
# Center for Cybersikkerheds Beretning 2017


Center for Cybersikkerhed
Kastellet 30
2100 København Ø

Telefon: 3332 5580
www.cfcs.dk

## Cybertruslen

Danmark står fortsat over for en meget høj cybertrussel, særligt fra fremmede stater. Nogle stater forsøger vedholdende at udføre cyberspionage mod danske myndigheder og virksomheder for at stjæle informationer, der er af strategisk, politisk eller økonomisk betydning. Spionagen udgør en sikkerhedspolitisk og samfundsøkonomisk trussel mod Danmark og danske interesser. Enkelte stater har desuden udvist en mere offensiv adfærd, hvor de er villige til at udføre angreb, der har andre formål end cyberspionage. Disse kan værer bl.a. hack og læk af følsomme oplysninger og destruktive cyberangreb. Hertil kommer en meget høj trussel fra cyberkriminalitet. Cyberkriminalitet stiger i omfang og kompleksitet, og truslen er rettet mod både myndigheder, virksomheder og borgere.

Cybertruslen udvikler sig løbende, i takt med at viden og hackerværktøjer bliver tilgængelige for flere, og den teknologiske udvikling giver angriberne nye muligheder for at udnytte sårbarheder i it-systemer og netværk. Den globale digitalisering medfører ydermere, at cyberangreb, der starter på den anden side af jorden, hurtigt kan sprede sig til systemer og enheder i Danmark.

Cyberangreb kan have meget alvorlige konsekvenser, hvis data fra en offentlig myndighed eller privat virksomhed kompromitteres eller stjæles. Konsekvenserne kan eksempelvis være nedbrud af samfundsvigtig infrastruktur, tab af tillid, produktionstab, tab af markedsandele, tab af intellektuel ejendom og skade på organisationens omdømme.

## Center for Cybersikkerheds indsatser i 2017

Center for Cybersikkerhed (CFCS) blev oprettet i december 2012 som en del af Forsvarets Efterretningstjeneste (FE), og er Danmarks nationale it-sikkerhedsmyndighed og nationalt kompetencecenter på cybersikkerhedsområdet. Det er centerets mission at styrke beskyttelsen af Danmarks digitale infrastruktur samt styrke Danmarks evne til at imødegå cyberangreb. Dette gøres i kraft af en reaktiv indsats igennem centrets Netsikkerhedstjeneste, og en proaktiv indsats, igennem centrets rådgivningstjeneste.

## Den reaktive indsats i 2017

Center for Cybersikkerheds Netsikkerhedstjeneste har til opgave at afdække, analysere og bidrage til at imødegå it-sikkerhedshændelser hos forsvaret samt danske myndigheder og virksomheder, der er tilsluttet Netsikkerhedstjenestens sensornetværk. Netsikkerhedstjenestens indsats fokuserer på de mest avancerede cyberangreb, der oftest udføres af statsstøttede aktører, og cyberangreb, der i øvrigt kan påvirke samfundsvigtige funktioner i Danmark.

Center for Cybersikkerheds Netsikkerhedstjeneste har i 2017 haft fokus på at implementere og rodfæste mange initiativer fra 2016. Derudover har tjenesten generelt styrket sin robusthed omkring kerneindsatsen på cyberområdet. Dette kom bl.a. til udtryk i den endelige overgang til en egenudviklet sensorplatform ved indgangen til 2017. Dette har givet en mere tidssvarende løsning og styrket den fremadrettede udvikling.

## Tilslutninger

CFCS har også i 2017 haft en målsætning om at styrke sit samarbejde med Netsikkerhedstjenestens tilsluttede myndigheder og virksomheder. CFCS indgik ingen nye tilslutningsaftaler i 2017, men har brugt året på konsolidering af de eksisterende myndigheder og virksomheder, bl.a. et konsolideringsprojekt målrettet de militære myndigheder.

### Sensornetværket

CFCS' netværksanalytikere indsamler løbende den nyeste viden om cyberangreb og finder de digitale spor og mønstre, der identificerer et angreb. Disse digitale fingeraftryk lægges ud i specialkonstruerede alarmenheder, som er placeret på internetforbindelserne ved de tilsluttede myndigheder og virksomheder. Tilsammen danner alarmenhederne et såkaldt sensornetværk, som alarmerer centeret ved tegn på cyberangreb.

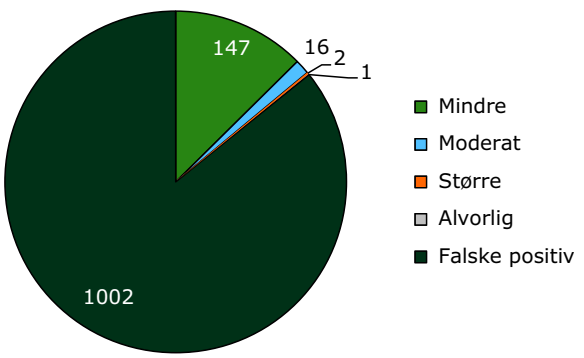
I 2017 modtog CFCS opsigelser af tilslutningsaftaler fra to private virksomheder.

Ved udgangen af 2017 havde CFCS i alt 39 tilslutningsaftaler til Netsikkerhedstjenesten, som inkluderer civile myndigheder (25), militære myndigheder (12) og private virksomheder (2).

### It-sikkerhedshændelser

Netsikkerhedstjenesten observerer fortsat udbredte forsøg på at udføre rekognosceringer mod tilsluttede kunder. Selv om dette ikke er et direkte forsøg på at opnå adgang til et system, kan succesfulde rekognosceringer udstyre angriberen med oplysninger, som kan udnyttes til at udføre mere målrettede angreb på et senere tidspunkt.

### Alvorlighedsgrad af sikkerhedshændelser




*Diagrammet angiver antallet af cybersikkerhedshændelser som Netsikkerhedstjenesten lukkede i 2017.*

I 2017 færdigbehandlede CFCS i alt 1168 it-sikkerhedshændelser, inkl. falske positive.

Angrebsforsøg via social engineering-metoder har i 2017 fortsat været udbredt. Dette indebærer eksempelvis forsøg på angreb via kundernes mailbokse ved hjælp af såkaldte phishing mails, som typisk forsøger at lokke modtageren til at aktivere ondsindede links og inficerede vedhæftninger.

### Cyberspionage mod Danmark

CFCS udgav i 2017 en undersøgelsesrapport, "Én aktør, mange angreb", som beskrev, hvordan et andet lands efterretningstjeneste i 2015 og 2016 udførte spionage mod Danmark. Netsikkerhedstjenesten fandt bl.a. tegn på, at aktøren havde haft adgang til og eksfiltreret data fra en række postkasser på et ikke-klassificeret mailsystem i forsvaret.

Efter rapportens udgivelse har centeret løbende haft fokus på sagen og udført analyser relateret til sagen. Analyserne har bl.a. vist, at der har været nye forsøg på kompromitteringer, som angriberne dog ikke har haft held med.

### Ransomware

I 2017 kom ransomware-begrebet på alles læber, da mange lande, heriblandt Danmark, blev udsat for to større ransomware-kampagner. Heraf viste den ene sig senere ikke reelt at være ransomware, men et destruktivt

### Definitioner på sikkerhedshændelser

| | |
|---|---|
| **Mindre:** | Reelt angreb, som ikke medførte 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 haft mærkbar betydning for den berørte organisation. |
| **Alvorlig:** | Kritiske systemer berørt eller system- eller administratorkonti kompromitteret. Hændelsen har haft alvorlig betydning for den berørte organisation. |
| **Falsk Positiv:** | Undersøgelse af alarm, men som ikke viste sig at være et angreb. |

**WannaCry**

Fredag den 12. maj 2017 blev der observeret en malwarekampagne, som var målrettet en kendt sårbarhed i en række styresystemer fra Microsoft. Malwaren indeholdt en komponent, en såkaldt crypto-locker, der går under navnet WannaCry, som går ind og krypterer udvalgte filtyper og sletter originalerne, hvorefter ofret automatisk opkræves en løsesum for at dekryptere filerne igen. Malware med disse egenskaber kendes også som ransomware. I den første bølge af WannaCry-kampagnen blev det observeret, at dem, der har designet malwaren, havde indbygget en form for nødstop – en såkaldt "kill switch". Malwaren indeholdt således et domæne, som malwaren kontaktede i forbindelse med infektionen. Hvis malwaren kunne kontakte domænet, ville krypteringen ikke blive udført. Domænet, som viste sig ikke at være taget i brug af andre, blev opkøbt og registreret i løbet af den 12. maj 2017 af en britisk it-sikkerhedsspecialist. Det betød, at malwaren nu kunne kontakte domænet og dermed ikke længere krypterede indholdet af de inficerede computere. Dermed blev den centrale del af angrebet de-facto standset.

Center for Cybersikkerhed gik tidligt i forløbet i gang med at skaffe overblik over situationen med et særligt fokus på eventuelle danske ofre. Center for Cybersikkerhed var bl.a. i kontakt med andre myndigheder og en større kreds af centrale danske internetudbydere. På det tidspunkt stod det klart, at der ikke var indikationer på, at danske statslige myndigheder eller samfundskritiske virksomheder var blevet ramt. I løbet af weekenden den 13.-14. maj 2017 blev situationen fulgt nøje, og der blev bl.a. udarbejdet og offentliggjort en trusselsvurdering om WannaCry, ligesom der blev udsendt et varsel til en kreds af myndigheder, virksomheder og andre interessenter.

Center for Cybersikkerheds varsel såvel som trusselsvurderingen baserede sig bl.a. på information fra det netværk af sensorer, som Center for Cybersikkerhed driver, og hvor det kunne observeres, at der i løbet af weekenden den 13.-14. maj 2017 skete et større antal scanninger efter sårbarheder. Der er fortsat ikke erkendt eksempler på danske statslige myndigheder eller samfundskritiske funktioner, der er blevet sat ud af drift på grund af kryptering som følge af WannaCry-kampagnen. Om vi i Danmark har et højere it-sikkerhedsniveau end andre lande, er et uafklaret spørgsmål.

Center for Cybersikkerhed har gennem længere tid haft fokus på behovet for, at sårbare systemer opdateres, og at systemer, der ikke længere kan opdateres, udfases eller afsondres fra internettet. Således advarede Center for Cybersikkerhed den 31. marts 2017 mod risikoen for udnyttelse af sårbare og ikke-længere opdaterbare Microsoftsystemer, og den 18. april 2017 blev kunder og interessenter specifikt varslet om nødvendigheden af at opdatere systemer mod en alvorlig pakke af sårbarheder, som bl.a. indeholdt den sårbarhed, der blev udnyttet af WannaCry.

angreb. CFCS havde i begge tilfælde skærpet opmærksomhed på udviklingen og omfanget af kampagnerne og publicerede relevante vejledninger og trusselsvurderinger på centrets hjemmeside, på baggrund af dialog med relevante virksomheder og partnere.

Selv om kampagnerne havde store konsekvenser for de enkelte ofre, vurderer CFCS, at den generelle skadesvirkning på dansk infrastruktur i disse konkrete tilfælde var begrænset.

**NotPetya**

NotPetya-cyberangrebet bredte sig i juni 2017 fra Ukraine til virksomheder i en række lande, herunder Mærsk, som har anslået, at angrebet kostede virksomheden mellem 1,6 – 1,9 mia. kr. NotPetya var maskeret som et ransomware-angreb, hvor ofrene kan få deres data tilbage mod en løsesum. NotPetya udgav sig derfor indledningsvist for at være ransomware, ligesom WannaCry. Men selv om malwaren afkrævede en løsesum, havde den reelt ikke funktionalitet til at genskabe adgangen til ofrenes filer, som det ellers teoretisk set er tilfældet ved ransomware. NotPetya bliver derfor anset som et angreb med destruktive formål og ikke som en ransomware-kampagne.

## Den proaktive indsats i 2017

CFCS' proaktive indsats har primært til formål at mindske risikoen for cyberangreb samt understøtte, at danske myndigheder og virksomheder er i stand til at håndtere cyberangreb, hvis de bliver ramt.

CFCS' proaktive indsats består primært af to opgaver: en rådgivningsindsats og tilsynsvirksomhed.

**Tabel over udvalgte proaktive indsatser i 2017**

| Kategorier | Antal |
|---|---|
| Rådgivnings- og kundemøder | 227 |
| Awareness-briefinger | 114 |
| It-sikkerhedsgodkendelser | 53 |
| Godkendelse af kryptoplaner | 57 |
| Sikkerhedstekniske eftersyn | 67 |
| Sikkerhedstekniske undersøgelser | 17 |
| Temptest-zoning (udstrålingskontrol) | 8 |

*Udvikling i tallene afhænger af til- og afgangene i de forskellige projekter.*

## Rådgivningsindsatsen

CFCS yder rådgivning på flere områder inden for informationssikkerhed, herunder om leverandørstyring, risikovurdering og SCADA-systemer[1]. Centeret oplever generelt en stor efterspørgsel på rådgivning og prioriterer indsatsen inden for målgrupper og områder, som er udpeget til at være af særlig samfundskritisk karakter. Det gælder eksempelvis sektorer inden for finans, energi, transport og tele, hvor fokus i rådgivningen i særlig grad har været på centerets trusselsvurderinger, herunder cyberspionage.

Som militær it-sikkerhedsmyndighed har CFCS en særlig opgave i forhold til at rådgive og vejlede forsvaret om cyber- og informationssikkerhed. Centerets største kunde er fortsat forsvaret med hensyn til såvel rådgivning som sikkerhedsgodkendelser i henhold til Justitsministeriets sikkerhedscirkulære.

CFCS har gennem hele 2017 ydet omfattende rådgivning i forbindelse med installation af infrastruktur og systemer i det nye domicil for Forsvarsministeriet og Værnsfælles Forsvarskommando. Opgaven med nyt kampfly til forsvaret har desuden været en omfangsrig opgave for centerets rådgivningskapacitet.

Som opfølgning på angrebet i 2016 mod forsvarets ikke-klassificerede, internetvendte mailsystem, mil.dk, har CFCS ydet rådgivning med fokus på sikring af internetvendte systemer, herunder med særligt fokus på mailsystemer. Det har også udmøntet sig i en skriftlig vejledning om og opfordring til brug af DMARC-teknologien.

**DMARC**

DMARC står for Domain-based Message Authentication, Reporting and Conformance. DMARC er et certifikatbaseret redskab til at forhindre mails med en forfalsket afsender i at nå ud til slutbrugere. DMARC kan samtidig begrænse misbrug af de domænenavne, organisationen ejer.

Den proaktive indsats voksede yderligere med støtte til dele af forsvarets operative myndigheder og elementer

[1] SCADA er en forkortelse for Supervisory Control and Data Acquisition, som også er en betegnelse for industrikontrol-systemer.

af den vitale danske infrastruktur. Dette var i form af sårbarhedsanalyser og awareness-briefinger om sårbarheder og tiltag til at modvirke disse. Der er igangsat en række initiativer med forsvaret og dele af energiforsyningssektoren om sårbarhedsanalyser af SCADA-/ICS[2)] -systemer.

### Tilsynsvirksomhed

CFCS har i 2017 ført tilsyn med informationssikkerheden på Forsvarsministeriets område, herunder styrelsernes implementering af it-sikkerhedsstandarden ISO 27001. Standarden ISO 27001 omhandler et ledelsessystem til risikostyring af informationssikkerhed, og tilsynet har bl.a. omfattet myndighedernes risikovurdering og udvalgte sikkerhedsforanstaltninger omkring eksempelvis leverandørstyring.

Tilsynsopgaven er voksende i forbindelse med en række større projekter i forsvaret.

### Teleområdet

I 2017 har CFCS, på baggrund af lov om net- og informationssikkerhed (NIS-loven), ført tilsyn med teleudbydere på såvel informationssikkerheds- som beredskabsområdet. Derudover har CFCS på baggrund af et strømnedbrud på Bornholm i starten af 2017 ført tilsyn med ejere af mobilnet i Danmark. Dette med henblik på at få afklaret deres strategi for etablering af nødstrøm, der en del af det beredskab, som gør, at udbydere i videst muligt omfang skal kunne opretholde udbuddet af net og tjenester i ekstraordinære situationer.

Derudover har CFCS fortsat arbejdet med it-sikkerhedsrevision af Nianets kontrakt med Moderniseringsstyrelsen om levering af datakommunikation til staten. CFCS har assisteret Statens og Kommunernes Indkøbsservice (SKI) med henblik på at definere de it-sikkerhedskrav, der indgik i forbindelse med etablering af en ny SKI-aftale om telefoni og mobilt bredbånd.

CFCS har i 2017 afholdt en række dialogmøder med teleudbydere omkring de informationssikkerhedsmæssige og beredskabsmæssige aspekter i forbindelse med teleudbydernes forhandlinger om nye leverancer af kritiske netkomponenter, systemer og værktøjer samt evt. drift heraf til det danske telenet. Der har ikke i 2017 været anledning til, med hjemmel i NIS-loven, at udstede påbud om ekstra sikkerhedsforanstaltninger. CFCS har modtaget et antal lovmæssige underretninger om brud på informationssikkerheden, der har væsentlige følger for driften af net og tjenester. Disse underretninger danner grundlag for CFCS' underretningsforpligtelse om hændelser i danske telenet over for ENISA (European Network and Information Security Agency).

### NIS-direktivet

Implementeringen af direktivet sker inden for en række forskellige ministerområder, hvis myndigheder hver især har ansvaret for at implementere direktivet inden for eget ressort. Med henblik på at sikre erfaringsudveksling og ensretning af de tværgående elementer af direktivet har CFCS i løbet af 2017 bistået med koordination af den nationale gennemførelseslovgivning. Herudover bliver CFCS tilsynsmyndighed for internetudvekslingspunkter og varetager rollen som nationalt kontaktpunkt og national CSIRT (Computer Security Incident Response Team).

#### NIS-direktivet

NIS-direktivet er et EU-direktiv, som trådte i kraft 9. maj 2018. NIS står for "net- og informationssikkerhed". Direktivet har til formål at sikre et højt fælles sikkerhedsniveau for net- og informationssystemer inden for en række samfundsvigtige sektorer i hele EU.

NIS-direktivet fastlægger krav til rammerne for dette fælles arbejde både nationalt og på EU-niveau, herunder krav til samarbejdsorganer og myndighedsstruktur. Der stilles også krav om, at der nationalt fastsættes sikkerhedskrav og underretningspligter for operatører af væsentlige tjenester og udbydere af digitale tjenester.

[2)] ICS er en forkortelse for Industrial Control System

### National strategi for cyber- og informationssikkerhed

I 2017 har CFCS deltaget i sekretariatet for udarbejdelsen af den nye nationale strategi for cyber- og informationssikkerhed. Strategien skal bidrage til at løfte det nationale niveau for cyber- og informationssikkerhed og fokuserer på arbejdet hermed i en række samfundsvigtige sektorer, i statslige myndigheder og blandt borgere og virksomheder. Flere initiativer i strategien vil berøre centerets arbejde de kommende år. Foruden de opgaver, der følger af forsvarsforliget 2018-2023, som også er indeholdt i strategien, vil CFCS bl.a. bistå arbejdet med at løfte cyber- og informationssikkerheden i samfundsvigtige sektorer. CFCS vil ligeledes indgå i et styrket samarbejde med andre myndigheder med ansvar for cyber- og informationssikkerhed.

### Om FE's Center for Cybersikkerhed

Center for Cybersikkerheds (CFCS') placeringen ved Forsvarets Efterretningstjeneste (FE) skaber en række synergieffekter og sikrer samtidig, at CFCS i sin indsats for at styrke Danmarks robusthed mod cyberangreb har adgang til den særlige efterretningsbaserede viden, som FE råder over."

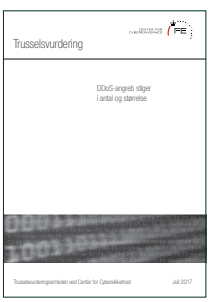
CFCS er en dynamisk arbejdsplads med mange forskellige typer af højtspecialiserede medarbejdere, herunder netværksanalytikere, malwareanalytikere, pen-testere, informationssikkerhedsrådgivere og teleingeniører. Størstedelen af centerets medarbejdere har en it-uddannelse eller anden teknisk baggrund. Men centeret har også medarbejdere, hvis formelle uddannelse er mindre vigtig, 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. Ved udgangen af 2017 var der knap 100 medarbejdere i centeret.

## Publikationer i 2017

Center for Cybersikkerhed udarbejder løbende trusselsvurderinger, undersøgelsesrapporter og vejledninger med henblik på at varsle om cybertruslen samt understøtte en forebyggende indsats.

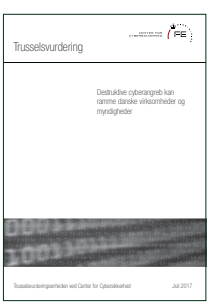

**Trusselsvurdering: Cybertruslen mod Danmark 2017**

I den årlige vurdering af cybertruslen mod Danmark tager CFCS udgangspunkt i fire formål med cyberangreb: cyberspionage, cyberkriminalitet, cyberaktivisme og cyberterror. CFCS vurderer, at truslen fra cyberspionage og cyberkriminalitet er meget høj, som er det højeste trusselsniveau, CFCS opererer med.




**Trusselsvurdering: DDoS-angreb stiger i antal og størrelse**

I denne trusselsvurdering vurderer CFCS, at antallet af Distributed Denial of Service-angreb (DDoS-angreb) er stigende, og at særligt hyppigheden og størrelsen af de kraftige angreb er øget.

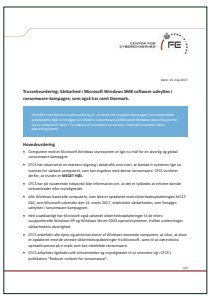



**Trusselsvurdering: Destruktive cyberangreb kan ramme danske virksomheder og myndigheder**

CFCS gør i denne trusselsvurdering danske virksomheder og myndigheder opmærksomme på, at risikoen for at blive ramt af destruktive cyberangreb er forhøjet i forhold til det generelle trusselsniveau, hvis de er til stede i særlige konfliktområder, f.eks. i Mellemøsten, Østeuropa og Asien.

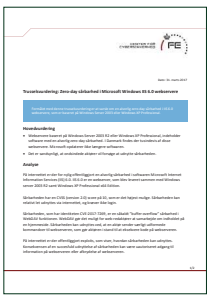
**Trusselsvurdering: Truslen fra hackerværktøjer mod Windows styresystemer**

I denne trusselsvurdering varsler CFCS om, at fremkomsten af nye hackerværktøjer mod Windows styresystemer vil medføre en øget risiko for, at virksomheder eller myndigheder, som anvender disse styresystemer, bliver inficeret med malware. Risikoen er særlig stor, hvis der anvendes Windows styresystemer, som ikke længere supporteres af Microsoft.



**Trusselsvurdering: Sårbarhed i Microsoft Windows SMB software udnyttes i ransomware-kampagne, som også har ramt Danmark**

CFCS varsler i denne trusselsvurdering om den verdensomspændende WannaCry ransomware-kampagne, som forsøger at inficere sårbare Microsoft Windows systemer.

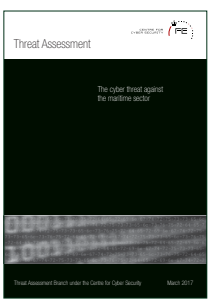


**Trusselsvurdering: Zero-day sårbarhed i ikke-supporterede Microsoft Windows IIS 6.0 webservere**

CFCS varsler i denne trusselsvurdering om en sårbarhed i webservere, som er baseret på Windows Server 2003 R2 eller Windows XP Professional.

**Trusselsvurdering: Zero-day sårbarhed i Cisco-servere kan udnyttes via Telnet**

I denne trusselsvurdering varsler CFCS om en sårbarhed i visse Cisco-servere med IOS-software. Sårbarheden kan udnyttes via åbne Telnet-forbindelser.

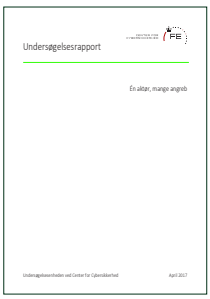



**Threat assessment: The cyber threat against the maritime sector**

In this assessment, Centre for Cyber Security analyses the cyber threats that particularly the commercial businesses in the maritime sector are exposed to. Old threats such as smuggling and theft are increasingly becoming cyber-enabled.

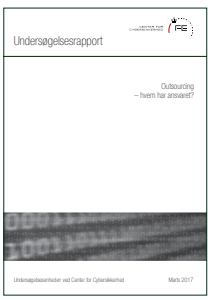

**Trusselsvurdering: Cybertruslen mod telesektoren i Danmark**

CFCS vurderer cybertruslen mod den danske telesektor. Truslen kommer især fra cyberkriminalitet og cyberspionage.




**Undersøgelsesrapport: En aktør, mange angreb**

Danske myndigheder og virksomheder er truet af spionage via internettet. Rapporten beskriver, hvordan en udenlandsk statslig aktør har forsøgt og til dels haft succes med at kompromittere en e-mail-tjeneste inden for Forsvarsministeriets myndighedsområde.




**Undersøgelsesrapport: Outsourcing – hvem har ansvaret?**

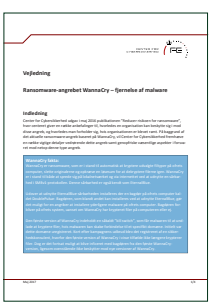
CFCS sætter fokus på udfordringerne med uklare aftaler mellem it-leverandør og kunde. Det sker med baggrund i en hændelse, hvor hackere udnyttede svagheder hos to it-hostingfirmaer og skaffede sig adgang til kundernes netværk.


**Vejledning: Reducér risikoen for falske mails**

CFCS anbefaler myndigheder og virksomheder at implementere DMARC for at reducere antallet af falske mails.


**Vejledning: Cyberforsvar der virker**

"Cyberforsvar der virker" er en praksisanvisning i robust cybersikkerhed. Budskabet er bl.a., at et effektivt cyberforsvar i en organisation ikke kan klares med tekniske løsninger alene, men også kræver handlingsplaner og forankring i ledelsen. Derudover beskriver vejledningen vigtigheden i, at de enkelte medarbejdere informeres, så de kan agere sikkerhedsbevidst.




**Vejledning: Ransomware-angrebet WannaCry – fjernelse af malware**

CFCS har undersøgt det konkrete angreb og giver i vejledningen en række anbefalinger til, hvad man gør, hvis man er blevet angrebet.

**Kontakt til Center for Cybersikkerhed**
CFCS kan inden for daglig kontortid (8-16) kontaktes på telefon 33 32 55 80 eller på e-mail cfcs@cfcs.dk.

Myndigheder og virksomheder, der beskæftiger sig med samfundsvigtige funktioner, kan i forbindelse med it-sikkerhedshændelser kontakte Netsikkerhedstjenesten døgnet rundt på vagttelefon 32 89 89 89 eller på e-mail cert@cert.cfcs.dk. Kontakt til telemyndigheden ved Center for Cybersikkerhed kan ske på telefon 33 32 55 80 eller på e-mail tele@cfcs.dk.