Spm. nr. S 4428

Til justitsministeren (21/8 03) af:
Line Barfod (EL):
»Vil ministeren kommentere artiklen i Politiken 21. august 2003 s. 15 »Giv netbanken en pause« om det virusangreb, der har været i denne uge, og oplyse om det forhold, at virussen kan have lagt et program ind, der aflæser, hvilke taster der bliver trykket på og sender besked videre til virussens afsender, der således kan få adgang til en række fortrolige oplysninger, en beskrivelse, der svarer til de snifferprogrammer politiet med terrorpakken har fået ret til at lægge ind på mistænktes computere, giver ministeren anledning til at revurdere regeringens beslutning om, at staten skal medvirke til at udvikle sådanne snifferprogrammer i stedet for at bruge ressourcerne på at udvikle programmer, der kan beskytte computere mod snifferprogrammer?«

Begrundelse

I forbindelse med vedtagelsen af terrorpakken i 2002, og igen da rockerloven her i foråret udvidede politiets adgang til at bruge snifferprogrammer, advarede flere edb-eksperter om den risiko, der er ved, at staten får en interesse i, at computere er åbne for angreb og skjulte programmer som snifferprogrammer. Mange mente, at staten hellere skulle bruge sine ressourcer på at udvikle programmer, der kan beskytte computere mod angreb for at øge brugen og tilliden til computere og internet.

Spørgeren mener, at det aktuelle virusangreb bør give regeringen anledning til at revurdere sin indstilling til problemet.

Svar (1/9 03)

Justitsministeren (Lene Espersen):
I artiklen »Giv netbanken en pause« beskrives virkningerne af computervirussen »Sobig F«. Ifølge artiklen kan computervirussen installere en »key-logger« – en tastetryksaflæser – på den angrebne computer. Key-loggeren giver computervirussens bagmand oplysning om tastetryk på den angrebne computer.

Installering af en key-logger er strafbart efter straffelovens § 263, stk. 2, medmindre installeringen foretages af politiet som led i en strafferetlig efterforskning, jf. retsplejelovens § 791 b (dataaflæsning).

Adgangen for politiet til som led i efterforskningen af alvorlige forbrydelser at foretage dataaflæsning af computere – f.eks. gennem installering af særlige edb-programmer (»snifferprogramer«) – blev indført som en del af den såkaldte anti-terrorpakke, som Folketinget vedtog i 2002.

Formålet med bestemmelsen var at forbedre politiets muligheder for at efterforske og opklare alvorlige forbrydelser, herunder forbrydelser, der begås som led i terrorvirksomhed. Efter bestemmelsen kunne dataaflæsning kun anvendes, hvis efterforskningen angik en af de i bestemmelsen særligt opregnede forbrydelser – f.eks. overtrædelser af straffelovens kapitel 12 (forbrydelser mod statens selvstændighed og sikkerhed) eller 13 (forbrydelser mod statsforfatningen og de øverste statsmyndigheder mv.).

Bestemmelsen er efterfølgende ændret ved lov nr. 436 af 10. juni 2003 (Bekæmpelse af rockerkriminalitet og anden organiseret kriminalitet). Ved lovændringen blev bestemmelsens anvendelsesområde udvidet, således at indgreb i form af dataaflæsning kan foretages, hvis efterforskningen angår en lovovertrædelse, der kan straffes med fængsel i 6 år eller derover, eller en overtrædelse af straffelovens § 286, stk. 1 (groft tyveri) eller § 289 (skattesvig, momssvig og indsmugling af særlig grov karakter).

Formålet med denne ændring var at fremme en effektiv politimæssig indsats mod visse alvorlige forbrydelser, der ofte begås som led i organiseret kriminalitet. Baggrunden for ændringen var navnlig, at der i stigende grad anvendes kryptering af elektroniske meddelelser i de organiserede kriminelle miljøer.

Det kan tilføjes, at politiet i forbindelse med dataaflæsning sikrer, at uvedkommende forhindres adgang til det pågældende edb-system.

Efter Justitsministeriets opfattelse har spørgsmålet om politiets adgang til at foretage dataaflæsning i forbindelse med efterforskning af alvorlige forbrydelser ikke nogen sammenhæng med ulovlig spredning af computervirus.