Notat

Til	Fra	Dato
Justiskomiteen, Stortinget	Tore Tennøe og Robindra Prabhu, Teknologirådet	Oslo, 25.05.2016

Innspill til Prop 68 L – skjulte tvangsmidler

Teknologirådet ønsker med dette å gi innspill til Stortingets behandling av Prop 68 L (2015-2016). Innspillet begrenser seg til regjeringens forslag om å innføre dataavlesning som nytt tvangsmiddel, slik det står omtalt i kap. 14. Vårt innspill baserer seg blant annet på EU-prosjektet SurPRISE[1] og en gjennomgang av relevante erfaringer fra Tyskland.

Kryptering og politiets behov for dataavlesing

Lovverk og tilsyn regulerer hvordan politi- og sikkerhetstjenester skal utøve sin virksomhet, og på hvilket grunnlag de kan overvåke innbyggerne. Men historisk har tekniske og økonomiske barrierer vært vel så viktige beskyttelser mot overvåking. Snowden-avsløringene viste tydelig at disse barrierene nå er i ferd med å forsvinne.[2]

Som en reaksjon på avsløringene om masseovervåkning, har kommersiell kryptering fått et betydelig løft. Store aktører som Google, Apple og WhatsApp krypterer nå store deler av sine tjenester. Dermed har kryptering i løpet av kort tid blitt vanlig praksis også for de fleste norske nettbrukere.

Utbredt kryptering vil vanskeliggjøre kommunikasjonskontroll fra politiets side. Dette gir behov for nye metoder og en tilpassing av regelverk til en ny teknologisk virkelighet dersom politiets evne til kriminalitetsbekjempelse skal opprettholdes.

Proposisjonen definerer dataavlesning svært bredt. Teknologien har bred funksjonalitet, mulighetsrommet for overvåkning er stort og inngrepet potensielt svært invaderende i borgernes privatsfære. Dette setter desto høyere krav til skranker for bruk av slike tvangsmidler, samt robust kontroll og tilsyn.

Dataavlesning er ikke én metode med en funksjonalitet, men kan i likhet med en sveitserkniv anvendes på ulike måter, til ulike formål. Derfor må en slik kontroll innebære både tradisjonelt tilsyn med politiets overvåkningsvirksomhet, men også kontroll med utforming av verktøyene som brukes og funksjonaliteten til disse. En slik kontroll med teknologien er nødvendig for å opprettholde rettsikkerheten og ivareta tilliten.

---

[1] http://surprise-project.eu

[2] «Metadata og den nye overvåkningen», Personvern – tilstand og trender 2014, Teknologirådet/Datatilsynet (2014)

Samfunnssikkerhet og handel i digitale sårbarheter

Kryptering styrker samfunnssikkerheten i Norge. Innbyggernes smarttelefoner, nettbrett og datamaskiner håndterer alt fra banktransaksjoner og helseinformasjon, til personlige bilder, eposter og meldinger. Kryptering gir viktig og nødvendig beskyttelse mot hacking, identitetstyveri, overvåkning og spionasje m.m. Tillit til sikker kommunikasjon og lagring og deling er viktig for vekst i den digitale økonomien, og samtidig en viktig forutsetning for digitaliseringen av offentlige tjenester. Teknologirådet støtter derfor det digitale sårbarhetsutvalgets anbefaling om at bruken av kryptering ikke bør reguleres eller begrenses.[3]

I mange tilfeller vil dataavlesning basere seg på å utnytte sikkerhetshull i digital teknologi for å skaffe innpass i systemer. I stedet for å rapportere sikkerhetshull til programvareprodusenten, utnyttes disse sikkerhetshullene for å gi betalende aktører tilgang til andres maskiner. Mange kommersielle aktører som tilbyr dataavlesningsteknologi driver i realiteten handel i digitale sårbarheter i et gråmarked. Menneskerettighetsorganisasjoner har dessuten pekt på at flere slike selskaper har solgt sine tjenester til regimer som bruker teknologien for å spionere på politiske motstandere og mot aktivister.[4]

Skal norsk politi ta i bruk dataavlesning, er det fare for at det blir en betalende aktør i et omstridt gråmarked, og slik underminerer arbeidet for styrket samfunnssikkerhet. Et annet moment er at eksterne tilbydere av programvare for dataavlesning kan legge inn skjult funksjonalitet som innhenter informasjon til andre interessenter enn norsk politi.

Disse dilemmaene er ikke diskutert eller adressert i proposisjonen.

Utfordringer ved dataavlesing

Alternativet til å kjøpe kommersielle overvåkningsverktøy på gråmarkedet, er å utvikle slik programvare i nasjonal regi. Her kan det være nyttig å trekke på tyske justismyndigheters erfaringer med å overvåke internet-telefoni før kryptering.

I 2011, avdekket den tyske hackergruppen Chaos Computer Club (CCC) flere svakheter ved en trojaner, som det viste seg var utviklet og tatt i bruk av tysk politi.[5] Dette gjaldt blant annet:

- *Svak sikkerhet og kontroll*: Dårlig kryptering og autentisering gjorde det mulig for CCC å få tilgang til alle maskiner som var infisert av trojaneren og ta over kontrollen av disse. Dårlig sikring gjorde dermed at både systemene til overvåkningsobjektene og politiet var sårbare for misbruk fra tredjeparter.
- *Jurisdiksjon*: Kommunikasjonen mellom trojaneren og tysk politi gikk via servere i USA, der dataene kunne eksponeres for overvåkning fra amerikanske sikkerhetsmyndigheter.

---

[3] «Digital sårbarhet – sikkert samfunn», NOU 2015:13, s 16

[4] SurPRISE – surveillance, privacy and security, D 3.1 Report on surveillance technology and privacy enhancing design (ss 33-44), url: http://surprise-project.eu/wp-content/uploads/2013/06/SurPRISE-D3.1-Report-on-surveillance-technology-and-privacy-enhancing-design.pdf

[5] «Anatomy of a digital pest», Frankfurter Allgemeine Feuilleton, 27.10.11, url: http://www.faz.net/aktuell/feuilleton/chaos-computer-club-anatomy-of-a-digital-pest-11508378.html?printPagedArticle=true#pageIndex_2

- *Manglende skranker*: Kontrolløren av trojaneren kunne installere og kjøre hvilket som helst program på den infiserte maskinen, også funksjonalitet som går utover tysk lov, slik som f.eks. å aktivere webkamera eller plante bevis på maskinen. Ifølge CCC var det også gjort bevisste tekniske forsøk på skjule funksjonaliteten til trojaneren.

Erfaringene fra Tyskland viser at de tekniske metodene som muliggjør dataavlesning gir tilsynsmyndigheter helt nye utfordringer. Det var tross alt et hackermiljø og ikke tyske tilsyns- og kontrollorganer som varslet om ovennevnte svakheter. Skal norsk politi ta i bruk slike metoder, må tilsynsutfordringene adresseres på tilfredsstillende vis. I tillegg må skranker for bruk inkluderes i den tekniske utformingen av verkøyet.[6]

Innspill for å fremme sikkerhet, kontroll og tilsyn

Dataavlesning er en inngripende overvåkningsmetode. Proposisjonen forbeholder derfor bruken til politiets etterforskning av alvorlig kriminalitet med høy strafferamme, med føringer som begrenser bruk over lengre tid.

Men ettersom teknologien for dataavlesning har en bred funksjonalitet og omfatter svært mange overvåkningsformer, og samtidig både har sikkerhetsmessige og etiske utfordringer, savner vi en diskusjon av hvordan man sikrer effektiv kontroll med teknologien og dens bruk.

Teknologirådet vil med henvisning til ovenstående komme med følgende innspill til innrammingen av politiets bruk av dataavlesning:

Dataavlesningsverktøy bør utvikles i Norge

Proposisjonen gir politiet stor frihet til å selv å velge praktisk fremgangsmåte for å gjennomføre dataavlesningen, og til benytte seg av egnede tekniske hjelpemidler og dataprogram. Samtidig åpner handel av kommersiell hyllevarer både sikkerhetsmessige og etiske dilemmaer som proposisjonen ikke adresserer. Tillit til politiets overvåkningsvirksomhet fordrer innsikt i hva programvaren faktisk gjør og kontroll med bruken.

For å gi norsk politi og tilsyn tilstrekkelig kontroll, kan det være hensiktsmessig å utvikle dataavlesningsverktøy i Norge. Det kan gi forsikringer om at informasjon ikke kommer på avveie til tredjeparter og muligens forenkle både politiets og tilsynsmyndigheters tilgang til kildekode. Det kan også gjøre det enklere for myndighetene å styre utformingen av verktøyene med f.eks. med funksjonalitetsbegrensninger i kildekode der dette er hensiktsmessig.

Verktøyene må bestå en sikkerhetstest

Erfaringer fra Tyskland viser at dataavlesning kan medføre en sikkerhetsrisiko for både den som overvåkes og for politiet. Proposisjonen forplikter politiet «så langt det er praktisk mulig» å beskytte den overvåkede mot uberettiget tilgang til datasystemet fra uvedkommende.

[6] Tyske justismyndigheter har etter avsløringene til CCC utviklet en ny versjon av trojaneren, se f.eks. http://www.deutschlandfunk.de/software-fuer-bundeskriminalamt-neuer-bundestrojaner-kurz.1773.de.html?dram:article_id=346293

Etter vårt syn er dataavlesning er en såpass inngripende overvåkningsmetode at proposisjonen bør gå lenger i å etablere robuste mekanismer for å ivareta sikkerheten. Verktøyene må imøtekomme høye sikkerhetsstandarder og prøves gjennom sertifiseringskontroller av en egnet sikkerhetsmyndighet for å sikre at både overvåkedes og politiets datasystemer ikke gjøres sårbare for angrep og misbruk fra tredjeparter, eller at kommunikasjonen mellom overvåkedes datasystem og politiet gjøres tilgjengelig for uberettigede tredjeparter.

Data bør holdes innenfor norsk jurisdiksjon

Erfaringer fra Tyskland viser at bruken av dataavlesning kan gjøre kommunikasjonen mellom den overvåkedes datasystem og politiet sårbar for overvåkning fra tredjeparter i andre land, f.eks. fremmede politi- og sikkerhetstjenester. Denne problemstillingen er ikke adressert i proposisjonen.

Det er viktig at overvåkningsvirksomheten til norsk politi er underlagt norsk lov og oversees av norske tilsynsorganer. Så langt det er mulig, bør dataavlesningen derfor ikke benytte seg av teknisk infrastruktur i andre jurisdiksjoner.

Kontroll og tilsyn av og med teknologien

Proposisjonen definerer dataavlesning svært bredt. Da er det desto viktigere at kontrollorganene kan utøve et robust og effektivt tilsyn med bruken.
Erfaringer fra Tyskland viser imidlertid at det kan være utfordrende å føre kontroll med en teknologi som har så bred funksjonalitet.

Proposisjonen fremholder at notoritet med hensyn til hvilke skritt politiet har tatt, er en forutsetning for å sikre tilfredsstillende kontroll.[7] Her bør det vurderes om dataavlesningsverktøy kan utformes slik at kontrollorganene automatisk får tilgang til en logg over alle operasjoner gjennomført med slike verktøy.

Det bør også vurderes om tilsynsorganene skal kunne ta kildekoden i ettersyn, særlig om det benyttes kommersiell hyllevare som ikke er underlagt et uavhengig kontrollregime.

[7] Prop. 68 L (2015-2016) Endringer i straffeprosessloven mv. (skjulte tvangsmidler), s 272