Kommunal- og moderniseringsdepartementet

Handlingsplan for informasjonssikkerhet i statsforvaltningen – 2015–2017

Innhold

Executive summary

The Ministry of Local Government and Modernisation (KMD) is responsible for coordinating the Government's policy for ICT in the public sector and is therefore also responsible for information security in this sector. Pursuant to the Cyber Security Strategy for Norway (2012), KMD also has specific responsibility for promoting a stronger and more comprehensive approach to information security in public administration. The team of information security experts in the Agency for Public Management and eGovernment (Difi) acts as KMD's executive body for achieving this objective.

KMD has prepared a two-year action plan (2015–2017) for information security in the public sector to meet this responsibility.

The action plan contains three objectives:

1) The general public, business and industry, and government itself must feel confident that all internal systems and networks and all digital services that are developed and operated by public-sector agencies are secure and reliable.

2) The sectoral ministries must have a common understanding of the specific challenges public administration faces in connection with developing and operating digital services.

3) Leaders, developers, system operators and users employed in public administration must gain more competence in and greater awareness of the need for information security.

The action plan defines five areas where measures will be implemented to support the plan's objectives: internal control, security in digital systems and services, cyber preparedness, national common components, and knowledge, competence and culture. Individually and combined, these five areas will contribute to achieving the action plan's objectives.

The guiding principles of liability, decentralisation, conformity, and cooperation form the basis of all national security and emergency preparedness activities during peacetime. In addition to these main principles, the action plan bases the work on information security in public administration on the following principles:

- ***Risk management:*** Risk management is the key element in information security. Public administration must possess a sound understanding of risk and must work systematically on risk assessment. Risk management must enable agencies to make informed decisions and set priorities when implementing security measures.

- ***Built-in information security:*** Information security must be part of every public administration digitisation project right from the start and throughout the system's life cycle. Information security must also be a natural element in public sector governance, and a topic with which all employees in public administration should, by virtue of their role, be familiar.

In accordance with the principle of liability, all sectoral ministries will be responsible for following up the action plan within their respective areas of responsibility. In cooperation with their subordinate agencies, the sectoral ministries will facilitate sectoral follow-up and ensure that measures are coordinated with other ministries as necessary. This will particularly apply to agencies with responsibilities linked to developing and operating national common components.

The sectoral measures will be financed within current budgetary frameworks. The cost of the measures to promote information security must be proportionate to the risk estimated for the respective areas of public administration. The risk of adverse consequences and loss must be assessed before risk mitigation measures are implemented.

Innledning

Norge har en nasjonal strategi for informasjonssikkerhet med tilhørende handlingsplan. Denne ble utgitt i 2012, og omhandler i hovedtrekk de sikkerhetsutfordringene som samfunnet står overfor. Det enkelte fagdepartement er ansvarlig for at strategien blir fulgt opp innenfor deres sektor.

Informasjonssikkerhet defineres her som hvordan informasjonen beskyttes mot uønsket innsyn (konfidensialitet), at informasjonen er tilgjengelig når det er ønskelig (tilgjengelighet), og at informasjonen er beskyttet mot endring/manipulering (integritet).

En sentral målsetning i Nasjonal strategi for informasjonssikkerhet er å sørge for at statsforvaltningen har en felles tilnærming til arbeidet med informasjonssikkerhet. Dette er Kommunal- og moderniseringsdepartementets (KMD) ansvar. Med bakgrunn i dette legger KMD nå frem en egen handlingsplan. Foruten å styrke informasjonssikkerheten i statsforvaltningen ønsker KMD at denne handlingsplanen skal bidra til å understøtte KMDs arbeid med å koordinere digitaliseringsarbeidet i offentlig sektor. Informasjonssikkerhet er her et viktig element for å bygge tillit til forvaltningens systemer, nettverk og de offentlige elektroniske tjenestene. I sum skal handlingsplanen understøtte regjeringens ambisjoner om å fornye, forenkle og forbedre statsforvaltningen og offentlig sektor som helhet, ved blant annet å ta i bruk de mulighetene som teknologien gir oss.

Handlingsplanens primære målgruppe er toppledelsen og sikkerhetsansvarlige i alle departementer. KMD forventer også at ledelsen i departementene, gjennom etatsdialogen, bringer videre føringene i handlingsplanen til ledelsen i de respektive underlagte virksomheter.

Handlingsplanen er en del av Nasjonal strategi for informasjonssikkerhet. Den er avgrenset til innretningen av arbeidet med informasjonssikkerhet i statsforvaltningen. Tiltaksområdene som skal iverksettes skal primært bidra til en helhetlig tilnærming til informasjonssikkerhet i statsforvaltningen.

Aktiviteter og tiltak som faller inn under sikkerhetslovens virkeområde (f.eks. beskyttelse av samfunnskritisk infrastruktur, objektsikkerhet mv.) er utenfor denne handlingsplanenes nedslagsfelt, og blir således ikke adressert direkte.

Selv om handlingsplanen omhandler statsforvaltningen vil det være tiltaksområder i planen som også kan ha relevans for offentlig sektor som helhet, herunder kommunene. Et konkret eksempel er etterlevelsen av eforvaltningsforskriftens § 15 (som forvaltes av KMD) hvor det fremgår at alle forvaltningsorgan som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi). Direktoratet for forvaltning og IKT (Difi) har her utarbeidet råd og veiledninger som alle virksomheter i offentlig sektor kan benytte, også kommunene.

Handlingsplanens tre delmål:

1) Befolkningen, næringslivet og forvaltningen skal ha tillit til at alle interne systemer og nettverk, samt alle digitale tjenester som utvikles og driftes i regi av virksomheter i offentlig sektor, er sikre og pålitelige.

2) Fagdepartementene skal ha en felles forståelse om hvilke særskilte utfordringer statsforvaltningen står overfor i forbindelse med utvikling og drift av digitale offentlige tjenester.

3) Ledere, utviklere, driftsansvarlige og brukere ansatt i statsforvaltningen skal få økt kompetanse og bevissthet omkring behovet for informasjonssikkerhet.

For å understøtte målsetningene er det fem tiltaksområder i handlingsplanen:

1) styring og kontroll
2) sikkerhet i digitale tjenester
3) digital beredskap
4) sikkerhet i nasjonale felleskomponenter
5) kunnskap, kompetanse og kultur

De fem tiltaksområdene skal hver for seg, og i felleskap, bidra til at handlingsplanens målsetninger blir nådd.

Handlingsplanens tidshorisont er avgrenset oppad til to år. IKT er et dynamisk fagfelt, og sikkerhetsutfordringene er i stadig endring. Dette kan medføre behov for å foreta endringer i tiltaksområdene. Risikobildet vil også kunne endre seg som følge av innføring av ny teknologi, at sikkerhetstiltak etableres, og at fagområdet påvirkes som følge av endringer i IKT-politikken for statsforvaltningen. Handlingsplanens tiltaksområder er likevel av mer langsiktig art. Innenfor en tidsramme på to år kan man starte en rekke tiltak, og i noen grad også måle effekt av tiltakene, men det er først over en lengre tidshorisont man vil kunne se den fulle effekten av de tiltakene som iverksettes.

Styrende prinsipper for arbeidet med informasjonssikkerhet

Overordnede prinsipper om ansvar, nærhet, likhet og samvirke ligger til grunn for alt nasjonalt sikkerhets- og beredskapsarbeid i fredstid. Disse prinsippene vil også være styrende for arbeidet med informasjonssikkerhet i statsforvaltningen.

- *Ansvarsprinsippet* innebærer at den etat som har ansvar for et fagområde i en normalsituasjon, også har ansvaret for å håndtere ekstraordinære hendelser på området.
- *Likhetsprinsippet* betyr at den organisasjon man opererer med til daglig skal være mest mulig lik den organisasjon man etablerer under kriser.
- *Nærhetsprinsippet* innebærer at kriser organisatorisk skal håndteres på et lavest mulig nivå.
- *Samvirkeprinsippet* stiller krav til at myndighet, virksomhet eller etat har et selvstendig ansvar for å sikre et best mulig samvirke med relevante aktører og virksomheter i arbeidet med forebygging, beredskap og krisehåndtering.

I tillegg til disse hovedprinsipper, legger handlingsplanen opp til at arbeidet med informasjonssikkerhet i statsforvaltningen skal bygge på følgende forutsetninger:

Risikostyring: Risikostyring er kjernen i arbeidet med informasjonssikkerhet. Virksomhetene i statsforvaltningen skal ha god risikoforståelse og arbeide systematisk med risikovurderinger. Risikostyring skal gjøre virksomhetene i stand til å ta informerte valg og gjøre prioriteringer ved innføring av sikkerhetstiltak.

Innebygd informasjonssikkerhet: Informasjonssikkerhet skal være en del av ethvert digitaliseringsprosjekt i statsforvaltningen fra starten, og i hele systemets livssyklus. Informasjonssikkerhet skal også være en naturlig del av virksomhetsstyringen, og et tema som alle ansatte i statsforvaltningen – ut fra sin rolle – skal ha et kjennskap til.

Ut over ovennevnte prinsipper og forutsetninger må alle virksomhetene følge de særskilte nasjonale og sektorielle krav som følger av regelverket den enkelte virksomhet er omfattet av. Det er her en gjennomgående forventning i alle disse regelverkene at sikringen baserer seg på en risikovurdering foretatt av den enkelte virksomhet.[1]

1 Ref Reglement for økonomistyring i staten § 4 Grunnleggende prinsipper

KMDs særskilte ansvar for å styrke informasjonssikkerheten i statsforvaltningen

Av Nasjonal strategi for informasjonssikkerhet (2012) fremgår det at det er fagdepartementene som har hovedansvaret for å ivareta sikkerheten i sektorenes IKT-infrastruktur, og for at det forebyggende informasjonssikkerhetsarbeidet i sektoren er tilfredsstillende. Hovedtyngden av alt informasjonssikkerhetsarbeid foregår således i sektorene, og da primært i den enkelte virksomhet. Beskyttelse av sektorenes samfunnskritiske IKT-infrastruktur har høyeste prioritet.

I tråd med ansvars-, nærhets-, likhets- og samvirkeprinsippet ligger det til grunn at hvert enkelt fagdepartement har et selvstendig ansvar for å føre tilsyn med, og følge opp, informasjonssikkerhetsarbeidet i egne underlagte etater og virksomheter spesielt, og i sektoren generelt. Dette bør inngå som en del av etatsstyringen.

Iht. Kgl.res. av 22.03.2013[2] har Justis- og beredskapsdepartementet (JD) et *ansvar for samordning av forebyggende IKT-sikkerhet i sivil sektor*. Samordningsansvaret innebærer at JD skal utforme en nasjonal politikk og nasjonale krav på IKT-sikkerhetsområdet. Slike krav vil kunne omfatte både offentlig og privat sektor. Rammer og krav skal være hjemlet i relevante lover og forskrifter.

Videre fremgår det av resolusjonen at Nasjonal sikkerhetsmyndighet (NSM) skal være det nasjonale fagmiljøet for IKT-sikkerhet, og skal understøtte JDs ansvar på området. NSM skal i denne sammenheng videreutvikles for å styrke den systematiske tilnærmingen til IKT-sikkerhetsutfordringene, og – ikke minst – vår kapasitet til å løse dette.

KMD har ifølge resolusjonen et særskilt ansvar for å arbeide for en styrket og mer helhetlig tilnærming til informasjonssikkerhet i statsforvaltningen, som følge av å være ansvarlig for å koordinere regjeringens politikk for IKT i offentlig sektor. KMD vil i utøvelsen av dette ansvaret forholde seg til de rammer og krav satt av JD som *samordningsansvarlig* departement på IKT-sikkerhetsområdet i sivil sektor, og andre krav som følger av relevante lover og forskrifter på området.

KMDs særskilte ansvar på informasjonssikkerhetsområdet er av *forebyggende* art, og innebærer i praksis å foreta valg av felles standarder, stille krav om internkontroll på informasjonssikkerhetsområdet, tilby veiledning på et overordnet nivå, tilrettelegge for en bedre koordinering av etatenes arbeid med informasjonssikkerhet samt drifte enkelte nasjonale fellesløsninger (f.eks. ID-porten og Sikker digital postkasse til innbyggerne). KMD skal i tillegg fremskaffe et kunnskapsgrunnlag om den generelle informasjonssikkerhetstilstanden i statsforvaltningen, og vurdere behovene for å iverksette særskilte tiltak i denne sammenheng. For å ivareta denne oppgaven har KMD i 2013 opprettet et kompetansemiljø i Direktoratet for forvaltning og IKT (Difi).

Kompetansemiljøet i Difi er KMDs utøvende organ for å nå målsetningen om en styrket og mer helhetlig tilnærming til informasjonssikkerhet i statsforvaltningen. KMD vil selv, ved behov, også kunne gjennomføre koordinerende aktiviteter på departementsnivå.

KMD har også – som ledd departementets ansvar for å koordinere regjeringens politikk for IKT i offentlig sektor – gitt Direktoratet for forvaltning og IKT (Difi) et ansvar for å lede Samarbeidsrådet for styring og koordinering av tjenester i e-forvaltning (SKATE).

2 Kgl.res. av 22.03.2013 Overføring av samordningsansvaret for forebyggende IKT-sikkerhet fra Fornyings-, administrasjons- og kirkedepartementet til Justis- og beredskapsdepartementet.

KMD utøver sitt koordineringsansvar med bakgrunn i følgende regelverk og bestemmelser:

- Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)
- Kgl.res av 19.12.1997 Omorganisering av departementsstrukturen fra 1. januar 1998 (jf. Pkt. 4 Overføring av samordningsansvaret for Regjeringens IT-politikk)
- Kgl.res. av 07.10.2005 Om et organ som har koordineringsansvar for forvaltningens bruk av sikkerhetstjenester og -produkter ved elektronisk kommunikasjon med og i forvaltningen (jf. eForvaltningsforskriften §36)
- Kgl.res av 22.03.2013 Overføring av samordningsansvaret for forebyggende IKT-sikkerhet fra Fornyings-, administrasjons-, og kirkedepartementet til Justis- og beredskapsdepartementet.
- Forskrift om IKT-standarder i offentlig forvaltning (Standardiseringsforskriften)
- Forskrift om frivillige selvdeklarasjonsordninger for sertifikatutstedere (Klageinstans jf. § 15)
- Personopplysningsforskriften

Statsforvaltningens utfordringer som følge av digitalisering

IKT-sikkerhet en svært viktig dimensjon, men ikke det eneste kriteriet når det foretas viktige strategiske valg. For sterk vekt på informasjonssikkerhet kan i noen tilfeller også være produktivitetshemmende ved at samfunnsøkonomisk lønnsomme prosjekter hindres, eller ikke blir gjennomført, pga. for strenge krav til informasjonssikkerhet. Risikovurderinger og bevissthet om akseptabel risiko bør derfor alltid ligge til grunn for en gjennomtenkt avveining mellom informasjonens konfidensialitet, tilgjengelighet og integritet. Hovedhensikten med risikoanalyser er først og fremst å bli klar over egen risikosituasjon, og basert på denne kunnskapen iverksette risikoreduserende tiltak, eller på annen måte sikre en forsvarlig håndtering av egen risiko.

Ambisjonen om økt digitalisering i offentlig sektor betyr også at informasjonssikkerhet blir viktigere. Dette gjelder særlig for de nasjonale fellesskomponentene, og for andre viktige systemer i forvaltningen.

En felles tilnærming til sikkerhetsutfordringer kan være svært nyttig med tanke på økt digital samhandling innad i statsforvaltningen, i offentlig sektor som helhet, og med brukere av offentlige tjenester. Samtidig er det like viktig at ansvaret ikke blir pulverisert. Ansvaret for gode og brukervennlige digitale tjenester innebærer også ansvaret for at tjenestene er sikre. Brukervennlighet og god sikkerhet koster, og skal sikres innenfor en virksomhets til enhver tid gjeldende budsjettrammer. Med utgangspunkt i regjeringens nye prinsipper for bedre styring og ledelse i staten vil en virksomhetsleder stå fritt til å velge virkemidler som skal sikre brukervennlige, sikre og kostnadseffektive IKT-løsninger.

Digitaliseringen av statsforvaltningen, og offentlig sektor generelt, kan skape flere informasjonssikkerhetsutfordringer. Noen konkrete eksempler på dette kan være:

Eksponering: For at ambisjonen om digitalt førstevalg skal lykkes må de av forvaltningens digitale tjenester som retter seg mot publikum og næringsliv være pålitelige, troverdige og tilgjengelige for alle. Det skal være enkelt og trygt å kommunisere digitalt. De digitale tjenestene skal bidra til å opprettholde tillit til statsforvaltningen. Samtidig vil de digitale tjenestene kunne eksponere forvaltningens digitale infrastruktur for feil og tilsiktede handlinger som kan true den grad av informasjonssikkerhet som forventes. Digitale tjenester rettet mot publikum og næringsliv forutsetter dessuten at statsforvaltningen er knyttet til et åpent nett med de tekniske utfordringer som det bringer med seg.

Automatisering av saksbehandling og vedtak: Bidrar til gevinstrealiseringen som følge av en vellykket digitalisering. Dette representerer et skritt videre innen digitalt støttet saksbehandling. Automatisering vil kreve sporbarhet, og at informasjonssikkerhet er bygget inn i programvaren. En konsekvens av digitaliseringen er at de tradisjonelle papirarkivene blir erstattet med digitale medier. Automatisering av vedtak vil kreve at forståelig dokumentasjon av automatisert saksgang og vedtak kan gjenfinnes i pålitelige digitale arkiv.

Samhandling: Innføring av ny teknologi som gir enkle og effektive løsninger fører også til at samfunnet som helhet blir mer avhengig av teknologien og den nye infrastrukturen. Det må derfor legges vekt på at den digitale infrastrukturen bygges tilstrekkelig robust. Informasjonssikkerhet må vektlegges fra starten slik at kritiske avhengigheter kan avdekkes tidlig. Offentlige virksomheter skal tilby effektive og brukervennlige tjenester for innbyggere, næringsliv og offentlig sektor. Det er i denne sammenheng forutsatt at disse tjenestene skal bruke forutsigbare og robuste nasjonale felleskomponenter. Felleskomponenter er i utgangspunktet komponenter

som flere andre systemer er avhengige av, og hvor avhengigheten gjerne er tverrsektoriell. Felleskomponentene krever derfor at både komponenteier og brukere etablerer en felles risikoforståelse for å oppnå tilfredsstillende grad av informasjonssikkerhet.

Kompetanse: Den utstrakte digitaliseringen av offentlig sektor medfører et utstrakt styrings og -kompetansebehov. Virksomhetsledelsen må f.eks. ha kompetanse til å jobbe med intern styring av informasjonssikkerheten, finne frem til gode og kostnadseffektive rutiner og prosedyrer, implementere tekniske tiltak, og foreta investeringer i kompetanse.

Kontroll og oversikt: Den økte samhandlingen internt i forvaltningen skaper tekniske og organisatoriske utfordringer. IKT-systemer blir stadig mer komplekse ved at tidligere atskilte systemer integreres. Resultatet av denne integrasjonen er at det kan være vanskelig å få oversikt over alle potensielle sikkerhetskonsekvenser, og at ingen enkelt virksomhet har den fulle og hele oversikten over alle nettverk og systemer.

Felles krav: Dagens IKT-løsninger i offentlig sektor er komplekse og sammensatte. Systemene er også i forskjellige stadier av sitt tekniske livsløp. Når det gjelder tekniske sikkerhetstiltak vil det være krevende å utvikle ett sett med felles tekniske krav for statsforvaltningen, eller alle virksomheter i offentlig sektor. Eventuelle fremtidige krav bør samsvare med risikobasert tilnærming til sikkerhet, og være hjemlet i relevante lover og forskrifter. Når det gjelder løsninger for departementsfelleskapet peker enkelte utredninger på at det vil bli dyrt for flertallet av departementene dersom sikkerhetsbehovene til et fåtall departementer med mye graderte dokumenter skal være bestemmende for dimensjoneringen av sikkerhet i IKT-løsningene i øvrige departementer uten tilsvarende behov.[3] Samtidig har departementene behov for en helhetlig, brukervennlig og sikker løsning for intern kommunikasjon.

3 Utredning om effektivisering mv av de administrative funksjonene i departementsfellesskapet, Rapport 2014, Capgemini Consulting/Agenda Kaupang

Risikobildet

Informasjonssikkerhetsarbeidet i statsforvaltningen skal bygge på det enhver tid gjeldende risikobildet. Denne handlingsplanens tiltaksdel tar utgangspunkt i NSMs rapport Risiko 2015[4], Nasjonalt risikobilde for 2014 (DSB)[5] og ENISA[6] Threat Landscape 2014.

NSMs vurdering er at sikkerhet har fått en tydeligere plass på dagsordenen, og at mange virksomheter gjør mye godt arbeid for å redusere risiko. NSM konkluderer med at mange virksomheters evne til å forebygge og forhindre sikkerhetstrusler har økt. Samtidig ser de at mottiltakene ikke utvikles i samme takt som truslene. Dette er et kontinuerlig løp, og NSM understreker derfor at det er viktig å fortsatt styrke arbeidet med å redusere gapet mellom trusler og sikkerhetstiltak. Tall fra Norwegian Computer Emergency Response Team (NorCERT) i NSM viser økning både i antall sikkerhetshendelser og i alvorlighetsgrad.

DSBs nasjonale risikobilde inkluderer to scenarier under risiko-området "det digitale rom": cyberangrep mot finansiell infrastruktur og cyberangrep mot elektronisk kommunikasjonsinfrastruktur. Begge scenarioer viser at et målrettet cyberangrep mot disse infrastrukturene kan få store konsekvenser, men at sannsynligheten for at slike hendelser inntreffer vurderes som lav. DSB presiserer at usikkerheten knyttet til denne sannsynlighetsvurderingen er stor.

ENISAs rapport omtaler teknologiske trusler og utviklingen av disse. I tillegg gir denne rapporten en oversikt over trender og kommende trusler innenfor et utvalg områder. Under omtalen av hendelser som medfører konfidensialitetsbrudd viser ENISA til en europeisk undersøkelse[7] som avdekket at 57 prosent av hendelsene skyldes forhold internt i virksomhetene, og ikke innbrudd fra eksterne aktører.

ENISAs undersøkelse viser at en stor andel av de uønskede hendelser som truer informasjonssikkerheten skyldes menneskelige feil, feil i programvare, utstyrsfeil eller naturhendelser. En analyse av sikkerhetshendelser i 95 land i 2014 forteller at 412 av 1367 hendelser med bekreftet informasjonssikkerhetsbrudd har slike årsaker.[8] Respondentene i EU-kommisjonens konsekvensutredning vedrørende forslag til Nettverks- og informasjonssikkerhetsdirektiv (NIS-direktivet) har gitt svar som samsvarer med dette.[9]

Difi har også gjennomført flere kartlegginger[10] [11] [12] som en del av grunnlaget for å forstå risikobildet i statsforvaltningen og offentlig sektor som helhet. Dette kartleggingsarbeidet viser at mange virksomheter har utfordringer med å få på plass et styringssystem for informasjonssikkerhet som fungerer i praksis, som oppleves som nyttig, og som henger sammen med virksomhetens helhetlige internkontroll. Flere virksomheter mangler også felles forståelse av hva risiko er, og hvilken risiko som kan defineres som akseptabel.

4 Nasjonal sikkerhetsmyndighet
5 Direktoratet for samfunnssikkerhet og beredskap
6 European Union Agency for Network and Information Security (ENISA)

7 Data Breaches in Europe: Reported Breaches of Compromised Personal Records in Europe, 2005-2014. Center for Media, Data and Society (CMDS), Central European University, 2014.
8 Verizon 2014 Data Breach Investigations Report.
9 SWD(2013) 32 final – Commission Staff Working Document – Impact Assessment accompanying the document Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and security across the Union.
10 SINTEF-rapport A25874 – Behov knyttet til informasjonssikkerhet i forvaltningen
11 Oppsummering fra workshop: Hvor trykker informasjonssikkerhetsskoen – hva trenger dere fra oss? (Difi)
12 Difi-rapport Rapport 2012:15 Styringssystem for informasjonssikkerhet – Erfaringer med og anbefalinger om standardene ISO 27001 og ISO 27002

Videre viser Difis kartlegginger at det ofte kan være vanskelig å få tilstrekkelig oppmerksomhet om, og forståelse for, informasjonssikkerhet hos ledelsen. Sikkerhetsarbeid blir ofte ikke tilstrekkelig integrert i virksomhetenes daglige arbeid, og blir ikke alltid vurdert som et middel til å nå virksomhetens mål. Difi har også observert at mange virksomheter har for lavt kunnskapsnivå, manglende opplæring av ansatte, og en svak sikkerhetskultur. I sum skaper dette flere sikkerhetsutfordringer på alle nivåer i virksomhetene.

Difis undersøkelser viser også at det er økende oppmerksomhet om sikkerhet under utvikling av nye digitale tjenester og nye interne systemer, men at tenkning omkring informasjonssikkerhet ofte kommer sent i utviklingsprosessen. Ønsket om funksjonalitet vinner ofte over sikkerhetskrav i utviklingsprosjekter. Det er også eksempler på at både bestiller og leverandør ofte mangler kompetanse om hvordan man kan ivareta sikkerhetskrav i utviklingsprosjekter på en god måte.

Avslutningsvis kan det også nevnes at Riksrevisjonen, i Dokument 1 (2014-2015), har påpekt at det er svakheter ved informasjonssikkerheten hos flere statsetater som forvalter store IKT-systemer og viktige samfunnsverdier.

Tiltaksområder for en mer styrket og helhetlig tilnærming til informasjons-sikkerhet i statsforvaltningen

Informasjonssikkerhet konkurrerer med mange andre viktige fagområder i statsforvaltningen. For å få den nødvendige prioriteten, og komme på ledelsens agenda, må informasjonssikkerhet integreres i virksomhetens øvrige mål. Det er viktig at hensynet til informasjonssikkerhet er med fra starten når det gjelder planlegging, utvikling og anskaffelse av IKT-løsninger. En viktig målsetning med handlingsplanen er å redusere antall mulige sårbarheter i systemene i statsforvaltningen, og i offentlig sektor som helhet. Systemutviklings- og driftskostnaden vil være lavere dersom dette kan gjøres i en tidlig fase av utviklingen. Dette bidrar til det som i denne handlingsplanen kalles innebygd informasjonssikkerhet. En annen viktig målsetning i denne sammenheng er at flere virksomheter etablerer god internkontroll for informasjonssikkerhet slik at effekten av sikkerhetstiltak kan følges opp, og konsekvensen av manglende sikkerhetstiltak kommer tydelig frem for virksomhetens ledelse.

KMD har, med bakgrunn i statsforvaltningens sikkerhetsutfordringer på informasjonssikkerhetsområdet, og gjeldende risikobilde omtalt ovenfor, utpekt fem prioriterte tiltaksområder som i felleskap skal bidra til å styrke informasjonssikkerhet i statsforvaltningen. Til grunn for disse fem tiltaksområdene ligger de to overordnede prinsippene som skal prege alt informasjonssikkerhetsarbeidet i statsforvaltningen: *risikostyring* og *innebygd informasjonssikkerhet*.

Hvert enkelt tiltaksområde i handlingsplanen behandler en overordnet problemstilling, og arbeidet som er planlagt kan gi flere mulige sikkerhetstiltak. Handlingsplanens tiltaksområder vurderes å ha lik viktighet. Difi vil, i samarbeid med berørte etater, infrastruktureiere, tilsynsmyndigheter mv., derfor legge opp til en balansert arbeidsinnsats når det gjelder oppfølgingen av de ulike tiltaksområdene. At hvert tiltaksområde behandler én overordnet problemstilling er en tilnærming som legger til rette for at sikkerhetstiltak kan koordineres med andre nasjonale fagmiljø som NSM og DSB slik at de ikke overlapper eller forstyrrer allerede etablerte sikkerhetstiltak. Samarbeid og faglig diskusjon mellom fagmiljøene er også viktig for å understøtte en kontinuerlig forbedring av informasjonssikkerheten i statsforvaltningen.

Den enkelte virksomhet i statsforvaltningen kan prioritere mellom de fem tiltaksområdene ut fra virksomhetens egenart og egne utfordringer, i tråd med nærhetsprinsippet. Virksomhetene har forskjellig grad av modenhet i sin tilnærming til informasjonssikkerhet, og kan velge relevante tiltak som vil være effektive for egen organisasjon.

Følgende tiltaksområder vil prioriteres for å styrke informasjonssikkerhetsarbeidet i statsforvaltningen spesielt, og sektorene generelt:

<table>
<tr><td rowspan="5">Innebygd informasjonssikkerhet</td><td>Styring og kontroll</td><td rowspan="5">Risikostyring</td></tr>
<tr><td>Sikkerhet i digitale tjenester</td></tr>
<tr><td>Digital beredskap</td></tr>
<tr><td>Nasjonale felleskomponenter</td></tr>
<tr><td>Kunnskap, kompetanse og kultur</td></tr>
</table>

Styring og kontroll er rettet mot ledelse og ansatte, og skal bidra til at informasjonssikkerhet er en godt integrert del av virksomhetenes samlede styring og bidra til at den enkelte virksomhet når sine mål.

Sikkerhet i digitale tjenester skal bidra til utveksling av kompetanse og erfaring, samt effektiv bruk av standarder og god bransje-praksis. Tiltaksområdet skal også gjøre det lettere for flere virksomheter å benytte sikker-hetstiltak som er utviklet av andre.

Digital beredskap skal bidra til at virksomhetene raskt oppdager og reagerer ved uønskede hendelser. Digital beredskap skal også bidra til at virksomhetene opprettholder god evne til å utføre prioriterte oppgaver i ekstraordinære situasjoner med minst mulig avvik fra forsvarlig informasjonssikkerhet.

Nasjonale felleskomponenter skal bidra til en bedre koordinering av informasjonssikkerheten i den viktige delen av den nasjonale IKT-infra-strukturen som de nasjonale felleskomponen-tene samlet representerer. Dette forutsetter at virksomhetene som forvalter nasjonale felles-komponenter har en felles risikoforståelse, og dermed også en felles forståelse av kritiske avhengigheter på tvers av virksomheter og sektorer

Kunnskap, kompetanse og kultur skal bidra til at den enkelte medarbeider tilegner seg nød-vendig kunnskap og forståelse om informasjons-sikkerhet for å kunne utføre sine oppgaver og bidra til å oppnå virksomhetens mål. Dette bidrar også til bedre risikoforståelse og utviklingen av en god sikkerhetskultur i organisasjonen.

Tiltaksområde 1: Styring og kontroll

I flere rapporter fra Riksrevisjonen og Nasjonal sikkerhetsmyndighet er det pekt på mangler i ledelse og styring av informasjonssikkerhetsarbeidet i virksomhetene, og at dette er en av de grunnleggende årsakene til at sikkerheten i offentlige virksomheter ikke har vært god nok. Med bakgrunn i dette er en av de strategiske prioriteringene i Nasjonal strategi for informasjonssikkerhet (2012) å *ivareta informasjonssikkerheten på en mer helhetlig og systematisk måte*.

I Nasjonal strategi for informasjonssikkerhet er dette omtalt slik: "(...) *Dette krever bevisst bruk av styringssystemer for informasjonssikkerhet som en del av virksomhetsstyringen. Anerkjente standarder skal legges til grunn. Kravene må tilpasses den risikoen den enkelte virksomhet må håndtere. Virksomhetens karakter, størrelse og samfunnsmessige betydning må være avgjørende for ambisjonsnivået og ressursinnsatsen på sikkerhetsarbeidet."*[13]

God styring og kontroll er helt avgjørende for at en virksomhet skal lykkes med sitt informasjonssikkerhetsarbeid. Styringssystemer er verktøy som skal sikre at ledelsen kan prioritere og ta gode og kostnadseffektive beslutninger. Det gjør virksomhetene i stand til å iverksette de riktige sikkerhetstiltakene og prioritere sine ressurser riktig. Risikovurderinger (herunder verdivurderinger[14]) er et av de verktøy som brukes. Bruk av styringssystemer vil derfor kunne understøtte god rapportering om risikobildet og sikkerhetstilstanden i den enkelte virksomhet.

Av eForvaltningsforskriften §15, som ble endret i 2014, fremgår det at forvaltningsorgan som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi). Disse skal danne grunnlaget for forvaltningsorganets internkontroll (styring og kontroll) på informasjonssikkerhetsområdet. Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annet regelverk. Forvaltningsorganet skal ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem.[15]

Det er stor variasjon i hvor langt statsforvaltningen har kommet med etablering og innføring av styringssystemer for informasjonssikkerhet, hvilken strategi som er brukt på innføring, og hvordan styringssystemet for informasjonssikkerhet er integrert med virksomhetens øvrige system. Difi har gjennomført en kartlegging av behov knyttet til informasjonssikkerhet i forvaltningen[16] som har bidratt til å utforme flere av aktivitetene som er beskrevet i dette tiltaksområdet.

Riksrevisjonen gjennomfører årlig revisjon og kontroll av disposisjonene i alle statlige virksomheter, herunder revisjon av regelverksetterlevelse og virksomhetenes internkontroll. Dette bør sees i sammenheng med at eForvaltningsforskriften § 15 slår fast at styring og kontroll av informasjonssikkerhet skal være en integrert del av den helhetlige virksomhetsstyringen.

Målsetning

For den enkelte virksomhet er målet for dette tiltaksområdet en god og effektiv etterlevelse av eForvaltningsforskriften § 15.

13 Nasjonal strategi for informasjonssikkerhet, kap. 4.1
14 Difis veileder «Internkontroll i praksis – informasjonssikkerhet» vil omfatte verktøy for risikovurdering og kartlegging av informasjonsverdier.
15 Se også Digitaliseringsrundskrivet 2014, punkt 1.6 Informasjonssikkerhet
16 SINTEF-rapport A25874 – Behov knyttet til informasjonssikkerhet i forvaltningen

Difi skal i denne sammenheng bidra til god styring og kontroll av informasjonssikkerheten i offentlige virksomheter ved å:

- Videreutvikle veiledningsmaterialet som hjelper virksomhetene å etablere god internkontroll
- Anbefale god praksis for kontinuerlig forbedring av internkontrollen på informasjons-sikkerhetsområdet.
- Anbefale god praksis for å oppnå sporbarhet fra identifisert risiko til sikkerhetstiltak.
- Gjennom rådgivning, kurs og foredragsvirksomhet være pådriver for at veiledningene blir tatt i bruk.
- Følge opp statsforvaltningens etterlevelse av eForvaltningsforskriften § 15 ved innhenting av statistikk og gjennom dialog med forvaltningsetatene.
- Bidra til samordnet regelverksutvikling på informasjonssikkerhetsområdet.

Tiltaksområde 2:
Sikkerhet i digitale systemer og tjenester

I 2014 ble eForvaltningsforskriften endret slik at hovedregelen nå er at forvaltningen skal kommunisere digitalt med innbyggere og næringsliv. Der det tidligere var krav til samtykke har man nå en reservasjonsrett. Digitalt førstevalg innebærer at man gjennom digitalisering av offentlige tjenester skal legge til rette for økt verdiskapning og innovasjon, og bidra til bedre og mer effektive offentlige tjenester[17] Dette betyr at forvaltningen utvikler stadig flere digitale tjenester, for å understøtte mer effektiv intern saksbehandling og legge til rette for en digital dialog med innbyggere og næringsliv.

En vellykket digitalisering av statsforvaltningen krever at innbyggerne har tillit til løsningene, og at løsningene oppleves som pålitelige, effektive, sikre og brukervennlige. I denne sammenheng må den enkelte virksomhet selv definere behov for informasjonssikkerhet. En kostnadseffektiv tilnærming til denne problemstillingen er å finne fram til løsninger som tilfredsstiller alle disse behovene på en balansert måte. Dette krever tverrfaglighet og tilstrekkelig kompetanse til å være i stand til å finne tekniske løsninger gode løsninger De sikkerhetskravene som stilles må balanseres opp mot med andre viktige samfunnsbehov. God informasjonssikkerhet er viktig både for offentlige tjenester til næringslivet, innbyggerrettede tjenester, og for digitale fagsystemer og saksbehandlingsverktøy som brukes internt i forvaltningen.

Informasjonssikkerhetsbehov må ivaretas allerede fra begynnelsen av prosessen med å utvikle eller anskaffe og forvalte en digital tjeneste.[18] For å oppnå dette må virksomhetene i offentlig sektor arbeide systematisk med informasjonssikkerhet og selv beskrive risiko og etablere tilfredsstillende risikohåndtering i anskaffelser, utvikling, drift og videreutvikling av digitale tjenester. Målsetningen er å redusere antall sårbarheter og å sikre at de digitale tjenestene blir pålitelige og robuste. Ved å ta hensyn til dette allerede ved utvikling og anskaffelse kan informasjonssikkerhet kostnadseffektivt bygges inn i løsningene.

Målsetning

For den enkelte virksomhet er målet for dette tiltaksområdet å forbedre sin evne til å gjøre løpende risikovurderinger for de digitale tjenester virksomheten har ansvaret for. Virksomheten må være i stand til å etablere og fase ut sikkerhetstiltak gjennom hele livsløpet til de digitale tjenestene på en kostnadseffektiv måte. Dette krever at virksomheten kan dokumentere hvilke sikkerhetstiltak som har tiltenkt effekt og hvilke sikkerhetstiltak som koster mer enn de bidrar til å redusere risiko.

17 Digitaliseringsrundskrivet, 26. august 2014

18 SINTEF-rapport A25874 – Behov knyttet til informasjonssikkerhet i forvaltningen. Funn 21: Informasjonssikkerhet involveres ofte for sent i utviklingsprosessen.

Difi vil i denne sammenheng bidra til å styrke informasjonssikkerheten i offentlige systemer og digitale tjenester ved å:

- Utvikle gode tiltak der modenhetskartlegging av programvaresikkerhet i offentlige virksomheter[1] har avdekket behov.
- Forbedre virksomhetenes evne til å kartlegge og møte et risikobilde i kontinuerlig endring ved å anbefale metode og verktøy basert på god praksis i offentlig og privat sektor.
- Utforme relevant og praktisk rettet veiledningsmateriale for å hjelpe virksomhetene med å ta i bruk anbefalte metoder og teknikker).
- Difi skal innarbeide informasjonssikkerhet som en integrert del av Prosjektveiviseren som Difi tilbyr.

Difi vil også vurdere å gjennomføre en ny modenhetskartlegging på området mot slutten av handlingsplanens virketid.

1 SINTEF rapport A26860, 2015-04-10
http://www.difi.no/rapport/2015/04/modenhetskartlegging-av-programvaresikkerhet-i-offentlige-virksomheter

Tiltaksområde 3: Digital beredskap

Alle virksomheter må være forberedt på uforutsette hendelser og ekstraordinære situasjoner. Virksomhetene må ha lagt planer, og sørge for å ha nødvendig personell med tilstrekkelig opplæring og utstyr tilgjengelig på kort varsel i tilfelle det ekstraordinære inntreffer. En viktig del av opplæringen er å øve på bruk av disse planene. Dette bør skje minst en gang i året. Erfaringer fra øvelser må brukes til å forbedre planene. Den digitale beredskap betegner hvor godt en virksomhet er i stand til å håndtere det uventede.

En del av god forebygging er å være forberedt på å håndtere det uventede. Undersøkelsen *Bruk av IKT i staten*[19] for 2014 viser at selv om 73 prosent av virksomhetene har etablert en beredskapsplan er det kun 29 prosent som gjennomfører årlige beredskapsøvelser.

Alvorlige uønskede hendelser kan utfordre virksomhetens evne til å utføre viktige oppgaver også under unormale forhold. Det er laget internasjonale standarder for håndtering av uønskede hendelser og for styring av virksomhetskontinuitet. Disse er godt tilpasset standardene som anvendes i handlingsplanens tiltaksområde 1 Styring og kontroll. Standardene kan, og bør, sees i sammenheng med arbeidet på dette tiltaksområdet. Arbeidet med digital beredskap vil også kunne resultere i veiledere for bruk av disse standardene.

Deltagelse i risikovurderinger og øvelser er viktig for å øke forståelsen for risiko, og det er avgjørende at de som eier risikoen deltar i slike aktiviteter. Øvelser gir erfaring i å håndtere sikkerhetsmessig utfordrende situasjoner og avdekker eventuelle svakheter i beredskapsplanene. Øvelser kan bidra til å synliggjøre kritiske avhengigheter mellom for eksempel virksomheter eller systemer og nettverk. Øvelser øker også risikoforståelsen. Det er derfor viktig å se den digitale beredskapen i offentlig sektor i sammenheng. Det er behov for å øve hver for seg og sammen.

Dette tiltaksområdet vektlegger øvelser med tema informasjonssikkerhet i den enkelte virksomhet. Terminologi og metode vil basere seg på den generelle veiledning om øvelser som er utarbeidet av DSB. Dette tiltaksområdet omfatter ikke større felles øvelser og nasjonale øvelser, men vektlegger å bidra til at flere virksomheter planlegger og gjennomfører interne øvelser. Det forutsettes at dette tiltaksområdet er godt koordinert med andre nasjonale fagmiljøer som NSM og DSB. Den felles øvelsen Difi gjennomfører med deltagere fra Nettverk for informasjonssikkerhet i offentlig sektor (NIFS) skal meldes inn i den nasjonale øvingskalenderen til DSB.

Målsetning

Det primære målet med dette tiltaksområdet er at antallet virksomheter som årlig øver sin IKT-beredskap skal øke. Videre er det en målsetning at også andelen virksomheter som har oppdaterte IKT-beredskapsplaner skal øke. Den enkelte virksomhet bør selv vektlegge å gjennomføre årlige øvelser med klare øvingsmål knyttet til informasjonssikkerhet. Både IKT-beredskapsplaner og øvingsvirksomhet skal være innarbeidet i virksomhetens system for styring og kontroll på informasjonssikkerhetsområdet.

19 Bruk av IKT i staten er en årlig undersøkelse som gjennomføres av Statistisk sentralbyrå, www.ssb.no

Difi vil i denne sammenheng bidra til å styrke den digitale beredskapen i statsforvaltningen gjennom å:

- Gjennomføre felles øvelser med tema informasjonssikkerhet og digital beredskap i forvaltningen for å styrke kompetansen på planlegging og gjennomføring av slike øvelser i fagmiljøet for informasjonssikkerhet.
- Være en pådriver og tilrettelegger for at beredskapsøvelser gjennomføres i den enkelte virksomhet.
- Gi råd om metoder, standarder, og scenarioer som hver enkelt virksomhet kan bruke i egne øvelser.
- Følge opp utviklingen på området gjennom innhenting av statistikk og direkte dialog med virksomhetene.

Tiltaksområde 4: Nasjonale felleskomponenter

Satsningen på fellesløsninger er et strategisk valg forankret helt tilbake i St. meld. nr. 17 (2006–2007). Det er bred enighet om denne satsingen, både på strategisk nivå, og operativt nivå i de offentlige virksomhetene som utvikler digitale tjenester. Tanken bak etableringen av slike fellesløsninger er at en del løsninger som mange offentlige virksomheter har behov for kun skal utvikles én gang, og deretter brukes av mange. Dette reduserer de totale kostnadene, gir brukerne gjenkjennelige grensesnitt å forholde seg til og reduserer kompleksitet. De eksisterende nasjonale felleskomponentene[20] forvaltes av ulike virksomheter underlagt forskjellige fagdepartementer. Dette gir utfordringer knyttet til samordning og sammenheng mellom felleskomponentene.
I tillegg finnes det utfordringer for de mange virksomhetene i offentlig og privat sektor som benytter disse felleskomponentene som et ledd i egne elektroniske tjenester. Det er derfor viktig at felleskomponentene fungerer til enhver tid, er pålitelige og forvaltes på en trygg og sikker måte.

Mange ulike virksomheter kan bruke en felleskomponent som innsatsfaktor for å utføre en eller flere oppgaver. Dermed oppstår det avhengigheter som det er en krevende utfordring for virksomheten som forvalter felleskomponenten å holde seg løpende orientert om. For å vurdere risikoen knyttet til en fellesløsning er det nødvendig å kartlegge disse avhengighetene. Det er særlig viktig å avdekke om en felleskomponent er kritisk for å kunne utføre oppgaver som er kritiske for samfunnet. Denne informasjonen er viktig for å vurdere om en felleskomponent er et skjermingsverdig objekt, jf. sikkerhetsloven og objektsikkerhetsforskriften. Det er sektordepartementet som utpeker skjermingsverdige objekter i egen sektor.

Nasjonale felleskomponenter som ikke er utpekt som skjermingsverdige objekter kan likevel utgjøre en virksomhetskritisk innsatsfaktor for flere virksomheter i offentlig sektor. Avhengighetene kan også være sektorovergripende. Disse felleskomponentene utgjør derfor en viktig del av den nasjonale IKT-infrastrukturen. Vekt på informasjonssikkerhet må derfor være sentralt i en koordinert utvikling og forvaltning av nasjonale felleskomponenter. Som et ledd i dette arbeidet leder Difi Samarbeidsrådet for styring og koordinering av tjenester i e-forvaltning (SKATE) som er et strategisk samarbeidsråd som skal bidra til at digitaliseringen av offentlig sektor blir samordnet, og gir gevinster for innbyggere, næringsliv og forvaltningen.

For virksomheter som forvalter en nasjonal felleskomponent er det primære målet for dette tiltaksområdet at virksomheten skal samle, og regelmessig oppdatere, en oversikt som viser hvor mange som er avhengig av denne felleskomponenten. Risikovurderinger for en nasjonal felleskomponent skal ta hensyn til slike avhengigheter.

Målsetning

For virksomheter som bruker nasjonale felleskomponenter er det primære målet med dette tiltaksområdet at virksomheten vurderer sin avhengighet av felleskomponentene og tar dette med i sine risikovurderinger.

20 Se Difi-rapport 2010:17 Nasjonale felleskomponenter i offentlig sektor.

Difi vil bidra til å styrke informasjonssikkerheten i nasjonale felleskomponenter ved å:

- Tilby råd og veiledning til de virksomhetene som forvalter nasjonale felleskomponenter.
- Være en pådriver overfor forvalterne av nasjonale felleskomponenter, for å sikre et tilstrekkelig oppmerksomhet om behovet for informasjonssikkerhet i utvikling og drift av disse komponentene
- Arbeide for at internasjonale standarder og rammeverk for sikkerhetsarkitektur tas i bruk som en del av virksomhetsarkitekturen.
- Bidra til at virksomheter som forvalter nasjonale felleskomponenter (anskaffelse, utvikling og drift av slike systemer) deler kunnskap og erfaring og gjør det mulig oppnå en sikker, kostnadseffektiv og koordinert forvaltning av denne viktige IKT-infrastrukturen.

Tiltaksområde 5: Kunnskap, kompetanse og kultur

For at en virksomhet skal kunne ta effektive beslutninger knyttet til informasjonssikkerhet er det viktig å forstå hvilken risiko virksomheten blir utsatt for. Forståelse av risiko innebærer forståelse av *hva* som medfører risiko, *og hvor stor* risikoen er. Virksomhetene i statsforvaltningen må også ha en formening om hvilken risiko som er akseptabel. Det er umulig, og heller ikke kostnadseffektivt, å forsøke å fjerne all risiko som knytter seg til bruk av IKT og Internett.

Forståelsen av risiko varierer mye mellom ulike virksomheter i statsforvaltningen, og mellom ulike grupper i virksomhetene. Dette gjelder både mellom ulike tilsynsmyndigheter, og mellom teknikerne og ledere i den enkelte virksomhet. Vurdering av risiko avhenger ofte av den intuitive forståelsen de involverte har av hvilken risiko som er akseptabel. I den enkelte virksomhet er denne forståelsen ofte ikke dokumentert, og heller ikke diskutert i ledelsen. Siden det er lederne som er ansvarlige for informasjonssikkerheten, og det er de som tar de sentrale beslutningene, er det svært viktig at ledere har en god forståelse av hva risiko er, og hva som er akseptabelt risikonivå.

KMD har gjennomført en analyse av behovet for avansert IKT-kompetanse fram mot 2030[21] som viser at etterspørselen etter personer med avansert IKT-kompetanse overgår dagens tilbud av personer med denne kompetansen. Analysens framskrivinger viser at det er en betydelig økning i behovet for IKT-utdannede fram mot 2030. Dette er en utfordring som også vil ramme arbeidet med informasjonssikkerhet. Mangelen på kompetent IKT-sikkerhetspersonell er dessverre ikke noe nytt. Dette ble også påpekt av sårbarhetsutvalget i 2000: "(...) *Kompetansemangelen er stor på IKT-området, og det er ofte et problem å få tak i dyktige IKT-medarbeidere som behersker systemene.*[22]

Virksomhetene i forvaltningen har behov for tilstrekkelig kunnskap og kompetanse om informasjonssikkerhet for å kunne utføre sine kjerneoppgaver og nå virksomhetens overordnede mål. Kompetansebehovene er ulike for ulike roller i virksomhetene.[23] Den enkelte ansatte har behov for tilstrekkelig kunnskap om informasjonssikkerhet for å utføre sitt daglige arbeid på en trygg og sikker måte i tråd med gjeldende retningslinjer i virksomheten. En etatsleder har behov for kunnskap om informasjonssikkerhet som understøtter strategisk ledelse. En etatsstyrer i et departement trenger kunnskap om informasjonssikkerhet for å følge opp virksomhetene i sektoren, og en saksbehandler trenger kunnskap om informasjonssikkerhet som er praktisk anvendbar innenfor eget fagområde.

Sikkerhetskultur er summen av de ansattes kunnskap, motivasjon, holdninger og atferd som kommer til uttrykk gjennom virksomhetens totale sikkerhetsatferd[24]. Det å skape en felles forståelse av risiko og utvikle en god sikkerhetskultur i statsforvaltningen er utfordrende, ressurskrevende og tar tid.

Difi gjennomførte tidlig i 2015 en undersøkelse[25] for å kartlegge hvilke opplæringstiltak virksomhetene har gjennomført eller har planlagt i 2015, samt hva det er ønskelig at Difi bidrar med på dette området. Det er den enkelte virksomhet selv som må kartlegge behovene i egen organisasjon, og tilpasse opplæringen ut fra disse

21 DAMVAD og Samfunnsøkonomisk analyse: Dimensjonering av avansert IKT-kompetanse. 12. juni 2014.

22 NOU 2000:24 Et sårbart samfunn, side 39.

23 SINTEF-rapport A25874 – Behov knyttet til informasjonssikkerhet i forvaltningen. Funn 25: Kompetanseutfordringer finnes på alle nivåer og områder i og utenfor virksomheten.

24 https://nsm.stat.no/tjenester/sikkerhetskultur/

25 Opplæringstiltak innen informasjonssikkerhet – oppsummeringsrapport fra undersøkelse – http://www.difi.no/artikkel/2015/02/opplaeringstiltak-innen-informasjonssikkerhet-oppsummeringsrapport-fra-undersokelse

behovene. Det er den enkelte virksomhetsleder som har ansvaret for å sikre at de ansatte i virksomheten har tilstrekkelig kompetanse, og legge til rette for at den enkelte medarbeider får mulighet til å tilegne seg den nødvendige kunnskapen. Tilstrekkelig og tilpasset kunnskap og kompetanse om informasjonssikkerhet vil danne grunnlaget for en god sikkerhetskultur i den enkelte virksomhet.

En annen viktig faktor som er nødvendig for å bygge en god sikkerhetskultur, er å skape gode forutsetninger for å lære av erfaringene til kollegaer i egen virksomhet og andre forvaltningsvirksomheter.[26]

Hvis virksomheten ikke er eier av samfunnskritisk infrastruktur, og derigjennom pålagt å iverksette sikkerhetstiltak, må den enkelte virksomhet ofte selv foreta en vurdering av hva som er nødvendig opplæring for den enkelte ansatte for å sikre at de ansatte har tilstrekkelig sikkerhetskompetanse. Virksomheten må også foreta en vurdering av behovet for å arbeide systematisk med utviklingen av en god sikkerhetskultur internt i virksomheten.

Målsetning

Målet med dette tiltaksområdet er at virksomheten styrker den interne kunnskapen, kompetansen og kulturen innen informajonssikkerhet i alle ledd, og at den totale sikkerhetskulturen i statsforvaltningen styrkes.

Difi vil i denne sammenheng legge til rette for å styrke kunnskap, kompetanse og kultur innen informasjonssikkerhet ved å:

- Organisere og drive praksisfellesskap som legger til rette for informasjonsdeling, slik som Nettverk for informasjonssikkerhet i offentlig sektor (NIFS).
- Utvikle og tilby opplæringstiltak på områder der det avdekkes spesielle utfordringer eller kompetansebehov i forvaltningen. Tiltakene skal være tilpasset rolle og ansvar, og i størst mulig grad være gjenbrukbare i hele forvaltningen.
- Legge til rette for felles tiltak for å styrke sikkerhetskulturen i virksomhetene, som f.eks. e-læringsprogram og kampanjer. Slike tiltak kan om det er hensiktsmessig gjennomføres i samarbeid med f.eks. Norsk senter for informasjonssikkerhet (NorSIS).
- Følge opp utviklingen på området ved innhenting av statistikk fra gjennomførte tiltak Difi tilrettelegger, samt innhente status fra virksomhetene på deres arbeid med opplæring og sikkerhetskultur.

26 SINTEF-rapport A25874 – Behov knyttet til informasjonssikkerhet i forvaltningen. Funn 27: Det kreves god kompetanse på organisasjonsutvikling for å lykkes med sikkerhetsarbeid.

Oppfølging av handlingsplanen

I samsvar med ansvarsprinsippet vil det enkelte fagdepartement ha et ansvar for å følge opp handlingsplanen innenfor sitt ansvarsområde. Fagdepartementene skal, i samarbeid med underlagte virksomheter, sørge for sektorvis oppfølging, og at tiltak i nødvendig grad blir koordinert med andre departementer. Dette vil spesielt gjelde for de virksomhetene som har et ansvar knyttet til utvikling og drift av nasjonale felleskomponenter.

KMD har et samordningsansvar for oppfølging av denne handlingsplanen. Difi skal i denne sammenheng fungere som en tilrettelegger, koordinator og pådriver innenfor de fem omtalte tiltaksområdene. I forbindelse med departementenes oppfølging av handlingsplanen forutsetter KMD at betydningen av god informasjonssikkerhet i statsforvaltningen på et generelt grunnlag blir formidlet til underlagte virksomheter. Dette kan med fordel inngå som en del av etatsdialogen, og tekster som understreker behovet for å arbeide målrettet på informasjonssikkerhetsområdet bør inngå som en naturlig del i fagdepartementenes årlige tildelingsbrev, gjerne med vekt på aktuelle risikoområder. Det vil ikke bli utformet en fellesføring, i stedet vil det være opp til det enkelte fagdepartement å formulere en tekst tilpasset sektorens behov.

KMDs digitaliseringsrundskriv gir føringer for hvordan virksomhetene skal digitalisere for å tilby bedre tjenester og effektivisere driften. Rundskrivet gjelder for departementene, statens ordinære forvaltningsorganer, forvaltningsorganer med særskilte fullmakter og forvaltningsbedrifter. Rundskrivet samler viktige pålegg og anbefalinger vedrørende digitalisering, og gir et helhetlig bilde av hvilke føringer som gjelder. I tillegg redegjør rundskrivet for krav til IKT-relaterte satsingsforslag i regjeringens budsjettprosess. Gjennom digitaliseringsrundskrivet kan KMD gi føringer for informasjonssikkerhetsarbeidet i statsforvaltningen for fagdepartementene, statens ordinære forvaltningsorganer, forvaltningsorganer med særskilte fullmakter og forvaltningsbedrifter.

Difi vil så langt som mulig koordinere sine anbefalinger og råd med andre myndighetsorganer på informasjonssikkerhetsområdet. Dette er en viktig forutsetning for å skape en helhetlig tilnærming til informasjonssikkerhet i statsforvaltningen. Difi har en tilnærming til informasjonssikkerhet forankret i forvaltningens IKT-politikk. Difi vil samarbeide med fagmyndigheter som NSM, Datatilsynet, NKOM og DSB for å sikre en felles forståelse av utfordringene forvaltningen står ovenfor, og for å sikre koordinerte og kostnadseffektive tiltak. Formålet med samarbeidet er å unngå overlapping av innsats, og å dra nytte av hverandres spisskompetanse og breddekompetanse på fagområdet informasjonssikkerhet.

I forbindelse med oppfølgingen av denne handlingsplanen vil KMD ta initiativ til at det enkelte fagdepartements ansvar for informasjonssikkerhet i statsforvaltningen blir mer synliggjort. Dette kan skje på flere måter. Eksempler på slike kan være a) at fagdepartementene skal komme med mer forpliktende formuleringer om nivået på informasjonssikkerheten i egen sektor i forbindelse med utarbeidelse av strategier og handlingsplaner, b) at fagdepartementene skal rapportere mer systematisk om status i arbeidet, og c) ved at flere fagdepartementer (og deres underlagte virksomheter) trekkes mer inn i det praktiske samordningsarbeidet for eksempel gjennom Difis nettverk for informasjonssikkerhet i offentlig sektor (NIFS).

KMD vil, halvveis i handlingsplanens virkeperiode, innhente status på departementer arbeid med handlingsplanen, herunder deres innsats på de fem prioritert tiltaksområdene i egen sektor.

Innhentingen av departementsrapporter vil bli avstemt med annen rapportering på sikkerhetsområdet. For å kunne se arbeidet som utføres i statsforvaltningen i en helhetlig sammenheng vil en samlet rapport om status for informasjonssikkerheten i statsforvaltningen bli presentert og behandlet i Nettverk for informasjonssikkerhet ledet av JD, der alle departementene deltar. En overordnet rapport vil deretter, i samarbeid med JD, bli lagt frem for regjeringen til orientering. JD kan på selvstendig grunnlag fremme ev. forslag til tiltak i etterkant av slik rapportering.

KMD vil evaluere Difis virkemiddelapparat på informasjonssikkerhetsområdet etter handlingsplanens utløp for å kontrollere at direktoratets innsats fungerer etter hensikten.

Økonomiske og administrative konsekvenser

Primæransvaret for sikring av informasjonssystemer og nett ligger hos den enkelte virksomhet, og er ledelsens ansvar. Sikkerhetsarbeidet må ivaretas i daglig oppgaveløsning, og finansieres innenfor rammene for finansiering av den ordinære virksomheten. Hvert fagdepartement har her et sektoransvar.

Tiltak i sektorene skal finansieres innenfor gjeldende budsjettrammer. Størrelsen på kostnadene til tiltak for å fremme informasjonssikkerhet må stå i forhold til den antatte risikoen på de enkelte forvaltningsområdene. Faren for uheldige konsekvenser og tap må vurderes forut for utarbeidelse og iverksetting av risikoreduserende tiltak.

KMD vil, gjennom sitt tildelingsbrev til Difi, bidra til å finansiere fellestiltak og -aktiviteter som gjennomføres i regi av Difi.

Utgitt av: Kommunal- og moderniseringsdepartementet

Offentlige institusjoner kan bestille flere eksemplarer fra:
Departementenes sikkerhets- og serviceorganisasjon

Internett: www.publikasjoner.dep.no
E-post: publikasjonsbestilling@dss.dep.no
Telefon: 222 40 000

Publikasjonskode: H-2353
Design: 07 Oslo
Trykk: Departementenes sikkerhets- og serviceorganisasjon
09/2015 – opplag 250