FOLKETINGET

Folketingstidende
Tillæg A

Til lovforslag nr. **L 215** Folketinget 2018-19

Skriftlig fremsættelse (27. marts 2019)

Forsvarsministeren (Claus Hjort Frederiksen):

Herved tillader jeg mig for Folketinget at fremsætte:

Forslag til lov om ændring af lov om Center for Cybersikkerhed (Initiativer til styrkelse af cybersikkerheden)

(Lovforslag nr. L 215)

Regeringen har den 27. februar 2019 indgået en politisk aftale med Socialdemokratiet, Dansk Folkeparti og Radikale Venstre om lovforslaget. Aftalen lyder således:

"I forlængelse af forsvarsforlig 2018-2023, der blandt andet indebærer en væsentlig styrkelse af beskyttelsen af Danmark mod cyberangreb, har regeringen (Venstre, Liberal Alliance og Det Konservative Folkeparti), Socialdemokratiet, Dansk Folkeparti og Radikale Venstre indgået aftale om lovforslag om ændring af den gældende lov om Center for Cybersikkerhed. Med lovforslaget vil der blive gennemført en række initiativer til yderligere styrkelse af cybersikkerheden.

Aftaleparterne noterer sig, at Forsvarets Efterretningstjeneste vurderer, at Danmark står over for en meget høj cybertrussel, særligt fra fremmede stater. Nogle stater forsøger vedholdende at udføre cyberspionage mod danske myndigheder og virksomheder, og det er stadig sværere at opdage deres aktiviteter. Visse stater har desuden vist vilje til også at udføre mere offensive cyberangreb, der f.eks. har til formål at påvirke meningsdannelsen i andre lande. Samtidig bliver avancerede hackerværktøjer også tilgængelige for flere ikke-statslige aktører. Danske myndigheder og virksomheder er i et vedvarende kapløb med fremmede stater, hackergrupper og individer, der hele tiden udvikler nye måder, hvormed de kan udnytte cyberangreb til at nå deres politiske eller økonomiske mål. Samtidig vurderer Forsvarets Efterretningstjeneste, at cyberangreb kan påvirke samfundsvigtige ydelser og befolkningens tillid til digitaliseringen, og at cybertruslen mod offentlige myndigheder, virksomheder og borgere i Danmark er blevet et grundvilkår, der fortsat vil gøre sig gældende på langt sigt.

Den hastige og alvorlige udvikling i trusselsbilledet betyder, at der er behov for at tilpasse lovgivningen, så Center for Cybersikkerheds muligheder for at imødegå cyberangreb mod den kritiske infrastruktur og vigtige samfundsfunktioner fremadrettet modsvarer truslerne. Samtidig betyder den teknologiske udvikling, at der er behov for at kunne anvende nye værktøjer til at modvirke cyberangreb.

Lovforslaget indebærer blandt andet, at gebyret for tilslutning til Center for Cybersikkerheds særlige netsikkerhedstjeneste helt fjernes, så det fremover vil være gratis for myndigheder og samfundsvigtige virksomheder at blive tilsluttet netsikkerhedstjenesten. I helt særlige tilfælde vil visse myndigheder og virksomheder, der er en del af Danmarks kritiske infrastruktur, desuden kunne få påbud om tilslutning til netsikkerhedstjenesten. Herudover får Center for Cybersikkerhed mulighed for – efter aftale med den enkelte myndighed eller virksomhed – at levere et aktivt cyberforsvar, hvor cyberangreb kan stoppes, inden de når at anrette skade.

En yderligere nyskabelse er, at Center for Cybersikkerheds nuværende monitorering af internetforbindelserne kan suppleres af sikkerhedssoftware, der installeres på f.eks. pc'ere og servere. Dermed får centeret mulighed for at opdage cyberangreb langt tidligere, også selv om angrebsværktøjerne er krypterede. Desuden vil forebyggelsen af cyberangreb blive styrket ved at give Center for Cybersikkerhed mulighed for at gennemføre forebyggende sikkerhedstekniske undersøgelser, hvor centeret – efter aftale med den enkelte myndighed eller virksomhed – søger at identificere sårbarheder og vurdere robustheden af it-systemer, således at sårbarhederne ikke først opdages, når de udnyttes af en ondsindet hacker.

Aftaleparterne hæfter sig ved, at tiltagene i lovforslaget – herunder den forventede forøgelse af antallet af virksomheder, der er tilsluttet Center for Cybersikkerheds netsikkerhedstjeneste – hverken kan eller skal erstatte de sikkerhedsløsninger, som udbydes på det private marked. Center for Cybersikkerheds ydelser giver et ekstra lag af sikkerhed, men myndigheder og virksomheder vil fortsat have behov for kommercielle sikkerhedsløsninger. Det er aftaleparternes forventning, at lovforslaget vil bidrage til at øge fokus på alvoren af cybertruslen – og dermed også styrke det private marked for it-sikkerhedsløsninger.

På baggrund af høringen over lovforslaget er aftaleparterne enige om, at der foretages visse tilpasninger af lovforslaget.

Muligheden for at give påbud om tilslutning ændres, således at der ikke kan gives påbud om installation af sikkerhedssoftware. Center for Cybersikkerheds afrapportering efter sikkerhedstekniske undersøgelser vil endvidere være anonymiserede, og oplysninger om identiteten på medarbejdere, der f.eks. har begået et sikkerhedsbrud, vil ikke kunne

Forsvarsmin., j.nr. 2019/001470

udleveres fra Center for Cybersikkerhed. Endvidere imødekommes et ønske fra bl.a. byretspræsidenterne og Dommerforeningen om, at der ikke skal medvirke indgrebsadvokater i editionssager.

I tillæg til lovforslaget er aftalepartnerne enige om, at der oprettes et offentligt-privat cybersikkerhedsråd. Formålet med rådet er at kvalificere myndighedernes og virksomhedernes arbejde og styrke det digitale demokrati, herunder udbredelse af viden om, og forståelse for, de trusler og muligheder, som digitaliseringen og den nye teknologi medfører. Rådet vil have deltagelse af Digitaliseringsstyrelsen, Center for Cybersikkerhed og repræsentanter med særlig it-sikkerhedsmæssig kompetence fra den private sektor, brancheorganisationer, forskningsverdenen og forbrugersiden. Rådet vil have delt offentligt-privat formandskab, og der vil blive afsat midler fra det indeværende forsvarsforlig til en sekretariatsfunktion for rådet."

Det foreslås, at lovforslaget træder i kraft den 1. juli 2019.

Idet jeg i øvrigt henviser til lovforslaget og de ledsagende bemærkninger, skal jeg hermed anbefale lovforslaget til det Høje Tings velvillige behandling.