FORSVARSMINISTERIET

Folketingets Forsvarsudvalg
Christiansborg

Dato: 17. april 2019

Enhed: JSN
Sagsnr.: 2019/002226
Dok.nr.: 897455
Bilag: Ingen

FORSVARSMINISTEREN
Holmens Kanal 9
1060 København K

Tlf.: 728 10000
Fax: 728 10300
E-mail: fmn@fmn.dk
www.fmn.dk

EAN: 5798000201200
CVR: 25 77 56 35

Folketingets Forsvarsudvalg har den 4. april 2019 stillet følgende spørgsmål nr. 11 vedrørende L 215, som hermed besvares. Spørgsmålet er stillet efter ønske fra Holger K. Nielsen (SF) og Eva Flyvholm (EL)

Spørgsmål nr. 11:
"Ministeren bedes uddybe, hvilke typer virksomheder der kan tænkes at blive pålagt installation af teknologi, der giver Center for Cybersikkerhed mulighed for at se ind virksomhedens interne it netværk, såfremt virksomhederne ikke frivilligt går med til, at Center for Cybersikkerhed overvåger dem og udsætter dem for cybersikkerhedstest."

Svar:
Center for Cybersikkerhed vil ikke kunne pålægge en virksomhed at installere teknologi, der vil give centeret mulighed for at se ind i virksomhedens interne it-netværk og servere.

Med lovforslaget foreslås det, at Center for Cybersikkerhed får mulighed for at foretage monitorering ved hjælp af to forskellige metoder.

Den ene metode – ekstern monitorering – som centeret benytter sig af i dag, indebærer, at en alarmenhed opsættes hos den enkelte myndighed eller virksomhed, hvorefter alarmenheden monitorerer ind- og udgående netværkskommunikation, herunder internetkommunikation. Alarmenheden kopierer den ind- og udgående trafik, hvorefter trafikken ved hjælp af automatiserede analyseværktøjer undersøges for eksempelvis skadelig kode. Når den automatiserede undersøgelse udløser en alarm, håndteres denne efterfølgende af medarbejdere i centerets netsikkerhedstjeneste.

Den anden metode – intern monitorering – indebærer, at Center for Cybersikkerhed vil få mulighed for at monitorere aktiviteter på lokale enheder ved hjælp af sikkerhedssoftware, der installeres lokalt på de enkelte enheder, som anvendes af myndigheden eller virksomheden. Disse enheder vil f.eks. kunne være pc'ere, servere, smartphones og tablets. Denne metode skal imødegå udviklingen, hvorefter mere og mere datatrafik krypteres, hvilket gør det vanskeligere for centeret at opdage sikkerhedshændelser ved hjælp af den eksterne monitorering.

Forsvarsministeriet noterede sig i forbindelse med den offentlige høring, at en lang række høringsparter gav udtryk for en særlig bekymring over, at den påbudsordning, der indgår i lovforslaget, også omfattede den interne monitorering ved hjælp af sikkerhedssoftware. Lovforslaget er på den baggrund blevet tilpasset, således at påbudsmuligheden alene vil omfatte den eksterne monitorering ved hjælp af alarmenheder. Center for Cybersikkerhed vil således ikke kunne pålægge virksomheder at installere sikkerhedssoftware.

Derudover indeholder lovforslaget et forslag om at give Center for Cybersikkerhed mulighed for at tilbyde myndigheder og virksomheder at få foretaget en forebyggende sikkerhedsteknisk undersøgelse. Den sikkerhedstekniske undersøgelse har til formål at afdække sårbarheder i myndighedens eller virksomhedens systemer og netværk, således at Center for Cybersikkerhed kan yde rådgivning om, hvilke konkrete tiltag, der kan gennemføres for at styrke beskyttelsen af den digitale infrastruktur. Det vil være helt frivilligt for myndigheder og virksomheder, om de ønsker at benytte sig af tilbuddet om en sikkerhedsteknisk undersøgelse.

Med venlig hilsen

Claus Hjort Frederiksen