FORSVARSMINISTERIET
DANISH MINISTRY OF DEFENCE

Folketingets Retsudvalg
Christiansborg

FORSVARSMINISTEREN
4. november 2014

Folketingets Retsudvalg har den 8. oktober 2014 stillet følgende spørgsmål nr. 5 til forsvarsministeren, som hermed besvares. Spørgsmålet er stillet efter ønske fra Pernille Skipper (EL).

Spørgsmål nr. 5:
"Ministeren bedes redegøre for, om Center for Cybersikkerhed i sin undersøgelse af det såkaldte hackerangreb mod CSC's mainframe fandt, at angrebet bl.a. blev muliggjort pga. manglende installation af et patch eller en zero day, samt hvorvidt konklusionerne bygger på en selvstændig undersøgelse eller oplysninger leveret af CSC, IBM eller andre. Der henvises bl.a. til http://www.version2.dk/artikel/csc-vidne-i-hackersag-zero-day-saarbarheder-havdeen-patch-68778."

Svar:
Center for Cybersikkerhed er anmodet om en udtalelse til brug for Forsvarsministeriets besvarelse. Center for Cybersikkerhed har i den anledning oplyst:

"Center for Cybersikkerhed og PET har udarbejdet to rapporter om kompromitteringen af et fællesoffentligt it-system hos it-leverandøren CSC. Formålet med rapporterne og de bagvedliggende it-sikkerhedstekniske undersøgelser har været at belyse den konkrete kompromittering samt at vurdere det aktuelle sikkerhedsniveau hos CSC.

De it-sikkerhedstekniske undersøgelser har vist, at visse sikkerhedsrettelser (patches), som blev udsendt af CSC's leverandør, IBM, først blev implementeret med en vis forsinkelse. Center for Cybersikkerhed og PET vurderer imidlertid, at denne forsinkelse ikke har haft betydning i forhold til den konkrete kompromittering, da kompromitteringen skete forud for IBM's udsendelse af disse patches. Kompromitteringen skete således ved at udnytte hidtil ukendte sårbarheder (zero-day sårbarheder).

HOLMENS KANAL 42
1060 KØBENHAVN K
TELEFON: 72 81 00 00
TELEFAX: 72 81 03 00
MAIL: FMN@FMN.DK
WEB: www.FMN.DK
CVR: 25-77-56-35
EAN: 5798000201200

Hverken Center for Cybersikkerhed eller PET har haft direkte adgang til at undersøge CSC's systemer og sikkerhedsopsætning. Det skyldes primært, at det alene er systemejeren, der har den indsigt i it-systemet, som gør det muligt at uddrage relevante informationer uden at risikere driftsforstyrrelser. CSC's systemer betjener en række forskellige myndigheder, og driftsforstyrrelser ville kunne få betydelige samfundsmæssige konsekvenser.

Center for Cybersikkerhed og PET har imidlertid været i løbende dialog med både Københavns Politi – som har varetaget den strafferetlige efterforskning i sagen – og CSC, og i forlængelse heraf har Center for Cybersikkerhed og PET modtaget og analyseret store mængder data. Der er endvidere inddraget data fra en række andre kilder, herunder en rapport fra et svensk konsulentfirma, som foretog en detaljeret undersøgelse af kompromitteringen hos CSC, og data fra computere, der tilhører de personer, som efterfølgende er blevet tiltalt i sagen.

Hverken data fra CSC eller fra andre kilder har givet Center for Cybersikkerhed og PET anledning til at betvivle, at CSC har stillet de tilgængelige data til rådighed for de it-sikkerhedstekniske undersøgelser.

Derudover har konsulentvirksomheden PwC efterfølgende foretaget en vurdering af informationssikkerheden hos CSC, herunder en vurdering af de konkrete initiativer, som CSC har planlagt (blandt andet på baggrund af Center for Cybersikkerheds indledende undersøgelser). PwC har dog ikke løst opgaver i forbindelse med de it-sikkerhedstekniske undersøgelser af kompromitteringen."

Med venlig hilsen

Nicolai Wammen