AFTALE OM ET STYRKET CYBERFORSVAR

24. juni 2021

Der er mellem regeringen og Venstre, Dansk Folkeparti, Radikale Venstre, Det Konservative Folkeparti og Liberal Alliance indgået en aftale om styrkelse af Danmarks cyberforsvar. Aftalen udmønter cyberreserven på 500 mio. kr. fra aftalen på forsvarsområdet 2018-2023, *jf. bilag 1*.

Cybertruslen mod Danmark er på et markant og vedvarende niveau. Vores virksomheder, myndigheder og borgere er dagligt udsat for cyberangreb fra kriminelle, stater og organisationer. Spionage, infiltrering af vores digitale netværk og mulige fjendtlige angreb er daglige trusler. Det danske samfund er gennemdigitaliseret. Vi er et oplagt mål for cyberangreb, der kan have store konsekvenser for Danmarks stabilitet, økonomi og levevis.

Partierne er enige om, at truslens alvor og udvikling kræver, at vi tager konkrete skridt for at styrke vores cyberforsvar. Derfor afsættes i årene 2021-2023 midler for at forbedre vores varslings- og forsvarssystemer og til øget rådgivning og støtte. Der er enighed om at styrke vores responsmuligheder, sanktioner samt kriseberedskab, herunder med prioritet til samarbejde med NATO og EU.

Forsvarets systemer har behov for øget beskyttelse, herunder ved styrket beskyttelse af forsvarets følsomme data samt af udsatte operative systemer. Samtidig skal forsvarets evne til at udføre militære cyberoperationer styrkes yderligere.

Partierne noterer sig, at cyberværnepligten har været en succes, og at ordningen gøres permanent som led i en bredere styrkelse af uddannelse og forskning indenfor cyberområdet. Herved øges andelen af cybertalenter og –kompetencer i Danmark til gavn for både virksomheder og myndigheder. Der etableres samtidig et cyberhjemmeværn, der kan styrke beredskabet og trække på borgere og civilsamfundets it-kompetencer ved etablering af et kompetent og stærkt cybernetværk.

Det er partiernes ønske, at cyberkompetencer udvikles i hele Danmark. Partierne prioriterer, at der er uddannelsesmuligheder og cyberarbejdspladser både i det østlige og vestlige Danmark, ligesom varslings- og forsvarssystemer og rådgivningsteams tilbydes til hele rigsfælleskabet. Dette samtidigt med fokus på, at sikre et højt fagligt niveau.

Partierne er særligt opmærksomme på, at investeringerne skal have både civil og forsvarsmæssig nytte. De noterer sig, at der foregår et vigtigt arbejde for at styrke små og mellemstore virksomheders cybersikkerhed gennem en række øvrige indsatser, herunder via den nationale cyberstrategi. Center for Cybersikkerhed (CFCS) skal yderligere styrke det gensidige samarbejde og partnerskab med den private sektors brancheforeninger, virksomheder og faglige fora, ikke mindst på energi- og teleområdet.

For at kunne evaluere og styrke CFCS' virke med særligt fokus på at øge den samlede indsats over for den private sektor igangsættes en analyse af CFCS' forankring under FE, herunder fordele og ulemper ved at lægge en del af virksomhedsindsatsen i en civil enhed på Forsvarsministeriets område. Analysen skal foreligge inden sommeren 2022, idet en delrapport om rådgivning og uddannelse skal foreligge i efteråret 2021.

Partierne noterer sig, at cyberforsvaret vil skulle styrkes yderligere i næste forsvarsforlig for at kunne følge med udviklingen, herunder knytte erhvervslivet og forsvarsområdet mere sammen gennem videndeling og uddannelse, tilgængelig rådgivning og et kompetent cyberhjemmeværn mv.

BILAG 1 – INITIATIVER TIL ET STYRKET CYBERFORSVAR

Implementeringen af aftalen om styrket cyberforsvar medfører investeringer for 500 mio. kr. i 2021-2023 og afledte driftsudgifter for 220 mio. kr. årligt fra og med 2024.

Der er tale om estimerede udgifter, *jf. tabel 1*, hvor der kan være behov for mindre justeringer mellem initiativerne. Større prioriteringer skal ske under inddragelse af forligskredsen

Forsvarsforligskredsen vil løbende blive orienteret om aftalens udmøntning.

Tabel 1. Initiativer til et styrket forsvar.

Initiativ	**Forligsperioden** *(mio. kr. i 2021-2023, afrundede beløb)*
1. Datamonitorering og varsling	175
Avanceret datahåndtering, styrket IT-understøttelse af cyberanalyse, analytisk kapacitet ift. cyber crime og spionage, (Host Analyse) Platform til detektion af avancerede cyberangreb og Phishingmailanalyse	
2. Cyberhjemmeværn	5
3. Cyberindsatshold	10
4. Teknisk bolværk	100
Fælles statslig DNS-tjeneste, GovShield (central datalogning i staten), Hybrid Defence Cloud Security, Configuration Management Database, Cross Domain Solutions, redundante forbindelser til kritiske installationer, honeypots og sinkholes, akkreditering og sweeping og sags- og dokumenthåndtering på klassificerede systemer	
5. Rådgivning og decentral understøttelse	100
Situationsbestemt rådgivning til statslige myndigheder, udbygning af samarbejdet mellem Center for Cybersikkerhed og de samfundskritiske sektorer, udvidet kapacitet i telesektion (5G), CFCS understøttelse af statslig hotline, CFCS styrkelse af cybersikkerhed på ambassader og styrket kapacitet for sikkerhedstekniske undersøgelser mhp. at opdage sårbarhed	
6. Uddannelse, forskning og videndeling	50
Cyberværnepligtige, styrkelse af uddannelse og forskning ved Forsvarsakademiet og Syddansk Universitet samt udbygning af forskning og uddannelse, styrkelse af den lokale cybersikkerhed, styrkelse af samfundets it-beredskab (øvelser), platform for videndeling af malware og Cybersikkerhedsråd, herunder reserve på 20 mio. kr. til opfølgning på delrapport om CFCS' virke	
7. Offensive værktøjer	40
Styrket cyberkapacitet til potentiel brug for indsættelser, planlægning, drift og udvikling af cyberspaceoperationer i Forsvarsstaben, styrket analytisk attribueringskapacitet, detektion af påvirkningstrusler på sociale medier og internationale cybersikkerhedsrelaterede stillinger	
8. Cyberforsvar i Rigsfællesskabet	20
Styrket indsats på cyberområdet frem til og med 2023, *i alt mio. kr.*	500