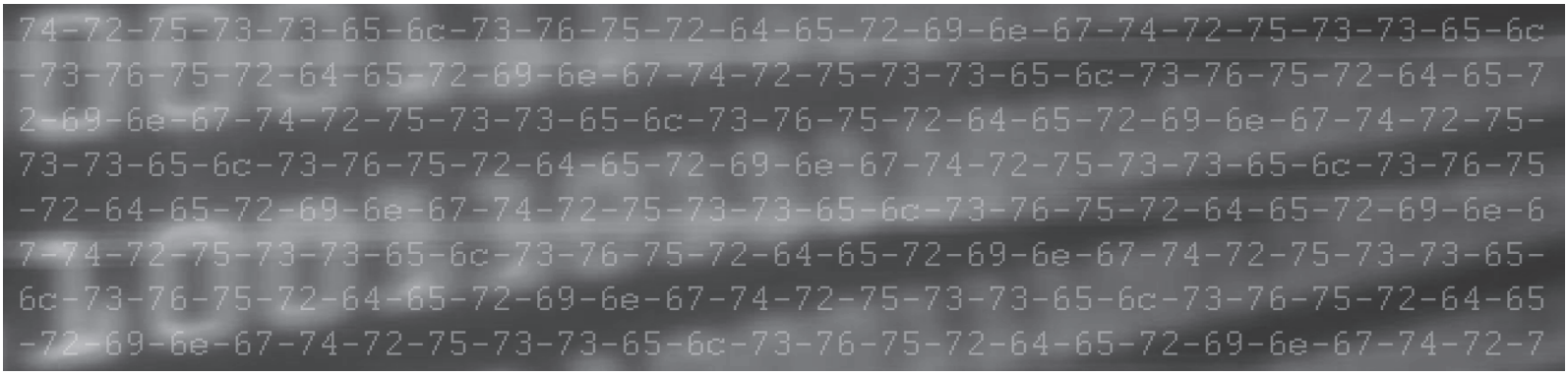
CENTER FOR CYBERSIKKERHED

Trusselsvurdering

Cybertruslen mod energisektoren



Trusselsvurderingsenheden ved Center for Cybersikkerhed

September 2018

CENTER FOR CYBERSIKKERHED

Trusselsvurdering: Cybertruslen mod energisektoren

Trusselsvurderingen redegør for de cybertrusler, som er rettet mod energisektoren i Danmark. Energisektoren har direkte betydning for samfundets funktion, stabilitet og sikkerhed. Trusselsvurderingen udgives til anvendelse i bl.a. risikovurderingen for sektoren i forbindelse med den nationale strategi for cyber- og informationssikkerhed.

Hovedvurdering:

- Truslen fra cyberspionage mod energisektoren er **MEGET HØJ.** CFCS vurderer, at fremmede stater blandt andet har interesse i at stjæle informationer til styrkelse og udvikling af deres egen energisektor eller til brug i en evt. politisk eller militær konflikt. Der har i det seneste år været forsøg på kompromittering af den danske energisektor.
- Truslen fra cyberkriminalitet mod energisektoren er **MEGET HØJ**. Cyberkriminelle angreb, der har til formål at låse it-netværk og it-infrastruktur, kan i værste fald true forsyningssikkerheden.
- Truslen fra cyberaktivisme mod energisektoren er **LAV.** Truslen er ofte motiveret af enkeltsager, og truslen mod energisektoren kan stige uden eller med kort varsel.
- Truslen fra cyberterror mod energisektoren er **LAV**. CFCS vurderer, at militante ekstremister har begrænsede evner og ressourcer til at udføre alvorlige cyberangreb, og selv om de i få tilfælde har ytret interesse for at udføre cyberterror, har de aktuelt ikke kapacitet til dette.
- CFCS vurderer, at det på kort sigt er mindre sandsynligt, at fremmede stater vil rette destruktive cyberangreb mod samfundsvigtig infrastruktur i Danmark, herunder i energisektoren. Truslen kan dog ændre sig i forbindelse med en skærpet politisk eller militær konflikt med visse lande.

Indledning

Denne vurdering beskriver cybertruslen mod energisektoren i Danmark. Energisektoren har en samfundskritisk opgave med at levere energi til hele Danmark, herunder landets samfundsvigtige sektorer. Forsyningssikkerhed er desuden en konkurrenceparameter for Danmarks evne til at tiltrække virksomheder med særlige energibehov såsom datacentre, der i 2040 vurderes at kunne stå for op mod en tredjedel af dansk elforbrug. Energisektoren er dermed kritisk for samfundets funktion, stabilitet og velfærd.

Energisektoren inkluderer virksomheder, der har betydning for produktion, transmission og distribution af elektricitet og naturgas i Danmark. Energisektoren er ikke kun vigtig for Danmark, men også for de nabolande det danske el- og gasnet er forbundet med. Trusselsvurderingen giver et overblik over

cybertruslerne mod sektoren som helhed, og der skelnes kun mellem enkeltdele af sektoren i et begrænset omfang.

Energisektoren i Danmark

Energisektoren i Danmark er opdelt i tre typer af virksomheder i forhold til deres rolle med at sikre energiforsyningen. De er hhv. opdelt i produktion af el og gas, transmission på nationalt plan og distribution til kunderne. Der er på nuværende tidspunkt i energisektoren cirka 80 virksomheder, der er forpligtiget til at være tilsluttet forsyningsnettene i forhold til den nationale forsyningssikkerhed.

Unikt for transmissionen er der kun én såkaldt Transmission System Operatør (TSO). Energinet ejer og driver det overordnede transmissionsnet i Danmark for el og naturgas. Mængden af produktion af el og gas bliver styret iht. retningslinjer fra Energinet.

Danmark er et knudepunkt i det europæiske el- og naturgasnet. Danmark er eksempelvis et knudepunkt i Baltic Pipe-projektet, der skal føre gas fra Nordsøen gennem Danmark til Polen. Danmark er serviceudbyder for driften af børsen for handel med el for landene i Norden og Baltikum. Danmark er udpeget til at være udbyder af et fælles nordeuropæisk center, Nordic Regional Security Coordinator, for de transmissionsansvarlige virksomheder i Danmark, Finland, Norge og Sverige.

Hvad er cybertrusler?

Forsvarets Efterretningstjenestes Center for Cybersikkerhed (CFCS) definerer cybertrusler som trusler fra cyberangreb, hvor en aktør forsøger at forstyrre eller få uautoriseret adgang til data, systemer, digitale netværk eller digitale tjenester.

Trusselsbilledet kan beskrives ud fra flere vinkler. I denne vurdering er der fokus på, hvilket formål anvendelsen af cyberangreb har for de aktører, der udfører dem. CFCS beskriver og vurderer her aktiviteter, der har til formål at udføre eller begå cyberspionage, cyberkriminalitet, cyberaktivisme eller cyberterror. Desuden vurderer CFCS den potentielle trussel fra destruktive cyberangreb.

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

Vurderingen beskriver det aktuelle trusselsbillede og har en varslingshorisont på 0-2 år. Da cybertruslen for energisektoren er dynamisk, kan trusselsbilledet på nogle områder ændre sig pludseligt, både generelt og for den enkelte myndighed eller virksomhed. Forsvarets Efterretningstjenestes trusselsniveauer og sandsynlighedsgrader er forklaret i slutningen af vurderingen.

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

Cyberspionage

Truslen fra cyberspionage mod energisektoren er **MEGET HØJ.** CFCS vurderer, at truslen især er rettet mod produktions- og transmissionsselskaber i energisektoren.

Dette underbygges af, at der i de seneste år har været forsøg på kompromittering af den danske energisektor. CFCS har eksempelvis konstateret, at der har været flere målrettede forsøg på at få uautoriseret adgang til organisationer i den danske energisektor i 2017 gennem såkaldte spear phishing og vandhulsangreb. CFCS vurderer, at hændelserne var forsøg på cyberspionage udført af en statslig aktør med tilknytning til et andet lands efterretningstjeneste. CFCS vurderer, at der er tale om en vedvarende trussel fra fremmede stater.

Danmark er et foregangsland indenfor energisikkerhed og overgangen fra fossile brændstoffer til grøn energi. Danmark er samtidigt et knudepunkt i det europæiske el- og naturgasnet, hvor Danmark spiller en væsentlig rolle i udveksling af el og gas i Europa. Den danske energisektors fremtrædende position betyder, at fremmede stater kan have en særlig interesse i sektoren, eksempelvis for virksomheder og myndigheder, der har tilknytning til gasledningsprojekterne Baltic Pipe og Nord Stream 2.

Udvekslingen af el og gas på tværs af landegrænser betyder, at truslen ikke er geografisk afgrænset. Interesse i energiforsyningen i et land kan motivere en aktør til at spionere mod nabolande, der leverer el eller gas til det pågældende land.

Cyberspionage mod energisektoren kan være både politisk og økonomisk motiveret. Spionagen kan bl.a. skaffe viden, der kan bruges til at komme i besiddelse af nye teknologier til at styrke og udvikle egen energisektor, eksempelvis inden for udvikling af grøn teknologi, eller viden, der kan fremme egne energipolitiske interesser.

Cyberspionage udgør også en potentiel trussel mod forsyningssikkerheden i Danmark. Indhentning af information om kritisk infrastruktur kan benyttes i forberedelsen af destruktive cyberangreb eller fysiske angreb rettet mod sektoren, i forbindelse med en krise eller konflikt.

Nogle lande udfører også cyberspionage mod virksomheder, der samarbejder med deres egne nationale virksomheder eller myndigheder. Denne spionage kan ses som overvågning af samarbejdspartnere og virksomheder, der kan have indflydelse på nationale organisationer. Amerikanske myndigheder har eksempelvis beskyldt Kinas militær for cyberspionage mod amerikanske virksomheder, bl.a. i forbindelse med forhandlinger med det statsejede China National Offshore Oil Corporation. Her gik kinesiske hackere ifølge amerikanske myndigheder specifikt efter oplysninger om forhandlingerne.

Andre lande står sandsynligvis også bag cyberspionage mod energisektoren verden over. Russiske hackere har ifølge amerikanske og britiske myndigheder stået bag flere globale forsøg på cyberspionage mod energisektoren i de seneste år.

Statsstøttede hackergrupper kompromitterer også it-systemer på tværs af sektorer, der deler samme it-sårbarheder, uafhængigt af deres umiddelbare relevans som spionagemål. Virksomheder i energisektoren kan derfor også blive udsat for sådanne cyberangreb.

Baltic Pipe og Nord Stream 2

Baltic Pipe anlægsprojektet har til formål at etablere en gasledningsforbindelse fra Nordsøen gennem Danmark til Polen via Østersøen. Det skal have en årlig gennemstrømningskapacitet på 10 milliarder kubikmeter gas.

Nord Stream 2 projektet har til formål at etablere en gasledningsforbindelse fra Rusland til det nordlige Tyskland via Østersøen. Forbindelsen skal have en årlig gennemstrømningskapacitet på 55 milliarder kubikmeter gas.

Danmarks samlede årlige gasforbrug er til sammenligning på cirka 2,5 milliarder kubikmeter.
Nord Stream 2 og Baltic Pipe forbindelserne skal krydse hinanden i Østersøen.

Faktaboksen er revideret 7. september 2018, så det klart fremgår, at der ikke er truffet dansk beslutning om projekterne.

Cyberkriminalitet

Truslen fra cyberkriminalitet er **MEGET HØJ.** Energisektoren står over for truslen fra både målrettede angreb fra cyberkriminelle og angreb rettet mod et stort antal ofre, der også rammer sektoren.

I denne trusselsvurdering dækker begrebet cyberkriminalitet i udgangspunktet tilfælde, hvor personer og netværk bruger cyberangreb til at begå kriminelle handlinger, hvor formålet er berigelse. Det er eksempelvis tyveri af penge eller finansielle og personlige oplysninger, bedrageri og afpresning.

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

Der er cyberkriminelle netværk, der arbejder organiseret og langsigtet. Nogle cyberkriminelle grupper kan udføre målrettede og avancerede cyberangreb, hvor de f.eks. stjæler fra eller afpresser myndighe-

der og virksomheder for meget store beløb. Andre netværk har specialiseret sig i angreb, der er i stand til at kompromittere et meget stort antal ofre verden over. Mens disse angreb teknisk set ikke er så avancerede, er der tale om velorganiserede, gentagne angreb i næsten industriel skala.

CFCS har kendskab til hændelser i energisektoren, hvor virksomheder er blevet ramt af ransomware. Eksempelvis var distributionsselskabet NRGi i 2015 udsat for et målrettet angreb fra cyberkriminelle, der påvirkede virksomhedens forretningssystemer i væsentlig grad. I NRGi-sagen havde cyberkriminelle ikke adgang til kritiske netværk, men ransomwareangrebet påvirkede deres it-infrastruktur på det administrative netværk.

Angreb med det formål at låse administrative it-netværk og it-infrastruktur kan i værste fald true forsyningssikkerheden. Det kan enten ske som en konsekvens af, at cyberkriminelle inficerer kritiske systemer med eksempelvis ransomware, eller hvis et ransomwareangreb mod administrative netværk vanskeliggør kontrol og vedligeholdelse af kritiske systemer. Angrebet kan også skade virksomhedens økonomi så alvorligt, at det lokalt kan påvirke energiforsyningen, hvis virksomheden ikke længere er finansielt i stand til at opretholde sin drift.

Virksomheder i energisektoren i Danmark har været udsat for forsøg på Business Email Compromise bedrageri (BEC), hvor kriminelle har forsøgt at snyde virksomheden til at overføre penge til de kriminelles egne konti ved at udgive sig for at være en ledende medarbejder. Energinet var eksempelvis udsat for et bedrageriforsøg i maj 2018 i forbindelse med et direktørskifte, hvor kriminelle udgav sig for at være den nye direktør. Opmærksomme ansatte i Energinet og gode procedurer afværgede dog bedrageriforsøget.

Mens der i dette bedrageriforsøg ikke var tale om en kompromittering af it-systemer, afspejler det truslen fra bedrageriske e-mails og misbrug af virksomheds- og personoplysninger. Sker sådanne angreb i fremtiden fra kompromitterede e-mailkonti i virksomhederne, vil det være vanskeligere for den enkelte virksomhed at erkende angrebet i tide.

Eksempler på kriminelle cyberangreb, der kan ramme sektoren

Her er en gennemgang af typiske angreb udført af cyberkriminelle, der kan ramme energisektoren. Listen er ikke udtømmende.

Ransomwareangreb

Ransomware bliver, som andre typer malware, typisk spredt via phishing-mails eller via inficerede hjemmesider, som offeret besøger. Ransomware gør offerets data eller systemer utilgængelige, og bagmændene kræver en løsesum for at gøre disse tilgængelige igen. Der findes mange varianter af ransomware. Mere målrettede ransomwareangreb forsøger at ramme eksempelvis administrative netværk i specifikke virksomheder og myndigheder.

Inficering med andre typer malware

Cyberkriminelle distribuerer fortsat flittigt andre typer malware. Disse typer malware bruges bl.a. til at

stjæle personlige og finansielle oplysninger, der kan sælges eller misbruges af kriminelle. En nyere type malware kaldet mineware inficerer computere med henblik på at misbruge maskinkraft til at tjene kryptovalutaer i såkaldt kryptomining.

Målrettet afpresning
Som en nyere tendens er der grupper, der specialiserer sig i at stjæle følsomme oplysninger om virksomheders kunder og forretning med henblik på afpresning. Trusler om overbelastningsangreb via internettet, såkaldte DDoS-angreb, benyttes også som afpresning. Ofte kræver de cyberkriminelle meget store pengebeløb af deres ofre.

Bedrageri
Såkaldte BEC (Business Email Compromise) scams har til formål at franarre virksomheder og organisationer penge gennem falske anmodninger om pengeoverførelser. For at udnytte medarbejdernes loyalitet udgiver de kriminelle sig typisk for at være en ledende medarbejder i organisationen. Bedrageri af denne type kaldes derfor også for CEO-fraud eller direktørsvindel.

Cyberaktivisme

Truslen fra cyberaktivisme er **LAV**.

Der er eksempler på cyberaktivisme mod energisektoren i udlandet, men CFCS vurderer, at der ikke er et fokus på energisektoren i Danmark fra cyberaktivister. Cyberaktivister retter generelt sjældent deres fokus mod danske myndigheder og virksomheder. Nogle hackergrupper og individer i cyberaktivistiske netværk har dog væsentlige evner og ressourcer til at udføre cyberangreb. Truslen kan derfor pludseligt stige, hvis danske myndigheder eller virksomheder i sektoren kommer i cyberaktivisters søgelys.

Cyberaktivister bruger forskellige typer simple cyberangreb, eksempelvis gør de hjemmesider utilgængelige ved hjælp af DDoS-angreb. De hacker også hjemmesider eller profiler på sociale medier og indsætter budskaber. Nogle lækker følsomme oplysninger fra hack af f.eks. personlige mailkonti for at skabe opmærksomhed om deres sag.

Cyberaktivistiske grupper benyttes af visse lande som dække i forsøg på at påvirke den folkelige meningsdannelse i andre lande. Truslen er størst, hvor der er modstridende interesser fra andre lande og hvor den offentlige meningsdannelse kan påvirke beslutningerne.

No Nuclear Power Plant Group

Der er eksempler fra udlandet på brug af falske cyberaktivister i forbindelse med hackerangreb mod energisektoren. I 2014 tog en tidligere ukendt gruppe ved navn No Nuclear Power Plant Group ansvaret for et cyberangreb, hvor der bl.a. blev brugt sletteværktøjer mod det sydkoreanske Korea Hydro & Nuclear Power Co Ltd. Sydkoreanske myndigheder tilskrev på baggrund af tekniske beviser imidlertid angrebet til Nordkorea.

Cyberaktivisme kan ledsage mere traditionel politisk aktivisme. I 2013 iværksatte cyberaktivister eksempelvis en kampagne mod myndigheder og virksomheder i kølvandet på protester i Canada mod etableringen af en gasledning med hack af en række hjemmesider. I 2016 iværksatte cyberaktivister en kampagne med DDoS-angreb og hack af hjemmesider i protest mod etableringen af Dakota Access Pipeline i USA.

Cyberaktivister angriber også myndigheder og virksomheder, som hackerne betragter som symbolske mål, selvom de ikke har været direkte indblandet i den sag, som har fanget hackernes opmærksomhed. I juli 2016 blev et tyrkisk energiforsyningsselskab, Izmir Gaz, eksempelvis udsat for cyberaktivisme som reaktion på den tyrkiske regerings håndtering af kupforsøget samme år.

Cyberterror

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

CFCS vurderer, at militante ekstremister har begrænsede evner og ressourcer til at udføre alvorlige cyberangreb, og selv om de i få tilfælde har ytret interesse for at udføre cyberterror, har de aktuelt ikke kapacitet til dette.

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

Destruktive cyberangreb

Evnen til at kunne gennemføre destruktive cyberangreb er et potentielt magtmiddel, som flere stater opbygger.

CFCS vurderer, at det på kort sigt er mindre sandsynligt, at fremmede stater vil rette destruktive cyberangreb mod samfundsvigtig infrastruktur i Danmark, herunder i energisektoren. Truslen kan dog ændre sig i forbindelse med en skærpet politisk eller militær konflikt med lande, der besidder denne kapacitet.

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.

Energisektorens samfundskritiske funktion betyder, at sektoren er et potentielt mål for destruktive cyberangreb, såfremt fremmede stater retter fokus mod Danmark.

Det er muligt, at danske virksomheder og myndigheder kan blive ramt som følgevirkning af destruktive cyberangreb mod mål uden for Danmark. Det gælder især danske virksomheder og myndigheder, der er til stede i konfliktområder i Østeuropa, Mellemøsten og Østasien, hvor fremmede stater flere gange har udført destruktive cyberangreb. NotPetya-angrebet i Ukraine i 2017 viste, at destruktive cyberangreb kan sprede sig til organisationer uden for de nævnte typiske konfliktområder.

Ukraine, Sydkorea og Saudi-Arabien har i de seneste år været udsat for flere destruktive cyberangreb rettet mod bl.a. energisektoren. Disse cyberangreb er sandsynligvis blevet udført af statslige aktører som led i regionale konflikter og spændinger.

Angrebene i udlandet har typisk været rettet mod produktionsvirksomheder, men CFCS vurderer, at der er tale om en potentiel trussel mod hele energisektoren, idet et nedbrud helt eller delvist kan påvirke forsyningssikkerheden.

De destruktive cyberangreb mod energisektoren i Ukraine, der førte til strømafbrydelse i hhv. 2015 og 2016, er kendte eksempler på cyberangreb rettet mod energisektoren i udlandet. CFCS vurderer, at den ukrainske energiteknologi, herunder protokoller og udstyr, i stor udstrækning er den samme som i den danske energisektor. Angrebene i Ukraine ville derfor også kunne ske på tilsvarende måde i Danmark.

Informationer indhentet gennem spionage kan bruges i planlægning af destruktive cyberangreb, og der er derfor en kobling mellem truslen fra cyberspionage og truslen fra destruktive cyberangreb. En allerede kompromitteret virksomhed eller myndighed er derfor mere sårbar over for destruktive cyberangreb.

Der er i de seneste år sket en udbredelse af metoder og værktøjer på internettet, såsom AutoSploit og ICSSploit, rettet mod bl.a. sårbarheder i industrielt udstyr. Disse værktøjer gør det lettere for hackere at finde sårbarheder i samfundsvigtig infrastruktur, som kan udnyttes i destruktive cyberangreb.

Trusselsniveauer

Forsvarets Efterretningstjeneste bruger følgende trusselsniveauer.

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

FE bruger denne skala for sandsynlighed i analyser: