SEKTOR CERT

De danske perspektiver på angrebet mod **Polens grønne elnet**

Rapport med fokus på de danske perspektiver af angrebet.
Baseret på CERT Polskas rapporter.



Oktober 2026

TLP:CLEAR



Indholdsfortegnelse

SIDE-3	**Opsummering**
SIDE-6	**Hvad betyder angrebet for Danmark?**
SIDE-7	Danmarks grønne angrebsflade
SIDE-7	Kan en angriber "vælte" det danske elnet?
SIDE-8	Var maj 2023 et dansk forvarsel?
SIDE-9	Loven var på plads i Danmark, men den er kun en del af svaret
SIDE-10	Anbefalinger
SIDE-14	**Overblik over angrebet**
SIDE-16	De fire mål
SIDE-17	Tidslinje
SIDE-20	**Appendiks: Detaljeret gennemgang af angrebet**
SIDE-21	Del 1: Vejen ind
SIDE-22	Del 2: Det store værk: fra marts til december
SIDE-23	Del 3: Anlæggene: udstyr sat ud af drift, men ingen strømafbrydelser
SIDE-25	Del 4: Det lille værk, hvor dampturbinen standsede
SIDE-26	Del 5: Virksomheden: et opportunistisk mål
SIDE-27	Del 6: Vejen fra vindanlægget til det lille værk
SIDE-28	Del 7: Hvor tæt på en katastrofe var det?
SIDE-29	Del 8: Det var nemt at komme ind, men resten af angrebet var mere sofistikeret
SIDE-30	Del 9: AI sænker barrieren
SIDE-31	Del 10: Attribuering: hvem stod bag?
SIDE-32	**Baggrund for denne rapport**
SIDE-34	**Kilder og noter**

SEKTOR CERT



Opsummering

Snefald over Polen

Sneen føg over Polen, og temperaturen lå under frysepunktet, da der blev gennemført et koordineret cyberangreb mod landets energisektor den 29. december 2025. Mindst 30 vind- og solanlæg, to kraftvarmeværker og en produktionsvirksomhed blev ramt i angrebet.
På det ene kraftvarmeværk blev produktionen af el og varme afbrudt som resultat af angrebet.

Eftersom angrebet ramte præcis den slags spredte, grønne infrastruktur, som få lande læner sig så tungt op ad som Danmark, er det særligt væsentligt at analysere og tage ved lære af.

Denne rapport gennemgår, hvad der skete i Polen, hvorfor angrebet henholdsvis lykkedes og fejlede, og hvilke erfaringer Danmark bør drage, så styrken ved mange små grønne anlæg ikke vendes til en akilleshæl.

Rapporten er udarbejdet i samarbejde med journalisten Henrik Moltke.

Angrebet

Angrebet mod Polens grønne elnet den 29. december 2025 krævede intet specialbygget cybervåben. Angriberne kom ind ad døre, der i praksis stod åbne, som illustreret i Figur 1.
Derefter fulgte den mere sofistikerede del af operationen med stjålne loginoplysninger, systematisk sabotage af genopretningen og, som vi først fik indsigt i i august, et spring ind i et andet anlægs styresystemer gennem et privat mobilnet. En angrebsform, vi ikke har set brugt før mod kritisk infrastruktur.

Resultatet var alvorligere, end de første analyser antog: udstyr sat ud af drift på mindst 30 anlæg, tab af fjernstyring, destruktiv computerkode stoppet i ellevte time og en dampturbine, der gik i stå. På det kraftvarmeværk, hvor dampturbinen standsede, mistede kunderne hverken varme eller strøm. Ikke fordi angrebet fejlede, men fordi operatørerne reagerede, mens angriberen stadig var i netværket.

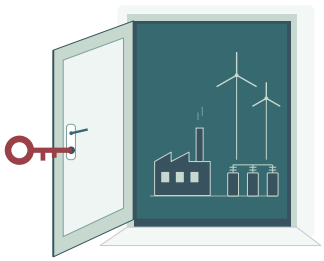
Det nye vi kan tage med fra angrebet, er ikke måden, angriberne kom ind på, men viljen.

Sporene peger mod Rusland

Baseret på flere karakteristika i angrebet konkluderer den polske CERT (cert.pl), at mange spor peger i retning af den russiske trusselsaktør Dragonfly, også kendt som "Static Tundra".

Den 30. juni skærpede Styrelsen for Samfundssikkerhed sin vurdering af truslen fra destruktive russiske cyberangreb mod Danmark med blandt andet angrebet i Polen som eksempel[1], og i juli udpegede Storbritannien og EU officielt Ruslands "FSB's Center 16" som ansvarlig for angrebet i Polen. Hvis denne attribuering er korrekt, har en russisk statsaktør gennemført et destruktivt angreb mod energisektoren i et EU- og NATO-land i fredstid.

Dragonfly er på SektorCERTs top 10-liste over de angrebsaktører, vi forventer vil angribe Danmark[7].
Selvom vi dermed har sandsynliggjort, at netop denne aktør vil angribe os, er det bemærkelsesværdigt, at det, EU kaldte "*forstyrrende sabotageoperationer mod kritisk infrastruktur, herunder kraftvarmeværker*"[2], nu sker i fuld åbenhed.



Figur 1 - Døren stod åben - og nøglen var genbrugt. Angrebet mod Polens grønne elnet den 29. december 2025 krævede intet specialbygget cybervåben. Fjernadgange uden multifaktorgodkendelse og udstyr på fabriksindstillede kodeord var vejen ind.



Det danske perspektiv

For Danmark har angrebet mod Polens grønne elnet gjort særligt tre ting konkrete.

- **Den første er skala**: Den standardisering, der gør små, fjernstyrede grønne anlæg billige at drive, gør også angreb mod dem skalerbare. Og Danmark har flere af den slags anlæg end mange andre lande.
- **Den anden er en helt ny trusselsvektor**: Fejlkonfiguration af mobile netværk i Polen gjorde, at selskaber, der intet har med hinanden at gøre, uforvarende kunne lukke angribere ind i hinandens OT-netværk. I Danmark bruges mobilnettene også i den kritiske infrastruktur, og vi bør derfor lære af Polen på dette punkt.
- **Den tredje er afstanden mellem lov og praksis**: Danmark har siden marts 2025 haft regler, der rammer præcis de polske fejl, men angrebet her rejser to spørgsmål: Bliver reglerne fulgt i praksis, og hvordan håndterer vi de små anlæg, som individuelt falder uden for reglerne, men som tilsammen er vigtige?

Et mønster begynder at danne sig

Det samme mønster har nu vist sig to gange på tre år. Først herhjemme i 2023, da 22 energiselskaber blev angrebet i det største cyberangreb mod kritisk infrastruktur vi har set i Danmark – og senest i Polen. Begge gange var vejen ind den firewall, der skulle holde vagt og forhindre uautoriseret trafik (se Figur 2).
I Danmark var adgangsbilletten i første bølge af angrebet en sårbarhed, leverandøren allerede havde rettet. I Polen var det fjernadgange uden multifaktor samt kodeord, der aldrig var skiftet.

Så længe den slags svagheder består, er omkostningen ved at angribe os ikke højere end fordelen.

Tilbage står derfor ikke et arbejde med at forsvare sig mod en aktør, der bryder ind via avancerede metoder, men det lidt trivielle, men afgørende arbejde: kodeord, der bliver skiftet, opdateringer, der bliver installeret til tiden, unødvendig eksponering, der bliver lukket, og netværk, man ikke selv kontrollerer, der bliver behandlet som usikre.
Det er dét, der gør forskellen, hvis, eller rettere når, turen igen kommer til os.



Figur 2 - Samme mønster, to gange på tre år
Begge gange var vejen ind den boks i kanten af netværket, der skulle holde vagt - og begge gange ramte angrebet mange mindre aktører med det samme udstyr og de samme svagheder



Tæt på en halv million mennesker uden varme

De første udmeldinger fra den polske regering efter angrebet var dramatiske. Vicepremierminister og digitaliseringsminister Krzysztof Gawkowski sagde den 13. januar, at Polen havde været *"tæt på et blackout"*, at der var tale om russisk sabotage, og at *"digitale kampvogne er her allerede"*[3]. Premierminister Donald Tusk anlagde kort efter en mere afdæmpet linje: et forsøg på at destabilisere energiinfrastrukturen, men transmissionsnettet havde *"ikke et øjeblik"* været truet, og et blackout havde *"ikke været på tale"*[4]. Op mod en halv million mennesker kunne dog have mistet varmen, hvis angrebet var lykkedes, sagde han.

Den polske CERT har i månederne siden angrebet arbejdet på at kortlægge, hvad der præcist skete, og har udgivet to dybdegående rapporter af høj kvalitet. Tilsammen tegner de et klarere billede: Nok var Polen ikke tæt på et blackout, men angrebet var heller ikke uden konsekvenser. Flere steder lykkedes det angriberne at gennemføre destruktive og forstyrrende handlinger. På mindst 30 vind- og solanlæg blev udstyr sat ud af drift, og operatørerne mistede evnen til at se og fjernstyre anlæggene. På et mindre kraftvarmeværk blev kraftvarmeproduktionen afbrudt. Forbrugerne blev skånet, fordi operatørerne reagerede med det samme, mens angrebet stadig var i gang.

I sin første rapport, fra januar, betegnede CERT Polska angrebene som *"rent destruktive"* og sammenlignede dem med *"forsætlige brandstiftelser"*. Sikkerhedsfirmaet Dragos, hvis analyse af angrebet også udkom i januar, beskrev hændelsen som det første større cyberangreb mod *"distribuerede energiressourcer (DER): de mindre vind-, sol- og kraftvarmeanlæg, der bliver føjet til elnet verden over"*[5].

Destruktive angreb er nu en realitet

Angrebet minder om den russiske statsaktør Sandworms historiske angreb mod Ukraines elnet. Lillejuleaften ti år før angrebet i Polen slukkede Sandworm for strømmen hos hundredtusindvis af kunder i det vestlige Ukraine, mens operatørerne måbende så fjernstyrede "spøgelseshænder" overtage deres skærme og klikke på afbryderne, én efter én. Et år senere vendte Sandworm tilbage mod Ukraine med Industroyer, et skadeligt program bygget til at kommunikere direkte med elnettets industrielle styresystemer.

Angrebet i Polen var destruktivt ad en helt anden vej. I stedet for at udvikle et højt specialiseret våben mod ét stort anlæg udnyttede angriberne ensartede svagheder i mange mindre anlæg. Den standardisering, der gør grøn energi billigere og lettere at drive, kan altså også hjælpe angribere.

De tekniske hovedkilder peger alle mod en russisk statsaktør, men ikke mod samme del af staten. CERT Polska konkluderer, at angrebets infrastruktur i høj grad overlapper med infrastrukturen benyttet af trusselsaktøren Dragonfly. Andre kilder (ESET og Dragos) peger derimod med moderat sikkerhed på Sandworm[6]. Den 13. juli 2026 udpegede Storbritannien og EU officielt FSB's Center 16 som ansvarlig og indførte sanktioner[2]. Det er den enhed, Dragonfly tilskrives.

For Danmark er to ting vigtigere end navnet:

- at en russisk statsaktør stod bag et destruktivt angreb mod energisektoren i et EU- og NATO-land i fredstid,
- at aktøren Dragonfly, som SektorCERT har på sin top 10-liste i Trusselsvurdering 2026[7] over aktører, der har Danmark i fokus, hermed for første gang offentligt er beskrevet med destruktiv aktivitet.

HVAD BETYDER ANGREBET FOR DANMARK?

Afsnittet gennemgår, hvilke erfaringer Danmark bør drage, så styrken ved Danmarks mange små grønne anlæg ikke vendes til en akilleshæl. Desuden gennemgås de anbefalinger vi har til den danske, kritiske infrastruktur baseret på det vi har lært fra angrebet i Polen.

Selve angrebet i Polen gennemgås i næste kapitel (side 14) samt i yderligere detaljer i Appendiks (side 20).



Hvad betyder angrebet for Danmark?

Danmarks grønne angrebsflade

Det, der gjorde de polske anlæg sårbare (deres antal, deres geografiske spredning og deres ensartede tekniske opsætning), gælder også i Danmark.

SektorCERT beskrev det i sin rapport om angrebet i 2023: *"I et meget decentraliseret energisystem med mange mindre operatører er et angreb mod én sjældent kritisk for samfundet, men den samme sårbarhed hos mange kan blive det"*[8].

Den mekanisme, der binder de to lande sammen, er opsætningen: ens udstyr, central fjernstyring og samme slags svagheder på mange anlæg.

De distribuerede systemer udgør en voksende del af forsyningen i Danmark og dermed en angrebsflade, der vokser i takt med den grønne omstilling. Og som Polen viste, er periferien ikke kun et mål i sig selv. Den kan være vejen ind til noget større.

Opfølgningsrapporten fra CERT Polska fremhævede yderligere en angrebsvinkel, som kan være relevant for danske selskaber med decentral infrastruktur: brugen af private mobilnetværk (såkaldte APN'er).

SektorCERTs vurdering på baggrund af samtaler med både teleselskaber og energiselskaber er, at Danmark står et bedre sted end Polen, fordi brugen af såkaldt klientisolation i disse mobilnetværk er mere udbredt. Men der findes også situationer, hvor klientisolation ikke er valgt til som standard og som dermed kunne blive udsat for et lignende angreb som i Polen[9].

Kan en angriber "vælte" det danske elnet?

Hvor tæt på det var i Polen, behandles i Appendiks (del 7). For danske læsere rejser angrebet et andet spørgsmål: Hvis vores elsystem i endnu højere grad hviler på små, decentrale anlæg, ville et angreb som det polske så kunne vælte det danske elnet?

Med et angreb som det, der ramte Polen, er det korte svar "nej". Men svaret afhænger af, hvilket scenarie man taler om, og af hvor langt den grønne omstilling er nået. Før man svarer, er det værd at skille de tre scenarier ad.

- Én ting er at sætte mange enheder ud af drift, som i Polen.
- Noget andet er at overtage mange enheder på én gang og tænde og slukke dem i takt.
- Det tredje, og mest vidtgående, er et egentligt systemsammenbrud i nettet.

De tre scenarier ligger langt fra hinanden.

Tænd/sluk-scenariet er ofte det, der bekymrer sikkerhedsfolk mest. Solinvertere og elbilladere er oplagte eksempler. De er internetforbundne, talrige og fjernstyrede. Kan adgangen til mange af disse samles ét sted, kan et koordineret indgreb i princippet få systemisk betydning. Det danske elsystem har til gengæld reserver, beskyttelsesrelæer og automatisk udkobling, der skal opfange den slags forstyrrelser, ligesom stærke udlandsforbindelser dæmper konsekvenserne.

Dragos gør regnestykket op for Polen: Selv et samtidigt tab af hele produktionen på de ramte anlæg ville næppe have udløst et landsdækkende blackout, om end lokale udfald var mulige. Men i takt med at lande skærer i de roterende reserver under den grønne omstilling, kan samme type angreb få alvorligere konsekvenser. I regioner med en høj andel af vedvarende energi og begrænset termisk backup kan et koordine-



ret angreb ifølge Dragos udløse kaskadefejl[10].

For Danmark vokser risikoen i takt med antallet af små, fjernstyrede anlæg. Det er ikke en udvikling, sektoren har råd til at lade det komme an på en prøve.

Var maj 2023 et dansk forvarsel?

Danmark havde allerede fået et varsel. I maj 2023 blev 22 selskaber i den danske energi- og varmesektor kompromitteret i det, vi i SektorCERT kaldte det hidtil mest omfangsrige cyberrelaterede angreb mod dansk kritisk infrastruktur[8].

Ligesom i Polen var fællesnævneren sårbare firewalls i kanten af netværket.

For den første bølge af angrebet fandtes der en rettelse: Zyxel havde den 25. april offentliggjort en kritisk sårbarhed med en score på 9,8 ud af 10, og SektorCERT havde sendt en ekstraordinær advarsel ud[11]. Alligevel var mange firewalls ikke opdateret, da angrebet kom den 11. maj, hvilket understreger behovet for mere fokus på den basale sikkerhed.

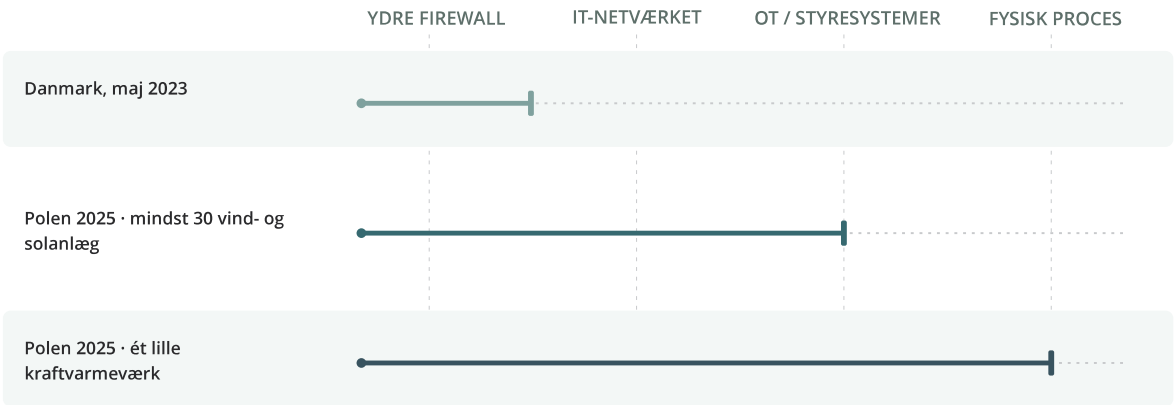
Angrebet ramte 16 nøje udvalgte energiselskaber; en enkelt, særligt konstrueret datapakke mod firewallens VPN-tjeneste var nok til at køre kommandoer med højeste rettigheder uden at logge ind. 11 af selskaberne blev på den måde kompromitteret med det samme. Hos dem overtog angriberne kontrollen med selve firewallen, det vigtigste værn mellem internettet og selskabets industrielle systemer. Men før angriberne nåede videre ind til styresystemerne, blev de opfanget af SektorCERTs sensornet, og samtlige 11 blev sikret i løbet af eftermiddagen, aftenen og natten. Danskerne mærkede derfor intet til angrebet.

Efter ti dages stilhed kom anden bølge den 22. maj, og antallet af kompromitterede selskaber voksede fra 11 til 22 i alt.

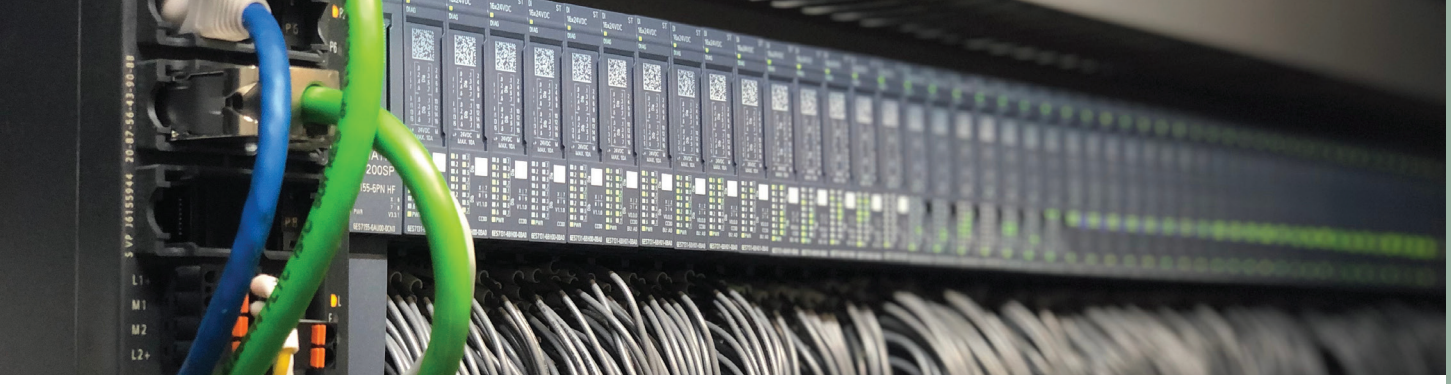
Lighederne med angrebet i Polen er slående. En Zyxel-boks i Danmark, en FortiGate i Polen. Begge steder udgjorde firewallen vejen ind, og begge steder ramte angrebet mange mindre aktører med samme udstyr og samme svagheder. "*Det var præcist det, vi så ske her,*" lød det om den systemiske sårbarhed i rapportens konklusion.

Forskellen lå i udfaldet. I Danmark opfangede sensornettet angriberne, før angrebet blev destruktivt. I Polen blev det standset eller begrænset flere steder (se også Figur 3):

- På det store kraftvarmeværk stoppede sikkerhedssoftware (EDR) wiperen
- På vind- og solanlæggene slap de HMI'er, der havde fået nyt kodeord
- På det mindre kraftvarmeværk blev afbrydelsen inddæmmet af hurtig genopretning



Figur 3 - Hvor langt nåede angriberen?
Samme slags vej ind, tre forskellige udfald. Forskellen lå ikke i metoden, men i hvor tidligt nogen opdagede det.



Alligevel endte det med fjernterminaler sat ud af drift, tabt fjernstyring og en afbrudt kraftvarmeproces.

Maj 2023 var altså et forvarsel. Ikke fordi attribueringen var den samme, men fordi mønstret var det:

- Sårbare enheder i kanten
- Mange mindre aktører med samme opsætning
- En svaghed, der først blev alvorlig, da den fandtes hos mange på én gang

Siden 2023 er de sikkerhedskrav, der ville gøre denne slags angreb væsentligt sværere, blevet skrevet ind i dansk lovgivning.

Det betyder dog ikke, at Danmark dermed er sikret.

Loven var på plads i Danmark, men den er kun en del af svaret

Den 7. marts 2025, ni måneder før angrebet i Polen, trådte Lov om styrket beredskab i energisektoren og bekendtgørelse nr. 260 om modstandsdygtighed og beredskab i energisektoren i kraft[12]. Reglerne udmønter EU's NIS2- og CER-direktiver for energisektoren i Danmark. Det vil sige, at loven sætter rammerne: hvem der er omfattet, tilsyn, påbud og straf for ikke at efterkomme dem.

De konkrete sikkerhedskrav står i bekendtgørelsen. Det er bemærkelsesværdigt, hvor præcist reglerne rammer de polske fejl, i hvert fald hvis de bliver overholdt:

- De polske VPN-adgange stod åbne uden multifaktor. Bekendtgørelsen kræver, at virksomheder "så vidt muligt og hvor relevant" anvender multifaktorautentificering eller kontinuerlig autentificering (§ 53).
- Udstyret kørte på fabriksindstillede kodeord. Bekendtgørelsen kræver, at standardpasswords skiftes ud, før udstyret kobles på virksomhedens netværk (§ 54, stk. 2).
- Angrebet ramte både Windows-siden og de industrielle systemer, og på det mindre kraftvarmeværk gik vejen fra en mobilforbindelse direkte til styringsenhederne. Bekendtgørelsen kræver netværkssegmentering, så forsyningskritiske systemer isoleres (§ 62).
- På det store kraftvarmeværk stoppede EDR-løsningen wiperen, mens den kørte. Bekendtgørelsen kræver logning og monitorering, der kan identificere hændelser, for virksomheder på niveau 2 og 3 (§ 65) og i realtid for niveau 4 og 5 (§ 66), som desuden skal kunne reagere på uregelmæssigheder i realtid (§ 68).
- Angriberne slettede spor og nulstillede udstyr. Bekendtgørelsen kræver en logpolitik og logning, der understøtter myndighedernes efterforskning (§ 64, jf. §§ 65-66).

§ 122 i bekendtgørelsen gør det strafbart at overtræde blandt andet disse bestemmelser. De to fejl, der lukkede angriberne ind i Polen, fjernadgang uden multifaktor og fabriksindstillede kodeord, svarer altså til krav, der var gældende og kunne have udløst bødesanktioner i Danmark, da angrebet skete.

Men billedet er mere nuanceret. Multifaktorkravet er kvalificeret med "så vidt muligt og hvor relevant" og efterlader dermed et fortolkningsrum. Kravet om at skifte fabrikskodeord er derimod ubetinget. Begge krav gælder dog kun for større virksomheder (på niveau 2 og derover). Mindre virksomheder på niveau 1 skal efter bekendtgørelsens § 5 kun overholde en kort, opregnet del af bekendtgørelsen, og hverken multifaktor, standardpasswords eller segmentering står på den liste.

Segmenteringen efter § 62 skal være gennemført senest den 1. marts 2027 for de virksomheder, overgangsreglen gælder for. Kravene om multifaktor og kodeord trådte til gengæld i kraft i marts 2025.

Én begrænsning er vigtig: Små virksomheder, under 50 ansatte og en omsætning eller balance på ikke over 10 millioner euro, er kun



omfattet, hvis de opfylder mindst én betingelse i lovens § 2, stk. 2. Blandt dem er 25 MW elproduktion eller derover, ladepunkter med en samlet kapacitet på 25 MW eller derover, eller et årligt salg på mere end 13,9 GWh fjernvarme eller fjernkøling i 2 ud af de sidste 3 år.

Under de tærskler falder små anlæg uden for loven, og forbrugernære solanlæg, invertere og elbilladere hos private er heller ikke dækket, medmindre ejeren er omfattet som virksomhed. Om de polske anlæg ville have været omfattet, kan ikke afgøres, for kilderne oplyser ikke deres størrelse.

Loven omfatter altså ikke de små anlæg, men en angriber skelner ikke. Polen viste netop, at det er den samlede effekt af mange små, ensartede anlæg, der gør dem interessante.

SektorCERT anbefaler derfor, at også de mindste operatører holder god sikkerhedshygiejne, uanset om reglerne formelt omfatter dem.

Anbefalinger

SektorCERT har samlet 25 konkrete anbefalinger til danske energiselskaber i en håndbog[13]. De bygger på vores analyse af alle succesfulde angreb mod kritisk infrastruktur i Europa siden 2014.
Ingen af anbefalingerne er nye, og ingen af dem er avancerede. Det er netop pointen. Angrebet i Polen udnyttede huller, der for længst burde have været lukkede. På modsatte side står de otte punkter, der taler direkte ind i det, der skete.

I Figur 4 henvises desuden til de relevante anbefalinger fra SektorCERTs 25 Anbefalinger og på side 12 beskrives de konkret i forhold til angrebet i Polen.



SÅDAN KOM ANGRIBERNE IND

A Konti og adgange

VPN-adgange uden multifaktor og enheder på fabrikskodeord gjorde det let at komme ind. Stærke kodeord og tvungen multifaktor skal bruges sammen.

7 9 19

B Eksponering mod internettet

En FortiGate-VPN vendte mod internettet på hvert ramt anlæg. Kun nødvendige services må være eksponeret – og man skal vide, hvilke.

2 15 25

C Opdatering og patching

Tre af fire firmwareversioner var for gamle til signaturkontrol. Patching kræver placeret ansvar og stadig kortere deadlines.

10 11

D Det private APN

Angriberen kom fra ét selskabs vindanlæg ind i et andet selskabs kraftvarmeværk via det fælles mobilnet. Slå klientisolation til, og behandl nettet som eksternt.

16 2 22

SÅDAN BLEV SKADEN BEGRÆNSET

E Segmentering

På det mindre kraftvarmeværk gik vejen fra en mobilforbindelse direkte til styringsenhederne. IT og OT skal holdes adskilt.

16 17

F Adfærdsbaseret detektion og logopsamling

Wiperen blev ikke fanget af antivirus, men af en EDR-løsning, der reagerede på adfærd. Detektion skal se adfærd – og på tværs af selskaberne.

3 13

G Backup af styringslogik og konfiguration

Gemte sikkerhedskopier af PLC'ernes logik gjorde genopretningen kort. Sikkerhedskopier skal også findes for OT.

4 18

H Beredskab

Værket troede først, at en underleverandør havde fejlet, og indrapporterede kun til orientering. Uforklarede driftsfejl bør indrapporteres, og beredskabsplanen bør antage, at modstanderen stadig er til stede.

12 24

1 Firewall	2 **Eksponering af services** B D	3 **Endpoint beskyttelse** F	4 **Backup** G	5 Passwordlængde
6 Ingen genbrug af password	7 **Ingen fælles logins og standard passwords** A	8 Fjern inaktive brugere	9 **Multifaktor validering** A	10 **Opdatering** C
11 **Identificere end-of-life systemer** C	12 **Beredskabsplan** H	13 **Logopsamling** F	14 Awareness	15 **Kortlægge netværksindgange** B
16 **Segmentering** D E	17 **Identificere enheder** E	18 **Dokumentation** G	19 **Begræns rettigheder** A	20 Politik for adgang
21 Politik for ændringer	22 **Leverandørstyring** D	23 Alternative kommunikationsformer	24 **Nødprocedurer** H	25 **Sårbarhedsscanninger** B

Figur 4 - SektorCERTs 25 anbefalinger og de af dem, som er relevante i forbindelse med angrebet i Polen. Tallene refererer til anbefalingerne og bogstaverne viser tilknytningen til de 8 punkter relateret til angrebet i Polen.

SEKTOR CERT



Sådan kom angriberne ind

- **Konti og adgange.** VPN-adgangene stod åbne uden multifaktor, og flere enheder kørte videre på de kodeord, de kom med fra fabrikken. Stærke kodeord og tvungen multifaktor skal bruges sammen, ikke hver for sig. Mange angreb er identitetsbaserede, og det er her, en angriber først forsøger sig.

- **Eksponering mod internettet**. På hvert eneste ramt anlæg vendte en FortiGate-VPN mod internettet. Kun nødvendige services må være eksponeret, og man skal vide, hvilke der er. Det var lærdommen fra Zyxel-sårbarheden i 2023, og fejlen gentog sig i Polen.

- **Opdatering og patching.** Tre af de fire firmwareversioner på fjernterminalerne var så gamle, at de ikke understøttede leverandørens signaturkontrol. Patching er en organisatorisk proces. Der skal placeres ansvar, og der skal sættes stadig kortere deadlines. Det må ikke være en god hensigt, der sættes på standby, når hverdagen presser på.

- **Det private APN.** Angriberen kom fra ét selskabs vindanlæg ind i et andet selskabs kraftvarmeværk, fordi enhederne i det fælles mobilnet kunne nå hinanden.
  Som vist på Figur 5: Slå klientisolation til. Behandl nettet som eksternt på linje med internettet, hvis I ikke selv kontrollerer det. Eksponér ikke webadministration, SSH eller Telnet mod det, og skift standardadgangskoderne[14].



Figur 5 - Fire spørgsmål til jeres eget net

Sådan blev skaden begrænset

- **Segmentering.** På det mindre kraftvarmeværk gik vejen fra en mobilforbindelse direkte til styringsenhederne. IT og OT skal holdes adskilt, så et indbrud på kontoret ikke giver adgang til de industrielle styresystemer.

- **Adfærdsbaseret detektion og logopsamling.** Wiperen på det store kraftvarmeværk blev ikke fanget af antivirus, men af en EDR-løsning, der reagerede på, hvad koden gjorde. SektorCERTs sensornet fangede tilsvarende angrebet i 2023 på tværs af sektoren. Detektion skal se adfærd, ikke kun kendte filer, og den skal se på tværs af det enkelte selskab.

- **Backup af styringslogik og konfiguration.** På det mindre kraftvarmeværk var det de gemte sikkerhedskopier af PLC'ernes logik, der gjorde genopretningen kort. Sikkerhedskopier skal findes for OT-siden, ikke kun for IT, og de skal kunne lægges tilbage under pres.

- **Beredskab.** Værket troede først, at en underleverandør havde begået en fejl, og indrapporterede derfor kun til orientering. Genopretningen begyndte klokken 07.30, mens angriberen var i netværket frem til cirka 10.10. Uforklarede driftsfejl bør indrapporteres, ikke kun bekræftede hændelser, og beredskabsplanen bør antage, at modstanderen stadig kan være til stede.

Det handler med andre ord om at få det basale og lovpligtige på plads.



Denne side er med vilje tom.

OVERBLIK OVER ANGREBET

I dette afsnit gennemgås angrebet i Polen i yderligere detaljer.

Dette er primært relevant for dem, der driver den kritiske infrastruktur og som arbejder med cybersikkerheden i infrastrukturen.



Angrebet

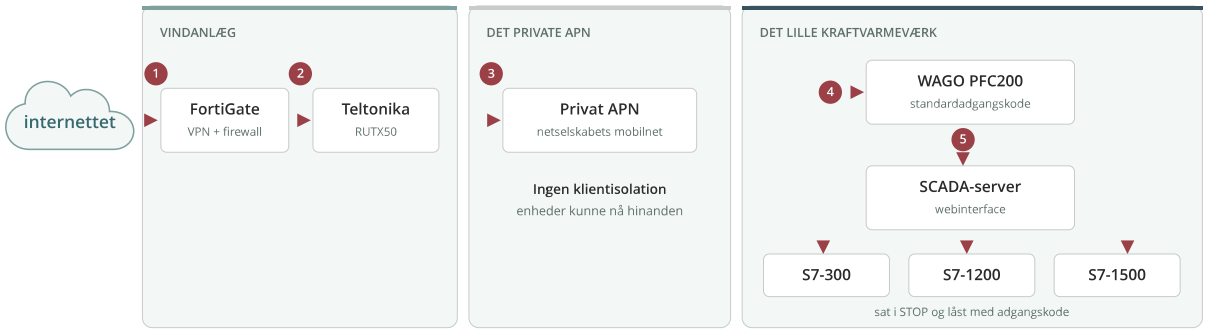
I december 2025 blev Polen ramt af et destruktivt cyberangreb mod energisektoren. Forud for dette havde aktøren været inde på det store kraftvarmeværk i flere måneder for at forberede angrebet. En aktør, som denne rapports hovedkilder sandsynliggør, kan være den russiske stat.
Den 29. december valgte aktøren at udløse det, der viste sig at være et koordineret angreb mod mindst 30 vind- og solanlæg, to kraftvarmeværker og en produktionsvirksomhed.
Angrebsvejen de benyttede, er illustreret i Figur 6.

Ved vind- og solanlæggene blev udstyr sat ud af drift. Produktionen fortsatte, men operatørerne mistede overblik og fjernstyring. På det store kraftvarmeværk, der leverer varme til knap en halv million forbrugere, blev DynoWiper (et stykke malware, der overskriver filer, så de ikke kan genskabes) eksekveret på over 100 maskiner. Men værkets sikkerhedsløsning (EDR) stoppede overskrivningen undervejs. På et mindre kraftvarmeværk med varme til omkring 50.000 forbrugere trængte angriberen ind gennem selskabets private mobilnet, standsede tre styringsenheder og afbrød kortvarigt kraftvarmeprocessen. Hurtig genopretning betød dog, at kunderne hverken mistede varme eller strøm.
Angrebet gennemgås i detaljer i Appendiks, men kan kort opsummeres således:

- Angriberne kom ind gennem klassiske sikkerhedshuller. Fællesnævneren var interneteksponerede FortiGate-VPN'er uden multifaktorgodkendelse. Dertil kom brug af standardkonti, fabriksindstillede adgangskoder og firmware, der ikke var opdateret. Men resten af angrebet var ikke trivielt: modificeret firmware, stjålne loginoplysninger, en lateral bevægelse fra et vindanlæg til et kraftvarmeværk gennem det private APN og systematisk sabotage af genopretningen.

- På det mindre kraftvarmeværk satte angriberen tre styringsenheder i stop, og kraftvarmeprocessen blev afbrudt. Det er det eneste af de fire ofre, hvor angriberen nåede den fysiske proces. Kunderne blev skånet, fordi operatørerne nulstillede enhederne og lagde sikkerhedskopierne af styringslogikken tilbage, mens angriberen stadig var i netværket[15].

- Fra et kompromitteret vindanlæg bevægede angriberen sig ind i netselskabets private mobilnet og videre ind i et kraftvarmeværks industrielle styresystemer. Det var muligt pga. en fejlkonfiguration: manglende klientisolation mellem enhederne i APN'et. Ifølge CERT Polska er det det første kendte tilfælde, hvor den vej er brugt i et reelt angreb.



1. Internetvendt VPN uden multifaktorgodkendelse.
2. Mobilrouter nået via Ethernet bag firewallen. Login på webinterface, derefter SSH.
3. SSH-tunnel ind i det private APN, som derefter scannes.
4. WAGO-controller fundet i APN'et med standardadgangskode. SSH aktiveres på WAN-grænsefladen.
5. SSH-tunnel videre ind i værkets OT-netværk, derfra til SCADA og PLC'er.

Figur 6 - Angrebsvejen: fra vindanlæg til kraftvarmeværk via netselskabets private APN
Fem spring. Nettet i midten drives af netselskabet og tilhører hverken vindanlægget eller kraftvarmeværket.



De fire mål

Angrebet ramte fire mål, som let blandes sammen. I resten af rapporten bruges derfor fire faste betegnelser. En oversigt over mål, angrebsvektor, ondsindede handlinger samt udfald kan ses i Figur 7.

Anlæggene. Mindst 30 vind- og solanlæg. Angrebet ramte nettilslutningspunkterne, ikke turbinerne eller panelerne. Ét af disse anlæg blev senere brugt som afsæt for angrebet på det lille kraftvarmeværk og omtales derfor særskilt som Vindanlægget. CERT Polska skriver *"mindst 30"* anlæg i den første rapport og *"mere end 30 nettilslutningspunkter"* i opfølgningen; her bruges konsekvent "mindst 30".

Det store værk. Ét stort kraftvarmeværk, der leverer varme til knap en halv million kunder.

Det lille værk. Ét mindre kraftvarmeværk, der leverer varme til ca. 50.000 indbyggere. Da CERT Polska udgav sin første rapport, var angrebet endnu ikke bekræftet. Det tog måneder at rekonstruere og kom derfor først med i opfølgningsrapporten fra august.

Virksomheden. Én produktionsvirksomhed uden tilknytning til energisektoren. CERT Polska mener, at målet var opportunistisk valgt.

CERT Polska vurderer i den første rapport, at samtlige angreb blev udført af samme aktør. Det lille værk kom først til i opfølgningen, hvor CERT Polska rekonstruerer bevægelsen, angriberne foretog fra ét af de kompromitterede vindanlæg og ind i værket. Det er den kæde, der binder det fjerde offer til de øvrige - ikke en selvstændig attribuering.

	Anlæggene	Det store værk	Det lille værk	Virksomheden
BESKRIVELSE	Nettilslutnings-punkter (GCP) på mindst 30 anlæg	Leverer varme til 500.000 forbrugere	Leverer varme til 50.000 forbrugere	Uden tilknytning til energisektoren
VEJ IND	Internetvendt FortiGate-VPN med konti uden multifaktor-godkendelse	FortiGate SSL-VPN med statisk definerede konti uden totrinsgodkendelse	Via det private APN fra et vindanlæg. WAGO-controller med standard-adgangskode	Fortinet-enhed med konfiguration lækket på et kriminelt forum
HVAD ANGRIBEREN GJORDE	RTU'er, relæer og serielle servere ødelagt eller nulstillet. DynoWiper eksekveret på HMI-maskiner	Månedlang rekognoscering, Diamond Ticket, hele Active Directory hentet. DynoWiper udrullet via GPO til 100+ pc'er	Tre Siemens-PLC'er sat i STOP og låst med adgangskode. Syv Moxa-servere og tre switche nulstillet	LazyWiper udrullet i Active Directory-domænet via script på en domænecontroller
UDFALD	Tab af fjernstyring og overblik. Udstyr måtte udskiftes. Elproduktionen fortsatte uændret	Standset af EDR-løsningens canary-mekanisme. Forsøg mod serverdiske mislykkedes også	Dampturbine og vandbehandling stoppet. Kraftvarmeprocessen afbrudt. Ingen kunder mistede varme	Tilfældigt offer, vurderer CERT Polska. Ikke knyttet til de øvrige ramte organisationer

Figur 7 - Fire selvstændige offergrupper ramt samme dag



Tidslinje

*Posterne står kronologisk. Perioderne for **det store værk** er upræcist angivet i kilden og overlapper med decemberposterne for de øvrige mål. "Marts til maj 2025" gælder alene **det store værk**. Datoen for den første adgang til **virksomheden** fremgår ikke af kilderne, og angriberens aktivitet i Microsoft 365 er hverken dateret eller entydigt knyttet til ét offer og er derfor holdt uden for tidslinjen (se Figur 8 på side 18).*

Ukendt tidspunkt – Anlæggene. Angriberen får adgang til anlæggenes FortiGate-enheder, som vender mod internettet og tillader login uden multifaktor. Datoen fremgår ikke af kilderne, fordi logfilerne blev slettet, da enhederne blev nulstillet.

Marts til maj 2025 – Det store værk. Angriberen får adgang til en jump host, hvor fjernskrivebordslogins registreres fra en adresse på en FortiGate-perimeterenhed. Derfra bevæger angriberen sig videre til andre systemer, herunder domænecontrolleren.

Marts til juli 2025 – Det store værk. Angriberen foretager rekognoscering med almindelige Windows-værktøjer, Diamond Ticket via Rubeus og i anden halvdel af juli tyveri af hele Active Directory-databasen.

Sidst i 2025 – Det store værk. Angriberen etablerer gentagne forbindelser til FortiGate-enhedens SSL-VPN-portal med flere statisk definerede konti uden totrinsgodkendelse, via Tor-noder samt polske og udenlandske IP-adresser, der ofte tilhører kompromitteret infrastruktur.

December 2025 – Vindanlægget. Angriberen logger flere gange ind via SSH, en krypteret fjernadgang, på en Teltonika RUTX50-mobilrouter i vindanlæggets netværk. Standardadgangskoden var skiftet af den virksomhed, der opsatte systemet, og det kunne ikke fastslås, hvordan angriberen fik den nye, eller om en sårbarhed blev udnyttet.

8. december 2025 – Anlæggene. På Mikronika Syndis HMI-maskiner, de Windows-computere operatørerne styrer anlægget fra, logger angriberen ind med den adgangskode, maskinerne fik ved opsætningen. Der er ingen tegn på gætteforsøg. Derefter slår angriberen fjernadgang til maskinerne til.

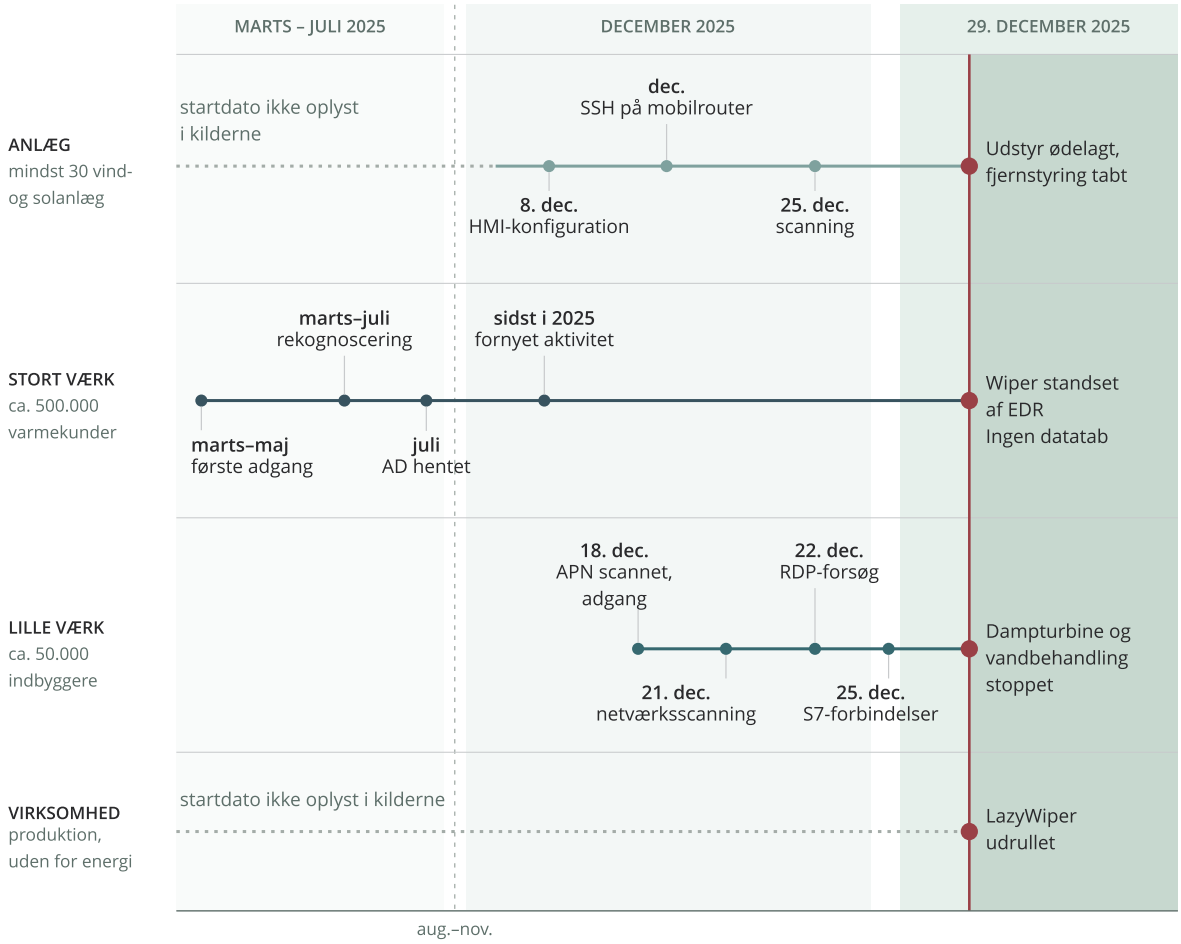
Fra 18. december 2025 – Det private APN. Fra mobilrouteren etablerer angriberen en SSH-tunnel ind i netselskabets private mobilnet, som både vindanlægget og det lille værk er koblet på, og scanner det gentagne gange. I nettet findes en WAGO PFC200-controller på det lille værk med standardadgangskode på webinterfacet. Angriberen aktiverer SSH på enheden og bevæger sig videre ind i værkets OT-netværk.

18. til 25. december 2025 – Det lille værk. Rekognoscering og forsøg på at udvide adgangen. Forsøg på at nå værkets egen firewall mislykkes. Søndag den 21. december scannes det interne netværk; i ét af netværkene begynder scanningen på adressen for SCADA-systemet, der overvåger og styrer værket.

25. december 2025 – Anlæggene og det lille værk. Netværksscanning og loginforsøg på alle anlæg med Mikronika-udstyr. På det lille værk succesfulde forbindelser til tre Siemens-PLC'er, industrielle styringsenheder, via S7-protokollen, vurderet som rekognoscering forud for de destruktive handlinger.

29. december 2025 – Alle fire. Angrebet udføres mod alle mål samme dag. På anlæggene bliver udstyr sat ud af drift, på det store værk og hos virksomheden forsøges data ødelagt, og på det lille værk sættes tre styringsenheder i stop, så kraftvarmeprocessen afbrydes. Kun det lille værk har et præcist timeforløb i kilderne: aktiviteten begynder ca. kl. 05.30 og slutter ca. kl. 10.10, og værkets folk begynder genopretningen ca. kl. 07.30, mens angriberen fortsat er i netværket. Til sidst ødelægger angriberen WAGO-enheden på det lille værk og fabriksnulstiller derefter mobilrouteren og FortiGate-enheden på vindanlægget.





Figur 8 - Tidslinje der viser, hvem der blev ramt hvornår.

EFTERSPILLET OG RAPPORTERNE

FØRSTE HALVDEL AF JANUAR 2026

Angrebet bliver offentligt kendt: Energiminister Miłosz Motyka bekræfter det[16], den 13. januar taler vicepremierminister Krzysztof Gawkowski om "*tæt på et blackout*", og premierminister Donald Tusk følger op i dagene efter.

23. januar 2026

ESET navngiver DynoWiper og attribuerer wiperen til Sandworm med moderat sikkerhed.

28. januar 2026

Dragos udgiver sin rapport med fokus på DER-vinklen.

30. januar 2026

CERT Polska udgiver den tekniske hovedrapport.

30. juni 2026

Styrelsen for Samfundssikkerhed (SAMSIK) skærper vurderingen af truslen fra destruktive russiske cyberangreb mod Danmark med henvisning til angrebet i Polen. Det samlede trusselsniveau fastholdes på "middel".

13. juli 2026

Storbritannien og EU attribuerer angrebet officielt til FSB's Center 16 og indfører sanktioner.

7. august 2026

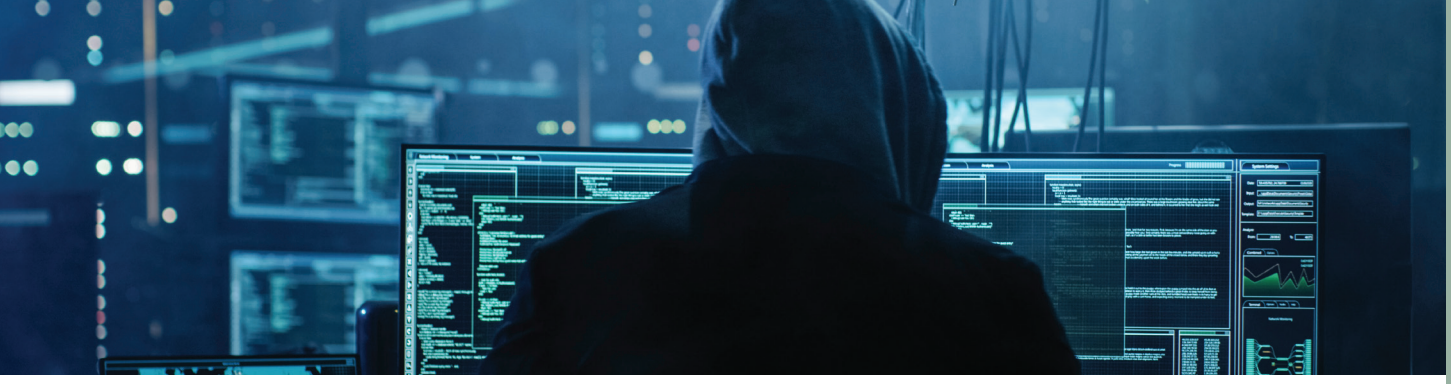
CERT Polska udgiver opfølgningsrapporten om det lille kraftvarmeværk og vejen gennem det private APN.



Denne side er med vilje tom.

APPENDIKS: DETALJERET GENNEMGANG AF ANGREBET

I dette appendiks gennemgås angrebet i detaljer.
Gennemgangen er opdelt i ti dele og er tiltænkt de personer, som ønsker en dyb forståelse af angrebets faser og de teknikker, der blev benyttet.



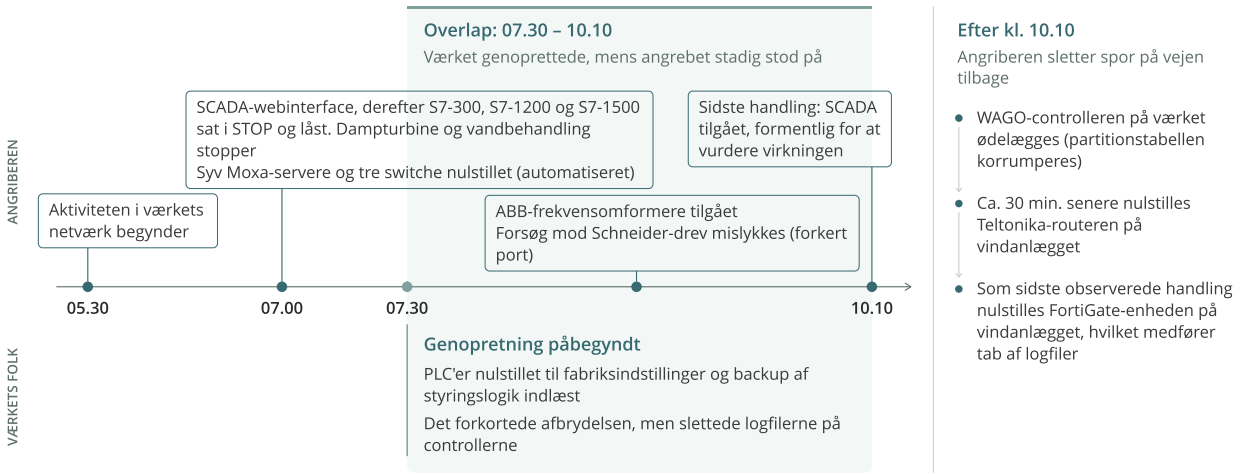
Del 1: Vejen ind

På det store værk ses de første spor af angriberen mellem marts og maj 2025. Både her og hos virksomheden gik vejen ind gennem en FortiGate-enhed, mens angriberen trængte ind på det lille værk (se Figur 9) ved at springe fra et kompromitteret vindanlæg gennem det private APN (Del 6). For anlæggene beskriver CERT Polska indgangen således:

"På hvert eneste af de ramte anlæg var der en FortiGate-enhed, der fungerede som både VPN-koncentrator og firewall. I alle tilfælde var VPN-grænsefladen eksponeret mod internettet og tillod login fra konti, der var defineret i konfigurationen, uden multifaktorgodkendelse. På grund af angriberens destruktive handlinger var det ikke muligt at gendanne fuldstændige logfiler fra nogen af de kompromitterede enheder." (CERT Polska, s. 7; egen oversættelse.)

Mindst lige så interessant er, hvad der ikke skete. CERT Polska knytter ikke indgangen til en navngiven, kendt FortiGate-sårbarhed. Nogle af enhederne havde i perioder været sårbare over for kendte fejl, men om de blev udnyttet, kan ikke afgøres, for angriberen fabriksnulstillede samtlige FortiGate-enheder på angrebsdagen. Det tjente to formål på én gang: at forsinke genopretningen og at slette sporene. Der var efter alt at dømme slet ikke brug for en ny sårbarhed eller sofistikeret hacking for at komme ind. Døren stod åben, og nøglen var oven i købet genbrugt. Tilgængelig information peger ifølge CERT Polska på, at genbrug af de samme konti og adgangskoder på tværs af anlæg er udbredt praksis i branchen, så én kompromitteret konto kan have åbnet flere døre.

CERT Polska konkluderer, at den samme aktør stod bag de tre angreb, der er beskrevet i den første rapport: mod anlæggene, det store værk og virksomheden. Ét forbehold står tilbage, og det gælder alene det store værk. Her sås to klynger af aktivitet, én fra marts til juli 2025 og én sidst på året. CERT Polska kan ikke med sikkerhed sige, om de stammer fra samme aktør. Rekognosceringen af industrisystemerne og den efterfølgende stilhed, efter at brugerdatabasen var stjålet, peger dog ifølge CERT Polska på én aktør, der har opereret over længere tid med "en konsistent operationel profil".



Figur 9 - 29. december 2025 på det lille værk.
Genopretningen begyndte, mens angriberen stadig var i netværket.



Del 2: Det store værk: fra marts til december

De næste måneder gik med rekognoscering. CERT Polska beskriver, hvordan angriberen bevægede sig fra maskine til maskine med almindelige Windows-værktøjer: fjernskrivebord (RDP), fildeling (SMB) og administrationsværktøjet PsExec. Angriberen tog skærmbilleder og indsamlede oplysninger om, hvad der befandt sig på de enkelte computere. Påfaldende mange af de maskiner, angriberen opsøgte, bar ordet SCADA i navnet. Det tyder på, at angriberen målrettet ledte efter industrielle styresystemer. Aktiviteten foregik overvejende i almindelig arbejdstid, hvor den lignede legitim administration.

På et tidspunkt lykkedes det angriberen at eskalere sine rettigheder. CERT Polska kan ikke rekonstruere præcis hvordan, men knap en måned efter adgangen til domænecontrolleren registrerede EDR-løsningen et sandsynligt forsøg på at stjæle loginoplysninger fra hukommelsen. Angriberen fortsatte alligevel og fik med værktøjet Rubeus oprettet en såkaldt Diamond Ticket: en forfalsket adgangsbillet, der giver meget omfattende rettigheder på tværs af et Windows-netværk. I anden halvdel af juli kopierede angriberen hele Active Directory, organisationens centrale register over brugere, grupper og adgangsrettigheder. Så blev der stille i flere måneder.

Sidst på året begyndte aktiviteten igen. Angriberen loggede gentagne gange ind på værkets FortiGate SSL-VPN-portal med flere konti, der var defineret direkte i enhedens konfiguration uden totrinsgodkendelse, via Tor og via adresser, som ifølge CERT Polskas senere analyse ofte kunne knyttes til kompromitteret infrastruktur. Bookmarks i portalen med gemte loginoplysninger gav adgang til jump hosts uden nyt login. Derfra fulgte en ny runde tyveri: registreringsdatabaser og Active Directory-databasen via en Volume Shadow Copy, forsøg på at sende data ud og konfigurationsfiler fra en række FortiGate-enheder, hentet via Microsoft Edge i privat tilstand, formentlig for ikke at vække opsigt. Angriberen tilføjede også en firewallregel med logning slået fra og gav den et navn, der efterlignede en institution, som allerede stod i konfigurationen.

Med brugerregisteret og FortiGate-konfigurationerne i hænderne havde angriberen i praksis nøglerne til store dele af organisationen. Det, der her ramte ét værk, gælder i endnu højere grad for anlæggene. Dragos ser netop her den centrale udfordring ved distribueret elproduktion:

Når samme firewallmodel med samme fejlkonfiguration står på mange anlæg, kan ét indbrud nemt skaleres. Den standardisering, der gør driften effektiv, betyder også, at én nøgle passer til mange døre[17].

Om morgenen den 29. december gik angriberen ind gennem VPN-portalen, videre til en jump host og derfra til en domænecontroller, hvor wiperen blev lagt. Herefter eksekverede angriberen DynoWiper på mere end 100 maskiner. Filen blev placeret på et delt netværksdrev og sat til at køre ved hjælp af et ekstra Group Policy Object (GPO) i Active Directory. Præcis på samme måde, som organisationer typisk udruller software og indstillinger til mange computere på én gang.

DynoWiper blev ikke fanget af antivirus. Til gengæld blev den stoppet af EDR-løsningens canary-mekanisme: lokkefiler uden driftsfunktion, som udløser en alarm, hvis nogen forsøger at ændre dem. Systemet reagerede, da wiperen begyndte at overskrive filer, og dataoverskrivningen blev stoppet på de mere end 100 maskiner, hvor filen allerede var eksekveret. Samme dag forsøgte angriberen igen at køre en let modificeret version, men også dette mislykkedes. Endelig startede angriberen et minimalt Linux-system, Tiny Core Linux, på en af værkets servere, overskrev dele af diskene og forsøgte at manipulere serverens diskopsætning (RAID).



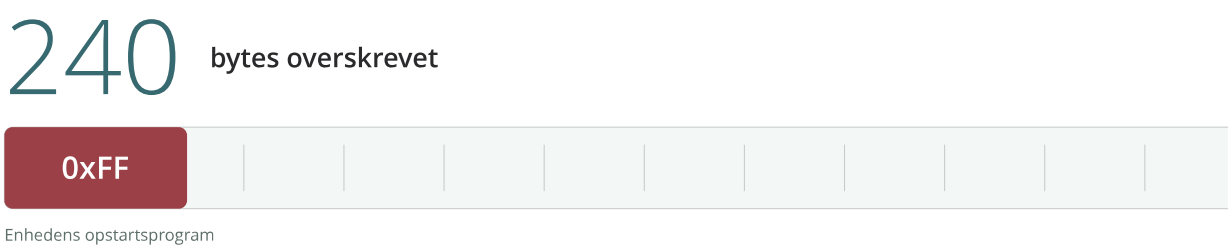
Del 3: Anlæggene: udstyr sat ud af drift, men ingen strømafbrydelser

Hvornår angriberen først kom ind på anlæggene, fremgår ikke. Logfilerne blev slettet, da FortiGate-enhederne blev nulstillet. Sporene før selve angrebsdagen er derfor få, men tydelige.

Den 8. december loggede angriberen ind på nogle af anlæggenes HMI-maskiner, de Windows-computere fra Mikronika, som operatørerne bruger til at følge og styre anlægget. De havde stadig den adgangskode, de fik ved opsætningen. Administrative shares blev slået til, og en firewallregel med navnet "Microsoft Update" åbnede port 445, så de kunne fjernstyres. Juledag scannede angriberen netværket og forsøgte at logge ind på samtlige anlæg med Mikronika-udstyr. Det ved vi, fordi Mikronika var i stand til at genskabe en del af logfilerne. Fire dage senere gik det løs.

Den 29. december gik angriberen fra kortlægning til destruktion. På mindst 30 vind- og solanlæg loggede angriberen ind på de industrielle fjernterminaler, RTU'erne: de små computere ude på anlæggene, som overvåger og styrer udstyret og sender data tilbage til netselskabet. Sabotagen ser ud til at have været i hvert fald delvist automatiseret: Enhederne blev beskadiget i stigende rækkefølge efter IP-adresse, og hvor angrebet fejlede ved en adresse, gik det ikke videre i det segment.

Det gennemgående greb var også her at bruge standardindstillinger. På Hitachi RTU560-enhederne, som stod på de fleste anlæg, brugte angriberen den indbyggede konto "Default" til at overskrive enhedens firmware, den grundlæggende software, der får den til at starte og fungere. 240 bytes blev sat til værdien 0xFF netop dér, hvor programkoden starter. Sagt enklere: Angriberen overskrev begyndelsen af enhedens opstartsprogram med indhold, der ikke er et program. Resultatet var, at processoren forsøgte at udføre en ugyldig instruktion og derefter sad fast i en uendelig genstartsløkke (se Figur 10). Ifølge Dragos betød det, at udstyret blev sat ud af drift uden mulighed for reparation på stedet.



Figur 10 - 240 bytes - og enheden kom aldrig op igen
Angriberen brugte den indbyggede konto "Default" til at overskrive begyndelsen af RTU'ens opstartsprogram med værdien 0xFF

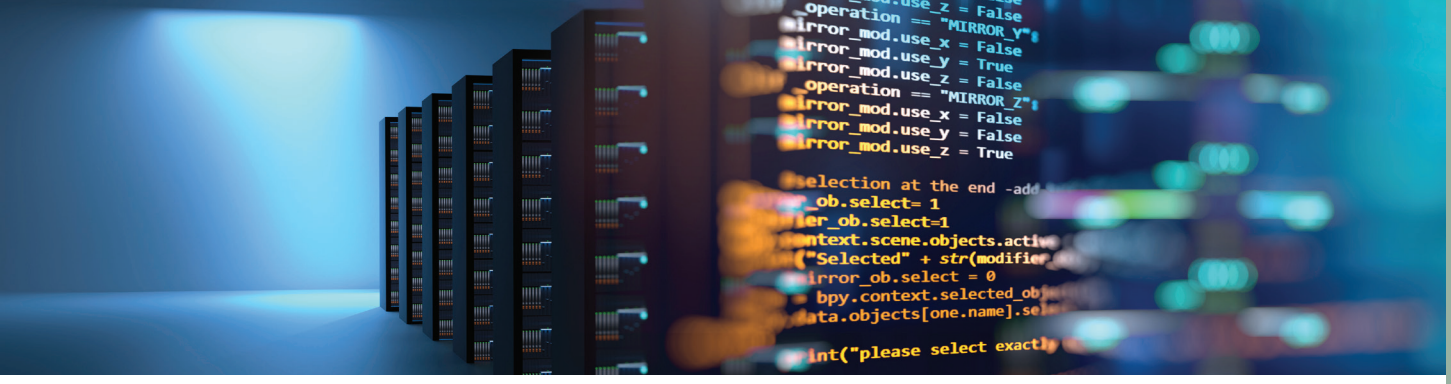


En detalje fortjener her særlig plads. Den firmware, angriberen installerede på enhederne, identificerede sig som version 13.5.3.0. Men den version kørte ikke på nogen af de ramte anlæg. Angriberen havde altså efter alt at dømme skaffet firmwaren et andet sted fra og modificeret den på forhånd. Hitachi har siden version 13.2.1 kontrolleret firmwarens signatur, før den installeres. Men den funktion skal slås til, og ingen af de enheder, der kunne bruge den, havde gjort det. Tre af de fire versioner i drift var desuden så gamle, at de slet ikke understøttede den. Og selv hvis kontrollen havde været slået til, fandtes der en sårbarhed, CVE-2024-2617, der kunne omgå den; den blev først rettet i version 13.7.7. Angriberen havde med andre ord en mulig trumf i baghånden, der aldrig kom i brug. Ifølge CERT Polska har Hitachi Energys sikkerhedsteam bekræftet forløbet[18].

Mikronikas Linux-baserede RTU'er blev slettet via SSH med root-adgang og standardadgangskode. I to tilfælde blev Hitachi Relion 650-beskyttelsesrelæer sat ud af drift via FTP med en indbygget konto, som ville have været deaktiveret, hvis relæerne havde været installeret efter leverandørens anvisninger.

På HMI-maskinerne blev DynoWiper startet direkte som filen Source.exe. De HMI'er, der havde fået en ikke-standard adgangskode, blev ikke beskadiget. Moxa-serverne, der forbinder serielt udstyr til netværket, blev fabriksnulstillet, fik ny adgangskode og en adresse, der ikke kan nås, som 127.0.0.1. Ændringen af adgangskode og adresse skete ifølge CERT Polska for at forsinke genopretningen. Samme dag blev FortiGate-enhederne selv nulstillet, hvilket både hindrede genopretning og slettede sporene.

Selve elproduktionen blev dog ikke ramt. Anlæggene fortsatte med at producere strøm, og ifølge CERT Polska påvirkede angrebet efter den polske transmissionsoperatør PSEs vurdering ikke stabiliteten i det polske elsystem. Men forbindelsen mellem anlæggene og distributionsselskaberne blev afbrudt, så operatørerne hverken kunne fjernstyre anlæggene eller vide, hvad der foregik på dem. Angrebet ramte ikke selve vindturbinerne eller solpanelerne, men nettilslutningspunktet, hvor anlægget kobles på distributionsnettet, og hvor RTU'er, HMI'er, relæer og kommunikationsudstyr står. Sådanne nettilslutningspunkter er typisk fjernstyrede og ubemandede.



Del 4: Det lille værk, hvor dampturbinen standsede

Samme morgen udspillede der sig et bemærkelsesværdigt forløb på et kraftvarmeværk, som ikke optrådte i CERT Polskas første rapport. Værket leverer varme til omkring 50.000 indbyggere. Klokken cirka 07.00 standsede dampturbinen og det anlæg, der producerer procesvand, og kraftvarmeprocessen blev afbrudt. Der blev udført vedligeholdelsesarbejde den dag, og man antog derfor, at en underleverandør havde begået en fejl. Hændelsen blev kun indrapporteret til orientering. Men da CERT Polska allerede kendte de andre hændelser, behandlede de sagen som et muligt cyberangreb og fik det bekræftet. Efterforskningen tog dog mere end tre måneder og foregik baglæns, fra den observerede effekt. Læren om at indrapportere uforklarede driftsfejl og ikke kun bekræftede hændelser er derfor direkte anvendelig for SektorCERTs medlemmer.

Den enhed, angriberen havde arbejdet fra, viste sig at være en WAGO PFC200-styringsenhed med indbygget mobilmodem. Den var ødelagt, og selv med hukommelseskredsen loddet af kunne der ikke hentes data ud. Angreb, der udgår direkte fra en PLC, hører ikke til de scenarier, man normalt ser i OT-miljøer, noterer CERT Polska. Enheden var ikke eksponeret mod internettet. Den talte med netselskabet gennem et SIM-kort i netselskabets private APN, hvilket var den vej, angriberen var trængt ind (Del 6).

Fra den 18. december rekognoscerede angriberen på indersiden af værkets netværk. Forsøg på at logge ind på værkets egen firewall fra det interne net mislykkedes, både første gang og tre dage senere. Et af brugernavnene hørte til den virksomhed, der opsætter fjernstyring på vedvarende energianlæg. Søndag den 21. december blev det interne netværk scannet for industriprotokollerne S7, Modbus og CODESYS samt fjernadgange og webtjenester. I ét af netværkene begyndte scanningen på SCADA-systemets adresse. Angriberen havde tilsyneladende allerede udpeget sine mål. Juledag lykkedes det at få forbindelse til tre Siemens-PLC'er via S7-protokollen.

Den 29. december begyndte aktiviteten cirka 05.30. Angriberen kom via WAGO-enheden ind på SCADA-serverens webinterface og derefter til en Siemens S7-300 og gentog forløbet mod en S7-1200 og en S7-1500.

Ifølge værkets personale blev PLC'erne sat i STOP-tilstand og låst med en adgangskode, så hverken driftstilstand eller styringslogik kunne ændres, hvilket fik dampturbinen og vandbehandlingen til at standse. Parallelt fik syv Moxa-servere og tre Moxa-switche samme omgang som på anlæggene: fabriksnulstilling, ny adgangskode, en adresse, der ikke kan nås. Ud fra tidsstemplerne vurderer CERT Polska med høj sikkerhed, at denne del var automatiseret. Der sås også forbindelser til to ABB-frekvensomformere, uden at det kunne afgøres, hvad der skete, samt mislykkede forsøg mod Schneider Electric-frekvensomformere.

Klokken cirka 07.30 gik værkets folk i gang med at genoprette driften. Angriberen var stadig i netværket indtil omkring 10.10. Den sidste observerede handling var et opslag i SCADA-systemets webinterface, formentlig for at vurdere skaderne. Operatørerne nulstillede PLC'erne til fabriksindstillinger og indlæste deres backups af styringslogikken. Det forkortede afbrydelsen, men slettede også logfilerne. Siemens' sikkerhedsteam har siden bekræftet, at de ikke kunne genskabes[15].

Resultatet var en kortvarig afbrydelse af installationen, og hverken forbrugernes varme eller strøm blev påvirket.

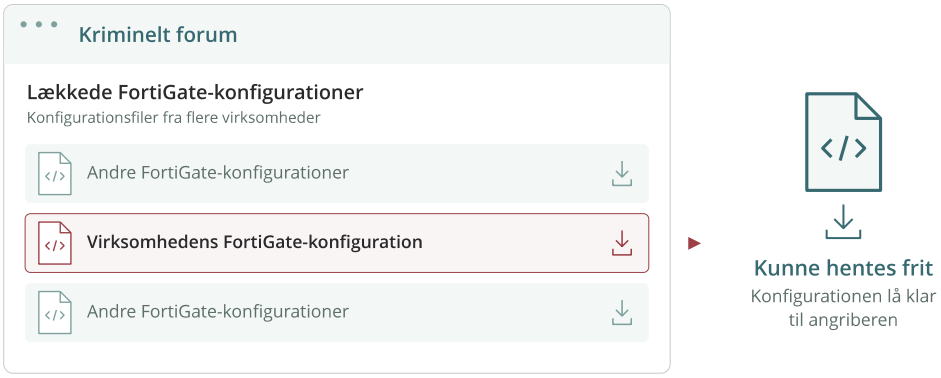
På vej ud ødelagde angriberen WAGO-enhedens partitionstabel, så den ikke kunne starte. Ingen logfiler kunne reddes. Tredive minutter efter den sidste aktivitet på værket blev mobilrouteren på vindanlægget fabriksnulstillet, fik ny adgangskode og adressen 127.0.0.1. FortiGate-enheden på vindanlægget blev nulstillet med tab af logfiler til følge. Det var den sidste observerede handling i en række af ødelæggelser og forsøg på at slette alle spor.

TLP:CLEAR



Del 5: Virksomheden: et opportunistisk mål

Samme dag (den 29. december) ramte angriberen også en produktionsvirksomhed uden tilknytning til energisektoren, som ifølge CERT Polska var et opportunistisk valgt mål (se Figur 11). Dens FortiGate-konfiguration var tidligere blevet stjålet og lækket på et kriminelt forum, hvilket gjorde den til et oplagt mål. Angriberen havde sikret sig en bagdør: to scripts i selve firewallen, som hver uge hentede en privilegeret brugers adgangskode og lempede på sikkerhedsindstillingerne, og et tredje, der sendte resultatet til en Slack-kanal under angriberens kontrol. Selv hvis virksomheden skiftede adgangskoder, ville angriberen få de nye tilsendt. Her anvendte angriberen en simplere wiper ved navn LazyWiper, skrevet i PowerShell og udrullet via Group Policy som på det store værk. I Del 9 vender vi tilbage til den, fordi den peger på en ny udvikling: brugen af kunstig intelligens til at skræddersy malware.



Figur 11 - et mål, der lå fremme.
Virksomhedens FortiGate-konfiguration var tidligere stjålet og lækket på et kriminelt forum.
CERT Polska vurderer, at målet blev valgt opportunistisk - det lå bare fremme sammen med alle de andre



Del 6: Vejen fra vindanlægget til det lille værk

CERT Polska opstiller 11 trin i en kæde, her forkortet til fem spring.

- **Fra internettet til vindanlægget.** Internet-eksponeret FortiGate-VPN, konti skrevet direkte ind i konfigurationen og uden multifaktor.
- **Internt på anlægget.** En Teltonika RUTX50-mobilrouter, som angriberen nåede gennem et netværkssegment bag den kompromitterede firewall. Først login via webinterfacet, derefter SSH. Routerens standardadgangskode var blevet skiftet ved opsætningen, og CERT Polska kunne ikke fastslå, hvordan angriberen fik den nye, eller om en sårbarhed blev udnyttet.
- **Fra vindanlægget til netselskabets private APN.** Gennem routeren oprettede angriberen en SSH-tunnel ind i netselskabets private mobilnet. Netselskabets krav om, at kommunikationen med fjernterminalen skulle gå over et serielt link med DNP3.0, var opfyldt. Men ingen havde stillet krav til, hvordan routerens admin-interface skulle sikres.
- **Fra det private APN til det lille værk.** WAGO PFC200-controller med standardadgangskode på webinterfacet mod APN'et. SSH blev aktiveret og brugt som tunnel ind i værkets OT-netværk.
- **Internt på det lille værk.** Fra OT-netværket til SCADA-serverens webinterface og til de tre Siemens-PLC'er.

Det afgørende ved denne nye rute er, at angriberen kom fra ét anlæg ind i et andet gennem et net, som ingen af dem selv kontrollerede. CERT Polska betegner det som det første kendte tilfælde, hvor et privat APN er brugt til at nå et OT-netværk i et reelt angreb. Dertil kommer, at den fejlkonfiguration, der muliggjorde angrebet, nemlig manglende klientisolation mellem enheder i APN'et, var udbredt i Polen på undersøgelsestidspunktet og vurderes også at være det i andre lande[19]. Hvad det betyder for Danmark, er behandlet i kapitlet "Hvad betyder angrebet for Danmark?".
CERT Polskas første rapport fremhævede, at polske netselskaber kræver seriel kommunikation over DNP3.0 eller IEC 101 mellem SCADA og nettilslutningspunktet, netop for at mindske risikoen for, at et kompromitteret anlæg kan bruges som springbræt ind i netselskabets net.

> Et privat APN er, i korte træk, et lukket mobilnet, som teleselskabet stiller til rådighed for én kunde, her netselskabet. SIM-kortene i anlæggenes mobilroutere og i styringsenheder ude hos kunderne taler ind i det net, og netselskabets SCADA-system svarer. Nettet er "privat" i den forstand, at det er adskilt fra det offentlige mobilnet og fra internettet. Men uden klientisolation kan enhederne i nettet tale med hinanden. Så er mobilnettet i praksis et lokalnet for alle, der har et SIM-kort i det.

Opfølgningen viser, at kravet virkede efter hensigten, men blev omgået: Mobilrouteren havde en anden netværksgrænseflade, der sad i det samme netværkssegment (VLAN) som den kompromitterede firewall. Det var ikke det serielle link, men selve APN'et, der blev den uovervågede sidevej. Det serielle krav er nødvendigt, men ikke tilstrækkeligt, når routerens administrationsadgang og APN'et omkring den bliver taget for givet som sikre og ingen holder øje med dem.



Del 7: Hvor tæt på en katastrofe var det?

Da angrebet i midten af januar blev offentligt kendt, lød de mest dramatiske meldinger på, at en halv million polakker kunne være endt uden varme kort før nytår, i frostgrader og snevejr. Det billede kræver tre præciseringer.

- For det første knytter CERT Polska tallet til det store kraftvarmeværk, der leverer varme til næsten en halv million kunder, og Premierminister Donald Tusk knyttede også kun tallet til varmen. Vicepremierminister Gawkowski derimod talte om blackout og strøm og kaldte det et angreb, *"som havde til formål at afbryde strømmen til borgerne"*[3]. Og da Storbritannien og EU den 13. juli officielt attribuerede angrebet, skrev det britiske udenrigsministerium, at 500.000 borgere kunne have mistet strømmen, mens EU's erklæring samme dag korrekt talte om kraftvarmeværker[2].

- For det andet var selve elsystemet slet ikke tæt på et blackout. CERT Polska skriver, at angrebet mod anlæggene, set fra den polske transmissionsoperatør PSEs perspektiv, ikke påvirkede stabiliteten i det polske elsystem. Der er dog et forbehold: I kraft af sin adgang havde angriberen mulighed for at forstyrre elproduktionen på de ramte anlæg. Selv da ville det samlede kapacitetstab på alle anlæggene ikke have påvirket stabiliteten *"i den pågældende periode"*[20]. Dragos når til samme vurdering: lokale udfald var mulige, ikke et landsdækkende sammenbrud. Vurderingen gælder for de mindst 30 anlæg og dagene omkring nytår, og den omfatter ikke det lille værk, som først blev kendt senere. Regeringens *"tæt på et blackout"* holdt altså ikke for elnettet.

- For det tredje blev en fysisk proces faktisk standset. På det lille værk satte angriberen styringsenhederne i stop, og kraftvarmeprocessen blev afbrudt. Dermed standsede produktionen af både el og varme på værket, uden at nogen kunder mistede nogen af delene.

Det var hurtig operatørrespons, ikke angriberens begrænsninger, der forhindrede, at det ramte kunderne. Elnettet var ikke tæt på et blackout, men på ét kraftvarmeværk var det faktisk "tæt på".

Ét træk går igen hos ofrene: den systematiske sabotage af genopretningen. På anlæggene blev Moxa-enhederne fabriksnulstillet, forsynet med ny adgangskode og sat til adresser, der ikke kan nås. FortiGate-enhederne blev nulstillet, så logfilerne blev slettet. På det lille værk fik syv enhedsservere og tre switche samme behandling, og døren ud, WAGO-enheden, blev ødelagt, sammen med mobilrouteren og FortiGate-enheden på vindanlægget. På det store værk gik angriberen efter servere og RAID-opsætning, ud over wiperen. Mekanismen var ikke den samme alle steder, men mønstret er tydeligt. Angriberen gik ikke kun efter ødelæggelse, men også efter nedetid.

Det, der gør angrebet i Polen alvorligt for Danmark, er derfor ikke, hvorvidt Polen var tæt på et blackout eller hvor mange kunder der var tale om. Det er snarere det faktum, at en angriber var i stand til at udnytte basale sikkerhedsfejl til at ramme mange decentrale energianlæg samtidig. Dertil kommer, at den samme angriber fandt vej fra ét anlæg og ind i produktionsudstyret på et andet, gennem et net ingen af dem selv kontrollerede.



Del 8: Det var nemt at komme ind, men resten af angrebet var mere sofistikeret

Var angrebet avanceret? Vejen ind var det ikke. Som vi så i Del 1 til 6, var det de mere simple ting: manglende multifaktor, genbrugte adgangskoder og fabriksindstillinger, der aldrig var skiftet.

Men det, der fulgte, var mere sofistikeret og velforberedt. RTU-firmwaren var efter alt at dømme skaffet uden for offermiljøerne og modificeret på forhånd. På det store værk brugte angriberen Rubeus og en Diamond Ticket, en reverse SOCKS-proxy og et Linux-image bootet gennem serverens fjernstyring. I Microsoft 365 brugte angriberen stjålne loginoplysninger til at hente mails og filer fra Exchange, Teams og SharePoint og var ifølge CERT Polska *"særligt interesseret i filer og e-mails om modernisering af OT-netværk, SCADA-systemer og teknisk arbejde"* (CP s. 26; egen oversættelse). Den aktivitet er ikke dateret og ikke entydigt knyttet til ét offer, men den fortæller, hvad angriberen ledte efter, og viser et vist niveau af sofistikation og forberedelse. Endelig fandt angriberen en kreativ og tilsyneladende ny vej gennem det private APN ind i et helt andet værks OT-netværk. Det var med andre ord nemt at komme ind, men resten af angrebet var mere sofistikeret.

Aktøren var heller ikke ufejlbarlig, og kilderne dokumenterer to fejl. DynoWipers liste over mapper, der skulle springes over, indeholder et forkert skrevet "program files(x86)" uden mellemrum.

Forsøgene mod Schneider Electric-frekvensomformerne på det lille værk mislykkedes, fordi angriberen ramte port 80, mens webinterfacet lyttede på en anden, hvilket CERT Polska anser for sandsynligvis at skyldes "ufuldstændig rekognoscering". Det er de klareste steder, hvor primærkilderne faktisk understøtter en læsning af, at aktøren ikke var særligt raffineret. Dragos, der på det tidspunkt ikke kendte til det fjerde offer, læser operationen som mere opportunistisk end angrebene i Ukraine, og vurderer med moderat sikkerhed, at opportunisme var en nøglefaktor, og med lav sikkerhed, at den begrænsede effekt skyldtes ufuldstændig forberedelse snarere end manglende evne[21].

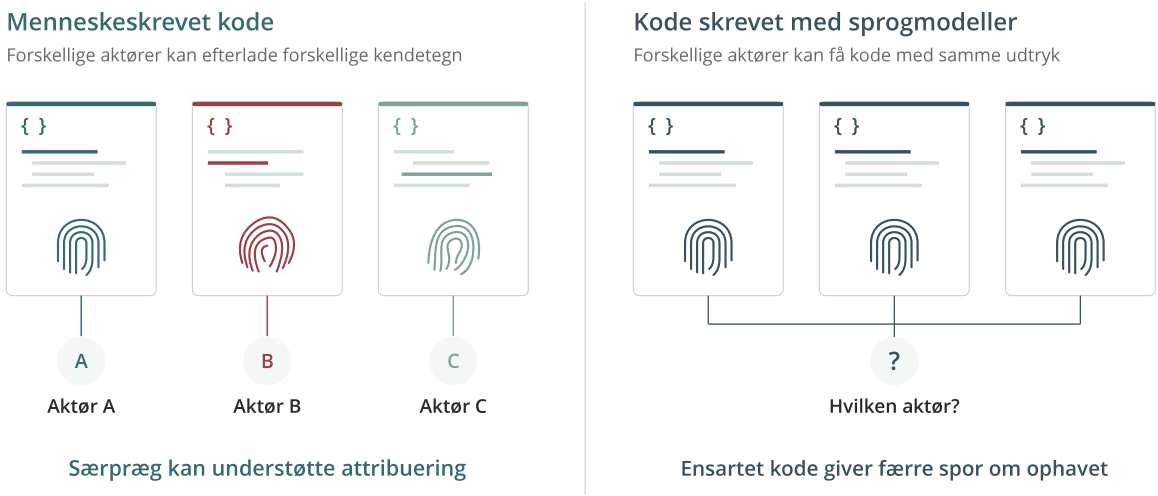
Angrebet blev heller ikke standset ét sted, men flere. På det store værk stoppede EDR-løsningen wiperen. På anlæggene blev de HMI'er, der havde fået ændret standardadgangskoden, ikke beskadiget, og RTU-sabotagen stoppede af sig selv, hvor den fejlede på en adresse. På det lille værk blev forstyrrelsen ikke forhindret, men inddæmmet af hurtig genopretning. Grundlæggende adgangskodehygiejne er dermed det bedst underbyggede punkt, vi kan lære af i hele materialet. Adfærdsbaseret detektion er det næstbedste lærepunkt: Uden EDR-løsningen ville angrebet på det store værk efter alt at dømme have haft langt større konsekvenser.



Del 9: AI sænker barrieren

Under efterforskningen fandt CERT Polska et lille, men interessant spor. LazyWiper, der blev brugt mod produktionsvirksomheden, indeholdt en funktion, som skilte sig ud i struktur og kodestil og rummede meningsløse kommentarer, et menneske sandsynligvis ikke ville have skrevet. Konklusionen var, at den sandsynligvis var genereret af en sprogmodel. Her er det værd at holde tungen lige i munden. Kun CERT Polska nævner sporet, og de understreger udtrykkeligt, at netop dette script, der ikke har særegne træk, ikke kan bruges til attribuering. Dertil kommer, at netop denne del af angrebet ramte et mål, som CERT Polska selv beskriver som opportunistisk og ikke forbundet med de øvrige ofre. Det er altså kun en indikation, ikke et bevis.

Uanset hvad sænker generativ kunstig intelligens sandsynligvis barrieren for at bruge unikke varianter af skadelig kode i stor skala. Det svækker klassisk detektion, der bygger på kendte hashværdier og signaturer, og tilskynder til brugen af adfærdsbaseret detektion. Det svækker også attribueringen: Analytikere leder i malware efter kodestil, fejl og andre særpræg, der kan føres tilbage til en udvikler, men kode skrevet af en sprogmodel bærer ikke den slags spor (se Figur 12). CERT Polska drager selv den konklusion for LazyWiper. Modtrækket sås allerede i Polen, hvor EDR-løsningens canary-funktion, en slags snubletråd af lokkefiler, stoppede DynoWiper. Ikke ved at genkende koden eller en hashværdi, men fordi lokkefilerne selv blev overskrevet. Det er den vej, cyberforsvarere i stigende grad orienterer sig mod for at kunne bekæmpe truslen fra mere eller mindre AI-assisterede angribere: systemer, der analyserer, hvad kode gør, frem for at matche kendte signaturer og filer.



Figur 12 - Kode uden håndskrift
Analytikere leder i malware efter kodestil, fejl og andre særpræg, der kan føres tilbage til en udvikler. Kode skrevet af en sprogmodel bærer ikke den slags spor.



Del 10: Attribuering: hvem stod bag?

Attribuering er noget af det mest omstridte i sagen, og de tre tekniske kilder når ikke frem til det samme. Det skyldes ikke uenighed om fakta, men at de kigger på hver sit spor.

CERT Polska analyserede den infrastruktur, angriberen brugte. Herunder kompromitterede servere og routere. Den overlapper i vidt omfang med infrastruktur, som Cisco og FBI tidligere har beskrevet, og som bruges af en aktør, der offentligt kaldes Static Tundra (Cisco), Berserk Bear (CrowdStrike), Ghost Blizzard (Microsoft) og Dragonfly (Symantec). Det er fire navne for det samme (se Figur 13).

Malwaren DynoWiper har enkelte fællestræk med wipere forbundet med Sandworm, men ligheden er efter CERT Polskas vurdering for lille til at knytte den til kendte aktører. LazyWiper er sandsynligvis genereret af en sprogmodel og kan slet ikke bruges til attribuering. CERT Polska kan derfor ikke afgøre, om aktøren bag Sandworm deltog i angrebet i noget omfang[6].

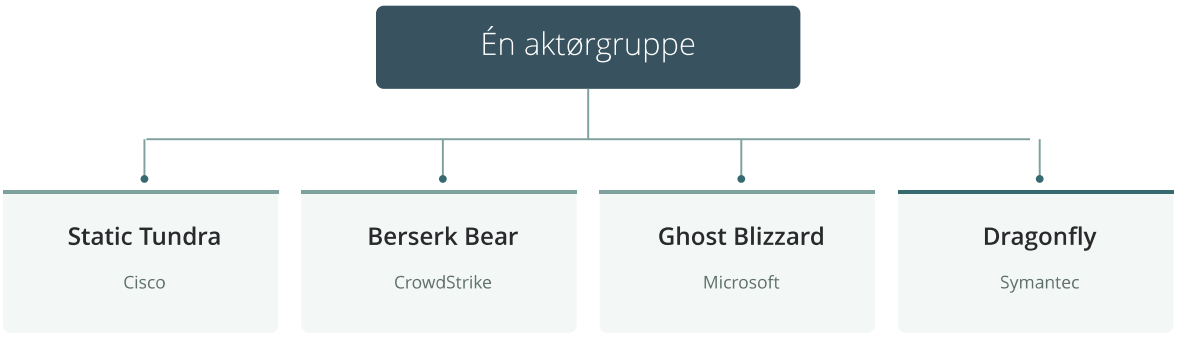
ESET og Dragos læser det anderledes, men på et smallere grundlag. ESET attribuerer med moderat sikkerhed wiperen DynoWiper til Sandworm. Dragos peger med moderat sikkerhed på aktøren ELECTRUM - en aktør relateret til Sandworm.

Den 13. juli 2026 attribuerede Storbritannien og EU officielt angrebet til den russiske stats FSB Center 16 og indførte sanktioner.
Samme dag udsendte myndigheder fra 13 lande, herunder Danmark og Polen, en fælles udmelding, der knytter Center 16 til netop Static Tundra- og Dragonfly-klyngen[2].

Den officielle attribuering følger altså CERT Polskas infrastrukturspor og ikke ESETs og Dragos' spor til Sandworm. Det er SektorCERTs vurdering, at attributionen dermed peger væk fra Sandworm og mod FSB. CERT Polska kan fortsat ikke afgøre, om Sandworm-klyngen deltog.

To ting er værd at bemærke ud over navnet. CERT Polska anfører, at det er den første offentligt beskrevne destruktive aktivitet fra denne aktør, som historisk har lavet spionage og præpositionering i energisektoren. Og aktøren er den samme, som SektorCERT angiver som Dragonfly på top 10-listen over de mest relevante trusselsaktører mod dansk kritisk infrastruktur[7]. ESET beskriver det uafhængigt som et meget sjældent tilfælde af en operatør af kritisk infrastruktur i et NATO-land, der rammes med en wiper[22].

Om motivet siger kilderne næsten intet. ESET skriver, at motiverne "forbliver uklare", men peger på, at operationen kan have haft til formål at belaste Ukraines net om vinteren, fordi Polen hjælper med at stabilisere landets elforsyning. Hverken CERT Polska eller Dragos går ind i mulige strategiske motiver[22].



Figur 13 - Fire navne, samme aktørgruppe
CERT Polska knytter angrebets infrastruktur til en aktør, som fire sikkerhedsleverandører har givet hver sit navn.

BAGGRUND FOR DENNE RAPPORT

Baggrunden for SektorCERTs udgivelse af rapporten.



Baggrund for denne rapport

Denne rapport er udarbejdet af SektorCERT i samarbejde med journalisten Henrik Moltke på baggrund af seks tekniske rapporter fra tre kilder.
CERT Polska har desuden gennemlæst rapporten inden udgivelsen. SektorCERT takker for hjælpen. Eventuelle fejl er alene SektorCERTs ansvar.

Rapporten er skrevet til SektorCERTs medlemmer og til beslutningstagere i og omkring den kritiske infrastruktur, men udgives offentligt under TLP:CLEAR og må frit deles og citeres, så længe der klart refereres til SektorCERT og til rapporten. Rapporten er udgivet på dansk og engelsk.

Rapporten erstatter ikke de tekniske analyser fra CERT Polskas rapporter.

Læsere, der ønsker det fulde tekniske grundlag, henvises til kilderne nedenfor.

CERT Polska

CERT Polska er Polens nationale CERT, en del af forskningsinstituttet NASK. Deres første rapport er den officielle hændelsesrapport for energisektoren og denne rapports primære tekniske kilde. I august 2026 fulgte CERT Polska op med en analyse af et fjerde offer, et mindre kraftvarmeværk. Her henvises til de to rapporter som CP og FU.

- CP: Energy Sector Incident Report, 29 December: https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/ (30. januar 2026)
- FU: Follow-Up Analysis of the 29 December 2025 Energy Sector Incident: https://cert.pl/en/posts/2026/08/incident-follow-up-report-energy-sector-2025/ (7. august 2026)

Dragos

Dragos er et amerikansk sikkerhedsfirma med speciale i industrielle styresystemer (OT/ICS). Firmaet analyserer angrebet i et net- og forsyningsperspektiv og er særlig relevant for DER-vinklen. Dragos tilskriver angrebet med moderat sikkerhed aktørklyngen ELECTRUM, som overlapper med Sandworm, om end Dragos selv bemærker, at ikke al Sandworm-aktivitet er ELECTRUM eller omvendt.

- ELECTRUM: Cyber Attack on Poland's Electric System 2025 (Intelligence Brief, opdateret januar 2026), præsenteret på Dragos' blog 28. januar 2026: https://www.dragos.com/blog/poland-power-grid-attack-electrum-targets-distributed-energy-2025

ESET

ESET er et slovakisk sikkerhedsfirma. Det var en EDR-løsning fra ESET, der stoppede wiperen på det store kraftvarmeværk. To blogposts er centrale, især for analysen af DynoWiper og attributionen til Sandworm, som ESET fastholder med moderat sikkerhed ("medium confidence").

- Sandworm behind cyberattack on Poland's power grid in late 2025: https://www.welivesecurity.com/en/eset-research/eset-research-sandworm-cyberattack-poland-power-grid-late-2025/ (23. januar 2026)
- DynoWiper update: Technical analysis and attribution: https://www.welivesecurity.com/en/eset-research/dynowiper-update-technical-analysis-attribution/ (30. januar 2026)
- APT Activity Report, October 2025 - March 2026: https://www.welivesecurity.com/en/eset-research/eset-apt-activity-report-q4-2025-q1-2026/ (28. maj 2026)

KILDER OG NOTER



Kilder og noter

Citater fra engelsk og polsk er oversat af rapportens forfattere, medmindre andet er angivet.

[1] Styrelsen for Samfundssikkerhed (SAMSIK), "Skærpet trussel fra destruktive cyberangreb", trusselsvurdering, 30. juni 2026: https://samsik.dk/publikation/skaerpet-trussel-fra-destruktive-cyberangreb/. Angrebet i Polen anføres blandt eksemplerne på russiske statslige hackergruppers "øget risikovillighed" over for europæiske NATO-lande; det samlede trusselsniveau for destruktive cyberangreb fastholdes på "middel".

[2] Foreign, Commonwealth & Development Office, "UK and EU strike Russian cyber networks with new sanctions", 13. juli 2026: https://www.gov.uk/government/news/uk-and-eu-strike-russian-cyber-networks-with-new-sanctions ("attributing the attack on Poland's energy grid to Russia's FSB Centre 16"; "could have caused 500,000 citizens to lose electricity"). EU-Rådet, Statement by the High Representative on behalf of the European Union, 13. juli 2026: https://www.consilium.europa.eu/en/press/press-releases/2026/07/13/cyber-russia-statement-by-the-high-representative-on-behalf-of-the-european-union-denouncing-russia-s-malicious-cyber-ecosystem-targeting-the-eu-its-member-states-and-international-partners/ ("disruptive sabotage operations against critical infrastructure, including combined heating and power plants"). Joint Cybersecurity Advisory AA26-194A, 13. juli 2026, medunderskrevet af myndigheder fra 13 lande, herunder Danmark og Polen: https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-194a (Center 16 knyttes til Berserk Bear, Dragonfly, Ghost Blizzard og Static Tundra).

[3] RMF FM, "Polsce groził blackout? Gawkowski: Cyfrowe czołgi już tu są", Popołudniowa rozmowa w RMF FM, 13. januar 2026: https://www.rmf24.pl/rozmowy/popoludniowa-rozmowa/news-polsce-grozil-blackout-gawkowski-cyfrowe-czolgi-juz-tu-sa,nId,8057521 ("Mieliśmy do czynienia z sabotażem ze strony rosyjskiej. Cyfrowe czołgi już tu są. Byliśmy blisko blackoutu"; "najpoważniejszy atak na infrastrukturę energetyczną, który miał na celu wyłączenie prądu obywatelom pod koniec grudnia").

[4] Polskie Radio 24 , 15. januar 2026: "Ani przez chwilę nie była zagrożona infrastruktura krytyczna, czyli sieci przesyłowe"; "To w ogóle nie wchodziło w rachubę": https://www.polskieradio.pl/399/7977/Artykul/3634277,Donald-Tusk-o-cyberatakach-infrastruktura-krytyczna-nie-byla-zagrozona. Om varmetallet, PAP via Radio Kielce, 15. januar 2026: "nawet do 500 tys. ludzi byłoby pozbawionych ciepła": https://radiokielce.pl/1374607/atak-cybernetyczny-na-polske-mogl-pozbawic-500-tys-ludzi-ciepla/. Begge citater stammer fra premierministerens pressemøde samme dag. Dragos, s. 3, daterer orienteringen af regeringen til 14. januar 2026, dagen før pressemødet.

[5] Dragos, "ELECTRUM: Cyber Attack on Poland's Electric System 2025", s. 2.

[6] CP, s. 36-37: CERT Polska knytter angrebets infrastruktur til den klynge, Cisco og FBI beskriver som Static Tundra, Berserk Bear, Ghost Blizzard og Dragonfly, betegner det som klyngens første offentligt beskrevne destruktive aktivitet og kan ikke afgøre, om Sandworm deltog; ligheden med tidligere wipere er "too low". ESET tilskriver alene wiperen til Sandworm med "medium confidence" (DynoWiper update; gentaget i APT Activity Report, 28. maj 2026). Dragos peger med "moderate confidence" på ELECTRUM, "not all Sandworm activity is ELECTRUM or vice versa" (Dragos, s. 2 og 6).

[7] SektorCERT, Trusselsvurdering for kritisk infrastruktur i Kongeriet Danmark 2026, s. 12, de 10 mest relevante trusselsaktører mod dansk kritisk infrastruktur.

[8] SektorCERT, "Angrebet mod dansk, kritisk infrastruktur", november 2023 (TLP:CLEAR): https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-Angrebet-mod-dansk-kritisk-infrastruktur-TLP-CLEAR.pdf. Tallene stammer herfra: 16 selskaber angrebet den 11. maj, heraf 11 kompromitteret, og 22 kompromitterede selskaber i alt efter anden bølge fra den 22. maj. Om indikatorerne på Sandworm og SektorCERTs forbehold, se s. 14-16.

[9] Bekræftet over for SektorCERT af samarbejdspartnere, som ikke kan navngives, august 2026. Omfanget af



medlemmernes brug af private APN'er var under afklaring ved redaktionens slutning.

[10] Dragos, s. 9 (blackout-vurderingen, roterende reserver og kaskadefejl) og s. 4 og 9 (det iberiske strømudfald 2025). ENTSO-E, Expert Panel Final Report on the 28 April 2025 blackout in Spain and Portugal, 20. marts 2026: https://www.entsoe.eu/publications/blackout/28-april-2025-iberian-blackout/

[11] Zyxel, CVE-2023-28771, offentliggjort 25. april 2023, CVSS 9.8. SektorCERTs ekstra advarsel, 1. maj 2023.

[12] Lov nr. 258 af 6. marts 2025 om styrket beredskab i energisektoren og bekendtgørelse nr. 260 af 6. marts 2025 om modstandsdygtighed og beredskab i energisektoren. Retsinformation. Ikrafttræden 7. marts 2025 (lovens § 38, bekendtgørelsens § 123). Overgangsreglen for § 62: bekendtgørelsens § 123, stk. 4 og 5. Små virksomheder: lovens § 2, stk. 2.

[13] SektorCERT, "Håndbog om SektorCERTs 25 anbefalinger", november 2024: https://sektorcert.dk/wp-content/uploads/2024/12/25-Anbefalinger_DK.pdf

[14] FU, s. 16-17, afsnittet Summary. Gengivet i sammentrængt form.

[15] FU, s. 11: PLC'erne blev sat i STOP og beskyttet med en adgangskode, hvorefter dampturbinen og vandbehandlingen til procesvand standsede, og kraftvarmeprocessen blev afbrudt. Genopretningen begyndte, mens angriberen fortsat var til stede i netværket. Operatørerne nulstillede enhederne til fabriksindstilling og genindlæste de tilgængelige sikkerhedskopier af styringslogikken.

[16] Reuters, "Massive cyberattack on Polish power system in December failed, minister says", 13. januar 2026: https://www.reuters.com/sustainability/climate-energy/massive-cyberattack-polish-power-system-december-failed-minister-says-2026-01-13/

[17] Dragos, "ELECTRUM: Cyber Attack on Poland's Electric System 2025", s. 12 (Critical Control 05): samme firewall-model med samme fejlkonfiguration på mange anlæg gør ét indbrud til et systemisk kompromis.

[18] CP, s. 8-9: firmwareversion 13.5.3.0 ikke i drift på nogen af de ramte anlæg; secure update fra version 13.2.1, ikke slået til; CVE-2024-2617 rettet i 13.7.7; forløbet bekræftet af Hitachi Energy PSIRT.

[19] FU, s. 16 (og s. 4): "the first observed instance of this attack vector being used in a real-world cyberattack"; konfigurationen "commonly encountered in Poland", og tilsvarende opsætninger vurderes udbredt i andre lande.

[20] CP, s. 5, PSE's vurdering: angrebet påvirkede ikke elsystemets stabilitet; givet angriberens adgang var der en risiko for at forstyrre produktionen på de ramte anlæg; selv da ville det samlede kapacitetstab på alle 30 anlæg ikke have påvirket stabiliteten "during the period in question". Dragos, s. 9: "unlikely to cause a nationwide blackout".

[21] Dragos, s. 8: "more opportunistic than the 2015 or 2016 operations"; "moderate confidence that opportunism was a key factor"; "low confidence that this was due to incomplete preparation rather than a lack of capability".

[22] ESET Research, "APT Activity Report, October 2025 - March 2026", 28. maj 2026: https://www.welivesecurity.com/en/eset-research/eset-apt-activity-report-q4-2025-q1-2026/. Om attribution, s. 22: "we attribute the data-wiping component of this activity to Sandworm with medium confidence". Om sjældenheden, s. 21: "a very rare (if not unprecedented) instance of a critical infrastructure operator in a NATO country being expressly targeted with a wiper". Om motiv, s. 22: "The ultimate motivations behind this incident remain murky", og s. 3: "Given Poland's role in helping stabilize Ukraine's electricity supply, it is possible that the operation was intended to strain Ukraine's power grid during the winter".



Denne side er med vilje tom.



Denne side er med vilje tom.

SektorCERT er de kritiske sektorers cybersikkerhedscenter. Vi er med til at opdage og håndtere, når den kritiske infrastruktur udsættes for cyberangreb. SektorCERT er en non-profit forening ejet og finansieret af selskaber inden for dansk kritisk infrastruktur.

SektorCERT samarbejder med Europas andre CERT'er og er med i en række sikkerhedsorganisationer, som gør, at vi har stor viden om angreb mod kritisk infrastruktur.

digital tryghed

Om rapporten

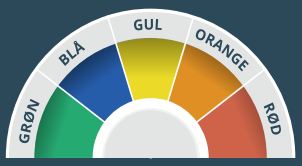
Denne rapport gennemgår:

- hvad der skete i Polen
- hvorfor angrebet henholdsvis lykkedes og fejlede
- og hvilke erfaringer Danmark bør drage, så styrken ved mange små grønne anlæg ikke vendes til en akilleshæl

Trusselsniveauer

SektorCERT anvender en 5-trins-skala til angivelse af trusselsniveau.

Skalaen er baseret på en international standard udarbejdet af Center for Internet Security (CIS).



SektorCERTs miljøfokus

CO2 neutral
CLIMATECALC
CC-000091/DK

SVANEMÆRKET
Tryksag
5041 0200

FSC
www.fsc.org
MIX
Papir | Støtter ansvarligt skovbrug
FSC® C109833

SektorCERT anvender følgende skala til vurdering af sandsynlighed:

Meget sandsynligt	>90 %
Sandsynligt	60 - 90 %
Muligt	40 - 60 %
Mindre sandsynligt	10 - 40 %
Usandsynligt	<10 %

Målgruppe

Alle de af SektorCERTs medlemmer, der har det operationelle ansvar for cybersikkerheden i dansk kritisk infrastruktur.

- ☑ **Strategisk**
- ☑ **Operationelt**
- ☐ **Taktisk**

Dette dokument er TLP:CLEAR

TLP:**CLEAR**
Publikationen må videreformidles til hele verden; der er ingen begrænsninger for videreformidling.

Med forbehold for de almindelige ophavsretsregler kan TLP:CLEAR-oplysninger deles uden begrænsninger.

Rapporten er udarbejdet i samarbejde med journalisten Henrik Moltke.

SEKTOR CERT

Telefonnummer:

+45 33 23 13 23

E-mail adresse:

info@sektorcert.dk

PGP nøgle:

C2EF 6314 7860 2B1E 2341 ACF4 DBC3 511D 3D06 BB3A

Besøgs- og postadresser:

Sommerfuglevej 2A
6000 Kolding

Bredgade 45
1260 København K

CVR nummer:

41369841

Satellittelefon:

+88 16 22 45 60 29

SINE radio:

73 12 056