerligt fokus på kommunens sikkerhedsniveau og behov for eventuelle ændringer. Det betyder, at der efter implementering af cybersikkerhedsprogrammet fortsat vil være behov for de personaleressourcer, som analyserer og vurderer kommunens aktuelle sikkerhedsbehov, ligesom udgiften til systemlicenser og -aftaler vil fortsætte efter implementering af cybersikkerhedsprogrammet for at fastholde sikkerhedsniveauet.

IT-afdelingen er meget opmærksom på, at medarbejderne i organisationen mærker mindst muligt til de sikkerhedstiltag, der er nødvendige. På nuværende tidspunkt er medarbejderne mødt med et behov for længere passwords samt øget awareness.

4. Kompenserende finansieringsforslag: (herunder konsekvenser af forslaget)

Det er ikke muligt at finde alternative finansieringsforslag inden for stabsområdet.

Med budget 2024 blev der afsat en foreløbig ramme på 6 mio. kr. i fremadrettet budget til skift fra den nuværende platform til "Microsoft 365". Om end dette beløb endnu ikke er disponeret, kan det ikke anbefales som kompenserende besparelse. Fra oktober næste år stopper Microsoft med at sikkerhedsopdatere kommunens nuværende mail-løsning. Opdateringen af den office-løsning, som kommunen pt. bruger, ophører også, her vil det dog være muligt at finde en løsning, der sikrer brugen i nogle år endnu.

Det betyder, at Ringkøbing-Skjern Kommune fra oktober næste år skal finde en ny mail-løsning, og at der inden for et par år skulle findes en ny løsning fremfor kommunens nuværende office-løsning.

Kommunen kan derfor forvente en større omkostning ved skifte af nuværende mail samt office-produkter.

5. Viden & Strategis bemærkninger til forslaget:

Ingen bemærkninger.

FORSLAGETS ØKONOMISKE KONSEKVENSER

(Beløb i 1.000 kr. ekskl. moms, + = budgetudvidelse og - = budgetreduktion)

Tekst	2025	2026	2027	2028	Efterfølgende år
Cybersikkerhedsprogram	6.500	6.500	6.500	6.500	6.500