Styrelsen for Samfundssikkerhed

TRUSSELSVURDERING

Cybertruslen mod transportsektoren

April • 2025

Indhold

Cybertruslen mod transportsektoren 3

Hovedvurdering 3

Indledning 4

Cyberspionage 6

Cyberkriminalitet 8

Cyberaktivisme 10

Destruktive cyberangreb 13

Cyberterror 16

Trusselsniveauer 17

Andre relevante publikationer 18

Datavej 20
3460 Birkerød
Telefon: + 4516 1666
E-mail: samsik@samsik.dk

April 2025

Cybertruslen mod transportsektoren

Formålet med denne trusselsvurdering er at beskrive cybertruslen rettet mod den danske transportsektor. Vurderingen kan styrke risikoejeres forståelse af cybertruslen og bl.a. indgå som en del af grundlaget for risikovurderingsarbejdet i sektoren.

Vurderingen erstatter "Cybertruslen mod land- og lufttransport", der blev udgivet i 2018 og løbende er blevet opdateret, "Cybertruslen mod dansk luftfart" og "Cybertruslen mod jernbanesektoren" og supplerer "Cybertruslen mod danske havne og logistikvirksomheder" fra 2023.

Hovedvurdering

- Truslen fra cyberspionage mod den danske transportsektor er **MEGET HØJ.** Truslen fra cyberspionage kan variere og er eksempelvis påvirket af, om en virksomhed understøtter Forsvaret eller indsatsen til støtte af Ukraine.
- Truslen fra cyberkriminalitet mod den danske transportsektor er **MEGET HØJ.** Særligt ransomware-angreb og datatyveri udgør trusler mod transportsektoren.
- Truslen fra cyberaktivisme mod den danske transportsektor er **HØJ**. Transportsektoren er blandt de mest udsatte mål, når det kommer til pro-russisk cyberaktivisme, der aktuelt dominerer det cyberaktivistiske trusselsbillede i Danmark.
- Truslen fra destruktive cyberangreb mod den danske transportsektor er **MIDDEL.** Det skyldes, at Rusland både har kapacitet til og intention om at bruge hybride virkemidler med destruktive effekter i europæiske NATO-lande.
- Truslen fra cyberterror mod den danske transportsektor er **INGEN**.

Indledning

Cybertruslen mod transportsektoren har, ligesom den generelle trussel mod Danmark, været omfattende siden den første trusselsvurdering for sektoren i 2018. Siden da har trusselsbilledet udviklet sig og er kun blevet mere komplekst. Transportsektoren skal forsvare sig mod statslige aktører, cyberkriminelle grupper og aktivister, der med forskellige hensigter angriber virksomheder og myndigheder i sektoren, både målrettet og mere vilkårligt.

Transportsektoren består af flere grupper af aktører, der hver især kan siges at udgøre delsektorer i den samlede transportsektor. De har alle forhold, systemer og sårbarheder, der er særlige for dem. Tidligere har cybertruslen mod transport sektoren været beskrevet i selvstændige trusselsvurderinger. For eksempel er der bl.a. udgivet vurderinger for hhv. jernbanesektoren og luftfartsektoren. Der er imidlertid meget af trusselsbilledet, der gør sig gældende som fælles vilkår i hele sektoren, og Styrelsen for Samfundssikkerhed (SAMSIK) vurderer derfor, at en samlet trusselsvurdering for transportsektoren er både relevant og retvisende. Trusselsvurderingen her dækker derfor den samlede transportsektor. Søfart er ikke medtaget, da søfart behandles som en selvstændig sektor af de danske myndigheder. Hvor trusselsvurderingen giver anledning til særlige bemærkninger for den enkelte delsektor, vil det fremgå af teksten.

Krigen i Ukraine og konflikten mellem Rusland og Vesten udgør fortsat en drivkraft bag store dele af cybertruslen. Konflikten har haft indflydelse på truslerne fra cyberspionage, cyberaktivisme og destruktive cyberangreb. Eksempelvis har pro-russisk cyberaktivisme flere gange ramt forskellige dele af transportsektoren i Danmark siden Ruslands invasion i februar 2022.

Et andet fællesvilkår i sektoren med stor betydning for cybertruslen er den stadigt større afhængighed af digitale systemer. Som i resten af Danmark er det en logisk udvikling i transportsektoren, at flere systemer, som før har været analoge, nu bliver afhængige af IT og koblet til internettet. Samtidigt kobles flere og flere nye enheder til internettet, såsom overvågningskameraer og sensorer. Det øger antallet af potentielle angrebsflader og flere systemer er sårbare overfor cyberangreb.

Systemnedbrud lammede togtrafikken

En synkroniseringsfejl i Banedanmarks digitale signalsystem påvirkede i november 2024 store dele af togdriften i Jylland med forsinkelser og aflysninger til følge. Selvom det ifølge Banedanmark ikke var et cyberangreb, der var årsag til fejlen, understreger hændelsen, hvilke konsekvenser det kan få for togdriften, hvis digitale systemer bliver utilgængelige.

Meget drift i sektoren afhænger desuden af, at en række systemer hver især er operative. I en lufthavn er der f.eks. systemer, der styrer paskontrol, billetter og bagagehåndtering, som alle er vigtige for, at passagererne kan komme med et fly til tiden. Sådanne systemer kan hver især være sårbare overfor cyberangreb, hvis de enten direkte eller indirekte er koblet til internettet.

Ikke alene er mange danskere afhængige af transportsektoren, men der er også en høj grad af intern afhængighed i sektoren. Lufthavnens passagerer er afhængige af luftfartsselskabet og af, at metro, tog og busser kører som planlagt. Samtidigt er andre kritiske sektorer også afhængige af transportsektoren. Derfor er det vigtigt, at sektoren samlet set har opmærksomhed på cybertruslen.

Trusselsvurderingen tager udgangspunkt i det aktuelle trusselsbillede. Cybertruslen er dynamisk, og trusselsbilledet kan ændre sig hurtigt både generelt og for den enkelte myndighed eller virksomhed. Vurderingen anvender Forsvarets Efterretningstjenestes trusselsniveauer og sandsynlighedsgrader, der er forklaret i slutningen af vurderingen.

Vurderingen tager afsæt i analyser af danske og internationale eksempler på cyberangreb mod transportsektoren. Det sammenholdes med viden om trusselsaktørers kapacitet og intention. Trusselsvurderingen er udarbejdet bl.a. på baggrund af dialog med flere virksomheder i transportsektoren.

Transportsektoren i Danmark

Transportsektoren i Danmark består af mange forskellige typer af organisationer. I denne trusselsvurdering anses alle myndigheder og virksomheder, der direkte eller indirekte leverer transportydelser, eller arbejder med regulering af området, som en del af transportsektoren.

Det er for eksempel jernbane- og luftfartsvirksomheder, havne, logistikvirksomheder, private vognmænd, busselskaber, forvaltere af vej-, bane- og broinfrastruktur og øvrige transportmyndigheder. Dog er søfart ikke medtaget, da søfart behandles som en selvstændig sektor af de danske myndigheder.

Vurderingerne heri er som udgangspunkt foretaget for hele transportsektoren. I de tilfælde hvor vurderingen er særligt relevant for specifikke dele af sektoren, skriver vi det. Vurderingen beskriver også de særlige forhold, der kan øge cybertruslen for den enkelte virksomhed eller myndighed.

Cyberspionage

Truslen fra cyberspionage mod transportsektoren er **MEGET HØJ**, og SAMSIK har kendskab til flere forsøg på cyberspionage mod aktører i sektoren både i Danmark og i udlandet. Det er meget sandsynligt, at myndigheder og virksomheder i den danske transportsektor vil blive udsat for forsøg på cyberspionage inden for de næste to år.

SAMSIK har tidligere udgivet trusselsvurderinger på delsektorniveau i transportsektoren, hvor trusselsniveauerne for cyberspionage har varieret. Den nuværende vurdering er dog, at truslen fra cyberspionage mod den samlede transportsektor er **MEGET HØJ**. Truslen kan variere mellem de enkelte virksomheder afhængigt af de specifikke forhold, der aktuelt driver truslen fra cyberspionage.

Truslen afhænger særligt af, hvorvidt en virksomhed aktuelt eller potentielt ligger inde med viden, som har fremmede staters interesse. Eksempler herpå kan være, hvis en virksomhed indgår en kontrakt med et lands forsvar, indgår i en militær øvelse eller spiller en rolle i forhold til ny forskning eller innovation. Truslen fra cyberspionage kan også blive rettet mod transportvirksomheder, der ligger inde med persondata om passagerer og deres rejsemønstre, som fremmede staters efterretningstjenester kan anvende til at følge bestemte personer.

SAMSIK vurderer, at statslige hackere forbereder sig på at kunne udføre destruktive cyberangreb mod Danmark – bl.a. ved hjælp af cyberspionage. Det er dog ikke alle destruktive cyberangreb, der kræver forudgående cyberspionage.

Sikkerhedspolitiske forhold er en drivkraft bag spionagetruslen
Fremmede stater, herunder Rusland og Kina, har en vedvarende interesse for viden om andre landes udenrigs-, sikkerheds- og forsvarspolitik.

Myndigheder og virksomheder i transportsektoren er særligt udsatte for truslen fra cyberspionage, hvis de understøtter dansk forsvar, NATO-samarbejdet eller andre landes militær. Truslen kan være skærpet, hvis en virksomhed er til stede i områder af geopolitisk interesse for fremmede stater, som konfliktområder og Arktis. SAMSIK vurderer, at dette kan have indvirkning på truslen mod eksempelvis danske logistikvirksomheder.

Krigen i Ukraine påvirker også truslen fra cyberspionage mod transportsektoren. Det er sandsynligt, at Rusland vil forsøge at tilegne sig viden om støtte til Ukraine fra danske transportvirksomheder og myndigheder, og virksomheder i sektoren kan blive udsat for forsøg på cyberspionage, hvis de potentielt eller aktuelt understøtter forsyningskæden af donationer til Ukraine. Rusland kan eksempelvis have en interesse i at få adgang til viden om leverancernes indhold, transportruter og logistiske knudepunkter.

Fremmede stater spionerer også for at styrke teknologiske og økonomiske udviklingsmål

Fremmede stater, herunder særligt Kina, udfører vedvarende forsøg på cyberspionage verden over for at understøtte egne økonomiske og teknologiske udviklingsmål.

Teknologisk og økonomisk motiveret spionage retter sig globalt i transportsektoren særligt mod virksomheder, som beskæftiger sig med udviklingen af nye transport-teknologier eller konstruktion og drift af avancerede transportsystemer. SAMSIK har kendskab til flere eksempler på cyberspionage mod mål i luftfartssektoren og jernbanesektoren i udlandet, der potentielt udgør mål for teknologisk og økonomisk motiveret cyberspionage.

Er en virksomhed i besiddelse af viden om eller involveret i større udbudsprocesser af national betydning, kan det også have fremmede staters interesse. Viden om ny teknologi, store investeringer og konkurrencemæssige forhold fra udbudsprocesser kan bruges af fremmede stater til at styrke deres position på det internationale marked og forvride konkurrencen i deres favør.

Cyberkriminalitet

Truslen fra cyberkriminalitet mod transportsektoren i Danmark er **MEGET HØJ**. Truslen mod sektoren følger det generelle trusselsniveau for cyberkriminalitet i Danmark. SAMSIK vurderer, at det er meget sandsynligt, at virksomheder i transportsektoren i Danmark vil blive ramt af forsøg på cyberkriminalitet inden for de næste to år.

SAMSIK bruger begrebet cyberkriminalitet som en fællesbetegnelse for handlinger, hvor hackere bruger cyberangreb til at begå kriminalitet, der er motiveret af økonomisk berigelse. Særligt ransomware-angreb og datatyveri udgør trusler for transportsektoren, da disse typer angreb er udbredte angrebsmetoder på tværs af de samfundsvigtige sektorer.

Myndigheder og virksomheder i transportsektoren kan blive udsat for cyberkriminalitet af mange årsager. Der er i sektoren virksomheder med høje omsætninger, som kan opfattes som værende i stand til at udbetale store løsesummer. Et ransomware-angreb mod en transportvirksomhed kan også skabe driftsforstyrrelser, og nogle kriminelle går bevidst efter denne effekt for at styrke deres forhandling om løsesum. Virksomheder i transportsektoren kan desuden ligge inde med værdifulde data, der gør dem udsatte overfor cyberkriminelles afpresning via datatyveri.

Ransomware-angreb kan skabe driftsforstyrrelser
Ransomware-angreb, hvor kriminelle forsøger at afpresse ofret ved at gøre deres data eller systemer utilgængelige, ofte ved at kryptere data, er en udbredt metode blandt cyberkriminelle. Lykkes cyberkriminelle med et ransomware-angreb, kan det give store økonomiske tab, skade offerets omdømme og svække tilliden fra dets kunder. Der har de seneste år også været eksempler på ransomware-angreb, der har skabt driftsforstyrrelser hos ofre i transportsektoren i udlandet.

I sommeren 2023 blev Japans største havn, Nagoya havn, ramt af et ransomware-angreb, der forårsagede driftsforstyrrelser på havnen i flere dage. Ifølge flere medier låste ransomwaren den it-infrastruktur, som understøttede det computersystem, der styrede lastning og losning af containere på havnens skibe. Det resulterede i, at havnens fem containerterminaler ikke kunne operere i to dage. Idet havnen håndterer 10% af Japans import og eksport af varer, kunne angrebet mærkes verden over.

Angrebet på Nagoya havn er et eksempel på, at ransomware kan forårsage driftsstop ved at kryptere nogle af de it-systemer, der er forbundne til driften. Langt de fleste driftstop i forbindelse med ransomware har dog været tilfælde, hvor offeret selv stopper driften for at undgå, at cyberangrebet spreder sig.

Afpresning uden kryptering kan skade virksomheder på lang sigt
Der har de seneste år været flere eksempler på, at datatyveri, særligt i form af tyveri af følsomme personoplysninger, har ramt virksomheder i transportsektoren i udlandet.

Ved datatyveri kan hackere forsøge at afpresse offeret uden at kryptere data eller systemer. Selvom denne type angreb ikke påvirker driften i samme grad, som hvis data blev krypteret, kan det stadig skade offeret. Det kan resultere i konsekvenser såsom GDPR-bøder, tab af omdømme og derved af kunder eller markedsværdi.

Mange virksomheder i transportsektoren ligger inde med værdifulde data, eksempelvis personoplysninger om medarbejdere eller passagerdata, følsomme systemoplysninger, regnskabsoplysninger eller andet, der gør dem til mulige mål for den type angreb.

Enhver kompromittering kan potentielt udvikle sig til større angreb
Det høje trusselsniveau understøttes af, at en del af det cyberkriminelle miljø er robust og professionelt organiseret. Grupper og individer samarbejder og handler med hinanden på tværs af landegrænser. Samarbejdet øger de kriminelles kapaciteter, bl.a. fordi de har mulighed for at specialisere sig og effektivisere deres angreb. Det betyder eksempelvis, at kriminelle, som er gode til at skaffe sig adgange til systemer, kan sælge adgangene videre til andre kriminelle, som herefter kan gennemføre et videre angreb. Derfor kan en kompromittering, der umiddelbart virker begrænset i omfang, udvikle sig til et alvorligt angreb senere, hvis adgangen sælges videre og offeret ikke når at lukke adgangen i tide. SAMSIK har kendskab til en række eksempler på, at cyberkriminelle har forsøgt at sælge adgange til udenlandske transportvirksomheders netværk.

Cyberaktivisme

Truslen fra cyberaktivisme mod den danske transportsektor er **HØJ**. Det er meget sandsynligt, at myndigheder og virksomheder i sektoren bliver ramt af aktivistiske cyberangreb inden for de næste to år. Truslen fra cyberaktivisme retter sig bredt mod sektoren på tværs af delsektorer. Både transportmyndigheder og aktører inden for luftfart, jernbane og havne har gentagne gange været ramt af cyberaktivistiske angreb i løbet af de seneste år.

Cyberaktivister er politisk eller ideologisk motiverede grupper og individer, som udfører cyberangreb for at skabe opmærksomhed omkring en sag. Angrebene kan også være udtryk for et ønske om at straffe organisationer, virksomheder eller lande, som cyberaktivisterne opfatter som politiske modstandere.

Transportsektoren er et populært mål blandt cyberaktivister
SAMSIK vurderer, at transportsektoren er blandt de mest udsatte sektorer, når det kommer til cyberaktivisme. Flere cyberaktivistiske grupper rettede eksempelvis en lang række angreb mod især mål i transportsektoren i flere europæiske lande i forbindelse med Europaparlamentsvalget i juni 2024.

Transportsektoren er sandsynligvis et oplagt mål for cyberaktivistisk aktivitet, fordi mange brugervendte hjemmesider i sektoren har stor synlighed og potentielt bruges af mange mennesker dagligt. Dette øger muligheden for at skabe opmærksomhed om et angreb, hvis det eksempelvis lykkes at blokere for adgangen til en hjemmeside, der sælger billetter eller indeholder rejse- og trafikinformation, som mange rejsende er afhængige af.

Transportsektoren er desuden et mål i kraft af sin samfundsvigtige funktion. Nogle cyberaktivistiske aktører fremhæver netop denne årsag, når de italesætter deres angreb. Et angreb på kritisk infrastruktur kan være et forsøg på at signalere, at man kan ramme sine politiske modstandere et sted, der er sårbart for deres samfund.

En høj trussel med begrænset effekt
Cyberaktivister anvender i overvejende grad Distributed Denial of Service-angreb (DDoS)-angreb mod danske virksomheder og myndigheder. Aktivisterne retter typisk angrebene mod brugervendte hjemmesider. DDoS-angreb kan gøre hjemmesiderne midlertidigt utilgængelige ved, at hjemmesiderne overbelastes med ondsindet trafik, så de ikke kan tilgås.

DDoS-angreb har en forstyrrende effekt, men er ikke ødelæggende for ofrenes systemer. Nedetid på brugervendte hjemmesider i transportsektoren kan dog være generende og påvirke kundekontakten og forretningen midlertidigt ved eksempelvis at blokere for muligheden for at anmelde et skib i en havn eller købe en togbillet. Nedetiden på ofrenes hjemmesider er desuden ofte med til at skabe omtale af aktivisternes dagsorden.

Cyberaktivisme kan være andet end DDoS
Selvom det primært er DDoS-angreb, der fylder i trusselsbilledet, udfører nogle cyberaktivister også andre former for cyberangreb.

For eksempel er det sandsynligt, at aktivistiske hackere udførte et destruktivt cyberangreb mod et dansk vandværk i december 2024. Der var tale om et simpelt angreb mod dårlig beskyttede systemer, som resulterede i, at adskillige kunder fik forstyrret deres vandforsyning. Aktivistiske grupper har flere gange tidligere påstået at have udført angreb i udlandet som det, der ramte det danske vandværk.

SAMSIK vurderer, at denne form for cyberaktivistiske angreb af destruktiv karakter er opportunistiske i forhold til måludpegning og rammer mål med lav beskyttelse. Omfanget af disse destruktive, aktivistiske cyberangreb med begrænset effekt er dog fortsat småt sammenlignet med de mange DDoS-angreb, som rammer mål i Danmark og Vesten.

Cyberaktivister overdriver for at skabe opmærksomhed

Aktivistiske hackeres kommunikation omkring deres angreb er ofte misvisende og overdreven. Dette betyder, at der i mange tilfælde er usikkerhed om, hvorvidt cyberaktivistiske angreb har fundet sted samt hvilken effekt angrebene har haft.

SAMSIK vurderer, at aktivisters kommunikation om både falske og reelle angreb har til hensigt at skabe offentlig opmærksomhed omkring deres dagsorden. De cyberaktivistiske grupper søger således omtale i vestlige medier og deler vestlige, herunder danske, mediers artikler om gruppernes egne angreb.

Selvom SAMSIK er bekendt med gruppernes navne, bliver de derfor ikke nævnt i publikationer, medmindre det er afgørende for at give et retvisende trusselsbillede.

Pro-russiske aktivister dominerer fortsat trusselsbilledet
Det høje trusselsniveau for cyberaktivistiske angreb i Danmark og transportsektoren drives især af pro-russiske cyberaktivister, der i kontekst af konflikten i Ukraine udpeger deres mål i EU- og NATO-medlemslande, der støtter Ukraine. Det er kendetegnende for især de pro-russiske cyberaktivister, at deres ofre sjældent spiller nogen rolle i den konkrete sag, der motiverer cyberaktivisternes angreb. De cyberaktivistiske grupper, der aktuelt dominerer trusselsbilledet i Danmark, italesætter således oftest angrebene mod deres mål som en hævn over Danmark som land, og de enkelte mål bliver sandsynligvis udvalgt alene som symbolske mål.

Dele af det cyberaktivistiske miljø besidder ressourcer og kapaciteter til at igangsætte angreb med kort varsel. Derfor har konkrete politiske begivenheder potentielt betydning for truslen, som kan ændre sig med kort varsel. Det var eksempelvis tilfældet, da en pro-russisk aktivistisk gruppe hævdede at have rettet et DDoS-angreb mod Din Offentlige Transports (DOT) hjemmeside i februar i 2024. Ifølge gruppen kom angrebet som reaktion på, at de i Jyllandsposten havde læst, at statsminister Mette Frederiksen på en sikkerhedskonference i München et par dage tidligere havde opfordret EU's medlemslande til at sende våben fra deres lagre til Ukraine.

De pro-russiske grupper er et godt eksempel på, hvordan cyberaktivister kan understøtte staters interesser. Det er dog ikke ensbetydende med, at de arbejder direkte for staten. SAMSIK vurderer, at nogle pro-russiske cyberaktivister har forbindelse til den russiske stat.

Selvom truslen fra cyberaktivisme mod Danmark primært udspringer fra pro-russiske aktivister, kan truslen også opstå fra andre cyberaktivistiske miljøer. Det var eksempelvis tilfældet ved den internationale opmærksomhed omkring koranafbrændingerne i Danmark og Sverige i starten af 2023. Som reaktion på afbrændingerne iværksatte flere cyberaktivistiske grupper DDoS-angreb mod danske og svenske hjemmesider. Samtidig opfordrede de også andre aktivister til at begå cyberangreb mod danske og svenske mål. I denne periode blev danske lufthavne- og luftfartsselskabers hjemmesider gentagne gange ramt af DDoS-angreb.

Destruktive cyberangreb

Truslen fra destruktive cyberangreb mod transportsektoren er **MIDDEL**. Truslen fra destruktive cyberangreb blev i juni 2024 hævet fra **LAV** til **MIDDEL** for Danmark generelt, og SAMSIK vurderer, at niveauet også gælder for transportsektoren.

Trusselsniveauet er **MIDDEL**, fordi Rusland er villig til at bruge hybride virkemidler med destruktive effekter mod europæiske NATO-lande. SAMSIK vurderer, at dette også indbefatter destruktive cyberangreb. Rusland har i årevis haft kapaciteten til at udføre destruktive cyberangreb. Netop fordi Rusland har kapaciteten til at udføre destruktive angreb, er det kun hensigten, der skal ændre sig, for at truslen ændrer karakter. Truslen fra destruktive cyberangreb kan derfor stige med kort eller ingen varsel. Det kan f.eks. ske, hvis den sikkerhedspolitiske situation eskalerer i retning af en militær konfrontation mellem Rusland og NATO.

Hvad er destruktive cyberangreb?

SAMSIK definerer destruktive cyberangreb som cyberangreb, hvor den forventede effekt er:

- Død eller personskade,
- Betydelig skade på fysiske objekter eller
- Ødelæggelse eller forandring af information, data eller software, så de ikke kan anvendes uden væsentlig genopretning.

Destruktive cyberangreb skal påvirke befolkning og beslutningstagere
SAMSIK vurderer, at et destruktivt cyberangreb vil have til formål at påvirke befolkning og beslutningstagere, eksempelvis ved at forsøge at svække danskernes opbakning til Ukraine.

Den konkrete fysiske effekt af angrebene vil sandsynligvis være sekundær i forhold til, om angrebene skaber opmærksomhed, fordi det primære formål med et angreb vil være påvirkning. Dette åbner op for en lang række potentielle mål, men udvælgelsen vil sandsynligvis være påvirket af, hvor hackerne har adgang eller nemt kan få det.

Transportsektoren kan udgøre et attraktivt mål for destruktive cyberangreb af flere årsager. Sektoren har en stor synlighed og berøringsflade med borgerne hver dag og transport understøtter en række helt kritiske funktioner i samfundet, fra centrale forsyningskæder til transport af den enkelte borger og dermed den samlede arbejdsstyrke. Derudover har dele af transportsektoren også berøring med Forsvaret og understøtter transporten af danske donationer til Ukraine. Der kan være stor signalværdi i at rette et destruktivt cyberangreb mod disse funktioner.

Destruktive angreb kan få betydelige konsekvenser
Det er mindre sandsynligt, at Rusland i den nuværende sikkerhedspolitiske situation vil gennemføre destruktive cyberangreb, hvor hensigten er at skabe alvorlige og omfattende konsekvenser for samfundsvigtige funktioner. Mindre omfattende cyberangreb kan dog stadig få betydelige konsekvenser for offeret og for samfundet. Det kan f.eks. være angreb, der påvirker samfundsvigtige funktioner i begrænset omfang. I transportsektoren kunne dette eksempelvis komme til udtryk ved angreb, der skaber aflysninger, forsinkelser og kødannelser i den offentlige transport eller lufthavnene i dele af landet. Det er effekter, som potentielt vil kunne mærkes af mange mennesker og skabe utryghed, men ikke have mere alvorlige konsekvenser i form af død eller personskade eller omfattende forsinkelser i store dele af landet. Men selv hvis destruktive cyberangreb kun har begrænsede konsekvenser for samfunds-vigtige funktioner, kan de skabe utryghed og påvirke samfundet.

Russiske hackergrupper har før stået bag flere destruktive cyberangreb mod Ukraine og sandsynligvis også mod andre lande. Ukraine har eksempelvis været udsat for angreb, hvor operationelle systemer i kritisk infrastruktur er blevet manipuleret, hvilket har medført strømafbrydelser. Langt størstedelen af de destruktive cyber-angreb, som Rusland har udført i Ukraine, har dog været såkaldte wiper-angreb. Wiper-malware sletter eller krypterer filer på det system eller netværk, det rettes imod. Wiper-angreb kan få alvorlige konsekvenser for ofrene, eksempelvis hvis centrale systemer eller data bliver utilgængelig og må genoprettes fra bunden.

Sandworms interesse for logistikvirksomheder

I Polen og Ukraine blev flere logistikvirksomheder i oktober 2022 ramt af et ransomware-lignende angreb, som ifølge Microsoft er udført af den russiske statsstøttede hackergruppe Sandworm. De krypterede data kunne efterfølgende ikke genskabes, hvorfor angrebet er blevet kategoriseret som et destruktivt cyberangreb. Angrebet, med en malware kaldet Prestige, blev rettet mod flere forskellige logistikvirksomheder på tværs af de to lande og blev udført hen over en periode på få timer.

Ruslands øgede risikovillighed vil også kunne komme til udtryk som omfattende DDoS-angreb mod centrale systemer. DDoS-angreb er ikke destruktive, men omfattende DDoS-angreb mod centrale systemer vil potentielt kunne afbryde eller forstyrre samfundsvigtige funktioner i kortere eller længere tid. Den type angreb vil derved kunne påvirke befolkningen og beslutningstagere på samme måde som destruktive cyberangreb.

Truslen kan være skærpet i konfliktområder
SAMSIK vurderer, at der nær konfliktområder er en øget risiko for, at destruktive cyberangreb kan sprede sig og ramme ofre uden for selve konfliktzonen. Det er muligt, at danske transportvirksomheder, der er til stede i og omkring konfliktområder, hvor fremmede stater med kapacitet til at udføre destruktive cyberangreb er aktive, vil blive ramt af destruktive cyberangreb eller følgevirkninger deraf. Det kunne eksempelvis være i form af strømafbrydelser og manglende internetadgang.

Stater udvikler løbende deres kapacitet til at udføre destruktive cyberangreb
SAMSIK vurderer, at fremmede stater løbende udvikler deres kapaciteter til at kunne udføre destruktive cyberangreb med kort varsel. Stater bruger bl.a. cyberspionage til at forberede destruktive cyberangreb, der f.eks. vil kunne iværksættes i tilfælde af en eskalerende krise eller krig.

Forberedelsen af destruktive cyberangreb vil ofte bestå i en kortlægning af organisationer, systemer og netværksenheder. Ved at opnå viden om organisationer og systemer kan hackere bl.a. udvikle specialiseret malware. Derudover kan hackere etablere såkaldte bagdøre på kompromitterede systemer, som de kan benytte i senere destruktive angreb. Hvis hackere allerede har en bagdør i et system, vil de hurtigere kunne iværksætte et destruktivt angreb mod systemet.

Cyberspionage vil ofte være en del af forberedelsen af destruktive cyberangreb, men er ikke en forudsætning for dem alle. Hackere kan i nogle tilfælde med begrænset forberedelse udføre simple, destruktive cyberangreb mod systemer med dårlig beskyttelse.

Andre aktører udgør også en potentiel trussel
Ikke-statslige hackere kan også udgøre en potentiel trussel. Det skyldes blandt andet, at stater kan forsøge at sløre deres involvering i et destruktivt cyberangreb ved at få kriminelle eller aktivistiske hackere til at udføre angrebene for dem.

Samtidig vurderer SAMSIK, som nævnt, at visse cyberaktivistiske grupper har intentioner om at udføre cyberangreb med destruktiv effekt. Det er dog kun i få tilfælde, at en reel effekt fra et cyberaktivistisk destruktivt angreb er blevet bekræftet, og SAMSIK vurderer generelt, at aktivisternes evne til at udføre den type angreb er begrænset sammenlignet med fremmede staters. De udgør derfor primært en trussel mod organisationer med svage sikkerhedsforanstaltninger.

Aktivister udførte destruktive cyberangreb mod Danmark

Et mindre dansk vandværk blev i slutningen af 2024 ramt af et destruktivt cyberangreb fra pro-russiske cyberaktivister. Ved angrebet blev vandværkets operationelle systemer manipuleret, hvilket medførte, at 450 husstande kortvarigt ikke havde vand på grund af lavt vandtryk. Efterfølgende var ca. 50 husstande uden vand i adskillige timer, da et vandrør sprang som følge af forhøjet vandtryk. SAMSIK vurderer, at vandværket blev ramt på grund af systemernes ringe beskyttelsesniveau, og dermed ikke fordi man gik målrettet efter vandsektoren.

Cyberterror

Truslen fra cyberterror mod transportsektoren er **INGEN**. Det er usandsynligt, at den danske transportsektor vil blive udsat for forsøg på cyberterror inden for de næste to år.

SAMSIK definerer cyberterror som cyberangreb, hvor hensigten er at skabe samme effekt som ved konventionel terror, f.eks. cyberangreb, der forårsager fysisk skade på mennesker eller omfattende forstyrrelser af kritisk infrastruktur.

SAMSIK vurderer, at militante ekstremister har begrænset hensigt til at udføre cyberangreb med samme effekt som konventionel terror, samt at de ikke har den fornødne kapacitet.

Trusselsniveauer

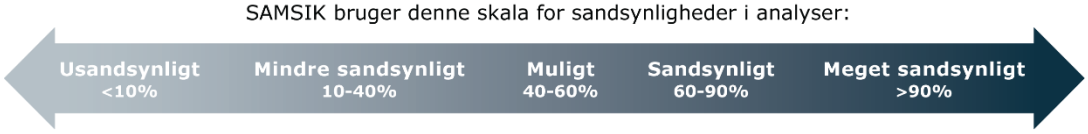
Styrelsen for Samfundssikkerhed anvender i sine trusselsvurderinger Forsvarets Efterretningstjenestes (FE) trussels- og sandsynlighedsniveauer.

Forsvarets Efterretningstjeneste bruger følgende trusselsniveauer:

INGEN	Der er ingen tegn på en trussel. Der er ingen aktør, der både har kapacitet til og intention om angreb/skadelig aktivitet.
LAV	En eller flere aktører har kapacitet til og intention om angreb/skadelig aktivitet. Men enten er kapaciteten eller intentionen eller begge dele begrænset.
MIDDEL	En eller flere aktører har kapacitet til og intention om angreb/skadelig aktivitet. Men der er ikke indikationer på specifik planlægning af angreb/skadelig aktivitet.
HØJ	En eller flere aktører har kapacitet til og foretager specifik planlægning af angreb/skadelig aktivitet, eller har allerede gennemført eller forsøgt angreb/skadelig aktivitet.
MEGET HØJ	Der er enten oplysninger om, at en eller flere aktører iværksætter angreb/skadelig aktivitet, herunder oplysninger om tid og mål, *eller* en eller flere aktører iværksætter kontinuerligt angreb/skadelig aktivitet.

Et givent trusselsniveau er udtryk for SAMSIK's vurdering af aktørers intention, kapacitet og aktivitet på baggrund af de tilgængelige oplysninger.

SAMSIK bruger denne skala for sandsynligheder i analyser:



En sandsynlighedsgrad er udtryk for et skøn, ikke en beregnet statistisk sandsynlighed.
"SAMSIK vurderer" svarer til "Sandsynligt", medmindre en anden sandsynlighed er angivet.

Andre relevante publikationer

Nedenfor fremgår en række af de publikationer, som kan være relevante for organisationer i den danske telesektor. Publikationerne kan tilgås på WWW.SAMSIK.DK.

Cybertruslen mod Danmark 2024
I denne årlige trusselsvurdering beskrives den generelle cybertrussel for hhv. cyberkriminalitet, cyberspionage, cyberaktivisme, destruktive cyberangreb og cyberterror mod Danmark.

Cybertruslen mod danske havne og logistikvirksomheder
I denne trusselsvurdering fra april 2023 beskrives cybertruslen mod danske erhvervshavne og logistikvirksomheder.

Cybertruslen mod IoT-enheder
Trusselsvurderingen beskriver cybertruslen mod IoT-enheder, inkl. netværksudstyr, der ligesom almindelige it-systemer rammes af cyberangreb.

Anatomien af et målrettede ransomware-angreb
Denne rapport kortlægger, hvordan særligt målrettede ransomware-angreb typisk forløber, og giver konkrete anbefalinger til, hvordan myndigheder og virksomheder kan beskytte sig endnu bedre.

Et wiper-angrebs anatomi
Rapporten belyser, hvordan den klart mest udbredte type destruktive cyberangreb, wiper-angreb, fungerer, og hvordan du forsvarer dig imod dem.

Logning – en del af et godt cyberforsvar
Vejledningen giver gode råd til, hvor i netværket man skal logge og hvad man bør logge. Den bygger på erfaringer fra bl.a. it-sikkerhedsfirmaer i forbindelse med bistand ved hændelseshåndtering.

Vejledning om cybersikkerhed i leverandørforhold
Vejledningen "Cybersikkerhed i leverandørforhold" giver gode råd til, hvordan man kan oprette og bibeholde et godt samarbejde mellem kunden og leverandøren af it-driften, gennem hele samarbejdsperioden. Fra valg af leverandør til ophør af samarbejdet.

Vejledning om password-sikkerhed
Vejledningen beskriver nogle af de angrebsmetoder, som hackere benytter sig af, samt nogle af de eksisterende udfordringer ved passwords. Vejledningen indeholder desuden en række konkrete anbefalinger til, hvordan man – på forskellige niveauer i en organisation – bør arbejde med password-sikkerhed.

Vejledning om at imødegå ransomware-angreb
Vejledningen "Reducér risikoen for ransomware" giver en række anbefalinger, som or-

ganisationer kan følge for at reducere sandsynligheden for at blive ramt af ransomware-angreb. Vejledningen giver desuden råd til, hvordan et ransomware-angreb kan håndteres, når skaden er sket.

Vejledning om at imødegå phishing-angreb
Vejledningen "Beskyt din organisation mod phishing-angreb" hjælper organisationer med at imødegå truslen fra phishing-mails.

Vejledning om beskyttelse mod DDoS-angreb
Vejledningen "Beskyt mod DDoS-angreb" kommer med en række forholdsregler, som en organisation kan tage for at beskytte sig mod DDoS-angreb.

Vejledning om beskyttelse af IoT-enheder
Vejledningen "Beskyt IoT-enheder" kommer med en række konkrete anbefalinger til, hvordan organisationer kan beskytte IoT-enheder efter best practice.