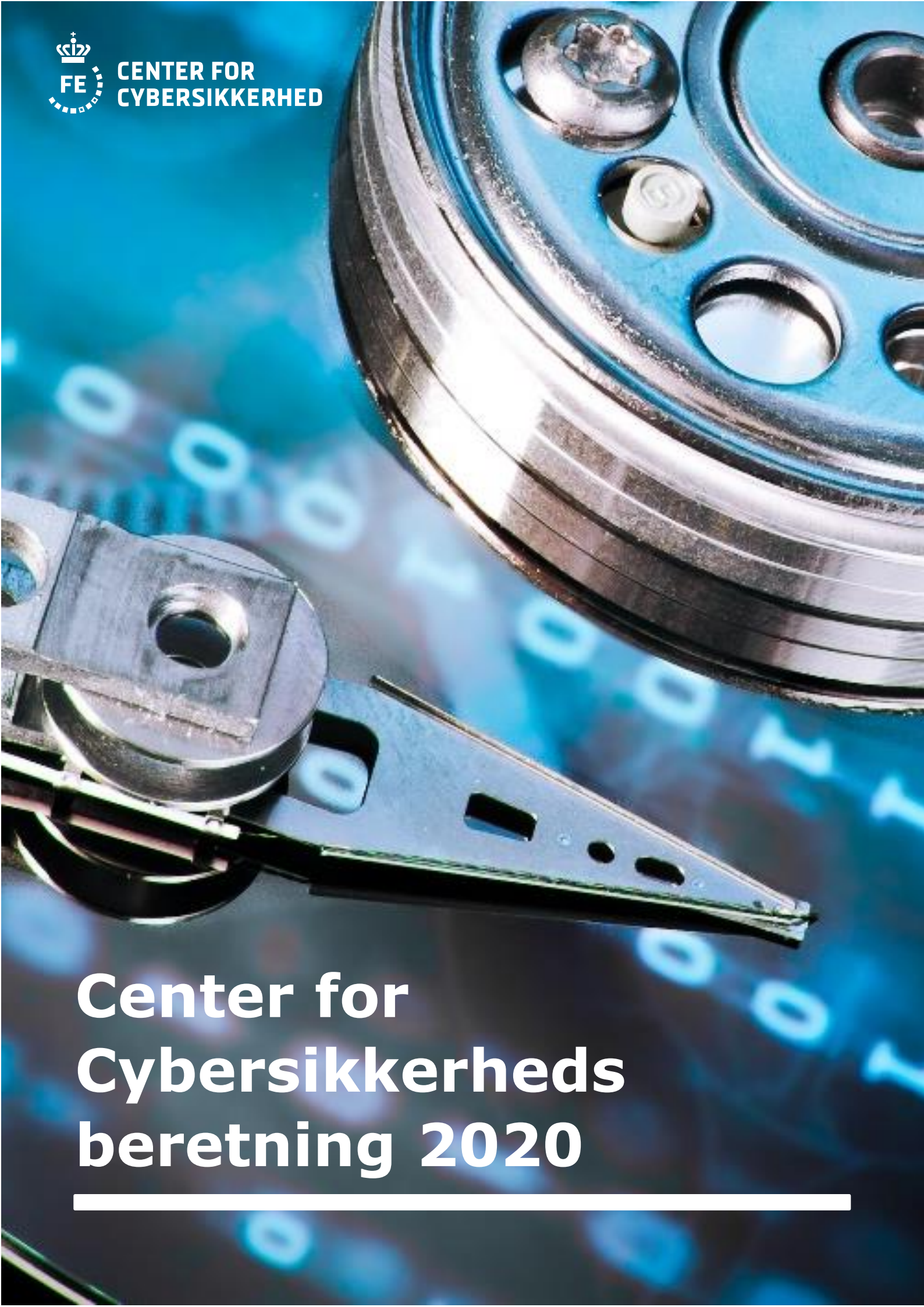


Center for Cybersikkerheds beretning 2020

Indhold

CENTER FOR CYBERSIKKERHED

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

1. udgave juni 2021

Forsideillustration: kubais/Shutterstock

Indledning

Danmark nyder godt af at være et meget digitaliseret land. COVID-19-pandemien har kun bekræftet dette og tydeliggjort nytten af digitale løsninger og vist, hvor værdifuldt det er, at vi kan arbejde, handle og være i kontakt med hinanden online. Men digitaliseringen gør os også sårbare over for cyberangreb. Derfor arbejder Center for Cybersikkerhed (CFCS) for et sikkert digitalt Danmark, så vi fortsat kan nyde godt af den velfærd og velstand, som digitaliseringen medfører. Centerets hovedopgave er således at understøtte sikkerheden i den digitale infrastruktur, som samfundsvigtige funktioner er afhængige af.[1]

Der er hele tiden hackere, der forsøger at udnytte aktuelle begivenheder, udviklinger eller vilkår til deres fordel. Det gælder også COVID-19-pandemien, der naturligt har fyldt i centerets arbejde i 2020. Hackere har eksempelvis udnyttet epidemien ved at sende phishing-mails med COVID-19 som tema. Derfor har centeret iværksat et målrettet arbejde med at finde ondsindede hjemmesider med henblik på at få disse nedtaget. Centeret har også udgivet en række korte vejledninger og gode råd til virksomheder, myndigheder og ansatte om sikkerhed ved hjemmearbejde. Endelig har centeret ydet særlig støtte til sikkerhedsarbejdet i forbindelse med Erhvervsstyrelsens kompensationsordninger.

Beretningen beskriver CFCS' indsatser i 2020 med at forebygge, opdage og håndtere sikkerhedshændelser i Danmark. Beretningen er uklassificeret og skrevet til offentliggørelse, og det afspejler sig naturligvis i formuleringerne og detaljeringsgraden. Men bag flere af indsatserne ligger et omfattende efterretningsmæssigt grundlag baseret på Forsvarets Efterretningstjenestes (FE) målrettede arbejde med – både på egen hånd og i samarbejde med vores partnere i udlandet – at tilvejebringe efterretninger.

[1] På CFCS' hjemmeside forklares en række begreber, herunder samfundsvigtige funktioner og kritisk infrastruktur: https://cfcs.dk/da/cybertruslen/ordforklaringer/

Om FE's Center for Cybersikkerhed

Efterretningsbaseret cyberforsvar
CFCS blev oprettet i december 2012 som en del af FE. De fleste cyberangreb mod Danmark kommer fra udlandet, og derfor er det vigtigt, at CFCS har viden om, hvad udenlandske aktører foretager sig. Placeringen i FE sikrer, at Danmark er med i den kreds af vestlige lande, som kan levere et efterretningsbaseret nationalt cyberforsvar. Grundlaget for arbejdet er primært Lov om Center for Cybersikkkerhed, der blandt andet regulerer centerets håndtering af personoplysninger.

Fra håndtering af avancerede cyberangreb til vejledning og rådgivning
CFCS varetager en række opgaver, der spænder bredt fra rådgivning og vejledning til imødegåelse af avancerede cyberangreb:

- Netsikkerhedstjenesten har til opgave at opdage, analysere og bidrage til at imødegå sikkerhedshændelser i den kritiske infrastruktur. Fokus er både på de mest avancerede angreb, der oftest udføres af statsstøttede aktører, og på angreb, der kan påvirke det danske samfund i væsentlig grad.

- CFCS er national it-sikkerhedsmyndighed og varetager opgaver inden for informationssikkerhed, som Danmark gennem sit medlemskab af blandt andet NATO og EU er forpligtet til. Centeret sikkerhedsgodkender og fører tilsyn med klassificerede elektroniske informationssystemer og udfører sikkerhedsteknologiske undersøgelser og tekniske sikkerhedseftersyn.

- Rollen som nationalt kompetencecenter på cybersikkerhedsområdet indebærer vejledning og rådgivning til myndigheder og virksomheder i at styrke cybersikkerheden.

- På teleområdet har centeret en særlig lovbunden opgave med at sikre beredskab og føre tilsyn med informationssikkerheden.

Medarbejdersammensætning
CFCS er en arbejdsplads med mange forskellige typer af højtspecialiserede med-arbejdere, herunder netværksanalytikere, forensicsanalytikere, malwareanalytikere, pen-testere, informationssikkerhedsrådgivere og teleingeniører. Størstedelen af centerets medarbejdere har en it-uddannelse eller anden teknisk baggrund. Men centeret har også medarbejdere uden formel uddannelse, der har udvist et særligt talent inden for et relevant teknisk område. Dertil kommer en gruppe medarbejdere med militærfaglig baggrund og akademikere med en samfundsvidenskabelig baggrund.

Cybertruslen i 2020

Udover COVID-19-pandemien vil cybertruslen i 2020 særligt blive husket for to typer af angreb: alvorlige ransomware-angreb og afsløringer af storstilede cyberspionagekampagner. De angreb, der blev opdaget i 2020, understregede, at truslen fra cyberkriminalitet og cyberspionage mod Danmark fortsat er meget høj. Truslen fra destruktive cyberangreb og cyberaktivisme var derimod lav i Danmark i 2020.

Truslen fra alvorlige ransomware-angreb var og er rettet mod alle dele af samfundet. I 2020 blev det tydeliggjort af, at alt fra hospitaler til bilproducenter blev ramt på globalt plan. I Danmark blev blandt andre pumpeproducenten DESMI ramt i foråret, og nyhedsbureauet Ritzau blev ramt i efteråret. Et naturligt fokus var derfor også ransomware i sundhedssektoren, hvor man blev ramt indirekte via medicin-indkøberen Amgros.

Flere store cyberspionageangreb blev opdaget i 2020. Det mest omfattende var kompromitteringen af tusinder af virksomheder verden over via software fra virksomheden SolarWinds. I Danmark har flere myndigheder og virksomheder fået installeret en bagdør via softwaren, og CFCS har været med til at undersøge, om denne bagdør er blevet udnyttet til at stjæle data. I udlandet var der også flere sager om cyberspionage mod COVID-19-forskning. Angrebene viser, at fremmede stater kan og vil stjæle andre staters og private virksomheders viden.

Tilsynets årlige redegørelse og CFCS' årlige beretning

Tilsynet med Efterretningstjenesterne (TET) udgiver årligt en redegørelse om tilsynet med CFCS. TET er et særligt uafhængigt kontrolorgan, der har ført tilsyn med CFCS' behandling af personoplysninger siden 1. juli 2014, hvor Lov om Center for Cybersikkerhed trådte i kraft. TET's årlige redegørelser kan findes på TET's hjemmeside, tet.dk

TET's årsredegørelse suppleres, jf. bemærkningerne til Lov om Center for Cybersikkerhed fra 2014, af en årlig beretning fra CFCS, der også beskriver centerets aktiviteter på det forebyggende område og bringer statistiske oplysninger herom. Desuden skal beretningen indeholde et overblik over de trusselsvurderinger mv., der er udsendt i årets løb, således at virksomheder og offentligheden kan få et overblik over risikoen for cyberangreb. Herudover udgiver centeret løbende vejledninger, situationsbilleder og lignende. Redegørelserne og den årlige beretning fra CFCS vil også blive offentliggjort på CFCS' hjemmeside, cfcs.dk

Center for Cybersikkerheds indsatser i 2020

COVID-19-pandemien har naturligt fyldt meget både i forhold til opgaveløsningen og organiseringen af arbejdet i CFCS i 2020. Fokus har overordnet været på:

- Bred rådgivning og vejledning om cybersikkerhed og trusselsbilledet til myndigheder og virksomheder, herunder tæt dialog med de seks samfundskritiske sektorer (energi, tele, finans, sundhed, transport og søfart) og forsvaret.

- COVID-19-relaterede opgaver, blandt andet udgivelse af særskilte trusselsvurderinger, herunder en række ikke-offentliggjorte vurderinger direkte til berørte organisationer, identifikation af COVID-19-relaterede ondsindede hjemmesider, øget rådgivning om sikkerhed ved distancearbejde samt sikkerhedsarbejdet vedrørende Smitte|stop-app'en.

- Monitorering, varsling og rådgivning om cybersikkerhed i Grønland som følge af ikrafttrædelsen af Lov om Center for Cybersikkerhed i Grønland samt rådgivning forud for etablering af klassificerede elektroniske informationssystemer hos myndighederne i Grønland og på Færøerne.

- Blandt de mange operative opgaver kan nævnes arbejdet i begyndelsen af 2020 med at afdække og imødegå kompromitteringer af et stort antal virksomheder og myndigheder, der var blevet ramt gennem en sårbarhed i netværksudstyr fra producenten Citrix Systems, og indsatsen i slutningen af året med at afdække og imødegå SolarWinds-angrebet, som ramte en række danske virksomheder og myndigheder.

- Udbygning af CFCS' sensornetværk med en ny type sensor, der sættes op hos myndigheder og virksomheder af samfundsvigtig karakter for at skabe overblik over det aktuelle cybertrusselsbillede i Danmark samt give mulighed for omfattende varsling fra det nu døgnbemandede situationscenter. Grundet nedlukningen, som følge af COVID-19-pandemien, og overgangen til virtuelt arbejde for mange myndigheder og virksomheder, er tidsplanen for udviklingen af den nye type sensor og selve udrulningen blevet kortvarigt forlænget.

- Gennemførelse af tekniske sikkerhedseftersyn og sikkerhedstekniske undersøgelser, herunder penetrationstest, og relevant rådgivning til myndigheder og virksomheder om mitigering af identificerede sårbarheder i de undersøgte systemer.

- Assistance til Forsvarsministeriet vedrørende lovgivningsmæssigt arbejde for eksempel teletekniske afklaringer i forbindelse med udarbejdelse af forslag til Lov om leverandørsikkerhed i den kritiske teleinfrastruktur (vedtaget i Folketinget i maj 2021).

- Arbejdet med en ny national strategi for cyber- og informationssikkerhed, der skal øge ambitionsniveauet både i sektorernes indsatser og de tværgående, nationale indsatser, arbejdet med 5G-værktøjskassen i NIS-samarbejdsgruppen og det forberedende arbejde med Europa-Kommissionens udkast til revideret NIS-direktiv (EU's direktiv om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen).

Særlige indsatser relateret til COVID-19-pandemien

Rådgivning og varsling
COVID-19-pandemien genererede stor efterspørgsel efter CFCS' rådgivning, både i form af specifik rådgivning og mere bred, generel rådgivning. Centeret har løbende varslet og publiceret gode råd til både it-afdelinger og ansatte på CFCS' hjemmeside, sociale medier (Twitter og LinkedIn) samt via sikkerdigital.dk og andre vidensdelingsfora.

I marts 2020 udgav CFCS en vejledning med gode råd om hjemmearbejde efterfulgt af en Q&A om cybersikkerhed ved hjemmearbejde, en vejledning til sikker brug af kommunikations- og samarbejdsplatforme og anbefalinger om adgang til SCADA-systemer fra hjemmearbejdspladser. I slutningen af april udgav centeret en vejledning om cybersikker tilbagevenden til arbejdspladsen. Desuden udgav centeret i midten af marts 2020 en trusselsvurdering, der omhandlede cybertruslen ved hjemmearbejde og i begyndelsen af april 2020 en mere detaljeret trusselsvurdering om cybertruslen mod Danmark under COVID-19-pandemien. Senere på året udgav CFCS en trusselsvurdering, der pegede på, at flere kriminelle hackergrupper over foråret og sommeren 2020 havde fornyet deres værktøjer, samarbejdsrelationer og aktiviteter blandt andet som følge af COVID-19-pandemien.

Opdagelse af ondsindede hjemmesider relateret til COVID-19-pandemien
Under COVID-19-pandemien er der løbende blevet oprettet en række falske hjemmesider, hvor navnet ligger tæt op ad forskellige myndigheders officielle domænenavne, herunder fra sundhedssektoren. CFCS har i den forbindelse intensiveret identifikationen af ondsindede domæner og IP-adresser. En række af disse er overgivet til Rigspolitiet, der med udgangspunkt i L 157 (ændring af straffeloven, retsplejeloven mv.) har fået mulighed for at pålægge internetudbyderne at DNS-blokere kriminelle hjemmesider med COVID-19-relateret indhold. I 2020 er over 1,3 mia. domæner blevet automatisk undersøgt, og over 70.000 domæner er udtaget og undersøgt yderligere for mistænkeligt indhold. Det har blandt andet resulteret i 314 varsler til hosting-udbydere. Rigspolitiet har efterfølgende anmodet teleudbyderne om at blokere 41 domæner. Arbejdet fortsætter i 2021.

Særlig assistance til sundhedssektoren og Erhvervsstyrelsen
Udover at hjælpe Sundhedssektoren med nedtagning af falske hjemmesider har CFCS assisteret Erhvervsstyrelsen med den tekniske udvikling af de digitale kompensationsløsninger til erhvervslivet. CFCS udarbejdede i den forbindelse en trusselsvurdering og assisterede med rådgivning og sikkerhedstekniske undersøgelser af de pågældende it-systemer i takt med, at de blev etableret.

Strategisk dialog med myndigheder og virksomheder m.fl.
Også i 2020 har CFCS arbejdet tæt sammen med en lang række interessenter, samarbejdspartnere og kunder om at forebygge, opdage og imødegå cyberangreb. Centeret er i løbende dialog med forsvaret samt myndigheder og virksomheder ikke mindst i de seks samfundskritiske sektorer (energi, tele, finans, sundhed, transport og søfart). Blandt andet var CFCS og Søfartsstyrelsen, sammen med myndigheder fra USA og Nederlandene, værter for et internationalt webinar om styrket maritimt myndighedsarbejde om cybersikkerhed. Derudover har centeret et tæt samarbejde med blandt andre politiet, herunder Politiets Efterretningstjeneste (PET), om særligt konkrete sager samt Digitaliseringsstyrelsen og Erhvervsstyrelsen.

CFCS faciliterer Strategisk Samarbejdsforum for Cybersikkerhed, hvor repræsentanter fra erhvervsliv og brancheorganisationer deltager. Forummet mødtes tre gange i 2020 og har blandt andet drøftet sikkerhed og distancearbejde, truslen fra målrettet ransomware og beskyttelse af den kritiske infrastruktur. Endelig har det offentligt-private Cybersikkerhedsråd mødtes i alt 12 gange i 2020 og drøftet blandt andet input til regeringens strategiske arbejde med cybersikkerhed i en national ramme, Smitte|Stop-app'en, den kommende mærkningsordning vedr. it-sikkerhed og ansvarlig dataanvendelse samt planlægning af eksterne webinarer, jf. nedenstående faktaboks.

Cybersikkerhedsrådets aktiviteter i 2020

Det offentligt-private cybersikkerhedsråd rådgiver regeringen om det strategiske arbejde med cybersikkerhed i en national ramme og har i 2020 især haft fokus på bidrag til en ny national cyber- og informationssikkerhedsstrategi og to velbesøgte webinarer i juni og oktober. På webinaret i juni var der debat om IoT-produkter, DNS-blokering og erfaringsudveksling om hændelser. Efterårets webinar bød som led i cybersikkerhedsmåneden på konkrete råd og vejledning til både borgere, myndigheder og virksomheder. I foråret 2020 deltog Cybersikkerhedsrådet desuden i en række temamøder forud for lanceringen af den danske app Smitte|stop til brug for smitteopsporing af COVID-19.

Om Cybersikkerhedsrådet
Cybersikkerhedsrådet er sammensat af medlemmer fra erhvervslivet, myndigheder, forbrugersiden og forskningsverdenen. Deres faglighed spænder bredt over strategiske og juridiske såvel som teknologiske kompetencer.

Møderne ledes af det offentligt-private formandskab bestående af Digitaliseringsstyrelsen, CFCS og koncerndirektør Bjarke Alling, Liga ApS. Cybersikkerhedsrådet blev nedsat i december 2019, og medlemmerne er udpeget for perioden 2019-2021.

Læs mere om Cybersikkerhedsrådet på cfcs.dk

Ny national strategi for cyber- og informationssikkerhed
For at sikre et højt cybersikkerhedsniveau, der følger med den løbende udvikling i trusler og sårbarheder, besluttede regeringen i 2020 at igangsætte arbejdet med en ny national strategi for cyber- og informationssikkerhed. CFCS har bidraget betydeligt til arbejdet med en ny strategi og deltager blandt andet i strategiens styregruppe, der har delt formandskab mellem CFCS og Digitaliseringsstyrelsen, og hvor alle ministerområder er repræsenteret.

Den nye strategi skal øge ambitionsniveauet både i sektorernes indsatser og i forhold til de tværgående, nationale indsatser. Formålet er at styrke den generelle robusthed og modstandsdygtighed i samfundet yderligere. Strategien vil have fokus på initiativer under fire overordnede temaer: ledelsesforankring og kompetenceudvikling, robusthed og resiliens, samarbejde og organisering samt internationale indsatser. Strategien forventes lanceret i løbet af 2021.

Opdagelse og håndtering af sikkerhedshændelser i 2020

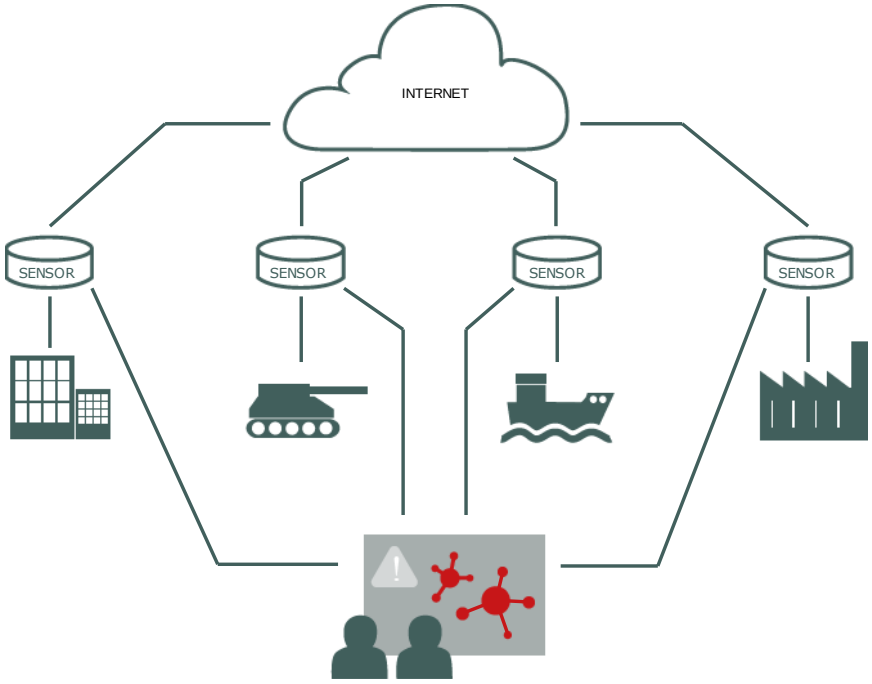
Cyberakademi og døgnbemanding af situationscenteret
FE gennemførte i 2020 sit andet Cyberakademi, og CFCS' situationscenter er nu bemandet med det nødvendige antal junioranalytikere, der sikrer døgnbemanding og er siden primo december 2020 fuldt operativt 24/7/365. Situationscenteret er den centrale indgang for myndigheder og virksomheder i forhold til de operative opgaver og arbejder tæt sammen med afdelingen for cyberoperationer som del af netsikkerhedstjenesten, der har til opgave at forebygge, opdage og imødegå sikkerhedshændelser.

Om Cyberakademiet
I 2020 gennemførte FE sit andet Cyberakademi. Uddannelsen retter sig mod kandidater, som har de rette it-interesser, evner og motivation til en karriere inden for cybersikkerhed. I løbet af tre måneder gennemførte 12 kandidater undervisning i datasikkerhed, netværksforståelse og programmering, angrebstyper, angrebsopdagelse, analyse af sikkerhedshændelser og brug af relevante tekniske værktøjer. Ud over FE/CFCS' egne kandidater deltog også en ekstern deltager fra en virksomhed fra telesektoren.

Udbygning af sensornetværket
CFCS har i 2020 forberedt en yderligere udbredelse af sensornetværket til myndigheder og virksomheder. Sensornetværket har til hensigt at opdage forsøg på cyberangreb og består af sensorer, der indeholder en række regler, der bruges til at genkende forsøg på cyberangreb. Det kan være IP-adresser eller internetdomæner, der bliver brugt af en hackergruppe, eller det kan være digitale fingeraftryk af filer, der indeholder malware. Når der registreres potentielt ondsindet trafik modtager netsikkerhedstjenesten en alarm.

Sensornetværket består af to typer sensorer. Dels et egenudviklet intrusion detection-system (IDS), som består af hardwareenheder med en betydelig lager-kapacitet placeret på internetforbindelsen foran ministerier m.fl. Dels en ny kommercielt udviklet sensor, der har til formål at bidrage til et nationalt situationsbillede. Udrulningen af den nye type sensor er i 2020 blevet kortvarigt forlænget som følge af COVID-19-pandemien og overgangen til virtuelt arbejde.

Figur af CFCS' sensornetværk



Figur af CFCS' sensornetværk. Sensornetværket består af sensorer placeret på internetforbindelsen foran bl.a. flere ministerier og offentlige myndigheder. Sensorerne indeholder en række regler, der bruges til at genkende forsøg på cyberangreb. Når der registreres potentielt ondsindet trafik, der passer på en regel, modtager netsikkerhedstjenesten en alarm.

Tilslutninger til sensornetværket

Ved udgangen af 2020 havde CFCS i alt 242 tilsluttede myndigheder og virksomheder fordelt på 168 offentlige myndigheder og institutioner m.fl., 36 enheder i forsvaret og seks private virksomheder. Hertil kom 32 offentlige myndigheder og institutioner m.fl. i Grønland.

I de seks samfundskritiske sektorer (tele, energi, finans, sundhed, transport og søfart), som defineret i den nationale cyber- og informationssikkerhedsstrategi, er i alt ni private virksomheder og offentlige institutioner m.fl. omfattet af sensornetværket. Tallet omfatter ikke myndigheder i de seks sektorer.

CFCS har tidligere opgjort tilslutninger til sensornetværket med udgangspunkt i antal tilslutningsaftaler, hvoraf en tilslutningsaftale kunne dække flere underliggende myndigheder. Centeret vil fremover opgøre tilslutninger med udgangspunkt i antal monitorerede organisationer frem for antal tilslutningsaftaler.

Sikkerhedshændelser i 2020

Danmark rammes hvert år af mange tusinde cyberangreb. Tallene for sikkerheds-hændelser i denne beretning er alene udtryk for antallet af hændelser, som CFCS har håndteret i 2020. Det vil sige hændelser, der er identificeret ved hjælp af sensornetværket, indberetninger, direkte henvendelser, tip fra partnere og ved hjælp af FE's efterretningsmæssige virke. Der eksisterer et stort mørketal for cyberangreb i Danmark, da kun relativt få hændelser indberettes til CFCS.

Definition af sikkerhedshændelse

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

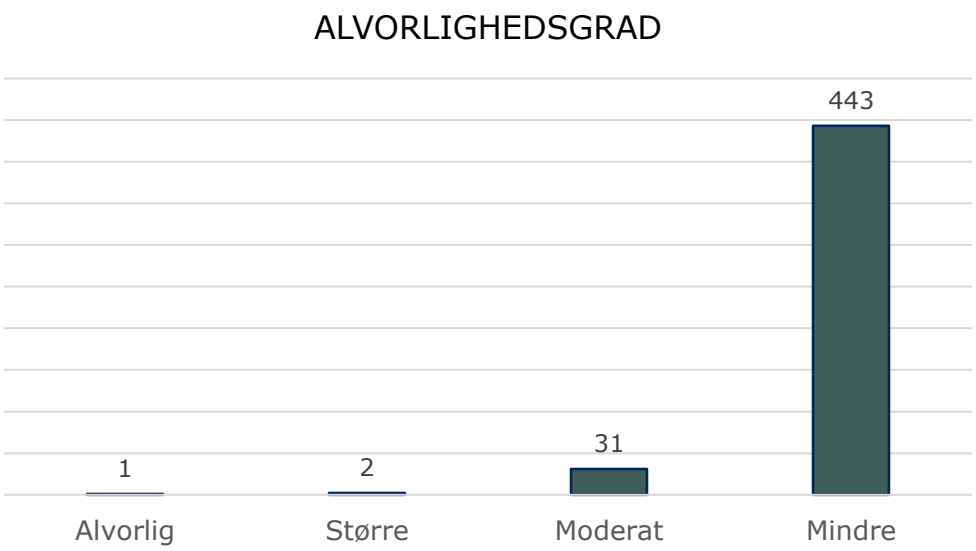
Kilde: Lov om Center for Cybersikkerhed

Centeret har i 2020 håndteret 477 hændelser, der har haft effekt på den berørte organisation. Tallet var i 2019 416 lignende hændelser. Tallene kan ikke sammenlignes direkte år for år, da forudsætningerne for datagrundlaget ændrer sig løbende. Det sker for eksempel, når CFCS opstiller en sensor hos en ny myndighed eller virksomhed og dermed får en bedre indsigt i hændelsesbilledet.

Ud over de 477 hændelser, der har haft effekt på den berørte organisation, har CFCS observeret en stor mængde 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 disse forsøg. I 2020 blev der observeret 4.503 tilfælde af potentiel ondsindet aktivitet, herunder falske positiver, der har haft ingen eller begrænset effekt.

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

Alvorlighedsgrad af hændelser



Kilde: Netsikkerhedstjenesten. Tallene for sikkerhedshændelser er alene udtryk for antallet af hændelser, som CFCS har håndteret i 2020. Det vil sige hændelser, der er identificeret ved hjælp af sensornetværket, indberetninger, direkte henvendelser, tip fra partnere eller ved hjælp af FE's efterretningsmæssige virke. CFCS har i tidligere beretninger medtaget sikkerhændelser af kategorien "Ingen/begrænset effekt" i søjlediagrammet. Kategorien er taget ud af diagrammet, da kategorien rummer falske positiver.

Alvorlighedsgrader af sikkerhedshændelser

Falsk positiv
Undersøgelse af alarm, som viser sig ikke at være et angreb.

Ingen/begrænset effekt
Aktiviteten har ikke haft nogen betydning for den berørte organisation. Der kan for eksempel være tale om rekognosceringer. Aktiviteten kan dog medføre et endda betydeligt analysearbejde, opfølgende rådgivning og tilpasning af sikkerhedstilstanden.

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 for eksempel skifte passwords, ændre administratorrettigheder mv.

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. Det kan også gælde en aktør, der har fået adgang til en brugerkonto med begrænsede rettigheder. Men angrebet har ikke spredt sig til kritiske systemer, og aktøren har ikke fået adgang til sensitive informationer.

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, og kan medføre alvorlige tab af data og langvarige afbrydelser af it-driften. Det kan også være angreb, hvor aktøren har haft fodfæste på organisationens netværk gennem længere tid og potentielt haft adgang til sensitiv information. Større sager med cyberspionage hører til i denne kategori.

Alvorlig
Kritiske systemer berørt eller system- eller administratorkonti kompromitteret. Hændelsen har alvorlig betydning for den berørte organisation. CFCS har en meget høj barre for, hvornår et angreb bliver regnet for et alvorligt angreb. Dette hænger sammen med, at CFCS' hovedopgave er at understøtte sikkerheden i den digitale infrastruktur, som samfundsvigtige funktioner er afhængige af.

To eksempler på håndtering af cyberangeb i 2020

Kompromitteringer af danske netværk gennem sårbarhed i Citrix Application Delivery Controller

Først på året i 2020 opdagede CFCS, at mindst tre forskelige aktører forsøgte at kompromittere et stort antal myndigheder og virksomheder via den samme nyopdagede sårbarhed i netværksudstyr fra producenten Citrix Systems, der anvendes bredt i Danmark. Situationscenteret udsendte en række brede varsler om sårbarheden med det formål at orientere om truslen og informere om nyttige sikkerhedstiltag.

Angrebene ledte til flere kompromitteringer i danske netværk, og CFCS samarbejdede med ofrene for at afdække aktiviteten og mitigere kompromitteringerne. CFCS afdækkede aktørernes metode og identificerede ondsindet aktivitet hos myndigheder via en række forskellige datakilder blandt andet sensornetværket og data modtaget fra mulige ofre. Analyserne af data indikerede, at der var tale om mindst tre forskellige aktører, der forsøgte at udnytte sårbarheden. Aktørerne brugte dog forskellige metoder og typer af malware. CFCS vurderer, at motivet for aktørerne var henholdsvis økonomisk kriminalitet og spionage.

Hacket af SolarWinds førte til kompromitteringer i Danmark

I december 2020 opdagede sikkerhedsfirmaet FireEye et af de mest omfattende cyberspionageangreb nogensinde, der er kommet til offentlighedens kendskab. Organisationer verden over, herunder i Danmark, var blevet kompromitterede via softwaren Orion fra virksomheden SolarWinds. Offentligt kendte ofre er blandt andet flere centrale amerikanske myndigheder, såsom det amerikanske finansministerium.

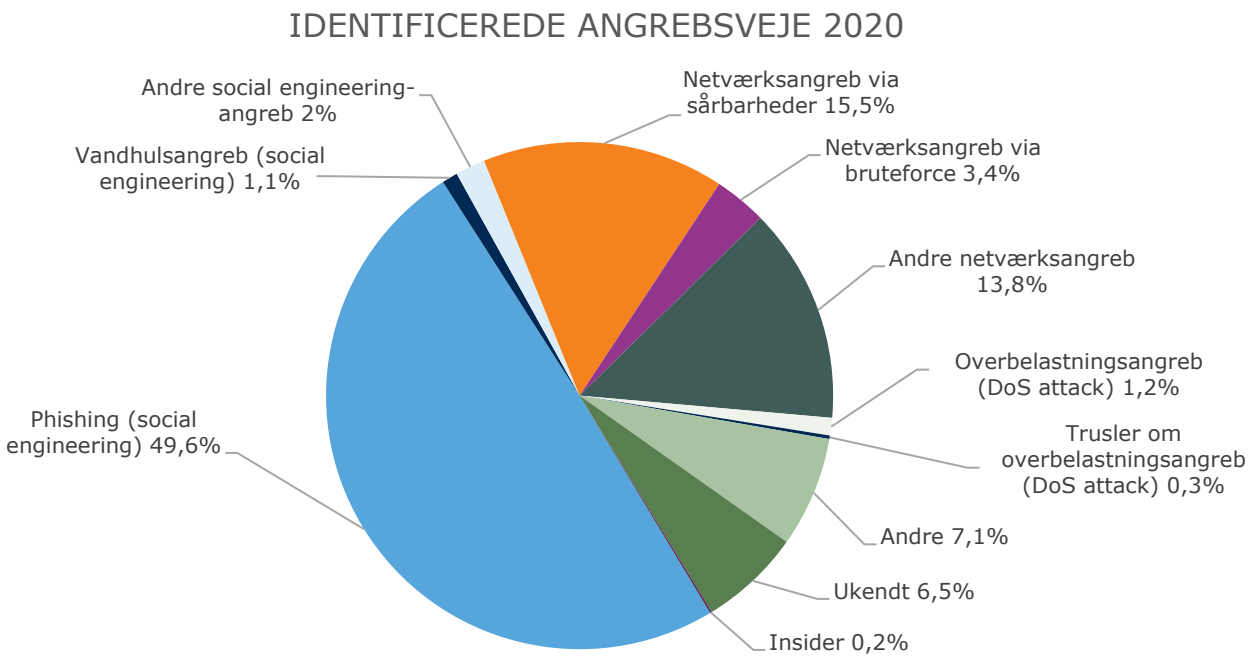
CFCS har varslet bredt om de mulige kompromitteringer, og CFCS' undersøgelser viser, at mindst 50 organisationer i Danmark har anvendt den kompromitterede version af Orion. Dermed har de fået installeret en bagdør i deres netværk. CFCS har samarbejdet med ofrene om at undersøge, om bagdøren har været udnyttet til at kompromittere ofrene yderligere med henblik på at stjæle data.

CFCS vurderer, at kompromitteringen via SolarWinds' software er et meget alvorligt angreb med en i dette tilfælde begrænset skadevirkning i Danmark. Det er sandsynligt, at formålet med kompromitteringen er spionage.

Angrebet blev ifølge åbne kilder udført ved, at hackere kompromitterede virksomheden SolarWinds, som leverer software til organisationer verden over. Hackerne tilføjede i foråret 2020 ondsindet kode i legitime opdateringer til SolarWinds' software Orion. I december 2020 oplyste SolarWinds, at de inficerede softwareopdateringer var distribueret til op mod 18.000 organisationer verden over. Den ondsindede kode gav hackerne en indledende adgang til ofrenes systemer, som de potentielt har kunnet forsøge at udnytte yderligere. Aktøren har sandsynligvis udvalgt de mest interessante ofre og er gået videre med disse.

Angrebsveje

Monitoreringen 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 nedenfor viser fordelingen af de identificerede angrebsveje for 2020. Diagrammet siger ikke noget om, hvilken indvirkning hændelsen har haft på den ramte organisation.



Kilde: Netsikkerhedstjenesten. 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. CFCS har i tidligere beretninger medtaget kategorien "rekognosceringer" i lagkagediagrammet. Kategorien er taget ud af diagrammet, da kategorien rummer falske positiver.

CFCS ser især forsøg på phishing, der bruges til at lokke fortrolige oplysninger ud af folk via for eksempel falske mails. Derudover ser CFCS en del netværksangreb. Netværksangreb dækker over angrebstyper, som søger at få adgang til it-systemer via angreb på eksponerede systemelementer over internettet for eksempel ved at udnytte sårbarheder og fejlkonfiguration af softwaren.

Ordforklaring – angrebsveje

Social engineering er en teknik, hvor der anvendes psykologiske greb til at få offeret til i god tro at udføre en handling, vedkommende ellers ikke ville have udført. Det kan eksempelvis være at afgive loginoplysninger eller videregive informationer om organisationen, dens processer, systemer eller kunder. Mere avanceret social engineering anvender ofte informationer om ofret eller arbejdspladsen, som er fundet på hjemmesider eller sociale medier ved forudgående rekognoscering. Social engineering kan blandt andet ske via mail (phishing), sms (smishing) eller telefon (vishing).

Phishing er et forsøg på at narre mailmodtagere til i god tro 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. Phishing-mails sendes ofte bredt ud til mange tilfældige modtagere uden at være tilpasset den enkelte modtager.

Netværksangreb dækker over angrebstyper, som søger at få adgang til ofrets it-systemer via angreb på eksponerede systemelementer over internettet. Det dækker for eksempel over forsøg på at udnytte sårbarheder og fejlkonfiguration af softwaren samt forsøg på at etablere uautoriseret systemadgang via brute force-angreb mod for eksempel login-oplysninger.

Brute force-angreb dækker blandt andet over at forsøge hyppigt brugte passwords som for eksempel "123456" mod mange brugernavne (for eksempel alle mailadresser i en organisation). Dette kaldes "password spraying". Det kan også dække over forsøg på at bruge kombinationer af brugernavne og passwords fra tidligere datalæk mod et system. Dette kaldes også "credential stuffing".

Overbelastningsangreb DDoS står for Distributed Denial of Service og er et overbelastningsangreb. Hackere udnytter kompromitterede computere til at generere usædvanligt store mængder datatrafik mod en hjemmeside (webserver) eller et netværk, så hjemmesiden eller netværket ikke er tilgængeligt for legitim trafik, mens angrebet står på.

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.

Insider er en person, som ved sine handlinger udgør en risiko for den organisation, vedkommende er eller har været ansat i. En person kan blive insider enten forsætligt eller uforsætligt. En uforsætlig insider-handling sker enten ved et uheld eller ved, at vedkommende bliver manipuleret eller vildledt til at foretage handlinger, der truer sikkerheden. En forsætlig insider har et ønske om at afsløre viden (brud på fortrolighed) eller påvirke interne systemer (brud på integritet eller tilgængelighed). Forsætlig insider kan være drevet af forskellige motivationer.

Forebyggende indsatser i 2020

Forebyggelse og rådgivning

Forebyggelse af sikkerhedshændelser og cyberangreb handler om at sikre sin organisation og sine systemer, så de er svære at angribe, og sin forberedelse af, hvordan man skal håndtere situationen, hvis man bliver ramt. CFCS udgiver løbende trusselsvurderinger og vejledninger og tilbyder konkret rådgivning til myndigheder og virksomheder som hjælp til at sikre Danmarks digitale infrastruktur. CFCS' arbejde har i 2020 naturligvis været påvirket af overgangen til virtuelt arbejde for et stort antal medarbejdere og af nye COVID-19-relaterede opgaver, herunder en voksende efterspørgsel på trusselsvurderinger, rådgivning og operativstøtte.

Oversigt over myndigheds- og forebyggelsesindsatser 2020

Kategorier	Antal
Rådgivnings- og kundemøder	643
Awareness-briefinger	130
Trusselsvurderinger	13
Undersøgelsesrapporter	2
Vejledninger	13
It-sikkerhedsgodkendelser	60
Godkendelse af kryptoplaner	61
Tekniske sikkerhedseftersyn	104
Sikkerhedstekniske undersøgelser	16
Tempest zoning (udstrålingskontrol)	30
Tilsyn med informationssikkerhed	17
Varsler	276
Varsler til hosting-udbydere om falske hjemmesider relateret til Covid-19	314
Varsler via Mit Digitale Selvforsvar*	131
Tweets	428

Note: Udover CFCS' offentligt tilgængelige publikationer, som fremgår af oversigten, kommer en række klassificerede produkter blandt andet trusselsvurderinger og undersøgelsesrapporter.
**CFCS påbegyndte i 2020 et samarbejde med Forbrugerrådet Tænk om udsendelse af advarsler om falske hjemmesider, phishing-mails mv. via appen Mit Digitale Selvforsvar.*

Trusselsvurderinger

CFCS offentliggjorde i 2020 13 trusselsvurderinger og to undersøgelsesrapporter, der er tilgængelige på cfcs.dk. Tre af trusselsvurderingerne omhandlede cybertruslen specifikt for de samfundskritiske sektorer, som centeret har et løbende samarbejde med blandt andet i form af indstationerede medarbejdere fra nogle af sektorerne. Dertil kommer en række klassificerede trusselsvurderinger og rapporter til udvalgte kunder samt briefinger i både åbne og lukkede fora blandt andet for at skabe

opmærksomhed om, at cybertruslen kræver et vedvarende ledelsesfokus hos myndigheder og virksomheder.

Særligt fokus på ransomware

Målrettede ransomware-angreb på danske virksomheder har ofte betydelige økonomiske tab til følge. Ved 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.

CFCS satte fokus på ransomware i 2020 med udgivelsen af en trusselsvurdering, en undersøgelsesrapport og en vejledning om ransomware. CFCS afholdt i den forbindelse et webinar med fokus på truslen fra ransomware-angreb og vejledning til at reducere risikoen for denne type angreb.

Undersøgelsesrapporten "Anatomien af målrettede ransomware-angreb" beskriver angrebsforløbet i et typisk målrettet ransomware-angreb på baggrund af indsigt i faktiske angreb mod danske og udenlandske organisationer.

Trusselsvurderingen "Kriminelle spænder den digitale tommelskrue" beskriver, hvordan hackere siden efteråret 2019 har udvidet afpresningen i forbindelse med ransomware-angreb ved også at true med at lække eller sælge følsom information stjålet i forbindelse med angrebet. Kombinationen af ransomware-angreb og trusler om læk kaldes for dobbelt afpresning.

CFCS' vejledning "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.

Vejledninger

CFCS har i 2020 offentliggjort 13 vejledninger, herunder om phishing, ransomware, sikring af domæner og logning. Der er også udgivet en vejledning om krav til brugen af transport layer security (TLS), en opdateret passwordvejledning og en opdateret vejledning til bestyrelser. Alle vejledninger er tilgængelige på cfcs.dk. Derudover har CFCS i 2020 udgivet en række gode råd og korte vejledninger til virksomheder, myndigheder og ansatte om sikkerhed ved hjemmearbejde under COVID-19-pandemien.

Reducer risikoen for falske mails

Cyberangreb starter ofte med, at medarbejderen modtager en mail, som ser ud til at være sendt fra eksempelvis en kollega, samarbejdspartner eller offentlig myndighed uden at være det.

Et redskab til at imødegå denne trussel er protokollen DMARC (Domain-based Message Authentication, Reporting and Conformance), som gør det muligt at forhindre mails med en forfalsket afsender i at nå ud til slutbrugere og samtidig begrænse misbrug af de domænenavne, organisationen ejer.

Læs mere i vejledningen "Reducer Risikoen for Falske Mails", der først og fremmest henvender sig til organisationers it-ledelse.

I 2020 har CFCS rådgivet myndigheder og virksomheder om blandt andet risikostyring, beredskab, adfærdsorienteret informationssikkerhed, leverandørstyring, uddannelse og kompetencer samt anskaffelser og udbud. Centeret har bistået Digitaliseringsstyrelsen med vejledning om informationssikkerhed til offentligt ansatte i regi af samarbejdet omkring Den fællesoffentlige digitaliseringsstrategi. CFCS har også bistået Erhvervsstyrelsen i forbindelse med sikkerheden i de statslige kompensationsordninger, ligesom private virksomheder og organisationer har benyttet rådgivningsydelser fra centeret.

Sikkerpånettet.dk

I oktober lancerede DK Hostmaster portalen sikkerpånettet.dk i samarbejde med CFCS, andre myndigheder og interesseorganisationer. Domæneejere og andre kan på portalen tjekke, om et domænes hjemmeside og mailtjeneste følger opdaterede standarder, og om der er implementeret en række grundlæggende sikringstiltag, hvoraf flere indgår i de tekniske minimumskrav, som statslige myndigheder skal leve op til. Portalen giver en overordnet score, men forklarer også de enkelte testresultater og henviser til yderligere information i blandt andet CFCS' vejledninger. CFCS bidrog med teknisk sparring og udbredelse af kendskab til platformen og fortsætter samarbejdet i 2021.

Internationalt webinar om styrket maritim cybersikkerhed

I Danmark og rundt om i verden rammes søfart og havne jævnligt af hackerangreb. Den største trussel kommer fra kriminelle hackere, der er økonomisk motiveret, og hackere fra fremmede stater, som udspionerer virksomhederne. Danmark er en af verdens største søfartsnationer, og søfart er Danmarks største eksporterhverv. Derfor har de forskellige hackergrupper betydelig interesse i danske organisationer i sektoren.

I 2020 var CFCS og Søfartsstyrelsen værter for et internationalt webinar om styrket maritimt myndighedssamarbejde om cybersikkerhed. Webinaret blev arrangeret i samarbejde med myndigheder fra USA og Nederlandene med deltagende myndigheder fra en lang række lande. Temaet for webinaret var implementering af den nye internationale regulering på området, som betyder, at rederierne fra 2021 skal medtage cyberrisici i skibenes systemer til sikkerhedsledelse.

Rådgivning
CFCS arbejder tæt sammen med de decentrale cyber- og informations-sikkerhedsenheder i de seks samfundskritiske sektorer blandt andet i et fælles videndelingsnetværk (DCIS-forum). DCIS-forum mødtes fem gange i 2020, hvor fokus blandt andet var på at udbygge samarbejdet om deling af information om hændelser i en fælles malwareanalyse-platform (MISP), videndelig i lyset af COVID-19-udfordringer og afholdelse af den første tværsektorielle cyberberedskabsøvelse i Danmark nogensinde, hvori også private virksomheder deltog.

Tværsektoriel beredskabsøvelse den 19. november 2020
De samfundskritiske sektorer og CFCS gennemførte den første tværgående øvelse af sin art den 19. november 2020. Øvelsen blev planlagt i et tæt samarbejde mellem centeret og repræsentanter fra de deltagende myndigheder og virksomheder.

Formålet var at undersøge og afprøve kommunikation og videndeling mellem myndighederne og virksomhederne i tilfælde af et større cyberangreb, som påvirker flere sektorer samtidig. Der var tale om en såkaldt skrivebordsøvelse, hvor deltagerne undervejs modtog forskellige brikker af viden, som så skulle deles for, at alle hurtigst muligt kunne lægge det samlede puslespil.

I øvelsen blev Danmark ramt af et fiktivt cyberangreb. Gennem otte timer samarbejdede medarbejdere fra CFCS og en række myndigheder og virksomheder på tværs af de seks samfundskritiske sektorer (tele, energi, finans, sundhed, transport og søfart) intenst for at stoppe angrebet og begrænse skaderne.

Varsler
CFCS udsender løbende varsler i forbindelse med væsentlige cyberangreb, aktuelle cybertrusler, it-sikkerhedshændelser eller væsentlige sårbarheder, som kan have relevans for myndigheder og virksomheder. Varslerne indeholder konkrete tekniske anbefalinger og udarbejdes blandt andet med udgangspunkt i viden fra sensornetværket, der monitorerer netværkstrafikken til og fra de tilsluttede myndigheder og virksomheder. Situationscenteret benytter også tweets til at gøre opmærksom på trusler og sårbarheder med henblik på håndtering i relevant omfang.

Forskning og uddannelse
CFCS har inden for rammerne af forsvarsforliget udmøntet i alt 7,6 mio. kr. til forskning og uddannelse i 2019-20. I 2020 er der afholdt sommerskole og cyberdage i samarbejde med en række uddannelsesinstitutioner med fokus på cybersikkerhed bredt og mere tekniske emner. Derudover er der i 2020 udmøntet støtte til fem forskningsprojekter samt midler til fortsat at færdiggøre en række e-læringsmoduler samt udvikle en træningsplatform til netværksanalyse. Der har også været fokus på børn og unge, herunder givet støtte til seks konkrete projekter med fokus på børn og unges cybersikkerhed. Endelig samarbejder CFCS med Danish Hub for Cybersecurity, der har til formål at fremme udviklingen af kompetencer inden for cybersikkerhed. Centeret har fra efteråret 2020 indgået i CyberHub'ens bestyrelse.

Uddannelse af cyberværnepligtige
CFCS har i 2020 støttet forsvaret med oprettelsen af en uddannelse for cyberværnepligtige og planlagde og gennemførte blandt andet den afsluttende øvelse for det første hold. Centeret simulerede under øvelsen et angreb på netværk, som de værnepligtige skulle forsvare under anvendelse af færdigheder, de har lært under værnepligten. Øvelsen vil også blive gennemført for de kommende hold af cyberværnepligtige.

Støtte og rådgivning i Grønland og på Færøerne
I 2020 blev Lov om Center for Cybersikkerhed sat i kraft i Grønland. CFCS har etableret monitorering hos centrale grønlandske myndigheder, hvilket i højere grad end tidligere giver centeret mulighed for at bistå grønlandske myndigheder i forbindelse med eventuelle cyberangreb. CFCS har sendt varsler direkte til grønlandske myndigheder med henblik på håndtering af både generelle og konkrete sårbarheder og delt råd og anbefalinger om cyber- og informationssikkerhed i forbindelse med COVID-19-pandemien med myndigheder og virksomheder i Grønland og på Færøerne. CFCS har også rådgivet om etablering af klassificerede elektroniske informationssystemer hos myndighederne i Grønland og på Færøerne.

Sikker kommunikation i staten
Regeringen har besluttet, at der skal etableres mulighed for, at statslige myndigheder kan anvende et klassificeret netværk med højt sikkerhedsniveau til at kommunikere med hinanden samtidig med, at adgang til internettet kan foregå effektivt og brugervenligt. Statens it har derfor i tæt samarbejde med CFCS og Forsvarsministeriets Koncern It designet og udviklet en it-løsning, som kan opfylde dette behov. Løsningen forventes udrullet og afprøvet i en indledende fase i foråret 2021.

Sikkerdigital.dk
Sikkerdigital.dk er myndighedernes fælles portal for råd og vejledning til en sikker digital hverdag. Her samles vejledninger og konkrete værktøjer samt gratis tilbud om online test, kurser, e-læring og brugbare apps, som henvender sig til borgere, virksomheder og myndigheder.

Portalen er etableret af Digitaliseringsstyrelsen og Erhvervsstyrelsen i samarbejde med CFCS, der bidrager med kendskab til cybertruslerne og med teknisk viden om, hvordan de imødegås. Portalen blev åbnet som led i den nationale strategi for cyber- og informationssikkerhed fra 2018.

Portalen findes på sikkerdigital.dk

Telesektorens decentrale cyber- og informationssikkerhedsenhed
CFCS er myndighed for informationssikkerhed og beredskab i telesektoren og indgår derfor også i den decentrale cyber-og informationssikkerhedsenhed i telesektoren, hvor de 11 største teleoperatører deltager. Enheden har i sommeren og efteråret 2020 udarbejdet en revideret version af "Sårbarheds- og risikovurderingen for telesektoren i Danmark". Derudover har fokus blandt andet været på samarbejde med den nye

EnergiCERT, på at styrke videndelingen gennem en række erfaringsudvekslingsmøder i sektoren om awareness, leverandørstyring og SPAM/spoofing samt deling af information om hændelser.

Cybersikkerhedsmåned i oktober

Cybersikkerhedsmåneden i 2020 bød på en lang række aktiviteter og kampagner. Måneden har til formål at bidrage til at styrke cyber- og informationssikkerheden blandt borgere, myndigheder og virksomheder og løfte danskernes viden om sikker digital adfærd og er en del af den europæiske cybersikkerhedsmåned. Ligesom det forudgående år stillede mange myndigheder, virksomheder og organisationer deres viden gratis til rådighed. Gennem hele måneden var det muligt at booke eksperter til oplæg om alt fra cybertruslen over effektive awareness-programmer til cybersikkerhed for børn.

Cybersikkerhedsrådet afholdt den 2. oktober et webinar med fokus på konkrete råd om bedre cybersikkerhed, hvor mere end 700 personer deltog, og DK Hostmaster lancerede i samarbejde med en lang række myndigheder og interesseorganisationer værktøjet sikkerpånettet.dk, hvor virksomheder nemt kan få styr på deres internetsikkerhed.

Læs mere om cybersikkerhedsmåneden på sikkerdigital.dk/ncsm

Tilsynsopgaver i 2020

Opgaver som national it-sikkerhedsmyndighed
Som national it-sikkerhedsmyndighed har CFCS til opgave at sikkerhedsgodkende it-systemer og -installationer, som anvendes til behandling af klassificerede informationer. CFCS har i 2020 udstedt 60 it-sikkerhedsgodkendelser.

Centeret fører også tilsyn med informationssikkerhed og kryptosikkerhed i relation til klassificeret information i elektroniske informationssystemer. Der er i 2020 gennemført tre tilsyn ved offentlige myndigheder, som arbejder med klassificerede informationer. Fire planlagte tilsyn i 2020 er enten blevet aflyst eller udskudt til 2021 grundet COVID-19-pandemien. Tilsynet har i 2020 særligt haft fokus på it-risikovurdering i forhold til elektronisk anvendelse af klassificeret information og myndighedens systemspecifikke sikkerhedsforskrifter.

CFCS har i 2020 desuden støttet Forsvarsministeriet med seks tilsyn med styringen af informationssikkerheden på Forsvarsministeriets område. Tilsynet har haft hovedfokus på myndighedernes ledelsessystem for informationssikkerhed i henhold til ISO27001-standarden.

Tilsynsopgaver på teleområdet
CFCS har som led i sin lovbestemte rolle som tilsynsmyndighed for informationssikkerhed og beredskab på teleområdet gennemført tilsyn hos udvalgte teleudbydere. Der er gennemført fem tilsyn med hovedfokus på at sikre, at teleudbyderne har gennemført en risikovurdering, der tager stilling til risikoen for tab af tilgængelighed i de net og tjenester, der udbydes. Herudover er der i 2020 påbegyndt fem tilsyn med andre teleudbydere vedrørende krav til sikkerhedsgodkendelse af blandt andet personer på beredskabsområdet.

EU-samarbejdet mv. i 2020

Fokus på EU-området i 2020 har blandt andet været på arbejdet med 5G-værktøjskassen, cybersikkerhedscertificering og forberedelse af Kommissionens forslag om et revideret NIS-direktiv.

Europæisk samarbejde om 5G-sikkerhed og lovforslag om leverandørsikkerhed i den kritiske teleinfrastruktur

Som myndighed for beredskab og informationssikkerhed i telesektoren har CFCS været involveret i et omfattende europæisk samarbejde om 5G-sikkerhed, der blandt andet har resulteret i Kommissionens værktøjskasse for cybersikkerhed i medlemslandenes 5G-netværk fremlagt i januar 2020. Værktøjskassen indeholder forskellige redskaber til implementering af eksempelvis leverandørsikkerhed og tekniske minimumskrav. Der følges løbende op på status for landenes arbejde med redskaberne i værktøjskassen, og CFCS har indrapporteret ad to omgange til Kommissionen i 2020.

Derudover har CFCS i 2020 ydet assistance til Forsvarsministeriet vedrørende teletekniske afklaringer i forbindelse med udarbejdelse af forslag til lov om leverandørsikkerhed i den kritiske teleinfrastruktur. Lovforslaget er vedtaget i Folketinget i maj 2021.

Cybersikkerhedscertificering

ENISA har i 2020 påbegyndt arbejdet med cybersikkerhedscertificering i EU med udgangspunkt i den europæiske ramme for certificering af cybersikkerhed, som blev etableret i 2019. Som led i arbejdet skal medlemslandene etablere en national certificeringsmyndighed, der får det overordnede ansvar for certificeringsordninger i informations- og kommunikationsteknologi i Danmark. Myndigheden skal være oprettet senest i juni 2021 og planlægges efter politisk behandling etableret under Sikkerhedsstyrelsen, hvor Erhvervsstyrelsen får ansvaret for EU-koordination. CFCS bidrager med faglig viden og sparring til begge myndigheder og vil i samarbejde med Sikkerhedsstyrelsen medvirke til de konkrete certificeringer.

Revision af NIS-direktivet

NIS-direktivet skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer inden for en række samfundsvigtige sektorer i hele EU.

NIS-direktivet

CFCS er nationalt kontaktpunkt i regi af NIS-direktivet (EU's direktiv om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen). Centeret har i den forbindelse deltaget i NIS-samarbejdsgruppens otte møder i 2020 og i samarbejdet mellem de europæiske CSIRT'er (Computer Security Incident Response Teams), der omhandler videndeling og koordination af operative anliggender. CFCS repræsenterer desuden Danmark i bestyrelsen for EU's Cybersikkerhedsagentur, ENISA.

Kommissionen har i 2020 gennemført en evaluering af NIS-direktivets virkemåde med inddragelse af medlemsstaterne og fremsatte i december 2020 et forslag til revision af direktivet, som indeholder en væsentlig udvidelse i bredden af direktivets dækningsområde og i dybden med en række nye krav til cybersikkerhed i de omfattede virksomheder og myndigheder samt til medlemsstaternes tilsyn. Forslaget lægger også op til en udvidelse af samarbejdet mellem medlemsstaterne ved cybersikkerhedshændelser og ved identifikation af sårbarheder og risici.

CFCS' deltagelse i internationale øvelser i 2020

BlueOlex
CFCS deltog i 2020 i den europæiske øvelse i cybersikkerhed, BlueOlex, der blev afholdt for anden gang i september. Øvelsen var en mulighed for at teste det nyetablerede CyCLONe-netværk og havde fokus på samarbejde og deling af information på operativt niveau i tilfælde af en større cybersikkerhedshændelse, hvor flere vigtige sektorer på tværs af EU var sat ud af drift.

Cyber Europe
CFCS deltog i forberedelserne af "CyberEurope", der afholdes hvert andet år, men den er grundet COVID-19-pandemien udskudt til 2022. Øvelsen skulle have taget udgangspunkt i et scenarie om et grænseoverskridende cyberangreb mod sundhedssektoren i Europa og ville have øvet cyberberedskab på både nationalt og europæisk niveau. Sidste CyberEurope fandt sted i 2018 med over 1.000 deltagere på tværs af EU.

Nato Cyber Coalition
CFCS deltog i NATO's største cyberøvelse, Cyber Coalition 2020, der fandt sted fra den 16. til 20. november 2020. Øvelsen havde omtrent 1.000 deltagere fra 28 NATO-lande og en række partnernationer. Øvelsens formål var at styrke NATO-alliancens evne til at modstå cybertrusler og gennemføre militære cyberoperationer samt at øve NATO's og landenes nationale procedurer for videndeling, situationsoverblik og beslutningsevne.

Cyber Spartan
CFCS var også en del af den britiske cybersikkerhedsøvelse, Cyber Spartan, hvor over 400 deltagere fra UK, Frankrig og Danmark øvede deres cyberkapabiliteter og cyberforsvar. Øvelsen blev afholdt for fjerde gang i starten af december 2020 og forventes fremover at blive afholdt årligt.

Publikationer i 2020

Vejledninger

Gode råd om hjemmearbejde
Kort vejledning om cybersikkerhed ved hjemmearbejde udgivet i marts 2020 i forbindelse med COVID-19-pandemien.

Q&A om cybersikkerhed ved hjemmearbejde under corona-krisen
Kort vejledning om cybersikkerhed ved hjemmearbejde udgivet i marts 2020 i forbindelse med COVID-19-pandemien.

Sikker brug af kommunikations- og samarbejdsplatforme
Kort vejledning til sikker brug af kommunikations- og samarbejdsplatforme udgivet i marts 2020 i forbindelse med COVID-19-pandemien.

Cybersikker tilbagevenden til arbejdspladsen
Kort vejledning om cybersikker tilbagevenden til arbejdspladsen udgivet i april 2020 i forbindelse med COVID-19-pandemien.

Særlige opmærksomhedspunkter omkring adgang til SCADA-systemer fra hjemmearbejdspladser
Råd om adgang til SCADA-systemer fra hjemmearbejdspladser udgivet i forbindelse med COVID-19-pandemien.

Phishing. Beskyt organisationen mod phishing-angreb
Vejledningen hjælper organisationer med at imødegå truslen fra phishing-mails i form af en række konkrete anbefalinger, der kan bidrage til organisationens arbejde med at beskytte sig mod phishing-angreb, herunder sikkerhedstiltag målrettet henholdsvis modtagelsen af og udsendelse af mails.

Reducér risikoen for ransomware
Vejledningen giver en række anbefalinger, som organisationer kan følge for at reducere sandsynligheden for at blive ramt af ransomware-angreb.

Sikker håndtering af domæner
Vejledning giver en række anbefalinger, der hjælper organisationer med at håndtere sine domæner på sikker vis. Vejledningen kommer med råd til administration og vedligeholdelse af domæner samt tekniske råd omkring navneserverdesign og DNSSEC.

TLS-vejledning
Publikationen henvender sig primært til personer, der skal fastlægge sikkerhedskrav til brugen af Transport Layer Security (TLS).

Logning - en del af et godt cyberforsvar
Vejledningen indeholder en konkret liste over de steder i netværket, hvor man med fordel kan generere logs fra. Vejledningen indeholder også en kort beskrivelse af de organisatoriske overvejelser, man skal gøre sig for at sikre, at logningen bidrager til cybersikkerheden.

Cybersikkerhed for bestyrelser
(i samarbejde med Bestyrelsesforeningen, Kromann Reumert og Industriens Fond)
Vejledningen er en indføring i bestyrelsens arbejde med cyber-og informations-sikkerhed og opstiller en række anbefalinger og spørgsmål, så bestyrelserne kan sparre med og udfordre direktionerne om virksomhedernes cyber-og informationssikkerhed. Vejledningen er opdateret ultimo 2020.

Opdateret DDoS-vejledning: Beskyt mod DDoS
Vejledningen kommer med en række anbefalinger til, hvordan man kan forebygge og forsinke angreb samt til, hvordan et eventuelt angreb kan håndteres.

Opdateret passwordvejledning
Vejledningen beskriver nogle af de mest anvendte angrebsmetoder, som hackere benytter sig af, samt nogle af de eksisterende udfordringer ved passwords. Den indeholder desuden en række tips til forskellige niveauer i en organisation med det formål at tilpasse passwordsikkerheden til den adfærd og risikoprofil, der karakteriserer organisationen.

Trusselsvurderinger

Hovedparten af trusselsvurderingerne er udgivet både på dansk og engelsk.

Trusselsvurderingen: Hackere misbruger legitime programmer i cyberangreb
Vurderingen beskriver en angrebsteknik, hvor hackere misbruger ofrenes egne programmer til at udføre cyberangreb. Teknikken kaldes "living off the land". Trusselsvurderingen indeholder anbefalinger til, hvordan truslen kan imødegås.

Trusselsvurdering: Cybertruslen mod skibes operationelle systemer
Cyberangreb kan påvirke de operationelle systemer og derved have negativ indflydelse på sejlads- og skibssikkerheden. Vurderingen supplerer den generelle vurdering af cybertruslen mod søfart.

Trusselsvurdering: Cybertruslen gælder også ved hjemmearbejde
Cybertruslen gælder også for brugen af hjemmearbejdspladser, der pga. den aktuelle COVID-19-pandemi anvendes hyppigere end normalt.

Trusselsvurdering: Cybertruslen mod Danmark under COVID-19-pandemien
Der er altid hackere, der forsøger at udnytte aktuelle begivenheder, udviklinger eller vilkår til deres fordel. Det er også tilfældet med COVID-19-pandemien, som hackere eksempelvis har udnyttet ved at sende phishing-mails, der har COVID-19 som tema.

Trusselsvurdering: Cybertruslen mod Danmark 2020
Formålet med denne årlige, nationale trusselsvurdering er at redegøre for den samlede cybertrussel, der møder danske myndigheder og virksomheder. Truslen er størst fra cyberkriminalitet og cyberspionage.

Trusselsvurdering: Cybertruslen mod søfart og havne
Trusselsvurderingen redegør for cybertrusler, der er rettet mod den danske søfarts-sektor. Søfartssektoren i Danmark er vigtig for samfundets funktion, stabilitet og økonomi. Vurderingen afløser den hidtidige trusselvurdering af truslen mod søfartssektoren fra 2019.

Trusselsvurdering: Drømmer cyberkriminelle om tillidsfulde relationer?
Veletablerede samarbejdsrelationer, arbejdsdeling og udveksling af tjenester i det kriminelle miljø bidrager til den meget høje trussel fra cyberkriminalitet i almindelighed og målrettede ransomware-angreb i særdeleshed.

Trusselsvurdering: HR-afdelinger rammes også af målrettede cyberangreb
Hackere forsøger at bruge HR-afdelinger som en nem vej ind i organisationer. Vurderingen indeholder også anbefalinger til, hvordan organisationer kan understøtte deres HR-afdelinger med både tekniske tiltag og awareness.

Trusselsvurdering: Cyberangreb mod it-serviceudbydere udgør en alvorlig leverandørtrussel
Hackere udnytter den tillid og adgang, som it-serviceudbydere har hos deres kunder. Ved at angribe netop disse virksomheder kan hackere kompromittere mange af udbydernes kunder.

Trusselsvurdering: Cybertruslen fra phishing-mails
Vurderingen går i dybden med, hvordan hackere benytter phishing- og spear phishing-mails i deres forsøg på at kompromittere virksomheder eller franarre dem følsomme oplysninger.

Trusselsvurdering: Cyberkriminelle opruster i pandemiens skygge.
Flere kriminelle hackergrupper har over foråret og sommeren 2020 fornyet deres værktøjer, samarbejdsrelationer og aktiviteter. Der er flere årsager til forandringerne, herunder COVID-19-pandemien, pres fra myndigheder og it-sikkerhedsfirmaer og nye indtjeningsmuligheder.

Trusselsvurdering: Cyberkriminelle spænder den digitale tommelskrue
Kriminelle hackere udvider afpresningen i forbindelse med ransomware-angreb med trusler om læk eller salg af følsomme informationer i såkaldt dobbelt afpresning.

Trusselsvurdering: Cybertruslen mod finanssektoren
Den danske finanssektor står over for en meget høj trussel fra cyberkriminalitet. Angreb fra cyberkriminelle kan være avancerede og få omfattende konsekvenser. Potentielt kan cyberkriminalitet forstyrre tilgængeligheden af den danske finanssektors ydelser.

Undersøgelsesrapporter

Undersøgelsesrapport: Glemmer du, så husker hackerne
Rapporten beskriver, hvordan en dansk organisation blev hacket fem gange på to år. Det skete via en sårbarhed, som havde været mulig at opdatere og dermed sikre sig mod i mere end seks år.

Undersøgelsesrapport: Anatomien af målrettede ransomware-angreb
Rapporten kortlægger, hvordan målrettede ransomware-angreb typisk forløber og giver konkrete anbefalinger til, hvordan myndigheder og virksomheder kan beskytte sig endnu bedre. Forløbet er generaliseret, men baserer sig på indsigt fra virkelige hændelser.

Andre publikationer

CFCS opdaterede i forbindelse med cybersikkerhedsmåneden i oktober 2020 sin liste med ordforklaringer, der viser, hvordan CFCS bruger ord og begreber inden for cybersikkerhed. Ordforklaringen kan findes på CFCS' hjemmeside cfcs.dk.

Twitter
CFCS har i løbet af 2020 udsendt 323 tweets fra @Cybersikkerhed, hvorfra CFCS tweeter bredt om cybersikkerhed, og 105 tweets fra Situationscenteret, @CFCSsitcen, hvorfra der tweetes om sårbarheder, varsler og rådgivning med et operativt og tidskritisk sigte.

@Cybersikkerhed: www.twitter.com/cybersikkerhed
@CFCSsitcen: www.twitter.com/CFCSsitcen

LinkedIn
CFCS har i løbet af 2020 lagt 160 opslag på LinkedIn, hvorfra centeret løbende deler nyheder, publikationer og jobopslag.

www.linkedin.com/company/center-for-cybersikkerhed

Eksempler på anonymiserede varsler udsendt af CFCS' situationscenter

Nedenstående varsler er anonymiserede versioner af udsendte varsler. Varsler fra CFCS' situationscenter er markeret efter Traffic Light-protokollen (TLP). Markeringen fortæller modtageren, hvorvidt eller hvordan indholdet af dokumentet kan deles på baggrund af, hvor følsomme informationerne er. TLP-skalaen er opdelt i fire niveauer (RED, AMBER, GREEN, WHITE), som indikerer, hvor følsomme informationerne er, og hvordan de må anvendes af modtageren. RED anvendes til de mest følsomme informationer, som ikke må deles med andre, og WHITE anvendes til de mindst følsomme oplysninger, som må deles frit.

Anonymiseret varsel: Nye ransomware-angreb mod danske virksomheder (oprindeligt TLP:AMBER)

Til den it-sikkerhedsansvarlige
Center for Cybersikkerhed (CFCS) har viden om, at virksomheder i mindst to forskellige sektorer i Danmark er ramt af ransomware-angreb.

Virksomhederne har inden for de seneste dage fået krypteret data af den samme type malware. Det er endnu ikke bekræftet, hvilken type malware, der er tale om.

Det er muligt, at det er en variant af en malware, der kaldes Sodinokibi eller REvil. Nederst i varslet er der indsat en række IOC'er fra denne malware. Da malwaren REvil bliver anvendt af flere forskellige aktører, er den forbundet til mange forskellige angrebsmetoder. CFCS opfordrer derfor til, at man løbende holder sig orienterede om IOC'er knyttet til REvil.

REvil er kun én blandt flere malware, der bliver brugt i ransomware-angreb mod mål i Danmark og Europa i disse måneder. Andre kendte malware er eksempelvis Ryuk, BitPaymer, Doppel-Paymer, RobbinHood, LockerGoga, Clop, Dharma og MegaCortex.

Truslen fra cyberkriminalitet, herunder ransomware-angreb, er MEGET HØJ. Det betyder, at det er meget sandsynligt, at danske virksomheder og myndigheder vil blive ramt af cyberkriminalitet på kort sigt. CFCS ser flere og flere ransomware-angreb, hvor hackerne bruger tid på at orientere sig og bevæge sig rundt i deres ofres systemer, før de krypterer data. Hackerne gør dette for at kunne ramme ofret, hvor det gør mest ondt. Hackerne forlanger derefter typisk meget høje løsesummer for at gøre data tilgængelige. Ofte er der tale om flere millioner kroner.

Man kan læse mere om ransomware-angreb, hvordan de foregår samt anbefalinger til at imødegå dem i CFCS' trusselsvurdering "Digitale gidseltagere på storvildtjagt".

Den kan findes på CFCS' hjemmeside eller via følgende link:
https://cfcs.dk/da/cybertruslen/trusselsvurderinger/malrettet-ransomware/

IOC'er:

Payment:
hxxp:// decryptor[.]top/
hxxp:// aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd[.]onion/

Readme:
<XXXXXXX>-readme.txt

SHA 256 Hash:

fe25f8c22488172bc5091cafc1c4e598ed7bb3b3e6ad2934243919c93c8f2b83
aedf3065010292103ad05099450a54c013b30e73b2aec76e6ecb8fc721cb14c1
ee792ec30391da23bd4611eee7cde00774cc362cd7265a4155bfa3090a3efb67

Vejledning
Center for Cybersikkerhed har udarbejdet en række vejledninger om cyber- og informationssikkerhed, herunder "Cyberforsvar der virker", som er en konkret og prioriteret plan til at komme i gang med cyber- og informationssikkerhedsarbejdet. Alle vejledningerne kan findes på centerets hjemmeside og kan frit benyttes.

Kontakt
Hvis du har spørgsmål til ovenstående varsel eller ønsker at høre mere om mulighederne for rådgivning, er du velkommen til at kontakte Center for Cybersikkerhed på telefon 33 32 55 80 eller på mail cert@cert.cfcs.dk.

Om Center for Cybersikkerhed
Center for Cybersikkerhed under Forsvarets Efterretningstjeneste har som hovedopgave at understøtte et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur, som samfundsvigtige funktioner er afhængige af.

Denne opgave løses blandt andet ved, at Center for Cybersikkerheds netsikkerhedstjeneste opdager, analyserer og bidrager til at imødegå avancerede cyberangreb mod myndigheder og virksomheder, der er beskæftiget med samfundsvigtige funktioner.

Anonymiseret varsel: Ny sårbarhed tillader hackere at kompromittere enheder som bruger Microsoft Teams

Til den it-sikkerhedsansvarlige
Center for Cybersikkerhed er blevet bekendt med en sårbarhed i Microsoft Teams. Sårbarheden tillader ondsindede aktører at sende arbitrær kode, i form af en harmløst udseende besked i en Teams chat. Så snart modtagere åbner chatten og ser beskeden, bliver den tilsendte kode eksekveret på deres enhed.

Yderligere information
Sårbarheden (CVE-2020-17091) er cross-platform, hvilket vil sige at den kan udnyttes mod Microsoft Teams på Windows (v1.3.00.21759), Linux (v1.3.00.16851), macOS (v1.3.00.23764) og web-klienten (teams.microsoft.com).

For yderligere oplysninger, venligst se nedenstående links.

https[:]//thehackernews[.]com/2020/12/zero-click-wormable-rce-vulnerability.html
https[:]//msrc[.]microsoft[.]com/update-guide/en-US/vulnerability/CVE-2020-17091

Anbefaling
Center for Cybersikkerhed anbefaler, at der overvejes passende modforanstaltninger for at sikre eventuelle enheder som benytter Microsoft Teams. Microsoft Teams version 1.3.00.13xxx og derover har patchet sårbarheden. Vi anbefaler derfor, at der køres opdatering af alle Microsoft Teams installationer.

CFCS opfordrer til, at indikatorer, tekniske konklusioner samt anden relevant viden om sikkerhedshændelsen i størst muligt omfang deles med sektorens DCIS.

Rådgivning
Center for Cybersikkerhed kan i nogle tilfælde bistå med rådgivning om cyber- og informationssikkerhed, herunder styring af informationssikkerhed og risikovurderinger. Center for Cybersikkerheds rådgivning tager som udgangspunkt afsæt i de vejledninger, der kan findes på centerets hjemmeside.

Vejledning
Center for Cybersikkerhed har udarbejdet en række vejledninger om cyber- og informationssikkerhed, herunder "Cyberforsvar der virker", som er en konkret og prioriteret plan til at komme i gang med cyber- og informationssikkerhedsarbejdet. Alle vejledningerne kan findes på centerets hjemmeside og kan frit benyttes.

Kontakt
Hvis du har spørgsmål til ovenstående varsel eller ønsker at høre mere om mulighederne for rådgivning, er du velkommen til at kontakte Center for Cybersikkerhed på telefon 33 32 55 80 eller på mail cert@cert.cfcs.dk.

Om Center for Cybersikkerhed
Center for Cybersikkerhed under Forsvarets Efterretningstjeneste har som hovedopgave at understøtte et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur, som samfundsvigtige funktioner er afhængige af.

Denne opgave løses blandt andet ved, at Center for Cybersikkerheds netsikkerhedstjeneste opdager, analyserer og bidrager til at imødegå avancerede cyberangreb mod myndigheder og virksomheder, der er beskæftiget med samfundsvigtige funktioner.

Anonymiseret varsel: Succesfuld shellcode injektion og kontakt med C2- IP (oprindeligt TLP:AMBER)

Til den it-sikkerhedsansvarlige
Center for Cybersikkerhed (CFCS) har konstateret shellcode injektion hos [myndighed/virksomhed] og efterfølgende observeret kontakt med en C2 IP.

Yderligere information
CFCS har i perioden 17/08-2020 – 27/08-2020 konstateret shellcode injektion hos [myndighed/virksomhed] og efterfølgende observeret kontakt med en C2 IP-adresse.

Både shellcode injektionen og C2 kontakten foregår på Microsoft Azure IP-adressen [IP-adresse] via HTTP. I alle tilfælde er Host headeren HTTP requestet sat denne IP-adresse, mens URI'en skifter afhængig af, om det er shellcode injektion eller C2 kanal. URI'erne er følgende:

[aktørens URI] – formodet C2 kanal
[aktørens URI] – Shellcode injektion

Kommunikationen foregår ved JSON-filerne [JSON-filnavn] og [JSON-filnavn]. Shellcoden er i værdien tilknyttet JSON-key'en [JSON-key] i filen [JSON-fil]

Eksempel: [tekniske detaljer]

Den første kontakt observeres d. 16/08 kl. 11:23:10 CEST fra den interne IP [myndighedens/virksomhedens interne IP-adresse] til [aktørens URI].
Den sidste kontakt observeres d. 26/8 kl. 07:27:20 fra [myndighedens/virksomhedens interne IP-adresse] til [aktørens URI]. Der er i alt 17 forskellige interne IP'er hos [myndighed/virksomhed], samt 2 eksterne IP'er, der har kontakt med C2 IP-adressen. IP'erne kan ses i nedenstående tabel.

[tabel med myndighedens/virksomhedens IP-adresser]

Vedlagt dette varsel er ligeledes en CSV-fil med mere info om trafikken.

Analysen af sagen pågår fortsat, og det er muligt, at der kommer mere info senere.

Anbefaling
Center for Cybersikkerhed anbefaler, at trafikken undersøges, og de ramte hosts lokaliseres, og at de tages af netværket. Det anbefales ligeledes, at de lokaliserede hosts ikke slukkes, så de kan analyseres.

CFCS er bekendt med, at der muligvis har været en Red Team øvelse hos [myndighed/virksomhed] i august. Det anbefales at finde ud af, om trafikken stammer herfra og informere CFCS, hvis det er tilfældet.

Ved bekræftelse af kompromittering er CFCS desuden interesseret i at få en eller flere af de påvirkede hosts til analyse.

CFCS opfordrer til, at indikatorer, tekniske konklusioner samt anden relevant viden om sikkerhedshændelsen i størst muligt omfang deles med sektorens DCIS.

Rådgivning
Center for Cybersikkerhed kan i nogle tilfælde bistå med rådgivning om cyber- og informationssikkerhed, herunder styring af informationssikkerhed og risikovurderinger. Center for Cybersikkerheds rådgivning tager som udgangspunkt afsæt i de vejledninger, der kan findes på centerets hjemmeside.

Vejledning
Center for Cybersikkerhed har udarbejdet en række vejledninger om cyber- og informationssikkerhed, herunder "Cyberforsvar der virker", som er en konkret og prioriteret plan til at komme i gang med cyber- og informationssikkerhedsarbejdet. Alle vejledningerne kan findes på centerets hjemmeside og kan frit benyttes.

Kontakt
Hvis du har spørgsmål til ovenstående varsel eller ønsker at høre mere om mulighederne for rådgivning, er du velkommen til at kontakte Center for Cybersikkerhed på enten telefon 33 32 55 80 eller på mail cert@cert.cfcs.dk.

Om Center for Cybersikkerhed
Center for Cybersikkerhed under Forsvarets Efterretningstjeneste har som hovedopgave at understøtte et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur, som samfundsvigtige funktioner er afhængige af.

Denne opgave løses blandt andet ved, at Center for Cybersikkerheds netsikkerhedstjeneste opdager, analyserer og bidrager til at imødegå avancerede cyberangreb mod myndigheder og virksomheder, der er beskæftiget med samfundsvigtige funktioner.

Kontakt
Center for Cybersikkerhed

CFCS kan inden for daglig kontortid (kl. 8-16) mandag-fredag kontaktes på telefon 33 32 55 80 eller på e-mail: cfcs@cfcs.dk.

Kontakt til cybersituationscenteret
Myndigheder og virksomheder, der beskæftiger sig med samfundsvigtige funktioner, kan i forbindelse med it-sikkerhedshændelser kontakte cybersituationscenteret på e-mail cert@cert.cfcs.dk eller døgnet rundt på telefon 33 32 55 80.

Kontakt til rådgivningsafdelingen
CFCS' rådgivningsafdeling kan kontaktes på telefon 33 32 55 80 eller på e-mail civil@cfcs.dk.

Kontakt til telemyndigheden
Kontakt til telemyndigheden ved CFCS kan ske på telefon 33 32 55 80 eller på e-mail tele@cfcs.dk.

Kontakt til policyafdelingen
CFCS' policyafdeling kan kontaktes på telefonen 33 32 55 80 eller på e-mail policy@cfcs.dk.

Følg Center for Cybersikkerhed
CFCS kan følges på Twitter og LinkedIn, hvor centeret løbende deler nyheder, publikationer og jobopslag.

Derudover kan CFCS' cybersituationscenter følges på Twitter, hvor der især tweetes om sårbarheder, varsler og råd med et operativt og tidskritisk sigte.

Twitter
@Cybersikkerhed: www.twitter.com/cybersikkerhed
@CFCSsitcen: www.twitter.com/CFCSsitcen

LinkedIn
www.linkedin.com/company/center-for-cybersikkerhed