Styrelsen for Samfundssikkerhed

TRUSSELSVURDERING

Cybertruslen mod Rumsektoren

Juni • 2025

Indhold

Datavej 20
3460 Birkerød
Telephone: + 45 4516 1666
Email: samsik@samsik.dk

Juni 2025

Cybertruslen mod rumsektoren

Formålet med denne trusselsvurdering er at beskrive cybertruslen rettet mod den danske rumsektor. Vurderingen skal styrke risikoejeres forståelse af cybertruslen og kan bl.a. indgå som en del af grundlaget for risikovurderingsarbejdet i sektoren. Trusselsvurderingen er den første for området fra Styrelsen for Samfundssikkerhed (SAMSIK) og skal ses i kontekst af NIS2-direktivet, der bl.a. også omfatter rumområdet.

Hovedvurderinger

- Truslen fra cyberspionage mod den danske rumsektor er **MEGET HØJ**. Fremmede stater har en vedvarende interesse i rumteknologier, som både kan tjene civile og militære formål.

- Truslen fra cyberkriminalitet mod den danske rumsektor er **MEGET HØJ**. Kriminelle hackere angriber løbende organisationer i Danmark på tværs af sektorer. Særligt cyberkriminelle, der udfører afpresningsangreb samt videresælger data og systemadgange, udgør en betydelig trussel.

- Truslen fra cyberaktivisme mod den danske rumsektor er **MIDDEL**. Trusselsniveauet er således lavere end for Danmark generelt, da cyberaktivister sandsynligvis ikke tilskriver sektoren samme symbolske betydning som andre sektorer.

- Truslen fra destruktive cyberangreb mod den danske rumsektor er **MIDDEL**. Truslen kommer primært fra Rusland, og rumsektoren kan i lighed med andre sektorer i samfundet udgøre mål for destruktive cyberangreb.

- Truslen fra cyberterror mod den danske rumsektor er **INGEN**. Cyberterror forudsætter kapaciteter, som militante ekstremister aktuelt ikke har. Samtidig er hensigten yderst begrænset.

Indledning

Rumbaseret teknologi og tjenester udgør essentielle tandhjul i det moderne samfund og understøtter kernefunktioner inden for bl.a. sikkerhed, finans, landbrug og transport. Eksempelvis er Forsvarets opgaveløsning afhængig af rumsystemer i forbindelse med overvågning, kommunikation og navigation, ligesom rumbaseret teknologi understøtter alt fra vejrobservationer til logistik og tidsstempling af finansielle transaktioner. Cyberangreb mod infrastruktur og organisationer i rumsektoren kan dermed potentielt få konsekvenser for de sektorer, som rumsektoren understøtter, samt for samfundet bredt set.

Rumområdets betydning for samfundet stiller store krav til cybersikkerheden hos organisationer og myndigheder i den danske rumsektor. Ikke mindst i lyset af, at både statslige og ikke-statslige hackere løbende retter cyberangreb mod mål på tværs af sektorer, herunder også rumsektoren.

Rumdomænet er præget af intens konkurrence mellem stater henset til de politiske, økonomiske og sikkerhedsmæssige interesser forbundet med rumteknologi og missioner. Samtidig er rumsektorens teknologier og tjenester også potentielle mål i en eventuel fremtidig konflikt. Der er altså flere grunde til, at fremmede stater kan have interesse i afdække infrastruktur og skaffe adgange til systemer hos organisationer i sektoren.

Det er således vigtigt, at rumsektorens infrastruktur og tjenester er tilstrækkeligt beskyttet mod cyberangreb, og her er viden om trusselsbilledet en central forudsætning.

Rumsektoren

Danmarks engagement på rumområdet strækker sig til virksomheder, myndigheder, forskningsinstitutioner, akademiske fakulteter, partnerskaber og mellemstatslige samarbejder. De enkelte aktører varetager forskellige funktioner i relation til rumbaseret infrastruktur og rumforskning. Derudover er nogle aktører led i en bredere værdikæde, der har både civile og militære formål.

Rumområdets økosystem er således bredt og svært at afgrænse til en enkelt underkategori. Uddannelses- og Forskningsministeriet, som i Danmark har ansvaret for regulering af rumaktiviteter, har ligeledes ikke en fast sektordefinition. Når "rumsektoren" omtales i denne vurdering, omfatter det rumagenturer, satellitsystemer, luft- og rumfartsorganisationer samt kommercielle virksomheder, myndigheder og forskningsinstitutter med klare snitflader til rumdomænet.

Denne trusselsvurdering behandler ikke truslen fra jamming og spoofing mod rumbaseret infrastruktur og teknologi.

Trusselsvurderingen beskriver cybertruslen mod rumsektoren med afsæt i fem kategorier baseret på angrebenes formål: Cyberspionage, cyberkriminalitet, cyberaktivisme, destruktive cyberangreb og cyberterror. På baggrund af en analyse vurderes trusselsniveauet for hver kategori i spændet fra **INGEN** til **MEGET HØJ** svarende til Forsvarets Efterretningstjenestes trusselsniveauer. Definitionerne af niveauerne kan findes bagerst i vurderingen.

SAMSIKs trusselsvurderinger baserer sig på en lang række forskellige kilder, herunder bl.a. dialog med organisationer i sektoren, analyser af danske og internationale eksempler på cyberangreb samt viden om trusselsaktørers kapacitet og intention.

Cyberspionage

Truslen fra cyberspionage mod rumsektoren i Danmark er **MEGET HØJ**.

Det er meget sandsynligt, at organisationer i den danske rumsektor bliver udsat for forsøg på cyberspionage inden for de næste to år.

Flere fremmede stater, herunder særligt Kina og Rusland, anvender løbende deres cyberkapaciteter til at udføre cyberspionage mod organisationer i rumsektoren verden over. SAMSIK vurderer, at aktiviteten er udtryk for en generel interesse for rumsektoren fra statslige hackere, som også er rettet mod rumsektoren i Danmark.

Cyberspionage mod rumsektoren er drevet af både teknologiske, økonomiske og sikkerhedspolitiske interesser. Eksempelvis udfører fremmede stater cyberspionage med henblik på at få indsigt i andre staters rumaktiviteter, stjæle ny og innovativ teknologi, herunder dual-use-teknologier, samt for at få adgang til viden om landes forsvarskapaciteter.

Rumagentur ramt af flere cyberangreb

Japans nationale rumagentur, Japan Space Exploration Agency (JAXA), beskrev i juli 2024, at de har været ramt af flere cyberangreb i løbet af 2023 og 2024. Ifølge agenturet var hackerne i nogle tilfælde lykkedes med at kompromittere dele af JAXA's systemer. I januar 2025 meldte japanske myndigheder ud, at en kinesisk hackergruppe gennem en årrække har udført cyberangreb mod mål i Japans sikkerheds- og teknologisektorer, herunder mod JAXA.

JAXA forestår blandt andet udvikling og lancering af satellitter i kredsløb samt mere avancerede missioner, herunder udforskning af himmellegemer og månelandinger.

Rumteknologi er interessant af både civile og militære årsager
De teknologier, systemer, maskiner og komponenter, som organisationer i rumsektoren ligger inde med, udgør et særligt interessant mål for fremmede stater. Det skyldes, at rumteknologi ofte har både civile og militære anvendelsesmuligheder, og at stater således kan bruge den viden, de stjæler fra rumsektoren, til både at fremme deres civile og militære interesser.

Hackere anklaget for cyberspionage mod USA's rumsektor

Amerikanske myndigheder har flere gange anklaget udenlandske hackere for at stå bag cyberspionage mod amerikanske virksomheder i rumsektoren.

I 2020 blev tre navngivne iranske statsborgere anklaget for bl.a. at have stjålet intellektuel ejendom fra amerikanske virksomheder inden for satellitteknologi.

I 2018 blev to navngivne kinesiske hackere fra hackergruppen APT10 anklaget for i mere end et årti at have udført cyberspionage mod amerikanske teknologivirksomheder, og i den forbindelse at have stjålet hundredvis af gigabyte sensitive data fra virksomheder, herunder data fra virksomheder inden for rumområdet.

I en civil kontekst kan fremmede stater f.eks. stille den viden, de har stjålet fra organisationer i rumsektoren, til rådighed for rumteknologivirksomheder fra deres eget land. På den måde får virksomhederne mulighed for at positionere sig stærkere på det internationale marked og dermed tage markedsandele.

I en militær kontekst kan stater potentielt bruge de stjålne oplysninger til at opbygge egne militære kapaciteter og derved styrke deres militær i forhold til andre stater. Derudover kan viden fra rumsektoren give staterne indsigt i andre landes militære kapaciteter, såfremt offeret er leverandør til eller samarbejder med forsvarsindustrien og militære organisationer. Cyberspionage mod mål i rumsektoren kan derved potentielt også bruges som en trædesten for videre cyberspionage mod eksempelvis NATO-allieredes forsvar.

Blandt andet derfor vurderer SAMSIK også, at truslen fra cyberspionage er skærpet for organisationer i den danske rumsektor, som er leverandør til eller på anden vis har samarbejdsrelationer med forsvarsindustrien. Cyberspionage drevet af militære interesser kan ramme virksomheder, der aktuelt eller potentielt i fremtiden understøtter Forsvaret.

Mange dual-use produkter er underlagt EU's eksportkontrol og kræver tilladelse fra myndighederne, inden de kan eksporteres. Blandt andet derfor kan denne type teknologi være særligt udsat for forsøg på cyberspionage. SAMSIK vurderer, at truslen gør sig gældende for alle led i produktionskæden ifm. tilblivelsen af et sådant produkt inden for rumsektoren.

Fremmede stater, herunder især Kina, udfører løbende cyberspionage mod virksomheder, forskningsinstitutioner og andre mål for at få adgang til sensitiv teknologi og viden. Formålet er at stjæle viden, som staterne kan bruge til at fremme deres økonomiske interesser, militære- og teknologiske udviklingsmål.

Cyberkriminalitet finansierer cyberspionage

I juli 2024 udstedte amerikanske, sydkoreanske og britiske myndigheder en arrestordre på en nordkoreansk statslig hacker. Ifølge de amerikanske myndigheder havde hackeren udført ransomware-angreb mod amerikanske hospitaler. Løsesummen blev dernæst brugt til at finansiere angrebsinfrastruktur, som nordkoreanske statslige hackere har anvendt til at udføre cyberspionage mod bl.a. amerikanske forsvarsleverandører, luft-og rumfartsvirksomheder samt NASA. I forbindelse med spionagen gik hackerne målrettet efter bl.a. kontrakter, designskitser og udstyrsoversigter.

Cyberspionage kan muliggøre destruktive cyberangreb

Cyberspionage mod rumsektoren kan udover at give fremmede stater adgang til informationer også bruges til at forberede destruktive cyberangreb. Forberedelsen af destruktive angreb kan bl.a. bestå i kortlægning og indsamling af teknisk viden om organisationers infrastruktur samt etablering af bagdøre i it-systemer. Derved får de statslige hackere bedre mulighed for at udføre destruktive cyberangreb mod deres mål med kort eller uden varsel, såfremt en stat skulle få intention herom.

Selvom cyberspionage således kan understøtte destruktive cyberangreb eller fysisk sabotage, er det dog ikke en forudsætning for alle destruktive cyberangreb. Hackere kan i nogle tilfælde udføre simple, destruktive cyberangreb mod systemer med dårlig beskyttelse med begrænset forberedelse.

Hyppige angrebsmetoder

I det følgende afsnit gennemgår vi nogle af hackernes forskellige angrebsmetoder. Listen er langt fra udtømmende, men indbefatter nogle af de gængse angrebsvektorer. Metoderne bruges af både cyberkriminelle og statslige aktører. Alle metoderne har været anvendt mod organisationer i den internationale rumsektor og i nogle tilfælde også mod organisationer i den danske rumsektor.

Phishing

SAMSIK vurderer, at phishing-mails fortsat er blandt hackeres foretrukne værktøjer. Hackere phisher i forsøget på at kompromittere mål i rumsektoren. Phishing er en forholdsvis billig og skalerbar angrebsmodus. Trænger en phishing-mail først igennem anti phishing-filteret, er det op til den enkelte medarbejder at agere firewall. Phishing-mails udnytter det menneskelige element og dermed risikoen for, at en medarbejder klikker på et ondartet link eller en vedhæftet fil.

Phishing-mails bruges bl.a. til at franarre modtageren sine login-oplysninger eller til at distribuere malware. Udbredelsen af generativ AI kan gøre phishing-mails endnu sværere at opdage, da hackere kan misbruge teknologien til at lave detaljerede, fejlfrie mails – også på sprog, hackerne ikke selv behersker.

Udnyttelse af svage eller genbrugte passwords

Brute force-angreb er fortsat effektive. Brute force-angreb dækker over forskellige variationer af angreb, hvor hackere forsøger at gætte kombinationer af brugernavne og passwords. Dette kan eksempelvis ske gennem udnyttelse af passwords fra tidligere datalæk eller via systematisk gæt af kombinationer fordelt på mange forskellige brugerkonti. Brute force-angreb rettes mod mange forskellige former for systemer, herunder alt fra mailkonti til organisationers fjernadgangssystemer, såsom Remote Desktop Protocol (RDP).

Insider-angreb

Truslen kommer fra medarbejdere med adgang til it-systemer, kundedata eller viden. Medarbejdere kan bevidst eller ubevidst facilitere eller udføre cyberangreb. Cyberangreb via insidere kan tilsidesætte organisationens sikkerhedsforanstaltninger og kan derfor være svære at dæmme op for i tide.

Der har i udlandet været eksempler på insidere i organisationer inden for rumsektoren, som med overlæg har faciliteret cyberangreb.

Både statslige og ikke-statslige aktører bruger insidere til eksempelvis at bistå med teknologioverførsel eller facilitering af cyberangreb.

Nogle cyberkriminelle bruger fora på the dark web til at forsøge at rekruttere virksomheders ansatte til angreb. Insidere har i nogle tilfælde også tilbudt deres services til interesserede købere på the dark web.

Udnyttelse af sårbarheder i software og systemer

Udnyttelse af sårbarheder i software, som ikke er opdateret, er en populær angrebsmetode for særligt kriminelle og stater. SAMSIK vurderer, at begge typer aktører generelt er hurtige til at udnytte deres viden om sårbarheder.

Stater har i længere tid haft ressourcer til at udvikle og købe sig til viden om zero days, også kaldet nul-dags-sårbarheder. Kina har siden 2021 vedtaget ved lov, at individer og virksomheder skal indberette viden om zero days til myndighederne inden for to dage fra, at de bliver opdaget. En zero day er en sårbarhed, hvor leverandøren af softwaren eller systemet endnu ikke kender til sårbarheden, og der derfor endnu ikke findes en opdatering, der kan lukke sårbarheden. Angreb udført via zero days kan derfor være svære at imødegå. SAMSIK vurderer, at flere kriminelle hackere nu også investerer tid og ressourcer i at opdage eller købe sig til zero days.

En del rumbaseret teknologi består i dag af såkaldte commercial-off-the-shelf (COTS) komponenter, som kan købes eller licenseres fra underleverandører. Sammenholdes dette med de vilkår, at rumbaserede systemer tager lang tid at udvikle, potentielt skal være operationelle i mange år, samt at legacy-systemer fortsat indgår i dele af sektorens økosystem, betyder det samlet set, at det kan være en udfordring at holde de forskellige systemer på tværs af værdikæden opdateret.

Disse faktorer betyder bl.a., at angreb via kendte sårbarheder og zero days udgør en væsentlig trussel for rumsektoren.

Angreb via leverandører

Leverandører, særligt softwareleverandører eller cloududbydere, er eftertragtede mål for både statslige hackere og cyberkriminelle. Angreb på leverandører, der har adgang til kunders it-systemer eller data, er attraktive, fordi de potentielt kan give hackere adgang til mange mål på én gang.

Hackerne kan også gå efter leverandører i mere målrettede angreb, hvor de udnytter leverandører til at få adgang til en ellers velbeskyttet organisation, der er svær at kompromittere direkte.

Selvom et angreb på en leverandør ikke fører til direkte operationelle konsekvenser for leverandøren, kan det stadig få negative konsekvenser for leverandørens kunder. Det gælder eksempelvis, hvis den ramte leverandør har adgang til andre virksomheders sensitive data, herunder intellektuel ejendom.

Tilgangen af flere interessenter sammenholdt med kompleksiteten i sektorens værdikæder og infrastruktur medfører en potentielt stor angrebsflade, som hackerne kan målrette.

Organisationer i den internationale rumsektor har været kompromitteret som følge af leverandørangreb.

Cyberkriminalitet

Truslen fra cyberkriminalitet mod rumsektoren i Danmark er **MEGET HØJ**.

Cyberkriminalitet truer samfundet bredt set, og det er meget sandsynligt, at også organisationer i rumsektoren bliver udsat for forsøg på cyberkriminalitet inden for de næste to år.

Cyberkriminelle er økonomisk motiverede og arbejder opportunistisk. Typisk forsøger de kriminelle at afpresse offeret, sælge offerets data eller systemadgange eller at svindle offeret til at overføre penge til hackeren.

Ransomware- og afpresningsangreb udgør en alvorlig trussel
Ransomware-angreb er en form for cyberkriminalitet, som er særligt udbredt, og som også udgør en alvorlig trussel for organisationer i den danske rumsektor.

Ved ransomware-angreb forsøger kriminelle at afpresse organisationer ved at gøre deres data og systemer utilgængelige ved at kryptere dem. Derefter kræver de kriminelle en løsesum, typisk i form af kryptovaluta, for at gøre data og systemer tilgængelige igen. Nogle gange lægger ransomware-aktører også yderligere pres på ofrene ved f.eks. at stjæle informationer og dernæst true med at lække eller sælge dem.

Ransomware-angreb kan få store konsekvenser for offeret, bl.a. i form af tabt fortjeneste og produktionsnedgang. Angreb kan også få mere langsigtede konsekvenser, hvis sensitive informationer bliver lækket. Endelig kan ransomware-angreb også få konsekvenser for samfundet bredere set, hvis angrebet medfører nedetid og driftsforstyrrelser i eksempelvis rumbaserede tjenester, som samfundskritiske sektorer benytter sig af.

Dele af det cyberkriminelle miljø råder over avancerede kapaciteter og formår derfor også at kompromittere ellers godt beskyttede virksomheder. Generelt finder der et højt antal ransomware-angreb sted verden over, herunder i Danmark. I udlandet har der de seneste år også været eksempler på vellykkede ransomware-angreb mod organisationer inden for rumsektoren. Dele af rumsektoren har adgang til store mængder sensitive data, hvilket kan gøre sektoren attraktiv for ransomware-aktører.

Ransomware-aktør afpresser Boeing

Ransomware-aktøren LockBit 3.0 tilføjede i 2023 luft- og rumfartsvirksomheden Boeing til sin Dedicated Leak Site (DLS). LockBit 3.0 påstod at have kompromitteret Boeings systemer og stjålet store mængder sensitive data. Lockbit 3.0 truede med at lække denne data, hvis Boeing ikke imødekom kravet om løsesummen på angiveligt $200 millioner. Boeing har efterfølgende bekræftet, at dele af virksomheden har været udsat for et cyberangreb.

Nogle aktører, der ellers er kendt for at udføre ransomware-angreb, vælger dog nogle gange kun at stjæle følsomme informationer uden brug af kryptering, for derefter at afpresse offeret med at lække disse.

Selvom afpresning uden kryptering ikke medfører direkte forstyrrelser af den operationelle drift, kan det stadig være nødvendigt at foretage en nedlukning af systemer, mens angrebet håndteres.

Adgang til sektorens systemer og data er i høj kurs

SAMSIK vurderer, at informationer og adgange stjålet fra rumsektoren er eftertragtede på de cyberkriminelle markedspladser. De cyberkriminelle kan derfor berige sig ved at sælge følsomme informationer, som de har hacket sig til.

Det er meget sandsynligt, at cyberkriminelle er opmærksomme på værdien af de følsomme data, rumsektoren har adgang til. Det ses f.eks. ved, at kriminelle hackere med jævne mellemrum påstår at have data fra organisationer med relation til rumsektorer i udlandet.

Udover at stjæle informationer for at sælge dem videre, beriger nogle kriminelle hackere sig også ved at skabe den indledende adgang til organisationer for at sælge adgangen videre på diverse undergrundsfora. Hackere, der specialiserer sig i at videresælge adgange til systemer, kaldes Initial Access Brokers (IAB). Deres salg af adgange indgår i et lukrativt økosystem og udgør en potentiel trussel for sektorer på tværs af samfundet, herunder for organisationer på rumområdet.

På disse undergrundsfora køber og sælger cyberkriminelle adgange, malware og tjenester af hinanden. Hackernes mulighed for at købe sig til specialiserede ydelser sænker adgangsbarrieren for at udføre et vellykket cyberangreb. Derudover understøtter samarbejdet og handlen de cyberkriminelles kapaciteter, da hackere kan specialisere og dygtiggøre sig i enkelte led af angrebskæden. Dette samarbejde øger derfor omfanget og det potentielle udbytte af cyberkriminelle angreb.

Det er meget sandsynligt, at enkelte fremmede stater udnytter det cyberkriminelle miljø ved eksempelvis at anskaffe sig malware fra cyberkriminelle. Det kan f.eks. ske via online fora, hvor hackere sælger og udveksler værktøjer og services. De kriminelle ved derfor ikke nødvendigvis, at de samarbejder med eller sælger til en statslig aktør.

Cyberaktivisme

Truslen fra cyberaktivisme mod rumsektoren i Danmark er **MIDDEL**. Truslen er dermed lavere end det generelle niveau for Danmark, som er **HØJ**.

Selvom truslen er lavere end det generelle niveau for Danmark, er det dog fortsat muligt, at danske organisationer i rumsektoren bliver udsat for cyberaktivistiske angreb.

Cyberaktivisme

Cyberaktivisme dækker over cyberangreb, der udføres af individer eller grupper for at få mest mulig opmærksomhed til deres dagsorden.

SAMSIK vurderer, at cyberaktivister foretrækker at målrette deres angreb mod sektorer med større interaktion med og direkte eksponering mod befolkningen, end hvad der er tilfældet for den danske rumsektor. I Danmark har særligt transport- og finanssektoren samt Forsvaret været hyppige mål for aktivistiske angreb siden Ruslands invasion af Ukraine i 2022. Rumsektoren i Danmark er forholdsvis lille sammenlignet med disse sektorer og har begrænset omfang af brugervendte systemer, som kan rammes og dermed skabe opmærksomhed.

Cyberaktivisme kan understøtte staters interesser
Pro-russiske cyberaktivister udfører hyppigt angreb mod skiftende mål, som de særligt udvælger inden for en bred vifte af lande, der står i et modsætningsforhold til Rusland

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 imidlertid, at nogle pro-russiske cyberaktivister har forbindelse til den russiske stat.

Cyberaktivister angriber ofte med DDoS
De pro-russiske aktivistiske hackere benytter sig særligt af DDoS-angreb. DDoS-angreb har ikke i sig selv varige eller destruktive effekter. Angrebene kan dog påvirke systemernes tilgængelighed. Derudover kan forstyrrelser eller udfald på rumbaserede systemer påvirke tilliden til den ramte organisation samt potentielt få alvorlige konsekvenser. Det gælder særligt, hvis en ydelse, der understøtter samfundskritisk infrastruktur, bliver utilgængelig som følge af et angreb.

DDoS-angreb

DDoS står for Distributed Denial of Service og er et overbelastningsangreb. Hackere udnytter kompromitterede computere til at generere usædvanligt store mængder datatrafik mod en hjemmeside (webserver) eller et netværk, så hjemmesiden eller netværket ikke er tilgængeligt for legitim trafik, mens angrebet står på.

I udlandet har der været eksempler på, at rumsektoren har været målrettet cyberaktivistiske angreb. Det gælder både virksomheder og organisationer, men også specifikke satellitsystemer, som servicerer et stort antal brugere.

Cyberaktivisme kan være andet end DDoS

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

Enkelte pro-russiske cyberaktivister har udført simple og opportunistiske destruktive cyberangreb mod mål i vestlige lande. Omfanget af disse angreb er dog begrænset sammenlignet med de mange DDoS-angreb, som rammer mål i Danmark og Vesten, og angrebene har primært også været rettet mod mål med lav beskyttelse. Selvom disse angreb er simple, kan de have store konsekvenser for det enkelte offer.

Cyberaktivister verden over har også med jævne mellemrum påstået at have udført hack og læk-angreb. Ved hack og læk-angreb stjæler de sensitive dokumenter eller personoplysninger for derefter at offentliggøre dem. Cyberaktivister har i udlandet særligt ramt organisationer inden for forsvarsområdet med sådanne angreb.

Destruktive cyberangreb

Truslen fra destruktive cyberangreb mod rumsektoren i Danmark er **MIDDEL**.

Truslen kommer især fra Rusland og retter sig bredt mod organisationer i samfundsvigtige sektorer i Danmark. Truslen er således ikke specifikt rettet mod rumsektoren.

Truslen er **MIDDEL**, fordi Rusland siden starten af 2024 har udvist en øget risikovillighed i forhold til at anvende hybride virkemidler med destruktive effekter mod europæiske NATO-lande. SAMSIK vurderer, at dette også omfatter destruktive cyberangreb.

Hvad er destruktive cyberangreb?

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

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

Formålet med angreb er sandsynligvis at påvirke befolkningen
Det er sandsynligt, at destruktive cyberangreb mod Danmark i den nuværende situation vil have til formål at skabe opmærksomhed og derved påvirke befolkning og beslutningstagere. Den konkrete fysiske effekt af eventuelle destruktive cyberangreb mod Danmark vil dermed sandsynligvis være sekundær for hackerne, der udfører det.

SAMSIK vurderer, at mange typer af organisationer i samfundsvigtige sektorer, herunder i rumsektoren, vil kunne blive udvalgt som mål for eventuelle destruktive cyberangreb.

Udvælgelsen af mål vil derudover sandsynligvis være påvirket af, hvor hackerne har adgang eller nemt kan få det.

Truslen kan stige i en konflikt
Sandsynligheden for, at denne type angreb finder sted mod Danmark, herunder mod rumsektoren, kan stige, hvis den sikkerhedspolitiske situation eskalerer i retning af en militær konfrontation mellem Rusland og NATO.

Rumkapaciteter spiller i dag en nøglerolle i moderne krigsførelse, og rummet betragtes i dag som et militært domæne på linje med luft-, jord-, vand- og cyberdomænet. Flere fremmede stater med betydelige offensive cyberkapaciteter opererer i dag også i rumdomænet. Oprustning og udbygning af militære kapaciteter i rumdomænet er derfor

blevet en vigtig sikkerhedspolitisk komponent, da dominans i rummet har potentialet til at påvirke militære konflikter.

Kinesisk cyberspionage skulle forberede destruktive cyberangreb

Cybersikkerhedsmyndigheder fra USA, Storbritannien, Canada, Australien og New Zealand advarede i februar 2024 om, at kinesiske hackere havde forsøgt at kompromittere organisationer i kritiske sektorer i USA, herunder infrastruktur på rumområdet. Ifølge myndighederne var det primære formål med angrebet at muliggøre destruktive cyberangreb i tilfælde af en større krise eller konflikt med USA. Hackerne forsøgte bl.a. at få adgang til IT-netværk, hvorfra det var muligt at sprede sig til organisationernes OT-netværk. Dermed ville hackerne kunne iværksætte destruktive angreb mod kritiske systemer, såfremt Kina skulle få intentioner herom.

Danske organisationer i sektoren, der leverer produkter eller tjenester relateret til krigen i Ukraine, kan være udsat for en højere risiko for at blive ramt af et angreb eller følgevirkningerne af et angreb, der er rettet mod Ukraine.

Angreb på rumbaserede tjenester kan bruges til at ramme andre mål
Destruktive cyberangreb mod systemer og teknologi i rumsektoren kan bruges til at ramme mål i andre sektorer. Rumbaserede tjenester og organisationer i sektoren understøtter både militære kapaciteter og civile sektorer. Et destruktivt cyberangreb med et militært sigte kan derfor også få følgevirkninger for civile sektorer.

Destruktivt cyberangreb mod Viasat KA-SAT

På dagen for Ruslands invasion af Ukraine blev virksomheden Viasat ramt af et wiper-angreb kaldet AcidRain, der blandt andet resulterede i, at tusindvis af satellitmodemmer, særligt i Europa, fik slettet deres opsætning. Viasat er en amerikansk udbyder af satellitkommunikation. Den manglende satellitkommunikation førte bl.a. til nedbrud i fjernstyringen af flere vindmøller i Tyskland. Det er sandsynligt, at målet med angrebet var ukrainske militære styrkers satellitkommunikation.

Danmark har sammen med EU og en række nære allierede vurderet, at Rusland stod bag cyberangrebet, og at Rusland var velvidende om, at angrebet ville have destruktive konsekvenser uden for Ukraine.

Angrebet mod Viasat illustrerer, at destruktive cyberangreb kan anvendes med det formål at skabe en effekt på militær infrastruktur i det fysiske domæne. Derudover illustrerer eksemplet også, at angreb på rumområdets infrastruktur kan få følgevirkninger for andre sektorer.

Rumområdet er ikke isoleret til en dansk kontekst, men er i sin natur grænseløs. Rumbaserede tjenester servicerer flere stater og sektorer. Samlet betyder det, at destruktive cyberangreb mod andre landes rumsektor, potentielt kan få en afsmittende virkning på Danmark.

Andre aktører udgør også en potentiel trussel
Selvom truslen fra destruktive cyberangreb især kommer fra Rusland, er der også en potentiel trussel fra andre stater. For eksempel er det sandsynligt, at hackergrupper fra Iran har udført destruktive cyberangreb mod vestlige mål.

Derudover kan der også være en trussel fra ikke-statslige hackere. 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, at visse cyberaktivistiske grupper har intentioner om at udføre cyberangreb med destruktiv effekt. For eksempel blev et mindre dansk vandværk i slutningen af 2024 ramt af et destruktivt cyberangreb fra pro-russiske cyberaktivister. Ved angrebet blev vandværkets operationelle systemer manipuleret, hvilket bl.a. medførte, at flere husstande var uden vand i en kortere periode.

SAMSIK vurderer dog, at cyberaktivistiske angreb af destruktiv karakter er opportunistiske i forhold til måludpegning og rammer mål, der har ringe beskyttelse. Alligevel er disse destruktive cyberangreb mere krævende at udføre end de angreb, som cyberaktivister normalt gør brug af.

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.

Cyberterror

Truslen fra cyberterror mod Danmark er **INGEN**.

Cyberterror defineres som alvorlige politisk motiverede cyberangreb, der har til hensigt at skabe samme effekt som mere konventionel terror.

SAMSIK vurderer, at ingen aktører aktuelt har kapacitet til eller intention om at udføre cyberterror. Det er derfor usandsynligt, at danske myndigheder og virksomheder inden for de næste to år vil blive udsat for forsøg på cyberterror.

Trusselsniveauer

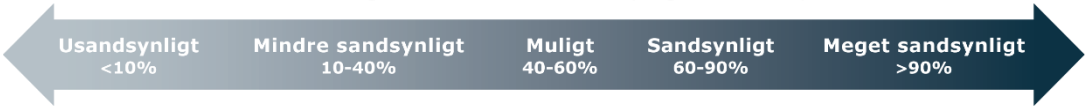
Styrelsen for Samfundssikkerhed anvender i sine trusselsvurderinger Forsvarets Efterretningstjenestes (FE) trussels- og sandsynlighedsniveauer.

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.