Nasjonal sikkerhetsmyndighet

Vår saksbehandler
Simon Kiil

Vår dato	Vår referanse
2013-09-10	A03 - S:13/02202-5
Deres dato	Deres referanse
2013-06-11	13/1249
Antall vedlegg	Side
	1 av 5

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

Digital kommunikasjon som hovedregel – endringer i eForvaltningsforskriften

Det vises til brev 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).

Nasjonal sikkerhetsmyndighet ser det som positivt at FAD gjennom Direktoratet for forvaltning og IKT (Difi), har satt fokus og fart på digitaliseringsprosessen av offentlig forvaltning som følge av Regjeringens digitaliseringsprogram.

NSM har tidligere uttalt seg om sikkerhetsutfordringer knyttet til digital kommunikasjon og da særskilt om sikkerheten i digital postkasse. NSM ønsker i denne høringsuttalelsen å komme med innspill for bidra til å gjøre løsningene så sikre som mulig, og at sikkerheten blir tatt hensyn til i relevant regelverk.

Generelt om sikker digital postkasse

Regjeringens ambisjoner fremgår av digitaliseringsprogrammet av april 2012, "På nett med innbyggerne", herunder ambisjoner om sikker digital kommunikasjon fra forvaltningen til landets innbyggere.

NSMs hovedbekymring har relatert seg til hvilke sikkerhetskrav som stilles for å beskytte informasjonen i den digitale kommunikasjonen fra forvaltningen.

Postadresse
Postboks 14
1306 BÆRUM
POSTTERMINAL

Sivil telefon/telefaks
+47 67 86 40 00/+47 67 86 40 09
E-postadresse
post@nsm.stat.no

Militær telefon/telefaks
515 40 00/515 40 09
Internetadresse (URL)
www.nsm.stat.no

Det fremgår av digitaliseringsprogrammet at Regjeringen ønsker en løsning som i motsetning til vanlig e-post er sikker. Det fremgår av høringsnotatet fra FAD og forslag til lovtekst at informasjonen i den digitale postgangen kun skal være tilgjengelig for mottakeren.

NSM mener at de krav som er stilt til sikkerheten for digital postkasse ikke er av en slik art at de oppfyller Regjeringens ambisjoner. NSMs hovedankepunkt er at løsningen ikke tilbyr såkalt ende-til-ende-kryptering.

NSM er imidlertid kjent med at Difi har laget en løsning som legger til rette for senere implementering av ende-til-ende-kryptering. Denne krypteringsformen anser NSM som en forutsetning for å kunne beskytte postkassens innhold mot avtitting, og ser at dette blir inntatt som et krav så snart som mulig. Uten ende-til-ende sikkerhet anser NSM at eForvaltningsforskriftens ønske om å beskytte brukernes digitale post mot innsyn ikke kan oppnås. Den digitale kommunikasjonen vil ikke være sikker, og forskriftsteksten vil kunne gi et annet bilde enn de faktiske forhold tilsier.

Høringsnotatet

I det videre følger kommentarer direkte knyttet til høringsnotatet "Digital kommunikasjon som hovedregel".

Befolkningens bruk av elektronisk kommunikasjon

I punkt 2.2 omtales befolkningens bruk av elektronisk kommunikasjon. Her fremgår det av en markedsundersøkelse gjort av Difi, at 31 % av de spurte vil reservere seg mot bruk av digital postkasse. De viktigste grunnene er bl.a. "frykt for dårlig sikkerhet", "usikkerhet om hvem som har ansvaret dersom noe skulle komme på avveie" og "lav datakunnskap".

På tross av at nær en tredjedel av respondentene frykter for at løsningen ikke vil ha tilstrekkelig sikkerhet, og at de selv besitter for lav datakunnskap til å vurdere om løsningen er sikker nok, fremhever departementet at brukeren selv skal kunne velge den løsningen de har mest tillitt til, jfr. forslag til ny § 36 *Bytte av postkasseleverandør*.

I kravspesifikasjonen fra 19. august har Difi stilt krav til informasjonssikkerheten. NSM mener Difi har gjort en god jobb hva gjelder styringssystemer, men at kravene er for vage hva gjelder teknologi. Postkasseleverandørene kan selv fastsette hva slags sikkerhetskrav de ønsker å følge, noe NSM mener er uheldig. Dette svekker brukernes vurderingsgrunnlag ved valg eller bytte av leverandør. At det i tillegg fremgår av forslag til ny § 33 (2) at det ved sikkerhetsbrudd er sentralforvalter som skal ta stilling til om mottaker skal varsles, bidrar ikke til å skape tillit til løsningen. Ettersom departementet ønsker at det skal være konkurranse i markedet og at brukerne skal ha sikkerhet som et vurderingskriterium for hvilken tilbyder de vil benytte, må brukerne ha kvalifisert informasjon om hvilke leverdører som er sikre og mindre sikre. NSM mener derfor at brukerne bør få informasjon om alle hendelser, både risiko og sikkerhetsbrudd, som forekommer.

Verdivurdering av informasjonen som sendes

Slik det fremgår av punkt 4.3.3 om avsendervirksomhetene og forslag til ny § 31 *Avsendervirksomhetenes ansvar*, legges det opp til at avsendervirksomhet selv skal definere hva slags informasjon som er forsvarlig å sende via løsningen. NSM har lang erfaring fra tilsyn med en rekke virksomheter og er kjent med at det ofte kan være dårlige rutiner hva gjelder verdivurdering av informasjon. Videre er det vanskelig for virksomhetene å vurdere dette uten tilstrekkelig veiledning, retningslinjer eller klare holdepunkter. NSM mener det bør etableres sikkerhetsnivåer med eksempler på hva slags informasjon som kan/ikke kan sendes via løsningen, slik at enkeltpersoner i forvaltningen enkelt kan vurdere om løsningen kan benyttes eller ikke.

Tilgang til digital postkasse

Til høringsnotatets punkt 4.8 og forslag til ny § 35 *Bruk av den digitale postkassen* vil NSM bemerke at det fremstår som et noe uklart forhold mellom forskriftstekst og den praksis departementet legger opp til etter høringsnotatet. Slik teksten er formulert i forskriften fremgår det at det *kun* er mottaker som kan få tilgang til digital postkasse og at det *kun* er mottaker som vil kunne se innholdet i de digitale brevene. Slik det fremgår av departementets beskrivelser i høringsnotatet, vil *"teknisk personell kunne ha behov for å gjøre postkassen utilgjengelig for mottakeren på grunn av systemoppdateringer (...). Dette vil imidlertid normalt ikke kreve tilgang til selve innholdet i de digitale brevene."* NSM mener dette er uheldig, og foreslår at det presiseres i forskriftsteksten at bare mottakeren skal ha tilgang til den digitale postkassen og *dennes innhold.*

NSM mener også at det bør være mulig å trekke tilbake brev fra mottakerens postkasse, men at dette bør være på grunnlag av metadata som identifiserer brevet som feilsendt, ikke på grunn av innholdet. Ordlyden i forslag til ny § 35 (4) hindrer imidlertid at andre enn mottakeren kan slette brevet som ligger i postkassen. Altså hindres sletting av feilsendte brev og brev som kan inneholde virus.

Bruk av tidsstempel

I punkt 6.1.1 omtales tidspunktregistrering for når mottaker har kunnet gjøre seg kjent med vedtaket. NSM mener det, i stedet for elektronisk logg, bør benyttes signerte tidsstempler som bekrefter tidspunkt for håndteringen av elektroniske brev. Det er som regel kun en administrator som har tilgang til logger, og mottaker vil ikke kunne få se disse før ved en eventuell tvist. Åpne tidsstempler som legges utenpå dokumentet sikrer notoritet for ulike deler av håndteringen.

Kryptografisk beskyttelse av digital post

Til høringsnotatets vedlegg 1 om kryptografisk beskyttelse av digital post vil NSM kommentere at så lenge mottaker selv kan redigere sin egen kontaktinformasjon, bør det ikke være noe i veien for at mottaker selv bestemmer hvilket sertifikat som benyttes. Det kan, og bør, stilles krav til sertifikatet, som format, algoritme, nøkkellengde mm., men for

konfidensialitetssertifikat burde det ikke være nødvendig med kvalifisert sertifikat. Dersom sertifikatet går ut på dato, vil det være opptil bruker å oppdatere sertifikatinformasjonen i kontaktregisteret.

Internkontroll på informasjonssikkerhetsområdet

NSM stiller seg bak presiseringen av kravene til internkontroll (styring og kontroll) på informasjonssikkerhetsområdet, at denne skal inkludere krav fastsatt i andre regelverk (herunder sikkerhetsloven med forskrifter), være basert på anerkjente standarder og være en integrert del av virksomhetens helhetlige styringssystem. NSM er av den oppfatningen at presiseringen i større grad vil synliggjøre at det er virksomhetens ledelse som er ansvarlig for informasjonssikkerheten i virksomheten, og at den skal underlegges både styring og kontroll.

NSM fører systemrettede tilsyn med internkontrollen på sikkerhetsområdet hos virksomheter underlagt sikkerhetsloven, herunder alle offentlige virksomheter. NSM kontrollerer i den forbindelse virksomhetens helhetlige styringssystem for sikkerhet, herunder at dette er samordnet, jf. forskrift om sikkerhetsadministrasjon § 1-1 tredje ledd andre punktum og integrert med øvrige aktiviteter jf. forskrift om sikkerhetsadministrasjon § 2-2 første ledd første punktum. Det er NSMs erfaring at virksomheter som har samordnet styringssystemer integrert med øvrige aktiviteter, og som legger anerkjente standarder til grunn for sikkerhetsstyringen, har bedre etterlevelse av krav gitt i og i medhold av sikkerhetsloven. Det er også mer effektivt for en virksomhet å sikre etterlevelsen av krav til å beskytte skjermingsverdig informasjon i et helhetlig styringssystem som også ivaretar krav til skjerming av taushetsbelagt og annen sensitiv informasjon, samt andre relevante forhold. NSM finner det derfor positivt at etterlevelse av flere krav til informasjonssikkerhet skal ivaretas gjennom samme styringssystem.

NSM noterer seg at ingen virksomhet fører tilsyn med etterlevelse av krav i eforvaltningsforskriften. Det bør vurderes at et organ fører kontroll med etterlevelsen av bestemmelsene. Hvem som utpekes bør med fordel sees i sammenheng med andre tilsynsorganer som fører tilsyn med styringssystemer og internkontroll på sikkerhetsområdet, slik at det ikke blir unødvendig mange kontrollorganer en virksomhet må forholde seg til. Videre bør metodikk for tilsyn samt hvilke krav som stilles til styringssystem i større grad samordnes.

NSM noterer seg at ISO/IEC 27001 er anbefalt standard for styringssystem for informasjonssikkerhet i statsforvaltningen og at denne er ment å legges til grunn som "anerkjent standard." Det er NSMs vurdering at etterlevelse av krav til styring og kontroll i ISO/IEC 27001 i stor grad vil bidra til etterlevelse av krav i forskrift om sikkerhetsadministrasjon og at dette er et godt utgangspunkt å basere sikkerhetsstyringen i en virksomhet på.

Nasjonal sikkerhetsmyndighet vil med dette takke for anledningen til å komme med synspunkter til høringsnotatet "Digital kommunikasjon som hovedregel", og ønsker departementet og Difi lykke til videre med innføringen av digital kommunikasjon i forvaltningen.

Med vennlig hilsen

Kjetil Nilsen

Direktør

Simon Kiil

Rådgiver