CENTER FOR CYBERSIKKERHED

Trusselsvurdering

Cybertruslen mod energisektoren

2. udgave februar 2023.

Indhold

CENTER FOR CYBERSIKKERHED

Kastellet 30
2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk

2. udgave, februar 2023

Cybertruslen mod energisektoren

Formålet med denne trusselsvurdering er at beskrive de forskellige cybertrusler, som den danske energisektor står over for. Vurderingen henvender sig bredt til beslutningstagere og interessenter i de virksomheder og myndigheder, som udgør energisektoren. Trusselsvurderingen kan anvendes i myndigheder og virksomheders arbejde med risikovurderinger.

Vurderingen erstatter den tidligere trusselsvurdering for sektoren, som senest blev opdateret i juni 2022, og gælder som udgangspunkt i op til to år. I denne 2. udgave er niveauet for cyberaktivisme hævet til **HØJ**.

1. udgave blev udgivet på tryk i januar 2023 og fremsendt til sektoren.

Hovedvurdering

- Truslen fra cyberkriminalitet er **MEGET HØJ**. Den alvorligste trussel fra cyberkriminalitet kommer fra ransomware-angreb, der løbende rammer virksomheder og underleverandører i sektoren. Presset på virksomheder fra ransomware-angreb øges, hvis der er tvivl om, hvorvidt et angreb også kan ramme den operative teknologi (OT).

- Truslen fra cyberspionage er **MEGET HØJ**. Den vedvarende trussel udgår især fra Rusland og Kina og fører løbende til cyberangreb mod danske mål. Energisektoren er et eftertragtet mål, både af civile og militære årsager. CFCS vurderer, at Danmarks fortsatte førerposition i den grønne omstilling også vil kunne drive truslen.

- Truslen fra cyberaktivisme er **HØJ**. Truslen udgår særligt fra pro-russiske hackere, der har øget deres aktivitetsniveau efter Ruslands invasion af Ukraine, og løbende rammer mål i Vesten – også i Danmark.

- Truslen fra destruktive cyberangreb er **LAV**. Selvom stater, herunder Rusland, har kapaciteten til at udføre destruktive cyberangreb mod Danmark, har de for nuværende ikke intentionen. Krigen i Ukraine har vist, at destruktive cyberangreb er blevet en del af moderne krigsførelse, og at energisektoren er et prioriteret mål i en konfliktsituation.

- Truslen fra cyberterror er **INGEN**.

Indledning

Energisektoren i Danmark

Den samlede energisektor i Danmark består af produktion og levering af forskellige former for energi. Når energisektoren omtales i det følgende, skal det forstås som de virksomheder, underleverandører og myndigheder, der understøtter den kritiske infrastruktur, som sikrer det danske samfund en stabil forsyning af energi, både nu og i fremtiden.

El, fjernvarme, olie og gas er for danskere og danske virksomheder kritiske for en velfungerende dagligdag. Ligesom vind- og solenergi i stigende grad er ved at blive det. Den grønne omstilling vil bane vejen for andre energiformer, som eksempelvis Power-to-X og grøn brint i takt med den teknologiske udvikling. Virksomheder i de forskellige dele af energisektoren adskiller sig fra hinanden, og har derfor også meget forskellige tilgange til cybersikkerhed. Nuancerne i denne komplekse sektor bliver ikke behandlet yderligere i denne trusselsvurdering, men bør indgå i den enkelte organisations risikovurdering.

Cybertruslen mod energisektoren har, ligesom den generelle trussel mod Danmark, været alvorlig, siden Center for Cybersikkerhed (CFCS) udgav den første trusselsvurdering for sektoren i 2018. Siden da har trusselsbilledet udviklet sig og er kun blevet mere komplekst. Energisektoren skal forsvare sig mod statslige aktører, cyberkriminelle grupper og aktivister, der med forskellige hensigter mere eller mindre målrettet angriber vestlige energiselskaber.

Trusselsniveauerne i vurderingen fortæller noget om sandsynligheden for, at cyberangreb med et givent formål vil blive udført. Trusselsniveauerne siger imidlertid ikke noget om, hvor sandsynligt det er, at angrebet vil lykkes. Og det fortæller heller ikke, hvad konsekvenserne af et succesfuldt angreb er.

Truslen fra både cyberspionage og cyberkriminalitet mod energisektoren er fortsat **MEGET HØJ**. Både stater og kriminelle grupper har interesse i at kompromittere virksomheder i sektoren. Stater af både militære og civile årsager og med specifik interesse i sektoren. Kriminelle af opportunistiske motiver i den evige jagt på nye ofre.

Den anspændte situation mellem Rusland og Vesten som følge af Ruslands invasion af Ukraine i februar 2022 har fået cyberaktivister til at skrue op for aktivitetsniveauet. Grupper som Anonymous og Killnet har været helt i front, men med hver deres agenda. Den store aktivitet hos særligt pro-russiske cyberaktivister har betydet, at det aktuelle trusselsniveau for cyberaktivisme er **HØJ**. CFCS vurderer, at energi-sektoren også er udsat for truslen fra cyberaktivisme. Dels fordi sektoren udgør kritisk infrastruktur og dels på grund af den særlige rolle, som energipolitik har i forholdet mellem Rusland og EU.

Krigen i Ukraine har pustet til frygten for destruktive cyberangreb, og flere af disse har siden krigens start ramt mål i Ukraine. CFCS vurderer dog, at truslen fra et destruktivt cyberangreb målrettet den danske energisektor fortsat er **LAV**. Selvom flere stater, herunder Rusland, har de fornødne kapaciteter til at kunne udføre sådanne angreb, er det fortsat mindre sandsynligt, at de har intentionen om at gøre det.

Efter Ruslands invasion af Ukraine er EU's afhængighed af russisk olie og gas blevet taget yderligere op til revision. Mange lande, herunder Danmark, har som direkte resultat af situationen besluttet at fremskynde den grønne omstilling og dermed løsrive sig fra afhængigheden af russisk energi. Projekter som de to kommende energiøer spås en central rolle i fremtidens energiforsyning. Også Esbjerg-deklarationen, der udnævner Nordsøen til EU's grønne kraftværk, placerer Danmark centralt i udfasningen af fossile – ofte russiske – energiformer. Uanset med hvilken fart, og i hvilken geopolitisk kontekst, den grønne omstilling udrulles i, vil den danske energisektor være kritisk for samfundet. Ikke alene for Danmark, men også for vores nabolande og EU. Det er med dette bagtæppe, at trusselsvurderingen for energisektoren 2023 er skrevet.

Cyberkriminalitet

CFCS vurderer, at truslen mod den danske energisektor fra cyberkriminalitet, herunder særligt ransomware-angreb, er **MEGET HØJ.** Det betyder, at det er meget sandsynligt, at myndigheder og virksomheder i sektoren vil blive udsat for forsøg på cyberkriminalitet inden for de næste to år.

Danske borgere, myndigheder og virksomheder bliver dagligt udsat for forsøg på kriminalitet i det digitale domæne. Det gælder også for energisektoren, hvor virksomheder og myndigheder løbende rammes af mere eller mindre komplekse angreb fra cyberkriminelle. Især udgør risikoen for ransomware-angreb en meget alvorlig trussel mod energisektoren. I en gennemgang af offentligt kendte succesfulde cyberangreb mod energisektoren i Europa har den danske EnergiCert vurderet, at 65% af angrebene mod sektoren siden 2015 var ransomware-angreb.

Både i Danmark og resten af Europa har ransomware-angreb ramt energisektoren bredt med ofre hos blandt andre forsyningsselskaber, gasdistributører, olieterminaler og raffinaderier, vindmølleproducenter og andre underleverandører. Ikke nok med at angrebene er hyppige og rammer bredt, så kan de have alvorlige konsekvenser for samfundet. Det blev bl.a. understreget af ransomware-angrebet mod Colonial Pipeline i maj 2021, der førte til brændstofmangel på den amerikanske østkyst.

Energisektoren har, hvad de kriminelle vil have

CFCS vurderer, at målrettede ransomware-angreb er økonomisk motiverede, opportunistiske og kan ramme alle typer virksomheder og myndigheder, også i energisektoren. Det skyldes flere ting. Den danske energisektor består af mange virksomheder, hvoraf en del har relativt høje omsætninger. For kriminelle grupper vil alene omsætningen betyde, at disse virksomheder er attraktive ofre, da de kriminelle kalkulerer med, at virksomhederne kan betale en høj løsesum.

Endnu et element, der kan gøre virksomheder i sektoren til attraktive mål, er, at virksomhederne og samfundet kan blive presset hårdt af eventuelle driftsforstyrrelser. For at få driften hurtigt op at køre igen kan det være fristende for virksomheden at betale løsesummen. At betale løsesummen er dog ikke nogen garanti for, at driften kan genoptages hurtigt. Det har eksempelvis været berettet i flere medier, at amerikanske Colonial Pipeline benyttede egne backups til at genoprette deres systemer. De havde ellers, ifølge åbne kilder, betalt 4.4 millioner dollars for en dekrypteringsnøgle, men dekrypteringsprocessen viste sig at være meget langsom.

Selvom Ruslands invasion af Ukraine fik nogle ransomware-grupper som eksempelvis CONTI til at give udtryk for et politisk ståsted, er det fortsat CFCS' vurdering, at de kriminelle grupper primært er motiveret af økonomisk gevinst og handler opportunistisk. Det vil sige, at de oftest udvælger deres ofre på baggrund af en cost-benefit-analyse af, hvor de kan skaffe adgange, hvilke ofre de forventer vil betale en løsesum, samt hvor stor en løsesum ofrene kan betale.

Vores mange forbindelser øger angrebsfladen

CFCS vurderer, at ransomware-angreb fortsat oftest rammer en virksomheds IT-miljø. Den stigende grad af forbundethed i samfundet øger muligheden for, at et angreb kan sprede sig fra IT til OT og vil dermed kunne forværre konsekvenserne af ransomware-angreb mod energisektoren.

IT, OT og IOT – flere forbindelser giver flere sårbarheder

I takt med den teknologiske udvikling er cybersikkerhed ikke længere begrænset til IT. Den stigende digitalisering, som moderne samfund undergår, betyder, at det ikke kun er vores informationer, der holder til i det digitale domæne. Store dele af samfundets produktion og drift er nu også forbundet til internettet. Herunder er CFCS' overordnede definitioner:

IT: Informationsteknologi. IT-systemer omfatter hardware og software og kan være både uafhængige eller forbundet med andre systemer i et netværk.

OT: Operationel teknologi. Systemer, der anvendes til overvågning og styring af mekaniske systemer, herunder industrielle kontrolsystemer (ICS).

IOT: Internet Of Things. Et udtryk for komponenter, der er koblet til internettet. Det drejer sig om alt fra termostater til hverdagsobjekter som f.eks. køleskabe eller kameraer. Når OT-enheder benytter IP-netværk og eventuelt er forbundet via internettet, kaldes det Industrial Internet of Things (IIoT).

Der er de seneste år kommet øget fokus på cybersikkerheden i virksomheders produktionsmiljøer. Det amerikanske agentur for cybersikkerhed og infrastruktur, CISA, har eksempelvis vurderet, at OT er sårbart over for både lettilgængelige hackerværktøjer, men også over for mere avanceret malware, skræddersyet til at ramme OT. Virksomheders arbejde med at få produktionen online for bl.a. at kunne følge processen på afstand, er i stigende grad blevet fulgt af en bekymring for, hvad den forbundenhed gør ved cybersikkerheden.

Europæiske ENISA har vurderet, at cyberkriminelle kan ramme OT, og beskriver fire mere eller mindre direkte måder, hvorpå virksomheders OT-miljøer kan blive ramt. Et cyberangreb kan anvende malware, der direkte rammer og krypterer enheder i virksomheders OT-miljøer. Eller manglende segmentering kan resultere i, at malware spreder sig fra IT til OT. Hvis en virksomhed er usikker på, hvorvidt systemerne er tilstrækkeligt segmenterede, kan et cyberangreb mod IT-systemet også resultere i, at virksomheden af egen drift stopper produktionen for at inddæmme malware. Endelig kan ransomware-grupper skaffe sig adgang til følsomme oplysninger om en virksomheds OT-enheder og benytte denne viden som afpresning.

Udfordringen for virksomheder med at have et komplet billede af infrastrukturen, herunder eventuelle forbindelser mellem IT og OT, vokser i takt med at både IT- og OT-miljø bliver mere komplekse. Det kan i sidste ende betyde, at et ransomware-angreb mod et selskabs IT-systemer får konsekvenser for OT-miljøet. Også her er angrebet mod Colonial Pipeline et sigende eksempel. Colonial Pipelines administrerende direktør Joseph Blount har overfor det amerikanske senat beskrevet, at man indledningsvist lukkede ned for rørledningen for at inddæmme angrebet og sikre, at malware ikke spredte sig til OT-netværket. Nedlukningen varede i seks dage og havde omfattende konsekvenser for brændstofforsyningen, da rørledningen er den længste og vigtigste på den amerikanske østkyst.

Omvendt kunne Vestas, der i 2021 blev ramt af ransomware, hurtigt meddele, at deres vindmøller kunne operere uafhængigt af de berørte systemer, og at angrebet derfor ikke påvirkede forsyningssikkerheden.

En yderligere udfordring for virksomheder i sektoren er, at det ikke kun er egen infrastruktur, de skal sikre. Energisektoren er kompleks, og mange produktions-, transmissions og distributionsselskaber benytter sig af underleverandører.

Leverandører bliver brugt som angrebsvinkel i såkaldte supply-chain-angreb. De leverandører, der har en legitim og privilegeret adgang til deres kunders it-systemer, er særligt attraktive for hackere. Der har været en række bemærkelsesværdige supply-chain-angreb de seneste år. Et eksempel er ransomware-angrebet i 2021 mod det amerikanske selskab Kaseya, som spredte sig til hundredvis af selskabets kunder.

Cyberspionage

Truslen fra cyberspionage mod den danske energisektor er **MEGET HØJ**. Det betyder, at det er meget sandsynligt, at myndigheder og virksomheder i sektoren vil blive udsat for forsøg på cyberspionage inden for de næste to år. Danmarks rolle i den grønne omstilling vil bidrage til, at sektoren i Danmark også på længere sigt forbliver et mål for cyberspionage.

CFCS vurderer, at energisektoren i både Danmark og udlandet løbende er ofre for cyberspionage. Cyberspionage bliver begået af fremmede stater med en særlig interesse for viden af udenrigs-, sikkerheds- og forsvarspolitisk karakter. Energisektoren, der både er vigtig for forsyningssikkerheden og understøtter staten, Forsvaret og Danmarks økonomi, er af særlig interesse.

Truslen fra cyberspionage kommer især fra Rusland og Kina, der råder over betydelige kapaciteter til at udføre cyberspionage. Begge lande udgør en vedvarende trussel mod danske myndigheder og virksomheder.

Rusland har meget store cyberkapaciteter, som landet bruger systematisk til at understøtte sine nationale interesser. Tidligere sager har understreget, at Rusland har interesse for den danske energisektor. I et eksempel på mere traditionel spionage blev en russisk statsborger idømt tre års fængsel i 2021 for at have spioneret mod Danmarks Tekniske Universitet (DTU) og energivirksomhed SerEnergy A/S. Manden havde i flere år udleveret oplysninger mod betaling til en russisk efterretningstjeneste.

Kina udfører omfattende cyberspionage verden over, også mod danske myndigheder, virksomheder og organisationer. Kinas militær og efterretningstjenester har meget væsentlige kapaciteter og evner til at skaffe sig fuld og vedvarende adgang til organisationers informationer. Der er tale om en konstant og langsigtet aktivitet, der gavner Kinas sikkerheds - og udenrigspolitiske samt økonomiske og kommercielle interesser.

Energipolitik er sikkerhedspolitik

Krigen i Ukraine har sat yderligere skub i den grønne omstilling. Der er opstået en udtalt sammenhæng mellem den grønne omstilling i EU og forholdet til Rusland. Bevægelsen mod vedvarende energi er blevet meget direkte italesat som en bevægelse væk fra russiske energikilder. Det er derfor sandsynligt, at fremmede stater, herunder særligt Rusland, ønsker indsigt i bl.a. de store anlægsprojekter, som kommer til at forme fremtidens energiforsyning i Europa, og som Danmark har en central rolle i.

Energiøer og vindparker – Danmark som europæisk knudepunkt

Danmark har i mange år været et foregangsland inden for vedvarende energi. Kommende store anlægsprojekter vil forstærke denne tendens og gøre Danmark til et knudepunkt for europæisk vedvarende energi. De planlagte energiøer i Nordsøen og Østersøen skal ifølge Energinet kunne levere 6GW effekt – svarende til det årlige elforbrug i seks millioner husstande.

Esbjerg-aftalen, der bl.a. blev indgået for at gøre EU energi-uafhængig, sætter et mål for, at Danmark, Belgien, Holland og Tyskland skal etablere et netværk af offshore-anlæg, der skal levere mindst 65GW effekt i 2030.

Cyberspionage kan også tjene som forberedelse til fremtidige, destruktive cyberangreb. Destruktive cyberangreb, der har til formål at forstyrre eller ligefrem ødelægge kritisk infrastruktur, vil oftest være komplicerede og tidskrævende operationer.

Den grønne omstilling sætter fokus på Danmark

CFCS vurderer, at den grønne omstilling og teknologien, der skal understøtte den, har stor interesse for fremmede stater af både civile og militære årsager.

Stater søger løbende at ruste sig bedst muligt til fremtiden, at opnå konkurrencemæssige fordele og sikre deres plads i det internationale hierarki. Uanset at den grønne omstilling i Europa er fremskyndet af Ruslands invasion af Ukraine, vil omstilling til vedvarende energi på et tidspunkt berøre hele verden.

Selvom truslen fra cyberspionage aktuelt primært kommer fra Kina og Rusland, vurderer CFCS, at andre lande også prioriterer at udvikle deres cyberkapaciteter. Det er meget sandsynligt, at flere stater i fremtiden vil udgøre en cybertrussel mod Danmark. CFCS vurderer, at blandt andre Iran, Nordkorea, Vietnam, Pakistan og Indien også har kapacitet til at udføre cyberspionage. Det er dog sandsynligt, at disse stater generelt ikke har en særlig interesse i at ramme danske mål.

Det er imidlertid muligt, at den grønne omstilling på længere sigt vil medføre, at nye statslige cyberaktører vil forsøge at få adgang til viden hos danske myndigheder og virksomheder. Motivet vil være at springe udviklingsfasen af den grønne omstilling over for at styrke egen konkurrenceevne. Den form for cyberspionage vil særligt ramme de virksomheder, der udvikler, sælger og producerer teknologi, der skal bære den grønne omstilling, og som det har været omkostningstungt at udvikle.

Stater bruger flere metoder i forsøg på at udføre cyberspionage

Cyberspionage er typisk målrettet it-systemer og netværk, der indeholder information såsom mails og dokumenter, som har fremmede staters interesse. Fremmede staters muligheder for at få adgang til disse informationer varierer og er bl.a. afhængige af offerets it-systemer og angriberens evner og værktøjer. Fremmede stater bruger derfor flere forskellige angrebsmetoder.

Helt simple angreb kan eksempelvis være såkaldte brute force-angreb, hvor hackerne forsøger at trænge ind i it-netværk ved at afprøve et stort antal mulige brugernavne og passwords. Hackere opretter også falske hjemmesider, hvor ofrene bliver lokket til at indtaste deres brugernavne og kodeord. Spredning af malware gennem eksempelvis phishing er også en relativt simpel angrebstype, der stadig er meget udbredt.

Cyberangreb kan også blive udført ved at misbruge sårbarheder i it-systemerne, såsom fejl i hard- og software, manglende opdateringer eller fejlopsætninger. I nogle tilfælde betyder opdagelsen af sårbarheder i udbredte it-systemer, at en bred vifte af organisationer udgør mulige mål.

Fremmede stater gør – i lighed med andre typer hackere - ofte brug af de samme værktøjer og fremgangsmåder i angreb mod flere mål. Genbrug af metoder og værktøjer gør det muligt for angriberne at økonomisere med deres ressourcer og forsøge at ramme mange mål på én gang eller over længere tid. Rusland og Kina har kapacitet til samtidigt at udføre flere spionagekampagner mod mål verden rundt, bl.a. i Danmark. Genbrug af metoder og værktøjer gør det imidlertid også nemmere at identificere angrebene og overføre erfaringen fra tidligere angreb til beskyttelsen af andre potentielle mål.

Truslen mod leverandører

Mere avancerede angreb kan ske gennem organisationernes leverandører. Det kan eksempelvis ske ved software supply chain-angreb, hvor aktører gemmer malware i ellers legitime opdateringer, som leverandører derefter distribuerer til deres kunder. Cyberspionage kan også blive rettet mod andre leverandører og samarbejdspartnere, der kan misbruges som trædesten i angreb mod de organisationer, staterne er interesserede i.

Den danske energisektor er, ligesom andre dele af den kritiske infrastruktur, afhængig af en række forskellige leverandører. Der er både tale om soft- og hardware-producenter, samt enheder, som leveres med serviceaftaler. Det er eksempelvis tilfældet i produktionen af forskellige vedvarende energiformer. Komplekse forsynings-kæder stiller store krav til de enkelte virksomheder i forhold til leverandørstyring.

I marts 2020 gemte hackere en specialudviklet bagdør i det udbredte it-ma-nagementsystem Orion fra virksomheden SolarWinds. Bagdøren blev ifølge SolarWinds distribueret via inficerede softwareopdateringer til op mod 18.000 organisationer verden over. Angrebet er et af de mest omfangsrige software supply chain-angreb nogensinde, og CFCS har vurderet, at angrebet blev udført af statsstøttede hackere med henblik på cyberspionage. Det har i åbne medier været berettet, at en række danske energiselskaber havde installeret den inficerede opdatering og derfor potentielt var berørt af SolarWinds-angrebet. CFCS vurderer dog, at hackerne primært udnyttede bagdørene hos centrale amerikanske myndigheder og virksomheder. Amerikanske myndigheder har anklaget den russiske udenrigsefterretningstjeneste SVR for at stå bag angrebet.

Cyberaktivisme

Truslen fra cyberaktivisme mod energisektoren er **HØJ.** Det betyder, at det er sandsynligt, at energisektoren vil blive ramt af aktiviske cyberangreb inden for de næste to år.

CFCS hævede d. 31. januar 2023 trusselsniveauet for cyberaktivisme fra **MIDDEL til HØJ,** bl.a. på baggrund af pro-russiske aktivistiske hackergruppers høje aktivitets-niveau mod NATO-lande, herunder Danmark, samt deres øgede kapacitet.

CFCS vurderer, at aktivister, særligt pro-russiske, primært går efter symbolske mål. Energi- og forsyningssikkerhed spiller en stor rolle i konflikten mellem Rusland og Vesten. Derfor kan virksomheder i den danske energisektor også blive mål for cyberaktivister, selvom der ikke nødvendigvis er tale om en særskilt trussel mod sektoren.

Den pro-russiske hackergruppe KillNet har været meget aktiv i deres støtteaktioner til fordel for det russiske styre. CFCS har kendskab til, at KillNet på mediet Telegram har truet en række navngivne, europæiske energiselskaber med DDoS-angreb og ransomware-angreb.

Cyberaktivisme udføres af individer og hackergrupper, der laver cyberangreb for at få mest mulig opmærksomhed til deres dagsorden eller for at straffe organisationer. Cyberaktivisme er typisk drevet af forskellige ideologiske eller politiske motiver, der strækker sig fra politiske enkeltsager til modstand mod magthavere. Cyberaktivister angriber både ofre, de ser som symbolske mål og modstandere af deres sag. Cyberaktivister er i stand til at udføre forskellige typer cyberangreb, fra simple overbelastningsangreb og defacement-angreb til mere ressourcekrævende hack og læk -operationer.

De pro-russiske cyberaktivistiske hackergrupper formaliserer i stigende grad deres planlægning og eksekvering af angreb. Flere af de mest aktive pro-russiske grupper har desuden oprettet platforme dedikeret til at mobilisere ressourcer til DDoS-angreb.

DDoS er aktivisternes foretrukne metode

Pro-russiske hackere udfører især overbelastningsangreb. Denne type angreb virker forstyrrende og tiltrækker sig opmærksomhed, men har ikke varige eller destruktive konsekvenser for ofrenes systemer.

Der har dog på det seneste være indikationer på, at nogle aktivistiske grupper har ambitioner om at udføre mere ødelæggende cyberangreb. Pro-ukrainske grupper har ved flere lejligheder beskrevet, hvordan man har ramt industrielle kontrolsystemer Rusland, også i energisektoren. Uanset om angrebet rent faktisk fandt sted er det en indikation på, at nogle cyberaktivister har interesse i mere avancerede cyberangreb.

Destruktive cyberangreb

Destruktive cyberangreb
CFCS definerer et destruktivt cyberangreb som et cyberangreb, hvor den forventede effekt af angrebet 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 truslen fra destruktive cyberangreb mod energisektoren er **LAV**. Det betyder, at det er mindre sandsynligt, at energisektoren vil blive udsat for forsøg på destruktive cyberangreb inden for de næste to år.

At trusselsniveauet er lavt betyder, at det er mindre sandsynligt – ikke usandsynligt – at energisektoren bliver ramt af destruktive cyberangreb. En række stater udvikler løbende deres kapaciteter til at udføre sådanne angreb, og både Rusland og andre stater har særdeles veludviklede kapaciteter. Truslen afhænger derfor i høj grad af, hvorvidt fremmede stater har intentionen om at udføre destruktive cyberangreb. Tilstedeværelsen af kapacitet betyder altså, at truslen kan stige hurtigt, hvis hensigten ændrer sig.

Fokus på forsyningssikkerheden
CFCS vurderer fortsat, at Rusland ikke ønsker at ramme Danmarks energiforsyning med et destruktivt cyberangreb.

Siden Rusland invaderede Ukraine i februar 2022 har bekymringen over russiske cyberangreb mod Danmarks energisektor fyldt meget i den offentlige debat. Den fysiske sabotage mod Nord Stream 1 og 2 gasrørene i Østersøen i september 2022 har kun styrket bekymringen for, at energi-infrastruktur bliver en del af konflikten, også uden for Ukraine. Det er på nuværende tidspunkt stadig uvist, hvem der stod bag sabotagen.

Ukraine har i 2022 været ramt af forskellige destruktive cyberangreb. Rusland har ifølge flere IT-sikkerhedsfirmaer udført en række såkaldte wiper-angreb mod ukrainske myndigheder og virksomheder, som har fået slettet data permanent. Det har også været beskrevet, at et ukrainsk energiselskab i april 2022 blev ramt af et avanceret cyberangreb, der ved hjælp af både malware rettet mod industrielle kontrolsystemer og wipere havde til formål at lamme landets strømforsyning.

Ruslands mere konventionelle angreb med bl.a. droner og missiler har understreget, at energisektoren er et prioriteret mål for Rusland i en konfliktsituation. Rusland gik målrettet efter kritisk infrastruktur, da angrebene mod Ukraine blev intensiveret i oktober 2022. Op mod 30% af landets kraftværker blev ifølge Ukraines præsident Volodymyr Zelenskiy sat ud af drift.

Destruktive angreb kan sprede sig

CFCS vurderer, at der i forbindelse med konfliktsituationer er en øget risiko for, at destruktive cyberangreb kan sprede sig og ramme ofre uden for selve konfliktzonen. Det er særligt aktuelt i forbindelse med krigen i Ukraine.

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 satellit-modemmer, særligt i Europa, fik slettet deres opsætning. Viasat er en amerikansk udbyder af 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 viste, hvordan destruktive cyberangreb kan have konsekvenser for mange andre end det umiddelbare offer. Ifølge åbne kilder betød angrebet, at den tyske energivirksomhed Enercon mistede evnen til at fjernkontrollere tusindvis af vindmøller. NotPetya-angrebet i 2017 er et andet kendt eksempel på cyberangreb, der fik alvorlige afledte konsekvenser langt fra det egentlige mål.

Stater udvikler løbende deres kapacitet til at udføre destruktive cyberangreb

CFCS 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.

Cyberspionage kan give adgang til kritisk infrastruktur, som stater kan forsøge at ødelægge eller forstyrre i en alvorlig krise eller krig. Amerikanske myndigheder har flere gange i 2022 advaret om cybertruslen mod industrielle kontrolsystemer. Russiske hackere, der tidligere har benyttet malwaren Triton, forsøger ifølge FBI stadig aktivt at kompromittere virksomheder i energisektorer verden over. Triton er en destruktiv malware, som er udviklet til at påvirke sikkerhedsmekanismer i industrielle kontrolsystemer. Triton kan derfor potentielt påvirke fysiske processer i eksempelvis energiproduktion. CISA advarede ligeledes om, at ondsindede aktører har udvist evnen til at få fuld systemadgang til visse industrielle kontrolsystemer.

Forberedelsen af destruktive cyberangreb vil ofte bestå i en kortlægning af organisationer, systemer og netværksenheder, f.eks. industrielle kontrolsystemer. Ved at opnå viden om organisationer og systemer kan hackere udvikle specialiseret malware. Derudover kan hackere etablere såkaldte bagdøre på kompromitterede systemer, som de kan benytte i senere destruktive angreb. Det er derfor vigtigt, at virksomheder og myndigheder er opmærksomme på, om deres systemer bliver forsøgt kompromitteret. En kompromittering kan nemlig, udover tab af vigtig viden, være første skridt mod fremtidige destruktive angreb.

Cyberterror

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

Det betyder, at det er usandsynligt, at energisektoren, vil blive udsat for forsøg på cyberterror inden for de næste to år.

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

Så alvorlige cyberangreb forudsætter tekniske evner og organisatoriske ressourcer, som militante ekstremister aktuelt ikke har. Hensigten er samtidigt yderst begrænset.

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 sandsynligheder i analyser

Usandsynligt | **Mindre sandsynligt** | **Muligt** | **Sandsynligt** | **Meget sandsynligt**

"FE vurderer" svarer til "Sandsynligt", medmindre en anden sandsynlighed er angivet.