Anbefalinger til en styrkelse af Danmarks cybersikkerhed

Indledning - Danmark har brug for øget styrke til at imødegå af cyberangreb.

De seneste omfattende cyberangreb så som Wannacry og senest "not-Petya", der i Danmark bl.a. ramte Mærsk hårdt viser, at virksomheder kan blive ramt vilkårligt af cyberangreb, men også at cyberangreb fra både statslige aktører og kriminelle grupper påfører samfundet betydelige omkostninger – de samlede skadesomkostninger er slet ikke gjort op endnu.

Private virksomheder og i særdeleshed små og mellemstore virksomheder er udfordret i forhold til at opretholde et beskyttelsesniveau, som modsvarer trusselsbilledet. Dels er der knaphed på medarbejdere med cyberkompetencer, og dels er angrebene i stigende grad designet til at lamme væsentlige digital infrastruktur.

Der er i Danmark brug for en ny tilgang til at bekæmpe cyberangreb.

I forbindelse med det kommende forsvarsforlig har flere partier i Folketinget givet udtryk for, at der skal gives et substantielt løft til Forsvaret, herunder særligt til cyberområdet, og regeringen har påbegyndt initiativer til at opruste på området.

Forsvaret har til formål at beskytte det danske territorium mod udenlandske angreb, og Forsvaret kan i den forbindelse tage midler i anvendelse, som civile myndigheder ikke kan, eksempelvis indhenter Forsvarets Efterretningstjeneste (FE) information i udlandet af interesse for Danmark. I sagens natur sker dette ofte uden de lokale myndigheds vidende. Der er - og skal selvfølgelig fortsat gælde - særlige regler for anvendelse af forsvarets kapaciteter. Eksempelvis kan FE ikke operere i Danmark og forsvaret yder støtte til politiet efter politiets anmodning. Tiden er inde til, at forsvarskapacitet også anvendes til at beskytte det danske digitale territorium.

Traditionelt har Forsvaret kun haft fokus på truslen fra andre stater – dette gælder også på cyberområdet. I Center for Cybersikkerhed har den såkaldte netsikkerhedstjeneste kun øje for angreb fra andre stater og af FE's årsberetning ses, at dette også gælder for tjenestens øvrige cyberaktiviteter. Tillige er støtten fra forsvaret på cyberområdet i dag passiv. Der er mulighed for råd og vejledning, og Center for Cybersikkerhed kan se, om et angreb har fundet sted, men ikke bidrage til at stoppe det, før skaden er sket.

Forslag

DANSK IT ønsker, at der i forbindelse med det kommende forsvarsforlig stilles krav til Forsvarets Efterretningstjeneste og til Center for Cybersikkerhed om at stille kapaciteter til rådighed for virksomheder og myndigheder, der aktivt kan imødegå truslen fra cyberangreb, og har udarbejdet seks konkrete forslag:

1) Gratis DNS-tjeneste

Efter britisk model skal der stilles en gratis DNS-tjeneste til rådighed for virksomheder og myndigheder. DNS-tjenesten indeholder en liste over domæner, som Forsvarets Efterretningstjeneste har valideret som værende relateret til cyberkriminalitet eller cyberspionage. Virksomheder og myndigheder kan frivilligt tilslutte sig tjenesten og dermed sikre, at organisationens trafik ikke uforvarende får kontakt til domæner, der kan skade organisationens infrastruktur.

2) Vidensdeling mellem FE og politiet

Som led i den styrkede bekæmpelse af angreb fra cyberkriminelle skal Forsvarets Efterretningstjeneste anvende sine indhentningskapaciteter til at indsamle viden om de cyberkriminelles infrastruktur og betalingsstrømme med henblik på at forhindre infrastrukturens anvendelse mod Danmark f.eks. via DNS-tjenesten, og ved at stille viden til rådighed for politiet om de cyberkriminelle med henblik på retsforfølgelse og konfiskation af fortjenesterne. De cyberkriminelle skal opleve, at det ikke er risikofrit at begå cyberkriminalitet mod Danmark.

3) Godkendelsesordning for samarbejde mellem FE og virksomheder

Selvom indsatsen styrkes for at forhindre cyberangreb, vil sådanne fortsat ramme virksomheder og myndigheder. Imødegåelse af cyberangreb – især fra statslige aktører og avancerede cyberkriminelle – kræver adgang til særlig viden. Når Forsvarets Efterretningstjeneste opnår viden om angrebsindikatorer, skal den viden stilles til rådighed for private virksomheder, der er specialiserede i at imødegå cyberangreb.

Den norske sikkerhedsmyndighed har etableret en godkendelsesordning for virksomheder, der er specialiserede i at imødegå angreb, via en godkendelsesordning sikres det, at disse virksomheder har den viden og kapacitet, som de bryster sig af, og sikkerhedsmyndigheden kan sikre, at disse virksomheder er i stand til at beskytte de fortrolige oplysninger, som de modtager. I forsvarsforliget bør Forsvarets Efterretningstjeneste pålægges at etablere en tilsvarende ordning og – ikke mindst – aktivt dele information med de godkendte virksomheder.

4) Oplysningstjeneste til borgerne om cybersikkerhed

Der er ikke et sted i dag, hvor borgerne kan få information og råd om cybersikkerhed. Frem til 2011 lå opgaven i It- og Telestyrelsen, men ved styrelsens nedlæggelse blev opgaven ikke overført til andre ministerområder. Der er behov for en oplysningstjeneste til borgerne. Der bør være en oplysningstjeneste til borgerne om cybersikkerhed. Denne opgave kunne løses af Digitaliseringsstyrelsen, som har de borgernære systemer.

5) Mulighed for at sælge tillægsbeskyttelse til private abonnenter

Danmark er blandt de mest digitaliserede lande, og opretholdelsen af borgernes tillid og tryghed i det digitale rum er afgørende for udnyttelse af de digitale muligheder. Der er i Danmark relativt få teleoperatører, som forbinder Danmark med udlandet. Teleoperatører bør få mulighed for at sælge en tillægsbeskyttelse til private abonnenter, som - på samme vis som DNS-tjenesten - forhindrer adgang til cyberkriminel infrastruktur baseret på viden som teleoperatørerne modtager fra Forsvarets Efterretningstjeneste.

6) Skærpet kontrol af Center for Cybersikkerhed

Det siger sig selv, at med en yderligere opgaver og dermed yderligere adgang til- og indsamling af - følsomme data, skal der ske en skærpet kontrol af Center for Cybersikkerheds håndtering af data. Der skal være en løbende og uafhængig kontrol af, at alle de data (og ikke kun persondata som tilfældet er i dag) som centeret behandler og deler, sker i overensstemmelse med lovgivningen og forsvarsministeriets retningslinjer.

Den skærpede kontrol af Center for Cybersikkerhed bør overlades til Tilsynet med Efterretningstjenesterne, der i dag kun kontrollerer dele af Center for Cybersikkerheds virke. Samtidig bør der dog indføres en bredere parlamentarisk kontrol med overvågningen ud fra samfundsmæssige betragtninger om sikkerhed og retssikkerhed ved eksempelvis at behandle Tilsynets årlige redegørelse i Retsudvalget, og dermed på årlig basis vurdere den retspolitiske balance i overvågningen.

Anbefalingerne er udarbejdet af medlemmer af DANSK IT's fagråd for informationssikkerhed