Udvalget for Digitalisering og It 2023-24
DIU Alm.del - Bilag 41
Offentligt

CENTER FOR CYBERSIKKERHED

Beretning 2022

FE CENTER FOR CYBERSIKKERHED

Forsvarets Efterretningstjeneste
Center for Cybersikkerhed
Kastellet 30
2100 København Ø

Telefon: 3332 5566
www.cfcs.dk
www.fe-ddis.dk

INDHOLD

FORORD

Den altoverskyggende begivenhed i året 2022 var Ruslands invasion af Ukraine i februar. Med et stod Europa i en ny sikkerhedspolitisk situation, som på cyberområdet udmøntede sig i et trusselsbillede, der udviklede sig både hurtigt og uforudsigeligt.

Fra start var det vores analyse, at Rusland ikke ville anvende destruktive cyberangreb direkte mod NATO-lande. Men der var stadig risiko for, at danske organisationer kunne blive ramt af afledte effekter af destruktive cyberangreb, der blev udført som en del af krigen. Cyberaktivister blev også tidligt en synlig og volatil trussel, som risikerede at forværre konflikten, hvis angrebene fik en ødelæggende eller forstyrrende effekt på kritisk infrastruktur.

På grund af øget aktivitet fra især prorussiske grupper, der i højere grad begyndte at fokusere på mål uden for Ukraine, hævede vi i maj 2022 trusselsniveauet for cyberaktivisme fra LAV til MIDDEL. Efterfølgende har vi hævet niveauet endnu en gang, så det nu - i oktober 2023 - ligger på niveauet HØJ. Det betyder, at det er sandsynligt, at danske organisationer vil blive ramt. Cyberaktivisme er blevet en del af normalbilledet – noget, vi i Center for Cybersikkerhed (CFCS) blandt andre fik at mærke, da aktivister lykkedes med at gøre vores hjemmeside utilgængelig i perioder over to dage i december 2022.

I CFCS gav Ruslands invasion af Ukraine naturligt ekstra travlhed. I den usikre situation måtte vi, i tæt samarbejde med det øvrige FE, hele tiden sammenholde og efterprøve vores analyser af aktørernes intentioner og metoder ekstra nøje. Samtidig var der naturligvis en øget efterspørgsel på vores rådgivning om cyberforsvar og -beredskab fra både myndigheder og virksomheder.

Du kan læse om, hvordan situationen påvirkede hverdagen i CFCS i et af de tre medarbejderportrætter, som vi har lavet til denne beretning. Du kan også læse om vores styrkede samarbejde med Grønland om cybersikkerhed. Det fortæller en af vores sektionschefer om i portrættet "Fra hemmelig til udadvendt". Endelig fortæller en cyberanalytiker i situationscenteret om, hvordan det er at blive ansat i CFCS via vores cyberakademi, som afsluttede sit tredje hold i april 2022.

Sidste år var også året, hvor jeg tiltrådte som chef for CFCS. Det var og er fortsat et privilegie at bruge hver dag på at støtte samfundets sektorer i deres arbejde med at opbygge et stærkt cyberforsvar og robusthed i tilfælde af cyberangreb sammen med de dedikerede medarbejdere i CFCS.

I denne beretning kan du læse mere om, hvordan vi har arbejdet for et sikkert digitalt Danmark i 2022. Vi har lagt vægt på at gå så tæt på vores konkrete opgaver som muligt gennem interviews med tre medarbejdere, der både fortæller om deres opgaver og om, hvordan det er at arbejde i CFCS.

God læselyst.

Thomas Flarup
Chef for Center for Cybersikkerhed

TIDSLINJE 2022

Her har vi udvalgt nogle vigtige cyberbegivenheder i 2022 set fra Center for Cybersikkerhed (CFCS).

JANUAR

13.
CFCS opdaterer vejledning om cybersikkerhed i forbindelse med tjenesterejser.

15.
Destruktivt cyberangreb med wiper-malware mod organisationer i Ukraine.

MARTS

1.
CFCS afholder webinar om cybertruslen mod Danmark i lyset af Ruslands invasion af Ukraine.

15.
CFCS udsender en trusselsvurdering om cybertruslen mod Danmark i lyset af Ruslands invasion af Ukraine.

25.
Selvstyret i Grønland ramt af cyberangreb.

APRIL

1.
Dimission for cyberakademiets tredje hold.

JUNI

2.
CFCS udsender trusselsvurdering for telesektoren.

8.-9.
CFCS deltager for Danmark i øvelsen Cyber Europe, der øver håndtering af cyberhændelser og -beredskab på tværs af de europæiske lande.

28.
CFCS udsender trusselsvurderingen Cybertruslen mod Danmark 2022.

OKTOBER

NATIONAL CYBERSIKKERHEDSMÅNED

4.
CFCS udgiver i samarbejde med en række brancheforeninger en strategi for cyber- og informationssikkerhed på teleområdet.

24.
Digitaliseringsstyrelsen i Grønland og CFCS indgår en samarbejdsaftale om cybersikkerhed.

29.
DSB-tog i hele Danmark holder stille efter et hackerangreb mod et testmiljø hos en underleverandør.

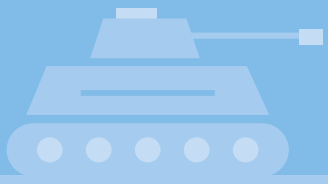
FEBRUAR

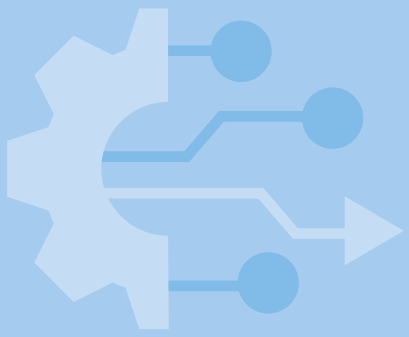
4.
CFCS udgiver liste med tiltag til at styrke organisationers robusthed over for cyberangreb.

17.
CFCS opdaterer vejledning om DMARC.

23.
Destruktivt cyberangreb med wiper-malware mod organisationer i Ukraine.

24.
Ruslands invasion af Ukraine. CFCS opfordrer myndigheder og virksomheder til at styrke cyberberedskabet.





MAJ

6.
CFCS og Digitaliseringsstyrelsen opdaterer vejledning om cybersikkerhed i leverandørforhold.

10.
Danmark vurderer sammen med EU og en række nære allierede, at Rusland stod bag cyberangrebet mod det amerikansk-ejede satellit-firma Viasat.

18.
CFCS hæver trusselsniveauet for cyberaktivisme fra LAV til MIDDEL.

AUGUST

12.
Digitaliseringsstyrelsen, Center for Cybersikkerhed, Statens It og Politiets Efterretningstjeneste udgiver opdaterede tekniske minimumskrav for statslige myndigheder.

SEPTEMBER

16.
Det danske cyberlandshold vinder EM i cyber i Wien.

NOVEMBER

27.
CFCS udsender en trusselsvurdering om cybertruslen mod hjælpemidler til navigation.

DECEMBER

8.-9.
DDoS-angreb mod blandt andet Forsvarsministeriets hjemmesider.

14.
CFCS udsender varsel om DDoS-angreb mod webapplikationer.

EU-Parlamentet og Rådet underskriver aftale om NIS2.

CFCS ARBEJDER FOR ET SIKKERT DIGITALT DANMARK

Center for Cybersikkerhed (CFCS) er nationalt kompetencecenter for cybersikkerhed. Vi vurderer cybertruslen mod Danmark og sikrer løbende et nationalt situationsbillede på cyberområdet.

Med afsæt i vores viden om cyberaktører, deres metoder og intentioner, rådgiver vi myndigheder og virksomheder for at styrke cyberresiliensen i det danske samfund. Cyberresiliens er evnen til at håndtere it-sikkerhedshændelser og stadig videreføre nødvendige samfundsfunktioner.

CFCS støtter samfundets sektorer i deres arbejde med at opbygge et stærkt cyberforsvar og være robuste i tilfælde af cyberangreb. Vores særlige viden, nationale overblik og rådgivning leverer det fundament, som myndigheder og virksomheder kan bygge deres digitale cyberforsvar på.

Cyberresiliens er en af forudsætningerne for at sikre opretholdelse af det danske samfunds vigtige funktioner i hverdagen såvel som under en krise. Det er også en forudsætning for, at myndigheder og virksomheder fortsat kan udnytte mulighederne i den digitale udvikling.

Cybertruslen er høj, og hastigheden, hvormed sårbarheder findes og kan udnyttes, accelererer. Det, vi beskytter, ændrer sig også dynamisk, og angrebsfladen vokser i takt med digitaliseringen og sammensmeltningen af det fysiske og digitale domæne. Dette stiller nye krav til, hvordan vi sikrer vores kritiske infrastruktur.

Derfor er vores vigtigste opgave at drive cyberresiliensen i de funktioner, som det danske samfund er afhængig af, for at bidrage til et sikkert Danmark.

EN DEL AF FORSVARETS EFTERRETNINGSTJENESTE OG MED EN ÅBEN OG UDADVENDT PROFIL

CFCS' placering ved Forsvarets Efterretningstjeneste (FE) giver os adgang til efterretningsmæssige oplysninger om avancerede cyberangreb. Vi drager nytte af de højt specialiserede kompetencer, FE har på cyberområdet. Det betyder, at FE's indsigt i trusselsaktørernes forudsætninger og fremgangsmåde understøtter vores produkter og rådgivning.

Selvom vi ligger i FE, har vi en mere åben og udadvendt profil. Vi udgør én myndighed sammen med FE, men vi har forskellige opgaver og virkemidler.

CENTER FOR CYBERSIKKERHED

GRUNDLAG

Efterretnings-analyse

Monitorering af netværk

PRIMÆRE PRODUKTER

Løbende nationalt situationsbillede

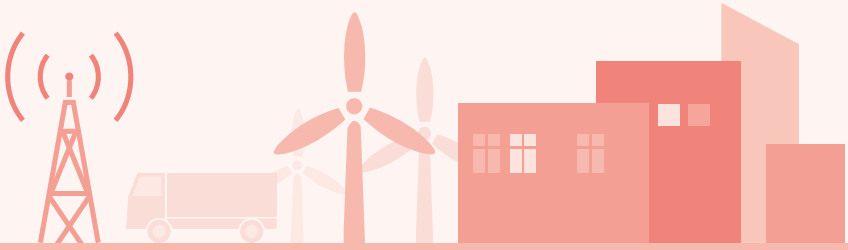
National vurdering af cybertruslen

YDELSER

Varsling og hændelseshåndtering

Rådgivning Og viden

KRITISK INFRASTRUKTUR



SAMFUNDSVIGTIGE SEKTORER OG FUNKTIONER

VIDENSDELING OM ANGREB OG ANGREBSFORSØG

VIDENSDELING OM ANGREB OG ANGREBSFORSØG

CFCS' MYNDIGHEDSOPGAVER

Center for Cybersikkerhed (CFCS) varetager en række myndighedsopgaver. Vi er national it-sikkerhedsmyndighed og nationalt kompetencecenter på cybersikkerhedsområdet. Rollen som national it-sikkerhedsmyndighed indebærer oplysning, vejledning og rådgivning af danske myndigheder og virksomheder i at styrke cybersikkerheden, så risikoen for cyberangreb mindskes, og så eventuelle cyberangreb håndteres på den mest hensigtsmæssige måde.

CFCS er desuden myndighed for informationssikkerhed og beredskab på teleområdet. Det betyder, at centeret stiller informationssikkerhedskrav til teleudbydere og fører tilsyn på området.

CFCS varetager også funktionen som nationalt centralt kontaktpunkt og beredskabsenhed, der håndterer it-sikkerhedshændelser (CSIRT).

CFCS samarbejder med øvrige nationale sikkerhedsmyndigheder om blandt andet beredskabsøvelser på cyberområdet og vejleder om beredskabsplanlægning og krisestyring på tværs af rigsfællesskabet.

CENTER FOR CYBERSIKKERHED

- har fokus på at fremme og sikre cyberresiliens i den kritiske infrastruktur i Danmark og rigsfællesskabet
- udnytter vores position som efterretningsbaseret enhed med særlige beføjelser til at styrke Danmark som et sikkert digitalt samfund
- samarbejder tæt med den private sektor for at løfte cyberresiliensen bredt

HÅNDTERING AF SIKKERHEDSHÆNDELSER

Danmark rammes hvert år af mange tusinde cyberangreb. Tallene for sikkerhedshændelser i denne beretning er alene udtryk for antallet af hændelser, som Center for Cybersikkerhed (CFCS) har håndteret i 2022. Det vil sige hændelser, der er identificeret ved hjælp af sensornetværket, indberetninger, direkte henvendelser, tip fra partnere og ved hjælp af Forsvarets Efterretningstjenestes (FE) efterretningsmæssige virke. Vi vurderer, at der eksisterer et stort mørketal for cyberangreb i Danmark, da ikke alle hændelser indberettes til CFCS.

Centeret har i 2022 håndteret 356 hændelser, der har haft effekt på den berørte organisation. Som det ses på næste side, har hændelserne forskellige grader af alvorlighed. Tallet var i 2021 379 hændelser. Ud over de 356 hændelser, der har haft effekt på den berørte organisation, har CFCS observeret et stort antal rekognosceringer, hvor en ondsindet aktør undersøger muligheden for at udnytte eksempelvis kendte sårbarheder og åbne porte. Rekognoscering har ikke effekt på den berørte organisation, men kan udstyre aktøren med viden, der kan udnyttes til et senere angreb. For at kunne konstatere hvorvidt et angreb har haft effekt, analyserer CFCS også disse forsøg.

Størstedelen af de hændelser, CFCS håndterer, er baseret på alarmer fra CFCS' sensornetværket. Når en alarm går, ser en netværksanalytiker på hændelsen med henblik på at vurdere, om der er tale om et cyberangreb.

DEFINITION AF EN SIKKERHEDSHÆNDELSE

En hændelse, der negativt påvirker eller vurderes at ville kunne påvirke tilgængeligheden, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale tjenester.

Kilde: Lov om Center for Cybersikkerhed

ALVORLIGHEDSGRAD AF HÆNDELSER

MINDRE
Reelt angrebsforsøg, som ikke medfører kompromittering. Når et angreb ikke medfører kompromittering, skyldes det i høj grad, at det stoppes af sikkerhedsforanstaltninger som for eksempel firewalls, spamfiltre og antivirusløsninger. Et mindre cyberangreb kan både være dyrt og besværligt, idet organisationen ofte skal bruge tid på at undersøge, hvad der er sket og gennemgå eksisterende sikkerhedsforanstaltninger.

MODERAT
Ingen kritiske systemer berørt, ingen system- eller administratorkonti kompromitteret. Begrænset betydning for den berørte organisation. Der er typisk tale om enkeltstående klientkompromitteringer (for eksempel pc eller server), hvor klienten har ingen eller begrænsede administratorrettigheder.

STØRRE
Kritiske systemer berørt eller system- eller administratorkonti kompromitteret. Hændelsen har mærkbar betydning for den berørte organisation. Det vil sige, at aktøren har fået adgang til at læse og kopiere sensitiv information og mulighed for at ændre eller slette information. Det kan for eksempel være ransomware-angreb, der rammer større dele af en organisations it-systemer, eller angreb hvor aktøren har haft fodfæste på organisationens netværk gennem længere tid.

ALVORLIG
Kritiske systemer berørt eller system- eller administratorkonti kompromitteret. Hændelsen har alvorlig betydning for den berørte organisation samtidig med, at CFCS vurderer, at hændelsen har betydning for sikkerheden i den digitale infrastruktur, som samfundsvigtige funktioner er afhængige af.

3
Alvorlig

2
Større

23
Moderat

328
Mindre

ANGREBSVEJE

Monitorering af datatrafikken i sensornetværket viser en lang række forskellige angrebsveje. Med angrebsveje menes den måde, hvorpå en angrebsaktør forsøger at få adgang til at udføre sit angreb. Diagrammet viser fordelingen af de identificerede angrebsveje i 2022. Diagrammet siger ikke noget om, hvilken indvirkning hændelsen har haft på den ramte organisation.

PHISHING
Phishing er et forsøg på at narre modtagere af beskeder som for eksempel mails til at videregive personlige eller andre beskyttelsesværdige oplysninger eller give uretmæssig adgang til blandt andet it-systemer. Ofte vil angriberen ved hjælp af simpel social engineering forsøge at få ofrene til at klikke på links til falske hjemmesider eller åbne inficerede filer.

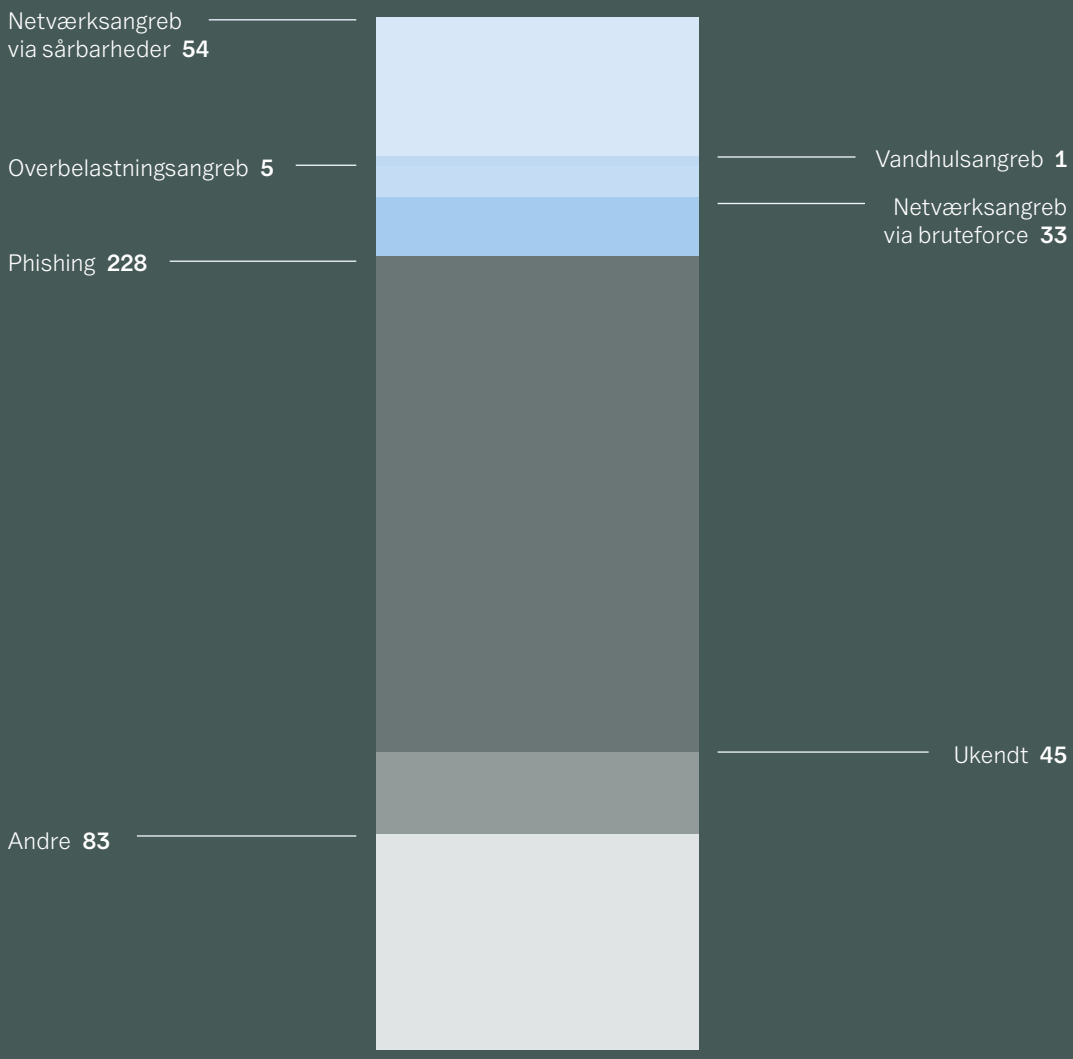
NETVÆRKSANGREB
Netværksangreb dækker over angrebstyper, som søger at få adgang til ofrets it-systemer via angreb på eksponerede systemelementer over internettet. Det dækker blandt andet over forsøg på at udnytte sårbarheder og fejlkonfiguration af softwaren.

BRUTE FORCE-ANGREB
Brute force-angreb er et angreb, hvor hackeren forsøger at gætte et password ved at kombinere alle mulige bogstaver, tal og tegn, der kan indgå i et password.

OVERBELASTNINGSANGREB
Overbelastningsangreb er også kendt som DDoS, der står for Distributed Denial of Service. Hackere forsøger at generere usædvanligt store mængder datatrafik mod en hjemmeside (webserver) eller et netværk, så hjemmesiden eller netværket ikke er tilgængelig for legitim trafik, mens angrebet står på.

VANDHULSANGREB
Vandhulsangreb dækker over en angrebsteknik, hvor en ellers legitim hjemmeside, for eksempel en webshop, inficeres med malware. Brugere, der normalt benytter hjemmesiden uden problemer, risikerer at blive inficeret med malware. Ved et vandhulsangreb er hjemmesiden udvalgt for at ramme en specifik målgruppe, som benytter den regelmæssigt.

Find flere ordforklaringer på www.cfcs.dk.



Note: Diagrammet viser de angrebsveje, det har været muligt at identificere ud fra CFCS' registrering. Kategorien "Ukendt" dækker over hændelser, hvor det ikke har været muligt at identificere angrebsvejen. Tallene i diagrammet dækker også sager, hvor CFCS har vurderet, at de ikke har haft effekt på den berørte organisation.

DA ALLE VILLE VIDE, OM INVASIONEN ÆNDREDE PÅ CYBERTRUSLEN

Allerede i ugerne op til Ruslands invasion af Ukraine var der travlhed hos analytikerne i Center for Cybersikkerhed (CFCS). Ruslands cyberkapaciteter er velkendte og truslen om hybrid krigsførelse lurede. Fra flere sider blev spørgsmålet rejst, om eventuel brug af destruktive cyberangreb mod Ukraine kunne få konsekvenser i Danmark.

Enheden for trusselsvurderinger i CFCS følger cybertruslens udvikling tæt, men den russiske opmarch af tropper nær grænsen til Ukraine og de internationale sikkerhedspolitiske spændinger i februar 2022 markerede en ny situation.

"Vi var nødt til at stoppe op og vurdere, hvad det betød for truslen. Situationen var på det tidspunkt uvis, så vi måtte kigge på vores analyser igen og se, om en eventuel konflikt kunne betyde noget for Danmark," fortæller Julie, som er én af de analytikere, der skulle forsøge at svare på de svære spørgsmål om en situation, der hurtigt kunne ændre sig.

En invasion kunne potentielt blive understøttet med destruktive cyberangreb. Det store spørgsmål var derfor, om effekten af sådanne angreb kunne få konsekvenser i andre lande. Da Rusland invaderede Ukraine den 24. februar 2022, skete det samtidig med et destruktivt cyberangreb mod udstyr fra den amerikanske udbyder af satellitkommunikation, Viasat. I maj 2022 vurderede Danmark sammen med EU og en række nære allierede, at Rusland stod bag angrebet vel vidende, at angrebet også ville have destruktive konsekvenser uden for Ukraine. Angrebet ramte blandt andet tusindvis af vindturbiner i Centraleuropa. Angrebet havde ikke umiddelbart konsekvenser i Danmark, men var i dagene efter invasionen med til at skabe stor usikkerhed om cybertruslen.

"Efter invasionen oplevede vi stor efterspørgsel fra både myndigheder og virksomheder, som ville vide, hvordan de skulle forholde sig. Så kort efter invasionen lavede vi en trusselsvurdering om cybertruslen mod Danmark i lyset af Ruslands invasion af Ukraine for at hjælpe med at forstå situationen," forklarer Julie.

Uvisheden om krigen og brugen af destruktive cyberangreb førte også til spørgsmål fra pressen og offentligheden.

"Vi fik rigtig mange spørgsmål til truslen fra destruktive cyberangreb, som vi skulle svare på og samtidig sikre os, at vores svar afspejlede vores aktuelle vurdering. Det handlede for os om at være tro mod vores analyse. Når der sker så store ting som invasionen af Ukraine, kommer man let til at spekulere i ragnarokscenarier. Der handler det om ikke at gå i panik," fortæller Julie.

Hold øje med nye jobopslag på **www.cfcs.dk** og på vores LinkedIn profiler.

For at beskytte vores medarbejdere, optræder de her under et alias.

Få uger efter invasionen var det en anden side af cybertruslen, som krævede opmærksomhed. Forskellige aktivistiske grupper med uklare tilhørsforhold blandede sig på begge sider af konflikten med forstyrrende cyberangreb.

"Aktivisme begyndte at fylde mere allerede inden invasionen. Efter invasionen skete der flere cyberaktivistiske angreb rundt om i Europa. Så vi hævede trusselsniveauet fra LAV til MIDDEL lige inden vi udgav vores store trusselsvurdering om cybertruslen mod Danmark," fortæller Julie.

Flere danske hjemmesider blev i 2022 ramt af DDoS-angreb, hvor aktivistiske grupper har taget ansvaret og angivet Danmarks støtte til Ukraine som motiv.

For Julie og de andre analytikere var det nyt, at cybertruslen ændrede sig så hurtigt som følge af den sikkerhedspolitiske udvikling snarere end på grund af ny teknologi eller nye muligheder for eksempelvis cyberkriminelle.

"I den tid, jeg har været i CFCS, har trusselsbilledet mest ændret sig, når for eksempel de kriminelle har taget nye metoder i brug. Så det har mest været i detaljerne, at truslen har ændret sig. Det her var første gang, at der er kommet en stor begivenhed udefra, som har ændret trusselsbilledet," forklarer Julie.

Analysen af cybertruslen mod Danmark som følge af krigen i Ukraine var ikke alene et spørgsmål om at se isoleret på cyberelementet. En væsentlig del af CFCS' vurdering bygger på en analyse af aktørernes motivation. I dette tilfælde hvorvidt Rusland havde intention om at udføre cyberangreb mod Danmark eller andre NATO-lande.

"Vi havde et endnu mere intensivt samarbejde på tværs af Forsvarets Efterretningstjeneste end normalt. Vi skulle forstå, hvad det betød, at vi stod med en ny situation. Så vi kiggede metodisk hele vores analyse igennem, også med de sikkerhedspolitiske briller," forklarer Julie.

Vurderingen blev hurtigt, at Rusland ikke havde interesse i at optrappe en konflikt med NATO ved bevidst at udføre destruktive cyberangreb mod alliancens medlemmer. Dog med det forbehold, at situationen kunne ændre sig.

Samtidig understregede CFCS, at trusselsniveauet fortsat var MEGET HØJT for cyberspionage og cyberkriminalitet, og at cyberspionage kan være en forudsætning eller forberedelse til på et senere tidspunkt at kunne udføre destruktive cyberangreb. Den væsentligste ændring blev dog, at trusselsniveauet for cyberaktivisme først blev hævet fra LAV til MIDDEL og derefter til HØJ som følge af flere målrettede angreb mod danske interesser. Selvom situationen i Ukraine fortsat spiller en betydelig rolle, så indgår det nu mere som endnu en faktor i vurderingen af trusselsbilledet end som en akut forandring, sådan som det så ud i tiden lige omkring Ruslands invasion.

"Vi følger løbende truslen mod blandt andet forskellige sektorer. På en måde er situationen i Ukraine blevet endnu ét af vores faste fokuspunkter. Det har ikke betydet, at vi har skullet ændre vores grundlæggende arbejdsmetoder, men vi har kunnet holde fast i vores gode processer, som vi allerede havde før invasionen," forklarer Julie.

HVEM ER JULIE?

Julie er analytiker i enheden for trusselsvurderinger, som er en del af cyberanalysen i CFCS. Hendes opgaver består i at følge, analysere og beskrive cybertruslen mod Danmark og konkret i at skrive trusselsvurderinger, der kan læses på CFCS' hjemmeside. Julie har især fokus på at følge truslen fra cyberspionage og destruktive cyberangreb, og arbejder tæt sammen med kollegaer, der har et særligt fokus på cybertruslen mod kritiske sektorer.

Julie har en samfundsvidenskabelig uddannelsesbaggrund og været ansat i CFCS i en årrække.

Vi havde et endnu mere intensivt samarbejde på tværs af FE end normalt. Vi skulle forstå, hvad det betød, at vi stod med en ny situation. Så vi kiggede metodisk hele vores analyse igennem, og også med de sikkerhedspolitiske briller

Hold øje med nye jobopslag på **www.cfcs.dk** og på vores LinkedIn profiler.

For at beskytte vores medarbejdere, optræder de her under et alias.

EN NY VEJ IND I CYBERSIKKERHED

Det er ingen hemmelighed, at der i hele Danmark er et stort behov for at skaffe kvalificerede medarbejdere til at arbejde med cybersikkerhed. For at kunne løse opgaven med et døgnbemandet situationscenter, oprettede Center for Cybersikkerhed (CFCS) i 2019 et tre måneders uddannelsesforløb kaldet cyberakademiet. Tanken var, at man kunne rekruttere og oplære de specialister, der skulle indgå i vagtholdsordningen, hvor de i en form for mesterlære kunne få praktisk erfaring og lære fra hinanden og de øvrige mere erfarne kolleger i CFCS. Siden 2019 har CFCS flere gange afholdt uddannelsesforløbet for at sikre bemanding til situationscenteret. Mange af dem, der gennemfører akademiet og får job i CFCS' situationscenter, vælger nemlig efter mesterlæren at specialisere sig yderligere, for eksempel ved at tage en længere videregående uddannelse eller ved at arbejde med cybersikkerhed andre steder i CFCS eller på en ny arbejdsplads.

"Jeg var halvt færdig med en it-uddannelse på et erhvervsakademi, da jeg kom ind. Så ja, jeg har en ufærdig uddannelse, men til gengæld er der rig mulighed for at videreuddanne mig herinde, så det ser jeg ikke som et problem," siger Magnus, som er én af dem, der har gennemgået forløbet på cyberakademiet og nu arbejder i CFCS.

Uddannelsen skal ganske vist først og fremmest klæde kandidaterne på til opgaverne i situationscenteret. Men fordi situationscenteret er et centralt kontaktpunkt for den omverden, CFCS hjælper med at beskytte, så kræver det også en bred grundlæggende viden om cybersikkerhed, netværk og programmering. Nogle af kandidaterne har i forvejen en vis viden om ét område, og en del af rekrutteringsforløbet er at sikre, at det er realistisk inden for tre måneder at opnå de rette faglige kompetencer på de øvrige områder. Derfor skal ansøgerne gennem flere forskellige test, inden de bliver udvalgt. På den måde

udvælges de kandidater, som har det største potentiale til at nå i mål, selvom indlæringskurven kan være stejl, når forløbet er så kort og intensivt.

"Hvis man er kommet ind og gennemfører cyberakademiet, så er der ikke nogen spørgsmålstegn ved, om man er god nok. Det skal man ikke være i tvivl om," siger Magnus.

Gode samarbejdsevner er lige så vigtige som de faglige kompetencer. Derfor er personlighedstest også en del af udvælgelsesforløbet, og undervejs i uddannelsen bliver der arbejdet med det psykologiske og evnen til at handle kompetent i bestemte situationer og miljøer. Målet er at udvikle kandidaterne til både at blive ideelle holdspillere samtidig med, at de skal være faglige eksperter.

"Vi har mange forskellige profiler og baggrunde, så vi er nok ikke så ensartet en gruppe, som man måske kunne tro til et så specialiseret arbejde. Det er kun en fordel, fordi ingen af os har alle kompetencerne, men til gengæld kan vi støtte hinanden og bruge de styrker og den ekspertise, vi hver især kommer med," forklarer Magnus.

På ét punkt er der dog en fællesnævner for profilerne til cyberakademiet. De er alle unge mennesker, som ikke har påbegyndt eller afsluttet en længere uddannelse inden for it. Det er netop én af pointerne ved uddannelsesforløbet. Udover at skaffe kvalificerede medarbejdere til CFCS' situationscenter, så åbner det også en ny indgang for dem, der har mere vilje og motivation end gennemsnittet til at dygtiggøre sig inden for cybersikkerhed, og som gerne vil lære faget ved at arbejde med det i praksis.

"Det her kan være en ny vej ind for nogle nye typer profiler. Undervisningen foregår mere i klasseform i stedet for forelæsninger, så det er helt naturligt at samarbejde om opgaverne. Vi bliver undervist af nogle virkelig dygtige folk på hver deres område, så det teoretiske bliver altid knyttet til noget praktisk, fordi det er folk, som for eksempel har 15-20 års erfaring med at sætte meget store netværk op," siger Magnus.

ET NYT HOLD KANDIDATER FRA CYBERAKADEMIET BLEV FEJRET 1. APRIL 2022

Det tredje hold fra Center for Cybersikkerheds cyberakademi blev færdiguddannet i 2022 og det blev fejret med dimission på Kastellet den 1. april med tale af daværende forsvarsminister, Morten Bødskov: "I bliver første led i håndteringen af konkrete cyberangreb. I skal opdage, for at myndigheder, virksomheder og borgere kan reagere. Det kræver store evner og specialiseret indsigt. Et stort ansvar hviler på jeres skuldre. Jeg ved, at uddannelsen på cyberakademiet har klædt jer godt på – både fagligt og personligt – til at varetage den vigtige opgave. I er en vigtig ressource, og det hårde arbejde er kun lige begyndt", sagde ministeren til den festlige begivenhed.

Den følgende mandag startede de nyudklækkede junioranalytikere i situationscenteret, hvor de bidrager til den døgnbemandede monitorering af netværkstrafikken i de samfundskritiske sektorer. Formålet med monitoreringen er at opdage og varsle om mulige cyberangreb mod Danmark. Cybersituationscenteret har også til opgave at fungere som nationalt kontaktpunkt i forhold til cyberhændelser.

Alle de kandidater, som gennemfører cyberakademiet med et tilfredsstillende resultat, bliver tilbudt fastansættelse som analytikere i CFCS' situationscenter. Det betyder også, at den teoretiske grundforståelse, de har fået gennem uddannelsesforløbet, hurtigt bliver omsat til praksis. Det er dog ikke ensbetydende med, at uddannelsen kun fører til en plads på et af vagtholdene i situationscenteret. Netop fordi der er stor efterspørgsel efter talenter inden for cybersikkerhed, så er cyberakademiet også en måde for CFCS at opfostre og udvikle egne kandidater.

> Vi har mange forskellige profiler og baggrunde, så vi er nok ikke så ensartet en gruppe, som man måske kunne tro til et så specialiseret arbejde. Det er kun en fordel, fordi ingen af os har alle kompetencerne, men til gengæld kan vi støtte hinanden og bruge de styrker og den ekspertise, vi hver især kommer med

Når kandidaterne er startet i CFCS efter cyberakademiet, er der mulighed for at videreuddanne sig. Nogle vælger at følge et praktisk spor med tekniske certificeringer eller enkeltkurser inden for cybersikkerhed. Andre vælger at begynde på en deltidsuddannelse sideløbende med fuldtidsarbejdet i CFCS. Og atter andre vælger at søge ind på en videregående it- eller naturvidenskabelig kandidatuddannelse og bliver tilbudt at fortsætte i CFCS i et studiejob på deltid.

Cyberakademiet er tænkt som et målrettet introduktionsforløb til blandt andet at arbejde med at håndtere alarmer fra CFCS' sensornetværk og varsle offentlige myndigheder og virksomheder, der håndterer kritisk it-infrastruktur om cyberhændelser. Men arbejdet giver også god praktisk erfaring, som er relevant andre steder i CFCS. Derfor er der flere af dem, der starter i wet, som efter mesterlæren siden skifter til andre funktioner af CFCS.

"Muligheden for at udvikle sig fagligt er noget, der blev lagt vægt på helt fra start. Vores arbejdsgiver er jo klar over, at vi er nogle unge mennesker, der ikke har færdiggjort kandidatuddannelser. Jeg har allerede skiftet job internt en gang. Jeg startede som analytiker og søgte derefter en stilling som operativ koordinator og teamleder. Men udover det er der også kurser inden for det faglige. Det kunne for eksempel være SANS-kurser, præsentationsteknik eller håndtering af stressede situationer. Det handler om at opbygge en kompetenceprofil, så man bliver en robust medarbejder inden for det her fag," siger Magnus.

Fra at være et enkeltstående forløb for at rekruttere til opstarten af situationscenteret er cyberakademiet nu et tilbagevendende initiativ, fordi erfaringerne med den skræddersyede uddannelse har været særdeles positive. Både i forhold til at supplere med nye folk til CFCS, men også i forhold til at åbne en ny vej til at arbejde praktisk med cybersikkerhed for nogle af de talenter, som har evnerne til at lære og viljen til at yde en ekstra indsats, men ikke har cyber stående på eksamensbeviset.

ARBEJDSOMRÅDER I CENTER FOR CYBERSIKKERHED

Center for Cybersikkerheds (CFCS) opgave er at støtte samfundets sektorer i deres arbejde med at opbygge robusthed i tilfælde af cyberangreb. Her kan du se nogle af de områder, vi arbejder med i CFCS.

ANALYSE

Analytikere i CFCS er med til at opdage og afdække cybertruslen mod Danmark. Analytikerne samarbejder ofte tæt med FE's organisation, og trækker på mange ressourcer og datakilder – åbne som lukkede – for at styrke centerets viden om trusselsaktørernes teknikker, metoder og kampagner.
Analytikerne indsamler, analyserer og formidler viden som blandt andet varsler og trusselsvurderinger med henblik på at styrke danske myndigheder og virksomheders evne til at beskytte sig selv – og dermed Danmark. Analytikere i CFCS har ofte en teknisk, humanistisk eller samfundsvidenskabelig baggrund, men det vigtigste fællestræk er et stærkt analytisk mindset.

RÅDGIVNING

Rådgivere vejleder og informerer om forebyggende cybersikkerhed til både den offentlige og den private sektor. Rådgiverne har viden om sikkerhedsarkitektur, it-sikkerhedsgovernance, design og implementering af sikkerhedsprocesser, anvendelse af standarder, risikostyring m.v. Rådgiverne bevæger sig overvejende i den åbne del af CFCS og har en udadvendt funktion, men de trækker også på den viden, der bliver genereret i den lukkede cyberanalyse. Rådgiverne har ud over viden om informationssikkerhed også solid viden om organisation og proces.

FORENSICS

Inden for netværkssikkerhed arbejder vi med at analysere netværkstrafik og aflæse de signaturer, som cyberangreb efterlader, herunder blandt andet forensics og malwareanalyse. Forensics-eksperter er specialister i hackernes angrebsmetoder. Ud fra systemdata og logfiler omsætter forensics-eksperterne de digitale spor til en rekonstruktion af, hvordan et cyberangreb har fundet sted. Malwareanalytikerne er trænede i at isolere og studere et angrebs enkeltkomponenter. Ved hjælp af reverse-engineering kan de genskabe de angrebsveje, der er brugt i cyberangreb.

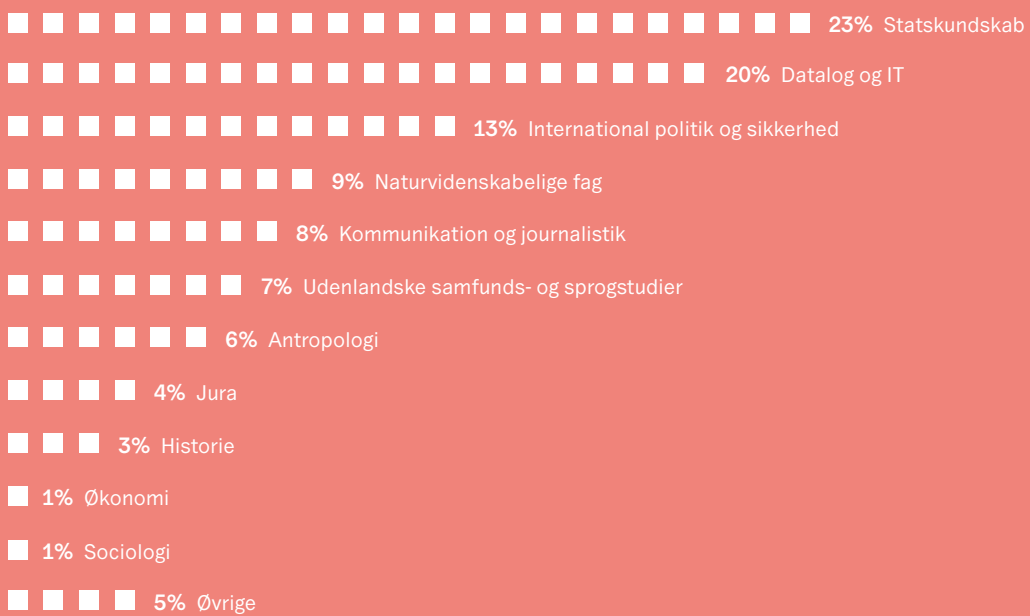
TVÆRGÅENDE FUNKTIONER

Vores opgaver kræver høj grad af samarbejde, både internt i CFCS og Forsvarets Efterretningstjeneste samt med eksterne samarbejdspartnere. De tværgående funktioner bidrager til opgaveløsningen på tværs af centeret – både politisk og med understøttelse af vores operative mission. De tværgående funktioner har forskellige kompetencer og arbejder for eksempel med forretnings- og organisationsudvikling, policy, kommunikation, ledelsesstøtte og andre administrative funktioner.

MEDARBEJDERFORDELING

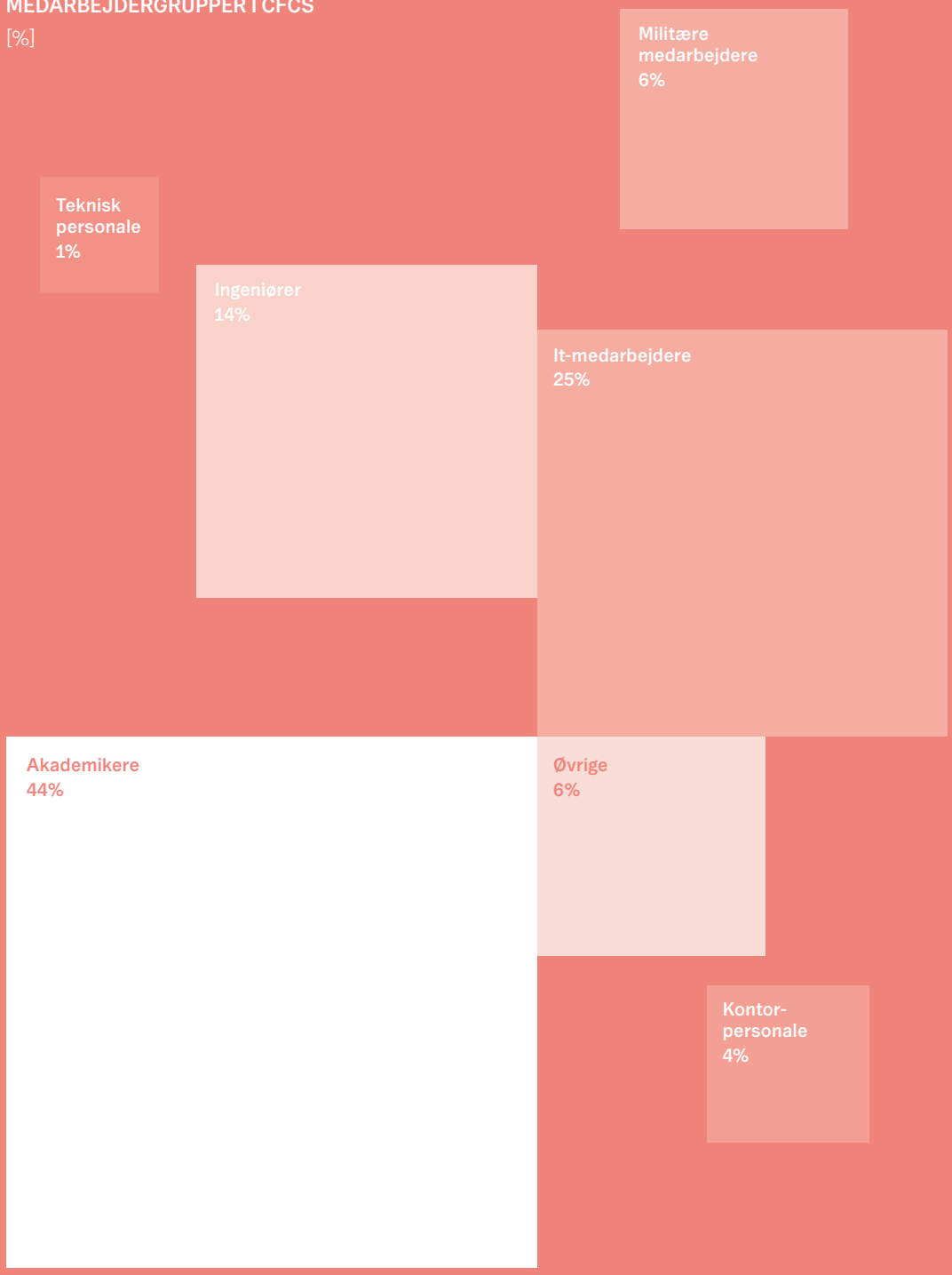
Center for Cybersikkerhed (CFCS) er en del af Forsvarets Efterretningstjeneste (FE). Men selvom vi arbejder med hemmelige opgaver, er vi også helt almindelige mennesker, der har taget en kort, mellemlang eller lang uddannelse eller er autodidakte inden for vores felt.

CFCS'S CIVILE AKADEMIKERE
[%]



MEDARBEJDERGRUPPER I CFCS

[%]



FRA HEMMELIG TIL UDADVENDT

"CFCS er et sted, hvor du kan få lov til at være nørd og blive specialist på et utrolig snævert område. Det er fedt i en verden, der er præget af generalister og bred viden," fortæller Marie. Hendes karriere i Forsvarets Efterretningstjeneste (FE) har været en rejse fra de mest hemmelige og lukkede dele af FE til det udadvendte Center for Cybersikkerhed (CFCS).

Som sektionschef sidder hun i dag med ansvar for to områder, hvor CFCS' rolle og opgaver er i hastig udvikling i disse år. Nemlig beredskab og kritisk infrastruktur på den ene side og rådgivning af Grønland og Færøerne om cybersikkerhed på den anden. CFCS har styrket sit fokus på samarbejdet med de nordatlantiske dele af rigsfællesskabet for at hjælpe med at styrke cybersikkerheden i en region, som mærker en betydelig interesse fra flere af de store geopolitiske aktører.

Marie startede sin karriere i FE som skrivende teknisk analytiker. Hun har en uddannelse i statskundskab og litteratur, og den tekniske viden har hun bygget på hen ad vejen. Hun oplever, at det er vigtigere at have den rigtige analytiske tankegang end at have den specialiserede viden på forhånd, for den kan være svær at få andre steder.

"Hvis du har et analytisk mindset, så kan du lære det tekniske. Jeg har taget kurser for at tilegne mig ekstra viden," forklarer Marie.

Efter nogle år som projektleder i FE, hvor hun arbejdede med at få de forskellige kapaciteter i FE til at spille sammen inden for cyberanalyse, skiftede Marie til et job som sektionschef i den teknisk operative del af CFCS.

"Jeg kom til CFCS med et blik for, hvad man kunne gøre for at arbejde efterretningsmæssigt. Men for mig personligt var det største skift, at jeg gik fra at være skrivende til at være udførende," siger Marie.

Erfaringerne med efterretningsarbejdet og med at lede tekniske specialister var en nyttig baggrund for Marie som sektionschef i CFCS'

Hold øje med nye jobopslag på **www.cfcs.dk** og på vores LinkedIn profiler.

For at beskytte vores medarbejdere, optræder de her under et alias.

netsikkerhedstjeneste, som undersøger de mest alvorlige it-sikkerhedshændelser mod statslige myndigheder og kritisk it-infrastruktur i Danmark. Ligesom hovedparten af FE's arbejde er netsikkerhedstjenestens operative opgaver for en stor del hemmeligholdt. Det er nødvendigt, fordi det dels kan involvere sårbar infrastruktur, og dels kan handle om fremmede stater, der forsøger at spionere mod danske interesser.

Den del af CFCS' arbejde repræsenterer dog kun den ene side af centerets mission. For nylig er Marie skiftet til at arbejde med rådgivningsdelen, hvor større åbenhed er en nødvendighed.

"Efter fire år skiftede jeg til en ny afdeling, hvor det ikke er den defensive eller reaktive indsats, der er i centrum. Derimod er det en afdeling, som arbejder med forebyggelse og resiliens," fortæller Marie om sin nye afdeling, hvor hun er chef for den sektion, som står for kortlægning af kritisk infrastruktur, beredskab på cyberområdet og rådgivning af Grønland og Færøerne.

Selvom Marie i sin nye rolle skal samarbejde mere åbent med andre myndigheder i hele rigsfællesskabet og med private virksomheder, så kan hun i høj grad videreføre sin erfaring fra sine tidligere opgaver i FE og CFCS. Fællesnævneren – og guleroden – for Marie er muligheden for at lede og rekruttere de specialister, der er nødvendige for at løse de særlige opgaver, som CFCS har.

CFCS er et sted, hvor du kan få lov til at være nørd og blive specialist på et utrolig snævert område. Det er fedt i en verden, der er præget af generalister og bred viden

"Jeg har god viden om trusselsaktørerne, og den måde de arbejder på. Det er nyttigt, når man skal rådgive om cybersikkerhed. Samtidig har jeg gerne villet beholde den forankring, jeg tidligere har haft med at lede et hold af eksperter. Nu er det så eksperter i beredskab og it-sikkerhed, men det er stadig en specialistafdeling," siger Marie.

Hun påpeger samtidig, at de erfaringer, hun har med, fra både de lukkede og åbne dele af FE og CFCS, er med til gøre hende til en stærkere leder i dag.

"I de forskellige afdelinger, jeg har været ansat i, har jeg opbygget en forståelse for de interesser og den viden, som folk har. Det bliver man en bedre leder af at forstå og kunne tale ind i," siger hun.

Den røde tråd i hendes karriere i FE er arbejdet med at få funktioner på tværs af organisationen til at spille sammen, kombineret med arbejdet med ledelse og rekruttering af specialister. Muligheden for at kunne skifte mellem meget forskellige opgaver inden for samme organisation er ifølge Marie noget helt særligt ved at arbejde i FE og CFCS.

"Det er fedt, at man kan udvikle sig som leder blot ved at skifte afdeling. Det er unikt at være ansat i en organisation, hvor det næsten kan være som at skifte arbejdsplads, når man skifter på den måde," siger hun.

Selvom opgaverne og åbenheden kan være vidt forskellig på tværs af organisationen, hæfter hun sig også ved, at den overordnede mission er den samme, og at den er nærværende for alle niveauer af medarbejdere i organisationen. Det oplever hun også som en særlig kvalitet i forhold til mange andre arbejdspladser.

"Her handler det altid om kvaliteten af det produkt, vi leverer. Vores "end goal" er hverken bundlinje eller profit, men Danmarks sikkerhed," siger Marie.

CFCS OG GRØNLANDS DIGITALISERINGSSTYRELSE INDGIK SAMARBEJDSAFTALE OM CYBERSIKKERHED

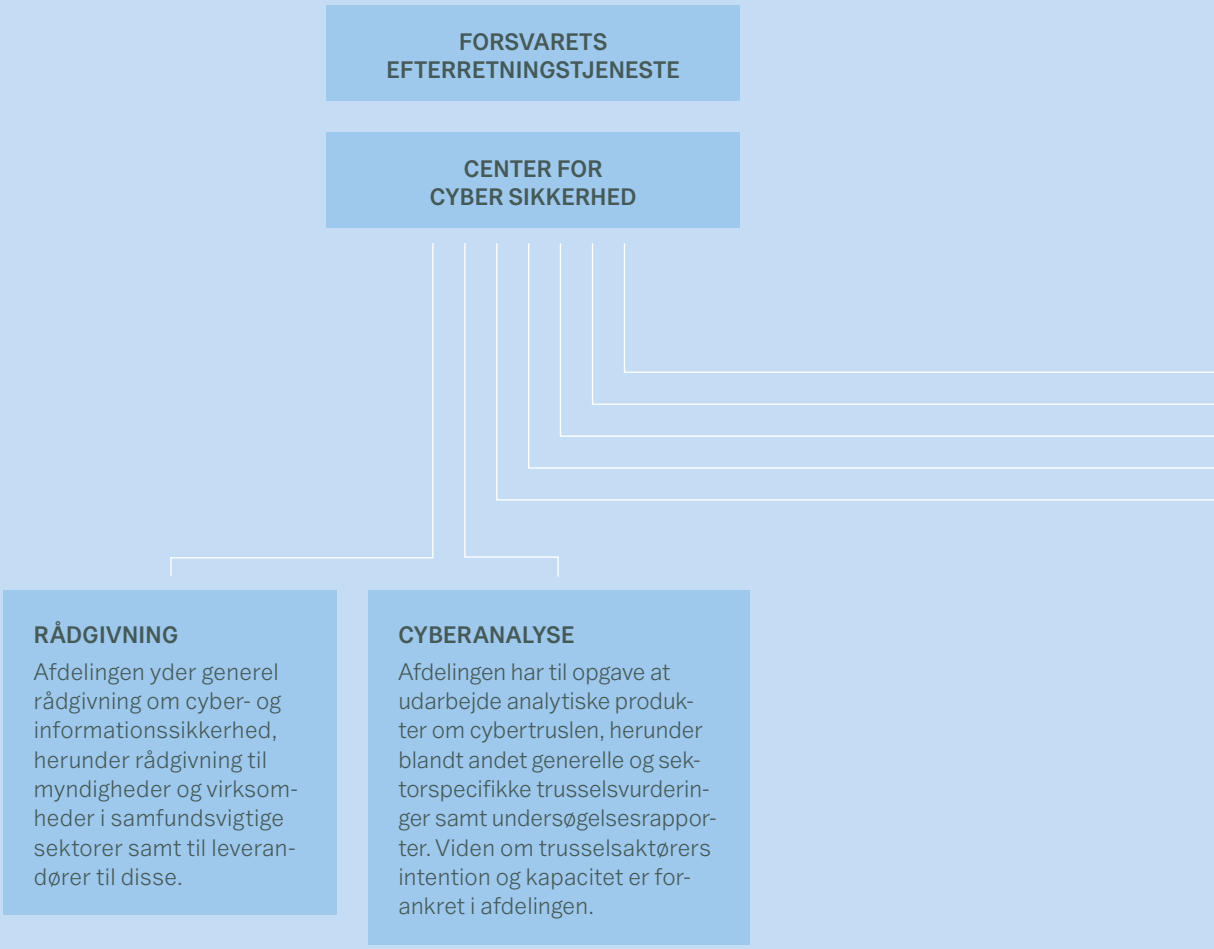
I oktober 2022 indgik CFCS og Grønlands Digitaliseringsstyrelse, som er ressortmyndighed for cyber- og informationssikkerhed i Grønland, en samarbejdsaftale som beskriver, hvordan og på hvilke områder de to parter vil samarbejde om at styrke cybersikkerheden i Grønland. Aftalen var afstedkommet af en tidligere fælles erklæring fra Grønlands Naalakkersuisut og den danske regering om at styrke samarbejdet om cyber- og informationssikkerhed mellem grønlandske og danske myndigheder med henblik på at øge det grønlandske samfunds robusthed over for cybertrusler.

Om samarbejdsaftalen sagde formand for Naalakkersuisut, Múte B. Egede: "I de seneste par år har Grønland oplevet en stigning i cyberangreb imod både offentlige myndigheder og private virksomheder. Det er tydeligt, at det trusselsbillede, som tegner sig internationalt, også gælder for Grønland. Derfor er det vigtigt, at Grønland kan trække på højt kvalificeret rådgivning og samtidig har et fokus på opbygning af kompetencer i Grønland inden for cyber- og informationssikkerhed. Det sikres blandt andet i vores samarbejdsaftale med Center for Cybersikkerhed."

Samarbejdsaftalen fastslår blandt andet, at CFCS og Grønlands Digitaliseringsstyrelse skal mødes løbende for at udveksle viden og erfaringer. Som en del af aftalen vil myndighederne derudover samarbejde om kompetenceudvikling og beskyttelse af kritisk infrastruktur, ligesom CFCS forpligter sig til løbende at afholde briefinger om cybertruslen for relevante myndigheder i Grønland og at styrke rådgivningsindsatsen rettet mod Grønland.

ORGANISATIONSDIAGRAM

Center for Cybersikkerhed (CFCS) er en del af Forsvarets Efterretningstjeneste (FE) og består af syv afdelinger som vist på dette organisationsdiagram.



CYBEROPERATIONER

Afdelingen for cyberoperationer har til opgave at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos statslige myndigheder, Forsvaret og private virksomheder, der varetager samfundsvigtige funktioner. Indsatsen fokuserer på de mest avancerede angreb, der oftest udføres af statsstøttede aktører, eller cyberangreb, der i øvrigt kan påvirke det danske samfund i væsentlig grad.

SITUATIONSCENTER

Afdelingen har til opgave at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos de statslige myndigheder og virksomheder, der er tilsluttet CFCS' netsikkerhedstjeneste. Afdelingen er desuden centralt operativt kontaktpunkt i forhold til myndigheder og virksomheder i samfundsvigtige funktioner, herunder i forhold til EU og NATO.

FORSVAR OG AKKREDITERING

Afdelingen varetager opgaven som national it-sikkerhedsmyndighed, herunder på vegne af NATO og EU. Afdelingen sikkerhedsgodkender og fører tilsyn med elektroniske informationssystemer og installationer, der behandler klassificerede informationer. Afdelingen leder og kontrollerer endvidere den militære it-sikkerhedstjeneste på Forsvarsministeriets område og yder rådgivning om cyber- og informationssikkerhed til myndigheder på Forsvarsministeriets område. Afdelingen udfører sikkerhedsteknologiske undersøgelser og tekniske sikkerhedseftersyn.

STRATEGI, KOMMUNIKATION OG LEDELSESSEKRETARIAT

Afdelingen bidrager blandt andet til det strategiske samarbejde om cybersikkerhed med myndigheder og virksomheder i samfundsvigtige funktioner inden for rammerne af den nationale cyber- og informationsstrategi samt en række internationale opgaver. Derudover har afdelingen ansvar for CFCS' eksterne kommunikation.

BEREDSKAB, TELE OG STANDARDER

Afdelingen producerer rådgivningsmæssig viden om cyber- og informationssikkerhed. Afdelingen varetager desuden CFCS' rolle som national myndighed for informationssikkerhed og beredskab i telesektoren.

CFCS' FORMIDLING I 2022

Center for Cybersikkerhed udgiver løbende trusselsvurderinger og rådgivningsprodukter rettet mod myndigheder og samfundsvigtige sektorer i Danmark og i rigsfællesskabet.

Her kan du se, hvad vi udgav i 2022:

VEJLEDNINGER

Cybersikkerhed på rejsen (opdateret)
13. januar
Vejledning om cybersikkerhed i forbindelse med forretningsrejser med fokus på organisationers og medarbejderes adfærd.

Reducer risikoen for falske mails (opdateret)
17. februar
Vejledning om at øge organisationens modstandsdygtighed over for phishing, misbrug og forfalskning af organisationens maildomæner gennem implementering af DMARC.

Cybersikkerhed i leverandørforhold (opdateret)
6. maj
Vejledning om organisationers styring af cyber- og informationssikkerhed i kunde-leverandørforhold ved outsourcing af it.

Beskyt din organisation mod phishing-angreb (opdateret)
7. oktober
Vejledning til organisationer om at imødegå truslen fra phishing-mails.

Domænesikkerhed (opdateret)
14. oktober
Vejledning til organisationer om sikker håndtering af domæner og beskyttelse af organisationens online identitet.

Beskyt mod DDoS-angreb (opdateret)
27. oktober
Vejledning om at beskytte organisationen mod DDoS-angreb.

Sikker brug af Transport Layer Security (opdateret)
11. november
Vejledning om sikker brug af Transport Layer Security.

TRUSSESLVURDERINGER

Cybertruslen mod Danmark i lyset af Ruslands invasion af Ukraine
15. marts
Trusselsvurderingen beskriver den aktuelle trussel og de faktorer, som kan få betydning for, hvordan truslen udvikler sig.

CFCS hæver trusselsniveauet for cyberaktivisme mod Danmark fra LAV til MIDDEL
18. maj
Trusselsvurderingen beskriver baggrunden for truslen fra aktivistisk motiverede cyberangreb mod Danmark.

Cybertruslen mod Danmark 2022
28. juni
Trusselsvurderingen beskriver cybertruslen mod Danmark, der kommer fra cyberspionage, cyberkriminalitet, cyberaktivisme, destruktive cyberangreb og cyberterror.

Cybertruslen mod energisektoren
8. juli
Trusselsvurderingen beskriver cybertruslen mod energisektoren.

Cybertruslen mod hjælpemidler til navigation
24. november
Trusselsvurderingen beskriver cybertruslen mod hjælpemidler til navigation.

TEMAARTIKLER

Tiltag til styrket cyberberedskab
4. februar
Oversigt over tiltag, som organisationer kan bruge til at identificere indsatsområder for den grundlæggende cybersikkerhed.

WEBINARER

Aktuel cybertrussel og rådgivning om cyberberedskab i lyset af situationen i Ukraine
1. marts

Hvad er nyt i NIS2?
23. juni

Cybertruslen mod Danmark 2022
29. august

FØLG OS PÅ
X @Cybersikkerhed
LinkedIn @Centre for Cyber Security

CENTER FOR CYBERSIKKERHEDS BERETNING 2022

UDGIVELSE
November 2023

FOTO
Side 19, Unsplash
Side 22, Unsplash
Side 31, FreePik
Dronerune

DESIGN
e-Types

TRYK
Dystan og Rosenberg

PAPIR
Indhold: Scandia 2000 White 130 g
Omslag: Scandia 2000 White 300 g

Forsvarets Efterretningstjeneste
Center for Cybersikkerhed
Kastellet 30
2100 København Ø

Telefon: 3332 5566
www.cfcs.dk
www.fe-ddis.dk