Pressemeddelelse 23. september 2017

Seks forslag, der kan styrke Danmarks cybersikkerhed

Forsvarets Efterretningstjeneste (FE) og Center for Cybersikkerhed bør stille sine ressourcer til rådighed for virksomheder og myndigheder, så cyberangreb kan stoppes før skaden er sket, lyder fra DANSK IT, der er klar med seks forslag, der kan give cybersikkerheden i Danmark et markant løft.

En liste over domæner relateret til cyberkriminalitet, en godkendelsesordning af virksomheder, der er specialiserede i at imødegå angreb og en oplysningstjeneste til borgerne om cybersikkerhed, er blandt de initiativer som DANSK IT ønsker indarbejdet i det kommende forsvarsforlig.

- Tiden er inde til, at vi som samfund går langt mere offensivt til værks for at beskytte os mod cyberangreb, som rammer myndigheder, virksomheder og borgere stadig hårdere. Og er det oplagt at kigge på om ikke FE og Center for Cybersikkerhed i højere grad kan stille deres ressourcer til rådighed for myndigheder og virksomheder, siger Rikke Hvilshøj, adm. direktør, DANSK IT.

DANSK IT hæfter sig blandt andet ved, at Center for Cybersikkerhed kan se, om et angreb har fundet sted, og komme med råd og vejledning, men centret stiller ikke sine kapaciteter til rådighed for myndighed og virksomheder, så de aktivt kan imødegå cyberangreb.

- Når vi anbefaler, at Center for Cybersikkerhed skal have flere opgaver, er det selvfølgelig under forudsætning af, at Center for Cybersikkerhed kommer under skærpet kontrol for sin håndtering af data, påpeger Rikke Hvilshøj.

De seks anbefalinger til en styrkelse af Danmarks cybersikkerhed er:

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

For mere information kontakt venligst
Rikke Hvilshøj, adm. direktør, DANSK IT, mobil 41 25 00 02, e-mail rh@dit.dk

Morten Larsen, pressechef, DANSK IT, mobil 61 20 74 75, mail ml@dit.dk

Om DANSK IT
DANSK IT er en non-profit interesseorganisation stiftet i 1958. DANSK IT arbejder for at fremme og understøtte it, hvor dette skaber værdi for samfundet og den enkelte. At samle, styrke og udvikle it-brugere og it-professionelles kompetencer og faglighed, og på et uafhængigt grundlag varetage samfundets og medlemmernes it-interesser. Mere information findes på www.dit.dk