CENTER FOR CYBERSIKKERHED

Trusselsvurdering:

Virksomheder i energisektoren er attraktive mål for ransomware

1. udgave oktober 2021

Indhold

CENTER FOR CYBERSIKKERHED

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

1. udgave oktober 2021

Virksomheder i energisektoren er attraktive mål for ransomware

Formålet med denne trusselsvurdering er at gøre virksomheder i den danske energisektor opmærksomme på den fortsatte trussel fra ransomware-angreb i kølvandet på angrebet mod Colonial Pipeline i maj 2021. Selvom truslen ikke er specifikt målrettet sektoren, er de mulige konsekvenser ved succesfulde angreb omfattende og kræver et højt beredskab.

Hovedvurdering

- Truslen fra cyberkriminalitet mod den danske energisektor er **MEGET HØJ.** Der er fortsat kriminelle grupper, der har kapacitet til og intention om at rette ransomware-angreb mod virksomheder i sektoren, på trods af at visse hackere har meldt ud, at de ikke længere vil ramme kritisk infrastruktur.

- Virksomheder i energisektoren er af flere årsager attraktive mål for cyberkriminelle. De mulige konsekvenser ved operationelle driftsforstyrrelser benyttes af nogle kriminelle til at øge presset på deres ofre.

- På trods af stor opmærksomhed på cybersikkerhed bliver OT-systemer (Operationel Teknologi) ramt af ransomware-angreb. Ransomware-angreb mod IT-systemer kan også indirekte påvirke den operationelle drift, som det skete for Colonial Pipeline.

Darkside er væk – det er truslen fra ransomware ikke

CFCS vurderer, at truslen fra cyberkriminalitet, herunder ransomware-angreb, rettet mod den danske energisektor, er **MEGET HØJ**.

Truslen er uændret på trods af, at flere store udbydere af ransomware-as-a-service (RaaS) i kølvandet på alvorlige angreb mod bl.a. Colonial Pipeline i foråret og sommeren 2021 meldte ud, at de fremover ikke vil angribe kritisk infrastruktur. Hackernes udmeldinger skete i en kontekst af, at amerikanske myndigheder øgede deres fokus på ransomware-angreb og nu betegner alvorlige ransomware-angreb som en trussel mod den nationale sikkerhed.

Selv hvis de få pågældende RaaS-udbydere fremover ikke angriber kritisk infrastruktur i bl.a. energisektoren, så er der andre grupper, der har kapacitet til og intention om at rette ransomware-angreb mod virksomheder i sektoren. At truslen er uændret understreges af nylige angreb som eksempelvis angrebet på Kalundborg Forsyning i slutningen af august 2021 og Lockbit 2.0's angreb på italienske ERG i slutningen af juli 2021.

Ransomware-as-a-Service (RaaS)
RaaS gør det muligt for kriminelle at købe sig til adgange, værktøjer og infrastruktur, som de bruger i ransomware-angreb, frem for at udvikle det selv. RaaS har introduceret en form for platformsøkonomi til cyberkriminalitet, hvor hackerne gennem ransomware-angreb samtidigt tjener penge til sig selv og til de bagmænd, der ejer platformen. Et eksempel på en RaaS-platform er Darkside, som blev brugt i angrebet mod Colonial Pipeline.

Efterspillet fra Colonial Pipeline
Den amerikanske virksomhed Colonial Pipeline, der forsyner store dele af den amerikanske østkyst med brændstof, blev i maj 2021 ramt af et ransomware-angreb. I seks dage holdt virksomheden rørledningen lukket, mens frygten for brændstofmangel og køerne ved tankstationer voksede. Angrebet blev udført med ransomwaren DarkSide, som blev udbudt via en RaaS-platform. Hackerne fik angiveligt adgang til Colonial Pipelines IT-systemer via en VPN-adgang, som skulle have været inaktiv. Den efterfølgende nedlukning af rørledningen skete ifølge Colonial Pipeline på deres eget initiativ ud fra et forsigtighedsprincip. Colonial Pipeline betalte en løsesum på over fire millioner dollars i forsøget på hurtigt at genetablere deres drift.

Det øgede fokus fra især amerikanske myndigheder på RaaS-udbydere efter Colonial Pipeline-angrebet medførte visse ændringer i Raas-miljøet. Blandt andet meldte udbyderne af Darkside ud, at det ikke var deres mening at ramme kritisk infrastruktur,

og at de ville undgå det i fremtiden. Darkside lukkede efterfølgende deres platform helt ned.

Ændringerne i RaaS-miljøet er uddybet i CFCS' trusselsvurdering "Gamle trusler på nye platforme", der er tilgængelig på CFCS' hjemmeside. Trusselsvurderingen konkluderer, at ændringerne ikke har sænket det generelle trusselsniveau. Trusselsvurderingen beskriver bl.a., at selvom flere dominerende RaaS-platforme lukkede ned i 2021, blev tomrummet efter nedlukningerne hurtigt udfyldt af andre platforme. Udbyderne af en af platformene, REvil, har derudover genaktiveret deres infrastruktur efter nedlukningen.

Ransomware kan ramme alle – også energisektoren

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 relativ stor finansiel omsætning. For kriminelle grupper vil alene omsætningen betyde, at disse virksomheder er attraktive ofre, da de kriminelle kalkulerer med, at virksomhederne er i stand til at betale en høj løsesum. Det er meget sandsynligt, at der de kommende par år fortsat vil være kriminelle, der vejer den mulige fortjeneste højere end risikoen for at komme i myndighedernes søgelys.

Et andet 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 derfor være fristende for virksomheden at betale løsesummen. At betale løsesummen er dog ikke nogen garanti for, at driften kan genoptages med det samme. Det har eksempelvis været berettet i flere medier, at Colonial Pipeline benyttede egne backups til at genoprette deres systemer, da dekrypteringsnøglen, som de havde betalt for, var meget langsom.

Nogle kriminelle bruger aktivt truslen om driftsforstyrrelser til at presse ofrene til at betale løsesum. RaaS-gruppen Lockbit 2.0 har eksempelvis brugt angrebet mod Colonial Pipeline som skræmmebillede for at lægge pres på et offer i transportsektoren i udlandet. Hvis ikke virksomheden betalte løsesummen, kunne konsekvenserne, ifølge de kriminelle, blive i målestok med Colonial Pipeline-angrebet.

OT-systemer under direkte og indirekte angreb

Et højt niveau af cybersikkerhed gør det svært for hackere at påvirke den operationelle drift via OT-systemer (Operationel Teknologi), men det viser sig gang på gang, at det ikke er umuligt. Eksempelvis har der i Danmark i 2021 været et ransomware-angreb mod en dansk virksomhed, hvor computere på OT-netværket fik krypteret filer, hvilket førte til et midlertidigt driftsnedbrud. Angrebet skete via en underleverandør. I 2021 har der også været flere udenlandske eksempler på ransomware-angreb, der har ramt enheder i OT-systemer, dog uden at det har haft alvorlige konsekvenser for produktionen.

Flere og flere virksomheder, også i energisektoren, udnytter muligheden for at overvåge eller automatisere fysiske processer via "smarte enheder", der forbinder dele af den industrielle proces til IT-systemet via internettet. Det bliver også kaldt det Industrielle Internet Of Things (IIoT). At den fysiske produktion går online medfører en række nye sikkerhedsudfordringer og sårbarheder.

Ransomware-angreb mod en virksomheds IT-system kan presse virksomheder til selv at lukke ned for deres OT-systemer for at imødegå angrebene og undgå, at de spreder sig. Det var som tidligere nævnt tilfældet hos Colonial Pipeline, der selv har beskrevet, at man lukkede ned for OT-systemerne for at undgå, at malwaren spredte sig til dem. Ransomware-angreb mod en virksomheds IT-system kan desuden tvinge virksomheder til at overgå til manuel produktion, som det var tilfældet, da Norsk Hydro blev ramt af ransomware i 2019.

Et direkte eller indirekte angrebet OT-system – eller usikkerhed herom - kan have store økonomiske konsekvenser for den ramte virksomhed. Rammes virksomheder i energisektoren, kan effekterne også påvirke den enkelte borger og samfundet som helhed. Den løbende sammensmeltning mellem IT og OT – mellem cyber og den fysiske verden – forstærker yderligere de konsekvenser, som et angreb kan have.

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 plan-lægning. 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.

Andre relevante publikationer

Center for Cybersikkerhed (CFCS) udgiver løbende vejledninger og trusselsvurderinger. Nedenfor er fremhævet en række produkter af særlig relevans for energisektoren. Alle produkterne er tilgængelige på CFCS' hjemmeside.

Ændringer i Ransomware-as-a-Service-landskabet efter Colonial Pipeline
Trusselsvurderingen "Gamle hackere på nye platforme" beskriver, hvordan de kriminelle netværk, der står bag ransomware-angreb, har omorganiseret sig efter angrebet mod Colonial Pipeline.
Læs vurderingen her:
https://cfcs.dk/da/cybertruslen/trusselsvurderinger/gamle-hackere-pa-nye-platforme/

Cybertruslen mod Danmark (2021)
I den årlige trusselsvurdering beskriver CFCS truslen mod Danmark fra cyberangreb, der understøtter kriminalitet, spionage, destruktive cyberangreb, aktivisme og terrorisme.
Læs vurderingen her:
https://cfcs.dk/da/cybertruslen/trusselsvurderinger/cybertruslen-mod-danmark/

Pas på din virksomheds produktion
I vejledningen "Ledelsens opgaver i forbindelse med sikring af industrielle kontrolsystemer" beskriver CFCS, hvad virksomhedens ledelse kan gøre for at sikre industrielle kontrolsystemer mod cyberangreb.
Læs vejledningen her:
https://cfcs.dk/da/forebyggelse/vejledninger/ics-ledelsen/

Cybertruslen mod energisektoren (2018)
I trusselsvurderingen beskriver CFCS det generelle trusselsniveau for energisektoren. Trusselsvurderingen henvender sig særligt til de myndigheder og organisationer, der deltager i udmøntningen af den nationale cyber- og informationsstrategi.
Læse trusselsvurderingen her:
https://cfcs.dk/da/cybertruslen/trusselsvurderinger/energi/

Samarbejdet mellem cyberkriminelle
Trusselsvurderingen "Drømmer cyberkriminelle om tillidsfulde relationer?" beskriver, hvordan veletablerede samarbejdsrelationer, arbejdsdeling og udveksling af tjenester i det kriminelle miljø bidrager til den meget høje trussel fra cyberkriminalitet i almindelighed og målrettede ransomware-angreb i særdeleshed.
Læs vurderingen her:
https://cfcs.dk/da/cybertruslen/trusselsvurderinger/organiseret-cyberkriminalitet/

Truslen fra målrettede ransomware-angreb
Trusselsvurderingen "Digitale gidseltagere på storvildtjagt" beskriver truslen fra målrettede ransomware-angreb, der kan have alvorlige konsekvenser for en organisation. Læs vurderingen her:
https://cfcs.dk/da/cybertruslen/trusselsvurderinger/malrettet-ransomware/

Reducér risikoen for ransomware
I vejledningen "Reducér risikoen for ransomware" kan du læse mere om en række anbefalinger, som organisationer bør overveje for at reducere risikoen for at blive ramt af et ransomware-angreb samt mindske konsekvenserne ved et evt. angreb. Læs vejledningen her:
https://cfcs.dk/da/forebyggelse/vejledninger/ransomware/