CENTER FOR
CYBERSIKKERHED

FE

Center for Cybersikkerheds beretning 2015

Center for Cybersikkerhed
Kastellet 30
2100 København Ø
Tlf.: 3332 5580
www.cfcs.dk

Om Center for Cybersikkerhed
Forsvarets Efterretningstjenestes Center for Cybersikkerhed 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.

Center for Cybersikkerhed 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- eller anden teknisk uddannelse. Dertil kommer en større gruppe af akademikere med en samfundsvidenskabelig baggrund. Ved udgangen af 2015 var der i alt 69 medarbejdere i centeret.

Center for Cybersikkerhed og FE
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 centeret i indsatsen for at styrke Danmarks robusthed mod cyberangreb har adgang til den særlige efterretningsbaserede viden, som FE råder over på cyberområdet.

Begivenheder i året
Center for Cybersikkerhed har etableret tre nye enheder i 2015, henholdsvis Trusselsvurderingsenheden, Undersøgelsesenheden og SCADA-kompetenceenheden. De nye enheder styrker og udvider centerets kernekompetencer inden for cybersikkerhed og udspringer af den nationale strategi for cyber- og informationssikkerhed.

Trusselsvurderingsenheden har til opgave at udarbejde generelle og sektorspecifikke trusselsvurderinger på cybersikkerhedsområdet. Trusselsvurderingsenheden har i 2015 udarbejdet trusselsvurderingen: *Cybertruslen mod Danmark.* Trusselsvurderingsenheden vil, ud over medarbejdere fra Center for Cybersikkerhed, bestå af repræsentanter fra de sektoransvarlige myndigheder fra samfundsvigtige sektorer. Indstationeringerne er med til at sikre, at den fornødne sektorspecifikke ekspertise er forankret i enheden. Den faste stab i Trusselsvurderingsenheden er bemandet. Der udestår dog endnu endelige tilbagemeldinger fra de relevante myndigheder og sektorer med hensyn til indstationeringerne i enheden.

National strategi
Den nationale strategi for cyber- og informationssikkerhed blev lanceret ultimo 2014. Strategien indeholder 27 konkrete initiativer på tværs af seks indsatsområder med henblik på at øge informationssikkerheden og styrke beskyttelsen mod cyberangreb. Center for Cybersikkerhed varetog sammen med Digitaliseringsstyrelsen sekretariatsfunktionen i forbindelse med udarbejdelsen af strategien og har i 2015 implementeret centerets konkrete initiativer fra strategien. Strategien skal revideres i 2016.

Undersøgelsesenheden er operativ og fuldt bemandet og har til opgave at undersøge større sikkerhedshændelser på cyberområdet med henblik på at indsamle og omsætte erfaringerne til konkrete sikkerhedsanbefalinger. Undersøgelsesenheden har i 2015 udarbejdet undersøgelsesrapporterne: *KingOfPhantom – bagdør til hovedmålet* og *Phishing uden fangst – Udenrigsministeriet under angreb.*

SCADA-kompetenceenheden er fortsat under opbygning. Den nye SCADA-kompetenceenhed skal bl.a. bistå og rådgive private virksomheder og offentlige organisationer med henblik på at imødegå sårbarheder i SCADA-systemer (indlejrede industrielle styringssystemer), som er en central del af den samfundsvigtige infrastruktur.

Som led i implementeringen af den nationale strategi for cyber- og informationssikkerhed har Center for Cybersikkerhed i samarbejde med Statens It udarbejdet en analyse af, hvordan statens internetforbindelser kan samles og sikres. På baggrund af analysen er der fremsat anbefaling om, at forbindelserne omlægges til Statens It. Center for Cybersikkerhed har desuden stået i spidsen for en arbejdsgruppe, som har udarbejdet en rapport med anbefalinger til en styrkelse af sikker kommunikation i staten. I rapporten gives anbefalinger om udbredelse af REGNEM (klassificeret netværk) og krypteret mobiltelefoni til ministerområderne.

Center for Cybersikkerhed har endvidere i 2015 udarbejdet og implementeret en kundestrategi med prioriteringer og proces for centerets kunderettede virksomhed. Kundestrategien vil bl.a. styrke dialogen med virksomheder og organisationer, som understøtter samfundsvigtige funktioner i Danmark, og som efter en konkret vurdering af modenhedsniveauet vil kunne tilslutte sig netsikkerhedstjenesten.

Den reaktive indsats i 2015

Center for Cybersikkerhed har i 2015 gennemført en organisatorisk sammenlægning af de to CERT-enheder (GovCERT og MILCERT) til en samlet netsikkerhedstjeneste. Gevinsterne består bl.a. i øget synergi i forbindelse med vagtberedskab og videndeling vedrørende sikkerhedshændelser på tværs af civile og militære netværk samt udnyttelse af fælles sensornetværk.

Center for Cybersikkerhed har til opgave at opdage, analysere og bidrage til at imødegå cyberangreb på civile og militære myndigheder og de virksomheder, der er tilsluttet netsikkerhedstjenestens sensornetværk. Netsikkerhedstjenesten analyserer løbende de værktøjer og metoder, som primært statssponsorerede aktører gør brug af, med henblik på at være på forkant med udviklingen. På baggrund heraf opdaterer centeret løbende dets netværk af sensorer (alarmenheder) med henblik på at levere den bedst mulige beskyttelse mod cyberangreb til de tilsluttede kunder ved netsikkerhedstjenesten. Center for Cybersikkerhed har i 2015 fortsat udskiftningen af sensorer ved tilsluttede kunder med en helt ny generation af egenudviklede alarmenheder. Udskiftningen af sensorer forventes afsluttet i 2016.

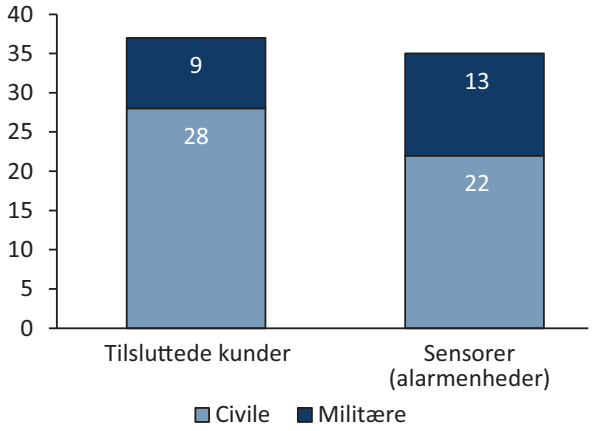
Netværk af alarmenheder

Centerets 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 de tilsluttede kunders internetforbindelser. Tilsammen danner alarmenhederne et såkaldt sensornetværk, som alarmerer Center for Cybersikkerhed ved tegn på cyberangreb hos de tilsluttede kunder ved netsikkerhedstjenesten.

I 2015 har der været en samlet tilgang af seks nye militære og civile kunder ved netsikkerhedstjenesten. Der har ikke været nogen kundeafgang eller midlertidige tilslutninger ved netsikkerhedstjenesten i 2015. Ressortomlægningen i forbindelse med regeringsskiftet har dog afstedkommet nogle ændringer i kundeporteføljen. Center for Cybersikkerhed har ved udgangen af 2015 i alt 37 tilsluttede kunder ved netsikkerhedstjenesten og 35 sensorer.

Det bemærkes, at antallet af tilsluttede kunder ved netsikkerhedstjenesten ikke er lig med antallet af sensorer. Dette skyldes, at der kan være anvendt flere sensorer pr. kunde, ligesom en enkelt sensor placeret hos en central it-leverandør kan dække flere kunder.

Oversigt over netsikkerhedstjenestens kunder og sensorer pr. 31. december 2015



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. 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.

Tilsyn med Center for Cybersikkerhed

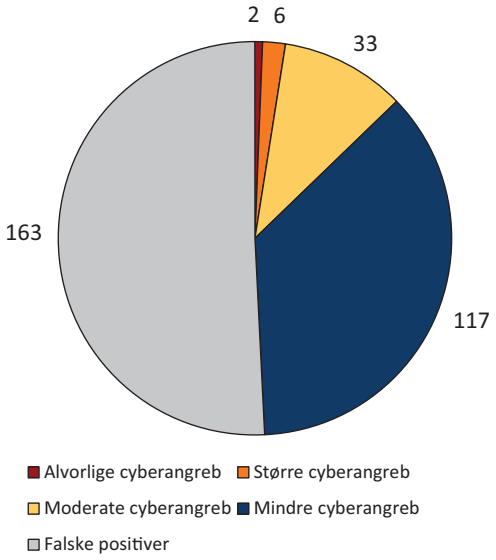
Tilsynet med Efterretningstjenesterne er et særligt uafhængigt kontrolorgan, der har ført tilsyn med Center for Cybersikkerheds behandling af personoplysninger siden 1. juli 2014, hvor lov om Center for Cybersikkerhed trådte i kraft. Tilsynet har i henhold til lov om Center for Cybersikkerhed tilsvarende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

Tilsynet med Efterretningstjenesterne har ultimo maj 2016 for første gang offentliggjort den årlige redegørelse om tilsynet med Center for Cybersikkerhed. Den årlige redegørelse er tilgængelig på Center for Cybersikkerheds hjemmeside www.cfcs.dk

Netsikkerhedstjenesten har i 2015 behandlet i alt 321 sikkerhedshændelser, som er inddelt efter alvorlighedsgrad ud fra, i hvilket omfang kunden er berørt. Centerets strategiske fokus på avanceret cyberangreb samt nye sensortyper og alarmindstillinger har, som forudset, ført til et samlet fald i antallet af registrerede sikkerhedshændelser i forhold til 2014.

Størstedelen af netsikkerhedstjenestens ressourcer allokeres til hændelseshåndteringen af de mest avancerede cyberangreb. Netsikkerhedstjenesten gennemfører løbende netværks- og malwareanalyser i forbindelse med sikkerhedshændelser, hvor der er grundlag for at foretage en nærmere sikkerhedsteknisk analyse. Netsikkerhedstjenesten har gennemført 123 sikkerhedstekniske analyser i 2015.

Oversigt over sikkerhedshændelser i 2015



Sikkerhedshændelser
En sikkerhedshændelse er en hændelse, der negativt påvirker eller vurderes at ville kunne påvirke tilgængelighed, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale tjenester. De alvorligste sikkerhedshændelser omfatter eksempelvis en særlig avanceret, målrettet og vedholdende cyberangrebstype, der kaldes APT-angreb (Advanced Persistent Threat).

En falsk positiv er en hændelse oprettet på en alarm, der giver positivt resultat, men hvor efterfølgende undersøgelse viser, at der ikke er grundlag for en videre behandling som sikkerhedshændelse.

Netsikkerhedstjenesten er løbende i dialog med Center for Cybersikkerheds complianceenhed, således at der i det daglige arbejde er fokus på overholdelse af lovgivningens detaljerede krav til bl.a. opbevaring, videregivelse og sletning af data.

Den proaktive indsats i 2015
Center for Cybersikkerhed varetager, som national it-sikkerhedsmyndighed og myndighed for informationssikkerhed og beredskab på teleområdet, en række opgaver af primært forebyggende karakter. Centerets proaktive arbejde omfatter blandt andet en indsats i forbindelse med oplysning, vejledning og rådgivning af danske myndigheder og virksomheder på cybersikkerhedsområdet.

En oversigt over udvalgte proaktive indsatser i 2015 fremgår af tabellen. Formålet med denne indsats er at mindske risikoen for cyberangreb og at sikre, at den enkelte organisation i størst muligt omfang er forberedt på at kunne imødegå cyberangreb.

Tabel over udvalgte proaktive indsatser i 2015

Kategorier	Antal
Afsluttede rådgivningssager	102
Awareness-briefinger	80
Sikkerhedsgodkendelser	78
Godkendelse af kryptoplaner	61
Tekniske sikkerhedseftersyn	57
Tempest zoning (udstrålingskontrol)	6
Tilsyn	24

Udgangspunktet for centerets rådgivningsmæssige opgaver er altid et samfundsmæssigt perspektiv. I 2015 har Center for Cybersikkerhed eksempelvis gennemført en større rådgivningsindsats med henblik på at styrke informationssikkerheden i telenettene. Centeret har i den forbindelse indgået i et konstruktivt samarbejde med teleudbyderne og telemyndighederne i nordisk regi om sårbarheder og risikoreducerende tiltag i signaleringssystem 7 (SS7), der anvendes internt mellem teleoperatørerne til opsætning og styring af brugernes taleopkald og dataforbindelser. Et konkret resultat af dette samarbejde er udgivelsen af fælles nordiske anbefalinger for at imødegå SS7-trusler stilet til de centrale teleudbydere.

Som national it-sikkerhedsmyndighed godkender centeret systemer og installationer til behandling af klassificerede informationer i overensstemmelse med Justitsministeriets sikkerhedscirkulære på både det civile og militære område. Forsvaret er derfor også en vigtig målgruppe for centerets rådgivning inden for cyber- og informationssikkerhed. Som grundlag for at styrke informationssikkerheden i Forsvaret på linje med øvrige statslige myndigheder har centeret udarbejdet et nyt sæt bestemmelser for informationssikkerhed som en del af den samlede militære sikkerhedstjeneste. Disse bestemmelser indgår i de militære sikkerhedsbestemmelser (FKOBST 358-1, kap. 6).

Proaktive teknologiske discipliner
Center for Cybersikkerhed har i 2015 samlet de proaktive teknologiske discipliner i centeret med henblik på at styrke det faglige miljø, som omfatter bl.a. de eksisterende discipliner inden for tekniske sikkerhedseftersyn og tempest zoning samt opbygningen af SCADA-kompetenceenheden og en proaktiv sikkerhedsteknologisk kapacitet.

I 2015 har Center for Cybersikkerhed udarbejdet en struktureret proces for akkreditering af it-systemer, installationer og tilkoblinger mellem eksterne og interne systemer. Processen har til formål at sikre, at it- og informationssikkerhedsmæssige krav, baseret på nationale, NATO- og EU-krav samt vurdering af informationssikkerhedsrisici, inddrages så tidligt som muligt i it-projekter. Processen er også med til at sikre, at akkrediteringer gennemføres på en grundig og ensartet måde gennem hele projektforløbet. Som led i dette arbejde har centeret udgivet vejledninger om akkrediteringsprocessen og it-risikovurdering.

Center for Cybersikkerhed lægger vægt på at have en åben, tillidsfuld og løbende dialog med bl.a. statslige myndigheder, brancheorganisationer og større virksomheder inden for de sektorer, der beskæftiger sig med samfundsvigtige funktioner. For at skabe øget awareness om cybertruslen og styrke den proaktive dialog har Center for Cybersikkerhed i 2015 udbygget centerets relationer med interessenter og samarbejdspartnere i Danmark.

Center for Cybersikkerhed har gennemført flere møder i Den Tværministerielle Kontaktgruppe vedrørende Cybersikkerhed, som er et netværk for ministeriers topledelser, og i Det Strategiske Samarbejdsforum om Cybersikkerhed, der har en lang række samfundsvigtige virksomheder fra den private sektor samt brancheorganisationer som medlemmer. Centeret har yderligere gennemført en fælles konference for medlemmerne af de to interessentfora med henblik på at styrke det offentlige-private samarbejde. I 2015 har Center for Cybersikkerhed yderligere etableret to nye tekniske fora, som adresserer cybersikkerhed på et teknisk niveau og cybersikkerhed i mainframeinstallationer.

Lovgivning
I december 2015 vedtog Folketinget en ny lov om net- og informationssikkerhed, som bl.a. skal medvirke til at fremme en mere robust teleinfrastruktur. Informationssikkerhed på teleområdet omfatter myndighedernes og virksomhedernes samlede indsats med henblik på at forebygge nedbrud i informationssystemer samt beskytte data, som behandles i systemerne, mod manipulation, tab eller tyveri.

Center for Cybersikkerhed har efter vedtagelsen af lov om net- og informationssikkerhed arbejdet på en række bekendtgørelser på området, som forventes at blive udstedt medio 2016.

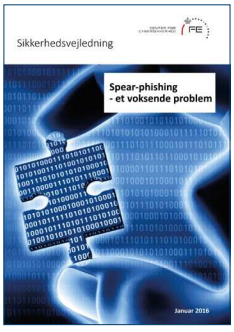
På europæisk plan forventes et direktiv om net- og informationssikkerhed vedtaget medio 2016, som efterfølgende skal implementeres i medlemsstaternes nationale lovgivning. Direktivet har til formål at fremme informationssikkerheden i en række sektorer, der leverer samfundsvigtig infrastruktur og løser opgaver af lignende karakter.

Net- og informationssikkerhedsdirektivet
I forlængelse af den politiske enighed i EU om net- og informationssikkerhedsdirektivet (NIS-direktivet) ultimo 2015 har Center for Cybersikkerhed iværksat forskellige forberedende tiltag i forbindelse med den nationale implementering af NIS-direktivet.

Center for Cybersikkerhed vil i kraft af sin rolle som national it-sikkerhedsmyndighed forestå den overordnede nationale implementering af NIS-direktivet. Center for Cybersikkerhed vil påtage sig funktionen som nationalt SPoC (Single Point of Contact) og CSIRT (Computer Security Incident Response Team), mens opgaven som tilsynsmyndighed (competent authority) lægges ud til de enkelte sektorer jf. sektoransvarsprincippet.

Publikationer i 2015

Center for Cybersikkerhed har i 2015 udsendt følgende trusselsvurderinger, undersøgelsesrapporter, sikkerhedsanbefalinger og vejledninger om specifikke emner inden for cybersikkerhed:



Spear-phishing – et voksende problem

Center for Cybersikkerhed har udgivet en sikkerhedsvejledning om spear-phishing, der vejleder om, hvordan man bedst muligt beskytter sin organisation mod spear-phishing-angreb, som er målrettet enkeltpersoner i organisationen.

Begræns risikoen fra ransomware

Center for Cybersikkerhed har udgivet en sikkerhedsbulletin, der indeholder en række forebyggende råd, som mindsker risikoen for at blive ramt af ransomware-angreb. Anbefalingerne indeholder også en række retningslinjer for, hvad myndigheder og virksomheder kan og bør gøre, hvis de først er blevet ramt af et vellykket ransomware-angreb (Center for Cybersikkerhed har udgivet en opdateret ransomwarevejledning i 2016).

It-sikkerhed på rejsen

Center for Cybersikkerhed har udgivet en sikkerhedsanbefaling om it-sikkerhed på rejsen, der indeholder råd og vejledning til sikker brug af it-udstyr under rejser i udlandet. Anbefalingerne er både rettet mod ledelsen, it-afdelingen og den enkelte medarbejder i offentlige myndigheder og private virksomheder.

Styrkelse af informationssikkerheden i mainframeinstallationer

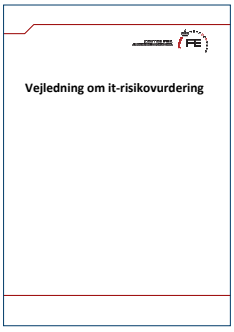
Center for Cybersikkerhed har udgivet en sikkerhedsanbefaling, som beskriver en række væsentlige sikkerhedstiltag, der bør overvejes af såvel mainframeejere og administratorer som kunder til mainframetjenester.

Fællesnordiske anbefalinger for at imødegå SS7-trusler

Center for Cybersikkerhed har sammen med de nordiske telemyndigheder udarbejdet en række anbefalinger til styrkelse af informationssikkerheden i telenettene. Anbefalingerne vedrører signaleringssystem 7 (SS7), der anvendes internt mellem teleoperatørerne til opsætning og styring af brugernes taleopkald og dataforbindelser (Offentliggøres ikke).

Akkrediteringsprocessen

Center for Cybersikkerhed har udarbejdet en vejledning om akkreditering af it-systemer, installationer og tilkoblinger mellem eksterne og interne systemer. Vejledningen er primært rettet mod Forsvaret og andre myndigheder, der anskaffer eller installerer it-systemer til behandling af klassificerede informationer efter Justitsministeriets sikkerhedscirkulære.

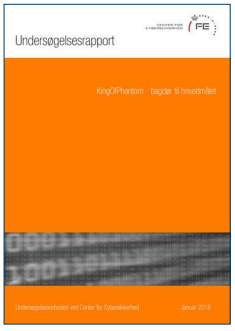


Vejledning om it-risikovurdering

Center for Cybersikkerhed har som supplement til akkrediteringsprocessen udarbejdet en vejledning om vurdering af it-risici. Vejledningen er rettet mod myndigheder, som ikke selv har defineret en proces herfor.

Cybertruslen mod Danmark*

Center for Cybersikkerhed har udgivet en trusselsvurdering, hvor centeret 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 grupper.



KingOfPhantom – bagdør til hovedmålet*
Center for Cybersikkerhed har udgivet en undersøgelsesrapport om et konkret målrettet og vedholdende cyberangreb mod to anonymiserede danske virksomheder. Med udgangspunkt i de konkrete angreb viser rapporten, hvordan andre virksomheder og myndigheder kan sikre sig bedre mod tilsvarende angreb.

Phishing uden fangst – Udenrigsministeriet under angreb*
Center for Cybersikkerhed har udgivet en undersøgelsesrapport om en konkret angrebskampagne mod Udenrigsministeriet, der stod på i mere end et halvt år. Med udgangspunkt i erfaringerne fra angrebet udledes en række konkrete anbefalinger henvendt til myndigheder og virksomheder.

De uklassificerede publikationer er tilgængelige på Center for Cybersikkerheds hjemmeside www.cfcs.dk. Endvidere udsender Center for Cybersikkerhed løbende situationsrapporter og varslinger til de it-sikkerhedsansvarlige hos myndigheder og virksomheder, der er tilsluttet netsikkerhedstjenesten. I 2015 har Center for Cybersikkerhed udsendt otte situationsrapporter og 99 varslinger.

Kontakt til Center for Cybersikkerhed
Center for Cybersikkerhed kan inden for almindelig kontortid kontaktes på telefon 3332 5580 eller på e-mail cfcs@cfcs.dk.

Myndigheder og virksomheder, der beskæftiger sig med samfundsvigtige funktioner, kan i forbindelse med større sikkerhedshændelser kontakte vagthavende hos netsikkerhedstjenesten døgnet rundt på vagttelefon 6093 4827 eller på e-mail contact@govcert.dk.

Alternativt kan Forsvarets Efterretningstjenestes vagthavende kontaktes på telefon 3332 5566.

Følg Center for Cybersikkerhed
Center for Cybersikkerhed er i 2015 kommet på de sociale medier LinkedIn og Twitter, hvor centeret løbende deler nyheder, publikationer, events og jobopslag etc.

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

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

**Det bemærkes, at trusselsvurderingen og undersøgelsesrapporterne er udarbejdet i 2015, men at de først blev offentliggjort primo januar 2016.*

Center for Cybersikkerhed
Kastellet 30
2100 København Ø

Telefon: 3332 5580
www.cfcs.dk