Center for Cybersikkerheds beretning 2018

Indhold

CENTER FOR CYBERSIKKERHED

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

1. udgave oktober 2019.

Forsideillustration: cosmin4000/Getty Images

Cybertruslen

Der er fortsat en meget høj cybertrussel mod Danmark. Flere stater forsøger at udføre cyberspionage mod danske interesser, og det er en udvikling, der fortsætter i takt med, at flere stater opbygger og udvikler deres cyberkapaciteter. Truslen er særligt udtalt mod de dele af staten, der beskæftiger sig med udenrigs-, sikkerheds- og forsvarspolitik. Truslen er også rettet mod myndigheder og virksomheder i samfundsvigtige sektorer, da hver sektor har forskellige typer viden, som fremmede stater har interesse i.

Myndigheder og virksomheder i samtlige sektorer i Danmark kan forvente løbende at blive udsat for cyberkriminalitet. Visse typer cyberkriminalitet kan have alvorlige konsekvenser for myndigheder og virksomheder i samfundsvigtige sektorer og derfor også for det danske samfund.

Cyberaktivister retter sjældent deres fokus mod danske myndigheder og virksomheder. Nogle hackergrupper og individer i cyberaktivistiske netværk har dog væsentlige kapaciteter. Truslen kan derfor stige pludseligt, hvis danske myndigheder eller virksomheder kommer i cyberaktivisters søgelys. Militante ekstremister har i få tilfælde vist interesse i at udføre cyberterror, men de har fortsat ikke kapacitet til dette.

Det er mindre sandsynligt, at fremmede stater har til hensigt at rette destruktive cyberangreb mod samfundsvigtig infrastruktur i Danmark på kort sigt. Det er dog muligt, at danske virksomheder og myndigheder kan blive ramt som følgevirkning af destruktive cyberangreb mod mål uden for Danmark.

Nye opgaver til Center for Cybersikkerhed i 2018

Center for Cybersikkerhed (CFCS) blev oprettet i december 2012 som en del af Forsvarets Efterretningstjeneste. CFCS' hovedopgave er at understøtte et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur, som samfundsvigtige funktioner er afhængige af. Danmark er et af de mest digitaliserede lande i verden, og digitaliseringen er et afgørende middel for udviklingen af både den offentlige sektor og for virksomheders vækst og konkurrenceevne. Centeret arbejder sammen med en lang række interessenter for et sikkert digitalt Danmark.

Truslen fra cyberangreb kan ikke elimineres, men med Forsvarsforliget 2018-2023 er der afsat betydelige midler til en styrkelse af cyberområdet, herunder:

- Opbygning af et cybersituationscenter
- Udbygning af sensornetværk
- Styrket forebyggelse og rådgivning
- Styrkelse af forskning og uddannelsesindsats
- Styrkelse af analytiske og teknologiske kompetencer
- Styrket indsats i forhold til opdagelse og håndtering af konkrete hændelser
- Styrket indsats i forhold til genoprettelse efter konkrete cyberangreb i myndigheder og virksomheder i særligt samfundskritiske sektorer (energi, finans, søfart, transport, sundhed og tele)

Arbejdet finder langt hen ad vejen sted inden for rammerne af regeringens nye nationale strategi for cyber- og informationssikkerhed og det seneste forsvarsforlig.

Ny national strategi for cyber- og informationssikkerhed
Regeringen præsenterede i maj 2018 en ny national strategi for cyber- og informationssikkerhed med 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 informationssikkerhed.

Strategien tager udgangspunkt i et sektoransvarsprincip, 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 afløser den tidligere nationale strategi for cyber- og informationssikkerhed, som blev lanceret i 2014, og som var den første nationale strategi på området.

CFCS har i 2018 bidraget betydeligt til arbejdet med styring og koordination af initiativerne under den nationale strategi bl.a. i den tværministerielle styregruppe, der har delt formandskab mellem CFCS og Digitaliseringsstyrelsen og deltagelse af de samfundskritiske sektorer, samt i den bredere kontaktgruppe bestående af alle ministerier. CFCS har desuden delt formandskab med Digitaliseringsstyrelsen i advisory boardet for cyber- og informationssikkerhed med deltagelse af repræsentanter fra virksomheder, brancheorganisationer, forbrugere med særlig teknisk og strategisk indsigt, der blev nedsat efteråret 2018 til at levere input til den nationale cyber- og informationsstrategis initiativer.

Med henblik på at sikre videndeling og koordination af aktiviteter er CFCS desuden vært for et strategisk samarbejdsforum med virksomheder og brancheforeninger, særligt inden for de samfundskritiske sektorer. Derudover har CFCS i regi af den nationale strategi etableret et vidensdelingsnetværk for de samfundskritiske sektorers decentrale cyber- og informationssikkerhedsenheder.

Nationalt cybersituationscenter

En væsentlig milepæl i 2018 var etableringen af et nationalt cybersituationscenter i CFCS. Situationscenteret er tænkt som en central indgang til CFCS og har blandt andet til formål at opretholde og videreformidle et nationalt situationsbillede over de aktuelle og potentielle cybertrusler mod Danmarks vigtigste digitale netværk. Situationsbilledet skal give et overblik over truslen på baggrund af den information, som CFCS får fra sensornetværket, indberetninger fra virksomheder og myndigheder og gennem underretninger og internationalt samarbejde. Cybersituationscenteret har siden sin åbning i oktober 2018 kunnet kontaktes uanset tidspunkt, men centerets kapacitet vil i løbet af forsvarsforligsperioden 2018-2023 blive udbygget til at være bemandet døgnet rundt.

Cybersituationscenteret er en del af CFCS' netsikkerhedstjeneste, der har til opgave at opdage og håndtere sikkerhedshændelser. Netsikkerhedstjenesten og cybersituationscenteret har i løbet af 2018 fokuseret på både mere generelle sikkerhedshændelser og trusler mod dansk samfundsvigtig infrastruktur og på de mere avancerede cyberangreb fra statsstøttede aktører.

Opdagelse og håndtering af sikkerhedshændelser i 2018

Udbygning af netsikkerhedstjenestens sensornetværk
CFCS' netsikkerhedstjeneste har til opgave at afdække, analysere og bidrage til at imødegå it-sikkerhedshændelser 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 indledt et arbejde med at forberede en yderligere udbredelse af det teknisk avancerede sensornetværk til myndigheder og virksomheder, bl.a. i form af et kommercielt indkøbt supplement til det eksisterende system af egenudviklede sensorer (se faktaboks nedenfor). Der er i den forbindelse i 2018 forberedt en kortlægning af kritisk infrastruktur og dertil hørende digitale tjenester, der er væsentlige for samfundsvigtige funktioner. Kortlægningen gennemføres i samarbejde med de ansvarlige myndigheder og virksomheder i bl.a. de seks samfundskritiske sektorer (energi, tele, finans, sundhed, transport og søfart), og resultatet af kortlægningen vil indgå i grundlaget for udbygningen af sensornetværket og centerets rådgivning.

CFCS' 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 baseret løsning, der bl.a. har til formål at bidrage til et nationalt situationsbillede, med henblik på at kunne varsle myndigheder og virksomheder på baggrund af observerede trusler.

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' cybersituationscenter en alarm.

Tilslutninger til sensornetværket
CFCS har i 2018 særligt haft fokus på installation af yderligere sensorer i sensornetværket inden for Forsvaret på dets forskellige lokaliteter rundt om i Danmark.

Ved udgangen af 2018 havde CFCS i alt 64 tilsluttede myndigheder og virksomheder fordelt på 28 civile myndigheder, 34 militære myndigheder og 2 private virksomheder. Private virksomheder vil udgøre en prioritet i årene fremover.

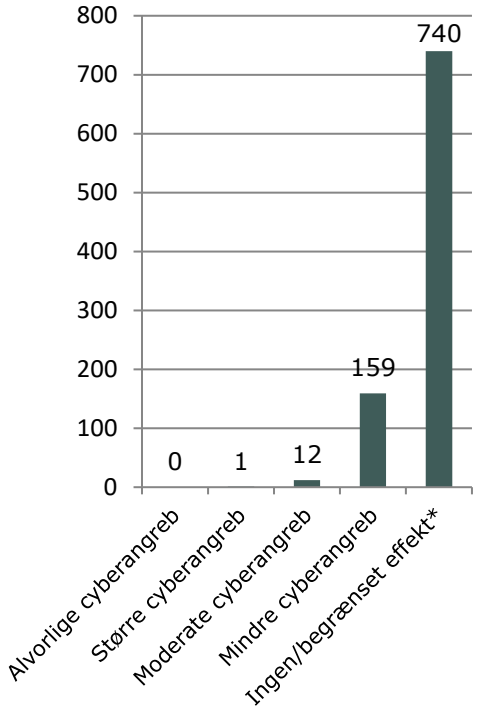
I 2018 har CFCS påbegyndt forberedelse af supplementet til det eksisterende sensornetværk, der ventes udrullet fra begyndelsen af 2020.

Sikkerhedshændelser
CFCS' netsikkerhedstjeneste 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 2018 håndteret 912 hændelser, hvoraf 740 er hændelser, der er vurderet til at have haft ingen eller begrænset effekt på den pågældende myndighed eller virksomhed. Der kan f.eks. 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. Det kan f.eks. ske ved sårbarheds- eller portscanninger. Iblandt de 740 hændelser, der er vurderet til at have haft ingen eller begrænset effekt, kan også være falske positiver. En falsk positiv er en alarm, som ved nærmere undersøgelse viser sig ikke at være et angreb.

Af de 912 hændelser, som netsikkerhedstjenesten har behandlet, har 172 hændelser haft effekt på den berørte organisation. 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.

Sikkerhedshændelser 2018



Kilde: Netsikkerhedstjenesten.
**Kategorien "Ingen/begrænset effekt" inkluderer falske positiver.*

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

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 cyberangrebet stoppes af de berørte organisationers etablerede sikkerhedsforanstaltninger som f.eks. 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 f.eks. skifte passwords i organisationen, ændre administratorrettigheder mv. Fordelingen af alvorlighedsgraden er ikke ændret nævneværdigt i forhold til 2017.

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 f.eks. 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.

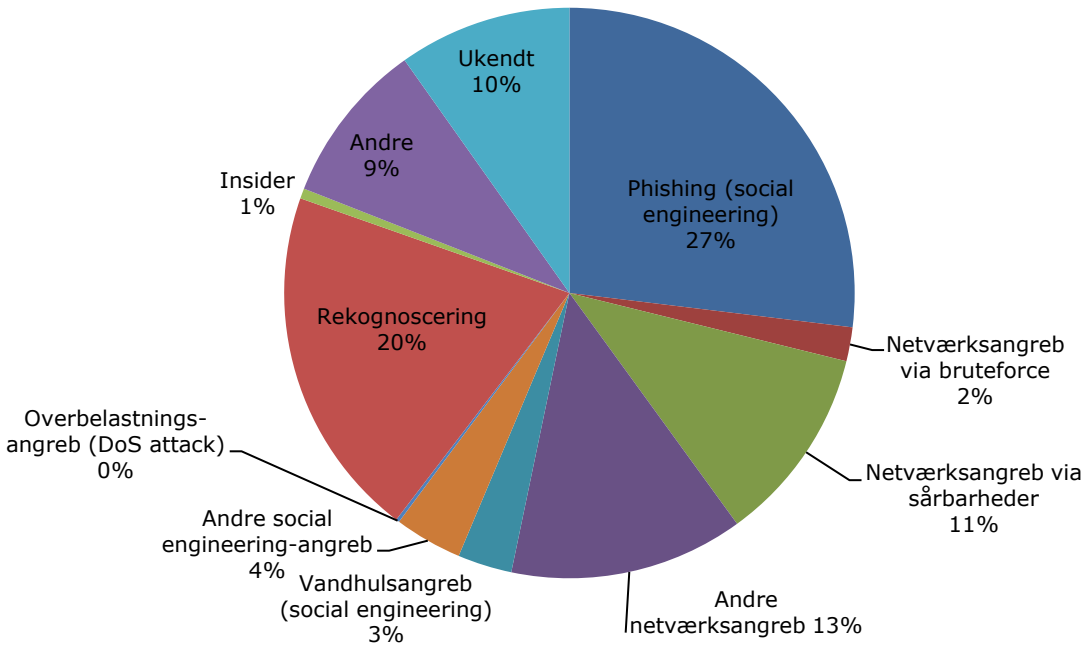
Alvorlig: Kritiske systemer berørt eller system- eller administratorkonti kompromitteret. Hændelsen har alvorlig betydning for den berørte organisation.

Kilde: Netsikkerhedstjenesten

Angrebsveje

CFCS' monitering 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 2018. Diagrammet viser ikke, hvilken indvirkning hændelsen har haft på den ramte organisation.

Identificerede angrebsveje 2018



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 især udbredte 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 f.eks. 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 f.eks. 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 f.eks. over forsøg på at udnytte sårbarheder og fejlkonfiguration af softwaren samt forsøg på at etablere uautoriseret systemadgang via brute force-angreb mod f.eks. login-oplysninger.

Brute force-angreb dækker bl.a. over at forsøge hyppigt brugte passwords (f.eks. "123456" mod mange brugernavne (f.eks. 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 f.eks. 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 2018

Styrket forebyggelses- og rådgivningsindsats
CFCS har i 2018 gennemført en væsentlig styrkelse af kapaciteten til at yde en forebyggende og rådgivende indsats i forhold til ikke mindst samfundsvigtige offentlige institutioner og virksomheder. Der er sket en væsentlig udvidelse af centerets trusselvurderingsindsats og af centerets rådgivningsvirksomhed, herunder særligt en styrkelse af centerets støtte til de seks samfundskritiske sektorer. Der er desuden sket en styrkelse af centerets forebyggende sikkerhedstekniske støtte til bl.a. Forsvaret. Som militær it-sikkerhedsmyndighed rådgiver og vejleder centeret også myndigheder på Forsvarsministeriets område om cyber- og informationssikkerhed. Det omfatter bl.a. rådgivning om installation af infrastruktur og systemer, samt sikkerhedsgodkendelse af disse. CFCS har desuden gennemført en række sårbarhedsanalyser på nogle af Forsvarets operative og administrative netværk og systemer og rådgivet om korrigerende tiltag, samt gennemført en lang række awareness-briefinger.

Trusselsvurderinger
CFCS offentliggjorde syv trusselsvurderinger og en undersøgelsesrapport i 2018. Fire af trusselsvurderingerne omhandlede cybertruslen i samfundskritiske sektorer som led i den nationale strategi for cyber- og informationssikkerhed. Dertil kommer en række klassificerede trusselsvurderinger til udvalgte kunder. Derudover bidrog CFCS med briefinger i både åbne og lukkede fora, bl.a. med sigte på at skabe opmærksomhed om, at cybertruslen kræver et vedvarende ledelsesfokus hos myndigheder og virksomheder.

Målrettet rådgivning til de samfundskritiske sektorer
En væsentlig del af CFCS' rådgivning i 2018 er sket som led i arbejdet i den tværministerielle task force nedsat i regi af den nationale strategi (foruden CFCS deltager Digitaliseringsstyrelsen og PET i task forcen). CFCS har derudover opbygget en dedikeret rådgivningskapacitet til de seks samfundskritiske sektorer til støtte for arbejdet med sektorstrategier og ikke mindst etableringen af decentrale cyber- og informationssikkerhedsenheder (DCIS'er) og et videndelingsnetværk for disse. Denne kapacitet har i sidste kvartal af 2018 gennemført 54 rådgivningsmøder målrettet sektorerne. Formålet med opbygningen af tætte og veldefinerede samarbejdsrelationer har været at højne den digitale cyber- og informationssikkerhed i de samfundskritiske sektorer og skabe sammenhæng i cyber- og informationssikkerheden på tværs af sektorerne, herunder gennem deling af erfaringer.

For telesektoren har CFCS som ansvarlig myndighed for informationssikkerhed og beredskab haft et særlig tæt samarbejde med de væsentlige erhvervsmæssige teleudbydere i forbindelse med etablering af en decentral cyber- og informationssikkerhedsenhed for telesektoren.

Oversigt over forebyggelsesindsatser 2018

Kategorier	Antal
Rådgivnings- og kundemøder	598
Awareness-briefinger	138
It-sikkerhedsgodkendelser	31
Godkendelse af kryptoplaner	44
Sikkerhedstekniske eftersyn	78
Sikkerhedstekniske undersøgelser	8
Tempest zoning (udstrålingskontrol)	16
Tilsyn på Forsvarsministeriets område	17
Varsler	167*
Tweets	218**

Note: Udvikling i tallene afhænger af behov og efterspørgsel efter CFCS' ekspertise. En del af den væsentlige stigning i rådgivnings- og kundemøder skyldes en særlig indsats på forsvarsområdet, som fandt sted i 2018.

** I 2018 er 66 af varslerne udsendt efter cybersituationscenterets åbning 1. oktober 2018.*

*** CFCS har i 2018 udsendt omtrent 218 tweets, hvoraf ca. 70 er udsendt af cybersituationscenteret, der blev oprettet pr. 1. oktober 2018. Dette har tilsammen genereret omtrent 714 retweets og 1.264.500 eksponeringer.*

Varsler

I forbindelse med væsentlige cyberangreb, aktuelle cybertrusler eller it-sikkerhedshændelser, som kan have interesse og relevans for en bred eller en begrænset kreds af myndigheder, virksomheder og andre, udsender CFCS' situationscenter varsler, som bl.a. indeholder konkrete tekniske anbefalinger i forbindelse med en aktuel trussel. Varslerne udarbejdes bl.a. med udgangspunkt i den viden fra CFCS' sensornetværk, der monitorerer netværkstrafikken til og fra de tilsluttede myndigheder og virksomheder. Centeret benytter også tweets fra bl.a. situationscenteret til at gøre opmærksom på trusler og sårbarheder med henblik på håndtering i relevant omfang.

SCADA-netværk

Efterspørgslen efter rådgivning i relation til industrielle kontrolsystemer som f.eks. SCADA-systemer (Supervisory Control And Data Aquisition) er i vækst. Området har stor betydning for it-driften i både Forsvaret, de samfundskritiske sektorer og national kritisk infrastruktur. CFCS har i 2018 faciliteret oprettelsen af et SCADA-forum i samarbejde med vigtige danske aktører på området. Derudover arrangerede CFCS et SCADA-kursus i Idaho, USA hos USA's Ministerium for Indenlandsk Sikkerhed (Homeland Seurity), hvor interessenter fra nogle af de samfundskritiske sektorer deltog.

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 går direkte videre til både de ansvarlige sektormyndigheder samt til Datatilsynet og CFCS og bidrager til at give et mere nuanceret og detaljeret billede over de sikkerhedshændelser, der rammer myndigheder og virksomheder i Danmark. I CFCS er det situationscenteret, der er første modtager af indberetninger om sikkerhedshændelser. CFCS modtog 20 indberetninger i 2018.

Informationssikkerhed i leverandørforhold
Særligt på Forsvarsministeriets område har CFCS i 2018 fokuseret på leverandørstyring, hvilket understøttes af initiativer i Forsvarsministeriets informationssikkerhedsstrategi 2018-2020. CFCS har også 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.

Mobilsikkerhed
CFCS har sammen med PET udarbejdet vejledningen "Råd om sikkerhed på mobile enheder". Vejledningen, der især henvender sig til centraladministrationens embedsfolk, beskriver en række organisatoriske, tekniske og adfærdsmæssige tiltag, der kan styrke mobilsikkerheden omkring anvendelse af mobile enheder.

Assistance til SKI og andre indkøbsaktører
CFCS har i 2018 ydet rådgivning om informationssikkerhed og sikkerhedskrav til SKI (Statens og Kommunernes indkøbsservice) og andre aktører, der indkøber it-udstyr og services til national anvendelse. Indsatsen har haft særligt fokus på rådgivning til udarbejdelse af krav til leverandører, hvor kravene kan anvendes til at højne sikkerhedsniveau under hensyn til den enkelte kundes særlige risikoforhold.

Sikkerdigital.dk
Som led i den nationale strategi er portalen sikkerdigital.dk åbnet, med henblik på at borgere, virksomheder og myndigheder kan finde viden, vejledning og konkrete værktøjer til en sikker digital hverdag. Portalen er udarbejdet i samarbejde med CFCS, der hermed bidrager til at højne kendskabet til cybertruslerne og kontinuerligt forbedre bevidstheden om, hvordan de imødegås med sikker adfærd.

Forberedelse af rådgivning til de opstillingsberettigede partier
Visse lande bruger påvirkningskampagner til at øve indflydelse på interne politiske forhold i bl.a. Vesten for at opnå egne udenrigspolitiske mål. For at modvirke og begrænse ekstern påvirkning af det danske folketingsvalg i 2019 udarbejdede regeringen i 2018 en valghandlingsplan med henblik på at styrke værnet mod påvirkningskampagner. Som led i valghandlingsplanen har CFCS i samarbejde med Politiets Efterretningstjeneste i løbet af 2018 forberedt, og i starten af 2019 gennemført, rådgivning for de opstillingsberettigede partier. Fokus for rådgivningen har været cybertrusler og imødegåelse.

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. CFCS har derfor i 2018 bidraget til regeringens forberedelse af et lovforslag vedr. opdatering af CFCS' lovgrundlag (lov om Center for Cybersikkerhed). Lovforslaget (lov nr. 555) blev vedtaget i Folketinget den 7. maj 2019.

Lovændringens indhold
Lovændringen indebærer for det første, at gebyret for tilslutning til CFCS' netsikkerhedstjeneste fjernes, således at tilslutning fremover vil være gratis for myndigheder og virksomheder, der har 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. Påbudsordningen vil ikke omfatte monitorering ved hjælp af sikkerhedssoftware samt aktivt cyberforsvar.

For det andet indebærer lovforslaget, at CFCS' netsikkerhedstjeneste vil kunne agere mere aktivt i beskyttelsen af samfundsvigtige myndigheder og virksomheder. Tidligere har centerets alarmenheder alene kunnet anvendes til, at CFCS kan registrere den skadelige trafik og derefter varsle myndigheden eller virksomheden om, at den har været udsat for et angreb. Med lovforslaget er der skabt mulighed for at anvende alarmenhederne til at stoppe igangværende cyberangreb, f.eks. ved at blokere eller omdirigere skadelig trafik hos de myndigheder og virksomheder, som har ønsket at tilslutte sig en sådan ordning.

For det tredje giver lovændringen mulighed for at installere sikkerhedssoftware på f.eks. pc'er og servere hos myndigheder og virksomheder, der er tilsluttet centerets netsikkerhedstjeneste. Det vil udvide CFCS' muligheder for tidligt at opdage cyberangreb hos de tilsluttede organisationer, idet sikkerhedssoftwaren vil kunne opdage unormal aktivitet, såsom kommandoer om at sende store mængder data til en ukendt enhed på internettet. Installation af sikkerhedssoftware vil være frivillig.

For det fjerde giver lovændringen CFCS mulighed for at fortage forebyggende sikkerhedstekniske undersøgelser hos myndigheder og virksomheder, der efterspørger centerets bistand til at identificere sårbarheder og vurdere robustheden af deres systemer. Dette vil altid foregå efter aftale med den pågældende myndighed eller virksomhed, og CFCS' afrapportering vil altid være anonymiseret, således at der ikke i forbindelse med den forebyggende sikkerhedstekniske undersøgelse videregives

oplysninger om konkrete medarbejderes handlinger eller undladelser til den pågældende organisation.

For det femte indebærer lovændringen, at CFCS får mulighed for at anvende såkaldte "honey pots", som vil kunne bruges som en form for afledningsmanøvre og kilde til viden om aktører bag angreb, og såkaldte "sinkholes", som potentielt vil kunne afskære angrebsaktøren fra at styre sin angrebsplatform.

Derudover indebærer lovændringen, at CFCS gennem såkaldt edition efter rettens kendelse kan få udleveret oplysninger om brugeren af en e-mailkonto, en ip-adresse eller et domænenavn, hvis det er nødvendigt for at afdække en sikkerhedshændelse. Endvidere vil de tidligere meget restriktive rammer for CFCS' mulighed for at videregive data blive lempet, så det eksempelvis bliver muligt at videregive selve den skadelige kode (malware), der ligger bag et angreb, til relevante aktører. Dertil kommer en forlængelse af slettefristerne, således at CFCS eksempelvis får bedre mulighed for at gemme data, der er knyttet til en konkret sikkerhedshændelse.

Tilsynsopgaver i 2018

Tilsynsvirksomhed på Forsvarsministeriets område
CFCS har i 2018 i lighed med tidligere år ført tilsyn med informationssikkerheden på Forsvarsministeriets område, herunder ved departementet og samtlige styrelser. Tilsynet har haft hovedfokus på myndighedernes ledelsessystem for informationssikkerheden i henhold til standarden ISO/IEC 27001. Tilsynet har i 2018 haft særlig fokus på ledelsesforankring og handleplaner, herunder særligt handleplaner for håndtering af identificerede risici og implementering af kontroller relevante for sikkerhedsniveauet samt for håndtering af væsentlige mangler ved implementering af standarden. Særlige fokusområder derudover har været internetvendte systemer, leverandørstyring og håndtering af hændelser.

Tilsynsopgaver mv. på teleområdet
CFCS har som led i sin lovbestemte rolle som tilsynsmyndighed for informationssikkerhed og beredskab på teleområdet i 2018 ført tilsyn hos udvalgte teleudbydere. Tilsynet har haft hovedfokus på at sikre, at teleudbyderne har etableret et ledelsesinformationssystem for informationssikkerhed efter en anerkendt international standard (som f.eks. ISO/IEC 27001). Derudover har der i 2018 været ført tilsyn med udvalgte teleudbyderes beredskab og krisestyring.

CFCS har i 2018 også lavet eftersyn på sikkerhedsaftaler, der er etableret på frivillig basis med større teleudbydere. Efter aftale med Moderniseringsstyrelsen og SKI har CFCS også gennemført it-sikkerhedsrevision af rammekontrakter på teleområdet.

CFCS har i 2018 samarbejdet med såvel grønlandske som færøske telemyndigheder om sikkerhedsrådgivning i forbindelse med leverandørstyring.

For Grønlands vedkommende har denne rådgivning været koncentreret om etablering af et søkabel langs den grønlandske vestkyst med tilhørende teknikhuse. Derudover er der ydet sikkerhedsrådgivning i forbindelse med udarbejdelse af it- og informationssikkerhedspolitik hos det grønlandske telesekslab, TELE-POST.

For Færøerne har CFCS samarbejdet med såvel de færøske myndigheder, som de to færøske teleselskaber, Føroya Tele og Hey, om sikkerhedsrådgivning i forbindelse med udrulning af de kommende 5G-mobilnet på Færøerne.

Arbejde i Grønland og Færøerne er sket på invitation fra de lokale myndigheder og teleselskaber, da CFCS ikke har myndighed på området, idet teleområdet er hjemtaget af henholdsvis de grønlandske og færøske myndigheder

EU-samarbejdet i 2018

Bidrag til europæisk samarbejde om cybersikkerhed
CFCS repræsenterer Danmark i bestyrelsen for ENISA (EU's Cybersikkerhedsagentur) og har i 2018 bidraget til formulering af dansk holdning på cybersikkerhedsområdet både relation til ENISA's løbende arbejde og i forhold til at revidere cybersikkerhedsforordningen, der bl.a. omfatter en udvidelse af ENISA's mandat, samt i forhold til forslaget om et europæisk cybersikkerhedscenter.

CFCS har forestået dansk deltagelse i samarbejdsgruppen og CSIRT-samarbejdet (Computer Security Incident Response Team), som er nedsat i regi af NIS-direktivet. Under samarbejdsgruppen er der etableret en række arbejdsgrupper vedrørende implementerings-, fortolknings- eller koordineringsspørgsmål, som opstår som led i medlemsstaternes arbejde i forbindelse med NIS-direktivet, og CFCS har koordineret danske bidrag hertil. CSIRT-samarbejdet omhandler videndeling og koordination af operative anliggender.

NIS-direktivet
NIS-direktivet trådte i kraft i 2018 og er implementeret sektorvist i Danmark. Det 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 bl.a. udbydere af væsentlige tjenester.

Om FE's Center for Cybersikkerhed

CFCS blev oprettet i december 2012 som en del af Forsvarets Efterretningstjeneste (FE) og er Danmarks nationale it-sikkerhedsmyndighed og den centrale nationale myndighed vedrørende cybersikkerhed, der udgør Danmarks forsvar mod cybertrusler. Centeret arbejder sammen med en lang række interessenter for et sikkert digitalt Danmark. 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, informations-sikkerhedsrådgivere og teleingeniører. Størstedelen af centerets medarbejdere 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. Ved udgangen af 2018 var der ca. 125 medarbejdere i centeret.

Om 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 Center for Cybersikkerhed trådte i kraft. Efter offentliggørelsen vil TET's årlige redegørelse være tilgængelig på CFCS' hjemmeside www.cfcs.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.

Publikationer i 2018

Vejledninger

Råd om sikkerhed på mobile enheder
Vejledning giver en række anvisninger til, hvordan man kan forbedre sikkerheden for mobiltelefoner, tablets og bærbare pc'er. Vejledningen kan hjælpe med at træffe en vurdering af, hvilke sikkerhedstiltag der er nødvendige for en organisation og dens medarbejdere, som anvender mobile enheder. Vejledningen bygger på et samarbejde med Politiets Efterretningstjeneste om at rådgive embedsfolk om god mobilsikkerhed, men rådene kan være brugbare for alle, der ønsker at være mere sikre i deres brug af mobile enheder.

Trusselsvurderinger

Hovedparten af trusselsvurderingerne udgives både på dansk og engelsk.

Trusselsvurdering: Cybertruslen mod land- og lufttransport
Denne trusselsvurdering redegør for cybertrusler, der er rettet mod den danske transportsektor. Transportsektoren i Danmark er vigtig for samfundets funktion og stabilitet. Hensigten er at orientere transportsektoren om truslerne, så den bedre kan beskytte sig. Trusselsvurderingen kan eksempelvis indgå i risikovurderingen for sektoren i forbindelse med den nationale strategi for cyber- og informationssikkerhed.

Trusselsvurdering: Cybertruslen mod energisektoren
Trusselsvurderingen redegør for de cybertrusler, som er rettet mod energisektoren i Danmark. Energisektoren har direkte betydning for samfundets funktion, stabilitet og sikkerhed. Trusselsvurderingen udgives til anvendelse i bl.a. risikovurderingen for sektoren i forbindelse med den nationale strategi for cyber- og informationssikkerhed.

Trusselsvurdering: Cybertruslen mod Danmark 2018
Formålet med denne årlige, nationale trusselsvurdering er at redegøre for den samlede cybertrussel, der møder danske myndigheder og private virksomheder. Truslen er størst fra cyberspionage udført af stater og fra cyberkriminalitet. Truslen er under fortsat udvikling.

Trusselsvurdering: Cybertruslen mod finanssektoren
Trusselsvurderingen redegør for de cybertrusler, der er rettet imod den danske finanssektor. Finanssektoren i Danmark er vigtig for samfundets funktion, stabilitet og økonomi. Hensigten er at orientere finanssektoren om truslerne, så den bedre kan beskytte sig. Trusselsvurderingen kan eksempelvis indgå i risikovurderingen for sektoren i forbindelse med den nationale strategi for cyber- og informationssikkerhed.

Trusselsvurdering: Cybertruslen mod sundhedssektoren
Denne trusselsvurdering redegør for cybertrusler, der er rettet imod den danske sundhedssektor. Sundhedssektoren i Danmark er vigtig for samfundets funktion, stabilitet og velfærd. Hensigten er at orientere sundhedssektoren om truslerne, så den bedre kan beskytte sig. Trusselsvurderingen kan eksempelvis indgå i risikovurderingen

for sektoren i forbindelse med den nationale strategi for cyber- og informationssikkerhed.

Trusselsvurdering: Danske universiteter er mål for cyberangreb
Et cyberangreb mod bl.a. danske universiteter understreger cybertruslen mod universiteter og
forskningsinstitutioner i Danmark.

Trusselsvurdering: Meltdown og Spectre gør computere sårbare over hele verden
Formålet med denne trusselsvurdering er at orientere om to sårbarheder ved computeres Central Processing Unit (CPU), som potentielt kan medføre alvorlige kompromitteringer af de systemer, CPU'erne sidder i. Det er vigtigt, at myndigheder og virksomheder følger denne vurderings anbefalinger.

Undersøgelsesrapporter

Undersøgelsesrapport: Målrettede forsøg på hacking af den danske energisektor
Denne undersøgelsesrapport beskriver flere målrettede forsøg på at få uautoriseret adgang til netværk i organisationer i den danske energisektor i 2017. Rapporten indeholder forslag til tiltag, der med udgangspunkt i erfaringerne fra hændelserne kan hjælpe myndigheder og virksomheder til at modvirke lignende forsøg på indbrud.

Eksempler på varsler udsendt af cybersituationscenteret

Anonymiseret varsel: Indgående inficerede e-mails (TLP: AMBER)

Til den it-sikkerhedsansvarlige

CFCS konstaterer, at der mellem d. 2. og 7. september 2018 er modtaget 22 mails hos [myndighed/virksomhed] indeholdende kendt malware.

Yderligere information

Følgende mails indeholder kendte typer malware:
[Tekniske detaljer]

Anbefaling

I alle tilfælde er mail accepteret, det er dog muligt at senere filtrering har identificeret og fjernet malware.
På baggrund af dette anbefaler CFCS, at I undersøger, om de pågældende mails er leveret hos modtageren. Skulle dette være tilfældet bør de pågældende maskiner undersøges for malware.

Rådgivning

CFCS kan tilbyde at bistå [myndighed/virksomhed] med rådgivning i relation til styring af informationssikkerhed generelt.

Anonymiseret varsel: Muligt phishing-forsøg (TLP: AMBER)

Til den it-sikkerhedsansvarlige

CFCS konstaterer tre besøg på en side relateret til phishing hhv. d. 8. og 9. november 2018. Besøgene indikerer, at en eller flere mails er modtaget og åbnet hos [myndighed/virksomhed].

Yderligere information

[Tekniske oplysninger vedr. de pågældende mails]

Anbefaling

CFCS anbefaler, at:

- [myndighed/virksomhed] identificerer den eller de brugere, der har tilgået domænet [angivelse af domænet] med henblik på at sikre, at de pågældende brugeres PC ikke er inficeret af malware.
- [myndighed/virksomhed] identificerer den eller de pågældende mails indeholdende link til domænet og sikrer, at disse slettes fra serveren såvel som på brugerens PC.

Rådgivning

CFCS kan tilbyde at bistå [myndighed/virksomhed] med rådgivning i relation til styring af informationssikkerhed generelt.

Anonymiseret varsel: Bunitu proxy botnet (TLP: AMBER)

Til den it-sikkerhedsansvarlige

CFCS konstaterer, at der den 25. september 2018 er sendt 'Bunitu proxy botnet registration messages' fra en maskine hos [myndighed/virksomhed].

Yderligere information

Den pågældende maskine har MAC-adressen [MAC-adresse] og booter 2018-09-25 kl. 10:49:16 og får tildelt IP-adressen [IP-adresse].

Anbefaling

Maskinen med IP/MAC [IP- samt MAC-adresse] vurderes at være inficeret med 'Bunitu proxy botnet'.
På baggrund af dette anbefaler CFCS, at maskinen lokaliseres, og at der foretages en re-installation af operativsystemet.

Rådgivning

CFCS kan tilbyde at bistå [myndighed/virksomhed] med rådgivning i relation til styring af informationssikkerheden generelt.

Kontakt til Center for Cybersikkerhed

Center for Cybersikkerhed kan inden for daglig kontortid (kl. 8-16) 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 Center for Cybersikkerhed kan ske på telefon 33 32 55 80 eller på e-mail tele@cfcs.dk.

Følg Center for Cybersikkerhed
Center for Cybersikkerhed kan følges på Twitter og Linkedin, hvor centeret løbende deler bl.a. 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