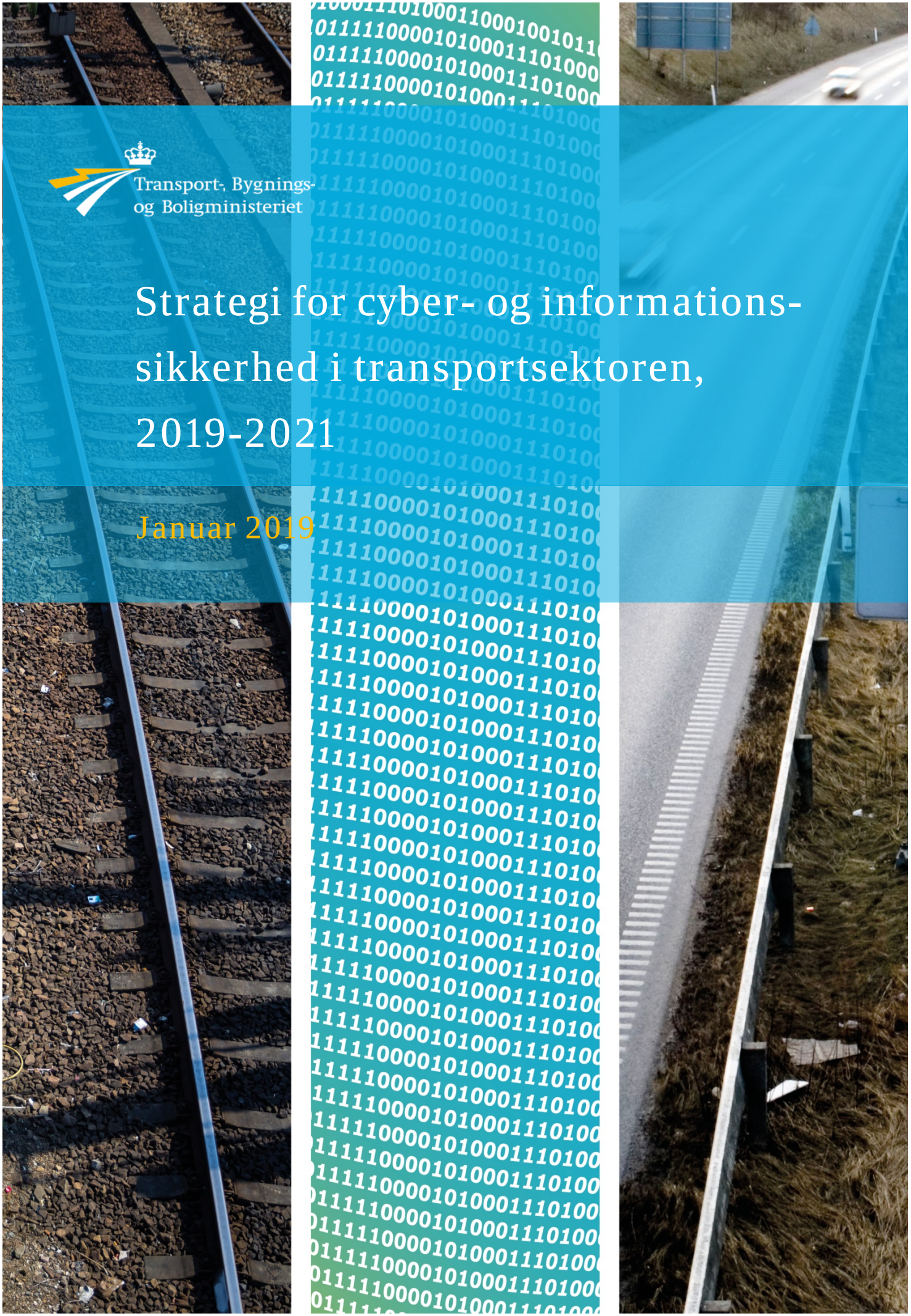


Transport-, Bygnings- og Boligministeriet

Strategi for cyber- og informationssikkerhed i transportsektoren, 2019-2021

Januar 2019

Strategi for cyber- og informationssikkerhed i transportsektoren, 2019-2021

Strategi for cyber- og informationssikkerhed i transportsektoren, 2019-2021

Udgivet af: Transport-, Bygnings- og Boligministeriet
Frederiksholms Kanal 27F
1220 København K

Udarbejdet af: Trafik-, Bygge- og Boligstyrelsen
ISBN netudgave: 978-87-93292-43-7
Forsideill.: Transport-, Bygnings- og Boligministeriet på baggrund af fotos af Ulrik Jantzen
Fotos i strategien: Ulrik Jantzen
side 41: René Strandbygaard

Indhold

Forord 7

1. Principper og retningslinjer for strategien 9
    1.1. Sammenhæng mellem national strategi og sektorstrategi 10
    1.2. Hvad forholder sektorstrategien sig til? 10
    1.3. God sikkerhedskultur skal overføres til cyber-området 11
    1.4. Øget afhængighed af digitale løsninger udfordrer sektoren 11
    1.5. Trusselsbilledet og transportsektorens sårbarheder 13
    1.6. Initiativer definerer det videre arbejde 15
    1.7. Sektorstrategiens løbende udvikling 16
    1.8. Afgrænsning 16
    1.9. Principper for sektorstrategien 17

2. Indstationering i CfCS 19
    2.1. Indledning 20
    2.2. CfCS og Trusselsvurderingsenheden 20
    2.3. Sektorspecifikke trusselsvurderinger 20
    2.4. Indstationering skal øge sårbarhedserkendelsen 20
    2.5. Ansættelse og kvalifikationskrav 21
    2.6. Arbejdsopgaver i CfCS og samarbejde med Trafik-, Bygge- og Boligstyrelsen 21

3. Etablering af DCIS 23
    3.1. Indledning 24
    3.2. Sådan arbejder sektorens DCIS 24
    3.3. Arbejde med transportsektorens strategi 25
    3.4. Internationale opgaver 25
    3.5. NIS-direktivet 25
    3.6. Samarbejde med CfCS 26
    3.7. Sparring med andre kritiske sektorer 26

4. Transportsektorens initiativer 29
    1. Overblik og selvindsigt 31
    2. Sårbarhedserkendelse og håndtering 34
    3. Internationalt arbejde og regulering 38

5. Afrunding 41

6. Referencer 43

Forord

Digitaliseringen har mange positive effekter for borgere, virksomheder og myndigheder. Smartphones, e-kommunikation, GPS, apps, cloud-løsninger og trådløs kommunikation er bare nogle af de grundlæggende teknologier og produkter, som gør livet lettere for os alle.

Den øgede digitalisering i hele samfundet er gået stærkt, men ikke alt som digitaliseringen har ført med sig er godt nyt. Det er gået op for mange, at digitaliseringen også fører problemer med sig, som man hverken havde fantasi eller evne til at forstå for bare få år siden.

Sager om privatlivskrænkelser, datatyveri, spionage, svindel og hacking pibler frem og er et problem for borgere, virksomheder, regeringer og organisationer.

For transportsektoren går udviklingen med en stigende afhængighed af digitale løsninger hånd i hånd med nye udfordringer, som sektoren skal tage alvorligt for at sikre en sikker trafikafvikling og høj mobilitet.

Anvendelsen og afhængigheden af digitale løsninger i transportsektoren er forskellig for luftfarten, jernbanen, vejområdet og den maritime sikring. Luftfartsbranchen er længst fremme i anvendelsen af digitale løsninger og anvendes b.la. i billetsalget, informationstavler, bagagehåndtering, vejrobservation, navigation og kommunikationssystemer.

Digitaliseringen på jernbanen er også fremskreden og med implementeringen af Signalprogrammet i de kommende år bliver afviklingen af togtrafikken digitaliseret.

For vejområdet er digitaliseringen endnu i sin spæde begyndelse med brug af f.eks. ITS-tavler[1], men udviklingen går i samme retning som i de andre brancher; digitaliseringen er på vej ind i bilerne og ud i selve infrastrukturen, hvor fremtiden byder på selvkørende teknologi.

Alle disse systemer bidrager til en mere effektiv trafikafvikling og et bedre passagerflow, men åbner også muligheden for ondsindede aktører til i værste fald at kompromittere personsikkerheden, men også forstyrre mobiliteten og dermed fremkommeligheden i Danmark.

Den foreliggende delstrategi beskriver dels det setup som sektoren arbejder efter med cybersikkerhed, dels de initiativer der vil gennemføres i strategiens periode med henblik på at bistå sektorens aktører i arbejdet med at sikre personsikkerhed og høj mobilitet i de kommende år.

Dette er første gang der udarbejdes en strategi for cyber- og informationssikkerhed for transportsektoren, og både setup og initiativer er derfor i sin spæde start. Begge dele forventes derfor at udvikle sig i takt med øget viden og bemanding på området.

[1] Elektroniske trafiktavler, f.eks. elektroniske hastigheds- og informationstavler

1. Principper og retningslinjer for strategien

1.1. Sammenhæng mellem national strategi og sektorstrategi

Regeringen offentliggjorde den 15. maj 2018 den Nationale Strategi for Cyber- og Informationssikkerhed ("strategien"). Strategien indeholder 24 initiativer, der skal medvirke til at øge den tekniske robusthed i den digitale infrastruktur, øge viden og kompetencer hos borgere, virksomheder og myndigheder og styrke den nationale koordinering og samarbejde.

Strategien tager afsæt i sektoransvarsprincippet, som indebærer, at den myndighed, der har ansvaret for en funktion i det daglige, også har ansvaret, når der sker en alvorlig hændelse.

I forlængelse heraf peges der i strategien på seks kritiske sektorer, herunder transportsektoren, der skal udarbejde en sektorspecifik cyber- og informationssikkerhedsstrategi ("sektorstrategien") inden udgangen af 2018. Sektorstrategien skal målrette indsatserne på området inden for den pågældende sektor i perioden 2019-2021.

Sektorstrategien tager afsæt i en risiko- og sårbarhedsanalyse, som belyser og overordnet vurderer de udfordringer inden for cyber- og informationssikkerhed, som transportsektoren står overfor. Analysen er udarbejdet af en ekstern it-sikkerhedsvirksomhed[2] for Transport-, Bygnings og Boligministeriet. Analysen belyser it- og dataunderstøttelsen af branchens kritiske funktioner, disses overordnede sårbarheder, og sikringstiltag som branchen allerede arbejder med. Analysen munder ud i anbefalinger, for hvad branchen og myndigheder fremover kan arbejde med for at imødegå identificerede sårbarheder.

Transport-, Bygnings og Boligministeriet har placeret opgaven med at udarbejde og implementere sektorstrategien i Trafik-, Bygge- og Boligstyrelsen (herefter TBST).

Formålet med sektorstrategien er grundlæggende at understøtte ministeriets overordnede mål, om at sikre en effektiv transportsektor med sikker trafikafvikling og høj mobilitet.

1.2. Hvad forholder sektorstrategien sig til?

Sektorstrategien tager afsæt i de rammer, som udstikkes i Regeringens nationale strategi og som led i varetagelsen af sektoransvaret i Beredskabsloven. Sektorstrategien skal således skabe overblik over de udfordringer, som transportsektoren står overfor som følge af den øgede digitalisering i sektoren.

Dermed vil strategien udgøre det grundlag, som sektorens arbejde prioriteres efter de kommende år.

[2] Dubex A/S

Sektorstrategien for transportsektoren skal dække hele ministeriets ressort, dvs. vejområdet, jernbaneområdet, luftfartsområdet og havneområdet ift. maritim sikring.

1.3. God sikkerhedskultur skal overføres til cyber-området

Transportsektoren har historisk set været vant til at arbejde med sikkerhed.

Sektoren har således en lang kultur for at arbejde med safety, dvs. sikkerhed fsva. utilsigtede hændelser, og security, forstået som forebyggelse og håndtering af tilsigtede hændelser.

Den øgede digitalisering og afhængighed af digitale løsninger vil fremover betyde større sammenfald mellem security og safety[3]. For hele sektoren gælder dertil at selvkørende teknologi og automatisering bliver et grundvilkår for fremtiden.

Samlet set betyder det, at både operatører og myndighed skal blive bedre til at samtænke områderne og betragte cyber- og informationssikkerhed som en udfordring, der går på tværs.

1.4. Øget afhængighed af digitale løsninger udfordrer sektoren

Digitale løsninger holder i mange tilfælde nøglen til at løse mange af nutidens største udfordringer på transportområdet, herunder trængsel, miljøbelastning, sikkerhed og rejsetid.

Effektive digitale løsninger får os således hurtigt igennem sikkerhedskontrollen i lufthavnen, ekspederer vores bagage og tilbyder os underholdning på lange flyture. På mange måder sørger de digitale løsninger også for øget sikkerhed i flyene og omkring flyene. Piloter styrer i dag flyene gennem computere, og langt de fleste informationer, der tilgår en pilot i cockpittet, er blevet bearbejdet af en computer.

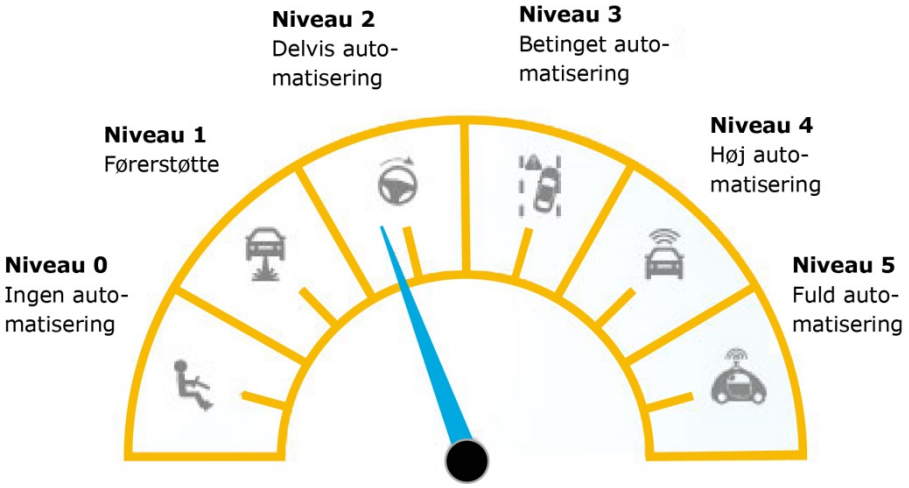
For jernbaneområdet bidrager digitale løsninger også til en mere effektiv trafikafvikling og bedre trafikinformation. Med Signalprogrammet er forventningen, at der kommer flere tog til tiden, kortere rejsetider og øget kapacitet (flere tog) på jernbanen.

På de danske veje er de digitale løsninger også med til bl.a. at lette trafikafviklingen gennem højere kapacitet (bedre vejudnyttelse) og bidrage til højere sikkerhed for bilister. Informationssystemer, varslingssystemer og variable hastighedstavler giver således realtidsinformation om trafikken og farer forude til bilister, som kan reagere tidsnok derefter.

[3] Dubex (2018), s. 12

I de kommende år vil udviklingen på vejområdet også gå stærkt. Særligt udviklingen inden for såkaldte intelligente veje og connected cars (biler forbundet gennem internetforbindelse med omgivelser og andre biler samt infrastruktur) forventes at gå stærkt, hvor gradvist mere selvkørende biler i højere grad skal kunne "tale sammen" med infrastrukturen i form af veje, skilte og anden trafik. "Society of Automotive Engineers" anvender en sekstrins-skala til at vurdere bilernes niveau af automatisering, og efter denne skala kører der i dag biler på vejene på niveau 2 (figur 1).

Figur 1.1 | Automatiseringsniveau, fra Vejdirektoratet.dk



Den udvikling stiller også store krav til cyber- og informationssikkerhed i sektoren.

Digitaliseringen i transportsektoren er ikke gået lige så stærkt som i visse andre sektorer. Sektoren har således i mange år været kendetegnet ved store og langsigtede investeringer i materiel, som kun med mange års mellemrum er blevet enten udskiftet eller ændret.

Over tid har digitale løsninger enten erstattet eller blevet indført som løsninger ovenpå eksisterende anlæg eller materiel. Dermed er afhængigheden af de digitale løsninger på tværs af sektoren langsomt, men sikkert steget de seneste mange år.

Den snigende digitalisering har blandt andet udfordret sektorens arbejde med risikovurderinger, som typisk er foretaget med udgangspunkt i ikke-digitale systemer. Dermed risikerer man, at de dynamiske trusler ift. cybersikkerhed ikke er inddraget[4].

[4] Dubex (2018), s. 39

1.5. Trusselsbilledet og transportsektorens sårbarheder

1.5.1. *Trusler*

CfCS' vurderer at den største trussel mod Danmark udgøres af truslen fra cyberspionage udført af stater samt cyberkriminalitet[5]. Truslerne vurderes således til meget høj, mens truslerne fra cyberaktivisme og cyberterror vurderes til hhv. middel og lav.

Cyberspionage vurderes af CfCS til at være et "grundvilkår" for danske myndigheder og virksomheder og betragtes således som en vedvarende trussel. For virksomheder udgør den stigende brug af outsourcing af it-drift også en trussel, og CfCS vurderer at det kan øge sårbarheden i og med at leverandører kan have adgang til følsomme data og centrale styringssystemer[6].

I samme stil betegnes cyberkriminalitet som et globalt fænomen, der også kan ramme danske myndigheder og virksomheder. Formålet med kriminaliteten er typisk berigelse i form af penge, finansielle og/eller personlige oplysninger, bedrageri og afpresning[7].

I den sammenhæng er det særligt værd at bemærke, hvordan CfCS observerer at der findes *"et økosystem af udviklere, brugere og udbydere af cyberkriminelle tjenester og værktøjer"*[8]. Kort sagt er cyberkriminelle aktører dygtige til at dele viden om metoder og samarbejder i det hele taget, når det kan fremme kriminaliteten.

Det og meget andet er årsagen til, at cybertruslen er dynamisk; når nye sårbarheder i virksomheder og myndigheder viser sig, deles den viden og metoderne til at udnytte det lynhurtigt mellem kriminelle aktører.

Center for Cybersikkerhed har d. 11. december 2018 offentliggjort en trusselsvurdering for transportsektoren. Trusselsvurderingen er udarbejdet på baggrund af CfCS' generelle viden om cybertrusler og tidligere eksempler på cyberangreb mod transportsektoren i Danmark og i udlandet.

Denne første vurdering for transportsektoren er således udarbejdet uden bistand fra en indstationeret medarbejder fra transportsektoren, hvorfor det også forventes at fremtidige trusselsvurderinger forholder sig mere specifikt til bl.a. sektortrends som det ses i andre trusselsvurderinger for kritiske sektorer.

CfCS' trusselsvurdering viser grundlæggende, at der er anseelige trusler mod den danske transportsektor. Grundlæggende ligger trusselsniveauet i transportsektoren dermed for nuværende på samme leje som i de andre kritiske

---

[5] CfCS 1 (2018), s. 1
[6] CfCS 1 (2018), s. 3
[7] CfCS 1 (2018), s. 6
[8] CfCS 1 (2018), s. 6

samfundssektorer, hvor truslen fra cyberspionage og cyberkriminalitet typisk svinger mellem høj og meget høj, ifølge CfCS' vurderinger.

Således vurderer CfCS truslen fra cyberkriminalitet mod sektoren for meget høj[9], mens truslen fra cyberspionage vurderes til høj. Cyberkriminalitet dækker over truslen om at afpresse penge fra virksomheder eller myndigheder, mens cyberspionage dækker over intentionen om tyveri af værdifulde informationer og teknologier.

Truslen fra cyberkriminalitet omfatter særligt forsøg på at afpresse virksomheder og myndigheder, f.eks. gennem ransomware-angreb eller DDoS-angreb. Grundlæggende er metoderne en slags gidselstagning med økonomisk vinding for øje. Tyveriet kan svække kundernes tillid til den pågældende virksomhed eller myndighed eller få betydelige økonomiske konsekvenser.

CfCS vurderer i den sammenhæng, at flere kriminelle hackergrupper verden over systematisk forsøger at hacke betalingssystemer på tværs af sektorer.

Truslen for cyberspionage mod Danmark vurderes af CfCS generelt som meget høj, mens det specifikt for transportsektoren vurderes til høj. Dette skyldes at CfCS ikke har kendskab til samme høje aktivitetsniveau mod sektoren, som der ellers generelt ses.

CfCS identificerer en række årsager til, at potentielle angribere ønsker at spionere på virksomheder og myndigheder i transportsektoren, herunder tyveri af nye teknologier, sikkerhedspolitiske interesser, økonomiske interesser samt personhenførbare oplysninger. CfCS vurderer også, at danske transportvirksomheder, der løser opgaver for dansk forsvar eller andre landes militær kan have fremmedes staters interesse.

Truslerne fra cyberaktivisme og cyberterror vurderes af CfCS som hhv. middel og lav.

1.5.2. *Sårbarheder*

Transport-, Bygnings- og Boligministeriet igangsatte i forsommeren 2018 en risiko- og sårbarhedsanalyse ved konsulentvirksomheden Dubex. Analysen giver en overordnet introduktion til sektorens styrker og sårbarheder fsva. cyber- og informationssikkerhed.

Dubex' rapport kommer med en række observationer omkring sårbarheder på tværs af sektoren, som overordnet kan deles ind i følgende kategorier[10]:

- Organisering af IT-sikkerhedsområdet (ledelsesforankring, sikkerhedskultur, risikovurdering, sårbarhedserkendelse og processer)
- Arkitektur og teknologi (opbygning af it-løsninger, anvendelse og underleverandører)

---

[9] CfCS 2 (2018), s. 1

[10] Dubex (2018), s. 28

- Overvågning (evner til at konstatere brud på sikkerhed)
- Beredskab (evner til at reagere på hændelser)

Observationerne for transportsektoren er et vigtigt pejlemærke for sektorens prioritering af initiativer og bidrager hertil. Dubex' observationer omhandler risikostyring, sårbarhedserkendelse, regulering og standarder, ressourcer, arkitektur og teknologi, SRO/ICS/OT-systemer, standardteknologier, kommunikation, outsourcing og brug af underleverandører, overvågning og beredskab[11].

Observationerne er gjort på tværs af transportsektoren og kan således ikke tillægges at tilhøre enkelte aktører. En del af myndighedsarbejdet fremadrettet består derfor i at blive klogere på hvilke observationer der gør sig gældende for hvem, og derefter bidrage til at sætte ind.

Helt grundlæggende vurderer Dubex, at transportsektoren har en god sikkerhedskultur som bl.a. udspringer af en tradition for at arbejde risikobaseret fsva. håndtering af sårbarheder omkring personsikkerhed[12]. Dubex observerer imidlertid en stor spredning i transportaktørernes modenhed omkring risikostyring og ledelsesforankring, hvor de aktører som har arbejdet med standarder har en højere modenhed[13].

Udgangspunktet for de initiativer på området, som i de kommende år vil blive igangsat i sektoren er derfor Dubex' risiko- og sårbarhedsanalyse, som blev færdiggjort i september 2018, den generelle trusselsvurdering, som CfCS har udarbejdet samt samarbejdet med sektorens aktører i sektorens nedsatte dialoggrupper.

Dermed står arbejdet med cyber- og informationssikkerhed i transportsektoren overordnet set på tre ben; de styrker og sårbarheder, som Dubex har identificeret i sektoren, det kontinuerlige trusselsbillede fra CfCS samt sektorens samarbejde om initiativer på området.

1.6. Initiativer definerer det videre arbejde

Som del af Regeringens nationale strategi, skal transportsektoren oprette en decentral cyber- og informationssikkerhedsenheder (herefter DCIS). DCIS er således en sektorforankret enhed, som beskæftiger sig med cyber- og informationssikkerhed.

Sektorstrategien skal omhandle DCIS' arbejde med at vurdere behovet for nye initiativer på cyber- og informationssikkerhedsområdet.

Initiativerne udarbejdes bl.a. i samarbejde med centrale transportaktører, for at sikre at disse svarer til branchens aktuelle modenhed og behov, og dermed styrker cyber- og informationssikkerheden i transportsektoren.

---

[11] Dubex (2018), s. 28-38

[12] Dubex (2018), s. 28

[13] Dubex (2018), s. 29

Der er derfor etableret hhv. et dialogforum for cybersikkerhed i luftfarten og et for jernbanen. Øvrige aktører i transportbranchen involveres på ad hoc basis.

1.7. Sektorstrategiens løbende udvikling

Cyber- og informationssikkerhed er et område i hastig udvikling. Transportbranchen er generelt præget af øget digitalisering og automatisering på flere centrale områder, som overordnet bidrager til en mere effektiv og moderne sektor med højere kapacitet.

Med udviklingen ændrer trusselsbilledet sig løbende, idet metoder og værktøjer til at udføre cyberrelaterede angreb hurtigt skifter karakter.

Udviklingen medfører også øget opmærksomhed fra internationale fagorganisationer, som søger at styrke indsatsen regionalt eller globalt ved at etablere ensartede standarder og lovgivning i relation til cybertrusler.

Sektorstrategien dækker de initiativer, som det er hensigten at arbejde med i perioden 2019 til 2021. Der vil i perioden foregå en kontinuerlig dialog med branchens aktører ift. kvalificering og udførsel af initiativer samt opbygningen af sektorens DCIS i takt med øget viden på området.

I overensstemmelse med branchens digitale udvikling, det omskiftelige trusselsbillede og udviklingen af international regulering vil der løbende i strategiens levetid blive taget stilling til, hvorvidt der er behov for at justere strategiens initiativer samt udførslen heraf.

1.8. Afgrænsning

Nærværende strategi har fokus på konkrete tiltag ift. transportsektoren. Dermed vil der som udgangspunkt ikke være tiltag ift. sektorens afhængighed af cybersikkerhed i andre sektorer. Eventuelle nedbrud som følge af cyberangreb i andre sektorer håndteres alene i henhold til de konsekvenser, som dette måtte generere for transportaktørerne, og ikke i henhold til grundårsagen.

Cybersikkerhed i andre sektorer kan dog være relevant såfremt, at der er tekniske snitflader mellem systemer i andre sektorer og transportaktørernes egne drifts- eller sikkerhedssystemer.

TBST indgår i det generelle arbejde med cybersikkerhed i dialog med andre myndigheder, hvoraf transportbranchen har særlige afhængigheder, med henblik på at sikre en god og gensidig dialog om afhængighederne.

1.9. Principper for sektorstrategien

Som tidligere beskrevet er området cyber- og informationssikkerhed en meget dynamisk størrelse, og truslerne udvikler sig i et hastigt tempo.

Dermed adskiller området sig væsentligt fra traditionel tænkning inden for transportsektoren og stiller nye krav til myndighedernes varetagelse af opgaverne.

For at skabe sammenhæng i indsatsen, bygger strategien på seks overordnede principper:

- ***Passagersikkerhed og mobilitet**:* Strategiens fokus er at sikre mobilitet, forstået som opretholdelse af samfundskritiske transportfunktioner, og på at sikre systemer, som er kritiske for passagernes sikkerhed, både i relation til security og til safety.
  Mobilitetsmålet afgrænser sig til de mest centrale aktører, herunder infrastrukturforvaltere indenfor de forskellige transportformer, hvor imens målet om passagersikkerhed har betydning for samtlige transportaktører.
  Strategien omfatter som udgangspunkt ikke forretningsrelaterede eller økonomiske mål, som gælder for de enkelte aktører.

- ***Gennemsigtighed**:* Initiativerne i delstrategien skal være operationelle for branchen og svare til aktørernes behov. Det er derved en forudsætning, at branchen inddrages i udarbejdelsen af sektorstrategien og de konkrete initiativer. Arbejdet med strategien skal være præget af gennemsigtighed og have en høj grad af brancheinddragelse.

- ***Aktøransvar**:* Strategien tager udgangspunkt i, at den enkelte aktør, der er ansvarlig for en opgave i dagligdagen, også er ansvarlig for at planlægge videreførelsen af denne i tilfælde af en hændelse ift. cyber- og informationssikkerhed. Den sektorspecifikke strategi skal således fastholde den nuværende rolle- og ansvarsfordeling mellem myndighed og aktør.

- ***Ensartet tilgang til hændelser og krisestyring**:* Hændelser i relation til cyber- og informationssikkerhed skal som udgangspunkt håndteres efter samme procedurer og kommandoveje, som andre beredskabshændelser. Strategien skal således sikre, at håndteringen følger den vedtagne struktur for hændelsesrapportering og krisestyring.

- ***Risikobaseret tilgang**:* Strategien og de initiativer der igangsættes som følge af strategien skal ske på baggrund en risikobaseret tilgang. Dvs. på baggrund af en vurdering af cyber- og informationssikkerheden, implicitte risici i branchen og en derpå følgende vurdering af, hvilke tiltag der vil være passende for at imødegå de identificerede risici. Strategien skal endvidere have fokus på, at eventuelle sikringstiltag bliver udarbejdede på en dynamisk og overordnet måde, således at reguleringen kan følge med i udvikling af både teknik og trusselsbillede.

- ***International ramme:*** Styrelsen vil søge at påvirke internationale initiativer i relation til cyber- og informationssikkerhed, således at de så vidt muligt understøtter danske behov og forudsætninger.

Styrelsen vil særligt arbejde for at undgå international detailregulering, og i stedet arbejde for at fremme rammelovgivning, der komplementeres af standarder udviklet af industrien. Strategiens initiativer kan underbygge dette arbejde.

2. Indstationering i CfCS

2.1. Indledning

Som del af initiativ 3.1 i Regeringens nationale cyber- og informationsstrategi, skal de samfundskritiske sektorer ansætte og indstationere en medarbejder i Center for Cybersikkerheds (herefter CfCS) Trusselsvurderingsenhed.

Nogle sektorer (energi, finans, tele og sundhed) har haft indstationerede medarbejdere i nogle år, mens det er en ny opgave for transportsektoren.

Dette afsnit beskriver rammerne for indstationering af medarbejderen samt de opgaver vedkommende skal varetage.

2.2. CfCS og Trusselsvurderingsenheden

CfCS er placeret i Forsvarets Efterretningstjeneste (herefter FE). CfCS består overordnet set af tre afdelinger; rådgivnings- og teleafdelingen, Netsikkerhedsafdelingen og Cyberanalyseafdelingen[14].

Trusselsvurderingsenheden er del af cyberanalyseafdelingen og har ansvar for at udarbejde vurderinger af cybertrusler mod de samfundsvigtige sektorer i Danmark, herunder transportsektoren. Enheden analyserer og opdaterer trusselsbilledet for danske myndigheder og virksomheder.

Enhedens primære funktion er at lave trusselsvurderinger, generelle såvel sektorspecifikke. De sektorspecifikke trusselsvurderinger udarbejdes bl.a. ved hjælp af den indstationeredes branchespecifikke viden og netværk.

2.3. Sektorspecifikke trusselsvurderinger

Et af hovedformålene med indstationeringen er udarbejdelsen af de såkaldte sektorspecifikke trusselsvurderinger. CfCS har indtil videre udgivet sektorspecifikke trusselsvurderinger for tele-, sundhed-, finans- og energisektoren. Vurderingerne redegør for de cybertrusler, som er rettet mod den pågældende sektor.

Trusselsvurderingerne offentliggøres på CfCS' hjemmeside og indeholder således ikke klassificerede oplysninger. Trusselsvurderingerne suppleres derfor med bilateral kontakt mellem CfCS og brancheaktører vedrørende viden og information, som ikke kan fremgå af trusselsvurderingerne.

2.4. Indstationering skal øge sårbarhedserkendelsen

Transportsektoren er generelt vant til at arbejde med sikkerhed. Branchens aktører og myndighederne har gennem mange år arbejdet med en risikobaseret tilgang, der har og det har skabt en god sikkerhedskultur både hvad angår safety og security.

[14] https://fe-ddis.dk/CFCS/OMOS/Pages/Omos.aspx

Både brancheaktører og myndigheder står imidlertid over for at opbygge den samme sikkerhedskultur, når det drejer sig om cybersikkerhed. Hvor sektoren tidligere hovedsageligt har været vant til at sårbarheder og trusler er noget som kan identificeres og inddæmmes, er cybersikkerhed karakteriseret ved, at trusler og sårbarheder hele tiden udvikler og ændrer sig[15]. Ligeledes er det et område, hvor sektoren kan få et stort udbytte af at dele viden og samarbejde om opbygning af kompetencer og tiltag.

Transportsektoren er, ifølge internationale studier, endnu ikke hårdt ramt af cyberrelaterede hændelser[16]. Men den digitale udvikling inden for f.eks. lufttrafikstyringen, signalerne på jernbanen og selvkørende teknologi i biler øger både afhængigheden af de digitale løsninger og angrebsfladen for ondsindede aktører.

Indstationeringen af en medarbejder i CfCS' Trusselsvurderingsenhed er et vigtigt skridt på vejen mod at give branchen ny viden og dybere indsigt i både de egne sårbarheder og det trusselsbillede, som retter sig specifikt mod sektoren gennem den sektorspecifikke trusselsvurdering.

De sektorspecifikke trusselsvurderinger og den affødte dialog mellem Trusselsvurderingsenheden, brancheaktørerne og myndigheder vil samlet løfte arbejdet med cybersikkerhed til et højere niveau.

2.5. Ansættelse og kvalifikationskrav

Trafik-, Bygge- og Boligstyrelsen er i proces med at ansætte en medarbejder, som skal indstationeres i CfCS for en 2-årig periode. Efter endt indstationering vil medarbejderen planmæssigt indtræde i Trafik-, Bygge- og Boligstyrelsens DCIS.

Ved ansættelsen har parterne særligt lagt vægt på at finde en kandidat som kan arbejde analytisk og har viden samt erfaring fra transportsektoren samt har gode evner for at knytte faglige netværk i fornødent omfang.

2.6. Arbejdsopgaver i CfCS og samarbejde med Trafik-, Bygge- og Boligstyrelsen

Den indstationerede medarbejder bliver del af et analytisk team bestående af fast stab fra CfCS og andre indstationerede medarbejdere fra de samfundskritiske sektorer.

Enhedens hovedopgave er at udarbejde de sektorspecifikke trusselsvurderinger og i øvrigt skabe opmærksomhed og viden om cybertruslen for virksomheder og myndigheder.

[15] Dubex (2018) s. 29
[16] Dubex (2018) s. 29

Den indstationerede medarbejder skal bl.a. indsamle information om hændelser i sektoren, udarbejde trusselsvurderinger, opbygge og bevare tæt kontakt til relevante aktører i transportsektoren og lejlighedsvist deltage i partnersamarbejde og internationale samarbejdsfora.

Den indstationerede medarbejder vil også få en kontaktflade ift. transportsektorens DCIS, hvor et tæt samarbejde bliver vigtigt for korrekt og rettidig varsling af relevante brancheaktører[17].

Det er forventningen, at den indstationerede medarbejder gør CfCS's trusselsvurderingsenhed i stand til at indgå som aktiv part i det samarbejde Trafik-, Bygge- og Boligstyrelsen har med transportsektorens virksomheder, f.eks. ved deltagelse eller oplæg ved i dialogmøder og temaarrangementer eller ved bistand til kvalitetssikring af DCIS' tiltag såsom analyser eller vejledninger.

Det er aftalt mellem parterne, at der vil være løbende møder mellem Trafik-, Bygge- og Boligstyrelsens DCIS og CfCS' trusselsvurderingsenhed.

[17] "Etablering af decentrale cyber- og informationssikkerhedsenheder i Danmark", CfCS, juni 2018

3. Etablering af DCIS

3.1. Indledning

Som del af Regeringens nationale strategi, skal de samfundskritiske sektorer oprette decentrale cyber- og informationssikkerhedsenheder (DCIS).

Regeringens formål med at oprette DCIS er at styrke evnen til at håndtere cyber- og informationssikkerhed i de samfundskritiske sektorer[18].

DCIS er dermed i praksis en sektorforankret enhed, som beskæftiger sig med cyber- og informationssikkerhed. For transportsektorens vedkommende er DCIS placeret i TBST. En nærmere beskrivelse af transportsektorens DCIS og ansvarsområder følger i dette afsnit.

DCIS skal sikre en sektorkoordination med CfCS og PET, og enheden kan i øvrigt bidrage til en række opgaver, herunder:

- beredskabsøvelser
- videndeling og vejledning
- sektorspecifikke trusselsvurderinger
- sikkerhedsopbygning
- sårbarhedsvurderinger

Helt grundlæggende afhænger udformningen af DCIS dog af sektorens modenhedsniveau og ressourcer.

3.2. Sådan arbejder sektorens DCIS

Transportsektorens DCIS blev oprettet i TBST i sommeren 2018 og er bemandet med en medarbejder samt ad-hoc tilknyttede ressourcer, herunder IT- og juridisk bistand. Da arbejdet med cybersikkerhed til dels betragtes som en del af styrelsens øvrige arbejde med beredskab for transportsektoren er der et tæt samarbejdet mellem de to enheder. Det er forventningen, at enheden vil vokse med 1-2 årsværk i indeværende strategiperiode.

I 2018 har enheden beskæftiget sig med tre hovedopgaver:

- at udarbejde transportsektorens delstrategi,
- at varetage internationale opgaver relateret til cybersikkerhed og luftfart
- at implementere direktiv EU 2016/1142 om sikkerhed i net- og informationssystemer, også kendt som ”NIS-direktivet”.

Enheden vil også fremadrettet arbejde inden for disse tre spor, som reelt med tiden forventes at flette sig sammen.

Grundlæggende vigtigt for varetagelsen af alle tre opgaver er en god og tæt dialog med branchen. Til det formål har TBST oprettet en dialoggruppe med hhv. luftfartsektoren og med jernbanesektoren. Derudover har TBST drøftet

[18] Initiativ 3.1

cybersikkerhed på TBST's brancheforum for Maritim Sikring samt påbegyndt dialog med Færdselsstyrelsen og Vejdirektoratet.

Med tiden vil det fra sag til sag blive overvejet, hvorvidt det giver bedst mening at foretage dialog med undersektorerne hver for sig eller samlet. Dialoggrupperne har under arbejdet med foreliggende strategi også deltaget i workshops om strategiens initiativer.

3.3. Arbejde med transportsektorens strategi

Som udgangspunkt for den foreliggende strategi igangsatte Transport-, Bygnings- og Boligministeriet i forsommeren 2018 en risiko- og sårbarhedsanalyse ved konsulentvirksomheden Dubex. Analysen giver en overordnet introduktion til sektorens styrker og sårbarheder fsva. cyber- og informationssikkerhed og foreslår en række initiativer, som kan igangsættes med henblik på at styrke sektoren på området. Analysens resultater vil blive gennemgået i fjerde afsnit af strategien. Initiativerne etableres dels på baggrund af regeringens strategi, analysens anbefalinger og enhedens dialog med branchen.

DCIS er ansvarlig for at drive delstrategiens initiativer fremad og på sigt identificere ny initiativer. Initiativer vil i høj grad blive gennemført i samarbejdet med sektorens operatører ligesom det kan komme på tale at benytte eksterne konsulenter eller indgå aftaler med uddannelsesinstitutioner. Enkelte initiativer vil primært være funderet og blive varetaget i enheden.

3.4. Internationale opgaver

Særligt på luftfartsområdet sker der i disse år en eksplosiv vækst af hhv. best practice, vejledninger og regler for arbejdet med cybersikkerhed. Enheden vil indgå i dette arbejde mhp. at sikre danske interesser jf. også principperne i afsnit 1. Enheden vil bruge dialoggruppen for luftfart i dette arbejde.

Det forventes, at også jernbaneområdet (særligt som følge af de ny signalsystemer på banen i Europa) og vejområdet (særligt på grund af arbejdet med selvkørende biler) vil blive et arbejdsområde for enheden.

3.5. NIS-direktivet

Direktivet om sikkerhed i net- og informationssystemer (EU 2016/1148)[19] er implementeret i den danske transportsektor ved lov nr. 441 om sikkerhed i net- og informationssystemer af 08/05/2018 samt bekendtgørelse 1042 om sikkerhed i net- og informationssystemer af 06/08/2018.

TBST har, som det er påkrævet i direktivet, i 2018 udpeget operatører af væsentlige transporttjenester, og har i forløbet op til udpegelsen haft dialog med operatørerne herom. Transportsektorens DCIS er kontaktpunkt for sektorens operatører af væsentlige transporttjenester og modtager af de

[19] https://eur-lex.europa.eu/legalcotent/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

pligtmæssige underretninger ved hændelser og har i denne forbindelse foreløbigt en koordinerende rolle mellem CfCS og aktørerne.

Der er fortsat et behov for dialog om det igangværende og kommende arbejde hermed, herunder vejledning til sektorens om indberetninger. Det er endnu ikke muligt at forudsige, hvor meget arbejdet med behandling af indberetninger vil fylde. Det er dog sikkert, at enheden vil skulle forholde sig til resultaterne af indberetninger og sørge for dialog med branchen om det billede der tegner sig. Det er meget muligt, at indberetningerne vil kunne fungere som bidrag eller ligefrem udgangspunkt for tilrettelæggelsen af fremtidige initiativer i sektoren.

På nuværende tidspunkt er enheden i en opbygningsfase både ift. bemanding og viden. Dette vil afspejle sig i de initiativer, der igangsættes i den første del af strategiens periode.

Fremadrettet vil sektorens DCIS udvikle sig i takt med et stigende modenhedsniveau, og ambitionsniveauet, ift. initiativer der årligt igangsættes, vil øges med tiden.

3.6. Samarbejde med CfCS

Samtidigt med udarbejdelsen af foreliggende strategi har TBST været i kontakt med CfCS. Da også CfCS er i gang med implementeringen af regeringens strategi, og der derfor foregår udviklingsarbejde hos alle parter, er det endnu for tidligt at tegne et klart billedede af det fremtidige samarbejde, herunder præcist hvad de enkelte sektorer kan forvente af støtte fra CfCS.

Enheden har dog på nuværende tidspunkt etableret et samarbejde med CfCS' rådgivningsafdeling, hvor en medarbejder er dedikeret til hver af de samfundskritiske sektorer. TBST inviterer denne kontaktperson med til TBST's sektor-dialoggrupper for at sikre et løbende vidensflow fra CfCS til transportbranchen og bidrage til at opbygge samarbejdet her imellem.

Samarbejdet forventes med tiden at tilføre sektoren en rådgivningskapacitet til arbejdet med bl.a. risikovurderinger og IT-rådgivning vedrørende cyber- og informationssikkerhed.

Sektorens DCIS arbejder sammen med CfCS om at udforme en samarbejdsaftale mellem parterne. Aftalen uddyber relationen mellem CfCS og sektoren, herunder hvilke ydelser CfCS tilbyder sektoren og hvilke opgaver sektoren, hovedsageligt sektorens DCIS, udfylder til gavn for CfCS.

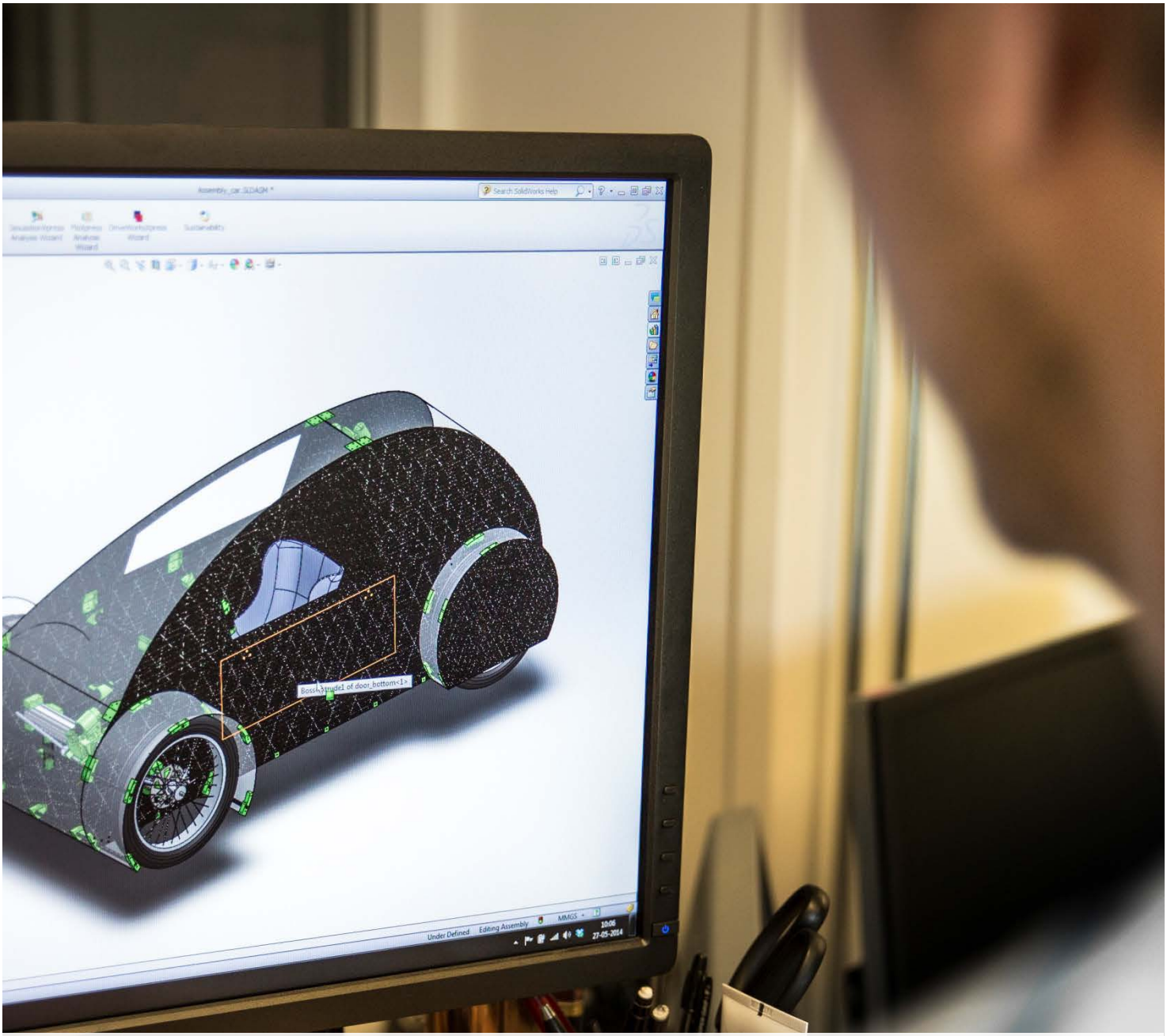
Aftalen forventes at ligge klar primo 2019.

3.7. Sparring med andre kritiske sektorer

Sektorens DCIS fungerer som kontaktpunkt til de andre samfundskritiske sektorers enheder. I forbindelse med udarbejdelsen af delstrategien er en-

heden gået i dialog med flere af de andre sektorer for sparring i forbindelse med udarbejdelse af initiativer og implementeringen af NIS-direktivet.

TBST vil arbejde for at der etableres et samarbejde om initiativer, som rækker på tværs af sektorerne, og hvor det kan give mening at samle ressourcer og udgifter. Det er væsentligt at enhederne ikke sideløbende duplikerer hinandens indsatser, men i stedet arbejder på at vidensdele og supplere hinanden. Dette så meget desto mere da flere sektorer er stærkt afhængige af de øvrige sektorers produkter.



4. Transportsektorens initiativer

Sektorens DCIS har udarbejdet 12 initiativer fordelt på tre kategorier (overblik og selvindsigt, sårbarhedserkendelse og håndtering og internationalt arbejde og regulering). Disse initiativer udgør det fokus som DCIS i denne strategis løbeperiode vil prioritere at arbejde med.

Enkelte af initiativerne kan blive udført af DCIS selv, mens langt de fleste fordrer tæt samarbejde med branchen. Dvs. der kan blive tale om, at nogle initiativer forankres hos operatører i transportsektoren i samarbejde med de respektive dialoggrupper og DCIS, eller at DCIS agerer tovholder, men udfører dele af arbejdet med branchen. Det er også en mulighed, at enkelte initiativer udføres ved brug af eksterne konsulenter.

Endeligt vil nogle initiativer falde sammen med det arbejde som digitaliseringsstyrelsens task force skal udføre, samt initiativer fra andre sektorer. I disse tilfælde vil transportbranchens DCIS søge samarbejde med henblik på effektiv videndeling og brug af ressourcer. Helt generelt gælder, at der for mange af emnerne findes internationale vejledninger, standarder mm. Det er målet i så vid udstrækning som muligt, at lægge sig op ad internationale standarder og best practice i det omfang det giver værdi.

De nedenstående initiativer vil ikke alle blive sat i gang samtidigt af både praktiske og ressourcemæssige årsager. I stedet vil sektorens DCIS i første halvår af 2019 drøfte med blandt andre branchen, hvilke initiativer, der efter en vurdering af hhv. risiko og væsentlighed, giver bedst mening af sætte i gang først. Visse initiativer sættes i gang først med henblik på at skabe en grundlæggende fælles forståelse for cybersikkerhedsudfordringen, f.eks. kortlægning af kritisk infrastruktur og tjenester. Andre initiativer er reelt allerede igangsat, men skal yderligere udbygges, struktureres og metodisk afdækkes. Det gælder f.eks. initiativer om oprettelsen af et fortroligt dialogforum, modenhedsmåling og internationalt arbejde om cybersikkerhed.

Endeligt er der nogle initiativer, som vil drage fordel af at blive igangsat når DCIS og branchen har dannet sig et første struktureret overblik over udfordringerne og opnået en vis modenhed. TBST og Transport-, Bygnings- og Boligministeriets departement udarbejder primo 2019 i fællesskab en handlingsplan med detaljerede succeskriterier og milepæle for arbejdet med initiativerne. Alt efter hvad der igangsættes i Digitaliseringsstyrelsens task force samt de øvrige sektorer kan handlingsplanen blive tilrettet. DCIS vil herefter halvårligt gøre status for fremdrift samt overveje evt. tilretning af den løbende handlingsplan.

Et væsentligt udgangspunkt for transportsektorens prioritering af initiativer i denne strategiperiode har været ledelsesforankring. Det er sektormyndighedernes vurdering, bl.a. på baggrund af Dubex rapport, at der indledningsvis forestår et vigtigt arbejde med få øget bevidstheden om cyber- og informationssikkerhed på ledelsesgangene hos transportaktørerne. Dertil er det også nyt for sektormyndighederne at beskæftige sig med cyber- og informationssikkerhed, hvorfor mere konkrete initiativer vil følge når både myndighed og sektor bliver klogere på området, og indsatserne kan konkretiseres yderligere.

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. OVERBLIK OG SELVINDSIGT

1.1. *Kortlægning af kritisk infrastruktur og tjenester*

I Regeringens nationale strategi fremgår det af initiativ 1.9, "Kortlægning af national it-infrastruktur"[20], at der ikke eksisterer en oversigt over digital infrastruktur og digitale tjenester, som er væsentlige for samfundsvigtige funktioner.

CfCS foretager løbende monitorering af cybertrusler og eventuelle angreb gennem sensornetværk ude hos virksomheder og organisationer, men der mangler et mere fuldkomment billede af it-infrastrukturen. Et sådant overblik vil kunne forbedre indsatsen over for cybertrusler i de samfundsvigtige sektorer.

Transportsektoren vil derfor i dialog med branchen igangsætte en kortlægning af kritisk it-infrastruktur og tjenester. En sådan kortlægning vil i første omgang omfatte de operatører som er udpeget som operatører af væsentlige transporttjenester, jf. NIS-direktivet og kan derpå trinvist udvides til at omfatte hele sektoren. Et væsentligt punkt for oversigten er en identifikation af, hvilke systemer som virksomhederne selv styrer og hvilke der reelt varetages af underleverandører.

Som supplement til initiativet skal der udarbejdes en oversigt over hvorledes rolle- og ansvarsfordelingen er ift. informationssikkerhed i sektoren.

[20] Fra Regeringens"National strategi for cyber- og informationssikkerhed 2018-2021"

Initiativet forventes at bidrage til en bedre forståelse, for både myndigheder og aktører, for transportaktørernes kritiske systemer, som ved nedbrud vil have alvorlig indvirkning på deres evne til at udføre den overordnede transporttjeneste.

Kortlægningen vil derved både kvalificere myndighedernes rådgivning og krav til aktørerne, som til gengæld får klarere svar på hvad forventningen er fra myndighedernes side samt bedre rådgivning herom.

Supplerende til den indledningsvise kortlægning, skal der udarbejdes en plan og proces for løbende opdateringer af oversigten over kritisk it-infrastruktur og tjenester, som foretages ved ændringer og/eller tilfælde af alvorlige cyberhændelser.

1.2. *Modenhedsmåling*

Modenhedsmålinger kan give den enkelte virksomhed en vurdering af, hvor moden virksomheden er i deres tilgang til cyber- og informationssikkerhed. Det kan være med til at skærpe virksomhedens opmærksomhed på, hvad der skal prioriteres og hvordan gevinster opnås med størst effektivitet og laveste omkostninger.

Et overblik over transportvirksomhedernes modenhedsniveauer kan ligeledes gives DCIS en vigtig indikation på, hvor der skal fokuseres ift. de enkelte brancher eller virksomheder. Initiativet omfatter som udgangspunkt alle de transportaktører, som ønsker at deltage i at udarbejde målingerne.

Derfor igangsættes et initiativ, som i første omgang skal afklare hvilken metode der kan benyttes til at foretage en modenhedsmåling hos de enkelte aktører, med henblik på dernæst at foretage egentlige modenhedsmålinger.

I første omgang vil DCIS derfor søge rådgivning hos CfCS samt opsøge viden i andre kritiske sektorer om deres erfaring og viden om at udføre modenhedsmålinger. Det er blandt andet transportsektoren kendt, at der på energiområdet i 2015 er udført en modenhedsundersøgelse ift. cyber- og informationssikkerhed.

I forbindelse med at finde en passende model skal det drøftes med branchen hvorvidt vurderingerne skal foretages ved f.eks. peer review, de enkelte virksomheder i samarbejde med DCIS eller ved brug af eksterne konsulenter.

Initiativet forventes at bidrage til, at transportsektorens modenhed ift. at imødegå trusler mod cyber- og informationssikkerheden klarlægges og forbedres samt at ministeriet får bedre overblik over sektorens evne til at håndtere hændelser.

1.3. *Fortrolige samarbejdsfora for cybersikkerhed*

Et indledende skridt til bedre cybersikkerhed i de enkelte virksomheder er deling af viden. Dvs. at sektoren bliver bedre til at have dialog om udfordringer og løsningsmuligheder på tværs af myndigheder og aktører.

Kendskab til angreb og sårbarheder, og indsigt i læringen af dem, skal i højere grad udveksles på tværs i branchen, så sektoren som helhed opnår en bedre awareness om trusler og deler løsninger til at imødegå dem bedst muligt. Deling af sårbarheder er imidlertid en øm tå for mange aktører, da der vil være tale om forretningsfølsomme informationer, som man måske nødigt vil dele med andre.

Transportsektorens DCIS har med dette for øje for nuværende nedsat to dialogfora om cybersikkerhed for hhv. luftfartssektoren og jernbanesektoren. Hvorvidt disse eksisterende fora er egnede til formålet skal afklares mellem myndighed og aktører. Det indebærer f.eks. at sikre og opretholde deltageres sikkerhedsgodkendelser og gennemgå procedurer for håndtering af fortroligt mødemateriale og afholdelse mm.

Der kan også være overvejelser om ét fælles dialogforum for hele sektoren, eller en opretholdelse af de eksisterende grupper med lejlighedsvise fælles aktiviteter (foredrag, workshops o.lign) samt hvordan hhv. maritim sikring og vejsektoren inddrages bedst i det vigtige arbejde.

Initiativet vil derfor først og fremmest skulle drøftes i de nuværende dialoggrupper, så det afklares hvordan et fortroligt samarbejdsfora etableres i praksis.

Udover de ovenfor nævnte dialoggrupper deltager DCIS i andre tværsektorielle og internationale vidensdelingsfora og videregiver information herfra til sektorens aktører.

Initiativet forventes at bidrage til en øget vidensdeling om cyber- og informationssikkerhed i sektoren hvilket giver mulighed for bedre forebyggelse og håndtering af hændelser, bedre varetagelse af de internationale opgaver samt en god løbende tilbagemelding ift. tendenser og udviklinger i trusselsbilledet.

1.4. *Ledelsesfokus på cybersikkerhed*

En god opmærksomhed på cybersikkerhed starter hos den enkelte virksomheds ledelse.

Det er helt afgørende at ledelsen har fornøden kompetence, dvs. forståelse og indsigt i virksomhedens kritiske infrastruktur, udefrakommende trusler og virksomhedens modenhed ift. at imødegå disse.

Initiativet skal dels afklare hvad der er af væsentlig viden og kompetencer hos en virksomheds øverste ledelse og dels give forslag til hvordan rette fokus kan tilvejebringes og/eller styrkes. Derudover skal der identificeres tiltag, det kan f.eks. være foredrag, vejledningsmateriale workshops o.l., som kan styrke virksomhedernes ledelser i deres arbejde.

Det er også væsentligt med en forventningsafklaring mellem branchens virksomheder og Transport-, Bygnings- og Boligministeriet ift. niveauet for

cybersikkerhed. Det vil være naturligt at ledelsesfokus og -involvering indgår i modenhedsvurderingen af den enkelte virksomhed.

Initiativet forventes at bidrage til øget forståelse og prioritering af cyber- og informationssikkerhed på ledelsesniveau hos transportaktørerne og dermed fremme en positiv sikkerhedskultur på cybersikkerhedsområdet hos operatørerne.

1.5. *Trusselskatalog*

Transportsektorens aktører har behov for at få et aktuelt trusselsbillede af de cyberrisici, som gælder for sektoren og potentielt også specifikt for deres virksomhed.

Initiativet er blevet døbt et "trusselskatalog", men skal som sådan fungere som et aktuelt og operationelt overblik over trusler mod sektoren. Der udestår indledningsvis et arbejde med at fastlægge en metodik for at udarbejde sådan et katalog. Trusselskataloget vil derfor indledningsvis være forankret i sektorens DCIS og dialoggrupperne med branchen.

Gennem DCIS' samarbejde med den indstationerede medarbejder i CfCS opnås mere indblik i truslen mod transportsektoren, men hvorvidt frekvensen af de sektorspecifikke trusselsvurderinger er tilstrækkeligt for sektoren er på nuværende tidspunkt uklart.

Initiativet vil derfor tilpasses løbende i takt med at samarbejdet med CfCS og Trusselsvurderingsenheden modnes. Det kan vise sig nødvendigt at supplere trusselsvurderingerne med mere løbende input til branchen.

Initiativet forventes at bidrage til, at sektorens aktører får bedre indsigt i hvilke trusler de skal forholde sig til. I drøftelser mellem aktører og myndighed, har aktørerne givet udtryk for at de er usikre på hvilke trusler det specifikt er, de skal forholde sig til.

2. SÅRBARHEDSERKENDELSE OG HÅNDTERING

2.1. *Risikovurderinger*

Fuldkommen cybersikkerhed er ikke en opnåelig mulighed. Det er derfor afgørende at hver enkelt virksomhed, på baggrund af en erkendelse af sin kritiske infrastruktur, de eksterne trusler samt den interne modenhed, foretager en risikovurdering af, hvor de største behov – samt størst mulige gevinst- for at sætte ind er.

Ifølge Dubex' risiko- og sårbarhedsanalyse, er der i transportsektoren stor spredning i aktørernes modenhed hvad angår tilgang til og proces for risikostyring og ledelsesforankring[21]. Her står sektoren overfor en udfordring i at omstille sig til at arbejde med mere dynamiske risikovurderinger, eftersom

[21] Dubex (2018), s. 29

trusler og risici indenfor cybersikkerhed er mere omskiftelige end traditionelle risici.

Initiativet indebærer, at der skal identificeres forslag til best practice for risikovurderinger samt evt. vejledning for brugen heraf. Der findes på dette område flere internationale standarder, der vil kunne danne grundlag herfor.

Det vil desuden være naturligt at den enkelte virksomheds evne til at foretage gode risikovurderinger, og evnen til at benytte disse formålstjenstligt, indgår i modenhedsvurderingen af den enkelte virksomhed.

Supplerende hertil skal DCIS udarbejde en plan for løbende revision af den risiko- og sårbarhedsvurdering, som blev udarbejdet i forbindelse med denne strategis udarbejdelse. Vurderingen skal opdateres ved ændringer og/eller alvorlige cyberhændelser, med henblik på at sikre en hensigtsmæssige prioritering af cyber- og informationssikkerhedsindsatsen.

Initiativet skal bidrage til, at virksomhederne får en realistisk forståelse af de risici som de skal forholde sig til. Som følge deraf vil de kunne træffe vidensbaserede valg om brug af ressourcer samt beslutning om hvilket risikoniveau der vurderes som acceptabelt. Alt i alt giver gode risikovurderinger forudsætningerne for en mere robust cybersikkerhed.

2.2. *Leverandørstyring*

Brugen af outsourcing i dele af driften er udbredt på tværs af transportsektoren. Det vurderes af Dubex, at udviklingen mod mere outsourcing fortsætter i de kommende år og at store dele af transportsektorens IT-systemer også lægges ud til eksterne leverandører[22].

Outsourcing af drift og IT-systemer betyder nødvendigvis at eksterne parter har adgang til potentielt vigtige tjenester og IT-infrastruktur. Det stiller naturligt store krav til sikkerheden hos de pågældende leverandører, som sidder med fjernadgang til aktørernes systemer.

Det fritager imidlertid ikke transportsektorens aktører for ansvaret for at sikre, at cybersikkerheden er i orden. Dette er aktørerne bevidste om, og flere udtrykker ønske om at få øget kontrol og kendskab til underleverandørers arbejde med cybersikkerhed.

Derfor igangsættes et initiativ, der skal medvirke til dialog og best practise ift. hvordan den enkelte virksomhed, kontraktligt og i daglig drift, sætter tilstrækkelige krav til underleverandørernes leverance af cybersikkerhed i de systemer, som de varetager på vegne af transportaktøren.

[22] Dubex (2018), s. 36

Initiativet forventes at bidrage til, at branchens brug af outsourcing og underleverandører klarlægges, og at kontrollen og kendskabet til underleverandørernes cybersikkerhed øges.

2.3. *Best-practice og vejledninger*

Der er stor spredning i transportaktørernes modenhed hvad angår tilgang til risikostyring og ledelsesforankring for cyber- og informationssikkerhed.

Visse transportaktører er langt i arbejdet med cyber- og informationssikkerhed og arbejder f.eks. efter internationale standarder, anbefalinger, arbejdsprocesser (f.eks. Prevent, Protect, Detect, Respond), mens andre har et efterslæb i både ledelsesforankring og awareness om risici inden for cyber- og informationssikkerhed.

Derfor bør det nærmere undersøges hvilke branchestandarder, anbefalinger, metoder og huskeregler der arbejdes efter hos de forskellige aktører, hvor langt de er hermed og dermed hvordan best-practice anbefalinger kan bidrage til at løfte det generelle sikkerheds- og vidensniveau hos aktørerne i transportsektoren.

Supplerende skal DCIS skabe et overblik over forpligtigende vejledninger eller retningslinjer som de enkelte virksomheder er underlagt ift. cyber- og informationssikkerhed.

Initiativet forventes helt overordnet at øge informationsudvekslingen om metoder mm. vedr. cyber- og informationssikkerhed. Det vil primært fungere som en løftestang både vidensmæssigt og metodisk for de aktører, som har et efterslæb ift. at beskæftige sig med området.

2.4. *Medarbejder-awareness*

Et godt værn mod cyber- og informationssikkerhedstrusler handler ikke udelukkende om tekniske foranstaltninger. Medarbejdernes adfærd på alle niveauer i en virksomhed kan udgøre en ligeså stor risiko for tilsigtede og utilsigtede cyberangreb, som utilstrækkelige it-foranstaltninger. Derfor skal indsatsen for bedre cyber- og informationssikkerhed ikke kun baseres på store og forkromede tekniske foranstaltninger.

De skal suppleres af medarbejdere, som er kompetente og vidende om risikoen for cybertrusler og hvordan disse kan tage sig ud i form af f.eks. *social engineering*[23], og som derfor ikke er i tvivl om, hvordan de skal agere i hverdagen.

God medarbejder-awareness er imidlertid ikke den enkelte medarbejders ansvar alene, men hele virksomhedens. I sidste ende er det således et ledelsesansvar at tilegne ressourcer i form af tid, materiale og mennesker til at

[23] Center for Cybersikkerhed (2017), "Cyberforsvar der virker", s. 8.

øge medarbejderkendskabet til potentielle cyber- og informationssikkerhedsrisici.

Der findes allerede i stort omfang materiale om medarbejder-awarenes som er både grundigt og frit tilgængeligt.

Initiativet vil indeholde en vurdering af kompetenceudfordringerne forbundet med cyber- og informationssikkerheden i sektoren og i den forbindelse overveje og evt. igangsætte konkrete tiltag til håndtering af disse udfordringer.

Initiativet vil medføre en identifikation af materiale som kan anbefales branchen, evt. supplere med nyt materiale, og indeholde overvejelser om tiltag for branchen. Det kan være i form af fælles dialog om udfordringer med awareness, fælles informationskampagner eller individuelle tests af medarbejdernes awareness.

Sidst, men ikke mindst, vil initiativet medføre en vurdering af behovet for sikkerhedsgodkendelse af medarbejdere, der arbejder med cyber- og informationssikkerhed, og, såfremt nødvendigt, en procedure for sådanne godkendelser.

Det vil være naturligt at medarbejder-awareness indgår i modenhedsvurderingen af den enkelte virksomhed.

2.5. *Cybersikkerhed som del af sektorberedskabet*

Transportsektoren er vant til at arbejde med beredskab i situationer hvor hændelser medfører atypiske situationer.

Beredskabsstrukturen og sektoransvarsprincippet er med til at sikre, at den enkelte virksomhed kan agere hurtigt, effektivt og fornuftigt ved en given beredskabsrelateret hændelse. Sektoransvaret på beredskabsområdet er således reguleret i beredskabslovens §24-28, hvor planlægningsansvaret fastsat i § 24 pålægger de enkelte ministre ansvar for at sikre opretholdelse og videreførelse af ministerområdets samfundsvigtige funktioner i tilfælde af ulykker og katastrofer. Dette princip er med til at sikre et robust beredskab ift. ekstraordinære hændelser.

TBST fører tilsyn med, at alle Transport-, Bygnings- og Boligministeriets underliggende transportaktører planlægger for at kunne videreføre kritiske funktioner i tilfælde af ekstraordinære hændelser, herunder udarbejder en beredskabsplan. Aktørerne varetager i dette medfør den operative del af beredskabet inden for transportsektoren.

Helt overordnet er det væsentligt for evnen til at håndtere potentielle angreb, at der gennemføres beredskabsøvelser, som simulerer cybersikkerhedshændelser. Dette bliver f.eks. gennemført i regi af EU-kommissionens cybersikkerhedsagentur, ENISA, der hvert andet år arrangerer en paneuropæisk cybersikkerhedsøvelse, Cyber Europe, der senest blev gennemført i sommeren 2018 og havde fokus på luftfartssektoren.

DCIS skal i samarbejde med styrelsens beredskabsenhed fremadrettet have fokus på at fremme dansk deltagelse i disse øvelser samt i det omfang det måtte være muligt, at påvirke tilrettelæggelse af øvelsesscenarier ift. scenarier som særligt vurderes at være relevante af virksomhederne. DCIS skal i samarbejde med styrelsens beredskabsenhed og branchen fastsætte planer og processer for jævnlige beredskabstest og øvelser, som gennemføres minimum en gang årligt.

Dubex' rapport konkluderer, at det er vanskeligt at vurdere hvorvidt aktørerne har de nødvendige foranstaltninger på plads hvad angår beredskab for cyber- og informationssikkerhedshændelser. Det er afgørende, at især transportsektorens store aktører planlægger for eventuelle cyberhændelser og øver sig på håndteringen af disse.

Initiativet indebærer derfor først og fremmest en afdækning af i hvor høj grad aktørernes nuværende beredskabsplaner tager højde for cyber- og informationssikkerhedshændelser. På den baggrund skal det drøftes, hvorvidt der er behov for at udarbejde retningslinjer for håndtering af cyber- og informationssikkerhedshændelser i aktørernes nuværende beredskabsplaner.

Ligeledes skal initiativet afklare, om der er uafdækkede behov for drøftelse af cybersikkerhed i de allerede eksisterende beredskabsfora i branchen, herunder Fagligt Koordinationsforum Transport (FKF) samt i ramme af NOST (National Operativ Stab).

Initiativet forventes at bidrage til, at sektoren som helhed rustes bedre til at håndtere cybersikkerhedshændelser.

3. INTERNATIONALT ARBEJDE OG REGULERING

3.1. *International interessevaretagelse*

Særligt på luftfartsområdet er der i dag flere forskellige internationale fora (i regi af EU, FN m.fl.) som drøfter udfordringerne med cybersikkerhed. Flere af disse arbejder pt. med udkast til regulering og vejledning om best practise. Udover de fora som TBST deltager i, findes der også på virksomhedsniveau foraer der drøftes cybersikkerhed for transportsektoren.

Initiativet har to primære formål. Dels en sikring af vidensdeling mellem DCIS/TBST og sektoren. Det er væsentligt, at sektoren høres om tiltag, som kan få betydning for dem, ligesom det er væsentligt at sektoren orienterer DCIS/TBST om den viden som de indhenter i f.eks. internationale branchefora. Dels har initiativet til formål, at kvalificere beslutningen om hvor der skal benyttes ressourcer på deltagelse. Der er løbende møder, konferencer, workshops med mere, og det er væsentligt at deltagelsen koncentreres om de fora der har størst betydning for sektoren.

Den øgede dialog skal primært finde sted ved dialogmøder, men kan også ske ved skriftlig høring om konkrete reguleringstiltag eller gensidig ad hoc information mellem DCIS/TBST og sektoren.

Initiativet skal bidrage til, at DCIS/TBST er bedre rustet til at arbejde for danske interesser i internationale fora, at branchen har en god forståelse for hvad der er undervejs af ny regulering, at DCSI/TBST kan fokusere sine ressourcer, der hvor det kan give størst gevinst samt generelt en god og

3.2. *Samarbejde med Færdselsstyrelsen, Vejdirektoratet og Transport-, Bygnings- og Boligministeriets departement om selvkørende teknologi*

Selvkørende teknologi er under hastig udvikling. På transportområdet bliver både biler og infrastruktur mere og mere digitaliserede. Selvkørende teknologi forventes at kunne bidrage til forbedret trafiksikkerhed, bedre udnyttelse af vejene og dermed også øget mobilitet i samfundet som helhed.

Infrastrukturen digitaliseres også i takt med udviklingen i bilerne. I fremtiden skal den selvkørende teknologi kommunikere både fra bil til bil og fra bil til infrastruktur. Bilerne skal således selv kunne holde øje med vejstriber, medtrafikanter, skilte mv.

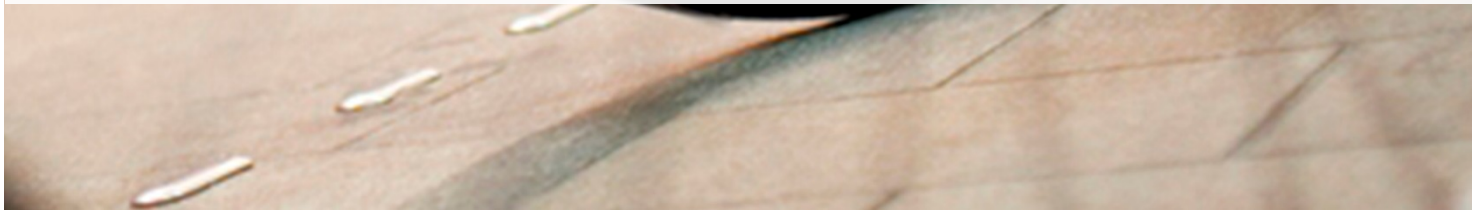
Udviklingen med selvkørende teknologi og integrationen i trafikken på vejene introducerer også risici for potentielle cyber- og informationssikkerhedstrusler, som vi kender meget lidt til i dag. Der er allerede i dag eksempler på at såkaldte ”connected cars”, dvs. biler udstyret med internetforbindelse, kan tilgås eksternt.

Derfor igangsættes et fast samarbejde mellem Transport-, Bygnings- og Boligministeriets departement, Færdselsstyrelsen og Vejdirektoratet om selvkørende teknologi og cybersikkerhed. Samarbejdet skal i første omgang klarlægge arbejdsfordeling mellem parterne og skabe overblik over relevante arbejdsgrupper i EU-regi, med henblik på at sikre den bedst mulige varetagelse af danske interesser ift. udarbejdelse af regler på området.

Det vil løbende blive vurderet, hvordan samarbejdet om selvkørende teknologi og cybersikkerhed kan integreres i det arbejde, der sker i det tværgående og koordinerende forum for ressortområdets ageren ift. intelligente transportsystemer (ITS-koordinationsforum), nedsat af departementet ultimo 2018.

Initiativet forventes at bidrage til et tættere samarbejde på området mellem departementet, Vejdirektoratet og Færdselsstyrelsen, så sektoren som helhed bliver rustet til at varetage udviklingen indenfor selvkørende teknologi.

5. Afrunding



Hændelser de seneste år samt CfCS' trusselsvurderinger, både de generelle og de sektorspecifikke, viser, at der findes nationer, grupper og enkeltpersoner med evnerne såvel som viljen til at udføre cyberangreb mod Danmark og kritisk dansk infrastruktur.

Transportsektoren i Danmark har gennem mange år etableret en god sikkerhedskultur ift. kendte trusler og sårbarheder, men der er behov for, at vi nu også indser at cybertrusler medfører et mere dynamisk risikobillede. Det kræver at vi udvider vores opfattelser og antagelser om sårbarheder. Det gælder ikke kun, når sektoren skal ruste sig mod konkrete destruktive cyberangreb, men også på hele vores tilgang til at omgås og håndtere fortrolig information på vores arbejdsplads.

Der er derfor al grund til at transportsektoren prioriterer ressourcer ift. arbejdet med cyber- og informationssikkerhed. Det gælder både for myndigheder såvel som for aktører, som i fællesskab har et ansvar for at sikre at danske borgere kan færdes sikkert rundt i landet med fly, tog eller bil.

Denne delstrategi er sektorens første indsats for at adressere nogle af de mange udfordringer, som vi står over for. Sektorens 12 initiativer er udarbejdet på baggrund af Dubex' risiko- og sårbarhedsanalyse og i samarbejde med sektorens aktører, og der udestår nu et stort og meget vigtigt arbejde med at konkretisere initiativerne til operationelle indsatser.

Det arbejde vil sektorens DCIS i samarbejde med blandt andre transportsektorens aktører, CfCS, PET, de andre kritiske samfundssektorer og Digitaliseringsstyrelsen stå for at drive fremad de kommende år. Til det formål er der indledningsvist etableret dialoggrupper for hhv. luftfarten og jernbanen samt et sideløbende samarbejde med Vejdirektoratet, hvor CfCS mfl. løbende vil blive inddraget.

Strategien udstikker retningen for arbejdet i de kommende tre år, og det må forventes at i takt med at sektoren som helhed oparbejder større viden på området kan initiativerne også tilpasses. Sektorens DCIS følger halvårligt op på strategiens fremdrift i samarbejde med en styregruppe med deltagelse af Transport-, Bygnings- og Boligministeriets departement og TBST.

Indsatsen bidrager til, at transportsektoren tids nok ruster sig til at håndtere truslen mod sektorens cyber- og informationssikkerhed. Vi har stort et ansvar for at sikre et samfund med sikker trafikafvikling og høj mobilitet.

6. Referencer

Dubex (2018), ”Analyse af cyber- og informationssikkerhed i transportsektoren”

CfCS 1 (2018), ”Trusselsvurdering: Cybertruslen mod Danmark”.
https://fe-ddis.dk/cfcs/publikationer/Documents/CTV2018_MAJ.pdf

CfCS 2 (2018), ”Cybertruslen mod land- og lufttransport”
https://fe-ddis.dk/cfcs/publikationer/Documents/ Trusselsvurdering_Cybertruslen_mod_land-_og_lufttransport.pdf

Center for Cybersikkerhed (2017), ”Cyberforsvar der virker”:
https://fe-ddis.dk/cfcs/publikationer/Documents/ Cyberforsvar%20der%20virker%20-%202017_110117.pdf

Transport , Bygnings og Boligministeriet
Frederiksholms Kanal 27F
1220 København K
Telefon 41 71 27 00
trm@trm.dk

ISBN netudgave: 978 87 93292 43 7