CENTER FOR CYBERSIKKERHED

TRUSSELSVURDERING

Cybertruslen mod vandsektoren

Januar • 2025

Indhold

CENTER FOR CYBERSIKKERHED

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

Januar 2025

Cybertruslen mod vandsektoren

Formålet med denne trusselsvurdering er at beskrive cybertruslen rettet mod den danske vandsektor. Vurderingen kan blandt andet styrke risikoejeres forståelse af cybertruslen og indgå som en del af grundlaget for risikovurderingsarbejdet i sektoren. Vurderingen er udarbejdet i dialog med den decentrale cyber- og informationssikkerhedsenhed (DCIS) for vandsektoren.

Hovedvurdering

- Truslen fra cyberkriminalitet mod vandsektoren er **MEGET HØJ**. Truslen udspringer primært fra ransomware-aktører, der krypterer it-systemer og data med henblik på at afpresse ofre for løsesummer.
- Truslen fra cyberaktivisme mod vandsektoren er **MIDDEL**. Vandsektoren er et mindre prioriteret mål end visse andre dele af samfundet. Der har dog været et markant cyberaktivistisk angreb mod sektoren i 2024, der midlertidigt udfordrede forsyningssikkerheden for et mindre antal kunder.
- Truslen fra destruktive cyberangreb mod vandsektoren er **MIDDEL**. Det er muligt, at myndigheder og virksomheder i sektoren vil blive udsat for destruktive cyberangreb.
- Truslen fra cyberspionage mod vandsektoren er **MIDDEL**. Den danske vandsektor udgør ikke et lige så højt prioriteret spionagemål som andre dele af Danmark.
- Truslen fra cyberterror mod vandsektoren er **INGEN**.

Indledning

Som følge af den globale sikkerhedspolitiske situation står Danmark over for et mere sammensat trusselsbillede end i mange år. Det, der foregår i den fysiske verden smitter også af på cyberdomænet, og den danske vandsektor står derfor, ligesom mange andre dele af det danske samfund, over for et dynamisk trusselslandskab.

Vandsektoren i Danmark

Denne trusselsvurdering dækker drikke- og spildevandssektoren i Danmark. Vandsektoren består af et stort antal virksomheder af forskellig størrelse og omfatter i denne trussels-vurdering bl.a. drikkevandsselskaber, der behandler og distribuerer drikkevand, spilde-vandsselskaber, der afleder og renser spildevand og multiforsyningsselskaber, der håndterer flere forsyningsarter. Den samlede vandsektor forsyner og håndterer drikke- og spildevand for virksomheder, myndigheder og private hjem. Sektoren har derved også berøring med andre samfundsvigtige sektorer, samt overlap med energisektoren gennem multiforsyningsselskaberne.

Cyberdomænet kan ligeledes have effekt på den fysiske verden, også i vandsektoren. En pro-russisk cyberaktivistisk hackergruppe kompromitterede i slutningen af december 2024 sandsynligvis operationel teknologi (OT) med svage sikkerheds-foranstaltninger hos et mindre dansk vandværk. Hændelsen resulterede i, at nogle kunder stod uden vand i flere timer og at et vandrør sprang som resultat af forhøjet vandtryk. Angrebet blev dog hurtigt opdaget og vandforsyningen genoprettet. Alligevel understreger angrebet, at cyberangreb kan påvirke forsyningssikkerheden – også i den danske vandsektor.

Vandsektoren er kritisk, både for de enkelte danske hjem, men også for virksomheder og myndigheder i andre samfundsvigtige sektorer, hvor vandsektoren er afgørende for driften. Kritisk infrastruktur kan komme i hackeres søgelys på forskellig vis. Statsstøttede hackergrupper udfører cyberspionage for at opnå viden, der ikke er offentligt tilgængelig, og kriminelle hackere forsøger med alle tilgængelige midler at tjene penge via cyberangreb. Ved en simpel internetsøgning kan eksempelvis cyberaktivister finde frem til internetvendte enheder med ingen eller begrænset beskyttelse, og en organisation kan blive ramt alene, fordi den er sårbar.

Center for Cybersikkerhed (CFCS) deler cybertruslen op i fem formålskategorier: cyberkriminalitet, cyberspionage, cyberaktivisme, destruktive cyberangreb og cyberterror. Vi beskriver trusselsbilledet med udgangspunkt i, hvorfor et givent angreb bliver udført. Ofte medfører det også en forståelse af, hvilken type aktør der står bag.

Det er dog ikke altid enkelt at fastslå formålet med et cyberangreb, og ofte kan der i et angreb være aspekter af flere formål. Samtidig kan der være overlap i cyberaktørers fremgangsmåde. De fem forskellige formålskategorier krydser på den måde nogle gange hinanden i både metode og hensigt, hvilket kan gøre analysen bag kompliceret. Det ovenfor nævnte angreb mod et vandværk understreger dette, idet cyberaktivister udførte et angreb, der også falder ind under kriterierne for et destruktivt cyberangreb.

Trusselsvurderingen tydeliggør hvilke kategorier af truslen, der er de mest aktuelle, men ikke hvilke angreb vandsektoren er mest sårbar over for, eller hvilke specifikke konsekvenser et givent angreb vil få. Den ekspertise findes i sektoren, som kan bruge denne trusselsvurdering til at kvalificere det samlede risikoarbejde.

Trusselsvurderingen bygger på CFCS' samlede vidensgrundlag fra ind- og udland, og har en varslingshorisont på to år. Vurderingen anvender de trusselsniveauer og sandsynlighedsgrader, der er forklaret sidst i trusselsvurderingen.

OT (Operational Technology)

OT dækker alle former for teknologi brugt til realtidsstyring, monitorering og indsamling af data i produktioner. På et vandværk er OT fx PLC'er (programmable logic controller) og andre systemer, som bruges til at overvåge og styre processer i eksempelvis sensorer, pumper og ventiler.

Cyberkriminalitet

CFCS vurderer, at truslen fra cyberkriminalitet mod vandsektoren er **MEGET HØJ**.

Det er meget sandsynligt, at myndigheder og virksomheder i sektoren vil blive udsat for forsøg på cyberkriminalitet inden for de næste to år. Især ransomware-angreb udgør en trussel mod den operationelle drift i vandsektoren.

Flere organisationer i den danske vandsektor har været ramt af de ransomware-angreb, som løbende rammer danske virksomheder og myndigheder. Særligt Ransomware-as-a-Service (RaaS) grupper udfører ransomware-angreb mod vandsektoren i hele Europa, herunder også i Danmark.

Ransomware-as-a-Service: professionel organisering i det kriminelle miljø

Ved et ransomware-angreb bliver data og systemer gjort utilgængelige for offeret, ofte ved kryptering, og derved holdt som gidsel. Angriberen kræver en løsesum, typisk i form af kryptovaluta, for at give offeret adgang til sine data igen.

RaaS-modellen kan sammenlignes med den platformsøkonomi, der kendes fra lovlige markeder. Modellen fungerer ved, at kriminelle bagmænd stiller en platform til rådighed for andre kriminelle partnere, som bruger platformen til at udføre ransomware-angreb. De udefrakommende kriminelle brugere kaldes for affiliates.

Modellen tillader selv mindre teknisk kyndige affiliates at tjene penge på ransomware-angreb, selvom bagmændene i RaaS-gruppen får størstedelen af løsesummen. LockBit 3.0, Black Basta og Cactus er eksempler på RaaS-grupper.

Et ransomware-angreb kan få konsekvenser for det enkelte offer, både i form af potentielle læk af sensitive data og økonomiske tab, men potentielt også for det omkringliggende samfund. For eksempel kan et ransomware-angreb i vandsektoren få konsekvenser for forsyningssikkerheden, hvis angrebet påvirker den operationelle drift.

De kriminelle hackere kan have en formodning om, at organisationer der producerer eller leverer en samfundsvigtig ydelse, herunder vandsektoren, kan være mere villige til at betale en løsesum end andre potentielle mål. Det skyldes, at samfundsvigtig produktion generelt har en lav tolerance for nedetid i driften

CFCS vurderer, at grupperne, der står bag ransomware-angreb, oftest er opportunistiske ift. deres måludpegning. Når grupperne rammer mål i eksempelvis vandsektoren, går de altså efter at ramme organisationer, der for dem udgør attraktive mål. Det primære formål for grupperne er at tjene penge og således ikke at sende et politisk budskab.

Phishing og spear-phishing som angrebsvektor
For at udføre et ransomware-angreb skal de kriminelle først opnå indledende adgang ind i et offers systemer. Denne adgang kan de forsøge at opnå ved at sende phishing-mails til en stor mængde potentielle ofre. Eksempelvis blev en række amerikanske vandværker i 2021 angrebet med ransomware af kriminelle aktører gennem spear-phishing inden for et halvt år.

Ved en phishing-mail forsøger de kriminelle at narre modtageren af mailen til f.eks. at give uretmæssig adgang til it-systemer, uden modtageren er klar over det.

Mere målrettede phishing-kampagner kaldes for spear phishing. Spear phishing-mails bliver skræddersyet til at ramme enkelte ofre ad gangen i stedet for en stor mængde. Spear phishing kræver ofte viden om de organisationer eller organisationers medarbejdere, som de kriminelle forsøger at ramme.

Phishing og spear phishing har flere fordele for de kriminelle. De kræver ikke store tekniske færdigheder at udføre, og de er målrettet det led i sikkerhedskæden, som er sværest at hærde – det menneskelige. Både phishing og spear phishing kan virke meget overbevisende på medarbejdere i en organisation, som uvidende og uden ond hensigt kan give de kriminelle adgang til systemerne.

OT-systemer kan blive ramt som følgevirkning
Langt størstedelen af de ransomware-typer, som kriminelle hackergrupper bruger i deres angreb, er designet til at kryptere it-systemer. Et angreb i en organisations it-system kan dog godt påvirke virksomhedens OT, der anvendes i den fysiske drift.

Manglende eller mangelfuld segmentering mellem it- og OT-systemer kan lede til, at OT-systemer rammes som følgevirkning af et ransomware-angreb, der egentlig var målrettet it-systemer.

Et ransomware-angreb kan få betydning for forsyningssikkerheden. Det kan f.eks. ske ved, at OT-enheder påvirkes af malwaren. Det kan også ske ved, at den ramte organisation vælger at lukke ned for driften af frygt for, at organisationens OT vil blive påvirket. Derved kan organisationen være tvunget til at overgå til manuel betjening eller at stoppe driften helt, hvis manuel betjening ikke er mulig.

Angreb på softwareleverandører kan også føre til driftstop
Driften kan også påvirkes ved, at en leverandør af f.eks. software eller applikationer til OT-systemer bliver angrebet med ransomware, og at leverandøren vælger at lukke for deres ydelser af frygt for spredning af ransomwaren.

Et sådant scenarie indtraf, da den norske teknologivirksomhed Volue blev ramt af ransomware i 2021. Virksomheden leverer bl.a. softwareløsninger til forsynings-selskaber i Europa, herunder i Norge. Som følge af angrebet og frygten for spredning, valgte Volue at lukke deres digitale infrastruktur hos vandværker i et stort antal norske kommuner.

At en leverandør bruges som angrebsvinkel af hackerne kaldes for et supply-chain-angreb. Et supply-chain-angreb kan påvirke forsyningssikkerheden hos mange vandværker på samme tid, hvis de er kunde hos den samme leverandør.

Cyberaktivisme

CFCS vurderer, at truslen fra cyberaktivisme mod vandsektoren er **MIDDEL**.

Selvom det er muligt, at myndigheder og virksomheder i sektoren vil blive udsat for et cyberaktivistisk angreb, er vandsektoren et mindre prioriteret mål end andre dele af samfundet.

Som beskrevet blev et mindre dansk vandværk i slutningen af 2024 angrebet af pro-russiske cyberaktivister, som manipulerede vandtrykket via vandværkets operationelle systemer. Angrebet medførte, at 450 husstande kortvarigt ikke havde vand på grund af lavt vandtryk. Senere var ca. 50 husstande uden vand i adskillige timer, da forhøjet vandtryk resulterede i et sprunget vandrør.

CFCS vurderer, at vandværket blev ramt på grund af systemernes lave beskyttelses-niveau og således ikke, fordi man gik målrettet efter vandsektoren.

Cyberaktivister rammer andre dele af samfundet med DDoS-angreb
På trods af det nævnte angreb er det fortsat hovedsageligt DDoS-angreb (Distributed Denial of Service), som aktivister retter mod danske organisationer. DDoS-angreb bruges til at ramme brugervendte hjemmesider og gøre hjemmesiderne utilgængelige. Sådanne angreb er hovedsageligt forstyrrende og af kortere varighed, og er ikke ødelæggende for ofrenes systemer. Nedetiden på ofrenes hjemmeside er med til at skabe omtale af aktivisternes dagsorden.

CFCS vurderer, at den danske vandsektor på nuværende tidspunkt ikke er et prioriteret mål for de pro-russiske cyberaktivister, der løbende udfører DDoS-angreb mod danske virksomheder og myndigheder. Derfor er trusselsniveauet lavere mod sektoren, end det generelle niveau er for hele Danmark.

Selvom trusselsniveauet mod vandsektoren er lavere end det overordnede niveau for Danmark, er det aktivistiske trusselsbillede omskifteligt, idet nye grupper eller mærkesager i det cyberaktivistiske miljø kan opstå og intensivere hastigt. Som angrebet i december 2024 illustrerer, kan organisationer i vandsektoren komme i aktivisternes søgelys uden varsel.

CFCS afstår fra at nævne aktivister ved navn

Formålet med aktivisme er at få opmærksomhed fra omverdenen. De cyberaktivistiske grupper opsøger omtale i vestlige medier og deler vestlige, herunder danske, mediers artikler om gruppernes egne angreb. Selvom CFCS er bekendt med gruppernes navne, bliver de derfor ikke nævnt i publikationer, medmindre det er afgørende for at give et retvisende trusselsbillede.

Aktivister kan også anvende andre angrebsmetoder
Ud over angrebet på det danske vandværk i december 2024, er der også i udlandet eksempler på aktivistiske grupper, der påstår destruktive cyberangreb på vandværker. De påståede angreb sker ofte i forbindelse med krig eller konflikt, f.eks. i konflikten mellem Israel og Hamas. Der er dog stadig tale om få angreb sammenlignet med de mange DDoS-angreb, som løbende rammer mål i Danmark og Vesten.

CFCS vurderer, at cyberaktivistiske angreb af destruktiv karakter er opportunistiske i forhold til måludpegning og rammer mål, der har lav beskyttelse. Alligevel er disse destruktive cyberangreb mere krævende at udføre end de angreb, som cyberaktivister normalt gør brug af. I mange tilfælde er det også usikkert, om angrebene har fundet sted, og om de har haft en reel effekt.

CFCS vurderer, at aktivisters både falske og reelle angreb af destruktiv karakter ligesom anden cyberaktivisme har til hensigt at skabe offentlig opmærksomhed omkring deres dagsorden.

Cyberaktivister verden over har også ramt deres ofre ved defacement-angreb, hvor de ændrer en hjemmesides visuelle udtryk eller indhold, og af hack og læk angreb, hvor data stjæles og offentliggøres, bl.a. for at skade den ramte organisations omdømme.

Cyberaktivisterne er en del af det nye normalbillede
Truslen fra cyberaktivisme mod danske virksomheder og myndigheder blev en del af normalbilledet efter Ruslands invasion af Ukraine. Truslen skal både ses i kontekst af Danmarks rolle som bidragsyder af militær støtte til Ukraine og som medlemsland i EU og NATO. Pro-russiske aktivister angriber løbende virksomheder og organisationer i Europa og NATO, som de ser som symbolske for vestlig støtte til Ukraine.

Den typiske cyberaktivisme er drevet af ideologiske eller politiske motiver og bliver som udgangspunkt udført uafhængigt af stater. Det kan dog være vanskeligt at vurdere en cyberaktivistisk aktørs tilhørsforhold til fremmede stater. I nogle tilfælde er det derfor ikke entydigt, om cyberaktivister handler overvejende på eget eller på en stats initiativ.

Destruktive cyberangreb

CFCS vurderer, at truslen fra destruktive cyberangreb mod vandsektoren, ligesom mod Danmark generelt, er **MIDDEL**.

Det ovenfor beskrevne angreb mod et dansk vandværk i 2024 falder ind under CFCS' definition på et destruktivt cyberangreb, selvom konsekvenserne var begrænsede.

Truslen fra destruktive cyberangreb mod Danmark udspringer primært fra Rusland, og landet er villig til at bruge hybride virkemidler med destruktive effekter i europæiske NATO-lande. CFCS vurderer, at denne risikovillighed også omfatter destruktive cyberangreb i vandsektoren. Russiske statslige hackergrupper har i årevis haft kapacitet til at udføre destruktive cyberangreb.

CFCS vurderer, at mange typer af organisationer i samfundsvigtige sektorer vil kunne blive udvalgt som mål for eventuelle destruktive cyberangreb, herunder organisationer i vandsektoren. Selvom truslen primært kommer fra Rusland, udgør Iran også en potentiel trussel.

Truslen fra ikke-statslige hackere
CFCS vurderer, at der også er nogle ikke-statslige aktører, som er i stand til at udføre destruktive cyberangreb med begrænset effekt. Angrebene kan have forskellige formål. Et formål kan f.eks. være at skabe opmærksomhed omkring en sag eller dagsorden, hvilket kendetegner cyberaktivisme. CFCS vurderer, at det destruktive cyberangreb mod et dansk vandværk i december 2024 netop er et eksempel på dette.

Selvom destruktive cyberangreb fra ikke-statslige aktører kan understøtte staters interesser, er det ikke ensbetydende med, at aktørerne arbejder direkte for staten. Pro-russiske cyberaktivister, som dem der ramte vandsektoren med et destruktivt cyberangreb i 2024, er et godt eksempel på, hvordan ikke-statslige hackere kan understøtte staters interesser. CFCS vurderer dog, at nogle pro-russiske cyberaktivister har forbindelse til den russiske stat.

Formålet med destruktive cyberangreb vil være påvirkning
CFCS vurderer generelt, at eventuelle destruktive cyberangreb primært vil have til formål at påvirke befolkningen og beslutningstagere, eksempelvis at svække danskernes opbakning til Ukraine. Den konkrete fysiske effekt af angrebene vil sandsynligvis være sekundær i forhold til, om angrebene skaber opmærksomhed.

Det er mindre sandsynligt, at Rusland i den nuværende sikkerhedspolitiske situation vil gennemføre destruktive cyberangreb, hvor hensigten er at skabe alvorlige og omfattende konsekvenser for samfundsvigtige funktioner, herunder for vandsektoren. Selvom disse angreb for nuværende er mindre sandsynlige, vurderer CFCS, at russiske hackergrupper forbereder sig på at kunne udføre den form for destruktive angreb mod kritisk infrastruktur i Danmark i tilfælde af en eskalerende krise eller krig. Truslen fra sådanne angreb kan derfor stige med kort eller uden varsel.

Mindre omfattende cyberangreb kan dog også få betydelige konsekvenser for vandsektoren. Det kan f.eks. være angreb, der påvirker forsyningssikkerheden i begrænset omfang. Selv hvis destruktive cyberangreb ingen konsekvenser har for forsyningssikkerheden, kan de skabe utryghed og påvirke samfundet.

Svage sikkerhedsforanstaltninger kan lede til angreb

Vandsektoren kan være et interessant mål for hackergrupper af flere årsager. Dels er det sandsynligt, at måludvælgelsen for eventuelle destruktive cyberangreb vil være påvirket af, hvor hackergrupperne har adgang eller nemt kan få det. Eksempelvis kan svage sikkerhedsforanstaltninger i OT-systemer komme i opportunistiske hackeres søgelys. CFCS vurderer, at netop svage sikkerhedsforanstaltninger var årsagen til, at et dansk vandværk blev udsat for cyberangreb i december 2024.

Samtidigt er sektoren afgørende for både civil og militær infrastruktur. Sektoren kan derfor være interessant for statslige hackergrupper, fordi den leverer ydelser til flere forskellige sektorer og myndigheder. Det inkluderer f.eks. producenter af medicin og samfundsvigtig teknologi. Det er muligt, at vandsektoren kan blive udsat for forsøg på cyberspionage som forberedelse til fremtidige destruktive cyberangreb, med henblik på at hæmme andre samfundsvigtige sektorer i tilfælde af en eskalerende krise eller krig.

Statslige hackergrupper kan f.eks. bruge cyberspionage til at etablere såkaldte bagdøre på ofres kompromitterede systemer. Disse bagdøre kan hackergrupperne anvende i fremtidige destruktive angreb.

Bagdøre – elektroniske smutveje ind i systemer

En bagdør er en uautoriseret måde at få adgang til et system. Det kan f.eks. være gennem en fejl i software eller konfiguration. En bagdør kan være bevidst placeret af en person, der har haft adgang til udviklingen af softwaren eller konfigurationen af systemet. En bagdør kan også være en del af malware på systemet.

Cyberspionage vil ofte ske forud for et destruktivt cyberangreb, men er ikke en forudsætning for dem alle. Hackere kan i nogle tilfælde med begrænset forberedelse udføre simple, destruktive cyberangreb mod systemer med dårlig beskyttelse.

Stater kan forsøge at sløre deres forbindelse til destruktive cyberangreb

Fremmede stater kan forsøge at sløre deres involvering i destruktive cyberangreb. På den måde kan stater f.eks. gøre det vanskeligere for lande, der rammes af de hybride aktiviteter, at reagere med et modsvar. Stater kan sløre deres forbindelse til angreb på forskellige måder.

CFCS vurderer, at Rusland i den nuværende situation vil forsøge at sløre sin forbindelse til eventuelle destruktive cyberangreb. Det kan russiske statslige hackere eksempelvis gøre ved at udføre angreb, der ligner kriminelle ransomware-angreb, hvor data bliver krypteret, men efterfølgende ikke kan dekrypteres.

Statslige hackere kan også forsøge at skjule deres forbindelse til destruktive angreb ved at udgive sig for at være aktivistiske hackere. Det kan de gøre ved eksempelvis at oprette hjemmesider eller konti på forskellige platforme, hvor de udgiver sig for at være cyberaktivister og tager ansvar for destruktive cyberangreb. Dette fænomen kaldes ofte for 'faketivisme'. Faketivisme er, i populær tale, når en statslig gruppe udfører cyberangreb, der ligner cyberaktivisme.

Cyberspionage

CFCS vurderer, at truslen fra cyberspionage mod vandsektoren er **MIDDEL**.

Det er muligt, at sektoren vil blive udsat for forsøg på cyberspionage inden for de næste to år.

CFCS vurderer, at den danske vandsektor ikke udgør et lige så højt prioriteret spionagemål som visse andre sektorer i Danmark. Det er sandsynligt, at truslen primært kommer fra brede spionagekampagner mod mange ofre, og truslen er således ikke målrettet den danske vandsektor.

CFCS vurderer dog, at fremmede stater, herunder Rusland og Kina, har en vedvarende interesse i den danske energisektor. Multiforsyningsselskaber, der både leverer energi og håndterer drikke- og spildevand, kan derfor være udsat for en større trussel for cyberspionage end den øvrige vandsektor.

Formålet med cyberspionage varierer

Fremmede stater udfører cyberspionage med forskellige formål. Statslige hackergrupper kan f.eks. udføre cyberspionage med det formål at få adgang til viden, der kan understøtte teknologiske udviklingsmål, og derved fremme staters økonomiske interesser.

Statslige hackere udfører også cyberspionage hvis muligheden for cyberspionage opstår, f.eks. som følge af udnyttelse af en udbredt sårbarhed. På den måde kan vandsektoren også blive udsat for cyberspionage, uden sektoren nødvendigvis var hackernes tiltænkte mål.

Generelt har fremmede stater som Rusland og Kina en vedvarende interesse i at udføre cyberspionage mod organisationer i Europa, herunder i Danmark. Interessen omfatter også organisationer i kritisk infrastruktur. Både Rusland og Kina har betydelige cyberkapaciteter, og begge stater anvender cyberspionage for at skaffe sig adgang til forskellige typer viden hos deres ofre.

Forsøg på cyberspionage kan bl.a. være rettet mod mailsystemer, som en organisation anvender. Hvis en hackergruppe lykkedes med at kompromittere et mailsystem, kan den opnåede adgang anvendes til at indhente viden om organisationen og dens medarbejdere. Den viden kan hackergruppen f.eks. bruge til at sende spear-phishing mails fra offerets system rundt til andre brugere i netværket.

Statslige hackergrupper kan også anvende opnåede adgange ind i ofres systemer til andre typer af cyberangreb. En kompromittering i kritisk infrastruktur med henblik på cyberspionage kan f.eks. også bruges som forberedelse til mulige fremtidige destruktive angreb, i tilfælde af krig eller konflikt. Det er dog, som beskrevet, ikke alle destruktive cyberangreb, der kræver forudgående cyberspionage.

USA: Kinesiske statslige hackere planlagde angreb i amerikansk kritisk infrastruktur

I februar 2024 meldte amerikanske myndigheder ud, at en kinesisk statsstøttet hackergruppe kaldet Volt Typhoon havde kompromitteret it-miljøer hos organisationer i flere samfundsvigtige sektorer i USA, herunder i vandsektoren.

Ifølge de amerikanske myndigheder peger hackergruppens aktivitet i ofrenes systemer på, at hovedformålet med kompromitteringerne ikke kun var spionage. Formålet med angrebene var i stedet at opnå adgange i de kompromitterede systemer, der kunne gøre hackergruppen i stand til at udføre destruktive cyberangreb i amerikansk kritisk infrastruktur, i tilfælde af krig eller konflikt. Det var ifølge myndighederne tydeligt, da Volt Typhoon havde positioneret sig på en sådan måde i flere ofres it-systemer, at gruppen kunne bevæge sig lateralt til forbundne OT-systemer, hvis det skulle blive nødvendigt.

De amerikanske myndigheder har i nogle af de observerede tilfælde fundet indikationer på, at Volt Typhoon har haft fodfæste i ofres it-miljøer i mindst fem år.

Cyberterror

CFCS vurderer, at truslen fra cyberterror mod vandsektoren er **INGEN**.

Det er usandsynligt, at myndigheder og virksomheder i sektoren vil blive udsat for forsøg på cyberterror inden for de næste to år.

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

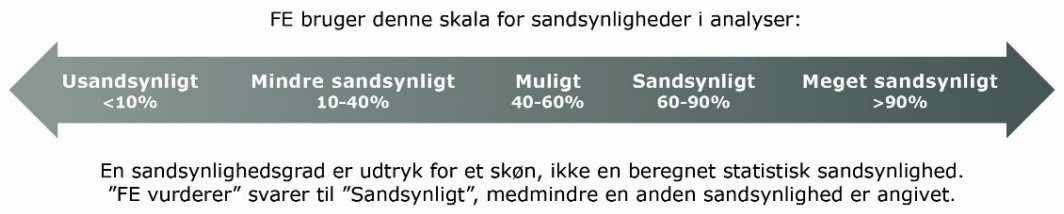
CFCS vurderer, at militante ekstremister hverken har intention om eller den fornødne kapacitet til at begå et cyberangreb med samme effekt som konventionel terror mod vandsektoren i Danmark.

Trusselsniveauer

Forsvarets Efterretningstjeneste bruger følgende trusselsniveauer.

INGEN	Der er ingen tegn på en trussel. Der er ingen aktør, der både har kapacitet til og intention om angreb/skadelig aktivitet.
LAV	En eller flere aktører har kapacitet til og intention om angreb/skadelig aktivitet. Men enten er kapaciteten eller intentionen eller begge dele begrænset.
MIDDEL	En eller flere aktører har kapacitet til og intention om angreb/skadelig aktivitet. Men der er ikke indikationer på specifik planlægning af angreb/skadelig aktivitet.
HØJ	En eller flere aktører har kapacitet til og foretager specifik planlægning af angreb/skadelig aktivitet, eller har allerede gennemført eller forsøgt angreb/skadelig aktivitet.
MEGET HØJ	Der er enten oplysninger om, at en eller flere aktører iværksætter angreb/skadelig aktivitet, herunder oplysninger om tid og mål, *eller* en eller flere aktører iværksætter kontinuerligt angreb/skadelig aktivitet.

Et givent trusselsniveau er udtryk for FE's vurdering af aktørers intention, kapacitet og aktivitet på baggrund af de tilgængelige oplysninger.



Andre relevante publikationer

Center for Cybersikkerhed udgiver løbende trusselsvurderinger og vejledninger på cyberområdet. Nedenfor er fremhævet en række af de publikationer, som kan være relevante for myndigheder og virksomheder i vandsektoren i Danmark. Alle publikationer kan tilgås på CFCS' hjemmeside.

Cybertruslen mod Danmark 2024
I denne årlige trusselsvurdering beskriver CFCS den generelle cybertrussel for hhv. cyberkriminalitet, cyberspionage, cyberaktivisme, destruktive cyberangreb og cyberterror mod Danmark.

Cybertruslen mod energisektoren
Trusselsvurderingen "Cybertruslen mod energisektoren" beskriver de forskellige cybertrusler, som den danske energisektor står overfor**.**

Beskyttelse af OT i vandsektoren
"Beskyttelse OT i vandsektoren" er en kort guide til, hvordan vandværker kan komme i gang med at beskytte OT-systemer i vandsektoren. Guiden kommer med anbefalinger til at sikre vandværker mod de mest udnyttede sikkerhedshuller, der bruges til angreb på OT-systemer.

Cyberforsvar der virker
"Cyberforsvar der virker" er Center for Cybersikkerheds grundlæggende vejledning om cyberforsvar og håndtering af cyberangreb.

Vejledning om at imødegå ransomware-angreb
Vejledningen "Reducér risikoen for ransomware" giver en række anbefalinger, som organisationer kan følge for at reducere sandsynligheden for at blive ramt af ransomware-angreb. Vejledningen giver desuden råd til, hvordan et ransomware-angreb kan håndteres, når skaden er sket.

Vejledning om beskyttelse mod DDoS-angreb
Vejledningen "Beskyt mod DDoS-angreb" kommer med en række forholdsregler, som en organisation kan tage for at beskytte sig mod DDoS-angreb.

Vejledning om at imødegå phishing-angreb
Vejledningen "Beskyt din organisation mod phishing-angreb" hjælper organisationer med at imødegå truslen fra phishing-mails.

Vejledning om cybersikkerhed i leverandørforhold
Vejledningen "Cybersikkerhed i leverandørforhold" giver gode råd til, hvordan man kan oprette og bibeholde et godt samarbejde mellem kunden og leverandøren af it-driften, gennem hele samarbejdsperioden. Fra valg af leverandør til ophør af samarbejdet.