Center for Cybersikkerheds beretning 2021

Indhold

CENTER FOR CYBERSIKKERHED

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

Forsideillustration: asharkyu/Shutterstock

1. udgave august 2022

Indledning

2021 blev præget af en række omfangsrige cyberangreb, som rakte ud over landegrænser og satte cyberforsvar endnu højere på dagsordenen i Danmark og internationalt: Fra SolarWinds-angrebet, der fortsat fyldte i 2021, til kritiske sårbarheder i Microsoft Exchange Server og opdagelsen af Log4j-sårbarheden i december. Ikke mindst blev ransomware-angrebet mod amerikanske Colonial Pipeline i maj 2021 dagsordenssættende som en illustration af, hvordan ransomware kan true kritiske forsyningskæder. Samtidig fortsatte det cyberkriminelle miljø med at bevæge sig mod øget professionalisering og specialisering, som har ledt til både flere og mere avancerede ransomware-angreb.

COVID-19 var fortsat en del af danskernes hverdag, og med distancearbejde, digitalt coronapas og online bestilling af test og vaccinationer understregede pandemien fordelene ved det høje niveau af digitalisering, som Danmark er kendt for. Men det blev også tydeligt, hvor afhængige vi er af digital sikkerhed på et højt niveau.

Center for Cybersikkerheds (CFCS) hovedopgave er at understøtte cybersikkerheden i den digitale infrastruktur, som samfundsvigtige funktioner er afhængige af. En række kernefunktioner i et samfund som det danske, for eksempel strøm til vores hospitaler, togsignaler og mobilnetværk, er helt afhængige af digital understøttelse. De ovennævnte begivenheder har derfor naturligt fyldt i centerets arbejde i 2021.

På de indre linjer har CFCS blandt andet haft fokus på den politiske aftale fra juni om udmøntning af en cyberpulje på 500 mio. kr., som blandt andet giver CFCS mulighed for at gennemføre en række tiltag, der skal styrke Danmarks cyberforsvar. I løbet af året har CFCS desuden bidraget betydeligt med vores faglighed og indsigt i cybertruslen til regeringens nye, ambitiøse nationale strategi for cyber- og informationssikkerhed, som blev lanceret i december.

Udviklingen på cyberområdet står aldrig stille, og derfor har CFCS i 2021 etableret en ny enhed, som skal være et videnscenter for sikkerhedsaspekter i den teknologiske udvikling. Enheden skal med et ben i forskningen og et ben i praktikken være på forkant med fremtidens teknologier – en viden, vi skal bruge, når vi rådgiver myndigheder og virksomheder, så Danmark kan være beredt på nye angrebsmetoder og nye sårbarheder.

CFCS' beretning beskriver centerets arbejde det foregående år med særligt fokus på centerets indsatser i forhold til forebyggelse og i forhold til opdagelse og håndtering af sikkerhedshændelser.

God læselyst.

Cybertruslen i 2021

Danmark har også i 2021 stået over for betydelige cybertrusler. Truslen fra både cyberkriminalitet og cyberspionage er fortsat **MEGET HØJ**, og danske myndigheder og virksomheder er blevet udsat for angreb fra både kriminelle og statslige aktører i løbet af året.

Truslen fra destruktive cyberangreb er **LAV**. CFCS opjusterede i maj 2022 trusselsniveauet for cyberaktivisme fra **LAV** til **MIDDEL**. Cyberterror udgør fortsat ikke en trussel mod danske virksomheder og myndigheder.

Truslen fra cyberspionage er vedvarende og fører løbende til cyberangreb mod danske mål. Nogle myndigheder og virksomheder er konstant udsat for en meget høj trussel, mens truslen kan variere over tid for andre. Truslen fra cyberspionage er drevet af økonomiske og politiske motiver og er særligt rettet mod Udenrigsministeriets og Forsvarsministeriets myndighedsområder, men også mod myndigheder og virksomheder inden for samfundsvigtige områder. CFCS hævede i 2021 niveauet for truslen fra cyberspionage fra **HØJ** til **MEGET HØJ** for transportsektoren samt danske universiteter og forskning.

Danmark bliver løbende udsat for mange forskellige typer cyberkriminalitet, der – ligesom andre typer kriminalitet – generelt baserer sig på forskellige former for tyveri, bedrageri og afpresning. Næsten alle danske borgere og virksomheder bliver udsat for forsøg på cyberkriminalitet. Nogle typer cyberkriminalitet går efter at ramme så mange potentielle ofre som muligt, eksempelvis gennem phishing spredt til tusinder af modtagere i Danmark og andre lande. Andre typer cyberkriminalitet går mere målrettet efter myndigheder og virksomheder, hvor det potentielle udbytte fra det enkelte offer kan løbe op i millioner af kroner.

Afpresning gennem ransomware-angreb er aktuelt den mest synlige og mest alvorlige trussel fra cyberkriminalitet mod det danske samfund. Her krypterer kriminelle centrale it-systemer hos myndigheder og virksomheder for derefter at afkræve ofrene en løsesum mod at låse systemerne op igen. Ofrene bliver også ofte truet med offentliggørelse af stjålne data, hvis løsesummen ikke betales.

Der er i de senere år sket en øget professionalisering og specialisering i det cyberkriminelle miljø, der har ledt til både flere og mere avancerede ransomware-angreb.

Center for Cybersikkerheds indsatser i 2021

CFCS' indsatser i 2021 afspejler et år, hvor cybertruslen fyldte, men hvor cybersikkerheden samtidig blev opprioriteret med en bred aftale om et styrket dansk cyberforsvar samt en ny ambitiøs national strategi for cyber- og informationssikkerhed. Fokus var i 2021 overordnet på:

- Bred rådgivning om cybersikkerhed og briefinger om trusselsbilledet til myndigheder og virksomheder, herunder tæt dialog med samfundsvigtige områder (som energi, tele, finans, sundhed, transport og søfart) og Forsvaret.

- Håndtering af cyberhændelser og kritiske sårbarheder, herunder efterdønningerne af SolarWinds-angrebet fra december 2020, kritiske sårbarheder i Microsoft Exchange Server i foråret og en alvorlig sårbarhed i it-værktøjet "Apache Log4j", som blev opdaget i december 2021.

- Etablering af et nordatlantisk rådgivningsteam med henblik på at styrke Grønlands og Færøernes cyberforsvar og dermed også løfte cyber- og informationssikkerheden i Rigsfællesskabet som helhed.

- Etablering af et nyt videnscenter for sikkerhedsaspekter i den teknologiske udvikling, der skal samarbejde med uddannelsesinstitutioner og virksomheder samt være bindeled til nationale og internationale forsknings- og udviklingsfora inden for nye teknologier og cybersikkerhed.

- Udbygning af CFCS' sensornetværk til myndigheder og virksomheder af samfundsvigtig karakter for at skabe overblik over det aktuelle cybertrusselsbillede i Danmark samt give mulighed for omfattende varsling fra situationscenteret.

- Bred aftale i Folketinget om et styrket dansk cyberforsvar med udmøntningen af 500 mio. kr. fra indeværende forsvarsforlig, der betyder en markant styrkelse af CFCS' muligheder for at opdage, advare om og beskytte mod cyberangreb.

- Udarbejdelse af en ny national strategi for cyber- og informationssikkerhed, der blandt andet stiller en række nye sikkerhedskrav til ministerområder, der har ansvar for samfundsvigtige funktioner eller samfundskritiske it-systemer, arbejdet med 5G-sikkerhed i EU og arbejdet 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).

Aftale om et styrket dansk cyberforsvar
I juni 2021 blev der indgået en bred aftale i Folketinget om at styrke Danmarks evne til at imødegå den stigende cybertrussel rettet mod virksomheder, myndigheder og borgere. Aftalen udmønter 500 mio. kr. fra indeværende forsvarsforlig, som fordeles til hele Forsvarets koncern, herunder KDO og Hjemmeværnet. Aftalen indebærer blandt

andet en markant styrkelse af CFCS' evne til at opdage, advare om og beskytte mod cyberangreb. Desuden afsættes der midler til at øge CFCS' rådgivning og støtte, ligesom den overordnede indsats inden for uddannelse, forskning og vidensdeling på cyberområdet opprioriteres. Konkret består aftalen af en række elementer inden for følgende hovedinitiativer: 1) datamonitorering og varsling, 2) cyberhjemmeværn, 3) cyberindsatshold, 4) teknisk bolværk, 5) rådgivning og decentral understøttelse, 6) uddannelse, forskning og videndeling, 7) offensive værktøjer og 8) cyberforsvar i Rigsfællesskabet.

Ny national strategi for cyber- og informationssikkerhed
Regeringen præsenterede i december 2021 en ny national strategi for cyber- og informationssikkerhed, som afløser den tidligere strategi fra 2018. Den nye strategi hæver ambitionsniveauet for cybersikkerheden i Danmark og stiller blandt andet en række nye sikkerhedskrav til ministerområder, der har ansvar for samfundsvigtige funktioner eller samfundskritiske it-systemer. Med strategien igangsættes også en række indsatser med fokus på at øge kompetenceniveauet og ledelsesforankringen inden for cyber- og informationssikkerhed. Strategien sætter ligeledes ind på vidensopbygning blandt borgere og styrker Danmarks deltagelse i den internationale kamp mod cybertruslen.

CFCS har i 2021 været en af de væsentlige bidragsydere i forbindelse med udarbejdelsen af den nye nationale strategi. Bidragene har blandt andet taget afsæt i CFCS' betydelige indsigt i cybertruslen mod særligt de samfundsvigtige områder og centerets tekniske kompetencer inden for cybersikkerhed. Strategien er udarbejdet i regi af en tværministeriel styregruppe, der har delt formandskab mellem CFCS og Digitaliseringsstyrelsen, som hører under Finansministeriet.

Strategisk dialog med myndigheder og virksomheder
En effektiv sikring af den kritiske it-infrastruktur og beskyttelse mod cyberangreb forudsætter, at CFCS indgår i et løbende og konstruktivt samspil med væsentlige interessenter i samfundet. Derfor har CFCS også i 2021 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 inden for samfundsvigtige områder som energi, tele, finans, sundhed, transport og søfart. Derudover har centeret et tæt samarbejde med blandt andre politiet, herunder Politiets Efterretningstjeneste (PET), samt Digitaliseringsstyrelsen og Erhvervsstyrelsen, som hører under Erhvervsministeriet.

CFCS faciliterer Strategisk Samarbejdsforum for Cybersikkerhed, som samler sikkerhedsgodkendte repræsentanter fra en række af de største danske virksomheder og brancheorganisationer inden for samfundsvigtige områder. Forummet mødtes tre gange i 2021 og drøftede blandt andet læring af SolarWinds-angrebet, kritiske sårbarheder i Microsoft Exchange Server og den nye nationale strategi for cyber- og informationssikkerhed, herunder hvordan strategien kan være med til at sikre cybersikkerheden endnu bredere i samfundet.

CFCS sekretariatsbetjener også det offentligt-private Cybersikkerhedsråd i samarbejde med Digitaliseringsstyrelsen. Rådet mødtes i alt syv gange i 2021 til fire ordinære

møder, hvor rådet blandt andet løbende har givet input til den nye nationale cyber- og informationssikkerhedsstrategi, og tre ekstraordinære møder om det digitale coronapas og MitID.

I regi af to arbejdsgrupper har Cybersikkerhedsrådet desuden givet input til tekniske minimumskrav for statslige myndigheder og drøftet kompetenceudfordringer på cyber- og informationssikkerhedsområdet, som mundede ud i et webinar i juni, hvor repræsentanter fra forskningsverdenen og danske virksomheder debatterede forskellige løsningsmodeller.

I oktober bidrog Cybersikkerhedsrådet til årets cybersikkerhedsmåned med webinaret "Kort og konkret om cybersikkerhed", som tilbød ekspertoplæg om vigtige emner inden for cybersikkerhed, som for eksempel logning i it-systemer og forebyggelse af ransomware.

CFCS deltog desuden i 2021 i en række nationale og internationale øvelser (se også afsnittet på side 25 vedrørende internationalt samarbejde) for at styrke det danske cyberberedskab. Blandt andet deltog CFCS i beredskabsøvelsen "TableTop21" den 10. juni 2021 afholdt af de samfundskritiske danske sektorer. Som telesektormyndighed deltog CFCS i øvelsen, blandt andet for at afprøve kommunikations- og beredskabsplaner for mail og telefoni samt deling af IoC'er (indicators of compromise) i en MISP (Malware Information Sharing Platform).

CFCS deltog blandt andet også i den finansielle sektors kriseberedskabsøvelse den 23. november 2021 i regi af FSOR – finansielt sektorforum for operationel robusthed. Under øvelsen skulle deltagerne koordinere viden modtaget i indspil om et fiktivt cyberangreb. CFCS modtog under øvelsen flere indspil og deltog på en række møder, hvor CFCS kunne bidrage med den akkumulerede viden. Formålet med øvelsen var at øve anvendelsen af finanssektorens kriseberedskabsplan- og organisering samt CFCS' interne procedurer.

Opdagelse og håndtering af sikkerhedshændelser i 2021

CFCS har i 2021 arbejdet på at forbedre grundlaget for en af centerets kerneopgaver: At opretholde et nationalt situationsbillede på cyberområdet. Det er blandt andet sket gennem en øget indsats i forhold til at udbygge CFCS' sensornetværk. En væsentlig forudsætning for indsatsen er et tæt samarbejde med øvrige myndigheder. Det gælder især myndigheder og virksomheder inden for de samfundsvigtige områder.

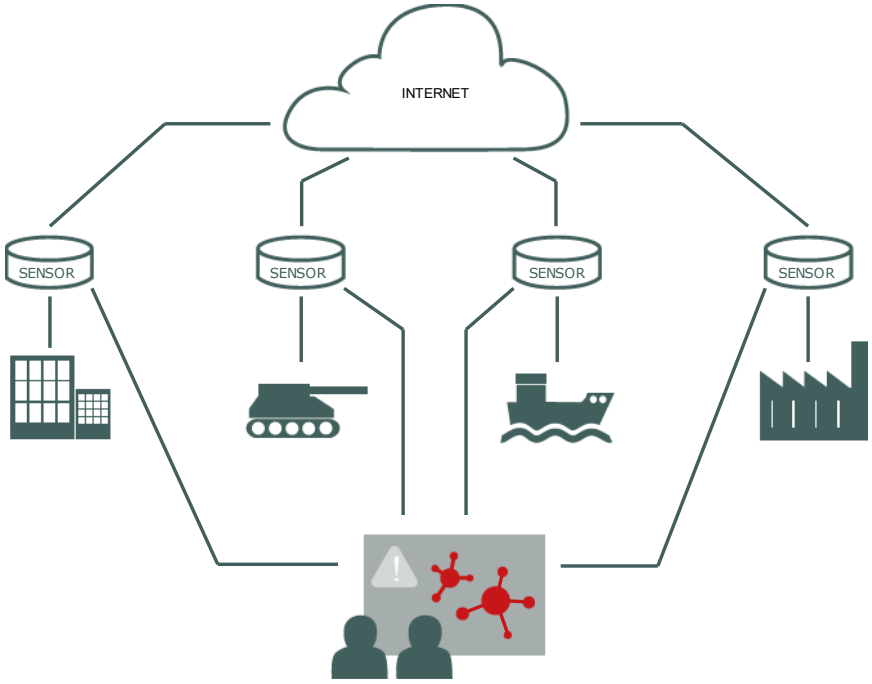
Øget operativt fokus på ransomware
CFCS har i 2021 øget sit fokus på ransomware-truslen mod samfundskritisk infrastruktur og virksomheder, der udfører samfundsvigtige funktioner. Formålet har været at styrke værnet mod ransomware-angreb, der kan ramme organisationer tilsluttet CFCS' sensornetværk, samt øvrige samarbejdspartnere. Det sker blandt andet ved at varsle om potentielle kompromitteringer, der kan lede til ransomware-angreb, samt ved at yde støtte til myndigheder og virksomheder, der er blevet ramt. På den baggrund har CFCS i 2021 været i kontakt med en række ofre for ransomware-angreb i Danmark og vil i 2022 fortsætte med at styrke kapaciteten til detektion, analyse og varsling på området.

Udbygning af sensornetværket
I 2021 har fokus været at sikre yderligere dækning og udbredelse af CFCS' to typer sensorer, NSS og NCSO. I alt er der i løbet af året indgået 44 nye tilslutningsaftaler med myndigheder og virksomheder.

CFCS har i løbet af 2021 fortsat udrulningen af den nye NCSO-sensor, hvis formål er at bidrage til det nationale cybersituationsoverblik. I 2021 har fokus for NSS-udrulningen været at sikre, at centraladministrationen er fuldt dækket. Dette arbejde fortsætter ind i 2022. CFCS har derudover haft løbende dialog med flere organisationer og private virksomheder i både Danmark og Grønland angående tilslutning til CFCS' sensornetværk.

I forhold til udrulningen af NCSO-sensorer har en række organisationer og virksomheder inden for de samfundsvigtige områder indgået tilslutningsaftaler med CFCS. Videreudvikling af denne indsats vil fortsætte i 2022 som et hovedfokusområde.

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 informationer, der bruges til at genkende forsøg på cyberangreb. Når der registreres potentielt ondsindet trafik, modtager CFCS en alarm.

Ved udgangen af 2021 havde CFCS i alt 265 tilsluttede myndigheder og virksomheder fordelt på 179 offentlige myndigheder og institutioner m.fl., 36 enheder i Forsvaret og 17 private virksomheder. Hertil kom 33 offentlige myndigheder og institutioner m.fl. i Grønland.

Varsler

CFCS udsender løbende varsler om sikkerhedshændelser, væsentlige sårbarheder og vigtige sikkerhedsopdateringer. 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. CFCS varsler altid bredest muligt. Når det er muligt at varsle bredt, benytter CFCS blandt andet Twitter til at gøre opmærksom på hændelser, sårbarheder og vigtige sikkerhedsopdateringer. Når CFCS er bekendt med, at en myndighed eller virksomhed er ramt af en sikkerhedshændelse, tager CFCS direkte kontakt til den berørte organisation.

Sikkerhedshændelser i 2021

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 2021. 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. Der eksisterer et stort mørketal for cyberangreb i Danmark, da kun relativt få hændelser indberettes til

CFCS.

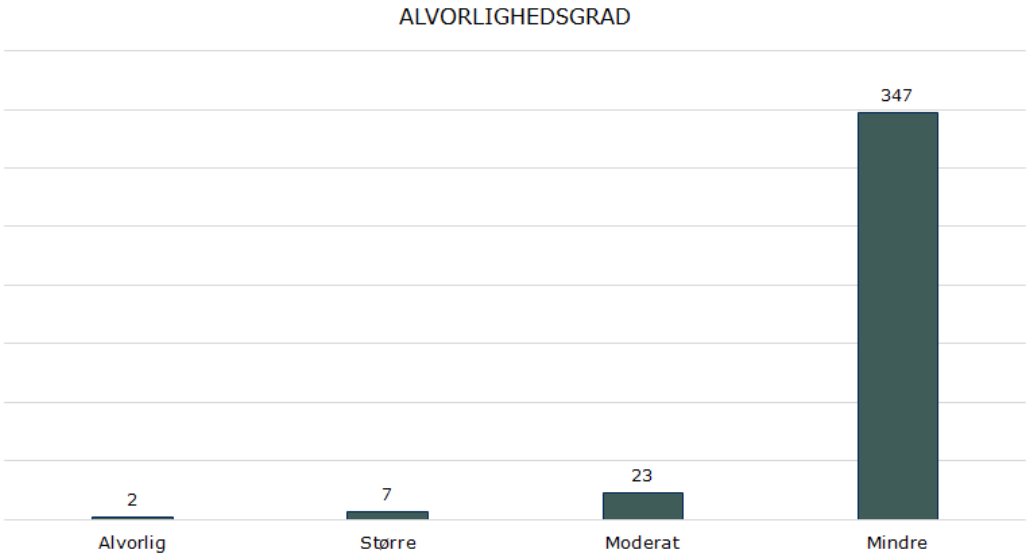
Definition af en sikkerhedshændelse
En hændelse, der negativt påvirker eller vurderes at ville kunne påvirke tilgængeligheden, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale tjenester.

Kilde: Lov om Center for Cybersikkerhed

Centeret har i 2021 håndteret 379 hændelser, der har haft effekt på den berørte organisation. Som det fremgår nedenfor, har hændelserne forskellige grader af alvorlighed. Tallet var i 2020 477 lignende hændelser. Ud over de 379 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 disse forsøg. I 2021 blev der observeret 5.677 tilfælde af potentielt 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 i 2021



Note: Tallene for sikkerhedshændelser er alene udtryk for antallet af hændelser, som CFCS har håndteret i 2021. 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.

Alvorlighedsgrader af sikkerhedshændelser

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.

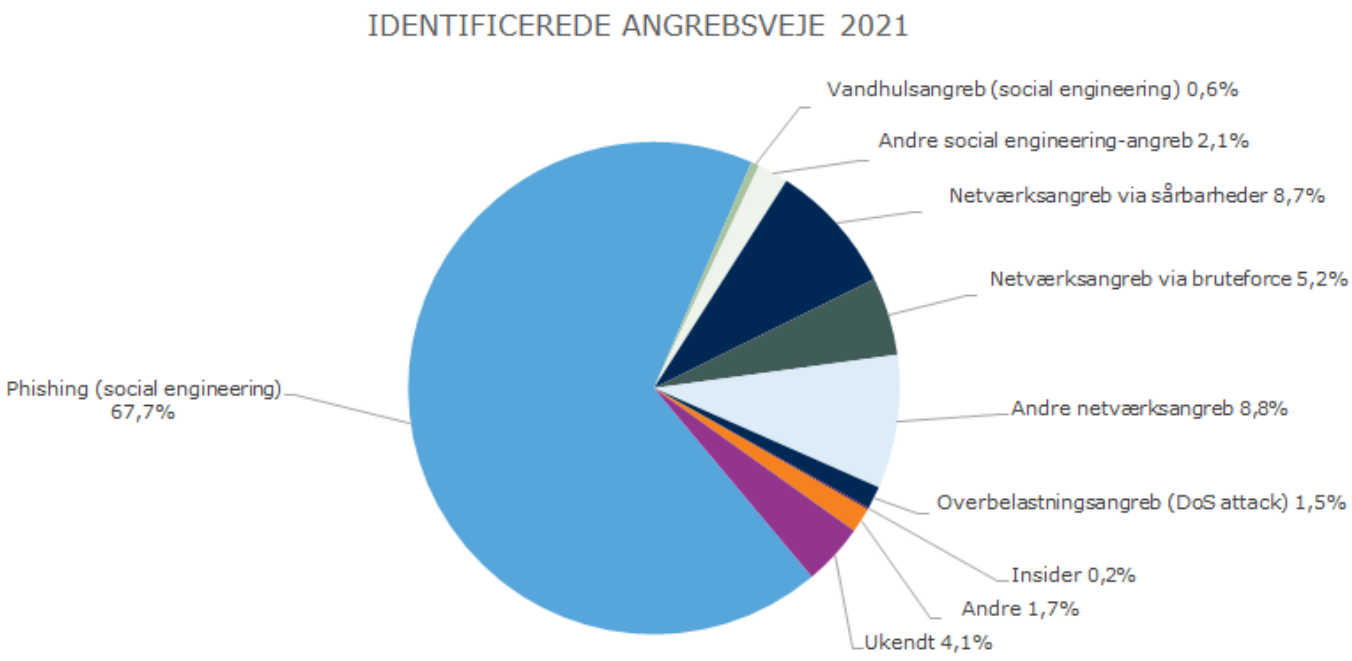
Større
Kritiske systemer berørt eller system- eller administratorkonti kompromitteret. Hændelsen har mærkbar betydning for den berørte organisation. Det vil sige, at aktøren har fået adgang til at læse og kopiere sensitiv information og mulighed for at ændre eller slette information. Det kan for eksempel 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 samtidig med, at CFCS vurderer, at hændelsen har betydning for sikkerheden i den digitale infrastruktur, som samfundsvigtige funktioner er afhængige af.

Fordeling af angrebsveje for hændelser i 2021

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 nedenfor viser fordelingen af de identificerede angrebsveje for 2021. Diagrammet siger ikke noget om, hvilken indvirkning hændelsen har haft på den ramte organisation.



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.

CFCS så i 2021 især forsøg på phishing-mails, der bruges til at lokke fortrolige oplysninger ud af folk. Derudover observerede 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 telefonopkald (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 Et (simpelt) 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. Et computerprogram kan gøre det meget hurtigt. Jo længere et password er, desto længere tid vil det alt andet lige tage at gætte den rigtige kombination.

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 tilgængelig 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
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, 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.

Find flere ordforklaringer på www.cfcs.dk

Eksempler på cyberangreb i 2021

SolarWinds
SolarWinds-angrebet var et globalt software supply chain-angreb, der blev offentligt kendt i december 2020. En statsstøttet hackergruppe havde gemt en specialudviklet bagdør i det udbredte it-managementsystem Orion fra it-virksomheden SolarWinds. Bagdøren blev ifølge SolarWinds distribueret via inficerede softwareopdateringer til op mod 18.000 organisationer verden over.

CFCS vurderer, at hackerne kun udnyttede bagdøren mod de mest interessante mål blandt ofrene. Disse udvalgte mål angreb gruppen til gengæld med specialkonstrueret malware og avancerede angrebsmetoder.

Selvom mere end 50 danske organisationer installerede den inficerede softwareopdatering, vurderer CFCS, at hackerne primært udnyttede bagdørene hos centrale amerikanske myndigheder og virksomheder. CFCS bistod løbende de berørte danske organisationer med rådgivning og teknisk analyse.

Microsoft Exchange Server/HAFNIUM
Tilbage i marts 2021 advarede Microsoft om, at en aktør, som Microsoft har givet kodenavnet HAFNIUM, havde udnyttet fire hidtil ukendte sårbarheder i Microsoft Exchange Server.

Der var tale om fire såkaldte "0-dags-sårbarheder". Det vil sige, at de er blevet udnyttet, før de er blevet opdaget af firmaet bag softwaren. Ifølge Microsoft udnyttede én aktør sårbarhederne i målrettede angreb. Sårbarhederne kunne tilsammen udnyttes til at få adgang til en Exchange Server og installere en bagdør (webshell) uden at være logget ind eller have adgang til et internt netværk.

CFCS bistod med analyse af, hvordan sårbarheden blev udnyttet, samt varslede og rådgav danske organisationer om imødegåelse af sårbarheden.

Colonial Pipeline
I maj 2021 blev det amerikanske olieselskab Colonial Pipeline udsat for et ransomware-angreb. Angrebet medførte, at Colonial Pipeline i seks dage måtte holde virksomhedens rørledninger lukket, mens køerne ved tankstationer langs den amerikanske østkyst voksede. Angrebet illustrerede, hvordan ransomware-angreb kan true kritiske forsyningskæder.

Kaseya
I juli udnyttede den cyberkriminelle gruppe REvil sandsynligvis en sårbarhed i it-virksomheden Kaseyas software, der gjorde det muligt at kompromittere flere af Kaseyas kunder verden over med ransomware. Angrebet spredte sig hurtigt, fordi flere af Kaseyas kunder var MSP'er (managed service providers), der selv leverer it-services som drift og support til deres kunder. På den måde kunne malwaren omgå normale sikkerhedsforanstaltninger. Coop Sverige var blandt ofrene og måtte lukke for omtrent 800 butikker i en dag, da alle kasseapparater var ude af drift efter angrebet.

CFCS bistod med en afdækning af, hvorvidt Kaseya havde ramt danske myndigheder og virksomheder blandt andet gennem søgninger i sårbarhedsdatabaser, som ikke viste nogle eksponerede Kaseya-servere i Danmark. CFCS er ikke bekendt med, at Kaseya havde danske ofre.

Vestas
I november 2021 blev den danske vindmøllegigant Vestas ramt af et ransomware-angreb, hvor hackerne ikke bare låste enkelte it-systemer hos virksomheden, men også truede med at lække data, hvis ikke Vestas betalte løsesum.

Log4j
CFCS advarede i december om en alvorlig sårbarhed i it-værktøjet "Apache Log4j". Apache Log4j er et open source Java-baseret logningsværktøj, der bruges i en lang række produkter og tjenester. Sårbarheden kunne udnyttes til at tilegne sig adgang og overtage kontrollen med servere og systemer. Log4j-komponenten indgår i en række applikationer, hvilket betyder, at sårbarheden også spredte sig til tredjepartsapplikationer.

Forebyggende indsatser i 2021

CFCS udgiver løbende trusselsvurderinger, vejledninger mv. og tilbyder konkret rådgivning til myndigheder og virksomheder som hjælp til at sikre Danmarks digitale infrastruktur. CFCS' trusselsvurderinger bygger på efterretninger og bidrager til at forstå cybertruslen. Denne indsigt kan myndigheder og virksomheder bruge i arbejdet med at lave risikovurderinger og fokusere deres forebyggelsesindsatser. CFCS' vejledninger og rådgivning bygger ligeledes til dels på klassificerede oplysninger om truslen og hændelser.

Oversigt over forebyggelsesindsatser 2021

Kategorier	Antal
Rådgivnings- og kundemøder	808
Awareness-briefinger	180
Trusselsvurderinger	17
Undersøgelsesrapporter	2
Vejledninger	9
Webinarer	7
It-sikkerhedsgodkendelser	51
Godkendelse af kryptoplaner	76
Tekniske sikkerhedseftersyn	107
Sikkerhedstekniske undersøgelser	26
Tempest zoning (udstrålingskontrol)	46
Tilsyn med informationssikkerhed	18
Varsler	196
Varsler via Mit Digitale Selvforsvar*	79
Tweets	302

Note: Tallene dækker både klassificerede og ikke-klassificerede indsatser. CFCS har ikke tidligere talt klassificerede skriftlige produkter med, hvorfor tallet for trusselsvurderinger ikke kan sammenlignes med tidligere år.

**CFCS påbegyndte i 2020 et samarbejde med Forbrugerrådet Tænk om udsendelse af advarsler om falske hjemmesider, phishing-mails mv. via appen Mit Digitale Selvforsvar.*

Analyse og vurdering af cybertruslen
CFCS offentliggjorde i 2021 ti trusselsvurderinger og to undersøgelsesrapporter, der er tilgængelige på www.cfcs.dk. CFCS hævede trusselsniveauet for truslen fra cyberspionage fra **HØJ** til **MEGET HØJ** for transportsektoren samt danske universiteter og forskning. CFCS har blandt andet fulgt udviklingen i cyberkriminelle grupper, som har været fokus for tre af vurderingerne.

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 logning

Selvom logning i sig selv ikke kan forhindre et cyberangreb, er det uundværligt, når et angreb skal opdages og undersøges. Alligevel er der manglende eller ufuldstændige logs i mere end tre ud af fire operative sager, som CFCS arbejder med, og det begrænser undersøgelsen af cyberangreb. Derfor satte CFCS fokus på logning i 2021.

Undersøgelsesrapport: Ingen logs – intet indbrud
CFCS udgav i 2021 undersøgelsesrapporten "Ingen logs – intet indbrud", som beskriver, hvordan manglende logning hos myndigheder og virksomheder betyder, at mange cyberangreb ikke kan undersøges og afhjælpes. Med udgangspunkt i en konkret sag, som CFCS har arbejdet med, viser rapporten, hvordan kvaliteten af logs hos den pågældende myndighed var direkte betydende for, hvor langt CFCS kunne nå i sine undersøgelser af cyberangrebet. Rapporten blev også præsenteret på et webinar i samarbejde med EnergiCERT.

Undersøgelsesrapport om SolarWinds: Statsstøttet globalt software supply chain-angreb
CFCS offentliggjorde i 2021 en undersøgelsesrapport om SolarWinds-angrebet, som kom til verdens kendskab i december 2020. Rapporten beskriver, hvordan det lykkedes en statsstøttet hackergruppe at udføre et globalt software supply chain-angreb via it-virksomheden SolarWinds. Sagen illustrerer, hvordan hackere kan bruge en leverandør til at kompromittere mange ellers velbeskyttede ofre på én gang. CFCS' afdækning af SolarWinds-sagen bekræftede igen, at der har været begrænset logning hos mange af de danske ofre. Det betyder, at det var svært at få et tilstrækkeligt overblik over det samlede omfang af hændelsen og dermed også vanskeligt at sikre, at hullerne var lukket og hackernes fortsatte adgang forhindret.

Nationale anbefalinger om logning
CFCS udgav i 2021 en række nationale anbefalinger om logning. Anbefalingerne omhandler blandt andet opbevaring af logs, DNS-logning, firewall-logning, autentificeringsservere mv.

CFCS' undersøgelsesrapporter og anbefalinger kan findes på www.cfcs.dk

Rådgivning
I 2021 har CFCS udbygget samarbejdet med de samfundsvigtige områder og de decentrale cyber- og informationssikkerhedsenheder, blandt andet gennem arbejdet med en fælles MISP (Malware Information Sharing Platform) og gennem løbende møder og drøftelser om cybersikkerhedsrelaterede emner som risikostyring og beredskab.

CFCS har rådgivet myndigheder og virksomheder om blandt andet risikostyring, beredskab, adfærdsorienteret informationssikkerhed, leverandørstyring, uddannelse og kompetencer samt anskaffelser og udbud. Og så har CFCS igangsat et arbejde med at udvikle nationale sikkerhedsanbefalinger, der skal gøre det mere enkelt for myndigheder og virksomheder at følge best practice for god cybersikkerhed.

CFCS har i 2021 udgivet ni vejledninger blandt andet om "Cyberforsvar der virker", adfærdsorienteret informationssikkerhed og distancearbejde, heraf nogle i samarbejde med Digitaliseringsstyrelsen. Alle vejledninger er tilgængelige på www.cfcs.dk.

Cyberforsvar der virker
CFCS opdaterede i 2021 sin grundlæggende vejledning om cyberforsvar og håndtering af cyberangreb. Vejledningen viser myndigheder og virksomheder vej til et robust cyberforsvar i seks konkrete trin.

Hvis vejledningens trin implementeres, vil det være muligt at forhindre en markant del af de cyberangreb, som myndigheder og virksomheder løbende er udsat for, samt være i stand til effektivt at håndtere de angreb, der lykkes.

En væsentlig pointe i vejledningen er, at topledelsens bevågenhed er den vigtigste forudsætning for et cyberforsvar, der virker. Ledelsen skal styre cyber- og informationssikkerheden og løbende støtte, prioritere og følge op på målsætninger og strategier efter samme principper som inden for eksempelvis økonomi og HR.

Vejledningen findes på www.cfcs.dk

Støtte og rådgivning i Grønland og på Færøerne
I 2021 indledte CFCS arbejdet med at etablere et nordatlantisk rådgivningsteam i centeret med henblik på at styrke rådgivningsindsatsen rettet mod Grønland og Færøerne vedrørende cyber- og informationssikkerhed. Rådgivningsteamet etableres med udgangspunkt i Grønland og Færøernes behov. Formålet er blandt andet at bidrage til at forbedre landenes cyberforsvar og dermed løfte cyber- og informationssikkerheden i Rigsfællesskabet som helhed.

I løbet af året har CFCS gennemført rådgivning om cyber- og informationssikkerhed på anmodning fra myndigheder og virksomheder i Grønland og på Færøerne, herunder telefaglig rådgivning. CFCS har også udbygget monitoreringen i Grønland, siden lov

om Center for Cybersikkerhed trådte i kraft i Grønland i 2020. Monitoreringen giver CFCS bedre mulighed for at bistå de omfattede grønlandske myndigheder og virksomheder ved cyberangreb. Desuden har CFCS været i dialog med en række grønlandske myndigheder og virksomheder om tilslutning til CFCS' sensornetværk. Dialogen fortsættes i 2022.

Ny enhed for sikkerhedsaspekter i den teknologiske udvikling
Som led i forsvarsforliget 2018-2023 har CFCS i august 2021 etableret et nyt videnscenter for sikkerhedsaspekter i den teknologiske udvikling. Centeret skal have en videnstung og forskningsbaseret tilgang og etablere et samarbejde med uddannelsesinstitutioner og virksomheder samt være bindeled til nationale og internationale forsknings- og udviklingsfora inden for nye teknologier og cybersikkerhed. Centeret bidrager med teknisk og forskningsbaseret viden, som skal bruges internt og eksternt i forbindelse med CFCS' rådgivning af myndigheder og virksomheder om cyber- og informationssikkerhed, herunder i relation til nye teknologier. Videnscenteret har i 2021 fokuseret på rekruttering af medarbejdere, herunder Ph.d.- studerende, samt relations- og netværksskabelse med relevante akademiske miljøer.

Sikkerhedstekniske undersøgelser
CFCS hjælper myndigheder, virksomheder og Forsvaret med at højne it-sikkerheden ved at gennemføre sikkerhedstekniske undersøgelser i form af trusselsbaserede sårbarhedsscanninger, penetrationstests og red-team-tests. CFCS' sikkerhedstekniske undersøgelser er en del af centerets forbyggende arbejde, som blandt andet omfatter rådgivning og vejledning om cyber- og informationssikkerhed.

Ved sikkerhedstekniske undersøgelser testes organisationens cyberforsvar og eventuelle reaktion på cyberangreb. Formålet er at styrke cyber- og informationssikkerheden og øge robustheden der, hvor et angreb vil gøre mest skade. Selve undersøgelsen foregår ved, at centerets sikkerhedsspecialister efterligner sofistikerede realistiske cyberangreb fra en ondsindet aktør. Gennem undersøgelsen får den enkelte organisation viden om konkrete sårbarheder i it-systemerne og om de tiltag og forbedringer, der kan iværksættes for at imødegå angreb.

CFCS har i 2021 gennemført 26 sikkerhedstekniske undersøgelser. Undersøgelserne afdækker generelt sårbarheder, som i meget vid udstrækning kan mitigeres ved at følge CFCS' vejledninger, herunder "Cyberforsvar der virker" og "Vejledning om passwordsikkerhed".

Uddannelse af cyberværnepligtige
CFCS bidrog også i 2021 til Forsvarets uddannelse af cyberværnepligtige. Uddannelsen omfatter blandt andet et besøg hos CFCS, hvor de værnepligtige bliver introduceret til CFCS' arbejde for et sikkert digitalt Danmark gennem forebyggelse, imødegåelse og håndtering af cyberangreb. Cyberværnepligten afsluttes med en øvelse, hvor CFCS angriber et netværk, som de cyberværnepligtige skal beskytte.

Styrket informationssikkerhed i staten
CFCS har i 2021 styrket indsatsen vedrørende teknisk sikkerhedsstøtte til statslige myndigheder og Forsvaret. CFCS' mål er at sikre, at statens højt klassificerede områder og informationer er beskyttet mod teknisk spionage. Opgaverne omfatter

blandt andet rådgivning om sikkerhedsforanstaltninger, tekniske sikkerhedseftersyn af lokaler, bygninger og installationer, monitorering, samt operative indsatser.

Telesektorens decentrale cyber- og informationssikkerhedsenhed
CFCS er myndighed for informationssikkerhed, beredskab og leverandørsikkerhed i telesektoren og indgår derfor også i den decentrale cyber-og informationssikkerhedsenhed i telesektoren, hvor 11 teleoperatører deltager. Enheden har i 2021 udarbejdet en revideret version af "Sårbarheds- og risikovurderingen for telesektoren i Danmark". Enheden har ligeledes styrket vidensdelingen, blandt andet gennem en række erfaringsudvekslingsmøder, tilskyndelse til øget monitorering med henblik på tidlig detektion af angreb mod telesektoren samt afholdelse af workshop om øvelse for teleudbydere om hændelseshåndtering og informationsdeling. Endvidere har enheden i samarbejde med EnergiCERT fået etableret en open source-baseret platform til udveksling af information mellem de decentrale cyber- og informationssikkerhedsenheder i forbindelse med kritiske hændelser.

Cybersikkerhedsmåned i oktober
Cybersikkerhedsmåneden i oktober var igen i 2021 præget af et højt aktivitetsniveau. Måneden er en udløber af den europæiske cybersikkerhedsmåned og sætter fokus på vigtige budskaber om cybersikkerhed for myndigheder, virksomheder og borgere.

CFCS bidrog blandt andet med oplæg om adfærdsorienteret informationssikkerhed, cybertruslen mod Danmark og meget mere for en række virksomheder og myndigheder. Der blev afholdt et velbesøgt arrangement for unge, der drømte om at prøve kræfter med jobbet som cyberanalytiker, i samarbejde med CyberSkills, og så kunne Kulturnattens publikum i Forsvarsministeriet opleve et live phishing-angreb udført af CFCS' specialister.

I løbet af oktober udgav CFCS desuden vejledningen "Cyberforsvar der virker", som også blev formidlet på et åbent webinar, en rapport om SolarWinds-angrebet, en temaartikel om sikkerhed på sociale medier og en trusselsvurdering om truslen fra ransomware mod energisektoren. Desuden blev CFCS' liste over ord og begreber inden for cybersikkerhed opdateret med ti nye ord, der afspejler aktuelle tendenser i cyberangreb.

Læs mere om cybersikkerhedsmåneden på sikkerdigital.dk/ncsm

Tilsynsopgaver i 2021

CFCS har som national it-sikkerhedsmyndighed og myndighed for informationssikkerhed og beredskab på teleområdet udført en række tilsyn og sikkerhedsgodkendelser i 2021.

It-sikkerhedsgodkendelser
CFCS varetager FE's opgave som national it-sikkerhedsmyndighed og har i den forbindelse blandt andet til opgave at sikkerhedsgodkende (akkreditere) it-systemer, -installationer og -forbindelser, som anvendes til behandling af klassificerede informationer i henhold til sikkerhedscirkulæret[1]. Gennem en akkrediteringsproces skal myndigheder sikre, at deres klassificerede it-løsninger overholder gældende sikkerhedskrav, politikker og lovgivning. CFCS rådgiver myndigheder i forbindelse med akkrediteringsprocessen og kan tillige udføre sikkerhedsteknologiske undersøgelser og tekniske sikkerhedseftersyn i forbindelse med en sikkerhedsgodkendelse.

CFCS har i 2021 udstedt 51 it-sikkerhedsgodkendelser. CFCS har ligeledes udstedt 76 godkendelser af kryptoplaner og 46 TEMPEST-zoningsgodkendelser.

Tilsyn med it- og kryptosikkerheden
Som led i varetagelsen af opgaven som national it-sikkerhedsmyndighed har CFCS også til opgave at føre tilsyn med de it-sikkerheds- og kryptosikkerhedsmæssige foranstaltninger, som Danmark er forpligtet til at gennemføre i relation til elektronisk behandling af klassificeret information jf. sikkerhedscirkulæret og med henblik på efterlevelse af sikkerhedsbestemmelser fra EU og NATO.

CFCS har i 2021 gennemført ni tilsyn hos offentlige myndigheder, der arbejder med klassificerede informationer. Tilsynsaktiviteten har i 2021 særligt taget udgangspunkt i sikkerhedsdokumentationen for de eksisterende klassificerede og sikkerhedsgodkendte it-systemer, -installationer eller -forbindelser ved de enkelte myndigheder samt afdækning af myndighedernes modenhedsniveau i forhold til sikkerhedsforståelse og håndtering af sikkerhedshændelser.

Tilsyn på teleområdet
CFCS har, som led i sin lovbestemte rolle som tilsynsmyndighed for informationssikkerhed, beredskab og leverandørsikkerhed på teleområdet, gennemført tilsynsaktiviteter hos udvalgte teleudbydere. Der er i 2021 gennemført fire tilsynsaktiviteter med hovedfokus på at sikre, at teleudbyderne til brug for risikostyringen har etableret og vedligeholder registre over sine kritiske netkomponenter, systemer og værktøjer. Herudover er der i 2021 gennemført fem tilsynsaktiviteter vedrørende krav til sikkerhedsgodkendelse af udbydernes personale.

[1] Cirkulære nr. 10338 af 17. december 2014 om sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO eller EU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt.

EU-samarbejdet i 2021

I 2021 har CFCS på EU-området særligt haft fokus på arbejdet med 5G-sikkerhed og lov om leverandørsikkerhed i den kritiske teleinfrastruktur samt revision af net- og informationssikkerhedsdirektivet, der danner rammen for, hvordan vi beskytter netværks- og informationssikkerheden i de samfundskritiske sektorer i EU.

Europæisk samarbejde om 5G-sikkerhed og lov om leverandørsikkerhed i den kritiske teleinfrastruktur
Som myndighed for beredskab og informationssikkerhed i telesektoren er CFCS involveret i et omfattende europæisk samarbejde om 5G-sikkerhed. I 2021 har der blandt andet været fokus på teletekniske sikkerhedsanbefalinger og minimumskrav.

I forlængelse heraf har CFCS i 2021 publiceret 224 handlingsrettede teletekniske sikkerhedsanbefalinger til danske 5G-udbydere på sin hjemmeside. CFCS har også indrapporteret til Europa-Kommissionen, at Danmark har taget disse anbefalinger i brug som led i implementeringen af Kommissionens værktøjskasse for cybersikkerhed i 5G-netværk.

Et yderligere led i den danske implementering af værktøjskassen var Folketingets vedtagelse og ikrafttrædelsen af lov om leverandørsikkerhed i den kritiske teleinfrastruktur, som skete i henholdsvis maj og juli 2021.

Revision af NIS-direktivet
Net- og informationssikkerhedsdirektivet (NIS) danner rammen for, hvordan vi beskytter netværks- og informationssikkerheden i de samfundskritiske sektorer i EU. Siden direktivet blev implementeret i 2018, er cybertruslen kun blevet mere udbredt, og digitaliseringen er blevet mere udbredt i de samfundskritiske sektorer i EU. På den baggrund står medlemsstaterne over for mange fælles, grænseoverskridende udfordringer i forhold til leverancen af samfundskritiske tjenester. Derfor præsenterede Europa-Kommissionen i december 2020 en revision af NIS-direktivet (NIS2), som der blev vedtaget en politisk aftale om i maj 2022.

NIS2 lægger op til at udvide direktivets dækningsområde i bredden og dybden blandt andet i form af nye krav til cybersikkerheden i de omfattede virksomheder og myndigheder samt til medlemsstaternes tilsyn med cybersikkerheden. Formålet er fortsat at sikre et højt fælles sikkerhedsniveau på tværs af EU gennem blandt andet ledelsesforankret risikostyring, implementering af organisatoriske og tekniske foranstaltninger, operativt samarbejde på tværs af organisationer og landegrænser i EU samt at sikre, at der er styr på beredskabet, så organisationerne er i stand til hændelseshåndtering (før, under og efter).

I 2021 har det Europæiske Råd forhandlet Rådets generelle indstilling til Kommissionens forslag til NIS2. CFCS har bidraget aktivt til forhandlingerne med faglige bemærkninger til indholdet af NIS2. De europæiske medlemsstater nåede til enighed om Rådets generelle indstilling i december 2021. NIS2 forventes vedtaget i

løbet af 2022, når de såkaldte trilog-forhandlinger mellem Kommissionen, det Europæiske Råd og Europa-Parlamentet er afsluttet.

CFCS' aktiviteter i relation til NIS-direktivet
CFCS er nationalt kontaktpunkt i regi af NIS-direktivet. Centeret har i den forbindelse deltaget i NIS-samarbejdsgruppens fire møder i 2021 og i samarbejdet i CSIRT-netværket mellem de europæiske CSIRT'er (Computer Security Incident Response Teams), der omhandler videndeling og koordination af operative anliggender. CFCS deltager også i samarbejdet i det europæiske cyberkrise-videndelingsnetværk CyCLONe (Cyber Crises Liason Organisation Network). CFCS repræsenterer desuden Danmark i bestyrelsen for EU's Cybersikkerhedsagentur, ENISA.

CFCS' deltagelse i internationale øvelser i 2021

CFCS repræsenterer Danmark i en række internationale cyberøvelser:

BlueOlex
CFCS deltog i 2021 i den europæiske øvelse i cybersikkerhed, BlueOlex, der blev afholdt for tredje gang i det europæiske cyberkrise-videndelingsnetværk CyCLONe (Cyber Crises Liason Organisation Network). Øvelsen blev afholdt som en blandet fysisk og virtuel øvelse med Rumænien som vært, og udgangspunktet var et fiktivt cyberangreb mod transportsektoren. Det overordnede formål med BlueOlex er at træne og skærpe det tværgående samarbejde og deling af information på operationelt niveau i EU, så der kan handles hurtigt og effektivt i tilfælde af en større cybersikkerhedshændelse, der rammer flere lande.

Locked Shields
I foråret afholdt NATO Cooperative Cyber Defence Center of Excellence øvelsen Locked Shields. CFCS var med i et af de 22 forsvarende blå hold, som deltog på øvelsen. Mere end 30 lande bidrog til afholdelse af øvelsen, der er en så kaldt live-firing exercise, hvor de blå hold i realtid udfordres af angribende røde hold. De blå hold fungerede som Rapid Reaction Teams, der deployeredes til et fiktivt land for at håndtere en større cyberhændelse.

CySOPEx
I maj 2021 afholdt det europæiske videndelingsnetværk CyCLONe øvelsen CySOPEx. Øvelsen tog udgangspunkt i et fiktivt cyberangreb med ransomware i transportsektoren, hvor både jernbaner og havne i EU var ramt. Undervejs fik medlemsstaterne forskellig information om angrebets udvikling og situationen i de enkelte lande, og så gjaldt det om at holde sig opdateret internt og videreformidle relevant viden til de øvrige deltagere.

NATO Cyber Coalition
CFCS deltog igen i 2021 i NATO's store cyberøvelse, Cyber Coalition 2021, som fandt sted i Estlands hovedstad, Tallinn. Mere end 1.000 deltagere fra 28 NATO-lande og en række partnernationer fra blandt andet Schweiz, Finland, Irland og Sverige var med i øvelsen.

Øvelsen har til formål at styrke NATO's evne til at modstå cybertrusler og gennemføre militære cyberoperationer. Deltagerlandene konkurrerer derfor ikke mod hinanden under

øvelsen men samarbejder om at udveksle information, erfaring og best practice om håndtering af cyberangreb. Derfor er Cyber Coalition også en lejlighed til at teste NATO's og landenes nationale procedurer for videndeling, situationsoverblik og beslutningsevne inden for cyberdomænet.

Cyber Viking II

CFCS deltog i Cyber Viking II øvelsen sammen med US Airforce Cyber Wing, der blev afholdt i San Antonio, Texas i USA. CFCS øvede sammen med US Airforce Cyber Wing det taktiske niveau og trænede beskyttelse af kritisk infrastruktur samt nøgleressourcer med det formål at styrke parathed og samarbejde på tværs ved udførelsen af koordinerede militære-til-militære cyberoperationer.

Cyber Flag

I november 2021 afholdt US Cybercommand øvelsen Cyber Flag, som er en multinational øvelse med fokus på at styrke samarbejdet i NATO for bedre at kunne identificere og imødegå cyberangreb. CFCS sendte et bidrag til øvelsen, der bestod af et angribende rødt hold såvel som et forsvarende blåt hold. Øvelsen blev afholdt på den amerikanske National Cyber Range, hvor øvelsesdeltagerne blev udfordret på at detektere ondsindet aktivitet, dele oplysninger med øvrige nationer, dele teknikker til at få smidt den ondsindede aktør af netværket samt at få hærdet og genoprettet systemerne.

Gordian Knot

NATO Maritime Interdiction Operational Training Centre afholdt i juni cyberøvelsen Gordian Knot, hvor CFCS støttede Forsvaret i deres deltagelse i øvelsen. Øvelsen bestod i at forsvare et netværk mod hackerangreb og holde kritiske it- og kommunikationssystemer kørende.

Om Center for Cybersikkerhed

Efterretningsbaseret cyberforsvar
CFCS blev oprettet i december 2012 som en del af FE. De fleste cyberangreb mod Danmark kommer fra udlandet. 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 behandling af personoplysninger. CFCS-loven er pr. 21. november 2020 sat i kraft i Grønland ved kgl. anordning nr. 1658.

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

Netsikkerhedstjenesten har til opgave at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos tilsluttede myndigheder og virksomheder. 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 varetager FE's opgave som national it-sikkerhedsmyndighed og de opgaver inden for informationssikkerhedsområdet, som Danmark er forpligtet til gennem sit medlemskab af blandt andet NATO og EU. 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 relevante myndigheder og virksomheder med henblik på at styrke sikkerheden i Danmarks digitale infrastruktur, herunder netværk, computere og andre systemer, som samfundsvigtige funktioner er afhængige af.

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 medarbejdere, 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.

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, www.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, www.cfcs.dk

Formidling i 2021

Vejledninger

Råd om sikkerhed på virtuelle mødeplatforme
Denne vejledning adresserer nogle af de sikkerhedsmæssige problemstillinger, som særligt risiko-ledelsen og it-ledelsen bør forholde sig til, når der skal anskaffes og konfigureres virtuelle mødeplatforme.
https://www.cfcs.dk/da/forebyggelse/vejledninger/distancearbejde/rad-om-sikkerhed-pa-virtuelle-modeplatforme/

God kultur ved distancearbejde
Som medarbejder spiller du en vigtig rolle for den samlede sikkerhed i den organisation, hvor du arbejder.
https://www.cfcs.dk/da/forebyggelse/vejledninger/distancearbejde/god-kultur-ved-distancearbejde/

Beskyt organisationen: Opdater sikkerhedspolitikkerne til en »ny normal«
Ved distancearbejde er der behov for, at organisationen genbesøger sine sikkerhedspolitikker og retningslinjer. Dels for at sikre at de faktisk understøtter denne måde at arbejde på, og dels for at sikre at organisationen får adresseret de særlige risici.
https://www.cfcs.dk/da/forebyggelse/vejledninger/distancearbejde/opdater-sikkerhedspolitikkerne/

Metode til at arbejde med adfærdsindsatser inden for cyber- og informationssikkerhed
Denne vejledning giver organisationer en metodisk ramme til at arbejde med adfærd inden for cyber- og informationssikkerhed.
https://www.cfcs.dk/da/forebyggelse/vejledninger/vejledning-metode-til-at-arbejde-med-adfardsindsatser/

Cyberforsvar der virker
"Cyberforsvar der virker" er Center for Cybersikkerheds grundlæggende vejledning om cyberforsvar og håndtering af cyberangreb.
https://www.cfcs.dk/da/forebyggelse/vejledninger/cyberforsvar-der-virker/

Nationale anbefalinger om logning
De nationale anbefalinger om logning giver konkrete anvisninger på, hvad man som organisation skal gøre for at leve op til best practice på området.
https://www.cfcs.dk/da/forebyggelse/nationale-anbefalinger/

Kodeks for gennemførsel af sikkerhedstest
IT-Branchen, KL og HK har i fællesskab udarbejdet et kodeks, der kan hjælpe med at sikre, at sikkerhedstest udføres både etisk og juridisk forsvarligt. Som afsendere står samlet: Akademikerne, Center for Cybersikkerhed, Dansk Erhverv, Dansk Industri,

Danske Regioner, Digitaliseringsstyrelsen, Erhvervsstyrelsen, Finans Danmark, HK, IT-Branchen, KL og SMV Danmark.
https://www.cfcs.dk/da/forebyggelse/sikkerhedstest/kodeks-for-sikkerhedstest/

Trusselsvurderinger

Hovedparten af trusselsvurderingerne er udgivet både på dansk og engelsk.

Fjern adgangen
Hackere kompromitterer sårbare fjernadgange og sælger dem videre til andre kriminelle, som udnytter dem til målrettede ransomware-angreb.
https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/fjern-adgangen/

Virksomheder i energisektoren er attraktive mål for ransomware
Center for Cybersikkerhed vurderer truslen fra ransomware-angreb mod den danske energisektor efter angrebet mod Colonial Pipeline i USA og de ændringer i det kriminelle miljø, der kom i efterspillet af angrebet.
https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/ransomware-mod-energisektoren/

Gamle hackere på nye platforme
I denne trusselsvurdering beskriver Center for Cybersikkerhed, hvordan de kriminelle netværk, der står bag ransomware-angreb, har omorganiseret sig efter angrebet mod Colonial Pipeline.
https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/gamle-hackere-pa-nye-platforme/

Cybertruslen mod dansk luftfart
Formålet med denne trusselsvurdering er at redegøre for cybertruslen mod den danske luftfartssektor. Trusselsvurderingen kan blandt andet bruges i sektorens videre arbejde med risikovurderinger.
https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/luftfart/

Cybertruslen mod land- og lufttransporten
Trusselsvurderingen beskriver cybertruslerne mod land- og lufttransport i Danmark.
https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/transport/

Cybertruslen mod dansk forskning og universiteter
Denne trusselsvurdering beskriver de mest alvorlige cybertrusler mod dansk forskning og universiteter.
https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/forskning-og-universiteter/

Hackere scanner dit netværk for sårbarheder hver dag året rundt
Trusselsvurderingen orienterer myndigheder og virksomheder om, at hackere konstant afsøger internettet for udstyr med sårbarheder, de kan udnytte til at kompromittere organisationen.
https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/hackere-scanner-dit-netvark/

Truslen fra destruktive cyberangreb
Formålet med denne trusselsvurdering er at øge opmærksomheden hos danske beslutningstagere, myndigheder og virksomheder på truslen fra destruktive cyberangreb. Selvom truslen er **LAV**, vil succesfulde angreb få betydelige konsekvenser.
https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/trusselsvurdering-truslen-fra-destruktive-cyberangreb/

Cybertruslen mod Danmark
Trusselsvurderingen beskriver den generelle cybertrussel mod Danmark fra cyberangreb, der understøtter kriminalitet, spionage, destruktive cyberangreb, aktivisme og terrorisme.
https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/cybertruslen-mod-danmark/

Cybertruslen mod jernbanesektoren
Denne vurdering beskriver cybertruslen mod den danske jernbanesektor, herunder passager- og godsoperatører samt infrastrukturforvaltere.
https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/Cybertruslen-mod-jernbanesektoren/

Undersøgelsesrapporter

Ingen logs – intet indbrud
Undersøgelsesrapporten "Ingen logs – intet indbrud" beskriver, hvordan manglende logs hos myndigheder og virksomheder har stor betydning for i hvilket omfang, cyberangreb kan undersøges og afhjælpes. Med udgangspunkt i en konkret sag, som CFCS har arbejdet med, viser rapporten, hvordan kvaliteten af logs hos den pågældende myndighed var direkte betydende for, hvor langt CFCS kunne nå i sine undersøgelser af cyberangrebet.
https://www.cfcs.dk/da/cybertruslen/rapporter/ingen-logs-intet-indbrud/

SolarWinds: Statsstøttet globalt software supply chain-angreb
Denne undersøgelsesrapport beskriver, hvordan en statsstøttet hackergruppe udførte et globalt software supply chain-angreb via it-virksomheden SolarWinds. Sagen illustrerer, hvordan hackere kan bruge en leverandør til at kompromittere mange ellers velbeskyttede ofre på én gang.
https://www.cfcs.dk/da/cybertruslen/rapporter/solarwinds/

Temaartikler mv.

CFCS' ordforklaringsliste
CFCS opdaterede i forbindelse med cybersikkerhedsmåneden i oktober sin liste med ordforklaringer, der viser, hvordan CFCS bruger ord og begreber inden for cybersikkerhed.
https://www.cfcs.dk/da/cybertruslen/ordforklaringer/

Temaartikel: Sikkerhed på sociale medier #SoMeSikkerhed
Twitter, Facebook, LinkedIn, Instagram og andre sociale medier giver organisationer mulighed for at tale med et bredt publikum på nye måder. Men hvis man ikke har sikkerheden på plads, kan det skade omdømmet.
https://www.cfcs.dk/da/temasider/sikkerhed-pa-sociale-medier/

Temaartikel: Dine apps ved, hvor du bor
Det kan være praktisk, at telefonen ved, hvor brugeren befinder sig. Men det er ikke altid en god idé. Denne temaartikel giver råd om brug af lokalitetsdata.
https://www.cfcs.dk/da/nyheder/2021/temaartikel-dine-apps-ved-hvor-du-bor/

Temaartikel: CFCS-Sinkhole sladrer om Sodinokibi ransomware
De kriminelle bagmænd bag ransomware-familien Sodinokibi har været banebrydende på ransomware-markedet. CFCS ser i denne artikel nærmere på Sodinokibi på baggrund af en teknisk analyse og statistiske data.
https://www.cfcs.dk/da/temasider/sodinokibi-ransomware/

QBot: Omstillingsparat malware kaprer mailtråde
QBot eller QakBot er endnu én af de malware-familier, der bliver brugt som et tidligt stadie i et cyberangreb, som i sidste ende kan føre til læk af data eller målrettede ransomware-angreb.
https://www.cfcs.dk/da/nyheder/2021/qbot-omstillingsparat-malware-kaprer-mailtrade/

SmokeBot og Bazar: På sporet af den malware, der fører til ransomware-angreb
Visse typer malware bliver misbrugt som brohoved i målrettede ransomware-angreb. CFCS udgiver i denne artikel en liste med tekniske indikatorer på to af disse malware-familier.
https://www.cfcs.dk/da/nyheder/2021/smokebot-og-bazar/

Varsel: Forebyggelse af ransomware kræver opmærksomhed på brugerkonti
CFCS anbefaler, at man etablerer og følger en fast procedure for håndtering af bruger- og administratorkonti. Proceduren skal sikre, at alle konti gennemgås periodisk med henblik på at afdække om de stemmer overens med de faktiske behov.
https://www.cfcs.dk/da/handelser/varsler/forebyggelse-af-ransomware-kraver-opmarksomhed-pa-brugerkonti/

Teletekniske anbefalinger til 5G-udbydere
CFCS har i 2021 publiceret 224 handlingsrettede teletekniske sikkerhedsanbefalinger til danske 5G-udbydere på sin hjemmeside.
https://www.cfcs.dk/globalassets/cfcs/dokumenter/telemyndighed/teletekniske-anbefalinger-til-5g-udbydere---20210910.pdf

Webinarer

CFCS har arbejdet med også at formidle centerets publikationer og viden om cybertruslen og cyberforsvar i mundtlig form via webinarer, hvor deltagere kan stille uddybende spørgsmål til CFCS' specialister.

I 2021 er der afholdt syv webinarer:

- SolarWinds-angrebet (for inviterede interessenter og samarbejdspartnere)
- Hafnium-angrebet/sårbarheder i MS Exchange Server i samarbejde med Dubex A/S (for inviterede interessenter og samarbejdspartnere)
- Cybertruslen mod Danmark 2021 (åbent webinar)
- Logning: Forskellen på at tro eller vide, at du er blevet hacket (åbent webinar)
- Introduktion til revideret NIS-direktiv (NIS2) (åbent webinar)
- Cybersikkerhedsrådets webinar "Kort og konkret om cybersikkerhed" (åbent webinar)
- Cyberforsvar der virker (åbent webinar)

Sociale medier

Twitter
CFCS har i løbet af 2021 udsendt 233 tweets fra @Cybersikkerhed, hvorfra CFCS tweeter bredt om cybersikkerhed, og 69 tweets fra Situationscenteret, @CFCSsitcen, hvorfra der tweetes om sårbarheder, varsler og rådgivning med et operativt og tidskritisk sigte.

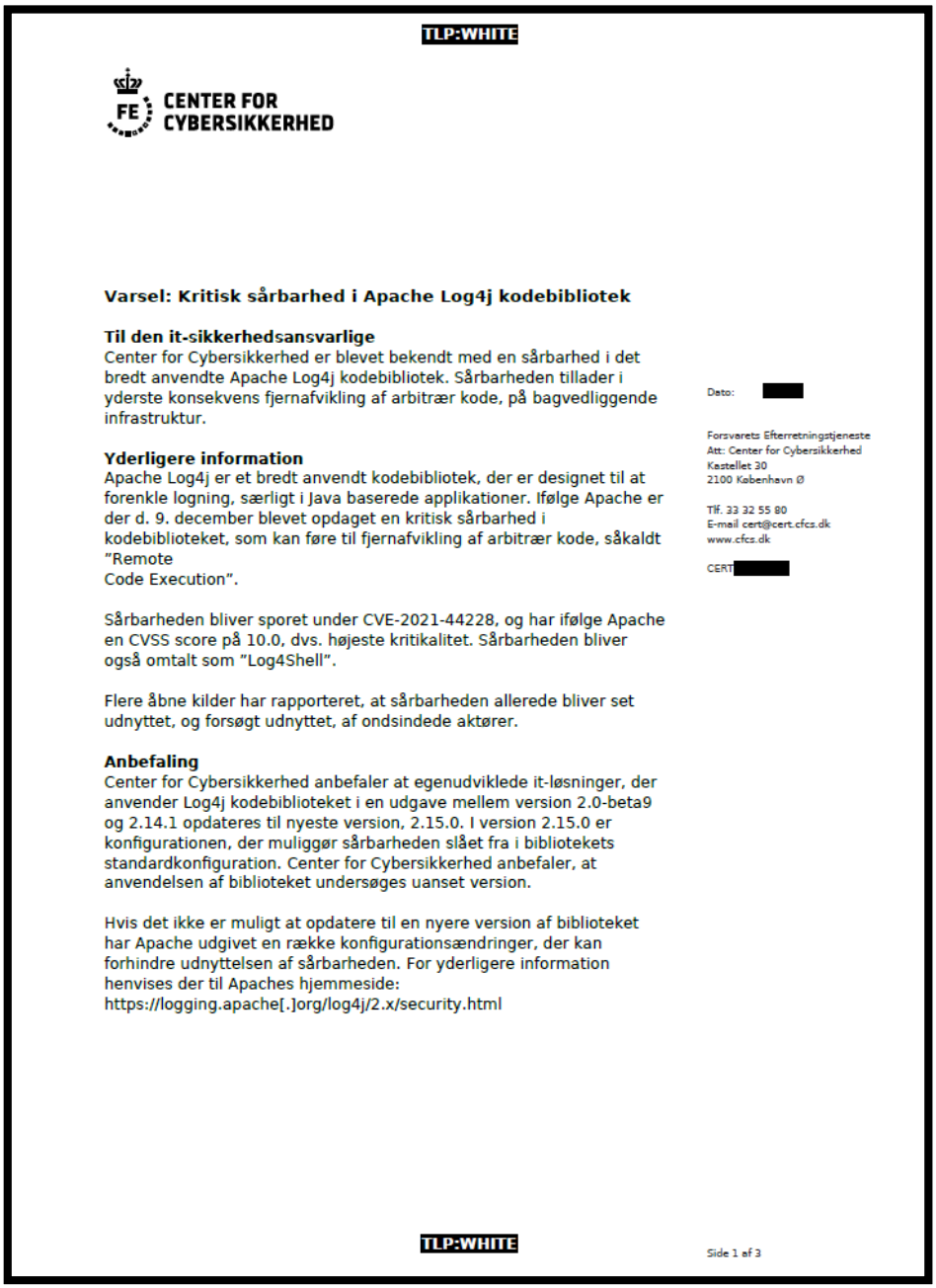
@Cybersikkerhed: www.twitter.com/cybersikkerhed
@CFCSsitcen: www.twitter.com/CFCSsitcen

LinkedIn
CFCS har i løbet af 2021 lagt 146 opslag på LinkedIn, hvorfra centeret løbende deler nyheder, publikationer og jobopslag.

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

Eksempler på varsler udsendt af CFCS' situationscenter

Nedenstående varsler er anonymiserede versioner af varsler udsendt i 2021. Varsler fra CFCS' situationscenter er markeret efter Traffic Light-protokollen (TLP). 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.



TLP:WHITE

CENTER FOR CYBERSIKKERHED

Varsel: Kritisk sårbarhed i Apache Log4j kodebibliotek

Til den it-sikkerhedsansvarlige
Center for Cybersikkerhed er blevet bekendt med en sårbarhed i det bredt anvendte Apache Log4j kodebibliotek. Sårbarheden tillader i yderste konsekvens fjernafvikling af arbitrær kode, på bagvedliggende infrastruktur.

Yderligere information
Apache Log4j er et bredt anvendt kodebibliotek, der er designet til at forenkle logning, særligt i Java baserede applikationer. Ifølge Apache er der d. 9. december blevet opdaget en kritisk sårbarhed i kodebiblioteket, som kan føre til fjernafvikling af arbitrær kode, såkaldt "Remote
Code Execution".

Sårbarheden bliver sporet under CVE-2021-44228, og har ifølge Apache en CVSS score på 10.0, dvs. højeste kritikalitet. Sårbarheden bliver også omtalt som "Log4Shell".

Flere åbne kilder har rapporteret, at sårbarheden allerede bliver set udnyttet, og forsøgt udnyttet, af ondsindede aktører.

Anbefaling
Center for Cybersikkerhed anbefaler at egenudviklede it-løsninger, der anvender Log4j kodebiblioteket i en udgave mellem version 2.0-beta9 og 2.14.1 opdateres til nyeste version, 2.15.0. I version 2.15.0 er konfigurationen, der muliggør sårbarheden slået fra i bibliotekets standardkonfiguration. Center for Cybersikkerhed anbefaler, at anvendelsen af biblioteket undersøges uanset version.

Hvis det ikke er muligt at opdatere til en nyere version af biblioteket har Apache udgivet en række konfigurationsændringer, der kan forhindre udnyttelsen af sårbarheden. For yderligere information henvises der til Apaches hjemmeside:
https://logging.apache[.]org/log4j/2.x/security.html

Dato: [redacted]

Forsvarets Efterretningstjeneste
Att: Center for Cybersikkerhed
Kastellet 30
2100 København Ø

Tlf. 33 32 55 80
E-mail cert@cert.cfcs.dk
www.cfcs.dk

CERT[redacted]

TLP:WHITE

Side 1 af 3

TLP:AMBER

CENTER FOR CYBERSIKKERHED

Varsel: Malware uploaded til [redacted]

Til den it-sikkerhedsansvarlige
Center for Cybersikkerhed har observeret forsøg på at uploade malware til en filserver hos [redacted]. Der er observeret forsøg på at logge ind på filserveren forinden, hvorefter malware gentagne gange forsøges uploaded.

Yderligere information
Trafikken er observeret d. [redacted] 2021 fra kl. 19:28 CEST.
Der er observeret indadgående forbindelser fra [redacted] mod [redacted]:21. IP-adressen resolver til "[redacted]".

Der forsøges at logge ind med forskellige brugere, herunder "ftp", "administrator", "admin" og "user".

Kl. 19:32:06 logges der ind som "[redacted]". Kort tid efter forsøges der at tilgå directories på FTP-serveren.
Kl. 19:41:44 forsøges der at uploade "[redacted]" til [redacted]. Filen er en executable på 5MB, og den er sandsynligvis en kryptominer.
(SHA1: [redacted])

Vores observationer viser, at ovennævnte fil lykkedes at blive overført til filserveren. Vi har ikke observeret, at nogen har downloaded filen.

Anbefaling
Center for Cybersikkerhed anbefaler, at den pågældende filserver undersøges for at afklare, om det er lykkedes at uploade ovenstående malware til serveren. Derefter bør man fjerne filen for at forhindre malwaren i at sprede sig samt undersøge om andre ondsindede filer er til stede på serveren.
Hvis malwaren er succesfuldt uploadet til filserveren, anbefales det derudover at undersøge om adgang til filserven kan begrænses for at forhindre anonyme brugere i at uploade vilkårlige filer.

Offentligt tilgængelige filservere bliver ofte scannet af automatiske værktøjer for at finde tilgængelige servere, hvor der kan uploades malware.

Dato: [redacted]

Forsvarets Efterretningstjeneste
Att: Center for Cybersikkerhed
Kastellet 30
2100 København Ø

Tlf. 33 32 55 80
E-mail cert@cert.cfcs.dk
www.cfcs.dk

CERT [redacted]

TLP:AMBER

TLP:AMBER

CENTER FOR CYBERSIKKERHED

Varsel: Krypto mining trafik

Til den it-sikkerhedsansvarlige
Center for Cybersikkerhed har observeret trafik, til en IP-adresse, der har været brugt i forbindelse med krypto mining.

Yderligere information
Center for Cybersikkerhed har observeret trafik, til IP-adressen ([redacted]), til portene; 750, 752, 753, 755, 756, 757, 758.
IP-adressen, har været set brugt i forbindelse med krypto mining.

Udsnit af forbindelserne til IP'en:

Dato (UTC)	Src	Dst
2021-[redacted] 08:00	[redacted]	[redacted]:753
2021-[redacted] 10:36	[redacted]	[redacted]:751
2021-[redacted] 11:00	[redacted]	[redacted]:758
2021[redacted] 08:27	[redacted]	[redacted]:751

Det er observeret, at der sendes data ud med ordet "XMRig".

Anbefaling
Center for Cybersikkerhed anbefaler, at der overvejes passende modforanstaltninger for at sikre systemet. Dette indebærer blandt andet, at lokalisere systemet, der afsender forespørgslerne og fjerne krypto miner på maskinen.

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

Rådgivning
Center for Cybersikkerhed kan i nogle tilfælde bistå med rådgivning om cyber- og informationssikkerhed, herunder styring af informationssikkerhed og risikovurderinger. Center for Cybersikkerheds

Dato: [redacted]

Forsvarets Efterretningstjeneste
Att: Center for Cybersikkerhed
Kastellet 30
2100 København Ø

Tlf. 33 32 55 80
E-mail cert@cert.cfcs.dk
www.cfcs.dk

CERT-[redacted]

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 3332 5580 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 3332 5580.

Kontakt til telemyndigheden
Kontakt til telemyndigheden ved CFCS kan ske på telefon 3332 5580 eller på e-mail tele@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