**Forslag til et fælles cybersikkerhedsråd**

**Problemfelt**

Det er nødvendigt at styrke det brede samarbejde omkring cybersikkerhed i Danmark ved at skabe et mere sammenhængende offentligt-privat samarbejde. I dette samarbejde kan myndigheder, erhverv, forskningsverden og borgere dele viden, koordinere initiativer og gennemføre kampagner og øvelser, så sikkerheden omkring vores kritiske infrastruktur kan løftes, og dermed gøres samfundet mere robust overfor cyberangreb.

Vores cybersikkerhed er for vigtig til, at vi kan tillade os at arbejde i siloer og ikke bruge hinandens viden.

**Baggrund**

Med den omfattende digitalisering af både erhvervslivet og den offentlige sektor stiger risikoen for og konsekvensen ved cyberkriminalitet. For eksempel vurderer Dansk Erhverv, at 3 ud af 4 danske virksomheder blev ramt eller forsøgt ramt af cyberangreb i 2017. Samtidig bliver de it-kriminelle hele tiden dygtigere og bedre organiseret. Endvidere fastslår en nylig undersøgelse fra Deloitte, at Danmark er det fjerde mest udsatte land i verden, hvad angår cyberkriminalitet og cyberangreb.

Den offentlige organisering af cybersikkerhedsområdet alt for fragmenteret og siloopdelt. Der nedsat en række branchespecifikke råd og overvågningstjenester, men de opererer uafhængigt af hinanden og med manglende koordination.

Center for Cybersikkerhed har det overordnede ansvar for at understøtte et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur, som samfundsvigtige funktioner er afhængige af. Det er det Centeret selv kalder for Netsikkerhedstjenesten.

Centeret har sin berettigelse, og deres placering i Forsvaret giver dem adgang til gode efterretninger. Ansvaret for Netsikkerhedstjenesten bør fortsat være forankret hos CfCS

Men CfCS militære placering gør omvendt også, at mange af deres efterretninger ikke kan deles med de danske civile myndigheder, virksomheder og borgere. Samtidig er omdrejningspunktet for Netsikkerhedstjenestens arbejde ikke almindelige cybertrusler og simple angreb men derimod kun de mest avancerede angreb, der oftest udføres af statsstøttede aktører, eller cyberangreb, der i øvrigt kan påvirke det danske samfund i væsentlig grad.

Centeret har derfor svært ved at varetage rollen med at oplyse, vejlede og rådgive danske myndigheder, virksomheder og borgere om it-sikkerhed og fungere som nationalt koordinations- og kompetencecenter på cybersikkerhedsområdet.

Det er denne rolle, vi ønsker varetaget af et fælles offentligt-privat Cybersikkerhedsråd.

**Løsning**

Vi ønsker at der etableres et offentligt-privat Cybersikkerhedsråd med repræsentanter fra myndigheder, erhverv, forskningsverdenen og borgere.

Cybersikkerhedsrådet skal have til opgave at:

* Koordinere indsamling af viden om trusler og hændelse vedrørende brud på cybersikkerhed.
* Videndeling og distribution af information om trusler og hændelser til alle relevante parter.
* Varsle ved alvorligt forestående angreb - ”awareness og early warning”.
* Udarbejde skabeloner for cyberøvelser og eventuel bistå organisationer med gennemførelse af dem.
* Varetage nationale informationskampagner omkring cybersikkerhed til både borgere og virksomheder.
* Koordinere dansk deltagelse i EU’s ”Cyber Security Month”, der gennemføres årligt i hele oktober måned.
* Vejlede, rådgive og støtte regeringen, embedsværket, de politiske partier og private virksomheder m.fl. på et strategisk niveau.
* Koordinere samarbejdet mellem de mange aktører der i dag arbejder for at styrke den danske cybersikkerhed – både offentlige, private, forskningsverden og interesseorganisationer.

Hvem bringer viden til rådet?

* Rådet indsamler viden fra eksisterende overvågningstjenester, bl.a. CERT’erne, CfCS, forskningsnettet mv.
* Forskningsinstitutioner bidrager med viden fra forskningsaktiviteter.
* Erhvervslivet skal have mulighed for at dele viden om hændelser anonymt og data skal fødes tilbage igen i aggregeret form.

Hvem skal sidde i rådet?

* Cybersikkerhedsrådet skal bestå af repræsentanter fra de vigtigste myndigheder brancheorganisationer, interesseorganisationer samt forskningsverdenen og borgerne.
* Rådet bør forankres i en civil myndighed, med et klart mandat.
* Formandskabet varetages på skift mellem en offentlig og privat instans.

Rådets arbejde skal støttes af et sekretariat forankret i en civil myndighed, der får til opgave at:

* Betjene rådet og iværksætte vedtagne initiativer for at understøtte den aktive vidensdeling.
* Sikre at den indsamlede viden bliver kommunikeret effektivt til borgere og virksomheder.
* Udarbejde vejledninger til og informere borgere om cybersikkerhed.

**Økonomi**

Sekretariatet skal bemandes med 10 medarbejdere.

Der skal sikres midler til løbende kampagner, indsatser og øvelser.

Der bør endvidere afsættes midler til at rådet kan iværksætte forskning der skal tilvejebringe evidens på området.

Der må endvidere afsættes midler til udvikling af digitale løsninger der understøtter de anonyme indberetninger af hændelser og systematiseret videndeling til relevante parter.