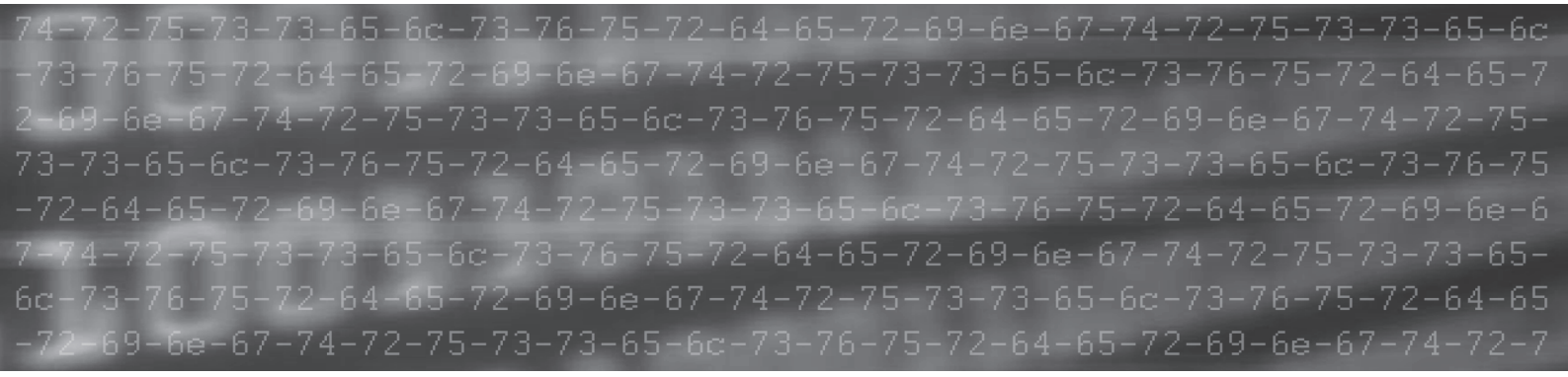
CENTER FOR CYBERSIKKERHED

Trusselsvurdering

Cybertruslen mod land- og lufttransport



Trusselsvurderingsenheden ved Center for Cybersikkerhed

December 2018

CENTER FOR CYBERSIKKERHED

Trusselsvurdering: Cybertruslen mod land- og lufttransport

Denne trusselsvurdering redegør for cybertrusler, der er rettet mod den danske transportsektor. Transportsektoren i Danmark er vigtig for samfundets funktion og stabilitet. Hensigten er at orientere transportsektoren om truslerne, så den bedre kan beskytte sig. Trusselsvurderingen kan eksempelvis indgå i risikovurderingen for sektoren i forbindelse med den nationale strategi for cyber- og informationssikkerhed.

Hovedvurdering

- Truslen fra cyberkriminalitet mod den danske transportsektor er **MEGET HØJ**. Der er særligt en trussel fra cyberkriminalitet, der sigter mod at afpresse penge fra virksomheder og myndigheder. Cyberkriminalitet kan i værste fald påvirke driften i transportsektoren og svække kundernes tillid.
- Truslen fra cyberspionage er **HØJ**. Ved at stjæle informationer kan fremmede stater bl.a. komme i besiddelse af nye teknologier til at styrke og udvikle egen transportsektor og give deres virksomheder fordele på det internationale marked.
- Truslen fra cyberaktivisme er **MIDDEL**. Truslen er ofte motiveret af enkeltsager, og truslen mod sektoren kan derfor stige uden eller med kort varsel. Særligt luftfart har været udsat for cyberaktivisme rundt om i verden.
- Truslen fra cyberterror er **LAV**. Militante ekstremister har i få tilfælde ytret intentioner om at udføre cyberterror, men de har ikke kapacitet til dette på nuværende tidspunkt.
- Det er mindre sandsynligt, at fremmede stater vil rette destruktive cyberangreb mod dansk samfundsvigtig infrastruktur, herunder transportsektoren. Det er dog muligt, at den danske transportsektor kan blive påvirket af destruktive cyberangreb i udlandet.

Indledning

Vurderingen beskriver den generelle cybertrussel, der er rettet imod den danske transportsektor. Transportsektoren dækker i denne vurdering over land- og lufttransport af personer og gods, inklusiv infrastruktur og tjenester, der understøtter dette. Droner og havne er også medtaget. Skibsfart er ikke medtaget, da skibsfart behandles som en selvstændig sektor af danske myndigheder. Transportsektoren består af mange forskellige delelementer med egne særpræg og sårbarheder. Denne trusselsvur-

dering analyserer cybertruslen mod transportsektoren som helhed, og der skelnes kun mellem enkeltdelene af sektoren i et begrænset omfang. Transport udført af Forsvarets enheder indgår ikke i vurderingen.

Udover at transportsektoren er en del af næsten alle danskeres hverdag, så er andre sektorer afhængige af transportsektoren. Det er derfor vigtigt, at sektoren er robust overfor cyberangreb.

I takt med at den teknologiske udvikling gør transportsektoren mere afhængig af digitale løsninger opstår nye angrebsflader for hackere. Biler, fly og toge er i stigende grad forbundet til eller styret af it-systemer, hvilket hackere i værste fald kan udnytte til at påvirke tilgængeligheden af eller sikkerheden omkring land- og lufttransport. It-nedbrud hos eksempelvis flyselskaber og lufthavne i udlandet, der ikke er relateret til cyberangreb, viser, hvor afhængige dele af transportsektoren allerede er af systemer, som kan rammes af cyberangreb.

Trusselsvurderingen tager udgangspunkt i Forsvarets Efterretningstjenestes Center for Cybersikkerheds (CFCS') generelle viden om cybertrusler og eksempler på cyberangreb mod transportsektoren. CFCS har endnu et relativt begrænset indblik i sektorspecifikke forhold i transportsektoren sammenlignet med andre samfundsvigtige sektorer.

Vurderingen tager udgangspunkt i det aktuelle trusselsbillede og har en varslingshorisont på op til to år. Da cybertruslen er dynamisk, kan trusselsbilledet på nogle områder ændre sig pludseligt, både generelt og for den enkelte myndighed eller virksomhed. Vurderingen anvender Forsvarets Efterretningstjenestes trusselsniveauer og sandsynlighedsgrader, der er forklaret i slutningen af vurderingen.

Der er mørketal, når det gælder viden om cyberangreb mod myndigheder og virksomheder i transportsektoren. Mørketallene skyldes bl.a., at nogle cyberangreb ikke bliver anmeldt til relevante myndigheder, enten fordi organisationen ønsker mindst mulig opmærksomhed omkring et angrebsforsøg, eller fordi de ikke er klar over, at de har været udsat for angreb. Der er ved lov, i maj 2018, indført nye indberetningsordninger, der forventeligt giver bedre indsigt i cyberangreb mod samfundsvigtige virksomheder.

Hvad er cybertrusler

CFCS definerer cybertrusler som trusler fra cyberangreb, hvor en aktør ved hjælp af it forsøger at forstyrre eller få uautoriseret adgang til data, systemer, digitale netværk eller digitale tjenester. Anden brug af internettet, der kan have negative konsekvenser for samfundet, såsom salg af ulovlige varer og tjenester på internettet, indgår ikke i denne definition af cybertrusler.

Trusselsbilledet kan beskrives ud fra flere vinkler. I denne vurdering er der fokus på, hvilket formål anvendelsen af cyberangreb har for de aktører, der udfører dem. CFCS beskriver og vurderer her aktiviteter,

der har til formål at udføre cyberspionage, cyberkriminalitet, cyberaktivisme eller cyberterror. Desuden vurderer CFCS den potentielle trussel fra destruktive cyberangreb.

Trusselsniveauerne er baseret på en analyse af aktørernes intention og cyberkapaciteter. CFCS vurderer en aktørs cyberkapacitet ud fra de menneskelige og materielle ressourcer, aktøren har til rådighed. Det kan være teknisk dygtige hackere og udviklere af malware eller viden om mål, der kan bruges til eksempelvis social engineering. Det kan også være it-infrastruktur, tid, penge og adgang til information. Hvor stor en cyberkapacitet, en aktør har, vil derfor afhænge af flere forskellige forhold og aktørens evne til at udnytte dem.

Cyberkriminalitet

Truslen fra cyberkriminalitet mod sektoren er **MEGET HØJ**. Cyberkriminalitet dækker i denne vurdering handlinger, hvor gerningsmanden bruger cyberangreb til at begå kriminalitet, som er motiveret af ønsket om økonomisk vinding.

Cyberkriminelle er opfindsomme i deres forsøg på at berige sig og anvender mange forskellige typer cyberangreb, hvoraf en del er avancerede og komplekse. Der er særligt en trussel fra cyberkriminalitet, der sigter mod at afpresse penge fra virksomheder og myndigheder. Denne trussel kommer især til udtryk i form af ransomwareangreb, men cyberkriminelle afpresser også deres ofre på andre måder, f.eks. ved hjælp af DDoS-angreb eller ved at true med at offentliggøre data, som de har stjålet ved hjælp af hacking.

Forsøg på afpresning gennem brug af ransomware kan i værste fald påvirke driften i transportsektoren. Et ransomwareangreb mod San Francisco Municipal Transportation Agency i USA i 2016, der ramte bl.a. billetsystemer, betød, at passagerer over tre dage kunne køre gratis med tog. Et ransomwareangreb mod Colorado Department of Transportation i 2018 krypterede tusinder af myndighedens arbejdsstationer. I september 2018 blev San Diego havn ramt af et ransomwareangreb, der medførte nedbrud i systemer og tjenester, men havnen kunne opretholde håndteringen af skibe. Angrebet skete kort tid efter, at Barcelona havn var blevet ramt af et cyberangreb, der havde lignende effekt. Det globale angreb med WannaCry-ransomware i 2017 ramte også transportsektoren, bl.a. Deutsche Bahn og FedEx.

Der er cyberkriminelle, der truer med at overbelaste virksomheders hjemmesider eller andre internetvendte services med såkaldte DDoS-angreb, medmindre ofret betaler. Sådanne trusler er typisk ikke rettet mod transportsektoren, så der er tale om en potentiel trussel mod sektoren. DDoS-angreb kan forstyrre transportsektoren ved eksempelvis at gøre billetsalg eller hjemmesider utilgængelige. I udlandet har der været tilfælde, hvor DDoS-angreb har medført forsinkelser for tog og fly. Motiverne for disse angreb var uklare og kan derfor ikke umiddelbart knyttes til forsøg på afpresning, men hændelserne viser, at sådanne angreb kan finde sted.

Hackere kan også stjæle data fra myndigheder og virksomheder i transportsektoren for at afpresse dem. Tyveri af eksempelvis personlige og finansielle oplysninger kan svække kundernes tillid til ramte virksomheder i sektoren. Kriminelle hackere kan derfor bruge datatyveri til afpresning.

DDoS-angreb mod transportsektoren

Distributed Denial of Service (DDoS) betegner cyberangreb, hvor angriberen udnytter kompromitterede elektroniske enheder til at generere store mængder datatrafik mod en hjemmeside (webserver) eller et netværk. Hjemmesiden eller netværket kan derfor blive utilgængeligt, mens angrebet står på.

Et DDoS-angreb mod DSB betød at DSB's billetsalg kortvarigt brød ned i maj 2018. DSB og rejseplanen blev udsat for flere DDoS-angreb i 2013, der medførte, at DSB's og rejseplanens hjemmesider kortvarigt var utilgængelige. I 2017 medførte et DDoS-angreb på Trafikverket i Sverige nedbrud i bl.a. web-baseret kommunikation mellem trafikstyringen og lokomotivførere, hvilket i sidste ende førte til togforsinkelser. I Polen forårsagede et DDoS-angreb mod Warszawa Chopin Lufthavn i 2015 flyforsinkelser, da systemer i lufthavnen gik ned.

Det er ikke klart, hvad motivationen bag angrebene var. Det kan have været chikane, afprøvning af de ramte organisationernes infrastruktur og sikkerhedsniveau eller kriminelle, der ønskede at demonstrere sine DDoS-værktøjer overfor potentielle købere.

Bedrageri i form af såkaldte Business E-mail Compromise-scams (BEC-scams) er fortsat en trussel på tværs af sektorer. BEC-scams har til formål at franarre virksomheder og myndigheder penge via bedrageriske e-mails, der indeholder instrukser om at gennemføre pengeoverførsler til aktøren. For at udnytte medarbejdernes loyalitet udgiver de kriminelle sig typisk for at være en ledende medarbejder i organisationen. Bedrageri af denne type kaldes derfor også ofte for CEO-fraud eller direktørsvindel. BEC-scams kan medføre betydelige økonomiske tab for den berørte.

I 2016 mistede den østrigske aerospaceproducent Fischer Advanced Composite Components AG eksempelvis 42 mio. euro i et BEC-scam. BEC-scams kan i sin yderste konsekvens påvirke tilgængeligheden af transportydelser, hvis f.eks. en leverandør af trafikydelser eller af kritiske komponenter til transportsektoren mister likviditet i en sådan grad, at den ikke længere kan levere disse ydelser.

Kriminelle begår også andre former for bedrageri mod transportsektoren, eksempelvis kompromittering og misbrug af frequent flyer-konti og konti til delebilstjenester.

Kriminelle hackere går også efter finansielle og personlige oplysninger med henblik på at misbruge dem til økonomisk vinding. Disse kriminelle kan forsøge at kompromittere virksomheder i transportsektoren, der er i besiddelse af sådanne oplysninger. Flere kriminelle hackergrupper går systematisk efter betalingssystemer på tværs af sektorer verden over. Tyveri af personlige og finansielle oplysninger kan som nævnt svække kundernes tillid til ramte virksomheder i sektoren.

Kriminelle spreder også malware, som misbruger ofrets computerkapacitet til at genere kryptovaluta. Malware, der generer kryptovaluta, kan påvirke it-netværk og skabe driftsforstyrrelser, længere svartider og i værste tilfælde nedbrud. I 2018 kom det frem i medierne, at Teslas Amazon Web Services cloudkonto var kompromitteret af hackere, der misbrugte computerkraften til at generere kryptovaluta. I forbindelse med kompromitteringen havde hackerne adgang til følsomme informationer om testbiler.

Cyberspionage

Truslen fra cyberspionage mod transportsektoren er **HØJ**. Det generelle niveau for cyberspionage mod Danmark er meget høj, da fremmede stater vedholdende forsøger at stjæle informationer fra staten og visse sektorer. CFCS har ikke kendskab til et ligeså højt aktivitetsniveau mod transportsektoren, men vurderer, at fremmede stater både har intention og kapacitet til at udføre cyberspionage mod dele af sektoren.

Der er ikke et ensartet trusselsbillede for sektoren. Transportsektoren er som nævnt meget forskelligartet og truslen varierer derfor væsentligt inden for sektoren. CFCS vurderer, at truslen fra cyberspionage er højest for virksomheder og organisationer i sektoren, der beskæftiger sig med udviklingen af nye transportteknologier og konstruktion og drift af avancerede transportsystemer. Truslen er også højest for virksomheder, der er i udbudsrunder eller samarbejder med virksomheder fra visse lande, transporterer militært personel eller udstyr eller er del af national kritisk infrastruktur.

Cyberspionage mod transportsektoren kan bl.a. være motiveret af økonomiske interesser. Ved at stjæle informationer i forbindelse med store investeringer i transportsektoren kan fremmede stater give deres virksomheder fordele på det internationale marked. Nogle lande udfører også cyberspionage mod virksomheder, der samarbejder med deres nationale virksomheder eller myndigheder. Her er der tale om en overvågning af samarbejdspartnere og virksomheder, der kan have en indflydelse på nationale organisationer.

Spionagen kan bl.a. skaffe viden, der kan bruges til at komme i besiddelse af nye teknologier til at styrke og udvikle egen transportsektor. Fremmede stater kan derfor have en interesse i at udføre cyberspionage mod virksomheder og forskningsinstitutioner, der udvikler nye teknologier eller komponenter til transportsektoren. Blandt andet virksomheder relateret til aerospace har i både Danmark og udlandet været mål for cyberspionage. Teknologier og projekter relateret til andre investeringstunge og avancerede transportsystemer såsom højhastighedstog er også potentielle mål for cyberspionage.

Spionage mod transportsektoren kan også være motiveret at sikkerhedspolitiske interesser. Transportsektoren indgår som nævnt i dansk kritisk infrastruktur, og fremmede stater kan derfor have interesse i at opbygge viden om kapaciteter og sårbarheder i transportsektoren, der kan have betydning i forbindelse med eksempelvis en militær konflikt. Indhentning af information om kritisk infrastruktur kan benyttes i forberedelsen af destruktive cyberangreb eller fysiske angreb rettet mod sektoren.

Sektoren ligger også inde med personhenførbare oplysninger om passagerer og rejsemønstre, som fremmede staters efterretningstjenester kan anvende til at følge bestemte personer.

I det omfang at dele af transportsektoren støtter dansk forsvar eller andre landes militær, eksempelvis transport af militært personel til missioner i udlandet eller militær brug af civile trafikknudepunkter såsom lufthavne og havne, kan dette også have fremmede staters interesse.

Cyberaktivisme

Truslen fra cyberaktivisme mod transportsektoren er **MIDDEL**. Cyberaktivisme er typisk drevet af ideologiske eller politiske motiver, og cyberaktivister fokuserer ofte på personer eller organisationer, de opfatter som modstandere af deres sag. Transportsektoren har stor betydning for danskernes hverdag, og angreb på eksempelvis offentlig transport kan skabe opmærksomhed om cyberaktivisters budskaber. Særligt luftfart har været udsat for cyberaktivisme rundt om i verden.

Nogle hackergrupper og individer i cyberaktivistiske netværk har væsentlige evner og ressourcer til at udføre cyberangreb. Mens vi ikke ser mange eksempler på sådanne angreb i Danmark, kan truslen pludseligt stige. Hackere kan hurtigt mobiliseres omkring en sag f.eks. i kølvandet på politiske debatter og hændelser, der involverer transportsektoren. Eksempelvis blev Wiens og Rotterdams lufthavnes hjemmesider ramt af overbelastningsangreb i henholdsvis 2016 og 2017, i begge tilfælde sandsynligvis som følge af politiske sager om tyrkiske borgeres indrejse i de pågældende lande.

Cyberaktivister angriber også myndigheder og virksomheder, som hackerne betragter som symbolske mål, selvom de ikke har været direkte indblandet i den sag, der har fanget hackernes opmærksomhed. Angrebene kan også være tilfældige i den forstand, at hackerne angriber, hvor de kan skaffe sig adgang eller udnytte sårbarheder.

Virksomheder eller myndigheder i transportsektoren kan blive mål for cyberaktivister, der forsøger at få større opmærksomhed på deres sag, da eksempelvis tog- og flyselskabers hjemmesider og informationsskærme på stationer eller i lufthavne har en høj grad af synlighed. I maj 2018 hackede en cyberaktivistisk gruppe eksempelvis informationsskærme i en iransk lufthavn og indsatte politiske budskaber, hvor de kritiserede regeringen. En islamistisk hackergruppe, Caliphate Cyber Army, påstod på sociale medier i 2016 at have slukket for kameraer i Bornholms Lufthavn, samtidigt med at nogen udsendte en række beskeder på Twitter med falske oplysninger om terrorangreb på lufthavnen. Mens der er tale om en udokumenteret påstand, viser det en interesse i lufthavne fra personer og netværk, der forsøger at opnå opmærksomhed.

En anden angrebsform er hack og læk af følsomme oplysninger, der kan skabe opmærksomhed om aktivisternes sag. Eksempelvis lækkede en cyberaktivist i 2016 en stor mængde følsomme data, der ifølge aktivisterne var stjålet fra et russisk flyselskab, i protest mod Ruslands handlinger i Ukraine og Syrien.

Endelig benyttes cyberaktivistiske grupper af visse lande som dække i forsøg på at påvirke den folkelige meningsdannelse i andre lande, eksempelvis ved hack og læk af følsomme oplysninger.

Cyberterror

Truslen fra cyberterror mod transportsektoren er **LAV**. CFCS vurderer, at selvom militante ekstremister i få tilfælde har ytret interesse for at udføre cyberterror generelt, har de aktuelt ikke kapacitet til dette.

Der er derfor en lav trussel også mod transportsektoren i Danmark fra cyberangreb, hvor hensigten er at skabe samme effekt som mere konventionel terror, f.eks. cyberangreb, der forårsager fysisk skade på mennesker eller materiel eller skaber omfattende forstyrrelser af transportsektorens infrastruktur.

Destruktive cyberangreb

En række lande har cyberkapaciteter, der potentielt kan bruges destruktivt mod samfundsvigtig infrastruktur såsom transportsektoren. CFCS definerer et destruktivt cyberangreb som et cyberangreb, hvor den forventede effekt er død, personskade, betydelig skade på fysiske objekter eller ødelæggelse eller forandring af informationer, data eller software, så de ikke kan anvendes uden væsentlig genopretning.

CFCS vurderer, at det er mindre sandsynligt, at fremmede stater har til hensigt at ramme dansk samfundsvigtig infrastruktur, herunder transportsektoren, med destruktive cyberangreb. Truslen kan stige i forbindelse med en skærpet politisk eller militær konflikt, hvor Danmark deltager.

På nuværende tidspunkt er det dog muligt, at danske myndigheder og virksomheder kan blive ramt som følgevirkning af destruktive cyberangreb mod mål uden for Danmark. Det gælder især danske virksomheder fra bl.a. transportsektoren, der er til stede i konfliktområder, hvor fremmede stater eller organiserede hackergrupper med kapacitet til at udføre destruktive cyberangreb har interesser, såsom i dele af Østeuropa, Mellemøsten og Sydøstasien.

I udlandet er transportsektoren blevet ramt af destruktive cyberangreb, som i mindre grad forstyrrede sektorens tilgængelighed. I juni 2017 blev flere virksomheder i transportsektoren i udlandet ramt af NotPetya-angrebet, der sandsynligvis var et destruktivt cyberangreb forklædt som ransomware.
I Ukraine blev Kiev metro og to lufthavne påvirket af angrebet. Logistikvirksomhederne FedEx og Deutsche Post DHL Group og DAMCO blev ramt med store økonomiske tab. Senere i 2017 ramte den såkaldte BadRabbit-malware bl.a. transportsektoren i Ukraine. Angrebet medførte bl.a. flyforsinkelser i Odessa lufthavn og nedbrud i billetsystemet i Kievs metro.

It-sikkerhedsspecialister og statslige sikkerhedstjenester har demonstreret, hvordan f.eks. biler eller fly kan hackes, så centrale systemer kan kontrolleres af hackerne. De fleste af disse angreb kan kun lykkes under bestemte forhold. Det er dog muligt, at bl.a. statsstøttede hackere har kapaciteten til at udnytte sårbarhederne.

Trusselsniveauer

Forsvarets Efterretningstjeneste bruger følgende trusselsniveauer.

INGEN	Der er ingen indikationer på en trussel. Der er ikke erkendt kapacitet eller hensigt. Angreb/skadevoldende aktivitet er usandsynlig.
LAV	Der er en potentiel trussel. Der er en begrænset kapacitet og/eller hensigt. Angreb/skadevoldende aktivitet er mindre sandsynlig.
MIDDEL	Der er en generel trussel. Der er kapacitet og/eller hensigt og mulig planlægning. Angreb/skadevoldende aktivitet er mulig.
HØJ	Der er en erkendt trussel. Der er kapacitet, hensigt og planlægning. Angreb/skadevoldende aktivitet er sandsynlig.
MEGET HØJ	Der er en specifik trussel. Der er kapacitet, hensigt, planlægning og mulig iværksættelse. Angreb/skadevoldende aktivitet er meget sandsynlig.

FE bruger denne skala for sandsynlighed i analyser: