Sandvika, 18. september 2013

Fornyings-, administrasjons- og
kirkedepartementet
Postboks 8004 Dep
0030 Oslo

Digital kommunikasjon som hovedregel—endringer i eForvaltningsforskriften

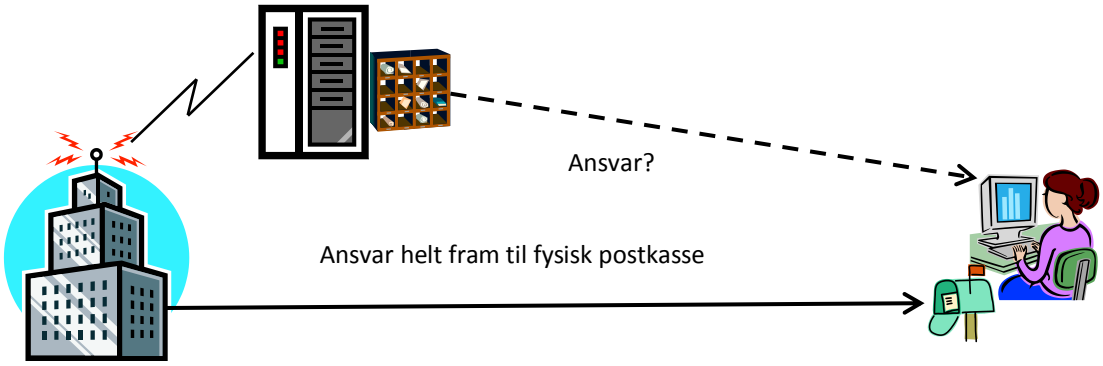
Jeg viser til høringsbrev fra Fornyings-, administrasjons- og kirkedepartementet (FAD) av 11. juni 2013 hvor det bes om kommentarer til endringer i forskrift 25. juni 2004 nr. 988 om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften).

Under følger mine kommentarer til høringsnotatet.

Slik høringsutkastet er formulert, har jeg ikke inntrykk av at departementet har benyttet god nok kompetanse innen informasjonssikkerhet. Et eksempel på det er Vedlegg 1 Kryptografisk beskyttelse av digital post.

Teknologiuavhengig regelverk?

Så vidt jeg forstår, har avsender ansvar for fysisk post helt fram til mottaker, mens i forslaget har avsender bare ansvar for elektronisk post fram til en elektronisk «postboks». Her blir det dermed en forskjellsbehandling av mottaker avhengig av hvilken teknologi avsender velger å bruke. Det gir ikke likebehandling for borgerne.



Et enkelt fysisk brev kan komme på avveie. Men når et elektronisk system, som en elektronisk postkasse eller et personregister, korrumperes, kan konsekvensene bli enorme. Det er også mye som kan skje mellom den elektroniske postkassen og mottakeren. Hvem har ansvar for det?

Sikkerhet koster

Sikkerhet koster på ulike måter for alle parter i en elektronisk samhandling. Isteden står det i 6.4.1 at det er vanskelig å lage gode sikkerhetsmål og sikkerhetsstrategier: «Det har vist seg å være vanskelig for forvaltningsorganer å få full oversikt over alle praktiske konsekvensen

av eForvaltningsforskriften § 13. Dette har også gjort det krevende for mange virksomheter å etterleve den på en god måte.» Er det slik at det ikke er alvorlig om forvaltningsorganene ikke følger regelverket, mens private foretak må følge det fra ikrafttredelse?

Departementet presiserer videre i 6.4.2 at internkontrollen med fordel kan være en integrert del av virksomhetenes helhetlige styringssystem. Det bør kanskje heller presisere at styringen blir dårlig og dyr hvis internkontroll og styring av sikkerhet ikke er integrert.

Risikovurdering

Forskriftsutkastet overlater ulike deler av sikkerheten til de forskjellige aktørene, og skriver noe om at de må foreta risikovurderinger. Men bør ikke departementet foreta en risikovurdering av hele forslaget? Det kom meg for øret at Difi har utarbeidet en risikovurdering, men det ble ikke sagt hva den vurderer. Den er ikke offentlig, og det skal lages en ny risikovurdering etter avtaleinngåelse med tjenestetilbydere. En helhetlig risikovurdering må gjøres før man starter store prosjekter. Er det akseptabelt at det fremmes et slikt regelverk uten å følge utredningsinstruksens krav om konsekvensutredning?

Notatet skriver lite om hvilke risikoer mottakerne løper. Det oppleves ikke betryggende.

Sikkerhet for mottakernes post

Departementet sier at det ikke fins teknologiske løsninger som gir en akseptabel sikkerhet for elektronisk post helt fram til norske borgere i dag. Høringsnotatet er dermed opptatt av å sikre dokumenter fram til en lagringsplass som kan være et eller annet sted i EØS- eller Safe Harbour-området. Der kan det gjelde til dels andre lover enn vi har i Norge.

- Har det blitt utredet hvor stort datavolum som kommer til å ligge lagret om den norske befolkningen ute i verden?
- Er konsentrasjonsrisikoen vurdert?
- Norske banker har solide sikkerhetsopplegg. Likevel erfarer de at deres kunder noen ganger har fått tilgang til informasjon om andre kunder. Har departementet vurdert risikoen og trussellandskapet for spionasje mot norske borgere? Vi er alle slags i dette landet.

Bekymringen for borgernes sikre tilgang til utsendt post ser ut til å smuldre bort på veien fra den digitale postkassen. Vi mottakere har vanlige PC-er med anti-virusprogrammer, og likevel vet vi at PC-ene er usikre. Det står ikke noe om hvordan «forvaltningsorganet skal forebygge risiko for berettiget innsyn i enkeltvedtak» (§8) for alle borgerne når mange PC-er er infisert med verktøy for å avlytte tastetrykk og informasjon om hva brukeren foretar seg på en datamaskin, eller annen ondsinnet kode.

Spesielt kan mottakerens PC eller mobile enheter som nettbrett eller mobiltelefon ikke virke. De er ganske annerledes komplekse enn et fysisk brev, Posten Norge og postkassen som vi har lært å vurdere risiko og sårbarhet til. Vår elektroniske virkelighet er at

- vi flytter og får ikke PC-en til å virke før etter 14 dager
- vi har glemt eller mistet passordet
- mobiltelefonen falt i vannet

- e-postleverandøren har stanset sin virksomhet, og vi vet ikke hvor vi finner en rimelig sikker ny leverandør
- strømmen går, nettleverandøren endrer noe, Java-appleten har hull, vi har ikke hatt tid til å oppdatere all programvare.

Jeg har ikke funnet noe om hvilke rettigheter og plikter mottaker har hvis hans «mottakerapparat» ikke virker korrekt og ikke oppfatter at det har kommet elektronisk post som han må reagere på innen en tidsfrist.

Høringsnotatet virker uklart mht. råderett over postkassen. I kap. 4.8 står det at «Departementet mener at det er viktig å fastholde prinsippet om at den digitale postkassen er mottakers postkasse og at mottaker skal ha full råderett over denne.» Samtidig står det at «det kan være hensiktsmessig at andre enn mottaker selv har tilgang til den digitale postkassen» og at teknisk personell normalt ikke vil kreve tilgang til selve innholdet i de digitale brevene. Under 10 Merknader til ny § 8 a står det: «Bruk av elektronisk ID tilhørende en annen må unngås.»

Det er uklart for meg hva departementet mener når det i 8.3 står at den enkelte også vil «kunne ha en viss påvirkning på sikkerhets- og personvernnivået i sin egen postkasse». Det står heller ikke under 10 Merknader til §2 hvordan mottaker kan behandle opplysninger i sin postkasse til andre formål.

Register over digital kontaktinformasjon

I § 39 står det at DIFI skal være behandlingsansvarlig for registeret og sikre det. Opplysningene som listes i § 40 gir assosiasjoner til et utvidet fødselsregister over den voksne befolkningen i landet. Det står ikke noe om at dette registeret ikke kan oppbevares utenfor Norge. Dette er også et område for konsentrasjonsrisiko som jeg ikke kan se at er behandlet.

I § 38 står det at forvaltningsorganer kan benytte kopier av registeret, men det står ikke noe spesifikt om hvordan forvaltningsorganene skal sikre dem.

Reservasjonsrett

Konsekvensene ved å reservere seg virker uklare. For folk som ikke vet hva et enkeltvedtak er, hvilken risiko man løper ved å bruke den elektroniske postkassen og hvilken elektronisk kontakt man likevel kan ha med forvaltningen, kan det bli vanskelig å gjøre et velbegrunnet valg. Det er også uklart om mottaker kan få rettet informasjon i registeret som hun mener er feil, jfr. forslag til §§ 41 og 42.

Urettmessig tilgang til datasystemer

Flere rapporter om informasjonssikkerhet påpeker at det kan ta måneder før urettmessig tilgang til datasystemer avdekkes. Dette er ikke en risiko som nevnes i høringsnotatet. Eksempler er Normans rapport Hangover om angrep på Telenor i vår, http://blogs.norman.com/2013/security-research/the-hangover-report , The 2013 Data Breach Investigations Report fra Verozon, http://www.verizonenterprise.com/DBIR/2013/ og at en fra The

Pirate Bay er tiltalt bl.a. for i en periode fra 2010 og frem til våren 2012 å ha brutt seg inn på servere som inneholdt informasjon fra flere danske myndighetsinstitusjoner.

Kommentarer til enkelte paragrafer

I § 9 står det at klage er rettidig framsatt dersom den er kommet fram … innen klagefristens utløp. Hvordan kan klager vite at posten er kommet fram?

I §§ 31, 32 og 33 gis de ulike aktørene ansvar. Det er forvirrende å lese, og jeg lurer på om noe ansvar forsvinner mellom «stolene», aktørene. Hvorfor brukes ikke personopplysningslovens begreper, behandlingsansvarlig og databehandler slik at vi klarer å plassere ansvarene på samme måte som for andre avtaler om tilsvarende arbeidsdeling? Hvordan skal mottaker vite hvem hun skal forholde seg til ved sikkerhetsbrudd av ulike slag?

§ 37 sier bl.a. at all post kan overføres til mottaker selv. Jeg har ikke funnet noe om hvordan mottaker skal kunne hevde å ha et gyldig dokument i tilfelle av en konflikt med forvaltningen.

Hilsen

Anne Karen Bonnevie Seip

Hamang Terrasse 81
1336 Sandvika