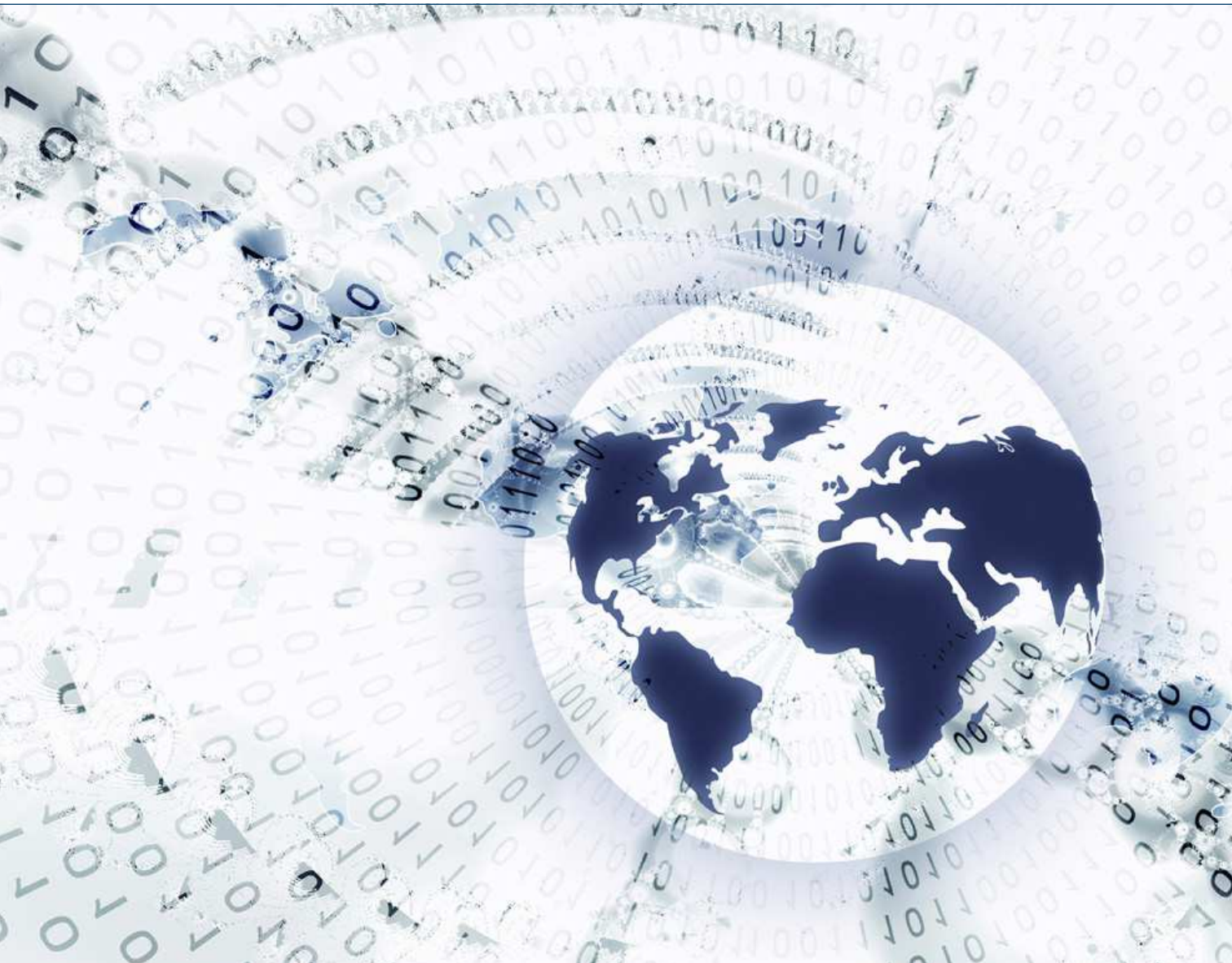
CENTER FOR
CYBERSIKKERHED

Center for Cybersikkerheds Beretning 2016



Center for Cybersikkerhed
Kastellet 30
2100 København Ø

Telefon: 3332 5580
www.cfcs.dk

Cybertrusler

Cybertrusler er et af de højst prioriterede områder i Forsvarets Efterretningstjeneste (FE), og FE's Center for Cybersikkerhed (CFCS) arbejder målrettet for at styrke Danmarks robusthed mod cyberangreb.

FE vurderer, at der er en meget høj cybertrussel mod Danmark, særligt fra cyberspionage, men også fra cyberkriminalitet. Hertil kommer en potentiel trussel fra fremmede stater, som benytter cyberangreb til at forsøge at påvirke meningsdannelsen i andre lande. Cybertruslen udvikler sig hastigt og løbende, i takt med at den teknologiske udvikling spredes til flere aktører og giver angriberne nye muligheder for at udnytte sårbarheder i it-systemer og netværk. Cybertruslen er en særdeles aktiv trussel, der har både sikkerhedspolitiske og samfundsøkonomiske konsekvenser for Danmark.

Cyberspionage mod offentlige og private mål udgør den alvorligste cybertrussel mod Danmark. Truslen kommer primært fra stater eller statsstøttede aktører, hvis interesse i at spionere mod Danmark kan være både strategisk, politisk og kommerciel. FE har gennem de seneste år konstateret en stigning i angreb fra stater, og der er kontinuerlige forsøg på at kompromittere både danske myndigheder og virksomheder. Cyberkriminalitet er ligeledes stigende i omfang og kompleksitet og udgør en meget høj cybertrussel mod både myndigheder, virksomheder og borgere.

Trusselsniveauet

Truslen fra cyberspionage og cyberkriminalitet mod danske myndigheder og virksomheder er MEGET HØJ. Det vil sige, at der er en specifik trussel. Der er således kapacitet, hensigt, planlægning og mulig iværksættelse. Angreb/skadevoldende aktivitet er meget sandsynlig.

Den reaktive indsats i 2016

Center for Cybersikkerheds netsikkerhedstjeneste har til opgave at opdage, 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.

Sensornetværket

CFCS udvikler og opdaterer løbende netsikkerhedstjenestens sensornetværk med henblik på at kunne imødegå de mest avancerede cyberangreb ud fra det aktuelle trusselsbillede. Centerets netværksanalytikere indsamler således 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 CFCS ved tegn på cyberangreb hos de tilsluttede myndigheder og virksomheder.

I 2016 har CFCS haft fokus på at udfase den hidtidige sensorplatform til fordel for et egenudviklet og mere tidssvarende system. Den endelige udfasning blev afsluttet ultimo 2016, hvor den gamle platform endegyldigt blev lukket ned.

Tilsyn med Center for Cybersikkerhed

Tilsynet med Efterretningstjenesterne er et særligt uafhængigt kontrolorgan, der har ført tilsyn med CFCS' behandling af personoplysninger siden 1. juli 2014, hvor lov om Center for Cybersikkerhed trådte i kraft. Tilsynet har i henhold til lov om Center for Cybersikkerhed tilsvarende bemyndigelser og adgang til oplysninger som efter FE-loven.

Hvert år offentliggør Tilsynet med Efterretningstjenesterne den årlige redegørelse om tilsynet med Center for Cybersikkerhed. Efter offentliggørelsen vil redegørelsen være tilgængelig på CFCS' hjemmeside www.cfcs.dk

Tilslutninger

CFCS har i 2016 haft en målsætning om at styrke sit samarbejde med netsikkerhedstjenestens tilsluttede myndigheder og virksomheder. Dette har affødt en række initiativer, såsom etableringen af et servicekatalog, et nyt kontaktpunkt, nye målrettede skriftlige produkter samt en mere opsøgende tilgang til eksisterende tilsluttede myndigheder og virksomheder.

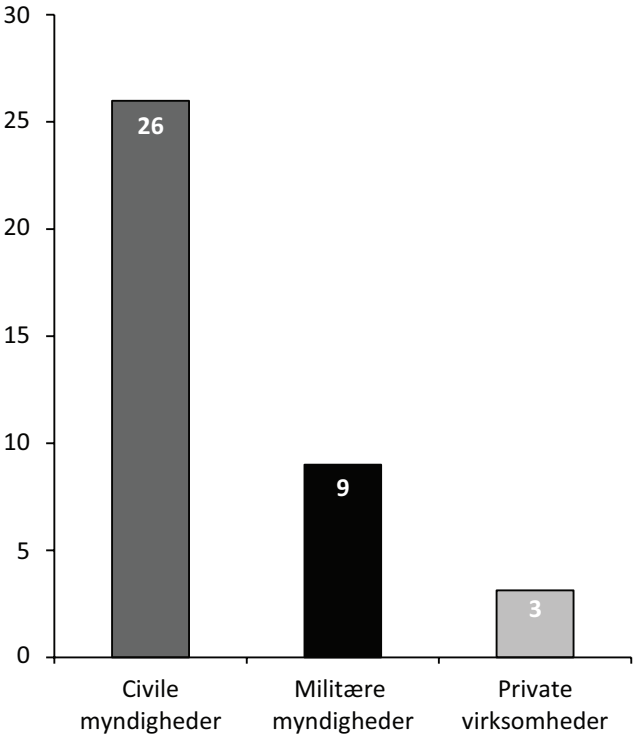
CFCS har endvidere iværksat en omfattende revidering af de interne processer omkring, hvordan sensortilslutningen håndteres i praksis. Dette har bl.a. haft til formål at effektivisere og yderligere strukturere hele forløbet, fra den indledende kontakt og til netværkssensoren er installeret.

CFCS indgik nye tilslutningsaftaler med tre civile organisationer i 2016. Denne fortsatte udvikling er et resultat af omlægninger på myndighedsområdet samt en generel øget opmærksomhed på nødvendigheden af at opprioritere it-sikkerheden blandt myndigheder og virksomheder, som i stadig højere grad håndterer data og udbyder services, der udgør samfundsvigtige funktioner. I 2016 har der ikke været nogen midlertidige tilslutninger til netsikkerhedstjenesten.

I 2016 modtog CFCS opsigelser af tilslutningsaftaler fra tre civile organisationer. I det ene tilfælde sluttede samarbejdet, idet en styrelse rent netværksmæssigt blev lagt under sit eget ministerområde og dermed blev dækket af den pågældende sensor. I de to andre tilfælde var der tale om et fravalg af forlængelsen af tilslutningsaftalen som konsekvens af de nye økonomiske rammer, som overgangen til det nye sensorsystem har medført.

CFCS har ved udgangen af 2016 i alt 38 tilslutningsaftaler til netsikkerhedstjenesten, som inkluderer civile myndigheder, militære myndigheder og private virksomheder.

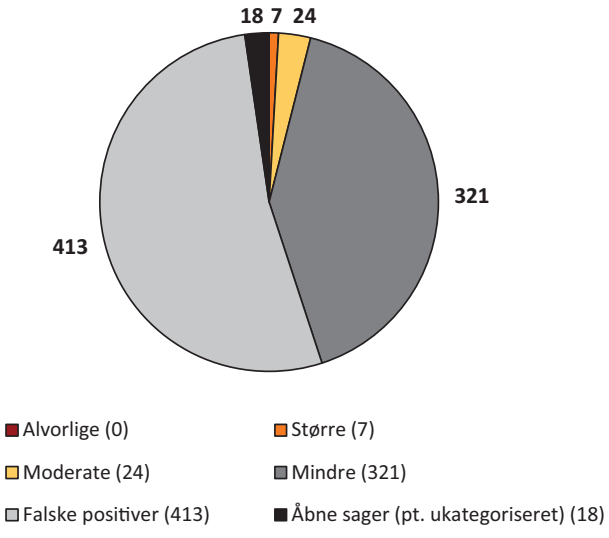
Oversigt over netsikkerhedstjenestens tilslutningsaftaler pr. 31. december 2016



Sikkerhedshændelser

Netsikkerhedstjenesten har i 2016 behandlet i alt 783 it-sikkerhedshændelser, som er inddelt efter alvorlighedsgrad ud fra, i hvilket omfang den tilsluttede myndighed eller virksomhed er berørt.

Oversigt over sikkerhedshændelser i 2016



Definitioner på sikkerhedshændelser

Alvorlig: Kritisk system berørt eller system- eller administratorkonti kompromitteret. Hændelsen har haft alvorlig betydning for den berørte organisation.
Større: Kritisk system berørt eller system- eller administratorkonti kompromitteret. Hændelsen har haft mærkbar betydning for den berørte organisation.
Moderat: Ingen kritiske systemer berørt, ingen system- eller administratorkonti kompromitteret. Begrænset betydning for den berørte organisation.
Mindre: Reelt angreb, som ikke medfører kompromittering.
Falsk positiv: Undersøgelse af alarm viser ikke tegn på angreb.

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.

I 2016 har CFCS bl.a. observeret eksempler på, at ondsindede aktører har kunnet tiltvinge sig adgang til servermiljøer hos danske myndigheder og virksomheder grundet fejlkonfigurationer og sårbarheder i ældre software. Netsikkerhedstjenesten assisterede i forskellig udstrækning de ramte myndigheder og virksomheder med at analysere og identificere omfanget af cyberangrebene.

De to mest hyppige angrebsforsøg, som netsikkerhedstjenesten observerede i 2016, var diverse former for social engineering og generel netværksrekognoscering. Selv om sidstnævnte ikke nødvendigvis udgør et decideret angreb, kan en succesfuld netværksscanning, der typisk ikke er specielt ressourcekrævende at udføre, give en ondsindet aktør afgørende oplysninger, som kan udnyttes til at målrette et senere cyberangreb.

Social engineering omfatter eksempelvis spear phishing-mails og watering hole-hjemmesider, som er kompromitterede, legitime hjemmesider, som bliver udnyttet til at inficere de besøgende med malware. Spear phishing-mails er målrettet enkeltmodtagere i en organisation med det formål at lokke modtageren til, i god tro, at aktivere ondsindede links eller vedhæftede filer, som inficerer computeren med malware. Disse former for angreb er således afhængige af handlinger fra en bruger for at kunne lykkes. Særligt spear phishing-angreb er fortsat en populær angrebsvektor for APT-aktører.

Frivillig underretningsordning

Den frivillige underretningsordning er et supplement til de obligatoriske underretningsordninger for offentlige myndigheder og for telesektoren.

I forbindelse med at lov om net- og informationssikkerhed trådte i kraft den 1. juli 2016, blev det muligt for virksomheder at indsende informationer om sikkerhedshændelser til CFCS uden at blive omfattet af aktindsigt.

Ved at opbygge en større og bredere viden om cyberangreb i den private og offentlige sektor bliver CFCS bedre rustet til at yde rådgivning og bistand i forbindelse med fremtidige cyberangreb.

Siden ordningen trådte i kraft, har CFCS modtaget 16 underretninger, som bl.a. vedrører DDoS-angreb, phishing-forsøg og CEO-fraud-mails.

Netsikkerhedstjenesten gennemfører løbende netværks- og malwareanalyser i forbindelse med sikkerhedshændelser, hvor der er grundlag for at foretage en nærmere sikkerhedsteknisk analyse. CFCS har gennemført 35 sikkerhedstekniske analyser i 2016.

Varslinger

I 2016 har CFCS udsendt 120 varslinger til de it-sikkerhedsansvarlige hos myndigheder og virksomheder, der er tilsluttet netsikkerhedstjenestens sensornetværk.

Den proaktive indsats i 2016

Center for Cybersikkerhed er national it-sikkerhedsmyndighed og ressortmyndighed for informationssikkerhed og beredskab på teleområdet. Centerets 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.

Tabel over udvalgte proaktive indsatser i 2016

Kategorier	Antal
Rådgivnings- og kundemøder	298
Awareness-briefinger	112
It-sikkerhedsgodkendelser	60
Godkendelse af kryptoplaner	104
Sikkerhedstekniske eftersyn	62
Sikkerhedstekniske undersøgelser	19
Tempest-zoning (udstrålingskontrol)	7

Rådgivningsindsatsen

CFCS yder rådgivning på flere områder inden for informationssikkerhed, herunder logning, leverandørstyring, it-risikovurdering og SCADA-industrielle kontrolsystemer. CFCS' rådgivning indbefatter både konkrete anbefalinger af teknisk karakter og anbefalinger af mere styringsmæssig karakter. Rådgivningen omfatter også konkrete anbefalinger i tilknytning til centerets trusselvurderinger til sektorer eller specifikke myndigheder, herunder i relation til cyberspionage- og insidertruslen. CFCS har i 2016 ydet rådgivning til myndigheder inden for en række forskellige sektorer, herunder finans-, energi-, transport- og telesektoren.

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 således gennem hele 2016 ydet omfattende rådgivning i forbindelse med installation af infrastruktur og systemer i det kommende nye domicil for Forsvarsministeriet og Værnsfælles Forsvarskommando på Holmens Kanal 9.

Forsvarets webmail til kommunikation af ikke-klassificeret information, mil.dk, har gennem 2015 og 2016 været udsat for en vedvarende angrebskampagne, og centerets analyse af indgående trafik til domænet samt analyser af logfiler viser, at der med meget stor sandsynlighed er tale om et angreb fra en statsstøttet aktør. Centeret har gennem 2016 ydet rådgivning i form af mere reaktive tiltag i relation til den eksisterende løsning og proaktivt i relation til en ny, sikrere løsning.

Sikkerhedsteknologi

På det sikkerhedsteknologiske område har CFCS i 2016 gennemført sikkerhedstekniske eftersyn, undersøgelser og analyser ved en lang række af Forsvarets myndigheder. Dette omfatter proaktive foranstaltninger mod aflytning, forholdsregler for udstrålingskontrol, penetrationstests samt specifikke og generelle awareness-briefinger om it-systemer og mobile enheder.

Tilsynsvirksomhed

CFCS har i 2016 styrket tilsynet med informationssikkerheden på Forsvarsministeriets område. Der er bl.a. gennemført tilsyn med informationssikkerheden ved samtlige styrelser under Forsvarsministeriet med fokus på myndighedernes implementering af it-sikkerhedsstandarden ISO 27001.

Standarden ISO 27001 omhandler et ledelsessystem til risikostyring af informationssikkerhed, og tilsynet har primært omfattet myndighedernes risikovurdering og risikohåndtering samt implementering af udvalgte sikkerhedsforanstaltninger med henblik på at sikre informationers fortrolighed, integritet og tilgængelighed.

Teleområdet

I 2016 har CFCS udstedt nye bekendtgørelser om informationssikkerhed og beredskab med hjemmel i lov om net- og informationssikkerhed (NIS-loven). Bekendtgørelserne trådte i kraft medio 2016 og primo 2017, og som følge heraf gennemføres der først tilsyn baseret på det nye lovgrundlag i 2017.

CFCS har i 2016 gennemført awareness-aktiviteter rettet mod telebranchen med henblik på at oplyse om de nye forpligtelser i NIS-lovgivningen. På tilsynsområdet har centeret primært kontrolleret, om de krav, der er til informationssikkerhed hos en række teleudbydere, bliver overholdt. CFCS har desuden påbegyndt en it-sikkerhedsrevision i henhold til Nianets kontrakt med Moderniseringsstyrelsen om levering af datakommunikation til staten.

Efter NIS-lovgivningens ikrafttræden 1. juli 2016 har CFCS haft en række dialogmøder med teleudbyderne i forbindelse med lovmæssige underretninger forud for påbegyndte forhandlinger om aftaler vedrørende leverancer af kritiske netkomponenter, systemer og værktøjer og eventuel drift heraf til danske telenet. Der har ikke været anledning til med hjemmel i NIS-lovgivningen at udstede påbud om sikkerhedsforanstaltninger. Derudover har CFCS modtaget et antal ligeledes 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).

CFCS har i 2016 i samarbejde med TDC, Telenor, Telia og Hi3G taget initiativ til en opdateret brancheaftale om prioriteret adgang for opkald i mobilnettene. Ordningen henvender sig til myndigheder og private beredskabsaktører, som ved varetagelsen af samfundsvigtige opgaver skal kunne gives forrang i mobilnettet, hvis nettet er overbelastet under ekstraordinære forhold som eksempelvis større ulykker eller katastrofer i samfundet.

Samarbejdsfora

For at skabe øget kendskab til cybertruslen og styrke den proaktive dialog om cybersikkerhed har CFCS udbygget centerets relationer med interessenter og samarbejdspartnere i Danmark. I 2016 har CFCS således gennemført en række møder i Den Tværministerielle Kontaktgruppe vedrørende Cybersikkerhed, som er et netværk for ministeriers topledelser, og i Det Strategiske Samarbejdsforum om Cybersikkerhed, hvis medlemmer omfatter en række samfundsvigtige virksomheder fra den private sektor samt brancheorganisationer.

CFCS har desuden i 2016 gennemført en fælles konference for medlemmerne af de to interessentfora med henblik på at styrke det offentlige-private samarbejde.

I 2016 har CFCS yderligere gennemført en række møder i to tekniske samarbejdsfora, som henholdsvis adresserer cybersikkerhed på et teknisk niveau og cybersikkerhed i mainframe-installationer. Sidstnævnte forum, som var en udløber af sikkerhedshændelsen hos it-leverandøren CSC i 2012, blev nedlagt ultimo 2016 efter fælles aftale mellem deltagerne.

NIS-direktivet

Den nationale implementering af NIS-direktivet berører mange ministerområder, idet der stilles krav til operatører inden for en række forskellige sektorer, herunder finans-, energi-, transport-, sundheds- og vandforsyningssektorerne samt udbydere af digitale tjenester.

Ud over at bidrage til den tværministerielle koordination vil CFCS varetage rollen som nationalt kontaktpunkt samt rollen som national CSIRT (Computer Security Incident Response Team).

NIS-direktivet

Net- og informationssikkerhedsdirektivet (Direktiv (EU) 2016 /1148 – NIS-direktivet) trådte i kraft i august 2016 og skal være implementeret i dansk lovgivning senest medio maj 2018. Direktivet har til formål at sikre et højt, fælles sikkerhedsniveau for net- og informationssystemer i EU.

National strategi

I 2016 har CFCS konsolideret centerets Trusselsvurderingsenhed og Undersøgelsesenhed i henhold til initiativerne i den nationale strategi for cyber- og informationssikkerhed. Den faste stab i Trusselsvurderingsenheden er fuldt bemandet og har udarbejdet 14 trusselsvurderinger i 2016, men indstationeringer af medarbejdere fra relevante myndigheder er ikke fuldt implementeret. Undersøgelsesenheden er operativ og fuldt bemandet og har udarbejdet fem undersøgelsesrapporter og deltaget i 19 incident response-udrykninger i 2016.

SCADA-kompetenceenheden i CFCS er endnu ikke fuldt opbygget, idet udbuddet af tekniske specialister på SCADA-området (indlejrede industrielle kontrolsystemer) er langt mindre end efterspørgslen. Dette har medført, at det er gået langsommere end planlagt med opbygningen på SCADA-området.

National strategi

Den nationale strategi for cyber- og informationssikkerhed blev lanceret i slutningen af 2014. Strategien indeholder 27 konkrete initiativer på tværs af seks indsatsområder med henblik på at øge informationssikkerheden og styrke beskyttelsen mod cyberangreb.

Om FE's Center for Cybersikkerhed

Center for Cybersikkerhed blev oprettet i december 2012 som en del af Forsvarets Efterretningstjeneste. Placeringen ved 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.

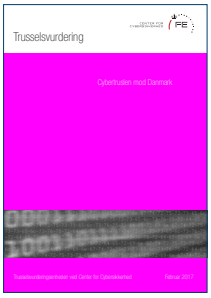
CFCS er en dynamisk arbejdsplads med mange forskellige typer af højtspecialiserede medarbejdere, herunder netværksanalytikere, malwareanalytikere, pen-testere, informationssikkerhedsrådgivere og teleingeniører. Størstedelen af centerets medarbejdere har en it-uddannelse eller anden teknisk baggrund. 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 2016 var der i alt 81 medarbejdere i centeret.

Center for Cybersikkerhed

CFCS er Danmarks nationale it-sikkerhedsmyndighed og nationalt kompetencecenter på cybersikkerhedsområdet. Vores mission er at styrke beskyttelsen af Danmarks digitale infrastruktur, samt styrke Danmarks evne til at imødegå cyberangreb.

Publikationer i 2016

CFCS udarbejder løbende trusselsvurderinger, undersøgelsesrapporter og vejledninger med henblik på at varsle om cybertruslen samt understøtte en forebyggende indsats. I 2016 har CFCS udarbejdet 14 trusselsvurderinger, fem undersøgelsesrapporter og syv vejledninger på cyberområdet. De uklassificerede publikationer fremgår nedenfor og er offentligt tilgængelige på CFCS' hjemmeside www.cfcs.dk.



Cybertruslen mod Danmark

CFCS redegør i denne trusselsvurdering for den samlede cybertrussel, der møder danske myndigheder og virksomheder. CFCS vurderer, at spionage mod offentlige myndigheder og private virksomheder udgør den alvorligste cybertrussel mod Danmark og danske interesser. Spionagen udføres primært af statslige og statsstøttede aktører.

Truslen fra "Stagefright"-sårbarheden i Android-styresystemet

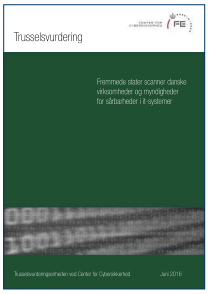
CFCS varsler i denne trusselsvurdering om en sårbarhed i Android-styresystemet. CFCS har observeret scanninger efter sårbare styresystemer, efter at sårbarheden er blevet offentliggjort.

Truslen fra sårbarhed i Cisco firewalls og routere som VPN-løsning

CFCS varsler i denne trusselsvurdering om en alvorlig sårbarhed i Cisco's Adaptive Security Appliance (ASA) software. Sårbarheden er relevant i de tilfælde, hvor Cisco firewalls og routere benyttes som VPN-løsning.

Cybertruslen mod forsvars- og aerospaceindustrien i Danmark

CFCS redegør i denne trusselsvurdering for cybertruslen mod forsvars- og aerospaceindustrien i Danmark, hvor der er en vedholdende cyberspionagetrussel. CFCS vurderer, at trusselsaktørerne har tilknytning til fremmede stater.



Fremmede stater scanner danske virksomheder og myndigheder for sårbarheder i it-systemer

CFCS redegør i denne trusselsvurdering for cybertruslen fra fremmede stater mod danske myndigheders og virksomheders it-systemer. CFCS vurderer, at fremmede stater scanner it-systemer i Danmark for at søge efter sårbarheder og installere bagdøre i systemerne.

Hjemmesider, som benytter CGI-scripts, kan være sårbare over for kompromittering af kommunikationen til eksterne servere

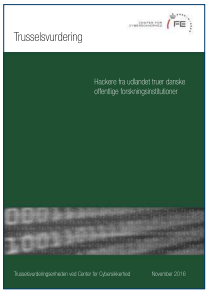
CFSC varsler i denne trusselsvurdering om en sårbarhed, der gør det muligt for en ondsindet aktør at kompromittere hjemmesider, som benytter CGI-scripts. CFCS har observeret scanninger efter sårbare hjemmesider, efter at sårbarheden er blevet offentliggjort.

”QuadRooter” sårbarhed i Android-enheder med Qualcomm processorchips

CFCS varsler i denne trusselsvurdering om en sårbarhed i Android-enheder, som benytter processorchips fra Qualcomm. CFCS vurderer, at hovedparten af producenterne til de berørte enheder endnu ikke har udsendt sikkerhedsopdateringer, som fjerner sårbarhederne.

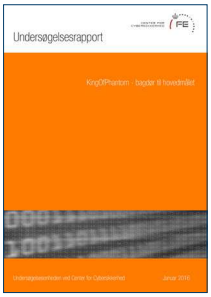
Nye sårbarheder i Cisco firewalls er blevet offentliggjort

CFCS varsler i denne trusselsvurdering om en ny sårbarhed i Cisco firewalls. CFCS vurderer, at det er meget sandsynligt, at der er ondsindede aktører, som på kort sigt vil forsøge at udnytte sårbarhederne.



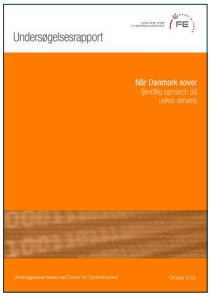
Hackere fra udlandet truer danske offentlige forskningsinstitutioner

CFCS redegør i denne trusselsvurdering for cybertruslen mod danske offentlige forskningsinstitutioner. CFCS vurderer, at fremmede stater udfører cyberspionage mod danske offentlige forskningsinstitutioner, som tilmed er lette mål på grund af forskningstraditioner for stor åbenhed.

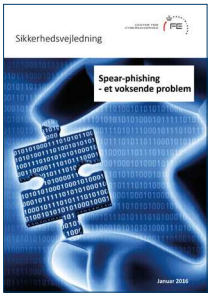


KingOfPhantom – bagdør til hovedmålet
CFCS redegør i denne undersøgelsesrapport for et konkret målrettet og vedholdende cyberangreb mod to anonymiserede danske virksomheder. Med udgangspunkt i de konkrete angreb beskriver CFCS, hvordan andre virksomheder og myndigheder kan sikre sig bedre mod tilsvarende angreb.

Phishing uden fangst – Udenrigsministeriet under angreb
CFCS redegør i denne undersøgelsesrapport for en konkret angrebskampagne mod Udenrigsministeriet, der stod på i mere end et halvt år. Med udgangspunkt i erfaringerne fra angrebet udleder CFCS en række konkrete anbefalinger henvendt til danske myndigheder og virksomheder.



Når Danmark sover – fjendtlig opmarch på usikre servere
CFCS redegør i denne undersøgelsesrapport for et vedholdende og bredspektret cyberangreb mod en række danske myndigheder og virksomheder. En ondsindet aktør bag angrebet har udnyttet svagheder i et open source it-system. Rapporten indeholder forslag til en række tiltag, der fremadrettet kan hjælpe myndigheder og virksomheder mod sådanne cyberangreb.



Spear phishing – et voksende problem
CFCS redegør i denne vejledning om spear-phishing, hvor ondsindede aktører målrettet indhenter bruger-id og adgangskoder mv. Disse oplysninger vil så kunne anvendes i forbindelse med et decideret cyberangreb. CFCS beskriver, hvordan man bedst muligt beskytter sin organisation mod spear phishing-angreb.

Logning – en del af et godt cyberforsvar
CFCS redegør i denne vejledning for logning, som ofte er afgørende for en organisations evne til hurtigt at opdage et cyberangreb og efterfølgende effektivt afdække konsekvenserne heraf. Vejledningen indeholder en række konkrete anbefalinger i relation til at inddrage logning i et godt cyberforsvar.

Reducér risikoen for ransomware
CFCS redegør i denne vejledning for ransomware, der er en særlig type malware, som via kryptering gør data utilgængelige. Ofte vil ondsindede aktører bag disse cyberangreb tilbyde at dekryptere data mod en løsesum – deraf navnet ransomware. Vejledningen indeholder en række anbefalinger i forhold til forebyggende tiltag samt anbefalinger til konkrete tiltag, hvis skaden er sket.

Passwordvejledning
CFCS redegør i denne vejledning for passwordsikkerhed. I vejledningen beskriver CFCS nogle af de mest anvendte angrebsmetoder, som hackere benytter sig af, samt nogle af de eksisterende udfordringer ved passwords. Vejledningen indeholder en lang række konkrete anbefalinger i forhold til at styrke passwordsikkerheden.

Kontakt til FE's Center for Cybersikkerhed

CFCS kan inden for daglig kontortid 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 contact@govcert.dk.

Følg Center for Cybersikkerhed

CFCS er aktiv på de sociale medier Twitter og LinkedIn, hvor centeret løbende deler bl.a. nyheder, publikationer og jobopslag. CFCS har i 2016 bl.a. udsendt 343 tweets på Twitter, som samlet har genereret 507 retweets og mere end 550.000 potentielle visninger.

Twitter (@cybersikkerhed): https://twitter.com/cybersikkerhed

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

Center for Cybersikkerhed
Kastellet 30
2100 København Ø

Telefon: 3332 5580
www.cfcs.dk