Fra: Thomas Gramstad <thomas@efn.no>
Sendt: 3. januar 2017 00:23
Til: Postmottak KUD
Kopi: styret@efn.no
Emne: EFNs høringsuttalelse om Forskrift for offentlige arkiv 2017 (fwd)

Elektronisk Forpost Norge (EFN)
CSS postboks 42
Middelthunsgate 25
0368 Oslo

HØRINGSUTTALELSE FRA ELEKTRONISK FORPOST NORGE OM NY "FORSKRIFT OM OFFENTLEGE ARKIV (ARKIVFORSKRIFTA)".

Jfr.
https://www.regjeringen.no/no/dokumenter/hoyring--ny-forskrift-om-offentlege-arkiv/id2515364/

Fra høringsnotatet side 6:
https://www.regjeringen.no/contentassets/3910ae06793244729c4ae0eba8e418ef/hoyringsnotat-forslag_til_ny_arkivforskrift.pdf

"Departementet ber om høyringsinstansanes syn på om det er ønskjeleg at det blir opna for skylagring, og på kva som eventuelt er formålstenlege løysingar."

Problemet mht. informasjonssikkerhet ved skylagring er undervurdert av norske myndigheter. Blant våre medlemmer er det mange med betydelig IKT-kompetanse, som er svært skeptiske til skytjenester.

Den foreslåtte § 22 i arkivforskriften åpner for at sensitive personopplysninger, som f.eks. pasientjournaler i aktiv bruk, kan skylagres i utlandet. Har ikke norske myndigheter lært noe av Snowden-saken? Selv ikke NSA klarer å holde på sine hemmeligheter, hvordan kan de da tro at skylagring skal være sikret mot utro tjenere eller datainnbrudd i utlandet?

Som det heter i et kjent slagord: "Det finnes ingen sky, bare andre menneskers datamaskiner".

UNNGÅ SKYLAGRING AV DATA OG PERSONOPPLYSNINGER SOM ER SENSITIVE

Vi mener det ikke bør åpnes for skylagring i det offentlige, hverken innenlands eller utenlands. Slike store honningkrukker virker tiltrekkende på personer med tvilsomme hensikter. Det beste er derfor lokal, desentralisert lagring. Med stor spredning av opplysningene er skadepotensialet betraktelig mindre om det først forekommer et datainnbrudd. Det må selvsagt stilles strenge sikkerhetskrav i lov og forskrift selv om lagringen skjer lokalt hos det enkelte offentlige organ.

Se Kjersti Toppes spørsmål om dette temaet til helse- og omsorgsminister Bent Høie:

https://www.stortinget.no/no/Saker-og-publikasjoner/Sporsmal/Skriftlige-sporsmal-og-svar/Skriftlig-sporsmal/?qid=66239

"I NRK-nyhetene 2. september kommer det frem at Helse Sør - Øst anbefaler å flagge ut datasystemet til Helse Sør- Øst til amerikansk IT-selskap. Tillitsvalgte frykter helsedata på avveie og tap av viktig kompetanse i Norge.

Sofie Nystrøm, direktør ved NTNU Center for Cyber and Information Security, har skrevet en kronikk på NRK Ytring 19. november 2016 som omhandler problemene med outsourcing av IKT-tjenester. Denne anbefaler vi å lese:
https://www.nrk.no/ytring/hvem-skal-sitte-med-_atomkodene_-vare_-1.13232673

(Sitat:)

Det er ikke likegyldig hvem som sitter med tilgang til persondata, helsedata, og tilgang til å styre samfunnets grunnleggende infrastruktur. Men det skulle man tro, siden sikkerhetslovgivningen for grunnleggende samfunnsfunksjoner er hullete som en helsetrøye.
Både menneskelig feil og ondsinnede handlinger er utenfor norsk kontroll. Og det er vi som lar det skje.
[…]

Det er ikke praktisk mulig å drifte IT-løsninger uten vide tilganger som gir innsyn i data på systemene som kan utgjøre kritisk informasjon som helsedata, data om kritiske infrastrukturer og konti-opplysninger. Da vil man ikke at personer i land som man er usikre på relasjonene til skal kunne ha fullt innsyn i sensitive data i Norge, og kunne påvirke Norge i en konflikt. Eller at en medarbeider skal kunne la seg presse til å selge viktig informasjon om meg eller Norge.

(Sitat slutt)

ANDRE ULEMPER VED SKYTJENESTER

Avhengighet av internettforbindelsen, rigide avtalevilkår, reduserte muligheter til å tilpasse tjenestene til det enkelte offentlige organs behov, mindre åpenhet og kontroll med IKT-systemene -- og leverandørinnlåsing, som innebærer at det kan være vanskelig å flytte innholdet til en annen skyleverandør, eller tilbake til lokal lagring, grunnet f.eks. proprietær programvare. Og hva sier avtalevilkårene om tap av data, datainnbrudd og konkurs hos skyleverandøren?

For å omgå noen av disse problemene, må arkivet lagres lokalt i tillegg til skylagringen. Men da vil det heller ikke være noen økonomisk fordel med skytjenester. Som i tillegg kan ha skjulte kostnader, f.eks. opplæring av brukerne, herunder også opplæring i avtalevilkårene, som brukerne må lese og forstå. Det å lagre et arkiv i sin helhet på ulike steder vil også øke risikoen, hvis det betyr at flere har tilgang.

DATA OG VERKTØY MÅ EIES OG KONTROLLERES LOKALT

EFN ser at maskinene for lokal lagring bør ha muligheten til å bli oppkoblet mot nettet. Men oppkobling til nettet må aldri være en forutsetning for å bruke IT-verktøyene. Vi ønsker lokalt eierskap og kontroll over både IT-verktøyene og dataene. Det ligger i sakens natur at skyløsningsteknologier som innebærer

at programvaren ligger på nett og ikke kan hverken kopieres, installeres eller brukes lokalt, aldri kan eies eller kontrolleres av brukeren, i dette tilfelle offentlige etater.

Dersom man tar hensyn til både sikkerhet og resiliens/robusthet/uavhengighet av oppkoblinger må maskinene være bestykket med nettuavhengig lokal programvare -- men samtidig også kommunikasjons/oppkoblingsmuligheter.

EKSTRA BACKUP I SKYEN?

Bruk av skylagring som ekstra backup for informasjon som ikke er sensitiv eller personvernkrenkende, samt for sluttbrukerstyrt backuplagring (selv om dataene er sensitive).

Dersom informasjonen ikke er sensitiv eller personvernkrenkende, ser EFN ikke noen problemer med ekstra backup i skyen (så lenge det ikke er hovedarkiv/eneste backup).

Tilsvarende gjelder for persondata selv om disse er private eller sensitive, dersom personen(e) selv aktivt velger å ha eller akseptere ekstra backup i skyen. Helst bør alle innbyggerne kunne velge dette på forhånd, på lignende måte som innbyggerne kan velge mellom elektronisk selvangivelse eller papirbasert selvangivelse.

SKYEN MÅ ALDRI VÆRE ENESTE ALTERNATIV

Et moment her er at markedskrefter ønsker å lansere skylagring ikke som et supplement, men som eneste alternativ - slik at vanlige mennesker ikke skal kunne lagre sine egne data lokalt.
Skylagring markedsføres helt klart med tanke på å være eneste løsning. Dette er meget farlig, og her har vi en parallell til Pamela Samuelson's berømte utsagn om at 'hovedpoenget med DRM ikke er å hindre folk i å kopiere. Hovedpoenget med DRM er å endre folks forventninger og begreper rundt hva de kan gjøre med digitalt innhold.'

På samme måte fyller nettbasert lagring og i enda høyere grad nettbasert programvare en tilsvarende funksjon: Å endre menneskers oppfatning om hvordan og hvem som skal lagre våre data, og å endre menneskers oppfatning fra at dataprogramvare skal være noe som brukerne kan kopiere, installere og re-installere til å være et objekt som bare tilbys som en abonnementstjeneste og som ikke kan hverken kopieres, re-installeres eller migreres - når man slutter å betale leien eller tjenesten blir utilgjengelig eller opphører får man ikke tak i sine data og kan heller ikke skape nye data.

HENSIKTSMESSIG SKYLAGRING

Det er når data skal være tilgjengelige og deles med andre at skylagringen virkelig kommer til sin rett. Dette kan skje enten ved at dataene er nedlastbare for alle eller et utvalg personer som har tilgang, eller det kan skje ved at dataene kan skrives til og endres i samarbeid mellom flere. I begge tilfellene ligger dataene i skyen, og poenget er at de ligger i skyen fordi de skal være tilgjengelige for andre.

UHENSIKTSMESSIG SKYLAGRING

Ved skybaserte løsninger outsourcer det enkelte offentlige organ alt det har, og alt innhold er potensielt tilgjengelig via Internett.

I dokumenter fra regjeringen, som Nasjonal strategi for bruk av skytenester (Kommunal- og moderniseringsdepartementet, 2016), er skylagring omtalt ukritisk, og problemene er ikke i tilstrekkelig grad drøftet og tatt på alvor.

Riksantikvaren har omtalt skylagring utenlands slik:
http://arkivverket.no/arkivverket/Arkivverket/Om-oss/Aktuelt/Nyhetsarkiv/Nyhetsarkiv-2014/Riksarkivaren-seier-nei-til-skyarkivering-i-utlandet

"At arkivmaterialet er tilgjengeleg frå Noreg via Internett er etter vårt skjønn ikkje tilstrekkeleg, fordi det ikkje vil gi god nok kontroll, med ei rekkje risikofaktorar. Etter vårt syn stiller arkivlova krav om at arkivdatabasen skal vere lagra og tilgjengeleg på server som er fysisk plassert i Noreg."

I forbindelse med høringen om "digitalt grenseforsvar", foreslås det at etterretningstjenesten skal kunne avlytte all informasjon som går gjennom fiberkabler inn og ut av landet. Dette må også vurderes som en risikofaktor. I tillegg vil det være andre lands etterretningstjenester som gjør lignende inngrep. Jfr. https://www.regjeringen.no/no/dokumenter/horing-av-rapport-avgitt-av-lysne-ii-utvalget-om-digitalt-grenseforsvar/id2513635/

KOSTNADER IKKE AVGJØRENDE

Når det gjelder kostnader, bør disse ikke være avgjørende for valg av arkiveringsløsning. Informasjonssikkerheten må alltid komme først. Flere vil bli skeptiske til å oppsøke og til å avgi sensitive opplysninger til f.eks. helsepersonell hvis dette skal skylagres.

Kort oppsummert: Vi sier nei til norsk og utenlandsk skylagring av sensitive data og personopplysninger fra/hos det offentlige.

Med vennlig hilsen for EFN,

Thomas Gramstad
thomas@efn.no
(styreleder)

Oslo, 2. januar 2017