Rådet for Digital Sikkerhed

2. februar 2016

Rådet for Digital Sikkerheds positionspapir for udvidet logning af danskerne internettrafik

Rådet for Digital Sikkerhed bakker op om Rigspolitiets bestræbelser for at sikre danske virksomheder og borgere mod kriminelle aktiviteter og anerkender behovet for effektive efterforskningsredskaber. Rådet mener dog ikke at konsekvenserne af Justitsministeriets meget indgribende forslag om at overvåge alle danske virksomheder og borgeres internettrafik, står mål med hensigten om at kunne retsforfølge kriminelle aktiviteter

Udvidet overvågning af danskernes internettrafik vil ramme skævt

Justitsministeriet og Rigspolitiet annoncerede for nyligt, at man ønsker at genindføre krav om internet sessionslogning - denne gang i en udvidet form, hvor der skal foretages en registrering af internettrafikken knyttet til hvert enkelt abonnent. Hensigten er at give Rigspolitiet bedre mulighed for efterforskning.

Rådet bakker op om Rigspolitiets bestræbelser for at sikre danske virksomheder og borgere mod kriminelle aktiviteter og anerkender behovet for effektive efterforskningsredskaber. Det noteres at argumentation for genindførelse for sessionslogning ikke er knyttet til terrorbekæmpelse, men almindelig kriminalitetsefterforskning.

Sessionslogning er ikke proportionalt

Rådet mener således ikke at Justitsministeriets meget indgribende forslag om at overvåge alle danske virksomheder og borgeres internettrafik, står mål med hensigten om at kunne retsforfølge kriminelle aktiviteter:

1. Det er allerede i dag muligt efter retsplejelovens bestemmelser, med dommerkendelse, at få etableret målrette overvågning af én eller flere brugers internettrafik.
2. En bred overvågning af alle abonnenters trafik er et meget omfattende indgreb i de grundliggende rettigheder, som sikrer beskyttelse af borgernes ret til privatliv og som er slået fast i EMRK, artikel 8 og UNDHR, artikel 12. Man kan frygte, at følgerne af et sådant indgreb er underminering af tilliden til brug af digitale tjenester, digitaliseringen og staten generelt. I hvert fald er der en risiko for at abonnenterne ændrer adfærd, når de overvåges.
3. Sessionslogningen pr. abonnent er en endog meget fintmasket logning. Der er imidlertid indbygget huller i forslaget i og med at ejendomsselskaber med under 100 boliger, forskningsinstitutioner og biblioteker undtages logningen.

Sessionslogning er ikke effektivt

Mange tjenester ringer op til servere i andre lande og den videre kommunikation, herunder til andre borgere, foregår fra disse servere. Man får kun derfor kun afsenderinformationerne og der er risiko for at såvel beregnet datastørrelse såvel som tidsstempling bliver uprækcis. Hertil kommer at sessionslogning kan omgås af brugere, der har en interesse deri. Det kan ske ved generelt at proxy internettrafikken til servere i udlandet, ved at bruge VPN-forbindelser, ved at bruge ”onion routing” som f.eks. TOR-netværket eller ved at camouflere hvem modtageren for kommunikationen er. Internettet indeholder mange gode råd til at undgå logning – f.eks. http://www.techsono.com/usenet/faq/avoid-ip-address-tracking.

Endelig findes der os bekendt endnu ikke tal som demonstrerer at logningen har nævneværdige effekter på kriminalitetsbekæmpelse. I 2012 blev der logget knap 1 billion transaktioner (1.000 milliarder) og alle disse data førte til 3 sigtelser - heraf ingen med relation til terror - og kostede teleindustrien 500 millioner kr. på bundlinjen.

Rådet for Digital Sikkerhed
Toldbodgade 12, 1253 København K
Telefon: +45 9137 5600 mail: info@digitalsikkerhed.dk web: www.digitalsikkerhed.dk

Sessionslogning er uforholdsmæssigt omkostningstungt

Den tidligere sessionslogning er således allerede demonstreret særdeles omkostningsfyldt og forslaget om en udvidet logning vil betyde behov for yderligere ændringer i systemer på tværs af hele telebranchen. Samlet vurderes investeringer til at kunne overvåge alle internetbrugers internettrafik, at beløbe sig til endnu et trecifret millionbeløb. Det vil være midler, der klart kunne investeres i mere værdiskabende teknologi til gavn for det danske samfund

Principper for evaluering

Danmark har allerede på en række områder etableret logning af borgernes færden og digitale interaktion. Med systemer som telelogning, ANPG (Automatisk NummerPladeGenkendelse), europæisk PNR og senest DSB's opsamling af ID/Pas-billeder i forbindelse med rejser til Sverige, er der etableret systematisk opsamling af data omkring borgernes færden og interaktion. I Rådet for Digital Sikkerhed' optik mangler der grundliggende principper og retningslinjer for, hvordan overvågning og logning skal ske, og hvordan vægtning mellem sådanne tiltag, udkomme (samfundsmæssig gevinst) og økonomiske byrder, skal foretages.

I forlængelse af tidligere udmeldinger om beskyttelse af personoplysninger og drøftelser i Rådet for Digital Sikkerhed' bestyrelse, anbefales at følgende principper skal efterleves ved logning:

- Logning af borgernes digitale færden og adfærd skal kun undtagelsesvist gøres til genstand for systematisk dataopsamling. I helt særlige situationer kan man forestille sig at kortvarig, national logning af såvel sessions- som indholdsdata og adgang til data-metriske analyser (Big Data analyse såsom datamining & mønstergenkendelse) kan iværksættes. Dette bør ske alene efter indhentning af en dommerkendelse.
- Dersom logning af lokations og indholdsdata på nye områder ønskes iværksat, bør dette alene ske efter en grundig offentlig debat og en offentlig vurdering af den digitale helhedskonsekvens såvel for borgernes ret til privatliv (personlig integritets konsekvens) som virksomhedernes administrative og økonomiske byrder (virksomheds-økonomisk konsekvens) som betydning for samfundets bekæmpelse af kriminalitet og terror (societal & demokratisk konsekvens).

Afslutningsvist skal det påpeges at myndigheders kortvarige logning – på helt afgrænsede, specifikke områder, som PNR og ANPG – vurderes i overensstemmelse med principperne, mens det for logning af samtlige tele/data (sessions- og indholdslogning – såkaldt telelogning) vurderes ikke i overensstemmelse med principperne, fordi logningen ikke vil stå mål med de samfundsmæssige gevinster eller de virksomhedsøkonomiske omkostninger.

Opfordring til dialog

Rådet vil derfor opfordre Justitsministeren til at udsætte fremsættelse af lovforslaget og i stedet invitere telebranchen og andre interessenter til dialog om Rigspolitiets behov i lyset af den stigende kommunikation over internettet og i forbindelse med denne dialog inddrage ovenstående principper i sine betragtninger. Det er nødvendigt at evaluere lovforslaget grundigt og have en grundig demokratisk dialog.

Vi anser det samtidigt for afgørende, at Danmark tager alle forholdsregler for at sikre, at der ikke indføres logning, der strider mod EU Charteret om Grundliggende Rettigheder.

Rådet for Digital Sikkerhed
Toldbodgade 12, 1253 København K
Telefon: +45 9137 5600 mail: info@digitalsikkerhed.dk web: www.digitalsikkerhed.dk

Rådet for Digital Sikkerhed

2. februar 2016

Faktaboks om logning

Et grundliggende træk ved digital interaktion er, at der efterlades digitale spor som oftest kan kobles til det individ som har forestået interaktionen. Gennem tidsmæssig opbevaring af disse spor (logning) kan man sammenkoble begivenheder, hændelser og mønster – som potentielt kan bruges til at hjælpe borgeren med at få bedre service (fx Cookie-bestemmelserne), bedre brugeroplevelser eller give myndigheder forståelse af fx kriminelle netværks interaktion.

Justitsministeriet ønsker at der for internettrafik pr. datasession skal logges:

- Afsendende internetprotokol-adresse
- Modtagende internetprotokol-adresse
- Transportprotokol
- Afsendende portnummer
- Modtagende portnummer
- Volumental (antal bytes overført)
- Tidspunkt for påbegyndelse og afslutning af datasessionen

For mobil internet- og teletrafik skal desuden logges:

- Maste- og celleoplysninger

Rådet for Digital Sikkerhed
Toldbodgade 12, 1253 København K
Telefon: +45 9137 5600 mail: info@digitalsikkerhed.dk web: www.digitalsikkerhed.dk