Ministeriet for Samfundssikkerhed og Beredskab

Dato: 14-05-2025
Sagsnr.: 2025 - 870
Akt-id.: 4612

SAMLENOTAT FOR RÅDSMØDET (TRANSPORT, TELEKOMMUNIKTATION OG ENERGI) DEN 6. JUNI 2025

Indholdsfortegnelse

3. Forslag til Rådets henstilling om et EU-blueprint for cyberkrisestyring (Cyber Blueprint)
   - *Politisk drøftelse og vedtagelse*
     KOM (2025) 66

Punkt 3: Forslag til Rådets henstilling om et EU-blueprint for cyberkrisestyring (Cyber Blueprint)

- *Politisk drøftelse og vedtagelse*
  KOM (2025) 66

Nyt notat.

1. Resumé

På rådsmødet for telekommunikation den 6. juni 2025 forventes vedtagelse af forslaget til Rådets henstilling om et EU-blueprint for cyberkrisestyring (Cyber Blueprint). Europa-Kommissionen fremlagde forslag til et revideret Cyber Blueprint den 24. februar 2025, som medlemslandene er nået til enighed om på teknisk niveau.

Formålet ved Cyber Blueprintet er at opnå en mere effektiv og koordineret respons på tværs af medlemslandene, under en cyberkrise eller større cyberhændelse i EU.

Cyber Blueprint udgør en ikke-bindende rådsanbefaling, hvor de relevante EU-aktører og netværks roller og ansvar er beskrevet gennem hele krisehåndteringscyklussen – fra beredskab, detektion, og respons til kommunikation, samarbejde og genoprettelse.

Cyber Blueprint har ikke i sig selv lovgivningsmæssige, økonomiske eller øvrige konsekvenser, da det er et vejledende dokument og ikke pålægger medlemslandene krav.

Regeringen støtter vedtagelsen af Cyber Blueprint.

2. Baggrund

Cyber Blueprint er en del af EU's styrkede indsats for at sikre en mere robust og koordineret håndtering af omfattende cyberhændelser og -kriser, der kan true kritiske infrastrukturer, samfundsfunktioner og den digitale økonomi. I takt med at cyberangreb bliver mere komplekse, grænseoverskridende og potentielt ødelæggende, er der opstået et behov for en klar og fælles europæisk ramme, der definerer roller, ansvar og samarbejdsformer på tværs af medlemsstater og EU-institutioner.

Blueprintet bygger videre på Kommissionens tidligere anbefaling fra 2017 om koordineret respons på omfattende cyberkriser og inddrager erfaringerne fra fælleseuropæiske øvelser og indsatser siden da.

Rådet anmodede om et revideret Cyber Blueprint i Rådskonklusionerne om en mere cyber-sikker og resilient union af den 21. maj 2024. Initiativet kommer ligeledes i forlængelse af en række nyere politiske og lovgivningsmæssige tiltag, herunder den fælles EU-beredskabsstrategi, NIS 2-direktivet, Netværkskodeksen for cybersikkerhed i elsektoren og det såkaldte Critical Infrastructure Blueprint. Sam-

men skal disse tiltag bidrage til at styrke modstandsdygtigheden i hele EU og beskytte det indre marked mod digitale trusler, herunder hybride angreb og informationspåvirkning.

Cyber Blueprint er en ikke-bindende rådsanbefaling og vejledende dokument er ikke pålægger medlemslandene krav.

3. Formål og Indhold

Formålet ved Cyber Blueprint er at forbedre koordinationen mellem EU-institutioner, medlemsstater og operative enheder, styrke kapaciteten til at opdage, håndtere og afbøde cyberangreb samt understøtte eksisterende mekanismer, herunder Integrated Political Crisis Response (IPCR), Cybersecurity Emergency Mechanism, EU's Cyber Diplomacy Toolbox, og det nye Critical Infrastructure Blueprint.

Derudover har Cyber Blueprint også til formål at fremme samarbejdet mellem civile og militære aktører, også med NATO, og øge modstandsdygtigheden mod hybride trusler.

Cyber Blueprint beskriver samarbejdsprocesserne på EU-plan, herunder hvilke aktører og netværk, der samarbejder med hvem og via hvilke kommunikationskanaler. Blueprintet beskriver dette samarbejde både på teknisk, operativt og politisk niveau, hvor særligt CSIRT-netværket og CyCLONe, der blev etableret i NIS 2-direktivet, spiller centrale roller. Blueprintet fokuserer særlig på beredskab, øvelser og forebyggende aktiviteter samt respons og genopretning.

Under forhandlinger har forslaget bevæget sig i en bestemt retning så teksten nu i højere grad uddyber processer og ansvarsområder ift. det oprindelige forslag fra Kommissionen. Dertil uddyber den endelig version også samarbejdsprocesser ved omfattende cyberhændelser og ikke kun cyberkriser, der kræver aktivering af IPCR, som ved det oprindelige forslag. Denne ændring forbedrer det samlede cybersikkerhedsniveau i EU, da man får flerlagskoordination inden en cyberhændelse nødvendigvis er på højeste krise niveau. De fleste cyberangreb når ikke det tilstrækkelige kriseniveau for aktivering af IPCR.

4. Europa-Parlamentets udtalelser

Europa-Parlamentet skal ikke høres.

5. Nærhedsprincippet

Spørgsmålet om nærhedsprincippet er ikke relevant.

6. Gældende dansk ret

Ikke relevant.

7. Konsekvenser

Cyber Blueprint har ikke i sig selv lovgivningsmæssige, statsfinansielle, samfundsøkonomiske eller erhvervsøkonomiske konsekvenser eller konsekvenser for beskyttelsesniveauet. I det omfang Cyber Blueprint senere hen måtte udmønte sig i konkrete tiltag, vil disse være genstand for særskilte konsekvensvurderinger.

8. Høring

Forslaget har ikke været i høring.

9. Generelle forventninger til andre landes holdninger

Der forventes generelt opbakning til vedtagelsen af af Cyber Blueprint efter enighed på teknisk niveau.

10. Regeringens generelle holdning

Regeringen støtter vedtagelsen af Cyber Blueprint.

11. Tidligere forelæggelse for Folketingets Europaudvalg

Sagen har ikke tidligere været forelagt Folketingets Europaudvalg.