Norges nasjonale toppdomener og personvern

HØRINGSSVAR FRA UNINETT NORID AS

Som vi nevnte på selve høringen så mener vi at dette primært dreier seg om hvordan man kan sikre tjenester, og at utgangspunktet bør være "hvordan kan vi sikre økt kontroll og råderett over egne data for norske brukere".

Bruk av et toppdomene kontra et underdomene under .no (eller for den saks skyld en sertifiseringsordning for tjenester direkte under .no) er etter vår mening noe som må avgjøres basert på en ren kost-nyttevurdering. Det vil være sentralt å skaffe seg oversikt over markedet, både blant tjenesteleverandører som skal selge "sikre" tjenester, og blant forbrukere som potensielt skal kjøpe disse tjenestene. I tillegg må man se på kostnadene ved de forskjellige løsningene, opp mot det potensielle markedet man mener man har.

Vi savner at man ser på alternative måter å oppnå sikrere tjenester og større kontroll over egne data for brukerne og sammenlikner disse for å finne den løsningen som best dekker behovene til de ulike aktørene Alternativer som: en merkeordning for web-steder, en spesiell sertifikatutsteder som sertifiserer tjenestene før sertifikater utstedes, bruk av ordinær markedsføring for å tiltrekke seg kunder til en sikrere tjeneste osv. Noe av det sentrale må være å vurdere hvilke krav som tjenesteleverandørene ønsker å levere tjenester innenfor. Dersom man setter krav til plassering av maskiner, eller til koblinger mellom tjenester som begrenser innovasjon i tjenestene som kan tilbys så har man neppe oppnådd hensikten.

* Kontroll av tjenester opp mot kravene.

Utfra det som har vært sagt til nå skal det stilles en del krav til tjenestene som leveres til brukerne. Det går både på oppførselen direkte mot brukerene (f.eks. forby setting av tredjepartscookies, kreve kryptert forbindelse), på hvordan tjenesten er implementert (f.eks. at data lagres i Norge) og på hvilken bruk av brukerdata som er tillatt (f.eks. ikke selge brukerdata videre til tredjepart.).

Det er kun de av egenskapene til tjenesten som er direkte synlige overfor brukerne og brukerens egen programvare som vil kunne kontrolleres maskinelt. Dette finnes det også verktøy for å gjøre, for noen type tjenester, eller en kan lage egne som er bedre tilpasset regelsettet en ønsker å operere under.

Forutsetningen for at en kan gjøre kontroll av dette er at en kjenner tjenesteadressen og protokollen som brukes. Ut av DNS kan en finne annonserte tjenester som f.eks. e-postkontor o.l. En kan også forsøke velkjente navn som f.eks. www.domene.tld eller ftp.domene.tld, og anta noe om hvilken type tjeneste som måtte tilbys fra disse. En kan vanligvis ikke finne en komplett liste over hvilke tjenester som tilbys

ut fra en gitt grein i DNS. Dersom det tilbys en tjeneste fra et ikke-gjettbart navn, f.eks. et-vanskelig-navn.domene.tld, (og merk, tjenesten kan f.eks. tilbys gjennom en app på brukerens mobile enhet, og trenger ikke være tilgjengelig gjennom f.eks. en web-leser) og en ikke "kommer over" dette navnet, så vil en ikke kunne teste egenskapene til tjenesten. Det kan også hende at tjenesten leveres over en protokoll definert av tjenestetilbyderen selv, og da vil den vanskelig kunne kontrolleres av utenforstående.

Gjennom kun å kontrollere brukergrensesnittdelen av tjenesten kan en ikke kontrollere bakenforliggende egenskaper. For å kunne si noe om f.eks. hvor data er lagret eller hvem som har tilgang må en studere hvordan tjenesten er implementert. Og da trenger en tilgang til leverandørens utstyr, programvare, organisasjon og avtaleverk. Dette er typisk en jobb for sertifiseringsorganer og IT-revisorer.

* Regulering av tjenester.

Et av problemene ved å bruke et TLD som avgrensning for egenskaper ved tjenestene er at det vil omfatte alle tjenester en registrant tilbyr/bruker. Noen av disse kan være bi-tjenester, dvs. støttetjenester som sluttbrukerne sjelden eller aldri bruker, men som likevel er nødvendige eller ønskelige for å kunne implementere hovedtjenesten. Det er ikke gitt at det er hensiktsmessig at disse har samme krav til seg som hovedtjenestene til brukerne.

Det er også vanlig at en under produksjon av tjenester benytter seg av tredjeparter til å utføre deler av oppgavene. F.eks. kan en ha en avtale med en leverandør av en distribusjonsnettjeneste (CDN) om framskutt plassering av innhold for distribusjon til brukerne. Dette for å gi rask respons for brukerne samt økt totalt transportkapasitet for innholdet. For noen tjenester vil innholdet være eller inneholde persondata. En tjenesteleverandør under det foreslåtte regimet vil da ikke kunne benytte slike leverandører, og vil levere en kvalitetsmessig dårligere tjeneste enn en som kan skyve ut innhold slik at det ligger nært sine australske brukere (f.eks.).

Mange nye tjenester øker attraktiviteten ved å koble seg sammen med andre tjenester. F.eks. ved å operere med samme kundedatabase, bruke felles autentiseringstjeneste, krysslenke til egen tilstedeværelse i andre tjenester, eller tillate brukerne å dele innhold på tvers av tjenester. Deler av dataflyten i slike integrerte tjenester vil kunne være persondata, og det er ikke klarlagt hva tjenesteleverandører som faller inn under den foreslåtte reguleringen kan gjøre med data som mottas fra tjenester som ikke faller inn under reguleringen, eller hva en kan dele ut til andre tjenester. Dersom en må ha (informert) samtykke fra brukerne i tillegg til standard brukeravtale (som en ønsker felles for alle tjenester under reguleringen) vil noe av vitsen med standard brukeravtale være borte.

Er det en ting en må regne med er at det vil komme til nye tjenester på Internett. Noen vil produseres vha. kjent teknologi, mens andre vil bli bygget med nye protokoller og implementasjoner. Det å regulere framtiden for detaljert vil lett kunne hindre nye tjenester i å bli tatt i bruk. Alternativet er å stadig måtte endre/tilpasse regelverket, og det er igjen uheldig for de som allerede har bygget opp tjenester.

* Finansiering av tjenestene.

Mange av dagens populære tjenester er eller har startet som gratis-tjenester. Driften finansieres ofte gjennom rettet markedsføring mot brukerne, ved å knytte seg opp mot et av de eksisterende annonsenettverkene. Dersom det blir mye vanskeligere å skaffe inntekter gjennom å "selge brukerne" (og deres informasjon) vil det være nærliggende å tro at sluttbrukerne selv må betale for tjenestene. Det er etter vår mening svært uklart om det er betalingsvilje i sluttbrukermarkedet til å finansiere tjenestene.

For noen tjenester som drar nytte av nettverkseffekten (dvs. dess flere som bruker tjenesten, dess mer attraktiv blir den), så vil noen ønskelige krav til tjenestene kunne virke ekskluderende, slik at det vil bli brukere som ikke kan bruke tjenesten (tenkt eksempel: krav om kryptering av flerparts videokonferanse vil gjøre utstyr dyrt).

* Manglende kontroll med sluttbrukerutstyr.

Sikkerhetsproblemer i tilknytning til Internettbaserte tjenester skjer faktisk oftest i sluttbrukerenden. Er det meningen at dette skal falle inn under reguleringen?

* Tilgjengelighet og forvaltning

Et sentralt poeng i administrasjonen av .no per i dag er sikker autentisering av søkeren (abonnenten). Dette er en trend som stadig flere av de europeiske registerenhetene ønsker å følge, og som spesielt påtalemyndigheter er opptatt av. For .no gjøres autentisering i flere ledd.

- Norids registrarer (domeneforhandlere) er pliktig til å kontrollere at søkeren er representert ved den personen som har kontaktet registraren, og at denne kontaktpersonen har de nødvendige fullmakter. Søkeren må oppgi enten et organisasjonsnummer i BRREG eller et personnummer (anonymisert) ved søknad om domenenavn, og Norid sjekker maskinelt at nummeret faktisk eksisterer i de aktuelle registrene og at navnet som er oppgitt på søker matcher dataene. Norid gjennomfører jevnlig vask av kunderegisteret (også maskinelt) for å sjekke om grunnlaget for registrering fremdeles er tilstede.

- Dersom man åpner for søkere utenfor Norge og skal opprettholde datakvalitet og sikkerhet i samme grad som for .no trenger man en måte å få autentisert søkeren. For mange europeiske land kan oppslag i European business register være en mulighet (dekker 23 land), men dette gjelder kun firma. Man har ikke gode løsninger for privatpersoner. Dersom det skal være mulig å søke fra hele verden blir bildet enda mer komplekst. Det må avgjøres hva slags dokumentasjon som skal være tilstrekkelig for hvert enkelt land. Det manuelle arbeidet ved å feks autentisere kinesiske søkere vil være betydelig, og kostnadsnivået deretter.

* Økonomi og marked

Oppstartskostnader for .sj som et "regulært" toppdomene er i en

forretningsanalyse estimert til å ligge på 12 – 13 millioner kroner. Dette inkluderer ikke nødvendig markedsføring for å gjøre toppdomenet til et salgbart produkt, da dette er sterkt avhengig av den valgte strategien for domenet.

Driftskostnader vil også være avhengig av hvilke regler som blir valgt:

- Autentisering av utenlandske søkere vil øke kostnadsnivået, på den annen side er det kanskje ikke nok interesse i det norske markedet i seg selv
- datavask av data fra utenlandske søkere vil øke kostnadsnivået
- drift av sertifiseringsordningen som skal sjekke at tjenester oppfyller de kravene som stilles må dekkes
- drift av en klageordning
- drift av kundesenter, informasjon, kundehåndtering
- drift av en registrarordning (krav til registrarer ihht Domeneforskriften)