Ministeriet for
Samfundssikkerhed og Beredskab

Dato: 5. februar 2025
Kontor: Cyber- og informationssikkerhed
Sagsbeh: RPB

Besvarelse af spørgsmål nr. 73 (Alm. del) fra Forsvars-, Samfundssikkerheds- og Beredskabsudvalget

Hermed sendes besvarelse af spørgsmål nr. 73 (Alm. del), som Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg har stillet til ministeren for samfundssikkerhed og beredskab den 9. december 2024. Spørgsmålet er stillet efter ønske fra Alexander Ryle (LA).

Torsten Schack Pedersen

Spørgsmål nr. 73 (Alm. del) fra Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg:

> ”Kan ministeren redegøre for, hvorfor muligheden i EU-direktivet for at omfatte kommuner som lokale eller regionale myndigheder ikke er blevet udnyttet i lovforslaget for NIS2, fremlagt den 5. juli 2024?”

Svar:

1. NIS 2-direktivet har til formål at sikre et højt og mere ensartet cybersikkerhedsniveau på tværs af EU. Det sker ud fra en risikobaseret tilgang, hvor de omfattede virksomheder og myndigheder skal sikre, at de gennemfører cybersikkerhedsforanstaltninger, der bl.a. skal omfatte politikker for risikoanalyse, håndtering af hændelser og forsyningskædesikkerhed.

2. Det fremgår af den version af udkastet til NIS 2-lovforslaget, som blev sendt i offentlig høring i sommeren 2024, at en offentlig forvaltningsenhed på lokalt plan eller en uddannelsesinstitution efter omstændighederne kunne blive omfattet af lovens anvendelsesområde, selvom bemyndigelsen i den foreslåede § 1, stk. 7, ikke var udnyttet. Dette ville eksempelvis kunne være tilfældet i en situation, hvor en kommune agerer som sundhedstjenesteyder i overensstemmelse med NIS 2-direktivets bilag. I denne situation ville kommunen kunne være omfattet af lovens anvendelsesområde på baggrund af disse aktiviteter, også selvom bemyndigelsen i den foreslåede § 1, stk. 7, ikke var udnyttet. Denne bestemmelse ville således alene være relevant, hvis man måtte ønske at omfatte offentlige forvaltningsenheder på lokalt plan eller uddannelsesinstitutioner som følge af andre aktiviteter eller tjenester end dem, der er oplistet i direktivets bilag.

3. Det følger af EU-Kommissionens meddelelse C/2023/6068 af 13. september 2023 om retningslinjer for anvendelsen af artikel 4, stk. 1 og 2, i NIS 2-direktivet, at direktivets forpligtelse i artikel 21, stk. 1 om, at væsentlige og vigtige enheder træffer passende og forholdsmæssige foranstaltninger til styring af cybersikkerhedsrisici, vedrører alle den pågældende enheds operationer og tjenester, og ikke kun specifikke it-aktiver eller kritiske tjenester, som enheden leverer.

Det er på denne baggrund Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at formuleringen »i net- og informationssystemer, som disse enheder anvender til deres operationer eller til at levere deres tjenester« i NIS 2-direktivets artikel 21, stk. 1, skal forstås som alle de net- og informationssystemer, som disse enheder anvender til deres operationer, eller til at levere

deres tjenester, og ikke kun specifikke informationsteknologiske (it) aktiver eller kritiske tjenester, som enheden leverer. I tilfælde hvor en enhed anvender flere forskellige typer af net- og informationssystemer, og hvor kun nogle af disse systemer er omfattet af direktivets bilag, vil samtlige af de net- og informationssystemer, som enheden anvender til sine operationer, eller til at levere sine tjenester, således blive underlagt direktivets krav.

Som følge heraf kommer det til at fremgå af udkastet til NIS 2-lovforslag, som forventes fremsat den 6. februar 2025, at kommunerne – på lige fod med andre enheder, der er omfattet af lovens anvendelsesområde – ikke alene vil skulle træffe passende og forholdsmæssige foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer vedrørende de aktiviteter, der er oplistet i direktivets bilag, men for samtlige af de net- og informationssystemer, som de anvender til deres operationer, eller til at levere deres tjenester.

4. Ministeriet for Samfundssikkerhed og Beredskab er i løbende dialog med KL og relevante myndigheder om betydningen heraf, herunder de nærmere rammer for kommunernes overholdelse af NIS 2-direktivets krav.

Ministeriet for
Samfundssikkerhed og Beredskab

Dato: 5. februar 2025
Kontor: Cyber- og informationssikkerhed
Sagsbeh: RPB

Besvarelse af spørgsmål nr. 74 (Alm. del) fra Forsvars-, Samfundssikkerheds- og Beredskabsudvalget

Hermed sendes besvarelse af spørgsmål nr. 74 (Alm. del), som Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg har stillet til ministeren for samfundssikkerhed og beredskab den 9. december 2024. Spørgsmålet er stillet efter ønske fra Alexander Ryle (LA).

Torsten Schack Pedersen

Spørgsmål nr. 74 (Alm. del) fra Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg:

> ”Såfremt det fastholdes i den endelige lov for NIS2, at kommunerne ikke omfattes som myndigheder, men alene ved udvalgte opgaver, kan ministeren da redegøre for, hvordan det i praksis sikres, at kommunerne ikke pålægges gensidigt modstridende krav fra statens forskellige sektorer/ministerier?”

Svar:

Der henvises til den samtidig besvarelse af spørgsmål nr. 73 (Alm. del) fra Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg.

Ministeriet for Samfundssikkerhed og Beredskab

Dato: 6. februar 2025

Besvarelse af spørgsmål nr. 89 (Alm. del) fra Forsvars-, Samfundssikkerheds- og Beredskabsudvalget

Hermed sendes besvarelse af spørgsmål nr. 89 (Alm. del), som Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg har stillet til ministeren for samfundssikkerhed og beredskab den 9. januar 2025.

Torsten Schack Pedersen

Spørgsmål nr. 89 (Alm. del) fra Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg:

> ”Hvordan vil ministeren konkret sikre, at virksomheder får tilstrækkelig tid til at efterleve kravene i NIS 2? Overvejer ministeren at indføre en periode efter ikrafttrædelsen af NIS2-lovgivningen, hvor der – i lyset af den meget forsinkede lovproces og den manglende vejledning – ikke føres tilsyn eller gives bøder for manglende efterlevelse?”

Svar:

Jeg kan indledningsvis henvise til min besvarelse af 29. november 2024 af spørgsmål nr. 22 (Alm. del) fra Folketingets Udvalg for Digitalisering og It, hvoraf det bl.a. fremgår, at der helt forståeligt er fokus på, hvordan de nye regler vil blive håndhævet af de kompetente tilsynsmyndigheder – særligt i den første tid efter, at reglerne træder i kraft.

Som det endvidere fremgår af besvarelsen, vil det i mine øjne vil være naturligt, at tilsynsmyndighederne ikke hiver bødeblokken frem som det første. I den forbindelse er det værd at bemærke, at overtrædelse af reglerne efter omstændighederne kan håndteres ved brug af andre reaktionsmuligheder, herunder påbud og forbud. Den tilgang vil Ministeriet for Samfundssikkerhed og Beredskab også tage med ind i det videre arbejde, hvor ministeriet som led i den koordinerende rolle i forhold til NIS 2-implementeringen bl.a. skal sikre et tæt samarbejde mellem tilsynsmyndighederne.

Jeg kan i forlængelse heraf oplyse, at der vil blive udarbejdet vejledningsmateriale vedrørende bl.a. lovens anvendelsesområde og krav til foranstaltninger, som vil foreligge senest ved lovens ikrafttræden forventeligt den 1. juli 2025. Hertil kommer, at de kompetente myndigheder i relevant omfang vil yde vejledning til enheder, der er omfattet af lovens anvendelsesområde.

Ministeriet for
Samfundssikkerhed og Beredskab

Dato: 29. november 2024
Kontor: Sikkerhedskontoret
Sagsbeh: Emilie Frederikke Bock

Besvarelse af spørgsmål nr. 22 (Alm. del) fra Udvalget for Digitalisering og It

Hermed sendes besvarelse af spørgsmål nr. 22 (Alm. del), som Folketingets Udvalg for Digitalisering og It har stillet til ministeren for samfundssikkerhed og beredskab den 1. november 2024.

Torsten Schack Pedersen

Spørgsmål nr. 22 (Alm. del) fra Folketingets Udvalg for Digitalisering og It:

> "Vil ministeren redegøre for sine overvejelser på cybersikkerhedsområdet, herunder planerne for den danske implementering af NIS2?"

Svar:

1. Vi står over for et mere sammensat og komplekst trusselsbillede end for blot få år siden. Det gælder ikke mindst på cybersikkerhedsområdet, hvilket understreges af den seneste trusselsvurdering fra Center for Cybersikkerheds. Det fremgår bl.a. heraf, at niveauet for cyberspionage og cyberkriminalitet er MEGET HØJT, truslen fra cyberaktivisme er HØJ. Truslen fra destruktive cyberangreb er tidligere på året blevet hævet fra LAV til MIDDEL. Niveauet blev hævet på baggrund af en udvikling i Ruslands risikovillighed i forhold til at anvende hybride virkemidler, herunder destruktive cyberangreb, mod europæiske NATO-lande

Det skærpede trusselsbillede er for mig en klar påmindelse om, at vi skal tage cybertruslen alvorligt. Cybersikkerhed er derfor også et vigtigt fokusområde for mig som minister for samfundssikkerhed og beredskab.

2. En vigtig opgave på cybersikkerhedsområdet i den kommende tid er implementeringen af NIS 2-direktivet, som skaber et højere og mere ensartet cybersikkerhedsniveau på tværs af EU. Det sker ud fra en risikobaseret tilgang, hvor de omfattede virksomheder og myndigheder skal sikre, at de gennemfører cybersikkerhedsforanstaltninger, herunder bl.a. politikker for risikoanalyse, håndtering af hændelser og forsyningskædesikkerhed. NIS 2-direktivet medfører desuden styrkede tilsyns- og håndhævelsesbeføjelser for de kompetente myndigheder.

Implementeringen af NIS 2-direktivet er dermed en grundsten i arbejdet med at sikre et højnet cybersikkerhedsniveau i hele Danmark. Vigtigheden af et generelt højt cybersikkerhedsniveau skal særligt ses i lyset af, at cyberkriminelle og ondsindede hackere ofte går efter det svageste led i kæden.

3. Samtidig har NIS 2-direktivet stor betydning for erhvervslivet og myndigheder.

Som minister for samfundssikkerhed og beredskab ligger det mig på sinde, at der sikres en så god proces som muligt for det videre arbejde med implementeringen frem mod reglernes ikrafttræden til sommer.

Det indebærer bl.a. en bred inddragelse af myndigheder, virksomheder og brancheorganisationer med henblik på at lytte til de input, der måtte være til den videre implementering. Det gælder også i forhold til udarbejdelsen af relevante vejledninger parallelt med færdiggørelse og behandling af lovforslaget.

4. Der er også helt forståeligt fokus på, hvordan de nye regler vil blive håndhævet af de kompetente tilsynsmyndigheder – særligt i den første tid efter, at reglerne træder i kraft.

Jeg vil i den forbindelse gerne understrege, at det i mine øjne vil være naturligt, at tilsynsmyndighederne ikke hiver bødeblokken frem som det første. I den forbindelse er det værd at bemærke, at overtrædelse af reglerne efter omstændighederne kan håndteres ved brug af andre reaktionsmuligheder, herunder påbud og forbud. Den tilgang vil Ministeriet for Samfundssikkerhed og Beredskab også tage med ind i det videre arbejde, hvor ministeriet som led i den koordinerende rolle i forhold til NIS 2-implementeringen bl.a. skal sikre et tæt samarbejde mellem tilsynsmyndighederne.

5. NIS 2-lovforslaget, som implementerer NIS 2-direktivet, forventes fremsat for Folketinget i februar 2025 og forventes at træde i kraft den 1. juli 2025.

Som det fremgår af mit brev af 30. september 2024 til Folketingets Udvalg for Digitalisering og It (DIU Alm. del (2024-25), bilag 28), følger det af NIS 2-direktivet, at fristen for implementering var den 17. oktober 2024, og at Ministeriet for Samfundssikkerhed og Beredskab derfor ville sørge for, at EU-Kommissionen underrettes om den forsinkede implementering. EU-Kommissionen blev orienteret om forsinkelsen den 15. oktober 2024.

Ministeriet for
Samfundssikkerhed
og Beredskab

Dato: 24. februar 2025
Sagsnr.: 2025 - 36
Akt-id.: 104

Besvarelse af spørgsmål nr. 120 (Alm. del) fra Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg

Hermed sendes besvarelse af spørgsmål nr. 120 (Alm. del), som Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg har stillet til ministeren for samfundssikkerhed og beredskab den 27. januar 2025. Spørgsmålet er stillet efter ønske fra Mike Villa Fonseca (UFG).

Torsten Schack Pedersen

Spørgsmål nr. 120 (Alm. del) fra Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg:

> ”Hvordan vil ministeren fremme samarbejdet mellem myndigheder, erhvervslivet og private aktører for at sikre et mere robust forsvar mod trusler som cybersikkerhed og angreb på kritisk infrastruktur? Kan ministeren f.eks. etablere en permanent offentligt-privat samarbejdsform, der inkluderer regelmæssige beredskabsøvelser og deling af kritisk information mellem disse aktører?”

Svar:

Som det også fremgår af *Aftale om beredskabsområdet 2025-2026* fra den 15. januar 2025, udgør erhvervslivet og civilsamfundet i Danmark en væsentlig ressource og medspiller i forhold til at styrke samfundssikkerheden og det samlede beredskab. Aftaleparterne noterer sig, at ministeren for samfundssikkerhed og beredskab vil nedsætte et forum for erhvervslivet og et forum for civilsamfundet, hvor relevante aktører kan drøfte, hvordan private virksomheder og civilsamfundet bedst muligt kan inddrages og bidrage til samfundssikkerhed og beredskab med deres særlige kompetencer og kapaciteter. Med aftalen afsættes der også midler til at gennemføre flere øvelser på tværs af sektorer, hvor private aktører vil blive inviteret til at deltage, hvor det vurderes relevant.

Ministeriet for
Samfundssikkerhed
og Beredskab

Dato: 24. februar 2025
Sagsnr.: 2025 - 36
Akt-id.: 104

Besvarelse af spørgsmål nr. 123 (Alm. del) fra Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg

Hermed sendes besvarelse af spørgsmål nr. 123 (Alm. del), som Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg har stillet til ministeren for samfundssikkerhed og beredskab den 27. januar 2025. Spørgsmålet er stillet efter ønske fra Mike Villa Fonseca (UFG).

Torsten Schack Pedersen

Spørgsmål nr. 123 (Alm. del) fra Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg:

> ”Hvad gør regeringen for at uddanne og træne både offentligt ansatte og borgere i at håndtere cyber- og hybridtrusler, og kunne simulationer og øvelser på tværs af sektorer være en del af løsningen?”

Svar:

Ministeriet for Samfundssikkerhed og Beredskab har til brug for besvarelsen af spørgsmålet indhentet en udtalelse fra Styrelsen for Samfundssikkerhed, der har oplyst følgende:

> ”Med kongelige resolution af 29. august 2024 fik Ministeriet for Samfundssikkerhed og Beredskab (MSSB) bl.a. ansvaret for rådgivning og kommunikation til myndigheder, virksomheder og borgere om forebyggelse og håndtering af de trusler, samfundet står overfor. Det udførende ansvar for denne opgave ligger i Styrelsen for Samfundssikkerhed (SAMSIK).
>
> Det bemærkes, at henset til, at MSSB først er etableret den 29. august 2024, er en lang række af nedenstående udviklings- og implementeringsindsatser sket i regi af andre myndigheder.
>
> **Initiativer målrettet borgere**
> Både på PETs hjemmeside og på informationsportalen Sikkerdigital.dk findes viden, vejledning, podcasts og konkrete værktøjer, der ruster borgere til at håndtere en hverdag med et stadigt mere komplekst trusselsbillede. Endvidere arbejdes der som en del af Sikkerdigital-universet løbende med forebyggende kampagneindsatser om digital svindel.
>
> Som følge af det skærpede trusselsbillede udgav Beredskabsstyrelsen i samarbejde med en række myndigheder i juni 2024 pjecen ”Forberedt på Kriser”, som bl.a. indeholder konkrete råd til, hvordan man som borger og husstand kan forberede sig på en krisesituation.
>
> Hertil kommer, at SAMSIK driver Cyberhotline for digital sikkerhed, hvor borgere og virksomheder kan ringe ind og modtage råd, hjælp og vejledning, hvis de vil forebygge

eller har været udsat for digital svindel eller cyberangreb. For at nå grupper af befolkningen med færre digitale kompetencer holder SAMSIK jævnligt webinarer og oplæg om digital sikkerhed for frontpersonale på fx borgerservicecentre, så de kan hjælpe borgerne direkte med at håndtere digitale trusler.

Initiativer målrettet offentlige myndigheder
Arbejdet med at højne sikkerheden for myndigheder og offentligt ansatte har været et vigtigt indsatsområde over en årrække. Som led i arbejdet gennemføres bl.a. briefinger, kurser og rådgivning af medarbejdere på alle niveauer i staten, ligesom der er udviklet kurser, e-læring, animationsfilm, vejledninger mv.

SAMSIK udbyder fx en række kurser målrettet offentligt ansatte om bl.a. samfundets beredskab, beredskabs-, og øvelsesplanlægning mv., ligesom at der er udarbejdet en række vejledninger og værktøjer målrettet danske myndigheders beredskabsplanlægning, herunder hybride trusler.

SAMSIK formidler via Sikkerdigital.dk materialer, som alle offentlige myndigheder kan bruge til at uddanne og træne offentligt ansattes adfærd og awareness inden for cyber- og informationssikkerhed.

Der er udviklet og gennemført en række initiativer målrettet topledere i staten. Der er desuden afholdt årlige topledерseminarer, hvor målgruppen er blevet præsenteret for udvalgte emner inden for cyber- og informationssikkerhed."

Ministeriet for
Samfundssikkerhed
og Beredskab

Dato: 24. februar 2025
Sagsnr.: 2025 - 36
Akt-id.: 104

Besvarelse af spørgsmål nr. 126 (Alm. del) fra Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg

Hermed sendes besvarelse af spørgsmål nr. 126 (Alm. del), som Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg har stillet til Ministeren for Samfundssikkerhed og Beredskab den 27. januar 2025. Spørgsmålet er stillet efter ønske fra Mike Villa Fonseca (UFG).

Torsten Schack Pedersen

Spørgsmål nr. 126 (Alm. del) fra Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg:

> ”Center for Cybersikkerhed har vist, at et dansk vandværk blev ramt af et cyberangreb, der kunne forstyrre forsyningen. Vil regeringen forpligte sig til at stille krav om minimumsstandarder for cybersikkerhed i alle samfundskritiske sektorer, og vil regeringen oprette et nationalt "cybersikkerhedscertifikat" for mindre aktører som lokale vandværker?”

Svar:

1. Danmark står over for et mere sammensat og komplekst trusselsbillede end for blot få år siden. Det gælder ikke mindst på cybersikkerhedsområdet, hvilket understreges af den seneste trusselsvurdering ”Cybertruslen mod Danmark” fra 2024 fra Styrelsen for Samfundssikkerhed samt af den specifikke trusselsvurdering af cybertruslen mod vandsektoren og angrebet på den danske vandsektor i december 2024.

Det skærpede trusselsbillede er for mig en klar påmindelse om, at vi skal tage cybertruslen alvorligt. Cybersikkerhed er derfor også et vigtigt fokusområde for mig som minister for samfundssikkerhed og beredskab. Det gælder ikke mindst for den kritiske infrastruktur, eksempelvis vandsektoren.

Implementeringen af NIS 2-direktivet er en grundsten i arbejdet med at sikre et højnet cybersikkerhedsniveau i hele Danmark. Med reglerne stilles der højere krav til cybersikkerhed inden for samfundskritiske sektorer, herunder vandsektoren.

Implementeringen sker ud fra en risikobaseret tilgang, hvor de omfattede virksomheder og myndigheder skal gennemføre cybersikkerhedsforanstaltninger, herunder bl.a. politikker for risikoanalyse, håndtering af hændelser og forsyningskædesikkerhed. NIS 2-direktivet medfører desuden styrkede tilsyns- og håndhævelsesbeføjelser for de kompetente myndigheder.

2. Hvad angår den del af spørgsmålet, der vedrører regeringens planer om at oprette et nationalt "cybersikkerhedscertifikat", har Ministeriet for Samfundssikkerhed og Beredskab til brug for besvarelsen indhentet en udtalelse fra Styrelsen for Samfundssikkerhed, der har oplyst følgende:

> "Der er ingen aktuelle planer fra myndighedernes side om at etablere et cybersikkerhedscertifikat til mindre virksomheder, men Styrelsen for Samfundssikkerhed har i regi af Cybersikkerhedspagten arbejdet med at udbrede en eksisterende cybersikkerhedsmærkningsordning som D-mærket, der også er målrettet mindre virksomheder. Samtidig arbejder Styrelsen for Samfundssikkerhed i regi af Cybersikkerhedspagten på at etablere et sæt nye minimumsanbefalinger til cybersikkerhed i mindre virksomheder, som har bred opbakning fra aktører i cybersikkerhedsbranchen.
>
> Cybersikkerhedspagten er et offentlig-privat samarbejde under Styrelsen for Samfundssikkerhed, som skal løfte cybersikkerheden i danske små- og mellemstore virksomheder."

Ministeriet for
Samfundssikkerhed
og Beredskab

Dato: 24. februar 2025
Sagsnr.: 2025 - 36
Akt-id.: 104

Besvarelse af spørgsmål nr. 127 (Alm. del) fra Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg

Hermed sendes besvarelse af spørgsmål nr. 127 (Alm. del), som Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg har stillet til ministeren for samfundssikkerhed og beredskab den 27. januar 2025. Spørgsmålet er stillet efter ønske fra Mike Villa Fonseca (UFG).

Torsten Schack Pedersen

Spørgsmål nr. 127 (Alm. del) fra Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg:

> ”Hvordan vil regeringen fremme samarbejdet mellem offentlige myndigheder og private virksomheder for at styrke cybersikkerheden? Kunne en model med deling af trusselsinformation i realtid være en løsning?”

Svar:

Offentlige-private samarbejder er en vigtig del af arbejdet med at styrke cyber- og informationssikkerheden i Danmark.

Derfor sætter jeg også stor pris på at få erhvervslivets, brancheorganisationers og Cybersikkerhedsrådets input til arbejdet med bl.a. implementeringen af NIS 2-direktivet og den kommende nationale strategi for cyber- og informationssikkerhed. Det vurderes løbende, hvordan det offentlige-private samarbejde kan styrkes og tilrettelægges på en hensigtsmæssig måde, herunder hvordan der kan skabes bedre rammer for at dele viden om trusler og sårbarheder med private aktører.

Der henvises i øvrigt til den samtidige besvarelse af spørgsmål nr. 118 (Alm. del) fra Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg.

Ministeriet for
Samfundssikkerhed
og Beredskab

Dato: 24. februar 2025
Sagsnr.: 2025 - 36
Akt-id.: 104

Besvarelse af spørgsmål nr. 118 (Alm. del) fra Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg

Hermed sendes besvarelse af spørgsmål nr. 118 (Alm. del), som Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg har stillet til ministeren for samfundssikkerhed og beredskab den 27. januar 2025. Spørgsmålet er stillet efter ønske fra Mike Villa Fonseca (UFG).

Torsten Schack Pedersen

Spørgsmål nr. 118 (Alm. del) fra Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg:

> ”Hvordan vil ministrene sikre bedre koordinering mellem forsvar, beredskab og civile aktører, så der opnås en helhedsorienteret tilgang til at imødegå hybride angreb på tværs af sektorer? Ministrene er velkomne til at koordinere besvarelsen, således den ene minister besvarer på vegne af begge”

Svar:

Ministeriet for Samfundssikkerhed og Beredskab har til brug for besvarelsen af spørgsmålet indhentet en udtalelse fra Styrelsen for Samfundssikkerhed, der har oplyst følgende:

> ”Styrelsen for samfundssikkerhed (SAMSIK) driver netværket, Strategisk Samarbejdsforum for Cybersikkerhed, hvor de største danske virksomheder inden for kritiske sektorer er repræsenteret og får klassificerede briefinger om både fysiske trusler og cybertrusler fra hhv. SAMSIK, FE og PET med henblik på at styrke virksomhedernes viden om trusselsbilledet for at blive bedre i stand til at sikre passende sikkerhedsforanstaltninger. SAMSIK sekretariatsbetjener desuden Cybersikkerhedsrådet, som har til formål at rådgive regeringen om, hvordan den digitale sikkerhed i Danmark styrkes, og bidrage til videndeling mellem myndigheder, erhvervsliv og forskningsverden.
>
> SAMSIK driver og sekretariatsbetjener Cybersikkerhedspagten, der er et offentlig-privat samarbejde, som skal løfte cybersikkerheden i danske små- og mellemstore virksomheder. Parterne i pagten arbejder for at skabe sammenhæng i de eksisterende tilbud og igangsætte nye fælles projekter, som særligt kan hjælpe de små- og mellemstore virksomheder med at løfte deres cybersikkerhed. Herudover fungerer pagten også som et netværk og forum for udveksling af viden, data og erfaringer om sikkerheden i danske virksomheder. Med skabelsen af Ministeriet for

Samfundssikkerhed og Beredskab vil Cybersikkerhedspagten fremover have et øget fokus på sammenhængen mellem cybersikkerhed og andre initiativer, der medvirker til at imødegå hybride trusler.

Der henvises i øvrigt også til den samtidige besvarelse af spørgsmål nr. 121 (Alm. del) fra Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg."

Ministeriet for Samfundssikkerhed og Beredskab

Dato: 24. februar 2025
Sagsnr.: 2025 - 36
Akt-id.: 104

Besvarelse af spørgsmål nr. 128 (Alm. del) fra Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg

Hermed sendes besvarelse af spørgsmål nr. 128 (Alm. del), som Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg har stillet til ministeren for samfundssikkerhed og beredskab den 27. januar 2025. Spørgsmålet er stillet efter ønske fra Mike Villa Fonseca (UFG).

Torsten Schack Pedersen

Spørgsmål nr. 128 (Alm. del) fra Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg:

> ”Hvis befolkningen og virksomhederne er mere modstandsdygtige, kan hybride angreb miste deres effekt. Vil regeringen arbejde for en national robusthedsplan, der inddrager både borgere og private virksomheder, og som for eksempel inkluderer skattefradrag for investeringer i beredskabsmaterialer og cybersikkerhed?”

Svar:

Styrkelse af modstandsdygtigheden for borgere og virksomheder har en høj prioritet for Ministeriet for Samfundssikkerhed og Beredskab, og der iværksættes flere indsatser i 2025, der skal bidrage til at styrke robustheden på tværs af samfundet.

Det er i regi af *Aftale om beredskabsområdet 2025-2026* aftalt, at der skal udarbejdes en ny strategi for at løfte cyber- og informationssikkerheden på tværs af samfundet i lyset af det komplekse og alvorlige trusselsbillede, som Danmark står over for.

Derudover spiller implementeringen af CER- og NIS 2-direktiverne en stor rolle. De to direktiver bidrager til et mere robust og modstandsdygtigt samfund, både hvad angår cybersikkerheden og den fysiske sikkerhed omkring vores kritiske infrastruktur. Lovforslagene, der skal implementere de to direktiver, blev fremsat for Folketinget den 6. februar 2025. CER-direktivet forpligter bl.a. medlemsstaterne til at udarbejde en national strategi og risikovurdering, som skal foreligge senest den 17. januar 2026, som bl.a. skal danne grundlaget for udpegningen af kritiske enheder.

Der henvises i øvrigt til den samtidige besvarelse af spørgsmål nr. 120 (Alm. del) fra Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg.

Ministeriet for
Samfundssikkerhed og Beredskab

Dato: 29. november 2024
Kontor: Sikkerhedskontoret
Sagsbeh: Emilie Frederikke Bock

Besvarelse af spørgsmål nr. 22 (Alm. del) fra Udvalget for Digitalisering og It

Hermed sendes besvarelse af spørgsmål nr. 22 (Alm. del), som Folketingets Udvalg for Digitalisering og It har stillet til ministeren for samfundssikkerhed og beredskab den 1. november 2024.

Torsten Schack Pedersen

Spørgsmål nr. 22 (Alm. del) fra Folketingets Udvalg for Digitalisering og It:

> "Vil ministeren redegøre for sine overvejelser på cybersikkerhedsområdet, herunder planerne for den danske implementering af NIS2?"

Svar:

1. Vi står over for et mere sammensat og komplekst trusselsbillede end for blot få år siden. Det gælder ikke mindst på cybersikkerhedsområdet, hvilket understreges af den seneste trusselsvurdering fra Center for Cybersikkerheds. Det fremgår bl.a. heraf, at niveauet for cyberspionage og cyberkriminalitet er MEGET HØJT, truslen fra cyberaktivisme er HØJ. Truslen fra destruktive cyberangreb er tidligere på året blevet hævet fra LAV til MIDDEL. Niveauet blev hævet på baggrund af en udvikling i Ruslands risikovillighed i forhold til at anvende hybride virkemidler, herunder destruktive cyberangreb, mod europæiske NATO-lande

Det skærpede trusselsbillede er for mig en klar påmindelse om, at vi skal tage cybertruslen alvorligt. Cybersikkerhed er derfor også et vigtigt fokusområde for mig som minister for samfundssikkerhed og beredskab.

2. En vigtig opgave på cybersikkerhedsområdet i den kommende tid er implementeringen af NIS 2-direktivet, som skaber et højere og mere ensartet cybersikkerhedsniveau på tværs af EU. Det sker ud fra en risikobaseret tilgang, hvor de omfattede virksomheder og myndigheder skal sikre, at de gennemfører cybersikkerhedsforanstaltninger, herunder bl.a. politikker for risikoanalyse, håndtering af hændelser og forsyningskædesikkerhed. NIS 2-direktivet medfører desuden styrkede tilsyns- og håndhævelsesbeføjelser for de kompetente myndigheder.

Implementeringen af NIS 2-direktivet er dermed en grundsten i arbejdet med at sikre et højnet cybersikkerhedsniveau i hele Danmark. Vigtigheden af et generelt højt cybersikkerhedsniveau skal særligt ses i lyset af, at cyberkriminelle og ondsindede hackere ofte går efter det svageste led i kæden.

3. Samtidig har NIS 2-direktivet stor betydning for erhvervslivet og myndigheder.

Som minister for samfundssikkerhed og beredskab ligger det mig på sinde, at der sikres en så god proces som muligt for det videre arbejde med implementeringen frem mod reglernes ikrafttræden til sommer.

Det indebærer bl.a. en bred inddragelse af myndigheder, virksomheder og brancheorganisationer med henblik på at lytte til de input, der måtte være til den videre implementering. Det gælder også i forhold til udarbejdelsen af relevante vejledninger parallelt med færdiggørelse og behandling af lovforslaget.

4. Der er også helt forståeligt fokus på, hvordan de nye regler vil blive håndhævet af de kompetente tilsynsmyndigheder – særligt i den første tid efter, at reglerne træder i kraft.

Jeg vil i den forbindelse gerne understrege, at det i mine øjne vil være naturligt, at tilsynsmyndighederne ikke hiver bødeblokken frem som det første. I den forbindelse er det værd at bemærke, at overtrædelse af reglerne efter omstændighederne kan håndteres ved brug af andre reaktionsmuligheder, herunder påbud og forbud. Den tilgang vil Ministeriet for Samfundssikkerhed og Beredskab også tage med ind i det videre arbejde, hvor ministeriet som led i den koordinerende rolle i forhold til NIS 2-implementeringen bl.a. skal sikre et tæt samarbejde mellem tilsynsmyndighederne.

5. NIS 2-lovforslaget, som implementerer NIS 2-direktivet, forventes fremsat for Folketinget i februar 2025 og forventes at træde i kraft den 1. juli 2025.

Som det fremgår af mit brev af 30. september 2024 til Folketingets Udvalg for Digitalisering og It (DIU Alm. del (2024-25), bilag 28), følger det af NIS 2-direktivet, at fristen for implementering var den 17. oktober 2024, og at Ministeriet for Samfundssikkerhed og Beredskab derfor ville sørge for, at EU-Kommissionen underrettes om den forsinkede implementering. EU-Kommissionen blev orienteret om forsinkelsen den 15. oktober 2024.

Ministeriet for
Samfundssikkerhed og Beredskab

Dato:	29. november 2024
Kontor:	Kontor for Cyber- og Informationssikkerhed
Sagsbeh:	Josefine Boolsen
Sagsnr.:	Sagsnummer
Dok.:	Dokumentnummer

Besvarelse af spørgsmål nr. 21 (Alm. del) fra Udvalget for Digitalisering og It

Hermed sendes besvarelse af spørgsmål nr. 21 (Alm. del), som Folketingets Udvalg for Digitalisering og It har stillet til ministeren for samfundssikkerhed og beredskab den 1. november 2024. Spørgsmålet er stillet efter ønske fra Dina Raabjerg (KF).

Torsten Schack Pedersen

Spørgsmål nr. 21 (Alm. del) fra Folketingets Udvalg for Digitalisering og It:

> ”Vil ministeren oplyse, om man i dag foretager tests lokalt for at vurdere og sikre, at virksomheder, installationer og organisationer i samfundskritiske sektorer er modstandsdygtige overfor cyberangreb – eksempelvis på hospitaler, men også energikraftværker, myndigheder med ansvar for udbetaling af sociale ydelser og forsyningsselskaber? Der henvises til, at blandt andet visse typer af finansielle virksomheder er pålagt at foretage tests af it- og cybersikkerheden, jf. § 333 i Lov om finansiel virksomhed. Såfremt man ikke udfører konkrete sikkerhedstests (penetrationstests), kan ministeren så bekræfte, at vurderingen af cybersikkerheden alene baserer sig på formel overholdelse af krav og regler og ikke virkelighedsnære test, der sikrer, at offentlige virksomheder reelt er modstandsdygtige overfor cyberangreb?

Svar:

Ministeriet for Samfundssikkerhed og Beredskab har med den kongelige resolution den 29. august 2024 fået ressortoverført en række sagsområder fra blandt andet Forsvarsministeriet og det daværende Digitaliserings- og Ligestillingsministerium vedrørende cybersikkerhed og digital informationssikkerhed. Det omfatter bl.a. opgaven med at vejlede og rådgive borgere, virksomheder og myndigheder inden for området. Det er en vigtig opgave, som bl.a. implementeringen af NIS 2-direktivet vil være med til at sætte rammerne for.

Tilrettelæggelsen af beredskabet omkring den samfundskritiske infrastruktur er afgørende for at skabe et sikkert og robust samfund. I Danmark følger det grundlæggende af sektoransvarsprincippet, at den enkelte sektor skal vurdere det konkrete risikobillede og træffe passende foranstaltninger. Det vil dog være en central opgave for Ministeriet for Samfundssikkerhed og Beredskab at rådgive og vejlede virksomheder og myndigheder på tværs af sektorerne for at sikre et ensartet og tilfredsstillende niveau af cybersikkerhed i Danmark.

Ministeriet for Samfundssikkerhed og Beredskab har til brug for besvarelsen af spørgsmålet indhentet en udtalelse fra Center for Cybersikkerhed (CFCS), der har oplyst følgende:

”CFCS er bekendt med, at nogle myndigheder og virksomheder – som led i varetagelsen af ansvaret for deres cyber- og informationssikkerhed – anvender sikkerhedstest, herunder penetrationstest. CFCS har dog ikke nærmere kendskab til anvendelsen af test i de enkelte sektorer.

Det følger af § 1, stk. 1, i lov om Center for Cybersikkerhed, at centeret har til opgave at understøtte et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur som samfundsvigtige funktioner er afhængige af.”

Herudover har Ministeriet for Samfundssikkerhed og Beredskab indhentet en udtalelse fra Forsvarsministeriet, der har oplyst følgende:

”Forsvarsministeriet har den 21. november 2024 anmodet Forsvarets Efterretningstjeneste (FE) om at bidrage til besvarelsen af spørgsmål nr. 21 (alm. del) fra Udvalget for Digitalisering og It, som er stillet til ministeren for samfundssikkerhed og beredskab.

FE kan til brug for besvarelsen oplyse følgende:

”Med henblik på at kunne rådgive myndigheder og virksomheder om forebyggelse af sikkerhedshændelser kan FE gennemføre forebyggende sikkerhedstekniske undersøgelser, herunder penetrationstest, når en myndighed eller en virksomhed har anmodet centeret herom, jf. § 6 a. i lov om Center for Cybersikkerhed.

Som led i en penetrationstest kan der udføres et simuleret angreb på et system eller netværk, hvor sårbarheder og potentielle angrebsvektorer identificeres. På baggrund af undersøgelsen kan myndigheden eller virksomheden rådgives om, hvilke konkrete tiltag der kan gennemføres for at opnå et højere sikkerhedsniveau.””

INDENRIGS- OG SUNDHEDSMINISTERIET

Slotsholmsgade 10-12
DK-1216 København K

T +45 7226 9000
M sum@sum.dk
W sum.dk

Folketingets Digitaliserings- og It-udvalg

Dato: 29-11-2024
Enhed: Digitalisering og hjemmebehandling
Sagsbeh: kkc
Sagsnr.:2024 - 13408
Dok. nr.: 250695

Hermed sendes besvarelse af spørgsmål nr. 20 (Alm. del), som Folketingets Digitaliserings- og It-udvalg har stillet til indenrigs- og sundhedsministeren den 1. november 2024. Spørgsmålet er stillet efter ønske fra Dina Raabjerg (KF).

Spørgsmål nr. 20:
"Vil ministeren oplyse, om det er regeringens vurdering, at man i sundhedssektoren i dag gør tilstrækkeligt for at sikre, at man er modstandsdygtige overfor cyberangreb? Der henvises til, at der er flere eksempler fra udlandet og Danmark, der indikerer, at sundhedssektoren er udsat."

Svar:
Center for Cybersikkerhed vurderer, at der fortsat er en alvorlig cybertrussel mod sundhedssektoren i Danmark. Samtidig er cybertruslen er omskiftelig og stiller derfor krav om, at arbejdet med cyber- og informationssikkerhed er en risikobaseret og dynamisk indsats, der kan tilpasses de løbende skift i trusselsbilledet.

Jeg kan oplyse, at arbejdet med cyber- og informationssikkerhed i Danmark er baseret på sektoransvarsprincippet, hvilket betyder, at regioner, kommuner og sundhedssektorens øvrige aktører har ansvaret for egen sikkerhed.
Sundhedssektoren består af mange forskellige aktører; både offentlige og private, og store, mellemstore og små aktører. Derfor er modenhedsniveauet for cyber- og informationssikkerhed også meget forskelligt aktørerne imellem. Jeg kan dog oplyse, at EU's NIS2-direktiv, som implementeres i dansk lov til næste år, har til formål i højere grad at ensarte cybersikkerheden og modstandsdygtigheden over for cybertrusler på tværs af EU, herunder også inden for sundhedssektoren.

Jeg kan desuden oplyse, at sundhedssektoren har en sektorstrategi for cyber- og informationssikkerhed 2023-2025, som er udarbejdet af stat, regioner og kommuner i fællesskab. Strategien danner rammen om sundhedsvæsenets fælles indsatser for at styrke cyber- og informationssikkerheden på tværs af sundhedsvæsnet, som koordineres og understøttes af sundhedssektorens decentrale cyber- og informationssikkerhedsenhed (DCISSund) i Sundhedsdatastyrelsen. DCISSund er bl.a. ansvarlig for sundhedssektorens sikkerhedsanalysecenter og følger løbende det aktuelle trusselsbillede og deler denne viden med aktørerne i sundhedssektoren.

Sektorstrategien indeholder bl.a. initiativer rettet mod cybersikkerheden hos sektorens mindre aktører, fælles rammer og værktøjer til løbende test af cybersikkerheden og fælles beredskabsøvelser.

Det er helt afgørende, at digitaliseringen af sundhedsvæsenet foregår i trygge og sikre rammer. Når vi digitaliserer sundhedsvæsenet, skal sikkerheden naturligvis også følge med. Borgerne skal kunne stole på, at sundhedsvæsenet er tilgængeligt, når de har brug for det, og at sundhedsvæsenet passer godt på de følsomme

personoplysninger, som de betror sundhedsvæsenet i forbindelse med et behandlingsforløb.

Med venlig hilsen

Sophie Løhde