Til Retsudvalget, Folketinget

Fra Stephan Engberg, Priway ApS
Stengaards Alle 33 D
2800 Kgs. Lyngby

30. marts 2006

Vedr.: Kriminalitetsskabende effekter i Anti-terror pakken.

Jeg er blevet opfordret til at komme med input til Retsudvalget med henblik på at udbede ministeren kommentar. Med ydmyghed overfor en kompliceret problemstilling følger:

Med baggrund i mange års arbejde med hvordan vi sikrer informationssamfundet og deltagelse i sikkerhedsforskning på EU-plan ser jeg grund til at rejse nogle flag før man med lov kræver noget, som er teknisk umuligt og rammer uskyldige hårdest. Anti-terror pakken vil efter min bedste vurdering virke destruktivt for formålet og på vitale samfundsinteresser.

Specielt gør jeg høfligst opmærksom på at sporings- og aflytningskravet i anti-terror pakken efter min bedste vurdering er både meningsløst og virker kriminalitetsskabende.

Tillad mig at underbygge dette.

a) Terrorister og seriøse kriminelle kan altid anonymisere deres kommunikation.

Man kan ALTID sende en stærkt krypteret besked over en usikret linje. Reelt medfører aflytningskravet at man skal kunne bryde krypteringen bag Digital Signatur, hvilket både er meningsløst og yderst selvdestruktivt. Det vil f.eks. umuliggøre såkaldt non-repudiation, dvs. muligheden for at frasige sig ansvar.

Anonym kommunikation er nem og tilgængelig for ikke-teknikkere. F.eks. eksemplificeret ved open source anonymiseringsnetværket TOR[1] - TOR er dog kun tiltænkt at gøre sikkerhed tilgængelig for almindelige borgere, dvs. TOR er ikke problemet.

De tunge kriminelle opererer deres egne netværk, som de givetvis også vil eller allerede lejer ud til andre på samme måde som man kan leje spamnetværk af angrebne computere – de såkaldte botnet. Der er profitabel forretning i at professionelle kriminelle stiller kommunikationsfaciliteter til rådighed for anden kriminalitet og herunder terrorisme.

Det helt fundamentale budskab er, at man næppe kan forhindre anonym kommunikation - det bliver og er måske allerede 100% trådløst og helt uafhængigt af central infrastruktur.

b) Hvis man kræver mulighed for identificeret sporing og aflytning, så blokerer det for nødvendige sikkerhedstiltag til at beskytte legitim kommunikation såsom kommercielle og offentlige transaktioner.

Hvis det skulle være undsluppet nogens opmærksomhed, så er sikkerheden i de elektroniske netværk ringe. Sikkerheden er desuden for nedadgående i takt med at man kobler systemer og databaser sammen og gør alting mere sårbart – risici akkumulerer.

[1] http://tor.eff.org

Heri kan indskydes, at bagdøre ikke kan sikres – hvilket bedst illustreres ved aflytningen af den græske premierminister og store dele af den græske politiske og sikkerhedsmæssige elite[2] med mobiltelefonens indbyggede aflytningsudstyr samt hackernes succes med at trænge ind i selv de helligste haller (f.eks. de amerikanske pinkode databaser[3]).

Vi arbejder indenfor EU sikkerhedsforskningen med at løse disse problemer og har generelt værktøjer til rådighed til at komme meget langt med at sikre borgerne og virksomhederne. Men det er komplekse problemstillinger, som kun kan løses, hvis man går væk fra kravet om konstant identifikation og central kontrol. Se f.eks. i2010/Trust in the Net[4] afholdt under Østrigs EU-formandskab for mere information.

Anti-terror pakken vil med de krav, der stilles om konstant sporing og aflytning, gøre det umuligt for lovlydige sikkerhedsleverandører at indføre de kritiske sikkerhedstiltag for at kunne sikre og beskytte de legitime og samfundskritiske kommercielle og offentligt relaterede transaktioner og kommunikation. Risikoen er dermed at It-kriminaliteten vil fortsætte med at vokse ukontrollabelt.

Konklusion:

Nettoeffekten vil dermed gøre det nemmere for kriminelle med anonym beskyttelse at begå kriminalitet mod stadigt mere sårbare borgere og virksomheder.

I næste række vil de kriminelle via identitetstyveri[5] nemt kunne angribe og underminere sikkerheden i centrale systemer. En problemstilling, der generelt er i færd med at underminere sikkerhedsmodellen i f.eks. Digital Forvaltning[6]. Identitetstyveri er en stærkt profitabel og voksende form for kriminalitet, hvor kun ca. 1 ud af 700 tilfælde opklares[7].

Konsekvensen er hvad man kan kalde "Falsk Transparens", dvs. svækker sikkerheden hos ofrene og gør dem "gennemsigtige", mens det styrker de kriminelle og andre magtfulde. Til ofrene hører også virksomheder, som ikke kan konkurrere eller beskytte sig uden mulighed for at holde information fortrolig. I en sådan verden eskalerer kriminaliteten ud af kontrol og samfundsøkonomien herunder almindelig handel belastes voldsomt.

Det er min personlige opfattelse, at selvom vi umuligt kan garantere at alle borgere bruger dem, så kan vi pålægge og lave kommunikationsværktøjer til lovlydige borgere med præcis de balancehensyn, som man politisk bliver enige om – vi kan f.eks. i dag lave Digitale anonyme kontanter, der er beskyttet mod tyveri og pengehvidvask[8]. Men hvis de politiske balancehensyn ikke tager højde for borgernes identitets- og datasikkerhed, så vil en stadig større del af kommunikationen blive tvunget over i de ukontrollerbare grå net.

Hvis hensynet til et stabilt demokrati, anti-kriminalitet og samfundsøkonomien skal vinde må vi ændre sikkerhedsforståelse fra overvågning og central kontrol af al kommunikation til at sikre ansvarligheden via borgernes selv-beskyttelse, dvs. sikre kommunikationsmodtager værktøjer til at sætte vilkårene og beskytte sig mod kommunikationsafsender.

---

[2] www.theregister.co.uk/2006/02/06/greece_mobile_snooping_scandal/

[3] bankwatch.wordpress.com/2006/03/12/pin-scandal-worst-hack-ever-citibank-only-the-start/

[4] www.egov2006.gv.at/Trust_in_the_Net.html

[5] www.ft.dk/samling/20041/almdel/REU/Bilag/76/117497.PDF

[6] crossroadscopenhagen.dk/Nyheder/Nyhedsarkiv/Pressemeddelelse_Dansker_baner_vejen_for_fremtidens_sikkerhedsstandarder

[7] swami.jrc.es/pages/Conference2006.htm

[8] www.cisco.com/web/learning/le21/le34/downloads/689/nobel/2005/docs/Stephan_Engberg2.pdf