

**DET KONGELIGE FORNYINGS-,  
ADMINISTRASJONS- OG KIRKEDEPARTEMENT***Statsråden*

Stortingets kontroll- og konstitusjonskomite  
Stortinget  
0026 OSLO

Deres ref  
kgj/2010

Vår ref  
10/4484

Dato  
10.01.11

**Svar på spørsmål fra Kontroll- og konstitusjonskomiteen  
vedrørende varsling om manglende sikkerhet i regjeringens  
datasystemer.**

Jeg viser til brev fra Kontroll – og konstitusjonskomiteen av 14. desember 2010 om ovennevnte sak.

***Spørsmål 1***

*Hva har departementet gjort for å bedre IKT-sikkerheten i DSS og for å følge opp innholdet i varslet?*

Da Departementenes servicesenter (DSS) rapporterte om sikkerhetsutfordringer omkring årsskiftet 2007/2008 ba Fornyings-, administrasjons- og kirkedepartementet (FAD) umiddelbart DSS om en plan for gjennomføring av tiltak på både kort og lang sikt. Planen dannet grunnlaget for forslag om ekstraordinær bevilgning som ble fremmet våren 2008 i forbindelse med revidert nasjonalbudsjett. Som nevnt i mitt brev til komiteen av 30. november 2010, er det uheldig at det tok lengre tid enn forutsatt å få gjennomført disse investeringene.

I oktober 2009 tok departementet initiativ til et forprosjekt med bistand fra en ekstern konsulent (*Watchcom Security Group*) for å få en vurdering av sikkerhetsnivået i Depnett/U. Hensikten var å få en oversikt over sikkerhetstilstanden i det ugraderte nettet for 13 departementer, som grunnlag for eventuelle videre oppfølgingstiltak. Den endelige rapporten fra forprosjektet forelå 9. mars 2010. Riksrevisjonens foreløpige

rapport ble sendt departementet 28. april 2010. Watchcom-rapporten viste det samme helhetsbildet som senere ble påpekt av Riksrevisjonen i deres foreløpige rapport til DSS av 26. april 2010. Riksrevisjonens rapport var mer detaljert og utdypende enn konsulentens forprosjekt.

I den videre oppfølging av DSS la FAD Riksrevisjonens foreløpige rapport til grunn.

- DSS ble i mai 2010 bedt om å utarbeide en oppfølgingsplan for innføring av et *StyringsSystem for Informasjons-Sikkerhet* (SSIS). FAD har inngått avtale med en ekstern konsulent (Ernst & Young) som skal kvalitetssikre DSS sin handlingsplan og gjennomføringen av den. Konsulenten er også bedt om å vurdere om det er andre forhold av betydning for informasjonssikkerheten som eventuelt ikke ligger i handlingsplanen. Det dreier seg altså ikke bare om et prosjekt som skal følge opp Riksrevisjonens påpekinger, men en grundig gjennomgang av det systematiske IKT-sikkerhetsarbeidet i DSS.
- Jeg har sett det nødvendig også å gjennomføre en uavhengig undersøkelse av den tekniske sikkerhetstilstanden i Depnett/U. Jeg ba derfor den 22. oktober 2010 NSM om å teste robustheten i nettet mot ondsinnet inntrenging. Rapporten fra NSM ble mottatt i FAD 22. desember 2010. NSM har påvist sårbarheter i Depnett-U. DSS er allerede pålagt å gjennomføre tiltak for å styrke sikkerheten. Rapporten vil bli fulgt opp av departementet og vil være et sentralt grunnlag for kvalitetssikring av informasjonssikkerheten i DSS og for vurdering av ytterligere tiltak.

Fungerende departementsråd i FAD ble innkalt til et møte på Statsministerens kontor (SMK) 23. juni 2010. På møtet ble det av en ansatt i DSS og dennes advokat lagt fram muntlig informasjon om datasikkerheten i DSS, og det ble også overlevert et tosiders notat med faktainformasjon. Notatet var verken påført avsender eller adressat.

I tillegg til utfordringene for sikkerhetsnivået, som også er tatt opp av Riksrevisjonen, påpeker varsleren forhold som berører ansvarsfordeling, sikkerhetskultur og kompetanse i forbindelse med forvaltningen av Depnett/U. Departementet har innhentet opplysninger fra ansatte i DSS som understøtter varslersens anførsler om sikkerhetskulturen og manglende systematikk i DSS sin ivaretagelse av informasjonssikkerheten. Det tyder på at sikkerhetsarbeidet i DSS har blitt nedprioritert på bekostning av tjenesteproduksjonen og framdriften i innfasingen av de 13 departementene på felles driftsplattform. Sikkerhetskultur, internkontroll og systematisk videreutvikling av sikkerheten i tråd med risikobildet for et ugradert nett, er forhold som vil bli fulgt opp i ovennevnte kvalitetssikring. I den forbindelse vil også forhold varsleren har tatt opp, være en del av vurderingsgrunnlaget.

Disse forholdene arbeides det nå videre med i departementet, også de forhold varsleren påpeker. Det er bl.a. nødvendig å se nærmere på både ansvarsforhold og organiseringen av sikkerhetsarbeidet.

**Spørsmål 2**

*Mener statsråden at departementet har behandlet varslersaken i samsvar med varslerens ønske om anonymitet?*

En advokat tok 21. juni 2010 kontakt med Statsministerens kontor på vegne av en person som ønsket et møte for å overbringe informasjon som gjaldt departementenes datasikkerhet, herunder de datasystemer som leveres av DSS. SMK la til rette for at det to dager etter, 23. juni 2010, fant sted et første møte om saken. Møtet fant sted på SMK og med deltakelse fra FAD, som ansvarlig departement for DSS. På møtet deltok varsleren og dennes advokat, embetsverk ved SMK og fungerende departementsråd i FAD. Varsleren ba om anonymitet og full beskyttelse som varsler, selv om identiteten var kjent for møtedeltakerne. I møtet ble det avklart at FAD som overordnet departement ville gå gjennom den informasjonen som hadde blitt framlagt og komme tilbake til den ansatte i DSS når det gjaldt den videre oppfølging. Det framkom ingen innvendinger til denne behandlingsmåten fra varsleren eller dennes advokat.

Fungerende departementsråd i FAD så dilemmaet som ligger i behovet for å undersøke innholdet i et varsel, samtidig som varslerens identitet skal holdes skjult. IKT-sikkerhet er et sentralt anliggende for FAD, og påstander av den karakter som varsleren tok opp, var det viktig å få undersøkt nærmere. Etter fungerende departementsråds oppfatning ville det være vanskelig å foreta en tilfredsstillende undersøkelse av varslerens påstander uten at DSS' ledelse ble forelagt den informasjonen varsleren hadde lagt fram.

Det ble altså vurdert som nødvendig for FAD å konfrontere direktøren i DSS med påstandene om sikkerhetsnivået i Depnett/U. DSS sin direktør fikk ikke informasjon om varslerens identitet, og det ble tydelig presisert overfor direktøren at varsleren ønsket å være anonym, og at dette var et ønske som alle involverte måtte respektere. Fungerende departementsråd informerte varslerens advokat om at notatet ble levert direktøren i DSS på disse betingelser.

Varslerens advokat opplyste 12. juli 2010 på telefon til fungerende departementsråd i FAD at varsleren hadde utarbeidet en redegjørelse som beskrev hvordan varsleren hadde tatt opp sin bekymring internt i DSS. Advokaten stilte som betingelse for å oversende redegjørelsen til FAD at denne ikke ble gitt videre. Fungerende departementsråd svarte at hvis han ikke kunne framlegge redegjørelsen for DSS, ville departementet ikke kunne undersøke innholdet i varslerens påpekinger, og de som eventuelt var omtalt, ville ikke kunne legge fram sin versjon av saken. Fungerende departementsråd forstod behovet for å dekke varslerens identitet, og mente han på advokatens premisser ikke kunne bruke redegjørelsen til å oppklare saken. Redegjørelsen ble derfor ikke overlevert fungerende departementsråd.

Etter at den faste departementsråden i FAD var tilbake, ble det avtalt møte mellom henne, varsleren og varslerens advokat. Møtet ble holdt 27. oktober 2010. Varsleren var forhindret fra å møte av private årsaker. Departementsråden redegjorde for det arbeidet som var gjort med varslingssaken og uttrykte at det på flere områder hadde vært vanskelig å etablere fakta. Advokaten trakk fram eksempler fra den redegjørelsen som FAD ikke hadde. Han ønsket ikke å overlevere den av hensyn til varslerens identitet. Det ble avtalt at advokaten skulle snakke med varsleren om hvorvidt opplysningene kunne gis i en form som ikke avslørte varslerens identitet.

I e-post av 4. november 2010 fra departementsråden til varslerens advokat ble det gjentatt at departementsråden var innstilt på å lytte til varsleren. Varslerens advokat meldte i e-post av 14. november 2010 til departementråden at varsleren anså det for nytteløst å forfølge saken videre overfor FAD. Jeg ba departementsråden om å prøve på nytt å få varsleren i tale for eventuelt muntlig å få utdypet vedkommendes bekymringsmelding. Departementsråden gjentok i e-post av 15. november 2010 tilbudet om å lytte til varsleren.

FAD gjennomførte etter dette også nye samtaler med personer i DSS for å prøve å få ytterligere klarhet i om det hadde vært reist spørsmål om IT-sikkerheten internt i DSS. Samtalene underbygget inntrykket av mangelfull sikkerhetskultur og manglende systematikk i DSS sin ivaretaging av informasjonssikkerheten.

I en henvendelse av 26. november 2010 fra departementsråden i FAD til varslerens advokat har jeg også tilbudt varsleren å møte meg.

Jeg konstaterer at varsleren mener seg utlevert i DSS. 2. november 2010 ble FAD, via kopi av en epost fra NSM hvor NSM ga en journalist innsyn i flere dokumenter i en tilsynssak, oppmerksom på at direktøren i DSS i juli 2010 hadde reist en diskusjon med NSM om intervjuplan og informanter. Dette skjedde i forbindelse med et tilsyn etter Sikkerhetsloven. I en epost av 14. november til departementsråden i FAD bekreftet varslerens advokat formelt at diskusjonen mellom NSM og DSS konkret gjaldt varsleren. Departementet innkalte direktøren i DSS til et møte 22. november og påpekte overfor ham at det var uheldig å forsøke å holde en sentral informant borte fra en tilsynsmyndighets informasjonsinnhenting, og at dette følgelig ikke skulle ha skjedd. I og med at denne informanten og varsleren viste seg å være samme person, kan varsleren ha oppfattet dette som gjengjeldelse. I henhold til Arbeidsmiljøloven skal en ikke utsette en som har varslet på riktig måte, for gjengjeldelse.

Direktøren for DSS trakk seg fra sin stilling 7. desember 2010. FAD bad deretter konstituert direktør i DSS undersøke om varsleren har blitt fratatt arbeidsoppgaver på grunn av varslingssaken. Gjennomgangen i DSS har ikke kunnet sannsynliggjøre at arbeidsgivers ønske om å unnta varsleren fra intervju med NSM ble bygget på saklige hensyn. Med unntak av dette er konklusjonen fra gjennomgangen at varsleren ikke er fratatt arbeidsoppgaver.

### **Spørsmål 3**

*Hvilke tiltak blir iverksatt for å sikre at staten har et bedre system for dem som tar belastningen ved å varsle?*

Retten til å varsle om kritikkverdige forhold i virksomheten er fastslått i Arbeidsmiljøloven. Her er det også utvetydig fastslått at gjengjeldelse mot arbeidstaker som varsler i samsvar med Arbeidsmiljølovens regler, ikke er tillatt. Etter § 3-6 i Arbeidsmiljøloven plikter arbeidsgiver å legge forholdene til rette for varsling i sin egen virksomhet.

I september 2007 fremmet det daværende Fornyings- og administrasjonsdepartementet ”Retningslinjer for utarbeidelse av lokale varslingsrutiner i staten”. Dette er retningslinjer som den enkelte statlige arbeidsgiver skal legge til grunn for sitt arbeid med å tilrettelegge for varsling i egen virksomhet.

Disse sentrale, statlige retningslinjene bygger på Arbeidstilsynets veileder om varsling om kritikkverdige forhold på arbeidsplassen. Arbeidstilsynets veileder er ikke i seg selv et eget regelverk, men presiseringer av hvilke hensyn loven skal ivareta og anbefalinger til arbeidsgivere om hvordan de skal innrette seg for å ivareta disse hensynene.

Behovet for egne statlige retningslinjer skyldes bl.a. at statlige virksomheter må forholde seg til offentlighetsloven og forvaltningsloven, også i varslersaker. Arbeids- og inkluderingsdepartementet og Arbeidstilsynet har bekreftet at retningslinjene er i tråd med Arbeidstilsynets generelle retningslinjer.

FADs retningslinjer har omfattende beskrivelser av hvordan varslingsrutinene bør legges opp, slik at den enkelte arbeidstaker kan varsle på en trygg måte. Det er også laget saksbehandlingsregler som mottakeren av varselet skal følge for å ivareta hensynet til at varslersens identitet blir behandlet konfidensielt, dersom identiteten er kjent for den som mottar varselet. Det er også beskrevet saksbehandlingsregler for å ivareta hensynene til taushetsplikt om eventuelle personlige forhold, arbeidsgivers ansvar for å forhindre gjengjeldelse, hvordan man skal håndtere hensynene til den/de det blir varslet om, tilbakemelding til varsleren om hva som ble resultatet av varslingen og hvordan man skal behandle personopplysninger som måtte fremkomme under varslingen.

I retningslinjene har FAD satt som en forutsetning at hver enkelt statlig virksomhet utarbeider egne rutiner for varsling, basert på virksomhetens behov og egenart. FAD har utarbeidet slike varslingsrutiner for sin egen del og det har også DSS. Det som blir avgjørende for om varsleren i en konkret sak er tilstrekkelig vernet, er om gjeldende regelverk og rutiner følges.

Som det tidligere er opplyst i Stortinget, er det besluttet at Arbeidsdepartementet skal foreta en gjennomgang av gjeldende varslingsregelverk i arbeidsmiljøloven. I den forbindelse vil FAD gjennomgå statens retningslinjer for varsling.

Varsel om kritikkverdige forhold stiller en virksomhet overfor mange vanskelige avveininger og dilemmaer. FAD vil ta initiativ til at kunnskap om – og holdninger til – varsling, etikk og etiske dilemmaer blir styrket i statsforvaltningen gjennom bl.a. lederopplæring og i seminarer og konferanser for statens embets- og tjenestemenn.

Med hilsen



Rigmor Aasrud