JUSTITSMINISTERIET
Politi- og Strafferetsafdelingen

Folketinget
Retsudvalget
Christiansborg
1240 København K

Dato: 28. november 2014
Kontor: Sikkerheds- og Forebyggelseskontoret
Sagsbeh: Andreas Christensen
Sagsnr.: 2014-0030-2517
Dok.: 1311286

Hermed sendes besvarelse af spørgsmål nr. 1540 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 17. september 2014. Spørgsmålet er stillet efter ønske fra Karina Lorentzen Dehnhardt (SF).

Mette Frederiksen

/

Rikke-Louise Ørum Petersen

Slotsholmsgade 10
1216 København K.

Telefon 7226 8400
Telefax 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 1540 (Alm. del) fra Folketingets Retsudvalg:

> ”Vil ministeren kommentere Politikens artikel »Politikere målløse over politiets håndtering af hackersag« fra den 12. september 2014 og redegøre for, hvorfor politiet ikke har haft fysisk adgang til it-systemerne hos CSC?”

Svar:

Justitsministeriet har til brug for besvarelsen af spørgsmålet indhentet en udtalelse fra Rigspolitiet, der har oplyst følgende:

> ”Rigspolitiet har til brug for besvarelsen af spørgsmålet indhentet et bidrag fra Københavns Politi, hvor efterforskningen af sagen har været forankret.
>
> **1.** Københavns Politi har oplyst, at repræsentanter fra Rigspolitiets IT-kriminalitetsbekæmpelsesenhed (det tidligere NITES, som nu indgår i Rigspolitiets Nationale Cyber Crime Center, NC3) i foråret 2013 orienterede politikredsen om hackerangrebet på CSC Danmark A/S (CSC). NITES havde konstateret angrebet på baggrund af en logfil, der efter forudgående aftale var modtaget fra svensk politi. Politiet i Sverige havde fundet logfilen i forbindelse med undersøgelse af en computer tilhørende den svenske statsborger Gottfrid Svartholm Warg, der på daværende tidspunkt var sigtet i Sverige for at have hacket sig ind i det firma i Sverige, som håndterede blandt andet svensk politis it-systemer.
>
> NITES havde forinden ved møder gjort CSC bekendt med angrebet. På møderne mellem relevant personale hos CSC og NITES var det aftalt, hvad der fremadrettet skulle ske, herunder hvordan politiet ønskede en ”incident rapport” udarbejdet, hvilke beviser der skulle sikres, og på hvilken måde de skulle sikres. Ligeledes var der aftalt løbende statusmøder mellem NITES og CSC med henblik på opfølgning på undersøgelserne og bevissikringen. Der var efter det oplyste tale om en helt normal fremgangsmåde i den type sager, hvor kun det ramte firmas teknikere kunne betjene systemerne, uden at disse led (yderligere) skade eller lukkede ned.
>
> Endvidere blev det på et møde mellem NITES og Københavns Politi besluttet, at der ud over den rapport, som CSC efter politiets retningslinjer skulle udarbejde, også skulle laves en parallel undersøgelse af et eksternt firma. Formålet hermed var bl.a. at undgå, at der kunne stilles spørgsmålstegn ved troværdigheden af den allerede igangsatte undersøgelse. Den eksterne undersøgelse er udarbejdet af et svensk firma, men er betalt af CSC. Under straffesagen er der blevet afhørt en række vidner,

der har forklaret om de foretagne undersøgelser, herunder et vidne fra det svenske firma, der udarbejdede den eksterne undersøgelse.

Det er i øvrigt Københavns Politis opfattelse, at samarbejdet mellem teknikerne i politiet og CSC er foregået upåklageligt under hele forløbet, og politiet har ikke haft anledning til på noget tidspunkt at sætte spørgsmålstegn ved hverken måden eller de personer, som har udført undersøgelser hos CSC.

2. Rigspolitiet kan mere generelt oplyse, at Rigspolitiets Nationale Cyber Crime Center (NC3), det tidligere NITES, efter anmodning yder bistand til politikredsenes efterforskning og retsforfølgning af it-kriminalitet mv., der kræver særlig avanceret teknologi, ekspertise eller rutine.

Ved NC3's bistand til politikredsenes efterforskninger af it-kriminalitet foretages en konkret vurdering af, hvorvidt digitale spor efter forbrydelsen skal tilvejebringes og sikres gennem en (midlertidig) beslaglæggelse af en genstand (f.eks. en computer), eller om genstanden for forbrydelsen har et omfang og/eller kompleksitet, der ikke muliggør en fysisk beslaglæggelse.

Således kan genstanden (f.eks. en computer, server eller mainframe) for forbrydelsen indgå som led i en virksomheds forretningskritiske systemer, herunder virksomhedens drift af andre kunder, eller være af væsentlig betydning for understøttelse af landets kritiske infrastruktur eller i øvrigt af samfundsvigtig karakter. Såfremt dette er tilfældet, foretager NC3 en vurdering af, hvorvidt en (midlertidig) beslaglæggelse af genstanden som led i efterforskningen kan forårsage nedbrud eller væsentlige driftsforstyrrelser. Hertil kommer, at genstanden kan være så kompleks, at kun medarbejdere i virksomheder, der til daglig beskæftiger sig med denne type genstand, til fulde kan gennemskue opsætningen og derved uddrage relevante data herfra uden at forårsage nedbrud eller væsentlige driftsforstyrrelser. På denne baggrund er det helt sædvanligt ved denne type angreb at lade virksomhedens egne teknikere varetage dele af den indledende undersøgelse enten efter politiets nærmere instruks eller i samarbejde med politiets teknikere eller særligt udpegede eksterne eksperter. Særligt ved visse former for mere avanceret it-kriminalitet kan kun længerevarende og mere dybdegående undersøgelse af genstanden samt analyse af de sikrede spor afdække, hvordan forbrydelsen konkret er udført og dermed afdække, hvad der konkret skal sikres, således at sporene kan indgå i uangribelig bevisførelse.

Som beskrevet af Københavns Politi har NC3 (tidligere NITES) ydet bistand til efterforskningen af hackerangrebet mod CSC. I denne sag kunne hackerangrebets omfang og betydelige

avancerethed ikke umiddelbart afdækkes, idet opsætningen og kompleksiteten af den angrebne mainframe hos CSC hindrede en umiddelbar bevissikring. Endvidere var der tale om en mainframe, hvor særdeles samfundskritiske systemer og registre blev hostet. På denne baggrund indledte NC3 en dialog med mainframens ejer, CSC, med henblik på at få afdækket, hvad virksomheden konkret var blevet udsat for, og hvor der kunne være relevante digitale spor fra forbrydelsen i CSC's systemer. Det bemærkes, at en sådan indledende dialog med ejeren af angrebet it-udstyr er helt sædvanlig i sager af den pågældende karakter. Herefter udarbejdede NC3 i samarbejde med Rigspolitiets Koncern IT et undersøgelsestema med spørgsmål til CSC, der ønskedes belyst. I den forbindelse anmodede Rigspolitiet CSC om, at der blev udarbejdet en "incident rapport" med en nøje beskrivelse af hændelsen. Kompleksiteten af CSC's systemers opbygning medførte dog, at Rigspolitiet vurderede, at en ekstern særlig sagkyndig bistand måtte inddrages i udarbejdelsen af rapporten med henblik på at søge påvist, hvilke dele af systemerne der kunne være kompromitteret, i hvilket omfang, og hvor digitale spor for forbrydelsen kunne forventes at blive fundet.

I den anledning anmodede Rigspolitiet CSC om at anvende en svensk virksomhed, idet denne virksomhed i forbindelse med efterforskningen af en sag om bl.a. hacking af et pengeinstituts it-systemer havde vist særlige kompetencer med den pågældende type mainframe. Rigspolitiet havde kendskab til den pågældende svenske virksomhed, idet Rigspolitiet havde samarbejdet med svensk politi om efterforskningen af en del af den svenske sag.

Sammenfattende kan det oplyses, at ved angreb på store, komplekse it-systemer er det ikke muligt for politiet uden risiko for at skabe nedbrud eller væsentlige driftsforstyrrelser selvstændigt at efterforske i det angrebne it-miljø. Der må således ud fra en konkret vurdering af karakteren af den angrebne genstand, herunder særligt samfundskritiske systemer, i et vist omfang inddrages den forurettede virksomheds egne teknikere eller eksterne særligt udvalgte ressourcer, hvilket også fandt sted i sagen om hackerangrebet mod CSC."