Digdir

# Nettverksmøte for veiledningsaktører innen styring og kontroll

Tidspunkt: 31. mars 2022, klokken 12:00 – 14:30, Økern Portal/Digitalt møte

## Til stede

| Navn | Virksomhet |
|---|---|
| Eivind Reiner Holm | NorSIS |
| Harald Torbjørnsen | KiNS |
| Suhail Mushtaq | KS |
| Randi Utstrand | SIKT |
| Tor Gjerde | SIKT |
| Eirik Guldbrandsen | Datatilsynet |
| Aasta Margrethe Hetland | Direktoratet for e-helse |
| Siw Tynes Jakobsen | Direktoratet for e-helse |
| Per Jakobsen | DFØ |
| Benjamin Marøy Gangvik | HK-Dir |
| Tor Jørgen Bergbye | Nkom |
| Geir Løvnes | NSM |
| Harald Næss | NSM |
| Eva Jean Elkjær Greenwood Ormerod | NSM |
| Katrine Aam Svendsen | Digitaliseringsdirektoratet |
| Silje Johansen | Digitaliseringsdirektoratet |
| Remi Longva | Digitaliseringsdirektoratet |
| Kjersti Nesheim | Digitaliseringsdirektoratet |
| Terje Overaae | Digitaliseringsdirektoratet |
| Fanny Emilie Bøhm-Pedersen | Digitaliseringsdirektoratet |

## Agenda:

- Velkommen, litt om nettverket, og nytt fra Digdir
- KVU Nasjonal sky v/NSM
- RTD og utredning om operative sikkerhetsbehov v/KS
- «Felles sikkerhet i forvaltningen» v/Digdir
- Strategi for digital sikkerhet i helse- og omsorgssektoren, kriterier for risikoaksept, og nytt veiledningsmateriell v/ Direktoratet for e-helse
- Det europeiske kompetansesenteret for cybersikkerhet og DIGITAL v/Digdir

## Oppsummering

| | |
|---|---|
| **Introduksjonsrunde** | Alle deltakerne i nettverksmøte introduserte seg selv. |
| **Velkommen, litt om nettverket, og nytt fra Digdir** v/ *Katrine Aam Svendsen, DigDir* | **Om nettverket**<br>- Nettverket for veiledningsaktører skal være en felles møteplass for koordinering og utveksling av erfaringer.<br>- Digdir er i gang med å lage en nettside på digdir.no med informasjon om nettverket. Her vil retningslinjer for samordning av veiledning, og korte referater publiseres.<br>- Alle aktører har et gjensidig ansvar for å sette seg inn i informasjonen de mottar, gi innspill og tilbakemeldinger. |

| | |
|---|---|
| | **Stifinneren**<br>- Stifinneren ble publisert i august 2021. En veiledning til hvordan man kan jobbe med etablering eller forbedring av arbeidet med informasjonssikkerhet. Det ligger opptak fra et frokostmøte om veiledningen ute her.<br><br>**Fornyet «Internkontroll i praksis»**<br>- Veilederen «Interkontroll i praksis – informasjonssikkerhet» er nå en del av digdir.no, og ikke lenger en separat portal.<br>- Tilsvarende samme innhold som før, men omstrukturert.<br>- Sterk oppfordring til møtedeltakere om å gi tilbakemeldinger.<br>- Se endringslogg for konkrete oppdateringer. |
| **KVU Nasjonal sky** v/NSM | **Sårbarheter knyttet til utenlandske skytjenester**<br>NSM er bekymret for avhengigheten til utenlandske leverandører og lange leverandørkjeder. Problematikken har vært på NSMs agenda siden 2016.<br>- Norge er sårbare for sikkerhetspolitiske saker - Skal vi stenge for visse skytjenester eller ikke?<br>- Skytjenester innebærer flere ledd av sårbarheter: fra skyriggen som kan stå i sjøen, eller et helt annet sted, til transportnettet (ofte internett/VPN) til klienten.<br>- Robustheten har noe å si for sikkerheten til en skytjeneste. Avhengighet til mange utenlandske driftssentre leder til spørsmål om hvem og hvor de ansvarlige for enkeltpersoners data er.<br>**KVU om nasjonal sky**<br>- Igangsatt prosjekt for en KVU om nasjonal sky. 9 NSM ressurser + 3 eksterne. Leveres til JD medio-mai med sluttleveranse 1.desember. Dette er et kort tidsskjema.<br>- Først skal prosjektet gjennom en standard og kvalitetssikres. Så bestemmes forprosjekt og senere blir det snakk om implementasjon. Det legges betydelige investeringer i dette arbeidet.<br>- Målgruppe: rettet mot statsforvaltningens behov. Vil omfatte skjermingsverdig, ugradert informasjon.<br>- Opprettet ekstern referansegruppe og gjennomført interessentanalyse og dybdeintervju med 22 virksomheter.<br>- Liknende eksempler/løsninger utenfor Norge: Bundescloud, Nederland, Sverige, UK Gov-Cloud. EUs GAIA-X skal tilby fri flyt av datatjenester på tvers av skytjenester.<br>**Spørsmål**: Baltiske land og Ukraina har flyttet datasentre ut av landet. Er dette et relevant aspekt?<br>**Svar**: Muligens. Det kan ligge en skynode utenfor Norge.<br><br>**Spørsmål**: Er kommunesektoren lagt utenfor – hvorfor?<br>**Svar:** Det er ikke en del av mandatet. Skytjenester eskalerer fint, så det vil være mulig å utvide senere. |

| | |
|---|---|
| **RTD og utredning om operative sikkerhetsbehov** *v/Suhail Mushtaq, KS* | **Rammeverk for trygg digitalisering (RTD)**<br>Hvordan skal vi digitalisere trygt og sikkert? Innsatsfaktorer for å ha tjenesteleveranse og funksjonsevne innebærer personell, teknologi, prosess og økonomi.<br>- Hvis sikkerhet og beredskap har feilet, hva vil skje? Østre Toten hadde nødvendig robusthet for å levere tjenester til en viss grad. Å kunne levere kommunale tjenester er det viktigste.<br>- RTD skal bestå av felles teknologiske krav. Første versjon antas å foreligge sommer 2022. Fremlegges på Sikker kommune 2022 15.-16.juni.<br>- Forebyggende og operativ bistand: innsiktsarbeid juni 2022.<br><br>**Spørsmål:** DFØ ser på konsept med security score cards. Er dette et relevant aspekt?<br>**Svar:** Det er godt mulig. KS vil diskutere nærmere med DFØ.<br><br>**Spørsmål**: Jobber dere med resten av aktørene i nettverket i dette arbeidet, og hvordan skal dette passe med veiledningen som resten her i nettverket gjør?<br>**Svar**: Planen er å involvere når første versjon er tilgjengelig. Det er viktig å enes og være samkjørt om «et språk», og vurdere mengden veiledning kan begrenses. |
| **«Felles sikkerhet i forvaltningen»** *v/ Kjersti Nesheim, Digdir* | **Utfordringsbildet og mulige tiltak**<br>Høst 2021 og vår 2022 har Digdir utredet utfordringsbildet (13 problembeskrivelser) som vi må finne løsninger på. I notatet som er utarbeidet vil man få bedre redegjørelse av dette. Ut fra dette har vi utpekt syv mulige tiltak.<br><br>Det er gjennomført workshops og møter med veiledningsaktører og brukere der en spørreundersøkelse ble gjennomført. Mottatt gode tilbakemeldinger<br><br>Det vil bli en semi-åpen høring av notat 0.9 over påsken. Tilgjengeliggjøres på Digdirs nettsider mot slutten av april. 4 ukers svarfrist på å gi tilbakemeldinger på notatet.<br><br>**Spørsmål**: Har Digdir sett på modenhetsvurdering av virksomhetene? Bakgrunn for spørsmålet ligger i at når NSMs grunnprinsipper for IKT-sikkerhet ble utviklet, ble det stilt dette spørsmålet.<br>**Svar**: Det er pr. nå ikke en del av foreslåtte tiltak å lage en modenhetsvurdering av virksomhetene. Vi foreslår å utvikle et minimum viable product (MVP) som et utgangspunkt for ett av konseptene vi vurderer innført som kan bistå virksomheter med utgangspunkt for egne vurderinger. Det vil typisk hjelpe virksomheter som ligger lavt på modenhetsskalaen.<br><br>**Spørsmål**: Hva tenker dere om mangelfull regulering på området?<br>**Svar**: Utgangspunktet som utvikles i dette arbeidet kan benyttes i regulering på et senere tidspunkt. |

| | |
|---|---|
| **Strategi for digital sikkerhet i helse- og omsorgssektoren, kriterier for risikoaksept, og nytt veiledningsmateriell** *v/ Siw Tynes Johnsen og Aasta Hetland, Direktoratet for e-helse* | **Kommende strategi for digital sikkerhet i helse- og omsorgssektoren**<br>- På vei mot en bred, offentlig høring på våren. Strategien lanseres i oktober 2022.<br>- Oppdraget fra HOD: utarbeide en strategi som skal være handlingsrettet, tilpasse sektorens sikkerhetsbehov, tydeliggjøre roller og ansvar, identifisere relevante strategiske virkemidler og tiltak.<br>- Styringsgruppa består også av Helsedirektoratet, Helsetilsynet, NHN, RHF og KS.<br>- Tiltaksoversikt skal være en delleveranse.<br>- 5 fokusområder i hoveddelen, i tillegg til realisering av strategien.<br>- Formål med strategien: legge til rette for forsvarlig helsehjelp gjennom sikker digitalisering i et risikobilde i endring.<br>- Flere målsettinger, innebærer blant annet å få høy tillit fra innbyggere og pasienter.<br>- Strategiske fokusområder (der man ser om man kan gjøre noen grep): kompetanse- og sikkerhetskultur, IKT-beredskap og øvelser, etterlevelse av regelverk (sektorspesifikke tilsyn), innovasjon m.m.<br><br>**Spørsmål:** Ang. støtte til mindre virksomheter og løsninger, hvordan gjennomføres dette?<br>**Svar:** første tiltak er å gjøre kartlegging på at vi treffer. Det trengs fellesløsninger.<br><br>**Spørsmål**: Sikkerhetsstyring: hvordan gi støtte til den enkelte virksomhet om dette?<br>**Svar**: Gjennom veiledning eller gjennom andre aktører. Særlig de små vet ikke helt hvor de skal begynne.<br><br>**Veiledningsmateriell i Normen**<br>Normen er en bransjenorm, en sektorveileder og sektorkravstiller – må se sin plass i annen veiledning. Materiellet skal derfor vise til andres veiledning, ev. utdype andres veiledning.<br><br>Ny strategi for Normen (2023-2025)<br>- Veiledere og faktaark.<br>- Internkontroll er et fokusområde som sier hva man må inkludere.<br>- Ny publisering: Tolkning av prinsipper for logg i helsejournal vedr. hvem som har dataansvar og hvor langt det ansvaret går ev. når går det ansvaret over.<br><br>**Krav om nivå for akseptabel risiko**<br>- Flere bruker *akseptkriterier* og dette kan være mer fleksibelt.<br>- Trolig behov for en oppdatering av selve Normkravet og formuleringen.<br>- Det blir opprettet en arbeidsgruppe for å se på hvordan dette skal gjøres i praksis. |

| | |
|---|---|
| | - Oppfordrer til å tenke på spørsmål. Se presentasjon og slide «Diskusjon». Oppfordring om å ta kontakt og komme med innspill. |
| **Det europeiske kompetansesenteret for cybersikkerhet og DIGITAL** *v/ Silje Johansen, Digdir* | **European Cybersecurity Competence Network and Centre (ECCC)**<br>- Nyeste satsingen fra EU på cybersikkerhetsområdet er å etablere dette senteret. Skal sørge for gjennomføring av forordninger og direktiver (som NIS-direktivet bl.a.)<br>- Består av ett europeisk kompetansesenter og egne nasjonale koordineringssentre, også i Norge.<br>- Mål med nasjonalt koordineringssenter: støtte opp under EUs eget kompetansesenter.<br>- Hvem burde ta denne rollen i Norge? Forskningsrådet, Digdir og NSM er koblet på.<br>- Visse land har gått for public-private-partnerships. Andre land som i Sverige er det kun offentlig sektor i regi av MSB, Vinnoba og DIGG, som vil lede det nasjonale senteret.<br><br>**Spørsmål**: Vedr. EØS-innlemmelse, hva bør skje først?<br>**Svar**: Innlemmelse må skje først, men føringen fra JD er at Norge ønsker å delta.<br>**Spørsmål**: Hva er budsjettrammen?<br>Svar: Maks 2 millioner hvorav 1 million euro skal gå til å støtte tredjeparter via cascading grants til SMB-er og andre nasjonale søkere, dvs man kan ikke få 2 millioner euro til å støtte bygging av nasjonalt koordineringssenter. Støtten man får er 50%, så det nasjonale senteret må komme opp med resterende 50% selv (og det kan tenkes at mange land søker om mindre enn 1 million euro). Budsjettet er for en 24 måneders periode. |