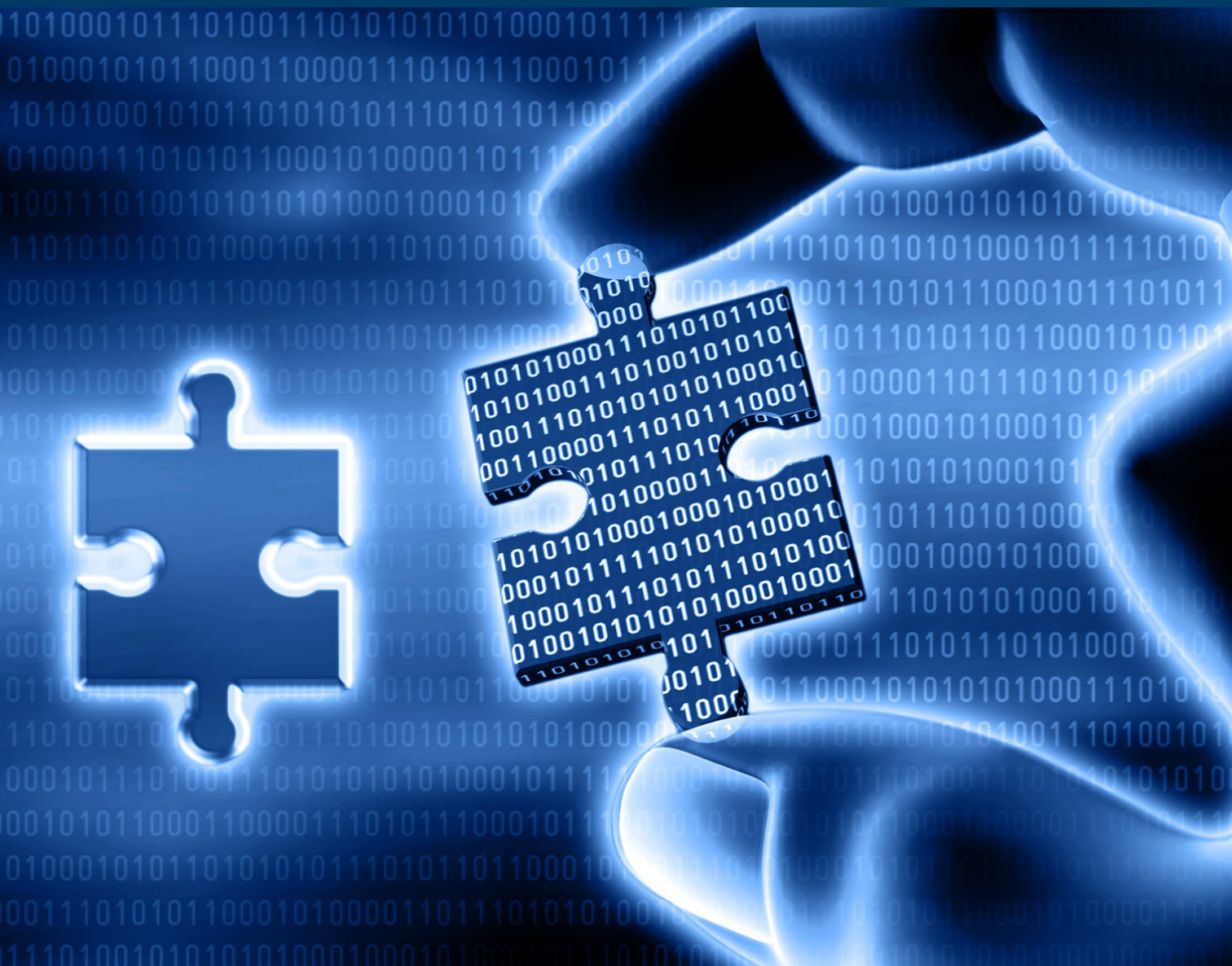
CENTER FOR
CYBERSIKKERHED

FE

Center for Cybersikkerheds beretning 2014



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

Om Center for Cybersikkerhed
Center for Cybersikkerhed blevet oprettet i 2012 som en del af FE. Centerets hovedformål er at styrke beskyttelsen af Danmarks kritiske informations- og kommunikationsteknologiske infrastruktur, samt at styrke Danmarks evne til at imødegå cyberangreb.

Center for Cybersikkerhed er nationalt kompetencecenter på cybersikkerhedsområdet og fokuserer på beskyttelse af samfundsvigtige funktioner mod avancerede cyberangreb. Centeret havde ved udgangen af 2014 i alt 72 medarbejdere.

Begivenheder i året
I 2014 har Center for Cybersikkerhed med den nye lov om Center for Cybersikkerhed fået et nyt samlet lovgrundlag. Baggrunden for loven er, at danske myndigheder og virksomheder i stigende grad udsættes for cyberangreb. Med loven er centerets muligheder for at undersøge og forebygge cyberangreb blevet styrket.

Center for Cybersikkerhed og FE
Center for Cybersikkerhed har siden oprettelsen været en del af FE, hvorved en række eksisterende men spredte it-kompetencer og specialiserede kundskaber er blevet samlet ét sted. Placeringen ved FE skaber dermed en række synergieffekter og sikrer samtidig, at centeret har adgang til den særlige efterretningsbaserede viden, som FE råder over på cyberområdet, til at styrke imødegåelsen af cyberangreb mod Danmark.

FE har i mange år haft til opgave at beskytte Forsvarets kritiske infrastruktur mod cyberangreb, og dermed har FE fået opbygget stærke kompetencer på netop cyberområdet. Som udenrigsefterretningstjeneste har FE endvidere stor viden om de udenlandske aktører på cyberområdet samt et veletableret samarbejde med udenlandske efterretningstjenester.

Med den nye lov om Center for Cybersikkerhed er der fastsat entydige og restriktive regler for behandling af data i centeret. I forbindelse med lovens ikrafttræden har centeret etableret en intern compliance-funktion, der medvirker til at sikre, at centeret til enhver tid efterlever gældende love og regler såvel som interne procedurer og relevante standarder. Der er endvidere betydelig ledelsesmæssig fokus på at sikre, at behandlingen af de ofte personfølsomme data, som løbende behandles i Center for Cybersikkerhed, til enhver tid sker med respekt for retssikkerheden og den personlige frihed. Også dette understøttes af den nye compliance-funktion.

Netværk af alarmenheder
For at bidrage til at forhindre hackerangreb, analyserer Center for Cybersikkerhed de værktøjer og metoder, som hackerne gør brug af. 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 netsikkerhedstjenestens kunders internetforbindelser. Her sammenholder alarmenheden hele tiden kundens datatrafik, der løber gennem forbindelserne, med de digitale fingeraftryk. Tilsammen danner alarmenhederne et såkaldt sensornetværk, som alarmerer Center for Cybersikkerhed ved tegn på cyberangreb hos de tilsluttede kunder.

For at levere den bedst mulige beskyttelse til centerets kunder, opdaterer centeret løbende dets netværk af alarmenheder. Ultimo 2014 påbegyndte centeret implementeringen af en helt ny generation af egenudviklede alarmenheder, der skal installeres hos centerets kunder. Det understøtter, at centeret er på forkant med udviklingen, hvor mængden af internettrafik stiger hele tiden, og hvor hackerne konstant udvikler nye og avancerede angrebsmetoder.

Som national it-sikkerhedsmyndighed varetog Center for Cybersikkerhed den it-sikkerhedsmæssige undersøgelse af den meget omtalte CSC-hackersag med henblik på at klarlægge konsekvenserne af kompromitteringen af it-systemer, som CSC varetager driften af for en række offentlige myndigheder. I 2014 færdiggjorde Center for Cybersikkerhed dette arbejde, hvilket blev fulgt op med udgivelsen af to afsluttende rapporter om hackerangrebet mod CSC. I en klassificeret rapport giver centeret en detaljeret beskrivelse af selve sikkerhedsbruddet hos CSC og dets konsekvenser. Denne rapport er udarbejdet af Center for Cybersikkerhed og PET i fællesskab. I en anden og offentligt tilgængelig rapport, som Center for Cybersikkerhed og Digitaliseringsstyrelsen har udarbejdet, tages der udgangspunkt i de indhøstede erfaringer og gives en række anbefalinger til styrkelse af sikkerheden i statens outsourcede it-drift.

Center for Cybersikkerhed har i 2014 sammen med Digi-

taliseringsstyrelsen varetaget sekretariatsfunktionen i forbindelse med udarbejdelsen af den nationale strategi for cyber- og informationssikkerhed. Strategien fokuserer på cyber- og informationssikkerhed i staten og i særlig grad på energi- og teleområdet. Flere initiativer i strategien vil direkte berøre centerets arbejde de kommende år, således at særligt centerets muligheder for at rådgive om cybersikkerhed i forhold til industrielle kontrolsystemer, for at udrede og analysere større cyberhændelser og endelig for at udarbejde sektorspecifikke trusselvurderinger på cyberområdet styrkes.

Den reaktive indsats i 2014

Center for Cybersikkerheds reaktive indsats er bygget op om arbejdet i centerets Netsikkerhedstjeneste. Netsikkerhedstjenesten i Center for Cybersikkerhed blev etableret i 2014 som en sammenlægning af varslingstjenesterne GovCERT og MILCERT.

Netsikkerhedstjenesten har til opgave at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos Forsvaret og de virksomheder og statslige myndigheder, der er tilsluttet netsikkerhedstjenesten. Netsikkerhedstjenestens indsats fokuserer på de mest avancerede angreb, der oftest udføres af statsstøttede aktører, og cyberangreb, der i øvrigt kan påvirke det danske samfund i væsentlig grad. Netsikkerhedstjenesten er løbende i dialog med centerets compliance-funktion, således at der i det daglige arbejde er fokus på overholdelse af lovgivningens detaljerede krav til bl.a. opbevaring, videregivelse og sletning af data.

Som det fremgår af tabellen herunder, registrerede Center for Cybersikkerhed i 2014 i alt 585 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). APT-angreb sker oftest med den hensigt at udøve spionage – og særligt industrispionage. Det er centerets vurdering, at det ofte er statssponsorerede aktører, der står bag APT-angreb.

Statistik over udvalgte dele af centerets reaktive indsats samt tilsluttede kunder i 2014.

Kategorier	Det civile område	Det militære område	I alt
Tilsluttede kunder*	25	6	31
Alarmenheder*	18	11	29
Midlertidige tilslutninger	0	0	0
Sikkerhedshændelser	453	132	585
Sikkerhedstekniske analyser	61	7	68

**) Pr. 31. december 2014*

Tilsyn med Center for Cybersikkerhed

Tilsynet med Efterretningstjenesterne har siden 1. juli 2014 ført tilsyn med Center for Cybersikkerheds behandling af personoplysninger. Tilsynet med Efterretningstjenesterne har på dette område erstattet det såkaldte GovCERT-tilsyn, hvis virke var reguleret i den tidligere gældende lov om behandling af personoplysninger ved driften af den statslige varslingstjeneste for internettrusler m.v. Tilsynet fører tillige tilsyn med, at PET's behandling af oplysninger om fysiske og juridiske personer er i overensstemmelse med lovgivningen, og at FE's behandling af oplysninger om i Danmark hjemmehørende fysiske og juridiske personer er i overensstemmelse med lovgivningen. Tilsynet har i henhold til lov om Center for Cybersikkerhed tilsvarende bemyndigelser og adgang til oplysninger som efter FE-loven.

Tilsynet med Efterretningstjenesterne og dets sekretariat er i løbende kontakt med Center for Cybersikkerheds særlige compliance-funktion. Tilsynets sekretariat gennemfører løbende inspektionsbesøg hos især Center for Cybersikkerheds Netsikkerhedstjeneste og har bl.a. modtaget nærmere beskrivelser af Netsikkerhedstjenestens it-systemer og arbejdsprocesser.

Som led i compliance-arbejdet udarbejder centeret på eget initiativ såkaldte afvigerapporter, når der konstateres hændelser, som er eller potentielt kunne have været i uoverensstemmelse med love, retningslinjer eller interne procedurer. Formålet med rapporterne er at sikre, at der sker indsamling, analyse og formidling af viden om utilsigtede hændelser, således at der skabes grundlaget for en systematisk læring. Centeret udarbejder rapporterne uanset hændelsernes omfang og karakter, og dermed også ved afvigelser, der vurderes som mindre alvorlige. Rapporterne tilgår altid Tilsynet med Efterretningstjenesterne. Centeret har udarbejdet fem af sådanne rapporter i 2014.

Den proaktive indsats i 2014
Som national it-sikkerhedsmyndighed og myndighed for informationssikkerhed og beredskab i telesektoren varetager Center for Cybersikkerhed en række opgaver af proaktiv og dermed primært forebyggende karakter.

Det proaktive arbejde omfatter blandt andet en indsats i forbindelse med oplysning, vejledning og rådgivning af danske myndigheder og virksomheder på cybersikkerhedsområdet. Formålet med denne indsats er at mindske risikoen for cyberangreb og at sikre, at organisationen i størst muligt omfang er forberedt på at kunne imødegå cyberangreb på en hensigtsmæssig måde. I forlængelse heraf lægger centeret vægt på at have en åben, tillidsfuld og systematisk dialog med bl.a. statslige myndigheder, brancheorganisationer og større virksomheder inden for de sektorer, der beskæftiger sig med samfundsvigtige funktioner.

For at styrke dialog og åbenhed har centeret i 2014 etableret Den Tværministerielle Kontaktgruppe vedrørende Cybersikkerhed, som har repræsentanter fra samtlige ministeriers topledelser som medlemmer. I 2014 blev der afholdt to møder i gruppen, der har til formål at sikre en fælles statslig koordination, dialog og indsats på baggrund af den særlige viden om cybertrusler, cyberangreb og andre sikkerhedshændelser, som Center for Cybersikkerhed og det øvrige FE stiller til rådighed for gruppen.

I 2014 etablerede Center for Cybersikkerhed ligeledes Det Strategiske Samarbejdsforum for Cybersikkerhed, der har en lang række samfundsvigtige virksomheder fra den private sektor samt brancheorganisationer som medlemmer.

Cybertruslen mod Danmark
Af Forsvarets Efterretningstjenestes Risikovurdering 2014 fremgår det, at danske myndigheder og virksomheder fortsat er truet af en omfattende og voksende spionage via internettet. Truslen er særlig alvorlig fra statslige eller statsstøttede angreb i form af såkaldte Advanced Persistent Threats (APT). Cyberkriminelle og politisk motiverede såkaldte hacktivister vurderes at udgøre en mindre trussel. Den teknologiske udvikling medfører imidlertid, at truslen er i konstant forandring, hvilket stiller store krav til sikkerhedsforanstaltninger og beredskab.

Formålet med samarbejdsforummet er især at systematisere videndelingen på cybersikkerhedsområdet og dermed understøtte virksomhedernes egen indsats på området. Samtidig fremmer arbejdet en tillidsfuld dialog mellem Center for Cybersikkerhed og private virksomheder.

Desuden gennemførte Center for Cybersikkerhed i 2014 en opdatering af de militære it-sikkerhedsbestemmelser (FKOBST 358-1, Kap. 6) som følge af Forsvarsministeriets it-strategi. Med opdateringen styrkes Forsvarsministeriets koncerns håndtering af it-sikkerhed efter it-sikkerhedsstandarden ISO 27001.

Statistik over udvalgte dele af centerets proaktive indsats i 2014.

Kategorier	Det civile område	Det militære område	I alt
Afsluttede rådgivningssager	39	4	43
Awareness-briefinger	43	18	61
Systemsikkerhedsgodkendelser	0	128	128
Tekniske sikkerhedseftersyn	3	59	62
Tilsyn på informationssikkerheds- og beredskabsområdet i telesektoren	12	0	12

Øvrige produkter i 2014
Center for Cybersikkerhed har som led i arbejdet med at understøtte et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur, som samfundsvigtige funktioner er afhængige af, offentliggjort en række rapporter, vurderinger og vejledninger om specifikke emner inden for cybersikkerhed i 2014.

Oversigt over centerets offentliggjorte produkter i 2014.

Produkter	Formål	Udarbejdet af	Antal
Trusselsvurderinger			2
APT-trusselsvurdering.	Oplyse om en særligt avanceret, målrettet og vedholdende cyberangrebstype - de såkaldte APT-angreb (Advanced Persistent Threat)- der har ramt danske myndigheder og virksomheder.	Center for Cybersikkerhed.	
Bidrag til FE's årlige risikovurdering.	Giver en aktuel efterretningsmæssig vurdering af cybersikkerhedsforhold i udlandet af betydning for Danmarks sikkerhed.	Center for Cybersikkerhed og FE.	
Vejledninger			2
Forholdsregler ved ophør af serviceopdateringer til Windows XP embedded.	Beskriver de væsentligste forholdsregler, der bør tages forud for ophøret af serviceopdateringerne til Windows XP embedded (WXPE).	Center for Cybersikkerhed.	
Anbefalinger til, hvordan sikkerheden i den outsourcede it-drift kan forbedres.	Rapport som opfølgning på CSC-hackersagen. 11 konkrete anbefalinger til, hvordan sikkerheden i statens out-sourcede it-drift kan forbedres.	Center for Cybersikkerhed og Digitaliseringsstyrelsen.	
Situationsbillede, situationsrapporter og temarapport			10
Situationsbillede. Situationsrapporter. Temarapport.	Giver et billede af den aktuelle sikkerhedstilstand på den danske del af internettet. Beskriver de væsentlige hændelsestyper, som centeret observerer på månedsbasis. Er henvendt til it-sikkerhedsansvarlige hos myndigheder og virksomheder, der er tilsluttet Netsikkerhedstjenesten. Beskriver truslen fra spear-phishing angreb, der ofte udgør første angrebsbølge i avancerede cyberangreb.	Center for Cybersikkerhed.	

Herudover er der i 2014 udarbejdet en række klassificerede produkter, der ikke er offentligt tilgængelige.

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.

I tilfælde af cyberangreb kan myndigheder og virksomheder, der beskæftiger sig med samfundsvigtige funktioner, kontakte vagthavende hos Netsikkerhedstjenesten (GovCERT) døgnet rundt på vagttelefon 6093 4827 samt e-mail contact@govcert.dk eller via Forsvarets Efterretningstjenestes vagthavende på telefon 3332 5566. Myndigheder under Forsvarsministeriet kan kontakte Netsikkerhedstjenesten(MILCERT) på vagttelefon 3091 6502 eller e-mail milcert@milcert.dk.

Følg Center for Cybersikkerhed på de sociale medier: Twitter (@cybersikkerhed) og LinkedIn.

Center for Cybersikkerhed
Kastellet 30
2100 København Ø

Telefon: 33 32 55 80
www.cfcs.dk