Transportministeriet

Cyber- og informations-sikkerhedsstrategi 2022-2025

September 2022

Udgivet af: Transportministeriet
Frederiksholms Kanal 27F
1220 København K

ISBN netudgave: 978-87-93292-72-7
Forsideill. Transportministeriet

Indhold

Forord

En sikker og effektiv afvikling af lufttrafik, togdrift, vejnettet og sikring af adgang til havne er kritiske funktioner i det danske samfund, som i vid udstrækning bliver mere og mere afhængige af digitale systemer og udstyr.

Cockpit, kontroltårne, signalsystemer, trafikovervågning med mere understøttes alt sammen af digitale systemer og udstyr som servere, software og hardware, SCADA-systemer, cloud-løsninger og meget andet. I mange tilfælde er digitale systemer og udstyr medvirkende til øget sikkerhed og effektiv fremkommelighed i form af overvågning og vedligehold af driftskritiske funktioner, hurtigere information og arbejdsgange.

Men en øget anvendelse af digitale systemer og udstyr medfører også en øget afhængighed af disse og i mange tilfælde en øget sårbarhed over for ondsindede aktører. Cyberangreb mod samfundets kritiske transportfunktioner kan resultere i store økonomiske konsekvenser for virksomheder, medarbejdere og - i yderste konsekvens - for sikkerheden og fremkommeligheden.

Center for Cybersikkerhed (CFCS) vurderer i 2022, at truslen fra cyberspionage og cyberkriminalitet mod dansk luftfart samt land- og lufttransport er meget høj. Det betyder, at danske lufthavne, flyselskaber, transportmyndigheder, infrastrukturforvaltere, togselskaber og havne er underlagt en vedvarende og specifik trussel fra aktører, som har evnen, hensigten og kapaciteten til at gennemføre cyberangreb.

Det er en alvorlig trussel, som i yderste tilfælde truer sikkerheden og mobiliteten i det danske samfund. Det tager transportmyndigheder og virksomheder meget alvorligt.

Denne strategi har derfor til formål at styrke transportsektorens evne til at forudse, forebygge, opdage og håndtere cyber- og informationssikkerhedshændelser. Det skal gøres i samarbejde med aktørerne i transportsektoren ved at gennemføre en række indsatser inden for fire udvalgte områder – 1) risikostyring, 2) cyberberedskab, 3) net- og informationssikkerhed (EU-regulering) og uddannelse & awarenes – som adresserer formålene.

Indsatserne tilrettelægges på baggrund af videreførelse af nuværende cybersikkerhedsarbejde, nationale krav til Transportministeriets cyberarbejde, trusselsvurderinger, Trafikstyrelsens egen sektorrisikovurdering (Cyber-ROS) og i løbende samarbejde med branchevirksomhederne.

Strategien udmøntes som del af "National strategi for cyber- og informationssikkerhed", som Regeringen offentliggjorde i december 2021.

1. Evaluering af transportsektor-strategien 2019-2021

I januar 2019 udgav Transportministeriet sin første cyber- og informationssikkerhedsstrategi.

Strategien havde sit ophav i den nationale cyber- og informationssikkerhedsstrategi for 2018-2021. Heri blev transportsektoren identificeret som én af seks samfundskritiske sektorer.

Den nationale cyber- og informationssikkerhedsstrategi pålagde overordnet de samfundskritiske sektorer at:

- Etablere en decentral cyber- og informationssikkerhedsenhed (DCIS).
- Udarbejde sektorstrategier for cyber- og informationssikkerhedsarbejdet.
- Indstationere en medarbejder i Trusselsvurderingsenheden i Center for Cybersikkerhed (CFCS).

Sektorstrategien definerede en række indsatser, der skulle gennemføres i løbet af strategiperiodens fire år. Den følgende evaluering fokuserer på de tre ovenstående områder.

Evalueringen er gennemført med input fra transportsektorens aktører. DCIS-TRP (decentral cyber- og informationssikkerhedsenhed for transportsektoren) har blandt andet afholdt workshops med centrale sektoraktører med det formål at drøfte såvel nuværende som det tidligere og kommende strategiarbejde.

Sammenfatning for evaluering

Med strategien for 2018-2021 blev transportmyndighedernes arbejde med cybersikkerhed forankret i den såkaldte DCIS-TRP.

DCIS-TRP har siden 2018 arbejdet med sektor- og myndighedskoordination og gennemførelse af konkrete indsatser med det formål at højne cybersikkerhedsniveauet på Transportministeriets ressortområde.

Strategien har bidraget til at styrke videndelingen, konkret adresseret risikostyringen og højnet kendskabet til trusselsbilledet på tværs af transportsektoren. På myndighedsniveau har strategien for første gang etableret et samlet og løbende overblik over cybersikkerhedsniveauet og virksomhedernes hidtidige indsatser.

Indstationeringen af en medarbejder fra transportmyndighederne i CFCS' trusselsvurderingsenhed har bidraget til et styrket samarbejde mellem Transportministeriets område og CFCS og har understøttet sektorspecifik vidensopbygning omkring cybersikkerhed i transportsektoren.

Det er på dette grundlag, at indsatsernes i sektorstrategien for 2022-25 er udtænkt. Erfaringerne fra den første strategiperiode udgør dermed det fundament, som det kommende strategiarbejde bygger videre på.

1.1 Etablering af DCIS

Nationalt var formålet med at nedsætte decentrale cyber- og informationssikkerhedsenheder (DCIS) at styrke evnen til at håndtere cyber- og informationssikkerhed i de samfundskritiske sektorer, herunder transportsektoren.

Den daværende sektorstrategi etablerede en decentral cyber- og informationssikkerhedsenhed (DCIS) i Trafikstyrelsen (DCIS-TRP), hvis primære opgave var at sikre sektorkoordination med CFCS og PET og sekundært skabe overblik over sektorens arbejde med cyber- og informationssikkerhed. På den baggrund skulle DCIS-TRP gennemføre relevante indsatser, som kunne bidrage til at højne cybersikkerhedsniveauet inden for Transportministeriets ressortområde.

Indsatserne kunne for eksempel være:

- Beredskabsøvelser
- Videndeling og vejledning
- Sektorspecifikke trusselsvurderinger
- Sikkerhedsopbygning
- Sårbarhedsvurderinger

Indsatserne er primært gennemført i samarbejde med branchevirksomhederne i nyetablerede virksomhedsfora ("Dialoggrupper for cybersikkerhed"), hvor virksomhederne har deltaget med deres *chief information security officer* (CISO) og lignende kompetencer. Dialoggrupperne har også været samlingspunkt for sektorens NIS-aktører[1], og implementeringen af NIS-direktivet i transportsektoren er løbende blevet drøftet.

DCIS-TRP fungerer også som samarbejdspartner for CFCS i transportsektoren og derved også som bindeled mellem sektorvirksomheder og CFCS. Det indebærer først og fremmest, at indsatser målrettet transportsektoren i den nationale cyberstrategi er blevet gennemført i samarbejde med DCIS-TRP, men også at DCIS-TRP faciliterer konkrete samarbejder mellem sektorvirksomheder og CFCS samt videreformidler sektorspecifikke trusselsvurderinger.

1.2 Sektorstrategiens initiativer 2019-2022

Det var – og er fortsat – en præmis for gennemførelsen af sektorstrategien, at samarbejdet mellem DCIS-TRP og sektorvirksomhederne i regi af strategien ikke er regelbundet. Samarbejdet er baseret på parternes vilje, ressourcer og kapacitet til i fællesskab at samarbejde om at styrke cyber- og informationssikkerheden i sektoren.

Samarbejdet forsøger så vidt muligt at komplementere og give værdi til virksomhedernes eksisterende arbejde med cyber- og informationssikkerhed.

Transportsektoren er i stigende grad genstand for øget EU-regulering på cyber- og informationssikkerhedsområdet, men ikke alle virksomheder rammes ens eller af samme regulering. Dette udgør også et afgørende rammevilkår og er en central opgave for DCIS-TRP for så vidt angår vejledning og kommunikation.

Det er ydermere et rammevilkår for arbejdet med cybersikkerhed i transportsektoren, at transportvirksomhederne er meget forskellige. Sektoren udgør en heterogen gruppe med meget forskellige ressourcer, kompetencer og erfaringer på tværs af virksomhederne. Virksomhedernes interesser, behov og forudsætninger for at deltage i det tværsektorielle samarbejde under DCIS-TRP er derfor også meget forskellige.

På Transportministeriets område blev der formuleret 12 indsatser i strategiperioden for 2019-2021 fordelt på tre kategorier; 1) overblik og selvindsigt, 2) sårbarhedserkendelse og 3) håndtering og internationalt arbejde og regulering, *jf. boks 1.1.*

Boks 1.1 | De primære indsatsområder i første strategiperiode for 2019-2021

1. OVERBLIK OG SELVINDSIGT
   - 1.1 Kortlægning af kritisk infrastruktur og tjenester
   - 1.2 Modenhedsmåling
   - 1.3 Fortrolige samarbejdsfora for cybersikkerhed
   - 1.4 Ledelsesfokus på cybersikkerhed
   - 1.5 Trusselskatalog

2. SÅRBARHEDSERKENDELSE OG HÅNDTERING
   - 2.1 Risikovurderinger
   - 2.2 Leverandørstyring
   - 2.3 Best-practice og vejledninger
   - 2.4 Medarbejder-awareness
   - 2.5 Cybersikkerhed som del af sektorberedskabet

3. INTERNATIONALT ARBEJDE OG REGULERING
   - 3.1 International interessevaretagelse
   - 3.2 Samarbejde med Færdselsstyrelsen, Vejdirektoratet og Transport-, Bygnings- og Boligministeriets departement om selvkørende teknologi.

[1] NIS = Direktiv (EU) 2016/1148, af 6. juli 2016 *(direktiv om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen). I transportsektoren er det pt. Københavns Lufthavn (CPH), Naviair, DSB og Banedanmark, som er underlagt NIS-reglerne.*

Indsatserne blev formuleret på baggrund af en risiko- og sårbarhedsvurdering af sektoren udarbejdet af konsulentfirmaet Dubex A/S samt inddragelse af sektorvirksomhederne.

Nogle indsatser var målrettede sektorens aktører, mens andre havde som primært fokus at bidrage til vidensopbygning i DCIS-TRP.

I løbet af 2018-2021 er der på Transportministeriets område arbejdet med og indfriet initiativer ud fra en konkret prioritering. Nogle initiativer blev i strategiperioden opprioriteret på grund af større efterspørgsel og merværdi i sektoren og trak derfor flere ressourcer og opmærksomhed i DCIS-TRP, mens andre blev nedprioriteret eller afsluttet efter en kortlægning af potentialet og værdien for henholdsvis sektoren og DCIS-TRP.

Som nyetableret cyberenhed i transportsektoren havde DCIS-TRP et behov for at tilegne sig viden om sektorens eksisterende cybersikkerhedsarbejde. Efterhånden som DCIS-TRP opbyggede viden, blev det mere tydeligt, hvilke indsatser der skulle prioriteres frem for andre.

Langt de fleste initiativer blev udtænkt som sektorvendte og med den hensigt at skabe anvendelige produkter og nytteværdi for transportaktørerne. Disse initiativer blev planlagt i samarbejde med transportsektorens aktører.

Etableringen af to dialoggrupper (henholdsvis for aktørerne i luftfarten og landtransporten) er et eksempel på et initiativ, der har mødt stor opbakning i sektoren, og som opleves at have bibragt værdi for deltagerne.

DCIS-TRP udarbejdede de formelle rammer og sammensatte deltagerkredsen. Siden 2018 er der afholdt 2-3 møder årligt. Dialoggrupperne har haft til formål at etablere et fortroligt rum til videndeling, erfaringsudveksling og drøftelse af strategiinitiativer og *best practice* i forhold til implementering af konkrete foranstaltninger. Sektoren har efterspurgt temabaserede møder og ekspertoplæg, der kan sætte fokus på aktuelle problemstillinger og give deltagerne mere dybdegående viden om konkrete relevante emner.

Et konkret initiativ, som blev opprioriteret i strategiperioden, er DCIS-TRP's værktøj til risiko- og sårbarhedsvurdering (Cyber-ROS), der blev udviklet med inspiration fra energisektoren og i samarbejde med transportsektoren og CFCS. Værktøjet er både en skabelon til at udarbejde risikovurderinger samt et indberetningsværktøj, hvis formål er at hjælpe organisationer med at arbejde risikobaseret med cyber- og informationssikkerheden. Værktøjet blev udviklet som et direkte anvendeligt redskab, aktørerne kan benytte til at forankre risikovurderingsprocesser i cyberarbejdet, og har desuden udgjort et grundlag for at drøfte

sårbarheder og risici på tværs af sektoraktørerne. Værktøjer kan ydermere anvendes til at efterleve reguleringskrav (AVSEC[2], NIS2[3]) om at gennemføre risikovurderinger.

Af øvrige initiativer kan nævnes DCIS-TRPs bidrag til at gennemføre en tværgående sektor-fælles cyber-beredskabsøvelse samt DCIS-TRPs arbejde med at kortlægge kritisk infrastruktur og tjenester. Sidstnævnte initiativer har dog haft et afgrænset fokus på udpegede NIS-aktørerne.

1.3 Indstationering af medarbejder i CFCS trusselsvurderingsenhed

Formålet med indstationeringen af en sektormedarbejder i CFCS' trusselsvurderingsenhed var at understøtte CFCS' arbejde med at udarbejde sektorspecifikke trusselsvurderinger for transportsektoren. Forud for ordningen blev der ikke udarbejdet sektorspecifikke trusselsvurderinger for transportområdet.

Trusselsvurderinger anvendes blandt andet i styrelsens og sektorens risikovurderingsarbejde og har til overordnet formål at give branchen ny viden og dybere indsigt i både egne sårbarheder og det sektorspecifikke trusselsbillede og dermed samlet set styrke sektorens forudsætninger for at modvirke trusler mod cybersikkerheden.

Den indstationerede medarbejder skulle ansættes i en to-årig periode og konkret bidrage med branchespecifik viden og netværk fra transportsektoren til udarbejdelsen af sektorspecifikke trusselsvurderinger. Derudover skulle medarbejderen skabe opmærksomhed og viden om cybertruslen for virksomheder og myndigheder. Endelig skulle medarbejderen fungere som bindeled mellem DCIS-TRP og CFCS trusselsvurderingsenhed.

Første trusselsvurdering udkom september 2018. Siden er der publiceret årlige sektorspecifikke trusselsvurderinger for henholdsvis luftfart, jernbane og land- og lufttransporten, *jf. tabel 1.*

---

[2] Kommissionens gennemførelsesforordning (EU) 2019/1583 af 25. september 2019 om ændring af gennemførelsesforordning (EU) 2015/1998 af om detaljerede foranstaltninger til gennemførelse af de fælles grundlæggende normer for luftfartssikkerhed for så vidt angår cybersikkerhedsforanstaltninger (EØS-relevant tekst).

[3] Det reviderede NIS-direktiv (NIS2) er ikke offentliggjort på tidspunktet for publicering af denne strategi.

Tabel 1: Udgivelse af sektorspecifikke trusselsvurderinger

Udgivelsesdato	Trusselsvurdering
08.09.2021	Cybertruslen mod dansk luftfart 2021
08.09.2021	Cybertruslen mod land- og lufttransporten 2021
11.02.2021	Cybertruslen mod jernbanesektoren 2021
14.10.2020	Cybertruslen mod søfart og havne
08.06.2020	Cybertruslen mod dansk luftfart 2020
08.06.2020	Cybertruslen mod land- og lufttransporten 2020
04.11.2019	Cybertruslen mod dansk luftfart 2019
08.09.2018	Cybertruslen mod land- og lufttransporten 2018

Såvel myndigheder som virksomheder har kunnet benytte trusselsvurderingerne, der har indgået i sektorens eksisterende arbejde med trusselsbilledet.

Det overordnede samarbejde mellem DCIS og CFCS trusselsvurderingsenhed har generelt været udbytterigt, og det har bidraget til CFCS's viden om og fokus på særlige sektorproblemstillinger.

Med den nationale cyberstrategi (2022-2024) er det besluttet, at ordningen udfases, men at CFCS' understøttelse af sektorerne i form af sektorspecifikke trusselsvurderinger i øvrigt fortsættes. Baggrunden herfor er blandt andet at styrke fastholdelse og udvikling af kompetencerne i trusselsvurderingsenheden, og idet ordningen ikke i alle sektorer har vist sig at være bæredygtig.

2. Arbejde med transportsektor-strategien

Transportsektorens Cyber- og informationssikkerhedsstrategi for 2022-2025 (herefter sektorstrategien) består af indsatser som 1) videreføres fra den forrige sektorstrategi, 2) gennemføres som krav fra den nationale cyber- og informationssikkerhedsstrategi og 3) er nye og planlagt til gennemførelse på Transportministeriets område i forbindelse med den nye sektorstrategi.

I det følgende beskrives kort rammerne for strategiarbejdet, herunder den nationale cyberstrategi, det tværsektoriale samarbejde og sektorspecifik regulering.

2.1 Nationalt og sektorielt set-up for cybersikkerhedsarbejdet

De involverede ministerområder samarbejder om gennemførelsen af den nationale strategi og sektorstrategier i DCIS-Forum. Dette var også tilfældet i det hidtidige tværministerielle samarbejde under den nationale cyberstrategi.

DCIS-Forum afholdes formelt af Digitaliseringsstyrelsen og Center for Cybersikkerhed med deltagelse fra de samfundskritiske sektorer i regi af den nationale cyberstrategi. I den kommende strategiperiode udvides kredsen af deltagende ministerområder betragteligt.

Det tværministerielle samarbejde kan både foregå i regi af DCIS-Forum, men også bilateralt mellem fagministerierne. DCIS-Transport har eksempelvis et godt samarbejde med DCIS-Energi inden for risikovurderinger af cybersikkerhedstrusler, mens samarbejdet med DCIS-Søfart har naturlige snitflader i forhold til håndteringen af cybersikkerhed på det maritime område.

2.2 Gennemførelse af nationale krav (initiativ 1.1, NCIS)

De strategiske indsatser i National strategi for cyber- og informationssikkerhed 2022-2024, som er relevante for de deltagende ministerområder, koordineres og gennemføres i regi af DCIS-Forum. I forlængelse af den nationale cyberstrategi er der opstillet ti krav/indsatsområder, som sektorernes DCIS'er skal forholde sig til i forhold til samfundskritiske funktioner i statsligt regi, *jf. boks 2.1*.

Boks 2.1 | Nationale krav til samfundskritiske funktioner i statslig regi

1. Strategi for cyber- og informationssikkerhed
2. DCIS med operativ kapacitet
3. Kortlægning af kritisk it-infrastruktur (statslig regi)
4. Behov for at kommunikere TTJ (til tjenestebrug)
5. Logningspolitik
6. Tilslutnings til CFCS' sensornetværk
7. Involvering af CFCS i forbindelse med indkøb og udbud
8. Indberetningspligt, sikkerhedsgodkendelser og beredskabsaftaler for samfundskritiske it-systemer
9. Vejledninger og anbefalinger
10. Lovgivning om cybersikkerhed

På transportområdet er udmøntningen af kravene udlagt fra Transportministeriet til DCIS-TRP i forhold til Banedanmark, DSB og Naviair. De tre aktører er som statslige enheder (styrelse og statsligt ejede virksomheder) udpeget som NIS-operatører med ansvar for samfundskritiske funktioner.

Banedanmark er infrastrukturforvalter på det statslige jernbanenet og dermed ansvarlig for vedligehold, planlægning og trafikstyring for den centrale baneinfrastruktur. DSB står for langt størstedelen af passagertransport med tog i Danmark, og Naviair er den eneste trafikledelses- og kontroloperatør for luftrummet over Danmark.

Gennemførelsen af ovenstående krav vil ske i direkte samarbejde mellem DCIS-TRP og de tre aktører.

2.3 Samarbejde med sektoren og øvrige eksterne partnere

Parallelt med tilblivelsen af den første sektorstrategi, nedsatte DCIS-TRP to virksomhedsfora for cybersikkerhed. Foraene samler CISO'er, it-sikkerhedsfolk og lignende fra henholdsvis luftfartssektoren samt jernbane- og vejrområdet. Dialoggrupperne er omdrejningspunkt for samarbejdet på cybersikkerhedsområdet mellem myndigheder og virksomheder.

I foraene drøftes blandt andet aktuelle cybersikkerhedsudfordringer, og der gennemføres indsatser som del af sektorens cyberstrategi. Foraene har hyppig deltagelse af eksterne parter, som bidrager med faglige oplæg, herunder for eksempel CFCS.

DCIS-TRP har også et veletableret samarbejde med CFCS Rådgivning, som er sparrings- og rådgivningspartner på konkrete strategiindsatser i sektoren. CFCS Rådgivning yder også rådgivningsforløb til sektorvirksomhederne inden

for risikostyring, leverandørstyring, beredskab samt uddannelse og kompetence.

2.4 Sektorspecifik international regulering

Det nationale cyberstrategiarbejde indgår i transportsektoren som led i en større sammenhæng på cybersikkerhedsområdet. Det drejer sig ikke mindst om international regulering, der i høj grad sætter retningen for cybersikkerhedsarbejdet i de kommende år.

NIS-direktivet (NIS1 & kommende NIS2)

NIS-direktivet blev vedtaget i EU i 2016 med det formål at styrke medlemslandenes beskyttelse, resiliens og hændelseshåndtering af cyberangreb mod kritisk it-infrastruktur.

Direktivet blev implementeret ved lov og bekendtgørelse i transportsektoren i 2018, hvilket medførte, at DCIS-TRP identificerede fire såkaldte operatører af væsentlige transporttjenester. Disse fire virksomheder blev blandt andet underlagt krav om at:

- Opnå en akkrediteret certificering i en international anerkendt standard for styring af informationssikkerhed.
- Indberette væsentlige sikkerhedshændelser til Trafikstyrelsen og CFCS.

Siden 2018 har DCIS-TRP hvert andet år vurderet, hvorvidt yderligere virksomheder i sektoren skulle omfattes af kravene.

Det oprindelige NIS-direktiv er i 2022 under revision og i kommende år vil det reviderede NIS2-direktiv skulle implementeres nationalt.

NIS2 udvider anvendelsesområdet, det vil sige antallet af omfattede sektorer og virksomheder, markant. Samtidig skærpes sikkerhedskrav, tilsynskrav og krav om indberetning af hændelser og såkaldte alvorlige nærved-hændelser.

Det forventes at kræve markante ressourcer af såvel myndigheder som virksomheder at implementere og efterleve kravene i det nye direktiv, og der vil blive øget efterspørgsel på kompetencer og personale, der kan løfte de nye opgaver både i transportsektoren og nationalt. Af samme årsag er NIS2 et selvstændigt indsatsområde i denne strategi med det formål at klargøre sektoren til efterlevelse af direktivet og følge den løbende implementering.

Cybersikkerhedsregler inden for luftfart/security

Ved udgangen af 2021 trådte nye cyberregler i kraft inden for de eksisterende regler om luftfart/security (forordning (EU) 2019/1583). Formålet med de nye cyberregler er at understøtte sikker luftfart ved at sikre, at virksomheder i luftfarten beskytter relevante systemer mod cyberhændelser.

Reglerne gælder i Danmark for lufthavnsoperatører, luftfartsselskaber, fragtagenter og sikkerhedsgodkendte leverandører.

De nye regler indebærer, at ovenstående aktører identificerer og beskytter deres security-kritiske informations- og kommunikationsteknologisystemer og data mod cyberangreb. Virksomheder forpligtes til at udarbejde risikovurderinger, forholde sig til mitigerende foranstaltninger og justere sikkerhedsplaner, der skal sendes til godkendelse hos Trafikstyrelsen, der efterfølgende fører tilsyn med, at reglerne efterleves.

Der stilles i øvrigt specifikke regler til, at personale, der arbejder med IT-sikkerhed for så vidt angår security-opgaver, skal uddannes og trænes i forhold til cybersikkerhed.

Cyberregler i regi af luftfart/safety (EASA)

Inden for de kommende år forventes det, at nye regler om cybersikkerhed vil træde i kraft for aktører på safety-området. Formålet med reglerne er at få alle aktører – både Trafikstyrelsen, luftfartsvirksomheder og aktører i sektoren – til at bidrage til beskyttelse af luftfartssystemer mod cyberangreb. Omdrejningspunktet for reglerne forventes at være et krav om etablering af et ledelsessystem for informationssikkerhed (ISMS). Derudover skal organisationer indberette cybersikkerhedshændelser.

Reglerne forventes offentliggjort ultimo 2022 med en overgangsperiode på 1-2 år til implementering.

3. Strategiske indsatsområder

De strategiske indsatsområder udgør cyberstrategiens fremadrettede del og rummer de spor, som i 2022-2025 udmøntes i form af aktiviteter til at højne sektorens evne til at modstå og håndtere cyber- og informationssikkerhedshændelser. Her er overordnet tale om indsatser, som skal styrke sektorens evne til at identificere, beskytte, detektere, respondere og genoprette som følge af cybersikkerhedshændelser.

På baggrund af CFCS' vurdering af cybertruslen mod transportsektoren og i dialog med aktørerne i transportsektoren, herunder om de risiko- og sårbarhedsvurderinger aktørerne har bidraget med i forhold til relevante trusselsscenarier, er der på Transportministeriets område identificeret fire strategiske indsatsområder. Formålet er at videreudvikle og styrke indsatsen for cybersikkerhed i transportsektoren under strategien.

Udmøntning af strategiens initiativer vil blive fastlagt af Transportministeriet og DCIS-TRP i årlige handlingsplaner, som etablerer arbejdsprogram og fremdrift på initiativer under strategien.

3.1 Indsatsområde I – Risikostyring

Målsætning

Strategien skal styrke bevidstheden om og styringen af risici på cybersikkerhedsområdet i transportsektoren. Risikostyringen i sektorvirksomhederne skal bidrage til at etablere ledelsesforankret risikostyring som et kerneredskab til at styrke sektorens robusthed over for cyberangreb.

Baggrund

Risikostyring er udtryk for den samlede proces, hvormed kontekst for risici etableres, risici vurderes, håndteres og accepteres[4].

Processen er central for myndigheder og virksomheder, når de forsøger at danne sig overblik over organisationens risici og prioritere ressourcer til indsatsen for at styrke cyber- og informationssikkerheden.

Strategiens indsatsområde for risikostyring af cyber- og informationssikkerhed skal understøtte transportaktørerne i forhold til at forstå, identificere og forebygge fremtrædende cybertrusler og risici mod passagersikkerhed og mobilitet.

[4] Baseret på ISO27005, risikostyringsprocessen

Formålet med risikostyringen er, at organisationen - også i topledelsen – er bevidst om, hvad der kan gå galt og planlægger for at undgå kompromittering af sikkerhed, mobilitet og/eller omfattende økonomiske konsekvenser.

Langt de fleste organisationer i transportsektoren er vant til at arbejde indgående med risikostyring af virksomhedens kerneaktiviteter. Risici på cyber- og informationsikkerhedsområdet er imidlertid anderledes fra de traditionelle risici og er derfor mere ukendt territorium for nogle. Hvorimod årtiers sikkerhedsarbejde har resulteret i udbredt erfaring og tæt samarbejde med myndighederne om andre typer af risici, er risici og trusler forbundet med cyber- og informationssikkerhed både en ny type trussel og en omskiftelig trussel.

Digitalisering er et grundvilkår også i transportsektoren, hvor teknologi skaber nye muligheder for at styrke fremkommelighed, reducere miljøbelastning mv. De risici, der er forbundet med øget brug af digitale løsninger, kan i nogle tilfælde være nye for virksomheder og myndigheder, og andre steder er risici velkendte, men indebærer nye afhængigheder for eksempel af eksterne leverandører i forhold til tjenesterne.

For at opfylde strategiens målsætning for risikostyringen gennemføres strategiske indsatser, som bidrager til viden om risici og trusler, samt hvordan risikostyringen forankres i virksomhedernes topledelser.

Strategiske indsatser

- **Cyber-ROS (IT-risikovurderingsværktøj).** DCIS-TRP og sektorvirksomhederne fortsætter samarbejdet med at udvikle et sektorfælles risikobillede for transportsektoren.

- Som forberedelse til Cyber-ROS gennemfører DCIS-TRP **oplæg om optakten til "den gode risikovurderingsproces".**

- **Indberetning af cyberhændelser**. Sektoren vil i fællesskab arbejde for øgede antal af indberetninger af hændelser via www.virk.dk, som kan kvalificere risikostyringen i sektoren. Dette skal blandt andet ske ved hjælp af øget vejledning fra DCIS-TRP og andre myndigheder om, hvordan og hvornår indberetninger skal foretages.

- DCIS-TRP koordinerer sektorvirksomhedernes **anvendelse af tværsektoriel MISP** (Malware Information Sharing Platform).

- DCIS-TRP gennemfører i dialoggrupperne en øget **vejledningsindsats i forhold til risikostyring af cyber- og informationssikkerhed.**

3.2 Indsatsområde II - Robust cyberberedskab i den danske transportsektor

Målsætning

Strategien skal understøtte et robust cyberforsvar på tværs af transportsektoren.

Der skal være klare rammer for håndtering og koordination i tilfælde af hændelser og forberedelse af aktørerne i transportsektoren til at håndtere hændelser effektivt og med færrest mulige konsekvenser for egen drift og økonomiske forhold.

Baggrund

For transportsektorens aktører er det en kernekompetence at opretholde mobilitet gennem stabil drift og høj sikkerhed. Det indebærer effektiv håndtering af hændelser, så konsekvenser for borgere, erhvervsliv og samfund minimeres.

En cyberhændelse, der rammer en eller flere aktører i transportsektoren, kan potentielt få store konsekvenser for mobiliteten i samfundet. En hændelse kan både have negative konsekvenser for den ramte aktør og forstyrre brugerne af aktørens mobilitetstjeneste. En hændelse kan desuden afføde store gener og have følgevirkninger for andre virksomheder og sektorer i samfundet.

Det styrende beredskabsprincip i transportsektoren er aktørprincippet, som indebærer, at den aktør, der er ansvarlig for en mobilitetsydelse i dagligdagen, også er ansvarlig for at håndtere en hændelse i forhold til cyber- og informationssikkerhed. Med andre ord er ansvaret for at forebygge og konkret håndtere en cyberhændelse i første omgang under den enkelte aktørs ansvar. Strategien tager afsæt i dette princip med fokus på at understøtte robust beredskab også i cybersammenhæng og sikre tværgående koordination.

Det indebærer klare rollefordelinger mellem aktører og myndigheder; altså, at alle ved, hvem der gør hvad og hvornår. Den enkelte aktør har det primære ansvar for sikring af egne systemer og tjenester, men der er mulighed for at opnå bistand fra andre aktører og myndigheder alt efter en hændelses omfang.

Et robust cyberforsvar forudsætter også, at sektoren er velforberedt og har gennemarbejdede IT-beredskabsplaner på plads, så de er forberedte i tilfælde af hændelser. Dette indebærer, at beredskabet testes, så både medarbejdere og ledelse er forberedt på deres roller og ansvar.

I takt med, at transportsektorens digitale forretningsunderstøttelse vokser og trusselsbilledet mod den digitale infrastruktur udvikler sig, vil transportsektorens aktørers efterspørgsel på koordination, videndeling, træning og assistance også ændre sig. Disse behov vil blive adresseret i strategiens indsatser for dette

område, der skal styrke overblik over ansvars- og rollefordeling med det formål at styrke det tværgående cyberberedskab.

Strategiske indsatser

- Udvikling og styrkelse af transportvirksomhedernes **beredskabsplaner** skal understøttes, således at transportvirksomhederne systematisk planlægger for håndtering af cybersikkerhedshændelser.

- DCIS-TRP faciliterer en tværgående indsats i sektoren, som sikrer kendskab til **ansvarsfordeling i cyberberedskabet,** herunder overblik over hvilke myndigheder og organisationer der kan bistå i tilfælde af hændelser.

- Transportaktørernes kompetencer til at håndtere uforudsete cybersikkerhedshændelser skal styrkes og vedligeholdes ved afholdelse af **en årlig cyberøvelse** i transportsektoren. DCIS-TRP vil planlægge den nærmere gennemførelse i samarbejde med sektoren.

- Styrkelse af sektorens **viden om reetablering** efter en cybersikkerhedshændelse med henblik på, at transportaktørerne kan implementere foranstaltninger til en hurtig, sikker og effektiv reetablering efter en hændelse.

- Det afklares i regi af sektorkredsen, om der er interesse og forudsætninger for at oprette **et operationelt cybersikkerhedsberedskabsteam eller -operationscenter**[5] for transportområdet, der kan bistå transportvirksomheder med detektion, beskyttelse og håndtering af cyberangreb, threat intelligence og rådgivning om cybersikkerhed.

3.3 Indsatsområde III - NIS2

Målsætning

Strategien understøtter forberedelse og implementering af det reviderede direktiv fra EU om net- og informationssikkerhed (NIS2) for såvel myndigheder som virksomheder i transportsektoren.

Baggrund

I 2016 blev det første direktiv fra EU om sikkerhed i net- og informationssystemer (NIS1) vedtaget. I den danske transportsektor blev fire aktører[6] udpeget til

[5] For eksempel Computer Emergency Response Team (CERT) eller Security Operations Center (SOC).

[6] Københavns lufthavn (CPH), Naviair, DSB og Banedanmark.

at følge direktivets krav om akkrediteret certificering efter en anerkendt cyberstandard. De fire aktører er i dag certificeret i medfør af ISO27001.

I december 2020 fremsatte Europa-Kommissionen forslag til revision af NIS-direktivet (NIS2), som blandt andet indebærer en udvidelse af den aktørkreds, som er omfattet af direktivet, og kravene til cyberforanstaltninger der skal efterleves. Dertil kommer krav om øget myndighedstilsyn.

Formålet med at revidere NIS-direktivet er at styrke cybersikkerheden og modstandsdygtigheden yderligere på en ensartet måde på tværs af medlemsstaterne både i bredden (antal aktører) og i dybden (antal krav).

På transportområdet betyder NIS2, at betydeligt flere aktører skal efterleve lovgivningskrav om cybersikkerhed. I takt med at implementeringen af direktivet i transportsektoren fastlægges over de kommende år, vil der parallelt være behov for at forberede og styrke aktørerne i sektoren til at håndtere cybersikkerhed. Strategien vil understøtte det lovgivningsmæssige arbejde ved at sætte fokus på dialog på tværs af sektoren og via centrale indsatser understøtte sektorens parathed til NIS2. Det skal være nemt at forstå for aktørerne i transportsektoren, hvem der er omfattet NIS2, og hvilke forventninger der er til efterlevelse af direktivets krav. Det kræver tydelig kommunikation og dialog mellem virksomheder og myndigheder.

I forbindelse med den første cyberstrategi for transportområdet (2019-2021) blev der etableret samarbejdsfora om cybersikkerhed på transportområdet mellem myndigheder og aktører i sektoren – de såkaldte virksomhedsfora. Som et led i den nye cyberstrategi vil samarbejdsformen blive udvidet til at omfatte transportvirksomheder, der ikke tidligere har været omfattet af NIS, således at disse aktører kan deltage i dialogfora og dermed få adgang til viden, erfaring og *best practice*. Det gælder blandt andet havnesektoren, som ikke hidtil har været inddraget i det tværgående arbejde om cybersikkerhed på transportområdet.

Strategiske indsatser

- Inklusion af de nye aktører, der bliver omfattet af NIS2, i transportsektorens virksomhedsfora. Transportmyndighederne skal facilitere denne **dialog og sparring** og afsøge interesse og forudsætninger for deltagelse i virksomhedsfora.

- DCIS-TRP skal understøtte, at aktører, der omfattes af NIS2, opnår **styrket viden og kompetencer** til at implementere direktivets krav – herunder om relevante internationale standarder til informationssikkerhed.

- DCIS-TRP vil **facilitere samarbejde med andre sektorer og EU-medlemslande** om *best practice* for implementering og efterlevelse af NIS-direktivet.

3.4 Indsatsområde IV - Uddannelse og awareness

Målsætning

Transportsektoren skal have adgang til de nødvendige kompetencer og kendskab til den nyeste viden for at kunne modstå cybertruslen i sektoren.

Baggrund

Cybersikkerhed er mere end risikovurderinger og tekniske foranstaltninger. Det er velkendt, at størstedelen af alle hackerangreb og brud på informationssikkerheden skyldes menneskelige fejl. Mangel på kompetencer og ressourcer udgør desuden en sårbarhed for it-sikkerheden i det private såvel som det offentlige Danmark.

Den udfordring er lige så presserende i transportsektoren som i øvrige kritiske sektorer, og derfor er det også en problemstilling, som cyberstrategien forholder sig til.

Grundlæggende betyder det, at samfundskritiske transportydelser i Danmark, både på myndighedsniveau såvel som for virksomheder, efterspørger ressourcer og viden, som kan være med til at forebygge alvorlige cybersikkerhedshændelser i sektoren.

Udfordringen skal også ses i lyset af kommende regulering i sektoren, som stiller yderligere krav til uddannelse og kompetencer med blandt andet øget styring af cyber- og informationssikkerhed.

Formålet med strategiens indsatser på området er i høj grad at afklare, om der meningsfuldt kan iværksættes indsatser fra centralt hold for at understøtte virksomhedernes behov og understøtte dialog på tværs af sektoren om håndtering af problemstillingen.

Strategiske indsatser

- DCIS-TRP udarbejder i samarbejde med sektoren **et overblik over kritisk personale**, for hvem cybersikkerhedsuddannelse er relevant, og hvilke eksisterende uddannelsesmuligheder der er til rådighed. Overblikket skal supplere sektorens arbejde og ansvarsforpligtelse med at sikre de nødvendige kompetencer og kaste lys over eventuelle afsavn i forhold til uddannelse i cybersikkerhed for safety- og securitykritisk personale.

- DCIS-TRP afdækker behovet og muligheden for fælles indsats mellem DCIS-TRP og sektorvirksomheder til **promovering af transportsektorens arbejde med cyber på uddannelsesinstitutionerne** med henblik på tiltrækning af arbejdskraft.

- DCIS-TRP faciliterer **videndeling og oplæg/gå-hjem-møder om uddannelse, rekruttering og awareness i dialoggrupperne** med egne og/eller eksterne fageksperter inden for cyber- og informationssikkerhedsområdet

Transportministeriet
Frederiksholms Kanal 27F
1220 København K

Telefon 41 71 27 00
trm@trm.dk
www.trm.dk