

Orientering om cybersikkerhed i Norddjurs Kommune

25/850 Åben Sag

Sagsgang

ØK

Sagsfremstilling

I denne sag orienterer IT og Digitalisering om status på cybersikkerhed i Norddjurs Kommune. Orienteringen tager afsæt i det øgede trusselsbillede og anbefalinger fra centrale aktører, som kommunerne støtter sig til i indsatsen med at beskytte kommunernes IT-infrastruktur og data.

Norddjurs Kommune øger løbende indsatsen mod cybertrusler som følge af CFCS (Center For CyberSikkerhed) og andre centrale myndigheders vurdering af, at risikoen for cyberangreb er stigende. Krigen mellem Rusland og Ukraine accelererer denne udvikling. I Norddjurs Kommune genkendes det øgede trusselsbillede blandt andet ved, at der registreres et stigende antal forsøg på gennembrud af kommunens firewall; herunder særligt fra lande, der har interesse i krigen.

KL har i en årrække undersøgt kommunernes arbejde med cyber- og informationssikkerhed. I den seneste undersøgelse fra december 2024 opfordrer KL generelt kommunerne til at give området øget opmærksomhed. Den årlige undersøgelse kendes som KL Baseline, og Norddjurs har som tidligere år deltaget i undersøgelsen. Det er en undersøgelse med mange elementer, men gennemsnitligt og samlet set ligger Norddjurs Kommune på et niveau lige under middel i forhold til de 83 andre kommuner, der har deltaget i undersøgelsen.

KL arbejder aktuelt på – bl.a. med ”KL’s udspil til ét samlet cyberforsvar” – at tilvejebringe økonomi til kommunerne via Forsvarsforliget og/eller ØA25. KL skriver bl.a., at.:

- Kommunerne skal indgå som en del af det danske cyberforsvar. Det offentlige er bundet sammen digitalt, og det svageste led kan hurtigt blive bagdøren ind.
- Folketinget skal sikre de nødvendige økonomiske og politiske prioriteringer, så landets samlede cyberforsvar bliver styrket.
- Kommunerne skal efterleve minimumskrav for cybertrusler, der er med til at sikre høj sikkerhed i et digitalt tæt koblet Danmark.

Der er allerede fastsat tekniske minimumskrav til cyberforsvar for statslige myndigheder. Disse krav gælder ikke for kommunerne, men opfattes generelt som anbefalinger. I lighed med langt de fleste kommuner, så lever Norddjurs Kommunes cyberforsvar ikke op til alle de gængse standarder.

Lovforslag om dansk implementering af NIS2-direktivet (Net- og Informationssikkerheds-direktivet fra EU) forventes at træde i kraft i juli 2025. Det vil betyde, at kommunerne bliver underlagt skærpede krav til cyber- og informationssikkerhed i forhold til kritisk infrastruktur.

Som følge af ”Sundhedssektorens strategi for cyber- og informationssikkerhed 2023-2025” skal kommunerne tilsluttes det centrale analysecenter for cyber- og informationssikkerhed i sundhedssektoren (DCIS Sund). Tilslutningen indebærer, at kommunerne skal anskaffe, implementere og drive overvågningsenheder, der overvåger netværkstrafikken både på indvendig og udvendig side af kommunernes firewalls. DCIS Sund har alene lovhjemmel til at overvåge cyberhændelser, der er relateret til sundhedsområdet i kommunerne. Derfor arbejder KL for at etablere et fælleskommunalt overvågningscenter (KommuneCERT) for cyberhændelser, der varetager opgaven for kommunerne og ikke kun sundhedsområdet.

På baggrund ovenstående undersøger IT og Digitalisering muligheder for at øge indsatsen mod cybersikkerhed med bl.a. følgende indsatser:

- Tiltrædelse til det fælleskommunale overvågningscenter/fælleskommunalt cyberværn. (KommuneCERT) der er under etablering i KOMBIT.
- Etablering af ekstern SOC (Security Operations Center). En SOC er en ekstern funktion, der sammen med kommunens IT-afdeling er ansvarlig for at overvåge, forebygge, registrere og reagere på trusler 24/7/365.
- En øget indsats internt i Norddjurs Kommune således kommunen fremadrettet kan leve op til tekniske minimumskrav samt kravene i NIS2-direktivet.
- Opsætning og drift af netværksovervågningsenheder (NDR - Network Detection and Response). Indsatsen øger evnen til at opdage cyberhændelser, som er en forudsætning for styrket sikkerhed. Enhederne overvåger netværkstrafikken i og til/fra Norddjurs Kommune og registrerer anormaliteter.

Sammenhæng til andre politikker/strategier og fagområder

Der er sammenhæng til Informationssikkerhedspolitik for Norddjurs Kommune, som er godkendt af Kommunalbestyrelsen 25. august 2020. Derudover er der sammenhæng til Politik for fortsat drift for Randers, Favrskov, Norddjurs og Syddjurs Kommuner (Beredskabsplanen).

Økonomiske konsekvenser

Ingen økonomiske konsekvenser i forbindelse med denne orientering, men en forventning om, at nogle af de nye indsatser i orienteringen kommer til at indgå i budgetprocessen for 2026-2029.

Lovgrundlag

Intet relevant lovgrundlag.

Indstilling

Chef for Borgerservice, IT og Digitalisering indstiller, at orientering om cybersikkerhed i Norddjurs Kommune godkendes.

Beslutning i Økonomiudvalget den 11-03-2025

Godkendt.

Bilag: