CENTER FOR CYBERSIKKERHED

# Center for Cybersikkerheds beretning 2019

## Indhold

CENTER FOR CYBERSIKKERHED

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

1. udgave oktober 2020

Forsideillustration: Getty Images/iStockPhoto/KittiBakai

# Indledning

Danmark er et af verdens mest digitaliserede lande, og digitaliseringen er afgørende for Danmarks vækst og velfærd. Center for Cybersikkerhed (CFCS) arbejder for et sikkert digitalt Danmark og har til opgave at understøtte et højt sikkerhedsniveau 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, signaler der sikrer at togene kører, og muligheden for at vi kan kontakte hinanden via vores telefoner, er helt afhængige af digital understøttelse.

CFCS arbejder for at beskytte den digitale infrastruktur i Danmark og for at styrke Danmarks robusthed mod cyberangreb. Centeret bidrager også til beskyttelsen af militære netværk mod cyberangreb. CFCS er Danmarks nationale it-sikkerheds-myndighed og nationalt kompetencecenter på cybersikkerhedsområdet. Centerets netsikkerhedstjeneste fokuserer på de mest avancerede angreb, der oftest udføres af statsstøttede aktører, eller cyberangreb, der i øvrigt kan påvirke det danske samfund i væsentlig grad. Centeret vejleder og rådgiver desuden danske myndigheder og virk-somheder i at styrke cybersikkerheden.

Hvert år udgiver CFCS en beretning, der beskriver centerets arbejde det foregående år med særligt fokus på centerets indsatser i forhold til forebyggelse og i forhold til op-dagelse og håndtering af sikkerhedshændelser.

# Om FE's Center for Cybersikkerhed

CFCS blev oprettet i december 2012 som en del af Forsvarets Efterretningstjeneste (FE).

Placeringen i FE skaber en række synergieffekter og sikrer, at Danmark er med i den kreds af vestlige lande, som kan levere et dybere og mere efterretningsbaseret nationalt cyberforsvar.

CFCS er Danmarks nationale it-sikkerhedsmyndighed og den centrale nationale myndighed for cybersikkerhed, der udgør Danmarks forsvar mod cybertrusler. Centeret arbejder sammen med en lang række interessenter for et sikkert digitalt Danmark.

CFCS er en arbejdsplads med mange forskellige typer af højtspecialiserede med-arbejdere, herunder netværksanalytikere, malwareanalytikere, pen-testere, in-formationssikkerhedsrådgivere og teleingeniører. Størstedelen af centerets med-arbejdere har en it-uddannelse eller anden teknisk baggrund. Men centeret har også medarbejdere uden formel uddannelse, fordi de har et særligt talent inden for netværks- og malwareanalyse. Dertil kommer en gruppe medarbejdere med militærfaglig baggrund og akademikere med en samfundsvidenskabelig baggrund.

**Tilsynets årlige redegørelse og Center for Cybersikkerheds 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 CFCS trådte i kraft. TET's årlige redegørelser kan findes på TET's hjemmeside *www.tet.dk*

CFCS udgiver supplerende hvert år en beretning, der 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.

# Cybertruslen

Cybertruslen er fortsat en af de alvorligste trusler mod Danmark. Særligt cyberkriminalitet og cyberspionage udgør en vedvarende trussel.

Cyberkriminalitet udgør en trussel mod alle danske myndigheder, virksomheder og borgere. Cyberkriminelle udfører oftest relativt simple angreb mod mange potentielle ofre på en gang blandt andet gennem phishing-angreb, hvor kriminelle gennem falske mails for eksempel forsøger at franarre login-oplysninger eller levere ransomware til efterfølgende afpresning. Der findes dog også netværk med kapacitet til at udføre mere komplekse cyberangreb, herunder målrettede ransomware-angreb og digitale bankrøverier.

Truslen fra cyberspionage er især rettet mod myndigheder, som arbejder med udenrigs- og sikkerhedspolitik samt virksomheder, der besidder en viden, som andre stater har interesse i. Cyberspionage kan føre til pres på danske beslutningstagere og skade dansk konkurrenceevne.

Det er mindre sandsynligt, at fremmede stater vil udføre destruktive cyberangreb mod Danmark. Det er dog muligt, at danske virksomheder og myndigheder, som har aktiviteter i regioner præget af konflikter, kan blive udsat for følgevirkningerne af et destruktivt cyberangreb.

# Center for Cybersikkerheds indsatser i 2019

CFCS fik i 2019 opdateret sit lovgrundlag for at gøre det muligt for centeret at følge med udviklingen i trusselsbilledet. Centeret har i 2019 desuden haft fokus på at styrke sine indsatser inden for rammerne af den nationale strategi for cyber- og informationssikkerhed fra maj 2018 samt forsvarsforliget 2018-2023. Det gælder blandt andet:

- Det reviderede lovgrundlag, der giver CFCS mulighed for dels at tilbyde gratis tilslutning til centerets sensornetværk, dels at kunne agere mere aktivt i beskyttelsen af samfundsvigtige myndigheder og virksomheder og for tidligt at opdage cyberangreb hos de tilsluttede myndigheder og virksomheder.

- Udbygning af situationscenteret, der nu er bemandet med analytikere, der er uddannet på FE's eget Cyberakademi. Situationscenteret kan kontaktes 24/7-365, men først ultimo 2020, når næste akademi er afsluttet, er der også fysisk bemanding døgnet rundt.

- Udvikling af sensornetværket i forhold til truslen og dialog med relevante myndigheder og virksomheder i særligt de seks samfundskritiske sektorer (energi, tele, finans, sundhed, transport og søfart) om tilslutning samt projektering af et nyt sensorsystem med det formål at kunne danne et nationalt situationsbillede.

- Rådgivning om cybersikkerhed og trusselsbilledet, hvor både bred vejledning og rådgivning og den tætte dialog med de seks decentrale cyber- og informationssikkerhedsenheder (DCIS'er), som er blevet etableret i de seks samfundskritiske sektorer, har været i fokus.

- Bidrag til en styrket forsknings- og uddannelsesindsats inden for cybersikkerhed gennem støtte til en række projekter og etablering af samarbejde med Danish Hub for Cybersecurity.

- Styrkelse af analytiske og teknologiske kompetencer til netværks-, forensic- og malware-analyse med henblik på at styrke indsatsen mod avancerede statsstøttede cyberangreb samt til gennemførelse af sikkerhedstekniske undersøgelser og egentlige penetrationstest ved myndigheder og virksomheder.

**Cybersikkerhed er en holdsport**

CFCS arbejder tæt sammen med en lang række interessenter om at forebygge, opdage og imødegå cyberangreb. Dette gælder for eksempel Forsvaret samt myndigheder og virksomheder i de seks samfundskritiske sektorer (energi, tele, finans, sundhed, transport og søfart), som er identificeret i den nationale strategi for cyber- og informationssikkerhed fra maj 2018. CFCS samarbejder også med blandt andre

Digitaliseringsstyrelsen og Erhvervsstyrelsen for at højne cybersikkerheden i det offentlige Danmark og erhvervslivet. Centeret er i tæt kontakt med større og mindre virksomheder og samarbejder endvidere med Politiets Efterretningstjeneste (PET) og politiet, hvor centeret efter anmodning kan bistå med kapacitet til politiets efterforskning af cyberkriminalitet.

**National strategi for cyber- og informationssikkerhed**
Den nationale strategi for cyber- og informationssikkerhed har sigte på at øge den tekniske robusthed og sikre bedre beskyttelse af statens kritiske it-systemer, viden og kompetencer hos borgere, virksomheder og myndigheder samt styrkelse af den nationale koordinering og samarbejdet om informations-sikkerhed.

Strategien tager udgangspunkt i sektoransvarsprincippet, der betyder, at den myndighed, der har ansvaret for en funktion i det daglige, også har ansvaret for at planlægge, hvordan man vil opretholde og videreføre funktionen i tilfælde af en ekstraordinær hændelse.

De seks samfundskritiske sektorer (energi, finans, søfart, transport, sundhed og tele) har hver udarbejdet en sektorstrategi for cyber- og informationssikkerhed og etableret en decentral cyber- og informationssikkerhedsenhed (DCIS) som led i strategien.

Strategien blev lanceret i maj 2018.

CFCS har i 2019 bidraget betydeligt til arbejdet med initiativerne i den nationale strategi for cyber- og informationssikkerhed i blandt andet styregruppen for strategien, der har delt formandskab mellem CFCS og Digitaliseringsstyrelsen, og hvor ministerier på tværs af de samfundskritiske sektorer deltager, samt i den bredere kontaktgruppe, der består af alle ministerier.

For at sikre yderligere videndeling og samarbejde om cybersikkerhed på tværs af myndigheder, virksomheder, organisationer og forskningsverdenen nedsatte regeringen i 2019 et offentligt-privat Cybersikkerhedsråd.

**Nyt offentligt-privat Cybersikkerhedsråd**

I december 2019 nedsatte regeringen et nyt offentligt-privat Cybersikkerhedsråd, som skal styrke samarbejde og videndeling mellem offentlige og private aktører om cyber- og informationssikkerhed. Rådet skal kvalificere myndigheders og virksomheders arbejde og styrke det digitale demokrati, herunder udbredelse af viden om og forståelse for de trusler og muligheder, som digitaliseringen og den nye teknologi medfører. Cybersikkerhedsrådet fokuserer på det strategiske niveau og har følgende arbejdsområder:

- Rådgivning til udvikling af den nationale strategi for cyber- og informationssikkerhed. Konkret kan rådet for eksempel gennemføre analyser, der kan danne baggrund for prioritering af igangsatte eller eventuelt kommende initiativer.

- Bidrage til videndeling, rådgivning og vejledning på strategisk niveau for eksempel gennem relevante publikationer, netværk og konferencer samt bidrag til videndeling i forhold til information om trusler, sårbarheder, hændelser og cyberøvelser til relevante parter.

- Undersøge behovet for og foreslå udvikling af relevante cybersikkerhedskompetencer blandt borgere og medarbejdere, for eksempel inden for uddannelse og forskning.

- Bidrage til den danske cybersikkerhedsmåned i forbindelse med ENISA's (European Network and Information Security Agency) årlige "cyber security month" i oktober samt bidrage til en årlig awareness-kampagne rettet mod borgerne.

**Om Cybersikkerhedsrådet**

- Cybersikkerhedsrådet består af 20 medlemmer, inklusive et delt offentligt-privat formandskab.

- Den offentlige del af formandsskabet varetages på skift af Digitaliseringsstyrelsen og CFCS, mens den private del af formandsskabet varetages af Bjarke Alling, koncerndirektør i softwarevirksomheden Liga ApS og formand for IT-Branchens it-sikkerhedsudvalg.

- Cybersikkerhedsrådet er sammensat af 20 medlemmer fra den private sektor, den offentlige sektor, forbrugersiden og forskningsverdenen. Medlemmernes faglighed spænder bredt, og rådet har dermed både strategiske, juridiske og teknologiske kompetencer.

- Medlemmerne er udpeget for perioden 2019-2021. Der er nedsat et sekretariat til at understøtte Cybersikkerhedsrådet i samme periode.

- Rådet kan efter behov nedsætte særskilte følge- eller arbejdsgrupper.

Læs mere om Cybersikkerhedsrådet på *www.cfcs.dk*

For at sikre videndeling og koordination af aktiviteter har CFCS etableret et strategisk samarbejdsforum for cybersikkerhed med udvalgte virksomheder og brancheforeninger. Derudover faciliterer CFCS som led i den nationale cyber- og informationssikkerhedsstrategi et forum for de samfundskritiske sektorers decentrale cyber- og informationssikkerhedsenheder, hvor også Digitaliseringsstyrelsen og PET deltager.

**Cybersituationscenteret og Cyberakademiet**
CFCS' situationscenter er den centrale indgang for myndigheder og virksomheder, ikke mindst i forhold til de operative opgaver. Situationscenteret er en del af netsikkerhedstjenesten, der har til opgave at forebygge, opdage og imødegå sikkerhedshændelser.

**Cyberakademi**
I 2019 gennemførte FE/CFCS sit første Cyberakademi. Uddannelsen retter sig mod kandidater, som har it-interesse, evner og lyst til en karriere inden for cybersikkerhed, men som ikke nødvendigvis kan fremvise et eksamensbevis. I løbet af tre måneder blev kandidaterne undervist i datasikkerhed, netværksforståelse og programmering, angrebstyper, angrebsopdagelse, analyse af sikkerhedshændelser og brug af relevante tekniske værktøjer. Ud over FE/CFCS' egne kandidater, deltog også eksterne deltagere fra forskellige statslige organisationer og en virksomhed inden for telesektoren. Akademiet gennemføres igen i 2020.

**Initiativer inden for forsvarsforligets pulje til forskning og uddannelse**
CFCS har inden for rammerne af forsvarsforliget ansvaret for en pulje på 10 millioner kr. til forskning og uddannelse i 2019-20. Det overordnede formål er at understøtte et bæredygtigt miljø for cyberuddannelser og forskning på tværs af uddannelsesinstitutioner ved at yde økonomisk støtte til relevante initiativer. Puljen har i 2019 støttet en række projekter blandt andet en sommerskole med bredt fokus på cybersikkerhed baseret på et samarbejde mellem en række uddannelsesinstitutioner og efterfølgende to "cyberdays" med samme sigte. Puljen har desuden støttet en undersøgelse af udbud og efterspørgsel efter it-sikkerhedskompetencer, udvikling af e-læringsmoduler, et initiativ vedrørende netværksanalyse og et forstudie om governance inden for cyber- og informationssikkerhed.

CFCS har indledt et tæt samarbejde med CyberHub'en, der har til formål at fremme udviklingen af cyberfaglige curricula, styrke start-ups inden for området, rekruttere til faget og bidrage til at udbrede efter- og videreuddannelse inden for cybersikkerhed. Centeret bistår for eksempel også Digitaliseringsstyrelsen og Moderniseringsstyrelsen i deres arbejde med at lave masterclasses og vejledningsmateriale til ansatte i staten.

**Analyse af udbud og efterspørgsel efter it-sikkerhedskompetencer**
CFCS deltog i 2019 sammen med Erhvervsstyrelsen, Digitaliseringsstyrelsen og Uddannelses- og Forskningsministeriet i arbejdet med en analyse af udbud og efterspørgsel efter it-sikkerhedskompetencer. Analysen var initieret af Virksomhedsrådet for it-sikkerhed.

Analysen peger på, at efterspørgslen efter medarbejdere med de rette kompetencer på området er steget kraftigt det sidste årti, og knap halvdelen af danske virksomheder og myndigheder forventer, at behovet for ansatte med informationssikkerhedskompetencer vil stige de kommende fem år. Samtidig har mere end hver femte virksomhed eller myndighed haft svært ved at rekruttere en profil med de rette informationssikkerhedskompetencer i løbet af de seneste seks måneder. Mange af de medarbejdere, der arbejder med informationssikkerhed, har ikke en formel videregående uddannelse inden for området. Derfor benytter mange virksomheder og myndigheder sig af intern og ekstern oplæring af deres medarbejderes kompetencer inden for området.

Analysen viser yderligere, at der i Danmark på nuværende tidspunkt er et begrænset antal videregående uddannelser med et højt indhold af informationssikkerhed. Udbuddet af uddannelser med informationssikkerhedsindhold er dermed i sin begyndelse, og det vil derfor tage tid at uddanne medarbejdere med de rette kompetencer.

# Ændring af lov om Center for Cybersikkerhed

Cybertruslen er dynamisk, og hackernes evner og redskaber udvikler sig hastigt. Den hastige udvikling i trusselsbilledet har medført et behov for at opdatere lovgivningen til det aktuelle trusselsbillede og den teknologiske udvikling således, at CFCS har bedre mulighed for at imødegå cyberangreb mod den samfundsvigtige infrastruktur. Lovgrundlaget for CFCS blev revideret i 2019 med vedtagelse af lov nr. 555 den 7. maj 2019.

**Lovændringens indhold**
Gebyret for tilslutning til CFCS' netsikkerhedstjeneste er med lovændringen blevet fjernet, hvorefter tilslutning er gratis for myndigheder og virksomheder af samfundsvigtig karakter, såfremt CFCS vurderer, at tilslutningen vil kunne bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet. Derudover er der med lovændringen skabt mulighed for, at der i helt særlige tilfælde vil kunne gives påbud til særligt samfundsvigtige virksomheder eller myndigheder om at blive tilsluttet netsikkerhedstjenesten. Der har ikke været behov for at anvende påbudsordningen.

Lovændringen indebærer også en forlængelse af slettefristerne for data vedrørende sikkerhedshændelser samt adgang til at videregive selve den skadelige kode (malware), der ligger bag et angreb, til relevante aktører som for eksempel private it-sikkerhedsfirmaer. Herudover giver lovændringen CFCS forskellige muligheder for både at kunne agere mere aktivt i beskyttelsen af samfundsvigtige myndigheder og virksomheder og for tidligt at opdage cyberangreb hos de tilsluttede myndigheder og virksomheder, som ønsker at tilslutte sig denne del af ordningen.

Med lovændringen har CFCS fået en række tekniske muligheder, der i det daglige medvirker til, at CFCS i endnu højere grad kan imødegå cyberangreb mod den samfundsvigtige infrastruktur. CFCS har i 2019 været i løbende kontakt med en række myndigheder og virksomheder om de nye tekniske muligheder.

Endelig har lovændringen styrket CFCS' muligheder for at foretage sikkerhedstekniske undersøgelser hos blandt andre myndigheder og virksomheder, der efterspørger centerets bistand til at identificere sårbarheder og vurdere robustheden af deres systemer. Centeret kan således med udgangspunkt i den styrkede lovhjemmel anvende mere realistiske metoder i forbindelse med gennemførelse af sikkerheds-tekniske undersøgelser, herunder blandt andet foretage social engineering. Det giver bedre muligheder for at sikkerhedsteste netværk og systemer blandt andet fra internetsiden.

CFCS har i 2019 foretaget flere mere dybtgående og virkelighedsnære sikkerheds-tekniske undersøgelser, hvor alle aspekter af sikkerheden er blevet afprøvet, og som dermed har givet mulighed for at foretage en opfølgende helhedsorienteret styrkelse af sikkerheden. CFCS afdækker ved de sikkerhedstekniske undersøgelser sårbarheder i it-systemer og rådgiver om, hvordan sårbarhederne kan udbedres, og sikkerheden styrkes. CFCS skaber på den måde grundlag for et løft af sikkerhedsniveauet hos de undersøgte myndigheder og virksomheder.

# Opdagelse og håndtering af sikkerhedshændelser i 2019

**Udbygning af sensornetværket**
CFCS' netsikkerhedstjeneste har til opgave at forebygge, opdage og imødegå cyberangreb hos danske myndigheder og virksomheder, der er tilsluttet CFCS' sensornetværk, samt hos Forsvaret.

Med sigte på en bedre beskyttelse af Danmark mod avancerede cyberangreb har centeret i 2019 forberedt en yderligere udbredelse af det teknisk avancerede sensor-netværk til myndigheder og virksomheder, blandt andet i form af et kommercielt indkøbt supplement til det eksisterende system af egenudviklede sensorer (se faktaboks nedenfor). CFCS har i 2019 i tæt samarbejde med de decentrale cyber- og informationssikkerhedsenheder i de samfundskritiske sektorer udarbejdet en

kortlægning af digitale afhængigheder for samfundets kernefunktioner i og på tværs af sektorerne som led i den nationale cyber- og informationssikkerhedsstrategi, jf. afsnittet om forebyggende indsatser i 2019 nedenfor. Overblikket er en vigtig forudsætning for at kunne prioritere udbredelsen af den nye type sensorer i sensornetværket, der skal bidrage til et nationalt cybersituationsoverblik.

**Center for Cybersikkerheds sensornetværk**
CFCS' netsikkerhedstjeneste driver et sensornetværk, som kan opdage forsøg på cyberangreb. Det nuværende sensornetværk er et egenudviklet intrusion detection-system, IDS, som består af hardwareenheder med en vis lagerkapacitet placeret på internetforbindelsen foran flere ministerier og offentlige myndigheder. Dette egenudviklede system vil blive suppleret af en kommercielt udviklet løsning, der har til formål at bidrage til et nationalt situationsbillede. Sensornetværket 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, der passer på en regel, modtager CFCS' netsikkerhedstjeneste en alarm.

**Tilslutninger til sensornetværket**
CFCS har i 2019 blandt andet haft fokus på installation af yderligere sensorer i sensornetværket inden for Forsvaret på dets forskellige lokaliteter rundt i Danmark.

Ved udgangen af 2019 havde CFCS i alt 70 tilsluttede myndigheder og virksomheder fordelt på 29 civile myndigheder m.fl., 36 militære myndigheder og fem private virksomheder.

**Sikkerhedshændelser**
Danmark rammes hvert år af flere tusinde cyberangreb. Tallene for sikkerhedshændelser i denne beretning er alene udtryk for, hvad der bliver registreret i CFCS' sensorer. Sager, der ikke er identificeret via sensornetværket, for eksempel via direkte henvendelse, tip fra en partner eller fra FE's efterretningsmæssige virke indgår ikke i opgørelsen. Der er desuden et stort mørketal for cyberangreb i Danmark, da de færreste private virksomheder frivilligt indberetter om sikkerhedshændelser.

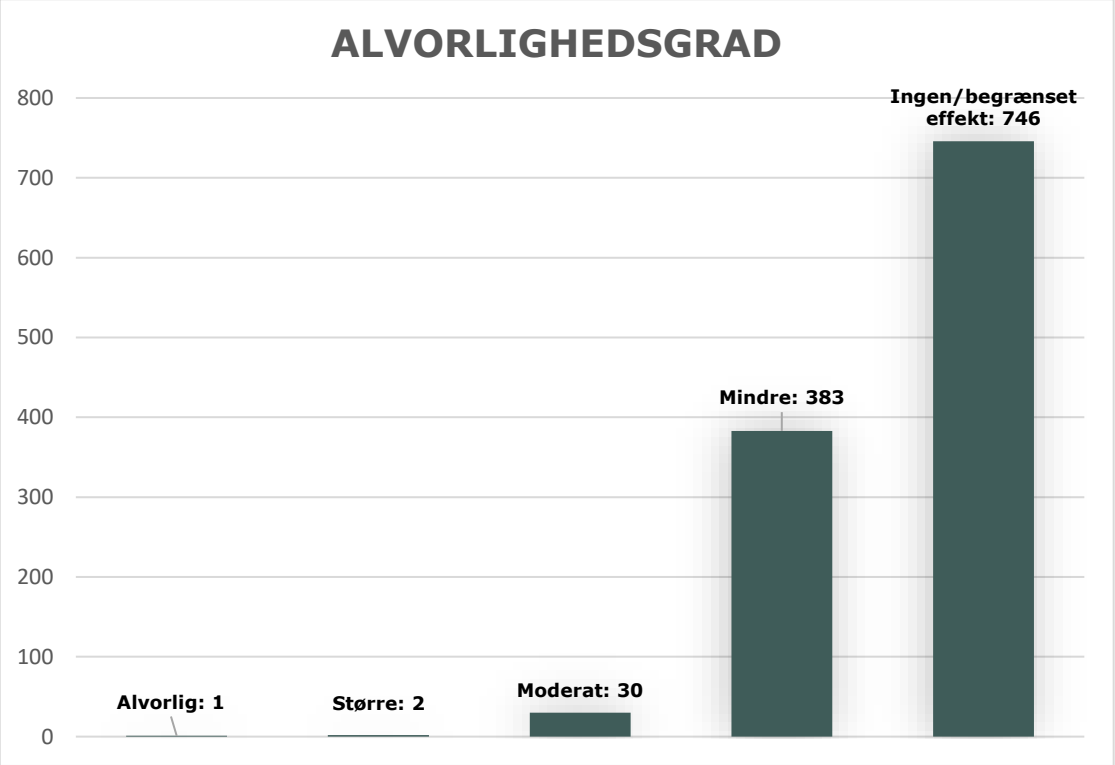
En sikkerhedshændelse er en hændelse, der negativt påvirker eller vurderes at ville kunne påvirke tilgængeligheden, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale tjenester.

CFCS får løbende en bedre indsigt i hændelsesbilledet i takt med, at flere myndigheder og virksomheder tilknyttes sensornetværket. Netsikkerhedstjenesten håndterer dagligt alarmer fra sensornetværket. Når en alarm går, ser en netværksanalytiker på hændelsen med henblik på at vurdere, om der er tale om et cyberangreb.

Netsikkerhedstjenesten har i 2019 håndteret 1.162 hændelser, hvoraf 416 hændelser har haft effekt på den berørte organisation. I 2018 håndterede netsikkerhedstjenesten 172 hændelser, der havde effekt på den berørte organisation. Tallet for

sikkerhedshændelser 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 derved får en bredere indsigt i hændelsesbilledet. Ikke desto mindre er der tale om en betydelig stigning i antallet af hændelser med effekt på de berørte organisationer. Det kan både hænge sammen med en stigende aktivitet mod danske netværk, og med det nyetablerede cybersituationscenters stadig stærkere evne til at opdage hændelser med sensornetværket, der løbende forbedres med indkøbte og efterretningsbaserede indikatorer.

**Sikkerhedshændelser 2019**




*Kilde: Netsikkerhedstjenesten. Kategorien "Ingen/begrænset effekt" inkluderer falske positiver. Tallene for sikkerhedshændelser i denne beretning er alene udtryk for, hvad der bliver registreret i CFCS' sensorer. CFCS får løbende en bedre indsigt i hændelsesbilledet i takt med, at flere myndigheder og virksomheder tilknyttes sensornetværket. Tallene kan ikke sammenlignes direkte år for år, da datagrundlaget ændrer sig, efterhånden som flere myndigheder og virksomheder tilknyttes sensornetværket.*

Af de 1.162 hændelser, som netsikkerhedstjenesten har behandlet, er der 746 hændelser, der er vurderet til at have haft ingen eller begrænset effekt på den pågældende myndighed eller virksomhed. Der kan for eksempel være tale om rekognosceringer, der er bevidste, ofte automatiserede handlinger fra en ondsindet aktør, som har til formål at identificere, indhente viden om og profilere it-systemer via internettet og udnytte denne viden til senere angreb. En hændelse uden effekt kan dog ofte være det første tegn på en fremtidig større hændelse. Cybersituationscenteret varsler derfor ofte om rekognosceringsforsøg til de tilsluttede virksomheder og myndigheder – og i visse tilfælde også mere bredt via de sociale medier. Hændelser

uden effekt kan også være en falsk positiv, som efter nærmere undersøgelse viser sig ikke at være et angreb.

Der er registreret få alvorlige eller større sikkerhedshændelser i sensornettet i 2019, hvilket også er at forvente. Formålet med det nuværende sensornet er netop at identificere cyberangreb så tidligt, at de ikke når at udvikle sig til større hændelser. For at blive betegnet som en større hændelse skal en angrebsaktør have lykkedes med at få adgang til ét eller flere kritiske systemer, herunder at få adgang på system- eller administratorniveau. Det vil sige med rettigheder, der giver adgang til at læse og kopiere sensitiv information og mulighed for at ændre eller slette information. Det kan derfor for eksempel dække over ransomwareangreb, der rammer større dele af en organisations it-systemer. Det kan medføre alvorlige tab af data og langvarige afbrydelser af it-driften. Større sikkerhedshændelser kan også omfatte angreb, hvor aktøren har haft fodfæste på organisationens netværk gennem længere tid og potentielt har haft adgang til sensitiv information. Større sager med cyberspionage falder dermed også ind under denne kategori.

Ved et moderat angreb kan enkelte enheder, for eksempel en pc eller en server, være kompromitteret. Der er typisk tale om enkeltstående klientkompromitteringer, 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 angrebsaktøren har ikke fået adgang til sensitive informationer.

CFCS ser flest af den type angreb, som centeret definerer som ”mindre cyberangreb”. Et mindre cyberangreb er et reelt angreb, der dog ikke medfører kompromittering. Når et cyberangreb ikke medfører kompromittering, skyldes det i høj grad, at cyber-angrebet stoppes af de berørte organisationers etablerede sikkerhedsforanstaltninger som for eksempel firewalls, spamfiltre og antivirusløsninger. Et mindre cyberangreb kan dog både være dyrt og besværligt for den ramte organisation, idet organisationen ofte skal bruge tid på at undersøge, hvad der er sket, og eventuelt gennemgå robustheden af eksisterende sikkerhedsforanstaltninger, herunder for eksempel skifte passwords i organisationen, ændre administratorrettigheder m.v. En sådan hændelse er også et tegn på, at den pågældende organisation har været genstand for uønsket interesse – og fortsat kan være det, og at der derfor generelt er behov for at sikre, at it-sikkerheden er på plads, herunder om niveauet skal styrkes.

**Ransomware mod danske virksomheder i 2019 – to eksempler**
**Demant**
Den danske høreapparatsproducent Demant blev den 3. september 2019 ramt af et ransomwareangreb. Selskabet valgte at lukke store dele af koncernens it-systemer ned, umiddelbart efter at have konstateret angrebet. Demant genetablerede systemer fra backup og kunne den 11. oktober meddele, at it-infrastrukturen atter fungerede normalt. Selskabet har vurderet, at koncernens samlede omkostninger afledt af ransomwareangrebet lå mellem 550 og 650 millioner kroner.

*Kilde: Demant.*

**GlobalConnect**
GlobalConnect, der leverer fibernetværksinfrastruktur og datacenterfaciliteter, blev den 23. november 2019 ramt af et cyberangreb. Angrebet ramte selskabets interne administrative systemer, og til pressen oplyste GlobalConnect, at der sandsynligvis var tale om en ny variant af ransomware. Blandt de ramte systemer var det interne telefonisystem og et system til fakturering. Ingen af kundernes netværk eller systemer i GlobalConnects datacentre blev ramt. Gen-opretningen af de ramte systemer tog mere end to uger, før driften var normal.

*Kilde: GlobalConnect. Computerworld.*

**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*

**Definition af alvorlighedsgraden af en sikkerhedshændelse**
**Falsk positiv**
Undersøgelse af alarm, som viser sig ikke at være et angreb.

**Ingen/begrænset effekt**
Aktiviteten har ikke haft nogen relevant betydning for den berørte organisation. Der kan for eksempel være tale om rekognosceringer.

**Mindre**
Reelt angrebsforsøg, som ikke medfører kompromittering.

**Moderat**
Ingen kritiske systemer berørt, ingen system- eller administratorkonti kompromitteret. Begrænset betydning for den berørte organisation.

**Større**
Kritiske systemer berørt eller system- eller administratorkonti kompromitteret. Hændelsen har mærkbar betydning for den berørte organisation.

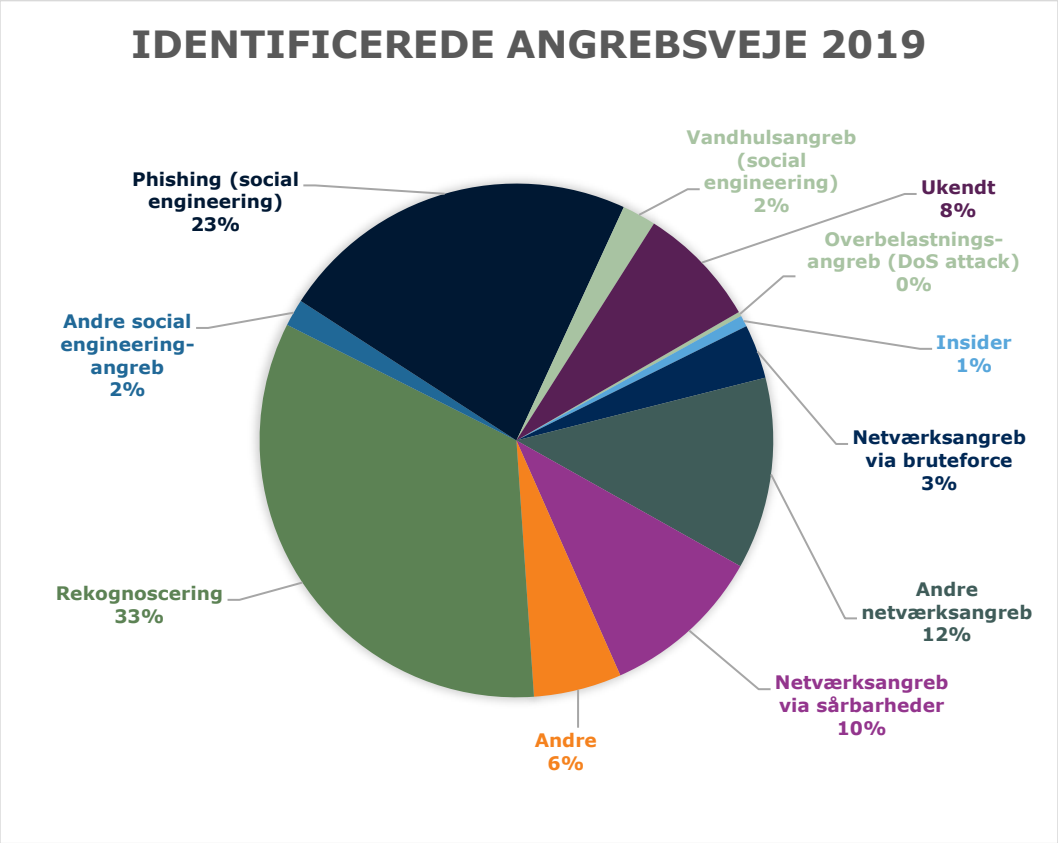
**Alvorlig**
Kritiske systemer berørt eller system- eller administratorkonti kompromitteret. Hændelsen har alvorlig betydning for den berørte organisation.

*Kilde: Netsikkerhedstjenesten*

**Angrebsveje**

CFCS' 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 2019. Diagrammet viser ikke, hvilken indvirkning hændelsen har haft på den ramte organisation.

**Identificerede angrebsveje 2019**




*Kilde: Netsikkerhedstjenesten. Diagrammet viser de angrebsveje, det har været muligt at identificere ud fra CFCS' registrering. Diagrammet rummer potentielt falske positiver. Kategorien "Ukendt" dækker over hændelser, hvor det ikke har været muligt at identificere angrebsvejen.*

CFCS ser mange sager, især forsøg på phishing og rekognosceringer, rettet mod myndigheder og virksomheder, som er tilsluttet netsikkerhedstjenesten. Phishing bruges til at lokke fortrolige oplysninger ud af folk via for eksempel falske e-mails. Rekognosceringer er ikke direkte forsøg på at opnå adgang til et system, men succesfulde rekognosceringer kan udstyre angriberen med oplysninger, som kan udnyttes til at udføre målrettede angreb på et senere tidspunkt.

**Ordforklaring – angrebsveje**

**Rekognoscering** dækker i denne sammenhæng over en bevidst, ofte automatiseret, handling fra en ondsindet aktør, som har til formål at identificere, indhente viden om og profilere it-systemer via internettet og udnytte denne viden til senere angreb. Det kan for eksempel ske ved sårbarheds- eller portscanninger eller forsøg på at forbinde fra IP-adresser, som tidligere har været sat i forbindelse med ondsindet infrastruktur.

**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 (for eksempel "123456") mod mange brugernavne (for eksempel alle e-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".

**Phishing** er forsøg på via social engineering at manipulere en person til i god tro at videregive personlige oplysninger eller klikke på inficerede filer eller links til falske hjemmesider. Phishing sker ofte ved at sende en e-mail til offeret.

**Vandhulsangreb** dækker over en angrebsteknik, hvor en ellers legitim hjemmeside 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.

**Overbelastningsangreb** (DoS, Denial of Service) dækker over angreb, hvor et it-system gøres utilgængeligt ved for eksempel at sende usædvanligt store eller særligt udformede datamængder mod systemet.

**Social** (Social Engineering) dækker bredt over cyberangreb, som er afhængige af og udnytter ofrets handlemønstre og interaktion med it-systemet. Angrebsteknikken anvender psykologiske greb til at opnå ofrets tillid.

**Insider** dækker over angreb på it-infrastruktur, hvor én eller flere medarbejdere har udnyttet deres brugerprivilegier til at udføre angrebet.

# Forebyggende indsatser i 2019

**Forebyggelse og rådgivning**
CFCS' rådgivning har i 2019 blandt andet haft fokus på at styrke samarbejdet på tværs af de samfundskritiske sektorer inden for rammerne af den nationale cyber- og informationssikkerhedsstrategi og på at skabe et ensartet og fælles afsæt og dermed højne cybersikkerheden på tværs. CFCS har også rådgivet Forsvaret samt myndigheder og virksomheder uden for de seks samfundskritiske sektorer.

**Trusselsvurderinger**
CFCS har et løbende samarbejde med de decentrale cyber- og informationssikkerhedsenheder samt sektorerne generelt om udarbejdelse af relevante trusselsvurderinger til sektorerne. Som en del af dette samarbejde har CFCS indstationerede medarbejdere fra de kritiske sektorer for at sikre kendskabet og forbindelsen til sektorerne. Centeret offentliggjorde syv trusselsvurderinger og en undersøgelsesrapport i 2019. Tre af trusselsvurderingerne omhandlede cybertruslen specifikt for de samfundskritiske sektorer. Dertil kommer en række klassificerede trusselsvurderinger og rapporter til udvalgte kunder. Derudover bidrog CFCS med briefinger i både åbne og lukkede fora blandt andet med sigte på at skabe opmærksomhed om, at cybertruslen kræver et vedvarende ledelsesfokus hos myndigheder og virksomheder.

**Trusselsvurdering**
**Digitale gidseltagere på storvildtjagt**
Der er en stigende trussel fra målrettede ransomware-angreb, hvor kriminelle afpresser myndigheder og virksomheder for store pengebeløb ved at kryptere data på centrale it-systemer. I efteråret 2019 blev høreapparatsproducenten Demant A/S og televirksomheden GlobalConnect ramt af ransomware-angreb.

Trusselsvurderingen blev publiceret den 29. december 2019 og kan findes på *www.cfcs.dk*

**Trusselsvurdering**
**Cyberangreb mod leverandører**
Hackere kan angribe en leverandør for at benytte denne som springbræt til at kompromittere organisationens kunder. Kompromittering af en leverandør kan på én gang give adgang til mange mål, til indhentning af leverandørens kunde-data eller adgang til væsentlige dele af en sektors infrastruktur.

Trusselsvurderingen blev publiceret den 24. oktober 2019 og kan findes på *www.cfcs.dk*

**Målrettet rådgivning til de samfundskritiske sektorer**
CFCS har en dedikeret rådgivningskapacitet rettet specifikt mod de seks samfundskritiske sektorer og har et tæt samarbejde med de decentrale cyber- og informationssikkerhedsenheder (DCIS'er) for at understøtte en bedre cyber- og informationssikkerhed i sektorerne.

Centeret faciliterer et videndelingsnetværk for sektorernes decentrale cyber- og informationssikkerhedsenheder (DCIS-forum), som har til formål at øge videndelingen, styrke koordinationen på tværs af de samfundskritiske sektorer samt igangsætte og gennemføre fælles indsatser. Digitaliseringsstyrelsen og PET deltager også i forummet. Forummet drives med udgangspunkt i sektorernes ønsker og behov ikke mindst med henblik på erfaringsudveksling. I 2019 blev der afholdt syv møder med fokus på blandt andet videndeling om varsler, hændelseshåndtering og beredskab. DCIS-forum har nedsat en arbejdsgruppe, som arbejder for at dele viden om varsler og hændelser mere effektivt på tværs, for eksempel ved brug af en videndelingsplatform.

CFCS har sammen med PET og Digitaliseringsstyrelsen været en del af den taskforce, der med den nationale strategi blev nedsat for at hjælpe sektorerne godt i gang med udviklingen af deres sektorstrategier og opbygningen af de decentrale cyber- og informationssikkerhedsenheder. Taskforcens arbejde blev afsluttet med udgangen af 2019.

**Tekniske minimumskrav til statslige myndigheder**
Et vigtigt skridt i arbejdet med at højne cyber- og informationssikkerheden i 2019 var beslutningen om at indføre 20 tekniske minimumskrav til statslige myndigheder som led i den nationale cyber- og informationssikkerhedsstrategi. CFCS deltog i udarbejdelsen af minimumskravene og har fulgt op på kravene med rådgivning og vejledning blandt andet om DMARC til beskyttelse af e-mails og DNS-SEC rettet mod domæner og har kunnet konstatere en markant forbedring af sikkerheden hos de statslige myndigheder på disse områder.

De tekniske minimumskrav har primært til formål at beskytte statslige it-arbejdspladser, herunder arbejdsnetværk og arbejdsstationer, mod ondsindede cyber- og informationssikkerhedshændelser som for eksempel hackerangreb og spredning af malware. Størstedelen af kravene følger af eksisterende vejledninger og anbefalinger på området fra CFCS, Digitaliseringsstyrelsen og Datatilsynet. De øvrige krav er udarbejdet på baggrund af udbredt best practice. Minimumskravene er blevet vel modtaget i myndighederne og anses for at være et godt konkret skridt i retning af en bedre sikkerhed i staten. Implementeringen er igangsat i to faser med tidsfrister henholdsvis 1. januar 2020 og 1. juli 2020.

**Sikker kommunikation**
CFCS har i forbindelse med et initiativ i den nationale strategi for cyber- og informationssikkerhed i 2019 støttet Statens It med udvikling af en arbejdsplads, der kan anvendes til behandling af lavt klassificerede informationer. Derudover har centeret i 2019 haft fokus på at understøtte etablering af sikre kommunikationskanaler i Grønland og på Færøerne med henblik på at forbedre mulighederne for udveksling af klassificeret information mellem alle dele af rigsfællesskabet.

**Digitale afhængigheder**
CFCS har i 2019 i tæt samarbejde med de decentrale cyber- og informations-sikkerhedsenheder udarbejdet en kortlægning af digitale afhængigheder for samfundets kernefunktioner i og på tværs af sektorerne som led i den nationale cyber- og informationssikkerhedsstrategi. CFCS har sammen med de samfundskritiske sektorer udviklet en model, der betyder, at der nu for første gang er etableret et indledende overblik over, hvordan de digitale services og tjenester, der understøtter de samfundskritiske sektorers kernefunktioner, er gensidigt afhængige af hinanden. Kortlægningen kan danne grundlag for en prioritering af arbejdet med cybersikkerhed nationalt, på sektorniveau og lokalt hos de enkelte virksomheder og myndigheder. Overblik er en vigtig forudsætning for at kunne prioritere udbredelsen af den nye typer sensorer i sensornetværket, der skal bidrage til et nationalt cybersituationsoverblik, og for at kunne sætte ind med en forebyggende rådgivningsindsats der, hvor det betyder mest.

**Indsats i forhold til Grønland og Færøerne**
CFCS har oprettet en taskforce, der har til formål at strukturere og koordinere de indsatser, der gennemføres i Grønland og på Færøerne. I 2019 har fokus blandt andet været på at bistå Forsvarsministeriets departement i arbejdet med at forberede og udarbejde et udkast til en kongelig anordning, der sætter lov om Center for Cyber-sikkerhed i kraft for Grønland. I den forbindelse er der blevet udarbejdet en afdækning af de tekniske og logistiske udfordringer i forbindelse med monitorering i Grønland. Endelig har der været drøftelser med grønlandske og færøske myndigheder og virksomheder om styring af informationssikkerhed samt drøftelser med grønlandske og færøske myndigheder om udpegning af kritiske aktører i forhold til cyber- og informationssikkerhed og dialog med de færøske myndigheder i relation til håndtering af 5G-telenetværk.

**Oversigt over myndigheds- og forebyggelsesindsatser 2019**

| Kategorier | Antal |
|---|---|
| Rådgivnings- og kundemøder | 645 |
| Awareness-briefinger | 178 |
| It-sikkerhedsgodkendelser | 29 |
| Godkendelse af kryptoplaner | 48 |
| Tekniske sikkerhedseftersyn | 79 |
| Sikkerhedstekniske undersøgelser | 7 |
| Tempest zoning (udstrålingskontrol) | 4 |
| Tilsyn med informationssikkerhed | 21 |
| Varsler | 169 |
| Tweets | 677 |

**Varsler**
I forbindelse med væsentlige cyberangreb, aktuelle cybertrusler, it-sikkerheds-hændelser eller væsentlige sårbarheder, som kan have interesse og relevans for såvel en bred som en begrænset kreds af myndigheder, virksomheder og andre, udsender cybersituationscenteret varsler, som blandt andet indeholder konkrete

tekniske anbefalinger. Varslerne udarbejdes blandt andet med udgangspunkt i den viden fra sensornetværket, der monitorerer netværkstrafikken til og fra de tilsluttede myndigheder og virksomheder, men også med udgangspunkt i centerets øvrige kilder til viden. CFCS benytter også tweets fra blandt andet situationscenteret til at gøre opmærksom på trusler og sårbarheder med henblik på håndtering i relevant omfang.

**Vejledninger**
CFCS har i 2019 udarbejdet eller bidraget til en række nye vejledninger om blandt andet informationssikkerhed i leverandørforhold i samarbejde med Digitaliserings-styrelsen og håndtering af industrikontrolsystemer målrettet henholdsvis ledelse og driftsorganisation. Derudover er der udgivet en vejledning om håndtering af falske mails fra passive domæner og en omfattende vejledning om cybersikkerhed for bestyrelser i samarbejde med Bestyrelsesforeningen, Kromann Reumert og Industriens Fond samt en vejledning i anvendelse af cloudservices i samarbejde med Digitaliseringsstyrelsen. Centeret har også revideret den eksisterende password-vejledning, så den inkluderer seneste tænkning inden for god passwordpraksis. Alle vejledninger er tilgængelige på CFCS' hjemmeside.

**Sikkerdigital.dk**
På sikkerdigital.dk samles vigtig viden, vejledninger og konkrete værktøjer til en sikker digital hverdag til borgere, virksomheder og myndigheder. Portalen er etableret af Digitaliseringsstyrelsen og Erhvervsstyrelsen i samarbejde med CFCS, der bidrager til at højne kendskabet til cybertruslerne og kontinuerligt forbedre bevidstheden om, hvordan de imødegås med sikker adfærd. Dette gør CFCS blandt andet ved at udgive vejledninger, trusselsvurderinger og nyheder på sikkerdigital.dk. CFCS bidrager også til kampagner på sikkerdigital.dk. Dette gælder ikke mindst den nationale cybersikkerhedsmåned i oktober, hvor CFCS blandt andet stiller sig til rådighed for, at der kan bookes oplæg af centerets specialister via sikkerdigital.dk. Læs mere om den nationale cybersikkerheds-måned nedenfor. Portalen blev åbnet som led i den nationale strategi for cyber- og informationssikkerhed fra 2018.

Portalen findes her: *sikkerdigital.dk*

**Telesektorens decentrale cyber- og informationssikkerhedsenhed**
CFCS er myndighed for informationssikkerhed og beredskab i telesektoren og har bidraget til oprettelsen af en decentral cyber-og informationssikkerhedsenhed i telesektoren som led i den nationale cyber- og informationssikkerhedsstrategi. Enhedens arbejde blev udført af CFCS fra den 1. januar 2019 til den 31. maj 2019, frem til de 11 største teleoperatører etablerede en decentral enhed i lokaler hos DKCERT. Den decentrale enhed har i efteråret 2019 sammen med teleoperatørerne opdateret "Sårbarheds- og risikovurderingen for telesektoren i Danmark" samt øget bevidstheden om cybersikkerhed hos teleoperatørerne blandt andet gennem afholdelse af en workshop om insidertruslen. Enheden har derudover for at styrke videndelingen udrullet en Malware Information Sharing Platform (MISP) til alle de tilmeldte decentrale cyber- og informationssikkerhedsenheder.

**Industrikontrolsystemer** (SCADA)
Industrikontrolsystemer som for eksempel SCADA-systemer (Supervisory Control And Data Aquisition) er it-systemer af særlig betydning for samfundets kernefunktioner som elektricitet, transport, vandforsyning med videre. CFCS har udarbejdet en vejledning til håndtering af industrikontrolsystemer med input fra aktører i de samfundskritiske sektorer. Derudover faciliterer CFCS et videndelingsforum for specialister inden for SCADA-systemer på tværs af de samfundskritiske sektorer.

**Informationssikkerhed i leverandørforhold**
CFCS har blandt andet sammen med Digitaliseringsstyrelsen som led i arbejdet med den nationale strategi for cyber- og informationssikkerhed bidraget til arbejdet med initiativer, der fokuserer på vigtigheden af arbejdet med leverandørstyring og fastsættelse af sikkerhedskrav. På Forsvarsministeriets område har CFCS i 2019 fokuseret særligt på leverandørstyring som led i Forsvarsministeriets informationssikkerhedsstrategi 2018-2020.

**Cybersikkerhed i udbud og indkøb**
CFCS har i 2019 ydet rådgivning om cyber- og informationssikkerhed og sikkerhedskrav til SKI (Statens og Kommunernes Indkøbsservice A/S) og Moderniseringsstyrelsen med flere, der har ansvar for indkøb af it-udstyr og services, som har relevans i en national ramme. Indsatsen har haft særligt fokus på rådgivning om udarbejdelse af krav til leverandører, hvor kravene kan anvendes til at højne sikkerhedsniveauet under hensyn til den enkelte kundes særlige risikoforhold. Rådgivningen har også fokuseret på evaluering af tilbudsgiveres løsninger på baggrund af stillede krav.

**Folketingsvalg 2019 – rådgivning til de opstillingsberettigede partier**
Visse lande bruger påvirkningskampagner til at øve indflydelse på interne politiske forhold for at opnå egne udenrigspolitiske mål. De seneste år har der været en række eksempler på, at valg og folkeafstemninger i både Europa og USA er blevet påvirket. Ifølge Forsvarets Efterretningstjeneste er det meget sandsynligt, at fremmede magter også vil kunne gennemføre påvirkningskampagner mod Danmark, for eksempel i forbindelse med folketingsvalg. Op til folketingsvalget den 5. juni 2019 deltog CFCS i regeringens taskforce for valghandlinger og afholdt i samarbejde med PET blandt andet to workshops for de opstillingsberettigede partier med fokus på at orientere om risikoen for udenlandsk påvirkning, ”Hack og Læk”-cyberangreb og give råd til, hvordan partierne konkret kan styrke deres cyber- og informationssikkerhed.

**National og europæisk cybersikkerhedsmåned**
I oktober 2019 afholdtes for første gang en national cybersikkerhedsmåned i Danmark i forbindelse med den europæiske cybersikkerhedsmåned. Initiativet havde til formål at bidrage til at løfte den digitale sikkerhed for borgere, virksomheder og myndigheder i Danmark.

En lang række myndigheder, virksomheder, biblioteker og organisationer stillede deres viden gratis til rådighed og stod bag store og små aktiviteter og begivenheder. Digitaliseringsstyrelsen var national koordinator for cybersikkerhedsmåneden i samarbejde med CFCS.

Måneden gav anledning til events, morgenmøder, debatter, ekspertoplæg og nationale kampagner, der skal ruste danskerne mod de digitale trusler. Digitaliseringsstyrelsen og CFCS bidrog også selv aktivt til måneden. CFCS' specialister afholdt en række oplæg om cybertruslen, og hvordan man beskytter sig mod den. Derudover opdaterede CFCS blandt andet sin passwordvejledning og udsendte i samarbejde med Digitaliseringsstyrelsen en vejledning i informationssikkerhed i leverandørforhold. Af andre publikationer og aktiviteter kan nævnes:

- **Livehacking-event på Kulturnatten**
  Som en del af Kulturnatten og national cybersikkerhedsmåned demonstrerede CFCS' it-specialister, hvordan det er muligt at hacke computere og it-systemer, og hvad der kan gøres for at beskytte sig mod dette.

- **Europæisk cybermesterskab 2019 i Rumænien**
  Som led i cybersikkerhedsmåneden deltog det danske cyberlandshold i de europæiske cybermesterskaber i Bukarest, Rumænien. Cyberlandsholdet blev udvalgt efter et intenst forløb med en landsdækkende Cyberhunt og efterfølgende bootcamp. Over 200 danske it-talenter var med fra starten, og de 10 dygtigste blev udvalgt til at forsvare Danmarks farver til årets europæiske mesterskab i Rumænien.

- **Cybersikkerhedsbegreber – ordforklaringsliste**
  Cybersikkerhed har et hav af begreber og fagudtryk. CFCS lancerede i cybersikkerhedsmåneden en liste med forklaringer, der viser, hvordan CFCS bruger begreberne.

- **Ét klik kan ændre alt. National kampagne**
  CFCS bidrog også til en national fællesoffentlig kampagne, der i oktober satte fokus på nogle af de vigtigste digitale trusler og forsøg på digital svindel, som danskerne møder i deres hverdag.

Læs mere om cybersikkerhedsmåneden på sikkerdigital.dk/ncsm

**Cybersikkerhed på tværs af Europa**
Initiativet er inspireret af og ligger i forbindelse med den europæiske cybersikkerhedsmåned, som hvert år løber af stablen i oktober. Det er et initiativ under EU-agenturet ENISA (European Network and Information Security Agency).

Den europæiske cybersikkerhedsmåned udgøres hovedsageligt af de mange nationale kampagner og aktiviteter fra EU-medlemslandene rettet mod virksomheder, borgere og myndigheder.

**Fælles digital indgang for indberetninger på Virk.dk**
Videndeling vedrørende sikkerhedshændelser er afgørende for at opretholde et højt digitalt sikkerhedsniveau. For at gøre det nemt og enkelt for virksomheder og myndigheder at indberette sikkerhedshændelser blev der den 10. maj 2018 lanceret én fælles digital løsning til indberetning af sikkerhedshændelser på tværs af sektorer og myndigheder placeret på Virk.dk. Indberetningerne bidrager til at give et mere nuanceret og detaljeret billede af de sikkerheds-hændelser, der rammer myndigheder og virksomheder i Danmark. I CFCS er det situationscenteret, der er første modtager af indberetninger om sikkerheds-hændelser. CFCS modtog 38 indberetninger i 2019.

# Tilsynsopgaver i 2019

**Center for Cybersikkerheds opgaver som national it-sikkerhedsmyndighed**
CFCS skal som national it-sikkerhedsmyndighed blandt andet i henhold til Justits-ministeriets sikkerhedscirkulære sikkerhedsgodkende it-systemer og -installationer, som anvendes til behandling af klassificerede informationer. Centeret har i 2019 udstedt 29 it-sikkerhedsgodkendelser.

CFCS fører som national it-sikkerhedsmyndighed endvidere tilsyn med informations-sikkerheden i relation til klassificeret information i elektroniske informationssystemer samt kryptosikkerhed. Der er i 2019 gennemført otte tilsyn ved offentlige myndig-heder, som arbejder med klassificerede informationer.

CFCS har i 2019 desuden gennemført 13 tilsyn med styringen af informationssikkerheden på Forsvarsministeriets område. Tilsynet har haft hovedfokus på myndighedernes ledelsessystem for informationssikkerhed i henhold til ISO/IEC 27001. Tilsynet har i 2019 særligt haft fokus på handleplaner for håndtering af identificerede risici og implementering af kontroller relevante for sikkerhedsniveauet,

samt handleplaner for det videre arbejde med standarden. Tilsynet har desuden haft et særligt fokus på leverandørstyring.

**Center for Cybersikkerheds tilsynsopgaver på teleområdet**
CFCS har som led i sin lovbestemte rolle som tilsynsmyndighed for informationssikkerhed og beredskab på teleområdet i 2019 ført tilsyn hos udvalgte teleudbydere.

Tilsynet med informationssikkerheden har haft hovedfokus på at sikre, at teleudbyderne har gennemført en risikovurdering, der tager stilling til risikoen for tab af tilgængelighed, integritet og fortrolighed i de net og tjenester, der udbydes. Tilsyn med informationssikkerheden er i 2019 sket hos fem teleudbydere, hvilket er en stigning på 25 procent i forhold til 2018.

Derudover har der i 2019 været ført tilsyn med udvalgte teleudbyderes beredskab og krisestyring i form af dokumentation af virksomhedens krisestyringsplan og rapporter som beskriver øvelsesformål, forløb og opnåede erfaringer. Tilsyn med beredskab og krisestyring er i 2019 sket hos fem teleudbydere, hvilket er uændret i forhold til 2018.

# EU-samarbejdet i 2019

CFCS repræsenterer Danmark i bestyrelsen for EU's Cybersikkerhedsagentur, ENISA, der i 2019 fik et permanent mandat, flere ressourcer og nye opgaver, da den nye cybersikkerhedsforordning trådte i kraft. ENISA vil fortsat fungere som EU's ekspertisecenter for cybersikkerhed og levere rådgivning og ekspertise i forbindelse med udvikling af politikker og lovgivning og får flere ressourcer til dets nye opgave med at støtte arbejdet med cybersikkerhedscertificering. ENISA har ikke fået egne operative beføjelser, men får mulighed for at understøtte operationelt samarbejde mellem medlemsstaterne og EU's institutioner blandt andet ved at planlægge cybersikkerhedsøvelser på EU-plan. ENISA skal desuden fremme cyberhygiejne blandt borgere, organisationer og virksomheder i EU, blandt andet gennem samarbejde med medlemsstaterne om oplysningskampagner.

**Cybersikkerhedscertificering**
Den nye cybersikkerhedsforordning etablerer også en ny europæisk ramme for udarbejdelse og indførelse af cybersikkerhedscertificeringsordninger for informations- og kommunikationsteknologi (IKT) i form af produkter, tjenester og processer. Det er som udgangspunkt frivilligt for virksomheder at få deres produkter, tjenester eller processer certificeret, medmindre andet fastsættes i EU eller national lovgivning.

Rammen er etableret for at forbedre betingelserne for det indre digitale marked og øge cybersikkerhedsniveauet i EU. Hermed kan virksomheder få certificeret deres informations- og kommunikationsteknologiske produkter, tjenester og processer én gang i ét medlemsland og få et certifikat, der er gyldigt i alle medlemslande.

Medlemslandene skal i medfør af forordningen etablere nationale certificeringsmyndigheder, nationale akkrediteringsorganer og såkaldte overensstemmelsesvurderingsorganer. Den nationale myndighed for cybersikkerhedscertificering får det overordnede ansvar for certificeringsordninger i informations- og kommunikationsteknologi i Danmark. Myndigheden skal være i drift senest i juni 2021 og etableres under Erhvervsministeriet.

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), og har deltaget i NIS-samarbejdsgruppen og i det samarbejdet mellem de europæiske CSIRT'er (Computer Security Incident Response Teams), som er etableret i regi af direktivet. NIS-samarbejdsgruppen har etableret en række arbejdsgrupper vedrørende krisestyring af større hændelser, sikkerhedskrav og sektorspecifikke anliggender, herunder identifikation af operatører af væsentlige tjenester. CFCS har bidraget til dette arbejde i samarbejde med danske sektormyndigheder. CSIRT-samarbejdet omhandler videndeling og koordination af operative anliggender.

**Europæisk samarbejde om 5G-sikkerhed**
I kraft af sin rolle som national telemyndighed har CFCS været involveret i et omfattende europæisk samarbejde om 5G-sikkerhed koordineret af NIS-samarbejds-gruppen. Samarbejdet blev iværksat efter, at Kommissionen i marts 2019 udsendte en henstilling, der opstillede en plan for at etablere en koordineret tilgang til cyber-sikkerheden i 5G-netværk.

CFCS har i samarbejde med blandt andet den danske telesektor bidraget til dette europæiske samarbejde, som efterfølgende resulterede i, at Kommissionen i oktober 2019 kunne fremlægge en fælles risikovurdering af cybersikkerheden i medlems-landenes 5G-netværk.

I EU følges der løbende op på dette 5G-samarbejde, blandt andet med danske bidrag, som koordineres af CFCS. Efter intense drøftelser og forhandlinger i slutningen af 2019 opnåede samtlige medlemslande i januar 2020 enighed om den såkaldte 5G-værktøjskasse, der opstiller afbødningstiltag for at modgå risikovurderingens identificerede risici ved 5G-netværk.

**NIS-direktivet**
NIS-direktivet (direktiv om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer) skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer inden for en række samfundsvigtige sektorer i hele EU. Direktivet omfatter en række krav til myndighedsstruktur og samarbejde samt krav om, at der nationalt fastsættes sikkerhedskrav og underretningspligter for blandt andet udbydere af væsentlige tjenester. NIS-direktivet trådte i kraft i 2018 og er implementeret sektorvist i Danmark.

Kommissionen besøgte i september 2019 Danmark som led i en runde af landebesøg i EU, idet Kommissionen skal forelægge en rapport om NIS-direktivets virkemåde inden udgangen af 2020. CFCS koordinerede som nationalt kontaktpunkt besøget, som også omfattede møder mellem Kommissionen og repræsentanter for nationale kompetente NIS-myndigheder på områderne søfart, finans og udbud af digitale tjenester samt større operatører på områderne maritim transport, sundhed og finans. Kommissionen fik indsigt i, hvordan implementeringen i Danmark er sket ud fra sektoransvarsprincippet. Kommissionens fokus for besøget var på samarbejdet mellem medlemsstater, herunder ved identifikationen af udbydere af væsentlige tjenester, og på muligheden for at udpege udbydere, som er væsentlige for opretholdelsen af økonomiske aktiviteter.

# Publikationer i 2019

## Vejledninger

**Informationssikkerhed i leverandørforhold**
*(i samarbejde med Digitaliseringsstyrelsen)*
Vejledningen behandler de særlige forhold vedrørende informationssikkerhed, der er, når en organisation vælger at lægge dele af sin it-drift ud til en ekstern leverandør. Vejledningen dykker ned i alle faserne af et kunde-leverandørforhold fra udbud til ophør af samarbejdet.

**Vejledning i håndtering af industrikontrolsystemer målrettet ledelsen**
Vejledningen beskriver otte forhold, som ledelsen i en virksomhed, der anvender industrikontrolsystemer, skal være særligt opmærksomme på for at opretholde en sikker drift.

**Vejledning i håndtering af industrikontrolsystemer målrettet driftsorganisationen**
Vejledningen beskriver syv skridt til at opnå bedre sikkerhed i digitale overvågnings- og styringssystemer. Skridtene skal omsættes til konkrete handlinger i den enkelte driftsorganisation, så det er tilpasset virksomhedens systemer, netværk og organisering.

**Falske mails fra passive domæner**
Denne korte guide beskriver, hvordan man med to simple tiltag kan beskytte domæner, der normalt ikke bruges til mail, mod at fremmede misbruger domænet til afsendelse af falske mails. Guiden er et supplement til CFCS' vejledning "Reducér risikoen for falske mails".

**Cybersikkerhed for bestyrelser**
*(i samarbejde med Bestyrelsesforeningen, Kromann Reumert og Industriens Fond)*
Vejledningen er en indføring i bestyrelsens arbejde med cyber-og informations-sikkerhed. I vejledningen opstilles en række anbefalinger og spørgsmål, der er med til at give danske bestyrelser forskellige værktøjer, så de kan sparre med og udfordre direktionerne om virksomhedernes cyber-og informationssikkerhed.

**Vejledning i anvendelse af cloudservices**
*(i samarbejde med Digitaliseringsstyrelsen)*
CFCS har i samarbejde med Digitaliseringsstyrelsen udarbejdet en vejledning, der hjælper myndigheder med at beslutte, hvornår anvendelsen af cloudservices er en god idé. Vejledningen gennemgår de forretningsmæssige, juridiske og sikkerhedsmæssige overvejelser, som myndigheder bør gøre sig ved anvendelsen af cloudservices.

**Revideret passwordvejledning**
Vejledningen giver gode råd om valg af sikre, unikke passwords, og til hvordan passwordmanagers kan hjælpe med at håndtere de mange passwords, vi anvender. Vejledningen gør op med tidligere praksis med hyppige tvungne passwordskift og

fokuserer i stedet på længde over kompleksitet. Der er også råd til ledelsen om passwordpolitikker og til systemejere om, hvordan de bør håndtere passwords på sikker vis i organisationens systemer.

# Trusselsvurderinger

Hovedparten af trusselsvurderingerne er udgivet både på dansk og engelsk.

**Trusselsvurdering: Cybertruslen mod søfartssektoren**
Trusselsvurderingen redegør for cybertrusler, der er rettet mod den danske søfarts-sektor. Søfartssektoren i Danmark er vigtig for samfundets funktion, stabilitet og økonomi. Hensigten er at orientere søfartssektoren om truslerne, så den bedre kan beskytte sig. Trusselsvurderingen kan eksempelvis indgå i sektorens arbejde med den nationale strategi for cyber- og informationssikkerhed.

**Trusselsvurdering: Cybertruslen fra bevidste og ubevidste insidere**
Formålet med denne trusselsvurdering er at orientere ledelsen ved myndigheder og virksomheder om truslen fra insidere med adgang til forretningskritiske it-systemer. Medarbejdere, som er uopmærksomme, uagtsomme eller har ondsindede intentioner, kan forårsage skadelige kompromitteringer af informationssikkerheden i disse organisationer.

**Trusselsvurdering: Cybertruslen mod Danmark 2019**
Formålet med denne årlige, nationale trusselsvurdering er at redegøre for den samlede cybertrussel, der møder danske myndigheder og virksomheder. Truslen er størst fra cyberspionage udført af stater og fra cyberkriminalitet.

**Trusselsvurdering: Cybertruslen mod telesektoren**
Trusselsvurderingen redegør for de cybertrusler, som er rettet imod telesektoren i Danmark. Telesektoren i Danmark er af kritisk betydning for samfundets funktion, stabilitet og sikkerhed. Trusselsvurderingen kan eksempelvis indgå i risikovurderingen for virksomheder i sektoren.

**Trusselsvurdering: Cyberangreb mod leverandører**
Fremmede stater og kriminelle angriber ofte deres mål gennem forsyningskæden ved at kompromittere leverandører. Denne trusselsvurdering kan bruges af virksomheder og myndigheder til at sætte fokus på cybertruslen mod forsyningskæden.

**Trusselsvurdering: 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. Målgruppen for trusselsvurderingen er ledelsen og it-medarbejdere i danske lufttrafikstyrings- og luftfartsmyndigheder, lufthavne, fly-selskaber og underleverandører til flyproducenter.

**Trusselsvurdering: Digitale gidseltagere på storvildtjagt**
Trusselsvurderingen har til formål at informere myndigheder og virksomheder om truslen fra og modforanstaltninger mod målrettede ransomwareangreb, der kan have alvorlige konsekvenser.

# Undersøgelsesrapporter

**Undersøgelsesrapport: Forsøg på kompromittering af netværksudstyr**
Formålet med denne undersøgelsesrapport er at beskrive forsøg på kompromittering af dansk internetvendt netværksudstyr. Rapporten gør opmærksom på en bestemt type af cyberangreb og indeholder forslag til tiltag, som kan hjælpe myndigheder og virksomheder til at beskytte sig mod lignende aktivitet. Målgruppen for denne rapport samt anbefalinger er it-ledelse og it-teknikere.

# Andre publikationer

CFCS udgav i forbindelse med den nationale cybersikkerhedsmåned i oktober 2019 en liste med ordforklaringer, der viser, hvordan CFCS bruger ord og begreber inden for cybersikkerhed. Ordforklaringen kan findes på CFCS' hjemmeside *www.cfcs.dk*.

# Eksempler på varsler udsendt af cybersituationscenteret

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. Nedenstående varsler er anonymiserede versioner af udsendte varsler.

**Anonymiseret varsel: Sodinokibi Ransomware**
(TLP:GREEN)

**Til den it-sikkerhedsansvarlige**
CFCS er blevet bekendt med, at mindst ét angreb er fortaget mod kritisk dansk infrastruktur med en ransomware kaldet Sodinokibi eller Revil. Ransomwaren er observeret i april 2019 og er en såkaldt Ransomware-as-a-Service. Ransomwaren er blandt andet blevet set spredt via sårbare servere, der ikke er patchet.

**Yderligere information**
Der kan findes yderligere teknisk info omkring Sodinokibi ransomware på følgende links:

- *https://www.mcafee.com/blogs/other-blogs/other-blogs/mcafeelabs/mcafeeatr-analyzes-sodinokibi-aka-revil-ransomware-as-aservice-what-the-code-tellsus/*
- *https://www.cybereason.com/blog/the-sodinokibi-ransomwareattack*
- *https://www.tesorion.nl/aconnection-between-the-sodinokibiand-gandcrabransomware-families/https://www.trendmicro.com/vinfo/us/threatencyclopedia/malware/ransom.win32.sodinokibi.a*

**Anbefaling**
CFCS anbefaler blandt andet følgende modforanstaltninger, for at undgå ransomware:

- Segmentering af netværk.
- Hold samtlige operativsystemer og applikationer opdateret med seneste rettelser.

En detaljeret anbefaling for at forbygge ransomware, og hvis skaden er sket, kan findes på CFCS' hjemmeside, under vejledninger (https://fe-ddis.dk /cfcs/publikationer/Vejledninger/Pages/default.aspx):

- *https://feddis.dk/cfcs/publikationer/Documents/Ransomware_maj2016.pdf*
- *https://fe-ddis.dk/cfcs/publikationer/Documents/WannaCryV1_1.pdf*

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

**Anonymiseret varsel: Mistanke om kompromittering af internetvendte Sharepoint-servere**
(TLP:AMBER)

**Til den it-sikkerhedsansvarlige**
CFCS har konstateret, at en eller flere ondsindede aktører har forsøgt at kompromittere et større antal internetvendte Sharepoint-servere i Danmark fra april 2019 og frem. I forbindelse med vores analyser er vi blevet opmærksomme på, at [myndighed/virksomhed] muligvis også har været forsøgt kompromitteret. I det tilfælde, I har internetvendte Sharepointservere i jeres it-infrastruktur, bedes I følge den vedlagte rådgivning.

**Yderligere information**
13. marts 2019 blev en sårbarhed, CVE-2019-0604, offentliggjort, som gør det muligt at installere webshells på upatchede internetvendte sharepoint-servere. Exploitet bliver leveret via http POSTs til uri'en 'Picker.aspx'.

Hvis det lykkes en ondsindet aktør at installere webshells på serveren, kan de udnyttes til at downloade yderligere malware, der muliggør exfiltration af data og yderligere kompromitteringer i det lokale netværk.

Microsoft har i perioden 12. marts og 25. april udgivet sikkerhedsopdateringer, der fjerner sårbarheden.

**Anbefaling**
Hvis internetvendte Sharepoint-services har været upatchede i april 2019 og frem, anbefaler vi at undersøge følgende for at finde tegn på kompromittering:

- Findes en eller flere af følgende filer på serveren: 'error6.aspx', 'stylejs.aspx', 't.aspx', 'signin.aspx', 'ua.aspx', 'layoutValidationDefaults.aspx'?
- Er der blevet oprettet nye .aspx-filer på serveren i tidsrummet for hændelsen, der ikke har en legitim funktion?
- Er filen 'Picker.aspx' blevet slettet fra serveren?

Hvis der kan svares bekræftende på en eller flere af punkterne, anbefales det, at der tages tiltag til at undersøge serveren nærmere for malware, samt om der har været yderligere spredning i netværket.

**Anonymiseret varsel: Forbindelser til EmpireMonkey-infrastruktur**
(TLP:AMBER)

### Til den it-sikkerhedsansvarlige

CFCS har observeret to typer mistænkelig trafik fra jeres IP-range til infrastruktur, der bliver eller har været benyttet af aktøren EmpireMonkey.

### Yderligere information

Der er mellem d. 30. marts 2019 og d. 14. juni 2019 set fuldt etableret SSH-trafik fra jeres IP-adresse [myndighedens/virksomhedens IP-adresse] til IP-adressen [aktørens IP-adresse] på en ikke-standard port (tcp 5100).

Der er derudover siden d. 19. august 2019 observeret et større antal forbindelser fra jeres IP-adresse [myndighedens/virksomhedens IP-adresse] til IP-adressen [aktørens IP-adresse], også til port 5100.
I dette tilfælde lader det dog ikke til at dreje sig om SSH-forbindelser, men formodentlig om cryptomining trafik.

Der er set DNS-opslag fra jeres netværk til domænet [aktørens domæne] fra 30. marts 2019 indtil dags dato.
Domænet har været hostet på begge af de ovennævnte suspekte IP-adresser og er blandt andet nævnt i en ESET-rapport om LoudMiner, der beskriver dets brug i en cryptomining-kampagne.

[tekniske detaljer]

### Anbefaling

CFCS anbefaler, at der overvejes passende modforanstaltninger for at sikre de systemer, der genererer trafikken. Dette indebærer blandt andet at lokalisere den eller de maskiner, der genererer trafikken, og undersøge den/dem for malware.

#### Rådgivning

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

# 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 telemyndigheden**
Kontakt til telemyndigheden ved CFCS kan ske på telefon 33 32 55 80 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 sigte.

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

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