12 Sikkerhets- og tilgangsløsninger

12.1 Formål og hovedprinsipper

Offentlige organer er underlagt flere ulike rettslige regelverk for informasjonssikkerhet, avhengig av hva slags informasjon de behandler og av hvilken funksjon organet har i samfunnet. Et gjennomgående trekk ved mange regelverk for informasjonssikkerhet er at de er basert på et internkontrollprinsipp. Det innebærer at regelverket trekker opp rammer for organets egne vurderinger av risiko, og beslutninger om utforming og iverksetting av sikkerhetstiltak. Målet for tiltakene er å ivareta informasjonens konfidensialitet, integritet og tilgjengelighet.

For en Noark-løsning dreier de fleste sikkerhetskravene seg om kontroll med tilgang til, bruk av og endring av metadata og dokumenter. Andre typer sikkerhetstiltak, som for eksempel sikkerhetskopiering og tiltak mot skadelig programvare, ivaretas normalt utenfor Noark-løsningen. Noark 5 har ikke som mål å dekke alle sider ved et offentlig organs informasjons-sikkerhet. Noark-løsningen må innordnes under og virke sammen med øvrige sikkerhetstiltak og tekniske infrastruktur. Noark-løsningen skal kunne konfigureres og brukes på en måte som er forenlig med organets egne mål og strategier for informasjonssikkerhet, besluttet i tråd med relevante rettslige rammer.[18]

Sikkerhetskravene for Noark 5 kjernen består derfor av en relativt beskjeden mengde obligatoriske krav, som er begrunnet i konfidensialitet, integritet og tilgjengelighet for arkiver, metadata og dokumenter. Antallet anbefalte sikkerhetsfunksjoner som en komplett Noark 5-løsning bør ha er derimot relativt høyt. En anbefalt funksjon i kravtabellene må det enkelte organ som tar i bruk en ekstern løsning selv vurdere om de har behov for å implementere. Det enkelte organs behov for å implementere ulike anbefalte funksjoner vil variere med informasjonens sensitivitet, organets arbeidsprosesser, samhandlingsmønstre, teknisk integrasjon, hva som er relevant rettslig regelverk på det aktuelle område etc.

Sikkerhetskravene er i de fleste tilfeller rene funksjonelle krav. Det stilles altså i liten grad konkrete ”styrkekrav”. Det vil si at det ikke settes målbare krav til hvor sterkt hver sikkerhetsfunksjon skal tvinges gjennom av løsningen, eller krav til hvor vanskelig det må være å omgå funksjonen.

12.1.1 Sikkerhetsfunksjoner versus sikkerhetsmål

Kravene til informasjonssikkerhet i Noark 5 er funksjonsorienterte. Det vil si at de er knyttet til ”ting som foregår” ulike steder i løsningen, enten i kjernen eller i en ekstern løsning. Innen informasjonssikkerhetsfaget er det kanskje mer utbredt å utforme krav til sikkerhets*mål*. Målene angis gjerne gjennom krav til de tre aspektene konfidensialitet, integritet og tilgjengelighet. Målorienterte krav kan være bedre egnet til å få fram det enkelte organs behov for og ansvar for å avveie kravene mot hverandre. Målorienterte krav gir også større fleksibilitet til å finne ulike virkemidler og tiltak for å oppnå tilstrekkelig sikkerhet.

[18] Hva som er relevante rettslige rammer for informasjonssikkerhet vil være noe forskjellig i ulike forvaltnings-organer. Avhengig av hva slags opplysninger som behandles, og hvilket beskyttelsesbehov opplysningene har, kan for eksempel personopplysningsloven § 13 med personopplysningsforskriften kapittel 2, sikkerhetsloven, eller eForvaltningsforskriften § 13 stille krav til organets helhetlige arbeid med informasjonssikkerhet.