Samfunnssikkerhet og beredskap

DMF har i brev til NFD av 15. januar 2013 vurdert at etaten ikke har ansvar for noen objekter som faller inn under kriteriene for skjermingsverdige objekter, eller særlig samfunnskritiske funksjoner som medfører behov for særskilte tiltak ut over grunnleggende sikringstiltak. DMF vurderer fortsatt at etaten ikke har skjermingsverdige objekter eller særlig samfunnskritiske funksjoner.

DMF har gjennomgått og skjerpet adgangskontroll inn til egne lokaler i 2017. Risiko for skade på eget personell er vurdert å være størst i forbindelse med reiser og tilsyn. DMF har innført som standard at befaringsreiser og tilsyn alltid skal gjennomføres av minst 2 personer. Ved reiser hvor store deler av organisasjonen eller DMFs ledelse reiser samtidig, vurdere risiko særskilt. Flyreiser for større grupper fordeles på ulike avganger.

IKT-sikkerhet
Størst risiko for DMF er fortsatt vurdert å være knyttet til IKT-sikkerhet. DMF har gjennomført tiltak for å redusere risiko knyttet til IKT-sikkerhet. Dette omfatter sikker plassering av DMFs servere (2015), etablering av eget domene (2016) og bruk av offentlige, sikre felleskomponenter så langt som mulig. Det er gjennomført en risikovurdering som del av beslutningsgrunnlaget for valg av sentrale tekniske løsninger. Det er derfor valgt å ikke benytte sky-løsninger.

DMF har fulgt opp anbefalinger fra Nasjonale sikkerhetsmyndigheter (NSM) i henhold til fellesføringer i tildelingsbrevet for 2017.

I 2017-2018 innførte vi NSM sine viktigste anbefalinger til lokal sikkerhet på våre medarbeideres PC-er. Dette medførte bl.a. at man som hovedregel ikke har lokal Admin-tilgang. Erfaringen så langt er at dette fungerer bra, men det har medført noen praktiske utfordringer for vår medarbeider på Svalbard.

Vi har ikke hatt alvorlige hendelser på lokale PC-er etter innføring av tiltak.

Vi har videre innført 2-faktor autentisering på VPN og Citrix-løsninger, og vil fortsette arbeidet med å innføre 2-faktor som hovedregel på alle eksterne påloggingsløsninger (epost, portal, eksternt prosjektområde m.m.).

Alle våre nettbaserte tjenester kjører på https, og vi stiller krav til at alle eksterne tjenester som vi benytter kjører på https. Pålogging via ID-porten til vår selvbetjeningsportal «Min side» fungerer utmerket for "norske" brukere.

Etter å ha jobbet med fysiske tiltak de siste årene, har vi i 2018 hatt fokus på opplæring av ansatte for å redusere IKT-risikoen ytterligere. Alle ansatte har gjennomført e-læringskurs i forbindelse med nasjonal sikkerhetsmåned. Toppleder og IKT-ansvarlig gjennomførte også kurs for ledere i forkant. Vi planlegger å følge opp med flere kurs i 2019.

DMF har i 2018 identifisert og kartlagt hvilke personopplysninger DMF behandler i henhold til den nye personopplysningsloven (GDPR).

Det er inngått avtale om prioritert abonnement for mobilnett i beredskapssituasjoner.

Sikkerhet i digitale tjenester
DMFs hjemmeside ble oppgradert i 2015. Sikkerhetsnivået på siden er oppgradert til sikkerhetsscore A i 2016. Sikkerheten på «Min side» har også sikkerhetsscore A. SLLabs.com er benyttet til testing av sikkerhetsnivå for både www.dirmin.no og Min side. Pålogging til Min side benytter ID-porten. Tilgang til rapportering via Min side styres via roller i Altinn. Det benyttes kun https i all web-basert kommunikasjon.

Atea har på oppdrag fra DMF i 2018 gjennomført en «securitycheck» av våre servere og vårt nett. Det ble ikke avdekket alvorlige avvik, men noen mindre avvik ble fulgt opp og lukket av vår IT-avdeling.

Sikkerhet i nasjonale felleskomponenter
DMF har tatt i bruk følgende nasjonale felleskomponenter i våre saksbehandlingssystemer og tjenester: Altinn, SvarUt, ID-porten, Difis kontakt- og reservasjonsregister, digitale registre fra Brønnøysundregistrene (enhetsregistret mm), Folkeregisteret og digitale offentlige kart-tjenester gjennom Norge Digitalt-samarbeidet.

DMF vurderes å være svært avhengig av de nasjonale felleskomponentene både i egen saksbehandling og for leveranse av tjenester til våre brukere. DMF har imidlertid konkludert med at tilgangen til de nasjonale felleskomponentene ikke er samfunnskritisk, og kan leve med en viss nedetid.