FORSVARSMINISTERIET
MINISTRY OF DEFENCE

DET TALTE ORD GÆLDER

Taleseddel til FOU (alm. del) samrådsspørgsmål T & U

Hackerangrebet WannaCry og
Danmarks beskyttelse mod hackerangreb

FOU samrådsspørgsmål T
Ministeren bedes redegøre for det seneste store hackerangreb mod Danmark, der begyndte fredag den 12. maj 2017.

FOU samrådsspørgsmål U
Mener forsvarsministeren, at vi i Danmark er tilstrækkeligt beskyttet mod hackerangreb? Her bedes ministeren redegøre for beskyttelsesniveauet i den offentlige sektor, i den private sektor og for borgerne.

Begge spørgsmål er stillet efter ønske fra Ida Auken (RV).

Besvarelse
Med udvalgets tilslutning vil jeg besvare de to spørgsmål samtidig. Jeg tænker at holde mig til spørgsmålenes alfabetiske orden og altså begynde med udvalgsspørgsmål T om hackerangrebet, der blev erkendt den 12. maj, altså det angreb, der er kendt som WannaCry.

Fredag den 12. maj blev der observeret en malwarekampagne, som var målrettet en kendt sårbarhed i en række styresystemer fra Microsoft. Malwaren indeholder en komponent, en såkaldt crypto-locker, der går under navnet WannaCry, og som går ind og krypterer udvalgte filtyper og sletter originalerne, hvorefter ofret automatisk opkræves en løsesum for at dekryptere filerne igen. Malware med disse egenskaber kendes også som ransomware.

I den første bølge af ransomware-kampagnen blev det observeret, at dem, der har designet malwaren af en eller anden grund havde indbygget en form for nødstop – en såkaldt "kill switch". Malwaren indeholdt således et domæne – altså en adresse på internettet – som malwaren kontaktede i forbindelse med infektionen. Hvis malwaren kunne kontakte domænet, så ville krypteringen ikke blive udført.

Domænet, som viste sig ikke at være taget i brug af andre, blev opkøbt og registreret i løbet af fredagen af en britisk it-sikkerhedsspecialist. Det betød, at malwaren nu kunne kontakte domænet og således ikke længere krypterede indholdet af de inficerede computere. Dermed blev den centrale del af angrebet de-facto standset.

Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste gik tidligt i forløbet i gang med at skaffe overblik over situationen med et særligt fokus på eventuelle danske ofre. I løbet af aftenen fredag den 12. maj var Center for Cybersikkerhed i kontakt med andre myndigheder og en større kreds af centrale danske internetudbydere. På det tidspunkt stod det klart, at der ikke var indikationer på, at danske statslige myndigheder eller samfundskritiske virksomheder var blevet ramt.

I løbet af weekenden blev situationen fulgt nøje, og der blev bl.a. udarbejdet og offentliggjort en trusselsvurdering om WannaCry, ligesom der blev udsendt et varsel til en kreds af myndigheder, virksomheder og interessenter. Varslet såvel som trusselsvurderingen baserede sig bl.a. på information fra det netværk af sensorer, som Center for Cybersikkerhed driver, og hvor

det kunne observeres, at der i løbet af weekenden skete et større antal scanninger efter sårbarheder.

Der er fortsat ikke erkendt eksempler på danske statslige myndigheder eller samfundskritiske funktioner, der er blevet sat ud af drift på grund af kryptering som følge af WannaCry-kampagnen. Om vi i Danmark har et højere it-sikkerhedsniveau end andre lande, eller om vi blot har været heldige, er et uafklaret spørgsmål.

Center for Cybersikkerhed har gennem længere tid haft fokus på behovet for, at sårbare systemer opdateres, og at systemer, der ikke længere kan opdateres, udfases eller afsondres fra internettet.

Således advarede Center for Cybersikkerhed den 31. marts 2017 mod risikoen for udnyttelse af sårbare og ikke-længere opdaterbare Microsoftsystemer, og den 18. april 2017 blev kunder og interessenter specifikt varslet om nødvendigheden af at opdatere systemer mod en alvorlig pakke af sårbarheder, som bl.a. indeholdt den sårbarhed, der blev udnyttet af WannaCry.

Tilbage står dog, at denne type angreb finder sted hele tiden, og at dette angreb næppe er det sidste. Et af de bedste midler til at forebygge angrebene er dog at holde sine it-systemer opdateret med de nyeste sikkerhedsopdateringer samt kun at anvende it-produkter, som fortsat modtager opdateringer fra leverandøren.

Samrådsspørgsmål U:

WannaCry-angrebet er et godt eksempel på de stigende cybertrusler, vi oplever, og det udgør jo derfor også et naturligt bagtæppe for at drøfte samrådsspørgsmål U om vores bredere beskyttelse mod cybertruslerne, både i den offentlige og den private sektor og for borgerne.

Vores samfund bliver stadigt mere afhængigt af, at de digitale systemer virker, som de skal. Det rejser en række udfordringer for alle med et ansvar for væsentlige funktioner i samfundet, både i private virksomheder og i offentlige myndigheder. Det gælder selvfølgelig ikke mindst i forhold til at beskytte systemerne mod hackerangreb.

I de seneste år har der været en væsentlig udvikling i beskyttelsesniveauet imod hackerangreb. Området er løbende blevet styrket med både ressourcer og med ny lovgivning.

Med etableringen af Center for Cybersikkerhed i 2012 og gennemførelsen af den nationale strategi for cyber og informationssikkerhed er der sket en styrkelse af vidensniveauet og af arbejdet med cyber- og informationssikkerhed i både staten og i virksomheder og på tværs af samfundet.

Samtidig er der arbejdet systematisk med at løfte arbejdet med styring af informationssikkerhed i staten efter standarden ISO 27001 med vejledning og styringsværktøjer, herunder har informationssikkerhed siden 2015 indgået i Statens It-projektråds vurderinger.

Med den seneste fællesoffentlige Digitaliseringsstrategi fra 2016 er det desuden aftalt, at regionerne og kommunerne også styrker deres arbejde med informationssikkerhed.

Vi skal vedholdende arbejde på at opretholde et passende beskyttelsesniveau. Center for Cybersikkerhed vurderer, at truslen fra cyberspionage og cyberkriminalitet mod danske myndigheder og virksomheder er meget høj. Og truslerne udvikler sig hastigt, hvilket stiller store krav til, at vi hele tiden følger med.

Vi ser angreb rettet mod vores viden og ideer i form af cyberspionage, mod vores økonomi i form af cyberkriminalitet og potentielt også mod vores samfundsmodel og demokratiske system i form af informations- og påvirkningskampagner og mod samfundsvigtige funktioner i form af ødelæggende hackerangreb, der vil kunne lægge vitale funktioner i vores samfund ned.

Det er et trusselsbillede, som både offentlige og private ledere er nødt til at tage alvorligt og sætte sig ind i. Det er helt centralt, at der kan være tillid til, at de funktioner, der er særligt vigtige for vores samfund, er tilstrækkeligt sikre.

Derfor skal der være et særligt fokus på digital sikkerhed i de sektorer, som understøtter samfundsvigtige funktioner. Og det er jo dem, der arbejder med et område til daglig, der kender det bedst og også bedst ved, hvordan man beskytter det i en krisesituation.

Derfor har vi i Danmark det, vi kalder sektoransvarsprincippet, hvor det er myndighederne med det daglige ansvar for den enkelte sektor, der skal sikre, at der også kan opretholdes væsentlige funktioner i en krisesituation, herunder i forbindelse med et cyberangreb. Myndigheder og virksomheder skal altså løbende tilpasse sig og sikre, at de har et tilstrækkeligt niveau for informations- og cybersikkerhed. Det gælder også i forhold til, at brugerne af private og offentlige tjenester kender til sikker internetadfærd.

For at sikre rettidig og relevant information om truslerne udgiver Center for Cybersikkerhed løbende specifikke trusselsvurderinger i tillæg til sin årlige vurdering af cybertruslen imod Danmark.

Der kommer til at ske mere på cyberområdet i det kommende år: I maj 2018 skal EU-direktivet om net- og informationssikkerhed, kendt som NIS-direktivet, være implementeret i dansk ret. Det betyder, at der fremadrettet vil blive stillet krav til informationssikkerheden i en række særligt samfundsvigtige sektorer – såsom energi, finans, transport og sundhed. De berørte virksomheder vil fremadrettet skulle leve op til en række sikkerhedskrav, herunder at der gennemføres relevante sikkerhedsvurderinger med udgangspunkt i det til enhver tid gældende trusselbillede, ligesom der også indføres en underretningsforpligtelse ved sikkerhedshændelser.

Jeg forventer også, at en styrkelse af indsatsen på cyberområdet bliver en del af udspillet til et kommende forsvarsforlig, og jeg har noteret mig, at der ser ud til at være bred tilslutning hertil.

Samlet set er vi godt på vej. Men et beskyttelsesniveau, som var passende i går, vil ikke nødvendig være tilstrækkeligt i morgen. I sidste ende er det op

til den, der har ansvaret for en væsentlig samfundsfunktion, at vurdere, om beskyttelsesniveauet af denne funktion til enhver tid er tilstrækkeligt.

Det er derfor nødvendigt løbende at forholde sig til trusselsbilledet og på den baggrund justere informationssikkerheden og forbedre den, når det er nødvendigt.

Det ligger mig naturligvis også på sinde, at der er et passende sikkerhedsniveau i alle offentlige myndigheder såvel som hos private virksomheder og også hos borgerne. I den forbindelse er udbredelse af viden om sikkerhedsbrud vigtig.

Tak.