Tomas Frydenberg

Fra: Nicholai Kramer Pfeiffer [NKP@CyberCity.dk]
Sendt: 28. februar 2006 21:19
Til: Tomas Frydenberg
Cc: Simon Skals
Emne: SV: Papir om logning af Internet-oplysninger

Vedhæftede filer: TFR40093 CC.doc

TFR40093 CC.doc
(367 KB)

Hej Tomas,

Hermed vores umiddelbare bemærkninger til det fremsendte.

Hvis I har ønske om at drøfte/få uddybet vores kommentarer, stiller vi gerne op til et telefonmøde - evt. kl. 14.30 i morgen (onsdag).

Vi tales ved.

Hilsen

Nicholai Pfeiffer
Cybercity

Fra: Tomas Frydenberg [mailto:tfr@jm.dk]
Sendt: ma 27-02-2006 18:06
Til: Nicholai Kramer Pfeiffer
Emne: Papir om logning af Internet-oplysninger

Kære Nikolai.

Som aftalt vedhæftes vores papir om logning af Internet-oplysninger.
Tanken er, at vi sender papiret til ekspertgruppen senest på fredag. Jeg håber derfor, at vi kan tale sammen om jeres eventuelle bemærkninger senest torsdag. Som tidligere nævnt, vil der naturligvis ikke være tale om, at I på nogen måde bliver taget til indtægt for jeres eventuelle bemærkninger.

Med venlig hilsen

Tomas Frydenberg
Politikontoret
Civil- og Politiafdelingen
Tlf: 7226 8553

Justitsministeriet Telefon: 3392 3340
Slotsholmsgade 10 Telefax: 3393 3510
1216 København K E-mail: jm@jm.dk
http://www.jm.dk

Justitsministeriet
Civil- og Politiafdelingen

Dato: 27. februar 2006
Kontor: Politikontoret
Sagsnr.: 2005-945-0019
Dok.: TFR40093

NOTITS

om

logning af Internet-oplysninger, herunder oplysninger om Internet-baserede e-mail-tjenester samt IP-telefoni

1. Baggrund

Ved lov nr. 378 af 6. juni 2002 – den såkaldte anti-terror lov – blev der bl.a. indsat nye bestemmelser i retsplejelovens § 786 om registrering og opbevaring af oplysninger om teletrafik og om telenet- og teletjenesteudbyderes praktiske bistand til politiet.

Efter retsplejelovens § 786, stk. 4, påhviler det udbydere af telenet eller teletjenester at foretage registrering og opbevaring i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Justitsministeren fastsætter i henhold til bestemmelsen efter forhandling med ministeren for videnskab, teknologi og udvikling nærmere regler om denne registrering og opbevaring.

Efter retsplejelovens § 786, stk. 5, kan justitsministeren endvidere efter forhandling med ministeren for videnskab, teknologi og udvikling fastsætte regler om telenet- og teletjenesteudbyderes praktiske bistand til politiet i forbindelse med indgreb i meddelelseshemmeligheden.

Justitsministeren fastsætter tidspunktet for ikrafttrædelsen af disse bestemmelser.

Det fremgår af lovens forarbejder, at det nærmere indhold af de administrative regler om logning og praktisk bistand til politiet forudsættes fastsat efter dialog med branchen.

Slotsholmsgade 10
1216 København K

Telefon: 33 92 33 40
Telefax: 33 93 35 10

E-post: jm@jm.dk
Internet: http://www.jm.dk

Justitsministeriet sendte den 24. marts 2004 et udkast til bekendtgørelse og vejledning om telenet- og teletjenesteudbyderes registrering og opbevaring af oplysninger om teletrafik samt praktiske bistand til politiet i forbindelse med indgreb i meddelelseshemmeligheden i høring hos en række myndigheder og organisationer mv. Høringsfristen udløb den 15. maj 2004.

På baggrund af drøftelser med branchen blev der herefter nedsat en ekspertgruppe med deltagelse af repræsentanter for IT- og telebranchen samt boligforeningerne med henblik på yderligere drøftelser af udkastet til bekendtgørelse og vejledning.

På baggrund af drøftelserne i ekspertgruppen er der senest udsendt et revideret udkast til bekendtgørelse i februar måned 2005.

Den 21. februar 2006 vedtog Rådet (retlige og indre anliggender) endvidere et EU-direktiv om logning af trafikdata.

På denne baggrund foreslås det, at ekspertgruppen på et kommende møde drøfter omfanget af logningsforpligtelsen for så vidt angår Internet-oplysninger.

2. Forslag til den videre proces

Justitsministeriet lægger op til en drøftelse af logningsforpligtelsen for så vidt angår Internet-oplysninger på mødet i ekspertgruppen om logning den 8. marts 2006.

Resultatet af drøftelserne vil herefter indgå i Justitsministeriets overvejelser med henblik på den endelige udformning af logningsbekendtgørelsen.

3. Forslag til model for logning af Internet-oplysninger, herunder oplysninger om Internet-baserede e-mail-tjenester samt IP-telefoni

Justitsministeriet har overvejet spørgsmålet om omfanget af logningsforpligtelsen for så vidt angår Internet-oplysninger, herunder oplysninger om Internet-baserede e-mail-tjenester samt IP-telefoni.

Det har bl.a. fra branchens side været anført, at Justitsministeriet tilsyneladende ønskede at logge samtlige Internet-oplysninger, og at dette bl.a. ville betyde, at den loggede datamængde ville være uhåndterbar, og at man samtidig ville blive pålagt at logge indhold.

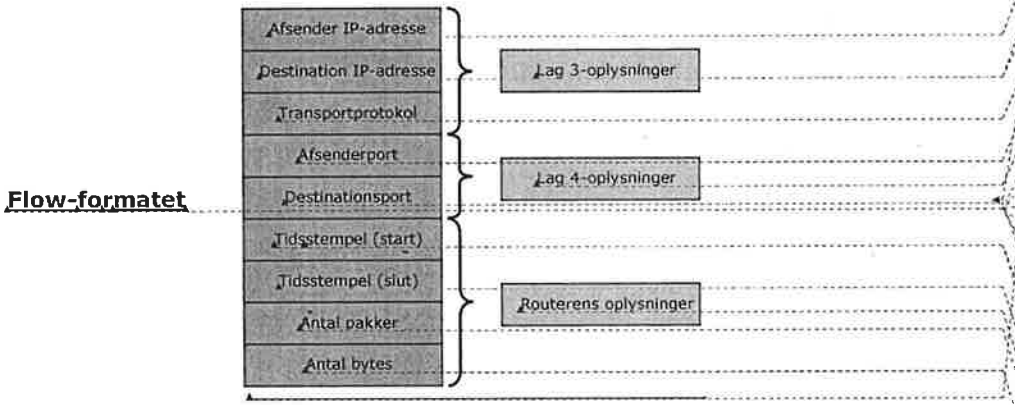
Justitsministeriet har på den baggrund særligt overvejet det politimæssige behov for trafikdata. Det kan på den baggrund bemærkes, at politiet typisk i indledningen af en konkret efterforskning vil have behov for hurtigt at kunne tilvejebringe et billede af, hvilke tjenester en Internetkunde gør brug af. På denne baggrund vil politiet kunne tilrettelægge og planlægge den fremadrettede efterforskning. Det vil således ud fra en politimæssig synsvinkel ikke altid være nødvendigt at logge samtlige Internet-oplysninger.

I det følgende er der redegjort for Justitsministeriets overvejelser og forslag til teknisk løsning, der på den ene side ikke lægger op til fuldstændig logning af samtlige Internet-oplysninger, men som på den anden side ses at opfylde de basale krav til tilrettelæggelsen af politiets videre efterforskning:

Ved en såkaldt "data-transmission" arbejdes der i forskellige lag. Lagene er defineret i forhold til den såkaldte "OSI-model", der er grundlaget for al data-transmission.

Routningsdata – eller i fagsprog IP-header-oplysninger – er data, der blandt andet indeholder informationer vedrørende IP-adressering og protokoltype på det følgende lag. Denne information foregår på OSI-modellens lag 3.

På OSI-modellens lag 4 findes header-oplysningerne for den anvendte transportprotokol. Herunder oplysninger om portnumre for TCP og UDP (de to hyppigst anvendte transportprotokoller).



Payload er dataindholdet i de øvre lag: Det vil sige grafik, dokumenter eller andet indhold, men også headeroplysninger fra højereliggende protokollag.
Det er i selve payload-delene, de brugerrelaterede data findes.

Slettet: de

Slettet: alene

Slettet: ,

Slettet: datatype på

Slettet: niveau, tidspunkt og datamængde

Slettet: Dette anvendes som en kontrolforanstaltning ved en data-transmission for at konstatere, at en transmission bliver korrekt gennemført.

Formateret: Skrifttype: CG Times, 12 pkt

Formateret: Centreret

Formateret: Skrifttype: 7 pkt

Formateret: Skrifttype: 7 pkt

Formateret: Skrifttype: 7 pkt

Formateret: Skrifttype: 7 pkt

Formateret: Skrifttype: 7 pkt

Formateret: Skrifttype: 7 pkt

Formateret: Skrifttype: Verdana, 10 pkt, Fed

Formateret: Skrifttype: Verdana, 10 pkt, Fed

Formateret: Skrifttype: Verdana, 10 pkt, Fed

Formateret: Skrifttype: Verdana, 10 pkt, Fed

Formateret: Skrifttype: Verdana, 10 pkt, Fed

Formateret: Skrifttype: 7 pkt

Formateret: Skrifttype: 7 pkt

Formateret: Skrifttype: 7 pkt

Formateret: Skrifttype: 7 pkt

Formateret: Skrifttype: 7 pkt

Formateret: Skrifttype: 7 pkt

Formateret: Skrifttype: 7 pkt

Som historiske teleoplysninger vil kombinationen af routningsdata og udvalgte header-oplysninger fra transportprotokollen typisk være efterforskningsmæssigt tilstrækkelige. Efter det for Justitsministeriet oplyste, har teleselskaberne i dag kendskab til produkter, der understøtter denne form for logning af routningsdata.

Teknologien omkring disse produkter er efter det oplyste indrettet således, at det vil være muligt at logge initierende pakke og afsluttende pakke med henblik på, at omfanget af en brugers data-session udelukkende vil omfatte de i eksemplet nedenfor nævnte oplysninger.

Eksemplet neden for viser en Tele 2-kundes opkobling mod BT's hjemmeside den 7. februar 2006 kl. 06:42:

IP-adresser	Transportprotokol
S: 212.56.170.123 D: 80.80.12.123	TCP S: 8080 D: 80
Antal pakker	**Tidsstempler**
500 pakker 499 KB	S: 07022006 06:42:01 E: 07022006 06:43:45

Afsender A's IP-adresse og modtager B's IP-adresse skal i den enkelte udbyders netværk registreres så tæt på abonnenten som overhovedet muligt.

Justitsministeriet skal på denne baggrund foreslå, at omfanget af logningsforpligtelsen for så vidt angår Internet-oplysninger, herunder oplysninger om Internet-baserede e-mail-tjenester samt IP-telefoni, begrænses til oplysningerne i det oven for beskrevne eksempel.

Man kunne i øvrigt overveje at fastsætte logningsforpligtelsen i form af en såkaldt "sampling".

+ evt. overveje DNS-logning.

"logning af DNS-opslag

Slettet: ¶

Slettet: anvender

Slettet: endvidere

Slettet: ¶
¶
---------Sideskift---------

Kommentar [NKP1]: Nedenstående tabel er en smule misvisende ift. traditionelle gengivelser af netflow. I stedet foreslås derfor indsatte eksempel.

Slettet: ¶
Dato/tid ... [1]

Formateret tabel

Formateret: Centreret

Slettet: ¶

Slettet: Hvis der var tale en almindelig e-mail, ville det fremgå, at protokollen POP 3 blev benyttet.

Slettet: ¶

Dato/tid	Afsender (IP)	Destination (IP)	Afsender-port	Destina-tionsport	Proto-kol	Antal pakker og by-tes
07.02.06 06:42	212.56.170. 123	80.80.12.12 3	80 80	80	TCP	2000399 kb