SINTEF Konsernstab
Postadresse:
Postboks 4760 Sluppen
7465 Trondheim

Besøksadresse:
Strindvegen 4
7034 Trondheim

Sentralbord: 73593000
Direkte innvalg: 45218102
Telefaks: 73594302

Foretaksregister: NO 948 007 029 MVA

Forsvarsdepartementet
Postboks 8126 Dep.
0032 Oslo

Deres ref.:	Vår ref.:	Prosjekt / Sak:	Dato
Deres ref	Vår ref	2016/2699	2017-01-09

Høringsuttalelse fra SINTEF vedr. Digitalt grenseforsvar

Som en av landets sentrale bidragsytere innen forskning på digitale teknologier og IKT-sikkerhet, takker SINTEF for muligheten til å gi tilbakemelding på rapporten fra Lysne II-utvalget om Digitalt grense-forsvar (DGF).

Digitalisering – av mange blinket ut som bærebjelken for fremtidens verdiskaping – er et av SINTEFs hovedsatsingsområder. I flere år har vi brukt Big Data, Internet of Things og kunstig intelligens til å lage nye og innovative løsninger for norske bedrifter og myndigheter.

Parallelt har vi i en årrekke drevet forskning også innenfor IKT-sikkerhet, blant annet med prosjekter viet kritisk IT-infrastruktur, risikovurderinger og personvern. Som største bidragsyter innen IKT-sikkerhet i EUs 7ende rammeprogram for forskning, opplever vi at vi har internasjonalt ledende innsikt.

Vårt syn i kortversjon

Lysne II-utvalget anser DGF som nødvendig for nasjonens sikkerhet og anbefaler innføring av DGF som beskrevet i rapporten. SINTEF er enig i at E-tjenesten har behov for økt innsyn i kommunikasjon over landegrensene i takt med den teknologiske utviklingen. For oss ser det imidlertid ut til at fordelene ved systemet ikke oppveier ulempene:

- Masseovervåking "ved landegrensen" blir en gigantisk håv som samler all slags datatrafikk til og fra uskyldige norske borgere. Nordmenn sender nemlig daglig store mengder data til utlandet gjennom bruk av sosiale medier, meldingstjenester, nettbetaling, og ikke minst skytjenester for datalagring. I forslaget som utvalget går for, er det kun juridiske og tekniske restriksjoner som vil hindre at E-tjenesten får tilnærmet uinnskrenket innsyn i nesten all datatrafikk mellom norske borgere.

- Samtidig vil den foreslåtte "håven" ha store hull for de som har onde hensikter og i tillegg er digitalt kompetente. Det vil derfor være fullt mulig å omgå DGF for den som virkelig ønsker det og har kompetanse.

- Vi risikerer i tillegg at mange aktører i samfunnet ikke tar i bruk viktige og helt legitime tjenester fordi brukerne ikke ønsker å bli overvåket. I så fall trues digitaliseringen av samfunnet og

dermed også de tilhørende mulighetene for verdiskapning. Et digitalt klasseskille kan oppstå, mellom de som klarer å omgå statlig overvåking og de som ikke gjør det.

Vi synes derfor det er grunn til å gjenta konklusjonen som 22.juli-kommisjonen trakk i sitt kapittel "Om åpne kilder og overvåking av Internett":

"Vi er ikke overbevist om at verdien av å overvåke generell trafikk på nettet ved bruk av søkeord oppveier den demokratiske omkostningen ved slik overvåking av den alminnelige meningsutveksling."

Rapporten burde etter vårt syn beskrive og drøfte alternative og mer treffsikre tiltak som kan gjøre Norge tryggere. I SINTEF har vi ikke gjort noen helhetlig analyse av tiltak som eventuelt kunne erstatte DGF. Men i høringsuttalelsen peker vi på noen muligheter.

Med DGF vil nordmenn oppleve at all kommunikasjon kan overvåkes

E-tjenesten har et legitimt behov for å samle inn og bearbeide informasjon for å kunne løse sitt oppdrag. Adgangen til innhenting av opplysninger begrenses av paragraf 4 i "Lov om Etterretningstjenesten" (E-loven) som sier: "Etterretningstjenesten skal ikke på norsk territorium overvåke eller på annen fordekt måte innhente informasjon om norske fysiske eller juridiske personer".

Det utvalget foreslår, er på mange måter å videreføre tradisjonell grensekontroll til den digitale verden. Men når DGF i tråd med forslaget vil avlytte trafikk som går til og fra utenlandske servere, ser den inn i mange nordmenns digitale rom. DGF, som foreslått av utvalget, har i realiteten kapasitet til å samle inn *all* informasjon som fysisk flyttes over landegrensen gjennom bruk av blant annet sosiale medier, meldingstjenester, nettbetaling, og ikke minst skytjenester for datalagring.

Om to norske borgere, som begge sitter i Norge, deler et dokument i den såkalte skyen, innebærer dette ofte bruk av en lagringstjeneste som er plassert i utlandet, slik at DGF potensielt kan lese dokumentet idet det passerer landegrensa. I realiteten må norske borgere og bedrifter legge til grunn at *all* bruk av nettbaserte tjenester kan bli overvåket gjennom DGF. Derfor mener vi at begrepet "grensekontroll" er lite treffende.

Utvalget foreslår en rekke juridiske og tekniske restriksjoner som skal hindre at kapasiteten til DGF brukes på en måte som bryter loven. Men disse restriksjonene kan bli utsatt for press fra flere hold, noe utvalget selv påpeker. Det å bygge kapasitet for så omfattende inngrep i norske borgeres private sfære, reiser i seg selv alvorlige, prinsipielle og etiske spørsmål.

I tillegg risikerer vi at kunnskapen om DGF fratar borgere og bedrifter lysten til å ta i bruk viktige og helt legitime, digitale tjenester fordi de ikke ønsker å bli overvåket. En slik nedkjølingseffekt er en reell trussel mot den digitale omstillingen av samfunnet, og dermed også mot mulighetene for verdiskapning som ligger i digitalisering. Dessuten kan det oppstå et digitalt klasseskille mellom de som er i stand til å omgå statlig overvåking, og de som ikke er det.

SINTEF

Et grenseforsvar med hull for de med onde hensikter

DGF vil riktig nok ha mulighet til å se omfanget av ikke-målrettede cyberangrep som rettes mot hele Norge. Mot slike angrep vil DGF derfor gjøre det mulig å iverksette blokkerende tiltak. Målrettede cyberangrep, derimot, kan fremdeles foregå på en måte som ikke lar seg fange opp av masse-overvåking.

En angriper kan fortsatt ringe virksomheten og få en ansatt til å gi bort passordet sitt, eller bruke andre metoder basert på sosial manipulering. Hver enkelt virksomhet må derfor ta ansvar for systematisk arbeid med cyber- og informasjonssikkerhet for å beskytte sine interesser.

Det er en kjent sak at trusselaktører i stadig større grad kommuniserer over krypterte kanaler. Et DGF som foreslått vil ha mulighet til å inspisere også kryptert trafikk. Til enhver tid vil det imidlertid finnes kryptering som det ikke er mulig å knekke. Det er all grunn til å tro at trusselaktører vil ta i bruk nye metoder for å kunne kommunisere risikofritt. DGF vil dermed kunne bli en mur med hull for de som har onde hensikter og i tillegg er digitalt kompetente. Dette vil redusere verdien av DGF.

Hele hensikten med kryptering for legale formål vil dessuten falle gjennom hvis nasjonale aktører skal ha en vedtatt rett til å bryte den. Et DGF med rett til innsyn i kryptert trafikk, kan tvinge norsk næringsliv samt forsknings- og innovasjonsmiljøer til å skaffe seg kostbare omveier i jakten på sikre kommunikasjonsløsninger. I tillegg risikerer vi at noen brukere vil unngå enkelte digitale tjenester på grunn av manglende tillit. Da vil digitaliseringen av samfunnet lide.

Usikkert vern ved maktovertakelse

Rapporten nevner dessuten at DGF som foreslått kan fungere med dagens demokratiske styresett, men ikke ved en eventuell ikke-demokratisk maktovertakelse. Utvalget antar at implementerte kontrollmekanismer av typen "slett alt materiale" kan tas i bruk i sistnevnte tilfelle.

Vi mener imidlertid det er på sin plass å minne om at en slik maktovertakelse kan skje raskt. Det vil si hurtig nok til at samfunnet ikke rekker å iverksette tiltak som hindrer misbruk av DGF og innsamlet informasjon. Det å sikre seg kontroll over denne typen informasjon, kan i seg selv være et viktig strategisk tiltak for de som eventuelt tar over makten.

Alternative tiltak må utredes

Med de betenkelighetene som er beskrevet overfor, mener vi det vil være hensiktsmessig å legge mer vekt på å få utredet alternative og mer målrettede tiltak for å beskytte Norge ikke bare mot terror, men også mot cyberangrep.

I SINTEF har vi ikke gjort noen helhetlig analyse av mulige alternativer til DGF. Men vi merker oss at rapporten, i en drøfting av forebyggende tiltak, nevner sensorene som NSM plasserer ut hos enkeltvirksomheter (såkalte VDI-sensorer).

Ett mulig alternativ til DGF kunne være å utplassere mange flere slike sensorer hos virksomheter som har særlig verdifulle ressurser. I dag koster det penger for virksomhetene å delta i VDI-nettverket. Det

kan vurderes om "medlemskapet" skal gjøres mye rimeligere, eventuelt kostnadsfritt. For dette ville være et sikkerhetstiltak på nasjonalt nivå. Angrep på nasjonale interesser vil nemlig ofte ramme et mindre eller et større utvalg av virksomheter som utgjør kritisk infrastruktur.

Risiko for falsk mistanke

Med DGF vil E-tjenesten besitte enorme datamengder som vil bli analysert på ulike nivåer og ved ulike tidspunkt. Dataanalyse som fagfelt er ennå ikke modent. Vår erfaring er at det er krevende å oppnå nyttige resultater ut ifra store datamengder, og muligheten for falske alarmer og falsk mistanke er derfor definitivt tilstede.

Dataanalyse har dessuten store kostnader. Men kostnadsbildet knyttet til DGF er ikke vurdert av Lysne II-utvalget.

Konklusjon

Vi forstår behovet for å vurdere innføring av DGF i Norge. Rapporten fra Lysne II-utvalget inneholder mange gode refleksjoner og fakta. Men SINTEF mener at utvalgets vurdering likevel ikke er grundig nok. *Alternative tiltak* har heller ikke vært vurdert i sterk nok grad. All den stund vi også ser en rekke uklarheter og svakheter ved de foreslåtte kontrolltiltakene, mener vi at DGF ikke er riktig vei å gå.

Med vennlig hilsen

Morten Dalsmo

Morten Dalsmo
Konserndirektør, SINTEF Digital