

Hvilke spørgsmål bør man stille før man vælger udbyder af anti-terror løsning:

I det følgende har vi givet nogle gode råd til, hvilke spørgsmål man skal stille, når man vælger sin anti terror løsning.

Der er flere love og direktiver som regulerer på området.

Det er derfor ikke tilstrækkeligt at en leverandør garanterer at logningsbekendtgørelsen overholdes, da denne kun er en del af lovgivningen på området.

Indholds fortegnelse

- 1 Hvem har ansvaret:
- 2 Kan systemet logge første og sidste pakke i en internet session:
- 3 Undtagelsen ”sampling” af hver 500. pakke
- 4 Hvor på nettet bliver data logget?
- 5 Logning af indholdsdata
- 6 Data sikkerhed
- 7 Data lagring

1 Hvem har ansvaret:

Loven siger:

Det er dog også muligt for udbydere at out-source pligten efter aftale, således at de praktiske foranstaltninger foretages i en anden udbyders domæne. Den udbyder, som forpligtelsen ifølge telelovens § 15 påhviler, har således mulighed for at aftale med sin eventuelle egen udbyder, at de praktiske indgreb foretages af denne. **Selvom pligten out-sources, er det dog altid den udbyder, der har selve slutbrugerforholdet, der er ansvarlig for, at reglerne i § 15 faktisk overholdes.**

Selv om man har out-sourcet logning af sit internet, kan det altså være en god ide at sikre sig at producentens løsning lever op til kravene.

2 Kan systemet logge første og sidste pakke i en internet session:

Loven siger:

2.2.Internet-oplysninger (bekendtgørelsens § 5)

2.2.1. Sessionslogning (bekendtgørelsens § 5, stk. 1)

Udbydere af adgang til internettet skal, for så vidt angår en internet-sessions initierende og afsluttende pakke, registrere oplysninger om den afsendende og den modtagende internetprotokol-adresse (herefter benævnt IP-adresse), afsendende og modtagende portnummer og transportprotokol.

Ved IP-adresse forstås den brugeridentitet, en internetbruger gør brug af ved anvendelse af internettet. IP-adressen tildeles elektronisk af internetudbyderen på baggrund af et abonnementsforhold eller lignende.

Modtagende IP-adresse identificerer en internet-sessions destination. Det kan f.eks. være en anden slutbruger, Hotmail, en anden hjemmeside eller lignende.

Ved kommunikation på internettet sendes oplysninger fra en port til en anden port. Et portnummer kan identificere, hvilken type kommunikation der finder sted som led i anvendelsen af internettet.

Ved oplysninger om transportprotokol forstås oplysninger om, hvilken protokol der har været anvendt til at transportere de pakker, der indgår i en internet-session. Det kan f.eks. være TCP, UDP eller lignende.

Ved "internet-session" forstås ikke en nærmere afgrænset teknisk definition. Med det begreb, der anvendes i bekendtgørelsen, skal imidlertid forstås den situation, hvor en slutbruger sender eller modtager data på internettet. En udbyder skal således registrere oplysninger om en internet-sessions initierende og afsluttende pakke, herunder oplysninger om afsendende og modtagende IP-adresse, afsendende og modtagende portnummer samt transportprotokol, hver gang en slutbruger tilgår f.eks. en server eller kommunikerer direkte over internettet med en anden slutbruger.

Hvis en udbyder registrerer oplysninger om den afsendende og den modtagende IP-adresse, afsendende og modtagende portnummer samt transportprotokol, vil man efter omstændighederne kunne sortere kortere sessioner med et mindre antal pakker fra, med henblik på, at disse oplysninger ikke registreres og opbevares. Det forudsættes, at en eventuel frasortering sker efter samråd med politiet. De nærmere retningslinjer herfor fastsættes i en senere bekendtgørelse.

Det er en forholdsvis kompliceret operation af "fange" den sidste pakke i en session og kræver at systemet holder øje med alle pakker der bliver transmitteret.

Routere vil i almindelighed ikke være i stand til at udføre denne opgave

3 Undtagelsen "sampling" af hver 500. pakke

2.2.2. "Sampling" (bekendtgørelsens § 5, stk. 4)

Forpligtelsen til at registrere oplysninger om en internet-sessions initierende og afsluttende pakke gælder ikke for udbydere, hvis en sådan registrering ikke er teknisk mulig i udbydernes system. Oplysningerne skal i så fald i stedet registreres for hver 500. pakke, der indgår i en slutbrugers kommunikation på internettet.

Hvis udbyderne registrerer oplysninger for hver 500. pakke, der indgår i en slutbrugers kommunikation på internettet, skal der registreres oplysninger om afsendende og modtagende IP-adresse, afsendende og modtagende portnummer samt transportprotokol.

Udbyderne er ikke forpligtet til at udvikle nye tekniske systemer med henblik på at være i stand til at registrere oplysninger om en internet-sessions initierende og afsluttende pakke (sessionslogging). En udbyder vil f.eks. leve op til logningsforpligtelsen, selv om udbyderen ændrer sine systemer eller udvikler nye systemer, der kun kan registrere for hver 500. pakke, der indgår i en slutbrugers kommunikation på internettet.

Læg mærke til at det er hver 500. pakke for hver slutbruger.

Det er en udbredt misforståelse at loven giver mulighed for at logge hver 500. pakke på netværket uden hensyn til slutbrugerforholdet.

Routere vil i almindelighed ikke være i stand til at udføre denne opgave

4 Hvor på nettet bliver data logget?

Loven siger:

2.2.4. Registrering ved overgangen til andre net (bekendtgørelsens § 5, stk. 5)

Registrering af internet-oplysningerne skal ske ved overgangen mellem udbyderens eget net og et andet eller andre net. Det gælder uanset, om udbyderne registrerer initierende og afsluttende pakke eller alene registrerer hver 500. pakke, der indgår i en slutbrugers kommunikation på internettet. Pligten til at registrere ved overgangen mellem udbyderens eget net og et andet eller andre net er illustreret nedenfor:

Figuren ovenfor illustrerer, at oplysninger om en slutbrugers tilgang til internettet skal registreres af udbyderen, hvis kommunikationen forlader udbyderens net. Figuren illustrerer ligeledes, at udbyderen skal registrere oplysninger om en slutbrugers anvendelse af udbyderens egne tjenester (pkt. 2.3.), uanset om tilgangen til tjenesten sker via udbyderens eget net eller via et andet eller andre net.

Her er det vigtigt at iagttage at logningen skal foregå ved overgang til anden udbyder, det er således ikke brugbart at placere en ”sort boks” på indersiden (LAN siden) af routeren.

Dette både af hensyn til korrektheden af IP og port numre men også tidsstempellet kan variere og gøre data ubrugelige for myndighederne

5 Logning af indholdsdata

Loven siger:

§ 1. Udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal etablere et døgnbetjent kontaktpunkt, der til enhver tid kan bistå politiet i forbindelse med iværksættelsen af indgreb i meddelelshemmeligheden, jf. lov om rettens pleje kapitel 71. **Oplysninger om det døgnbetjente kontaktpunkt skal meddeles Rigspolitiets Telecenter.**

LOV nr 545 af 08/06/2006 § 15, stk. 1,

»Udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere som nævnt i § 6, stk. 1, skal uden udgift for staten, herunder for politiet, sikre,

1) at det tekniske udstyr og de tekniske systemer, udbyderen anvender, er indrettet således, at politiet kan få adgang til at foretage indgreb i meddelelshemmeligheden i form af aflytning, fremadrettet teleoplysning og udvidet teleoplysning og indgreb i form af teleobservation, jf. lov om rettens pleje, kapitel 71,

2) at det tekniske udstyr og de tekniske systemer, udbyderen anvender, er indrettet således, at politiet kan få adgang til at foretage indgreb i meddelelshemmeligheden, jf. lov om rettens pleje, kapitel 71, i form af fremadrettet teleoplysning og udvidet teleoplysning umiddelbart efter, at disse oplysninger registreres,

I § 15 »Stk. 4. Det påhviler udbyderen at sikre, at politiets anmodninger om fremskaffelse af historisk teleoplysning og udvidet teleoplysning behandles straks og på en måde, så hensigten med indgrebet ikke forspildes.«

Lovgivningen giver anledning til fortolkning om hvorvidt udbyderen blot skal bistå politiet med indgrebet eller kunne foretage indgrebet.

Det er dog ubestridt således at udstyret skal være indrettet således at også fremadrettet indholdslogning skal kunne iværksættes umiddelbart.

Der hersker heller ikke tvivl om at politiets forventning er, at udbyderen foretager indgrebet og fremsender trafikken for ”så hensigten med indgrebet ikke forspildes”.

Man må desuden forvente at der i fremtiden bliver påkrav om at trafikken streames direkte til politiets datacenter efter ETSI standard for indholds streaming.

6 Data sikkerhed

Loven siger:

Artikel 7: Databeskyttelse og datasikkerhed

Med forbehold af bestemmelser vedtaget i medfør af direktiv 95/46/EF og direktiv 2002/58/EF skal hver medlemsstat sikre, at udbydere af offentligt tilgængelige elektroniske kommunikationstjenester eller af et offentligt kommunikationsnet som et minimum respekterer følgende datasikkerhedsprincipper for data, der lagres i overensstemmelse med nærværende direktiv:

- a. de lagrede data skal være af samme kvalitet og være omfattet af den samme sikkerhed og beskyttelse som de data, der findes på nettet
- b. dataene skal være omfattet af de fornødne tekniske og organisatoriske foranstaltninger, så de er beskyttet mod hændelig eller ulovlig tilintetgørelse eller hændeligt tab, mod forringelse, ubeføjet eller ulovlig lagring, behandling, adgang eller udbredelse
- c. dataene skal være omfattet af de fornødne tekniske og organisatoriske foranstaltninger, så det sikres, at kun særligt autoriserede personer får adgang til dataene, og
- d. dataene skal tilintetgøres ved udløbet af lagringstiden, bortset fra data, der har været givet adgang til, og som er blevet gemt.

Det er således en god ide at undersøge om data behandles og lagres på en forsvarlig måde, samt at der foretages backup af data.

Det må ligeledes kraftigt anbefales at opkobling på neværket foretages ved en krypteret forbindelse, for at undgå at identiteten mellem to slutkunder ”stjæles” eller ”forveksles”

7 Data lagring

Loven siger:

Artikel 8: Krav til lagringen af data

Medlemsstaterne sørger for, at de i artikel 5 nævnte data lagres i overensstemmelse med dette direktiv på en sådan måde, at de lagrede data og alle andre nødvendige oplysninger vedrørende disse data kan fremsendes uden unødigt forsinkelse til de kompetente myndigheder på disses anmodning.

I praksis skal der kunne foretages udtræk på ”gamle data” samtidig med at friske data skal kunne afleveres uden unødigt forsinkelse.

De fulde lovtekster kan findes her:

<https://www.retsinformation.dk/Forms/R0710.aspx?id=29282&exp=1>
<http://logningsdirektivet.dk/>

For yderligere information kontakt:

Unispeed A/S
Engvej 139
DK-2300 København S
Phone +45 33445500
Fax +45 33445501
Web: www.unispeed.dk
mailto: sales@unispeed.dk

