FORSVARSMINISTERIET
DANISH MINISTRY OF DEFENCE

NOTAT

Bilag:
FMN-CHSNO
2018/001603 - 763530
13. marts 2018

CENTER FOR CYBERSIKKERHEDS ROLLE I FM. IMPLEMENTERING AF NIS-DIREKTIVET

Etableringen af Center for Cybersikkerhed

I forbindelse med regeringsdannelsen efter Folketingsvalget i 2011 blev en række it-sikkerhedsmæssige opgaver og den såkaldte GovCERT ressortoverført til Forsvarsministeriet. Regeringen besluttede endvidere at samle "de forskellige myndigheders indsats i et IT sikkerhedscenter (under Forsvarsministeriet), der skal varetage opgaven som den nationale IT-sikkerhedsmyndighed og Governmental Computer Emergency Response Team (GovCERT)."

På den baggrund oprettede den daværende regering Center for Cybersikkerhed som en del af Forsvarets Efterretningstjeneste (FE) i 2012. Baggrunden for placeringen af Center for Cybersikkerhed ved FE var særligt at opnå synergieffekter i form af eksempelvis udnyttelse af FE's erfaringer inden for it-sikkerhedsområdet, viden om det internationale trusselsbillede på cyberområdet og særlige adgang til oplysninger fra udlandet om cybertrusler.

De fleste alvorlige cyberangreb kommer fra udlandet, og FE har som udenrigsefterretningstjeneste en særlig fortrolig viden om avancerede cyberangreb, og hvem der står bag. Den viden har Center for Cybersikkerhed adgang til som en del af FE, og den udgør fundamentet i det ekstra lag af beskyttelse mod avancerede cyberangreb, som Center for Cybersikkerhed kan bibringe Danmark. Den viden ville Center for Cybersikkerhed ikke kunne opnå ved en placering uden for FE, og dermed ville muligheden for at beskytte Danmark mod cyberangreb blive ringere. Endvidere sikrer placeringen ved FE, at Danmarks meget specialiserede, men knappe ressourcer på it-sikkerhedsområdet samles ét sted, og hermed undgås det at opbygge parallelle kapaciteter.

Med Aftale på forsvarsområdet 2013-2017 skete der en styrket indsats på cyberområdet, herunder specifikt en styrkelse af Center for Cybersikkerhed.

Med Folketingets vedtagelse af FE-loven i 2013 blev det endvidere fastsat ved lov, at Center for Cybersikkerhed er en del af FE, og at centerets virksomhed skal reguleres særskilt, hvilket skete med Folketingets vedtagelse af CFCS-loven i 2014. Folketinget vedtog i 2015 desuden lov om net- og informationssikkerhed, der gav Center for Cybersikkerhed øgede beføjelser til at varetage myndighedsopgaver i forhold til teleudbyderne mhp. at styrke informationssikkerheden i telesektoren og dermed beskytte danske borgeres, virksomheders og myndigheders oplysninger.

Med Aftale på forsvarsområdet 2018-2023 er der opnået bred politisk enighed om en markant styrkelse af Danmarks cyberforsvar. De konkrete initiativer i forsvarsforliget vil først og fremmest styrke Center for Cybersikkerheds forebyggende indsats gennem styrket rådgivning og vejledning med særligt fokus på samfundsvigtige sektorer, herunder i forhold til myndigheder og virksomheder. Samtidig styrkes indsatsen i forhold til detektion og håndtering af konkrete hændelser samt genoprettelse af sikkerhed efter konkrete angreb inden for samfundsvigtige sektorer i både offentligt og privat regi.

<u>Reguleringen af Center for Cybersikkerheds virksomhed</u>
Center for Cybersikkerhed og den øvrige del af FE er – selvom de udgør én myndighed – ved lov tillagt forskellige opgaver og virkemidler. Center for Cybersikkerhed er særskilt reguleret i CFCS-loven, hvor der i bemærkningerne er forudsat en hvis organisatorisk adskillelse mellem centeret og den efterretningsmæssige del af FE. Det er også forudsat, at centeret har en åben og udadvendt profil, og at centerets virksomhed skal være præget af åbenhed, vejledning og information.

EU's databeskyttelsesdirektiv finder ikke anvendelse på behandlinger af personoplysninger, der vedrører aktiviteter, som ikke er omfattet af fællesskabsretten, f.eks. aktiviteter vedrørende statens sikkerhed. På den baggrund gælder den danske persondatalov – der implementerer databeskyttelsesdirektivet i dansk ret – heller ikke for behandlinger af personoplysninger, der udføres af FE, herunder Center for Cybersikkerhed.

En række af de centrale bestemmelser i persondataloven er imidlertid indarbejdet i CFCS-loven, der regulerer centerets virksomhed. Endvidere fører Tilsynet med Efterretningstjenesterne, som er et uafhængigt kontrolorgan med en landsdommer i spidsen, tilsyn med Center for Cybersikkerheds behandling af personoplysninger, herunder også centerets videregivelse af personoplysninger. Tilsynet kan hos CFCS kræve enhver oplysning og alt materiale,

der er af betydning for tilsynets virksomhed, og tilsynet har til enhver tid adgang til alle lokaler, hvorfra der er adgang til de oplysninger, som behandles, eller hvor tekniske hjælpemidler anvendes. Man kan som borger klage til tilsynet, hvis man mener, at centeret ulovligt behandler personoplysninger om en. Tilsynet afgiver endvidere hvert år en redegørelse om kontrollen med Center for Cybersikkerhed, og redegørelsen offentliggøres.

Denne retstilstand videreføres som udgangspunkt, når EU's databeskyttelsesdirektiv fra 25. maj 2018 erstattes af den nye databeskyttelsesforordning samt den foreslåede danske databeskyttelseslov. Det bemærkes dog, at der med lovforslag nr. L 155, der konsekvensændrer CFCS-loven som følge af den nye regulering på databeskyttelsesområdet, er lagt op til, at forsvarsministeren får hjemmel til helt eller delvist at sætte databeskyttelsesforordningen og databeskyttelsesloven i kraft for dele af Center for Cybersikkerheds virksomhed, herunder centerets virksomhed i medfør af det såkaldte NIS-direktiv (Europa-Parlamentets og Rådets direktiv 2016/1148/EU af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen). Dette lovforslag er fortsat under behandling i Folketinget.

Det bemærkes i øvrigt, at Center for Cybersikkerhed er undtaget fra offentlighedsloven og dele af forvaltningsloven. I praksis er centeret imidlertid omfattet af begge love. Det fremgår således af bemærkningerne til CFCS-loven, at centeret forudsættes i videst muligt omfang at efterleve bestemmelserne i de to love.

<u>Center for Cybersikkerheds opgaver som nationalt centralt kontaktpunkt og it-beredskabsenhed (CSIRT) i medfør af NIS-direktivet</u>

Center for Cybersikkerhed skal varetage funktionen som nationalt centralt kontaktpunkt i Danmark. Det nationale centrale kontaktpunkt skal bl.a. udgøre et forbindelsesled, som faciliterer det grænseoverskridende samarbejde med bl.a. de andre medlemsstater. Center for Cybersikkerhed er i forvejen national it-sikkerhedsmyndighed og står for en forebyggende national rådgivnings- og oplysningsvirksomhed om cybersikkerhed i forhold til både den offentlige og private sektor samt en reaktiv indsats. Centeret varetager endvidere en række myndighedsopgaver og er således Danmarks centrale nationale myndighed vedrørende cybersikkerhed. Funktionen som nationalt centralt kontaktpunkt ligger derfor i naturlig forlængelse af disse opgaver.

Center for Cybersikkerhed vil fremover varetage funktionen som Danmarks nationale it-beredskabsenhed (CSIRT). Det indebærer, at centeret bl.a. skal løse følgende opgaver:

- Monitorering af hændelser på nationalt plan.

- Tidlig varsling, advarsler, meddelelser og formidling af information til relevante interessenter om risici og hændelser.
- Reaktion på hændelser.
- Udarbejdelse af dynamiske risiko- og hændelsesanalyser og situationsrapporter.
- Deltagelse i det europæiske CSIRT-netværk.
- Etablering af samarbejde med den private sektor.
- Fremme anvendelsen af fælles eller standardiserede procedurer for håndtering af hændelser og risici.
- Fremme anvendelsen af fælles eller standardiserede systemer til klassificering af hændelser, risici og oplysninger.

CSIRT-funktionen efter NIS-direktivet har en nær sammenhæng med Center for Cybersikkerheds eksisterende opgaver, bl.a. som netsikkerhedstjeneste. Center for Cybersikkerhed besidder derfor allerede i dag mange af de kompetencer, der er nødvendige for f.eks. at kunne varsle sektorerne samt reagere på hændelser, ligesom centeret tillige vil kunne operere døgnet rundt. Funktionen som CSIRT ligger derfor også i naturlig forlængelse af centerets eksisterende opgaver.

Behandling af personoplysninger i forbindelse med NIS-direktivet

NIS-direktivet stiller krav om, at de omfattede myndigheder og virksomheder skal underrette enten sektorens egen tilsynsmyndighed eller it-beredskabsenheden (CSIRT'en), når der sker væsentlige hændelser. En hændelse kan f.eks. være et hackerangreb eller et alvorligt nedbrud.

I Danmark er der valgt en model, hvor underretninger om hændelser tilgår både tilsynsmyndigheden i sektoren og Center for Cybersikkerhed. Tilsynsmyndigheden vil primært skulle anvende underretningen til at vurdere, om myndigheden/virksomheden overholder reglerne og har et tilfredsstillende sikkerhedsniveau, mens Center for Cybersikkerhed skal foretage en operativ behandling, hvor man f.eks. udsender varslinger om et hackerangreb, der kan brede sig, eller underretter myndighederne i andre EU-lande.

De underretninger, som Center for Cybersikkerhed modtager, vil typisk bestå af en-to A4-sider med en faktuel beskrivelse af hændelsen. De eneste personoplysninger, som underretningerne forudsættes at indeholde, er kontaktoplysninger på afsenderen samt f.eks. en ip-adresse, der er knyttet til selve angrebet. Der er således ikke tale om, at Center for Cybersikkerhed får adgang til myndighedens/virksomhedens it-systemer, eller at der er nogen forventning om, at underretningerne indeholder oplysninger fra disse systemer.