Nasjonal strategi for informasjonssikkerhet

Handlingsplan

Oslo, 17. desember 2012

Innhold

Innledning

Nasjonal strategi for informasjonssikkerhet ble lansert av regjeringen 17.12.2012.

Denne handlingsplanen beskriver mer i detalj hvordan strategiens prioriteringer skal følges opp. Handlingsplanen utgis separat, og skal revideres ved behov.

Handlingsplanen er delt inn i to deler:

- En utfyllende beskrivelse av dagens sikkerhetsutfordringer og trender på området
- Et utvalg tiltak som er strategisk viktige, og som det er vedtatt skal gjennomføres.

Tiltakslisten fokuserer i hovedsak på de tiltakene som departementene og underlagte virksomheter har et ansvar for å følge opp. Gjennomføringen av tiltakene vil også ha konsekvenser for, og kreve medvirkning fra, kommunesektoren og privat sektor. Proaktivitet og evne til handling i alle ledd er nødvendig for det nasjonale informasjonssikkerhetsarbeidet.

Den raske teknologiske utviklingen på dette området tilsier at det må tas forbehold om at handlingsplanen ikke vil være fullt ut dekkende til enhver tid. De tiltakene som her blir opplistet kan også bli justert og endret fortløpende som følge av for eksempel nye sikkerhetsutfordringer, introduksjon av ny teknologi eller organisasjonsendringer som kan medvirke til at de prioriterte tiltakene må tas opp til ny vurdering.

Sikkerhetsutfordringer og trender

I dette kapittelet gis det en oversikt over de mest fremtredende sikkerhetsutfordringene og trendene som enkeltvis, eller i sum, kan påvirke den nasjonale informasjonssikkerheten. Oversikten er oppdatert per desember 2012.

Samfunnet er mer avhengig av IKT-infrastruktur

Samfunnet har i de senere årene blitt mer sårbart for selv kortere driftsavbrudd i systemer og nett. Den økte sårbarheten skyldes økt teknisk kompleksitet, men også at befolkningen, organisasjoner, næringsliv og forvaltning er avhengig av fungerende IKT i langt større grad enn tidligere.

IKT, herunder internett, inngår som en integrert del av kritisk infrastruktur og de fleste samfunnsfunksjoner er avhengig av infrastrukturen for å fungere tilfredsstillende. Tendensen er at ulike typer enheter, maskiner og brukere kobles sammen på nye måter. Når så mange ting skal fungere samtidig må IKT-infrastrukturen være robust. Eksempelvis vil det gjelde for overvåknings- og styringssystemer for industri og næringsliv, private husholdningers bruk av automatisk avlesning av strømforbruk og for systemer for kjøretøy på veiene. Det er en utfordring å forstå samfunnets avhengigheter i forhold til de nye og mer komplekse teknologiske systemene.

Konsekvenser av ekstremværet «Dagmar»

Ekstremværet «Dagmar» rammet blant annet Nord-Vestlandet 25.desember 2011 og førte til konsekvenser på veldig mange samfunnsområder. Det omfattende og langvarige bortfallet av strøm- og teleforsyningen ble av mange oppfattet som den alvorligste konsekvensen av uværet. Hendelsen viste at samfunnet i for liten grad har planlagt for å kunne håndtere langvarige bortfall av ekomtjenester. Tall fra Post- og teletilsynet viser at et stort antall basestasjoner ble satt ut av spill. Det estimeres at ca. 20 000 husstander var uten fasttelefon og ca. 7500 uten

internett/bredbånd. Deler av sendernettet til Norkring falt også ut. For mange varte bortfallet av strøm og ekomtjenester i flere døgn. I enkelte områder varte bortfallet i flere uker. Også kystradiotjenesten ble rammet da stasjonen Florø radio falt ut under ekstremværet.

Det er et tett avhengighetsforhold mellom IKT-infrastruktur og strømforsyning. Tilbydere av IKT-infrastruktur og -tjenester har i varierende grad beskyttet seg mot uregelmessig tilførsel av strøm, men i hovedsak er denne beskyttelsen dimensjonert for korte utfall. Sikker tilgang på kraft er særlig kritisk for tilbyderne og for virksomheter som er avhengig av IKT. Denne avhengigheten representerer en vesentlig sårbarhet i et moderne samfunn som Norge.

Konvergens i nett, terminaler og tjenester skaper økt kompleksitet

Statistikk fra Post- og teletilsynet viser at bruken av mobiltelefon har økt fra 12 prosent av taletrafikken i 2001, til 72 prosent i første halvår 2012. Vi ser også at veksten i taletrafikken avtar noe, mens det er en kraftig økning i datatrafikken over mobilnettene. Med denne endringen i bruksmønsteret følger det en stor nedgang i antall brukere som har tradisjonell fastnettelefon. Samtidig forventes det at ekomnettet skal kunne brukes til utveksling av alt fra enkle tekstmeldinger og telefonsamtaler, til styring av komplekse industrisystemer. Teknologien i telefonnettet fornyes. Det teknologiske generasjonsskiftet er både en utfordring og en mulighet til å sikre at disse tjenestene fortsatt har den stabilitet og sikkerhet som brukere forventer.

Måten innhold distribueres over internett på har endret seg betydelig på grunn av økt bruk av audiovisuelle tjenester som genererer store datamengder. Nye typer tjenesteplattformer, som for eksempel nettbaserte tjenester, vil også bidra til denne endringen. Dette er en utvikling som kan gjøre det mer krevende for brukere å vurdere risiko og sårbarhet i tjenestene de benytter.

Redundans gjør IKT-systemer mer robuste. Redundans kan oppnås gjennom etablering av alternative framføringsveier for signalkabler og duplisering av styringssystemer og databaser. Dette kan igjen medføre systemer med høy kompleksitet og tett kobling mellom ulike deler av nettverkene, noe som i seg selv kan gi sårbarheter og flere tilgangspunkter til nettet. Redundans vil ofte medføre høyere investeringer i etablering av nett, og tilfredsstillende stabilitet vil kreve at tilbydere har høy kompetanse på drift av tjenester og nett.

Sårbarheter i program- og maskinvare

Sårbarheter finnes i alle typer program- og maskinvare. Produsentene er kjent med dette, og de arbeider fortløpende med å kartlegge og tette disse sikkerhetshullene. Sikkerhetshull kan benyttes til ondsinnet aktivitet. Derfor vil de mest nyttige sikkerhetshullene for en trusselaktør være de som produsentene ennå ikke har fått kjennskap til og utviklet kode for å tette svakhetene til. Manglende rutiner for sikkerhetsoppdatering av programvare og nettverkskomponenter i virksomhetene og befolkningen generelt bidrar til å forsterke dette problemet. Det går ofte lang tid fra en produsent lanserer en oppdatering til alle virksomheter har oppdatert sine nettverk og systemer. Dette gjelder særlig for store komplekse systemer. På den andre siden må man være sikker på at nye programvareversjoner ikke har svakheter som vil påvirke ellers sikre og stabile systemer. Det eksisterer i tillegg mange egenproduserte, ofte bransjespesifikke, systemer. Feil, mangler og sårbarheter i disse kan få store konsekvenser.

Oppdatering av programvare som blir brukt til å styre og kontrollere industriproduksjon og kritisk infrastruktur kan føre til avbrudd i produksjon og leveranser. Samtidig kan en sårbarhet i programvaren utnyttes til å sabotere både industriproduksjon, leveranser av strøm og elektronisk kommunikasjon eller andre viktige samfunnsfunksjoner. Gammel programvare blir ofte ikke fjernet fra systemene, noe som kan medføre mangelfull sikkerhet. Det er en utfordring at eldre systemer ikke kan oppgraderes fordi nye versjoner av delsystemer og operativsystemer ikke er kompatible med andre delsystemer. I tillegg vil det i enkelte tilfeller ikke finnes tilgjengelige oppgraderinger. Systemer som tidligere ikke har vært tilknyttet internett kobles i mange tilfeller til nettet uten at en kjenner risikoen dette medfører.

Det er en urovekkende utvikling at sårbarheter også kan finnes i selve maskinvaren i IKT-systemene. Særlig risikabelt vil det være om sårbarhetene er plassert i maskinvaren for å kunne gi uautoriserte tilgang til informasjon i, eller kontroll med, systemene. Nye terminaler som mobiltelefoner og lesebrett er i utgangspunktet ikke mer usikre enn en tradisjonell PC, men de krever like fullt at brukeren får oppdatert sikkerhetsopplæring og installerer sikkerhetsprogramvare. Sårbarheter som følge av den økte bruken av mobilapplikasjoner vil bli mer synlige i tiden fremover.

Økt risiko for målrettede angrep på IKT-infrastrukturen

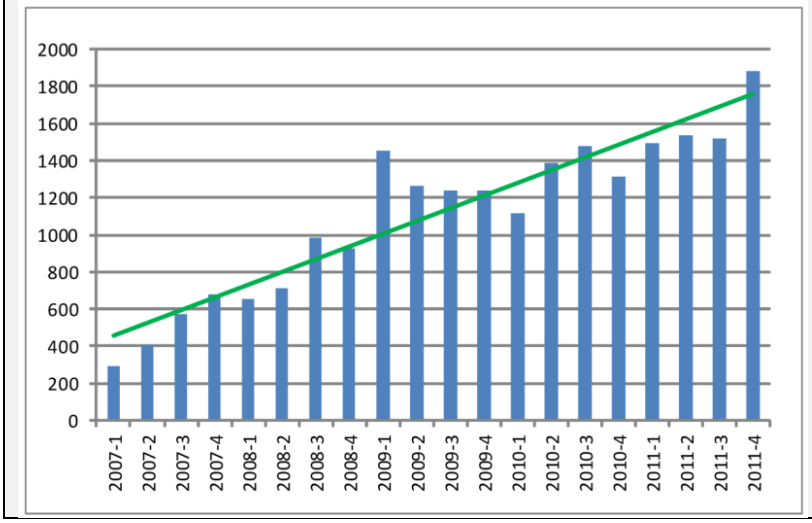
I de årlige trusselvurderingene fra myndighetene blir det konstatert at trusselen knyttet til IKT-basert spionasje og sabotasje har økt de siste årene. Mange stater bygger opp etterretnings- og angrepsevne til bruk i og mot IKT-infrastruktur. Målrettede spionasjeaktiviteter mot vitale nasjonale sikkerhetsinteresser utgjør nå en betydelig sikkerhetsutfordring. Målet med aktivitetene kan være å skaffe seg tilgang til, manipulere eller fjerne sensitiv informasjon. Vi må regne med at sofistikerte sabotasje- og påvirkningsangrep vil bli rettet mot samfunnskritiske informasjonsressurser, herunder datasystemer som styrer industriprosesser og kritisk infrastruktur.

Dataspionasje mot Norge
I 2011 ble det oppdaget dataangrep rettet mot olje- og gassektoren, energisektoren og forsvarsindustrien. Samme aktør står trolig bak en rekke forsøk på spionasje, hvor spesiallagde e-poster er sendt til utvalgte personer for å stjele alt fra dokumenter og industritegninger til brukernavn og passord. Det er første gang Norge avdekker et så omfattende og bredt dataspionasjeangrep.

Angrep på IKT-infrastruktur utføres av mange forskjellige aktører, fra tradisjonelle hackere til politiske aktivister på nett, kriminelle og representanter for staters etterretningstjenester. De siste årene har nasjonale operative erfaringer vist at det oppdages et økende antall aktiviteter og operasjoner med høy alvorlighetsgrad. Noen av de mest alvorlige truslene mot Norge og norske interesser kommer fra andre stater som med nettverksangrep og -operasjoner spionerer på statsforvaltning, Forsvaret, industri og finansinstitusjoner og ikke minst sine egne lands dissidenter og opposisjonsgrupper i Norge. I spente situasjoner og under kriser vil fremmede stater, enten på egen hånd eller gjennom mellomaktører, kunne spre desinformasjon og skade kritisk kommunikasjonsinfrastruktur for å begrense vår nasjonale handlefrihet.

Stadig flere IKT-hendelser
NSMs avdeling NorCERT oppdager stadig flere IKT-hendelser i Norge. Antall håndterte IKT-hendelser er tredoblet fra 2007 til 2011. Mange av sakene er håndtert med enkle grep eller videreformidling av informasjon til andre aktører nasjonalt og internasjonalt, men det kan også ta

måneder med analyse og arbeid for å håndtere de mest alvorligste tilfellene, som digital spionasje. Tallene utover i 2011 og 2012 viderefører utviklingen som beskrevet i grafen nedenfor.



Internett har raskt blitt et viktig verktøy for moderne internasjonal kriminalitet. Det benyttes i økende grad for å utføre bedrageri, narkotikahandel, våpensmugling mv. Denne utviklingen er blitt tydeligere og vil bli mer truende i årene framover.

Mangelfull sikkerhet hos privatpersoner kan også få konsekvenser for samfunnssikkerheten. Sentralt i denne sammenheng står den utstrakte bruken av botnet – nettverk bestående av titusentalls av virusinfiserte pc-er kontrollert av kriminelle aktører uten eiernes viten. Disse brukes til å stjele brukerinformasjon (f.eks. kredittkortinformasjon) og virksomhetsinformasjon (f.eks. strategier, patenter mv.). Den stjålne informasjonen selges videre på det illegale markedet, og brukes blant annet til identitetstyveri, utpressing og svindel av kredittkort og nettbanker. Botnet brukes også til å sende ut uønsket e-post i stor skala, eller til utleie til aktører som vil drive kriminell aktivitet som sabotasje av datanettverk, nettsider og annet. Utfordringene knyttet til effektiv forfølgelse av slike kriminelle handlinger er store, blant annet på grunn av vanskelig sporbarhet. Graden av sannsynlighet for å kunne iretteføre påvirker politiets prioriteringer av slike saker. Handlingenes globale og grenseoverskridende natur stiller dessuten store krav til internasjonalt samarbeid.

Utsetting av arbeidsoppgaver utfordrer mulighetene for kontroll og tilsyn

Norske foretak setter i økende grad ut drifts- og systemutviklingsoppgaver til leverandører som befinner seg i andre land og på andre kontinent. Ansvaret for virksomhetens informasjonssikkerhet kan ikke utkontrakteres. Dersom kontraktsvilkårene ikke er klare, og det ikke finnes mulighet for kontroll/verifikasjon, kan det oppstå en driftsmessig utfordring. Lokale driftsforhold og andre lands regelverk og praksis på området kan for eksempel avvike fra norske krav til sikker IKT-drift. Nasjonalt tilsyn og mulighetene til å føre kontroll med hvordan den utkontrakterte virksomheten håndterer data kan bli svekket. Det kan også være vanskelig å skjerme mot eventuelle utro tjenere.

Utkontraktering av kritiske IT-driftsoppgaver

Finanstilsynet er kjent med at flere banker og andre finansforetak i Norge har utkontraktert hele eller deler av sin IKT-virksomhet til leverandører utenfor Norge. En ny situasjon oppsto i 2010 da EDB flyttet deler av sin virksomhet til et deleid selskap av EDB i Ukraina. Finanstilsynet foretok derfor en nærmere undersøkelse av forholdene, og konstaterte manglende, mangelfulle og utilstrekkelige risikoanalyser, både hos leverandøren og berørte foretak. Alvorlige sikkerhetsbrudd

ble også avdekket.

Den utstrakte praksisen med å sette ut datatjenester til utlandet kan på sikt også føre til at deler av kritisk infrastruktur i praksis styres utenfor Norges grenser. Stabiliteten i det daglige kan dermed forringes ved at virksomhetene, og norske myndigheter, har liten innflytelse på situasjoner som for eksempel arbeidskonflikter og streiker ved utenlandske datasentraler som leverer tjenester som har innvirkning på kritiske samfunnstjenester til Norge. Slik utsetting av tjenester kan i tillegg vise seg å være problematisk i en beredskapssituasjon, hvor evne til styring må være garantert av hensyn til nasjonal sikkerhet.

Nettbaserte tjenester har bredt om seg de siste årene. De nærmeste årene vil informasjonslagring i all privat og offentlig virksomhet vokse betydelig. Enkelte norske tjenestetilbydere kan garantere at tjenestene deres utføres og lagres i Norge, og enkelte globale aktører kan garantere at tjenestene utføres innenfor EU/EØS-området. Mange av skytjenestene utføres imidlertid utenfor landets og EUs grenser, og kjøperen vet oftest ikke i hvilket land tjenestene utføres, hvordan de utføres eller hvor dataene lagres. Virksomhetenes og myndighetenes mulighet til å føre kontroll blir vanskelig. I denne situasjonen vil andre lands lover og regler kunne slå inn. Dette kan f.eks. berøre informasjonens konfidensialitet (jf. myndigheters rett til innsyn i databaser) og spørsmål om hvem som eier de lagrede dataene.

Mange av de tekniske komponentene som virksomhetene bruker i sine nettverk og systemer, produseres utenfor Norge. Ved behov for å få utført service og reparasjoner sender leverandørene ofte ut teknisk personell og utstyr fra en sentralisert enhet. Svikt i transportsektoren, som f.eks. flyforsinkelser og kanselleringer, kan dermed indirekte skape store driftsproblemer for et foretak som har basert sin virksomhet på denne typen serviceavtaler. Dette gjør Norge sårbart for globale hendelser som naturkatastrofer, finanskriser og politisk ustabilitet.

På sikt kan en offensiv bruk av utkontraktering til utlandet føre til nedbygging av norsk IKT-kompetanse, slik at gjenværende IKT-kompetanse blir redusert til ren bestillerkompetanse. På sikt kan dette svekke den nasjonale evnen til å ivareta den tekniske siden ved informasjonssikkerheten. Det er i dag få store datasentraler i Norge, og dermed få norske valgmuligheter. Dette vil kunne føre til at foretakene må se utover landets grenser ved valg av drifts- eller utviklingsleverandør.

Endringer i måten teknologi tas i bruk på skaper nye sikkerhetsutfordringer

Forskjellen mellom mobiltelefoner, nettbrett og bærbare pc-er har i løpet av de senere årene blitt mindre tydelig, og disse terminalene kan i stor grad brukes til de samme tjenestene. Skillet mellom hva vi kaller telefon og hva vi kaller datamaskin er i større grad et uttrykk for terminalens størrelse og ikke funksjonalitet. Nedlastning av både arbeidsrelatert og privat informasjon til samme terminal skaper nye risikobilder. Tjenester som tradisjonelt har vært håndtert på sikre systemer, utføres på systemer som i større grad er åpne. Dette gjør det til en stadig større utfordring å sikre at informasjon ikke kommer på avveie og å beskytte utstyret mot ondartet programvare.

Smarte mobilterminaler og nettbrett gjør at nye tjenester kan utnytte avansert funksjonalitet og skape nye innovative tjenester. Samtidig kan slike tjenester hente opplysninger om hvor brukeren er og hvem som bruker telefonen. Dette skaper utfordringer for personvernet, og det kan være vanskelig for den enkelte bruker å kontrollere hvilke opplysninger som lagres i telefonen og hva slags

opplysninger som gjøres tilgjengelige for tilbydere av både elektroniske kommunikasjons- og innholdstjenester. Store og omfattende databaser er også en utfordring, og representerer en økende trussel for informasjonssikkerheten dersom disse dataene ikke forvaltes av profesjonelle driftsaktører.

Mange organisasjoner bruker nettverk og systemer som er mer standardisert enn tidligere. Dette åpner for utstrakt gjenbruk av programvare og for sammenkobling av virksomheters datasystemer ved hjelp av internett på tvers av organisasjonsstrukturer og sektorer. Teknisk integrasjon av verdikjeder over nettet utfordrer etablerte samarbeidsmønstre mellom organisasjoner. En kunde kan raskt forflytte seg mellom datasystemer hos flere virksomheter for å bestille en vare eller en tjeneste. Overføring av brukerdata fra system til system skjer ofte ved at tiltrodde brukere får adgang til virksomhetenes systemer uten ny autentisering og autorisasjon.

Ansvarsprinsippene for informasjonssikkerhet i egen organisasjon blir også utfordret av virksomhetenes nye måter å samarbeide på. Offentlige virksomheter vil dele eller gjenbruke programvarefunksjonalitet (felleskomponenter) i langt større grad enn tidligere. I et slikt perspektiv vil informasjonssikkerhetsvurderinger være helt sentrale. Blant annet vil en ikke lenger alene kunne basere seg på virksomhetens egen sikkerhetspolicy. Trenden med etablering av felleskomponenter, som Altinn og ID-porten, bidrar til økt profesjonalisering av sikkerhetsarbeidet, men det stiller også skjerpede krav til koordineringen.

Utover den standard som sikkerhetsloven representerer, hemmes utveksling av sensitiv informasjon i forvaltningen av mangel på en felles tilnærming for klassifisering av informasjon og informasjonssystemer, og av omforente krav til sikringstiltak. Utgangspunktet har vært den enkelte virksomhet, den enkelte sektor eller det enkelte regelverk. Dette medfører at samhandlingsevnen svekkes og at informasjon blir inkonsekvent behandlet ved at sikringstiltak og behandlingsregler for den samme informasjonen i forskjellige forvaltningsorganer varierer.

Manglende sikkerhetsbevissthet utgjør en høy og økende risiko

Kompleksiteten i IKT-systemene, sammen med økningen i antall angrep, krever en stor innsats for å bevisstgjøre om trusler, opplyse om tiltak og påvirke til gode holdninger. Eiere av kritisk infrastruktur har i mange tilfeller for liten bevissthet og kunnskap om sårbarheter, infrastrukturenes gjensidige avhengigheter og hva den enkelte virksomhet må gjøre for å beskytte infrastrukturen.

Det er et stort gap mellom brukerens kompetanse og ressursbruk og angripers vilje og evne til å gå direkte på brukeren. Økende bruk av sosial manipulering (phishing, med mer), der angriperen bruker elementer av frykt, tillitsbygging eller tilfredsstillelse av ønsker, brukes i avanserte målrettede angrep. Brukeren forventes å gjenkjenne falske websider, falske e-poster, falske antivirusprogrammer, suspekte bilder og infiserte vedlegg. I tillegg skal det installeres og brukes sikkerhetsverktøy og sikkerhetsprogrammer som brukeren ikke er i stand til å betjene. Dette er en stor utfordring.

Lav sikkerhetsbevissthet om verdi av informasjon
Næringslivets Sikkerhetsråds Mørketallsundersøkelse for 2012 viser at det er et større gap enn tidligere mellom trusler og sikkerhetstiltak blant norske virksomheter parallelt med at IT-avhengigheten øker. Norske virksomheter, særlig ledere, mangler kunnskap om informasjonssikkerhet og har ikke oversikt over trusler og hendelser. Dette kan forklare at mange

virksomheter ikke har tatt i bruk tilgjengelige sikkerhetstiltak og heller ikke har fokusert på sikkerhetskultur.

Store virksomheter som har immaterielle rettigheter (IPR) eller bedriver forskning og utvikling (FoU) er mer utsatt for dataangrep enn andre virksomheter.

13 % av virksomhetene har opplevd tyveri av IT-utstyr, mens kun 1 % oppgir at de har vært utsatt for tyveri av informasjon. Dette viser at virksomhetene har manglende forståelse for verdien av konsekvensene ved tyveri av informasjon.

Tap av minnepinne og e-post sendt til feil adressat er de viktigste årsakene til at informasjon kommer på avveie.

Aktiv bruk av sosiale medier forutsetter bevisste virksomheter og brukere. Nettsamfunn og nettaktiviteter basert på brukerskapt innhold gjør det mulig å dele informasjon på en helt ny måte. Dette har mange fordeler, men det skaper også en rekke sikkerhetsutfordringer, spesielt relatert til kompetanse- og bevisstgjøring av den enkelte bruker. Det er behov for kunnskap om personvern, potensielle sikkerhetsfarer og det ansvar den enkelte har for å hindre spredning av ondartet programkode med påfølgende konsekvenser for andre brukere på nettet. Sosiale medier har ofte en uformell tone og er preget av en kultur for informasjonsdeling. Grensen mellom det private og profesjonelle kan ofte være uklar. Utvikling av interne retningslinjer for virksomheters bruk av sosiale medier kan være krevende. Informasjon fra nettsamfunn kan gi verdifull bakgrunnsinformasjon som kan benyttes for sosial manipulering.

Kompetanseutfordringene øker i takt med kompleksiteten

Den økte kompleksiteten i systemer og nett har gjort det vanskeligere for bestillere av IKT-systemer å stille klare og presise krav til sikkerhet. Riktig valg av IKT-systemer og leverandører fordrer inngående kjennskap til de tilgjengelige løsningenes styrker og svakheter. Mangel på slik kunnskap kan føre både til feilinvesteringer og utilstrekkelig informasjonssikkerhet. Teknologiens kompleksitet gjør det dessuten vanskeligere for den enkelte virksomhet å ha oversikt over alle sikkerhetsutfordringene som knytter seg til bruk av IKT. Velger man å bruke konsulenter i slike prosesser, uten først å foreta bakgrunnssjekk av de som leies inn, kan man også stå overfor en sikkerhetsutfordring med utro tjenere. Stilles det ikke gode sikkerhetskrav til eksterne leverandører blir det vanskelig å følge opp sikkerheten i produktene og systemene i etterkant.

Utkontraktering av virksomhetens IKT-drift er en juridisk og kompetansemessig utfordring. Klare definisjoner av hvilke tekniske krav som skal omfattes av en avtale, kan være vanskelig. Kompleksiteten kan dessuten føre til at viktige sikkerhetsspørsmål blir glemt eller utelatt i en kontrakt. I utkontrakteringsprosesser er det følgelig svært viktig å vite om leverandøren følger gjeldende lover og forskrifter, samt om det er gjennomført risikovurderinger knyttet til tjenestene som skal leveres. For å opprettholde eget sikkerhetsnivå må man kunne stille riktige sikkerhetskrav. Man må også verifisere at leverandører kan oppfylle sikkerhetskravene. En forutsetning for dette er at også IKT-driftsleverandører kan vise til egen sikkerhetsdokumentasjon.

Virksomheter kan være underlagt mange regelverk som ikke er harmonisert fra myndighetenes side. Regelverk behandler ulike områder og er utformet av ulike myndigheter, Mange har også for dårlig kunnskap om rettsreglenes eksistens, hva kravene går ut på og hvordan de skal eller kan etterleves.

Bevisstheten om sikkerhet hos ledelse, mellomledelse og medarbeidere har et betydelig forbedringspotensial i mange virksomheter. Dette bekreftes i årlige tilsynsrapporter fra bl.a. Datatilsynet, Nasjonal sikkerhetsmyndighet, Finanstilsynet og Riksrevisjonen.

Tiltak som støtter opp om strategiens prioriterte områder.

I denne delen av handlingsplanen listes det opp en rekke tiltak som er, eller vil bli iverksatt på informasjonssikkerhetsområdet. Oversikten lister kun opp et utvalg av alle de aktiviteter som pågår innenfor informasjonssikkerhetsområdet.

Først presenteres tiltak som underbygger flere av strategiens prioriterte områder. Deretter følger tiltak som understøtter de enkelte områdene.

Tiltak som støtter opp under flere av de strategiske prioriteringene

Tiltak 0.1: Etablere forbedret informasjonsunderlag for IKT-risikobildet

Bakgrunn: Oppdatert kunnskap om risikobildet for IKT-systemer er viktig med tanke på sikkerhetsarbeidet generelt, herunder målrettet utvikling av forebyggende tiltak og beredskapstiltak, håndtering av aktuelle hendelser og formidling av tidsriktig informasjon til målgrupper. NSM har fra 2008 hatt i oppdrag å utvikle og vedlikeholde et helhetlig IKT-trusselbilde, senere benevnt IKT-risikobildet. Til støtte for dette arbeidet er det etablert en koordineringsgruppe mellom NSM og de øvrige EOS-tjenestene slik at bildet blir beskrevet på en mest mulig helhetlig måte. Situasjonen er at metodikk og rutiner er innarbeidet, men det mangler empiri for et større analysegrunnlag enn i dag. Dette skyldes delvis manglende innrapporteringsrutiner fra sektorene for data om hendelser og vurderinger.

Tiltak: Det tas initiativ for at innrapportering skal komme bedre på plass fra sektorene til NSM. En viktig forutsetning vil bl.a. være etableringen av CSIRT-miljøer i den enkelte sektor som vil kunne virke som katalysatorer for dette. Kripos og Økokrim er også viktige aktører fordi de har ansvar for trusselvurderinger vedrørende organisert kriminalitet. Det er også viktig å utvikle det internasjonale samarbeidet slik at man får en bredest mulig tilgang til informasjon.

Ansvarlig departement: JD og FD

Tiltak 0.2: Videreføring av kartleggingen av kritiske samfunnsfunksjoner, herunder understøttende infrastruktur og innsatsfaktorer

Bakgrunn: Alle aktører med ansvar for kritiske samfunnsfunksjoner må identifisere hvilke tjenester og oppgaver disse omfatter – og hvilke kritiske infrastrukturer (f. eks. ekomnett) og *innsatsfaktorer* (f. eks. ekomtjenester) disse er avhengige av for å kunne opprettholdes. Kongelig resolusjon av 15. juni 2012 *Instruks for departementenes arbeid med samfunnssikkerhet og beredskap, Justis- og beredskapsdepartementets samordningsrolle, tilsynsfunksjon og sentral krisehåndtering* setter krav til mål- og resultatstyring av samfunnssikkerhetsarbeidet, krav til øvelser, og krav til departementene om å vurdere risiko, sårbarhet og robusthet i kritiske samfunnsfunksjoner i egen sektor. Kravene

utdypes i Meld. St. 29 (2011-2012) *Samfunnssikkerhet*. På oppdrag fra Justis- og beredskapsdepartementet har DSB utredet en modell for overordnet risikostyring som kan benyttes innenfor rammen av de ansvarsprinsipper som gjelder i norsk forvaltning. Modellen omtales som KIKS – kritisk infrastruktur, kritiske samfunnsfunksjoner og er beskrevet i en rapport[1] utgitt i forbindelse med prosjektet. Arbeidet har to dimensjoner: et system for oppfølging av sikkerheten på overordnet nivå, og en tydeliggjøring av hvilke samfunnsfunksjoner som er å regne som kritiske. Identifisering av kritisk infrastruktur følger av dette. I rapporten er kritiske samfunnsfunksjoner og kritiske innsatsfaktorer definert. I tillegg blir innholdet i de forskjellige kritiske samfunnsfunksjonene og innsatsfaktorene konkretisert. Mer presist blir den funksjonsevne samfunnet må være i stand til å opprettholde nærmest uavhengig av hvilke påkjenninger det utsettes for beskrevet.

Tiltak: Foreta en sektorvis konkretisering av hva som ligger i de ulike kritiske samfunnsfunksjonene. Som ledd i dette arbeider DSB nå opp mot ulike sektormyndigheter -og virksomheter for å avklare hva som ligger i de ulike samfunnsfunksjonene og innsatsfaktorene. En slik konkretisering vil føre til en bedre oversikt over sårbarhet og avhengighet til innsatsfaktorer, som ekomtjenester, i samfunnet, og vil kunne bidra til å styrke risikostyringen hos ulike aktører. Arbeidet vil også gi et grunnlag for planlegging og prioritering av forebyggings- og beredskapstiltak og vil kunne bidra til å sikre robuste løsninger og kontinuitet i myndighets- og samfunnsfunksjoner.

Ansvarlig departement: JD, alle sektordepartementer

Tiltak 0.3: Gjennomgang av Koordineringsutvalget for forebyggende informasjonssikkerhet (KIS)

Bakgrunn: KIS ble etablert i 2004. Utvalget omfatter både departementer og etater med særlig ansvar innen informasjonssikkerhet, herunder regelverksansvar.

Tiltak: Gjennomgå utvalgets mandat, sammensetning, arbeidsform og oppgaveløsning for å se om utvalget fungerer etter hensikten.

Ansvarlig departement: JD og FAD

Tiltak 0.4: Videreutvikling av Nasjonal sikkerhetsmyndighet (NSM)

Bakgrunn: Det endrede trusselbildet siden NSM ble opprettet har skapt behov for en mer helhetlig tilnærming til de ulike sikkerhetsutfordringene som samfunnet står overfor, på tvers av dagens sektortenkning. Endringer i sikkerhetstilstanden generelt gir et økt behov for sterkere fokus på blant annet beskyttelse av informasjon og infrastruktur avbetydning for samfunnskritiske og andre viktige samfunnsfunksjoner. Regjeringen har besluttet å videreutvikle NSM som det sentrale direktorat for informasjons- og objektsikkerhet. FD og JD har opprettet en prosjektgruppe som skal se på etatsstyringsmodell, innretting og oppgaver for direktoratet. En viktig premiss for gruppen er

[1] Sikkerheten i kritisk infrastruktur og kritiske samfunnsfunksjoner – modell for overordnet risikostyring. KIKS.prosjektet – 1. delrapport, DSB 2012.

regjeringens beslutning om særlig å prioritere styrking av arbeidet med forebyggende sikkerhet og IKT-sikkerhet på tvers av samfunnssektorene.

Tiltak: Videreutvikle NSM i tråd med regjeringens beslutning og vurdere anbefaling fra prosjektgruppen.

Ansvarlig departement: FD og JD

Tiltak 0.5: Etablering av et kompetansemiljø for informasjonssikkerhet i statsforvaltningen i Difi

Bakgrunn: Et kompetansemiljø i Difi vil være pådriver når det gjelder bedre styring av informasjonssikkerhet *i statsforvaltningen*, bl.a. gjennom bruk av anerkjente internasjonale standarder. Kompetansemiljøet er også tiltenkt en sentral rolle når det gjelder informasjons- og opplysningsvirksomhet knyttet til informasjonssikkerhet i statlige etater.

Tiltak: Regjeringen har foreslått å bevilge 12 mill. kroner til arbeidet med styrket IKT-sikkerhet i statlig sektor i 2013. Midlene skal nyttes til etablering av et kompetansemiljø for informasjonssikkerhet i Difi.

Ansvarlig departement: FAD

Tiltak 0.6: Revisjon av lov om elektronisk kommunikasjon

Bakgrunn: EU vedtok i 2009 to endringsdirektiver som endrer ”ekompakken” norsk regulering på området bygger på. I tillegg vedtok EU en forordning om opprettelse av The Body of European Regulators for Electronic Communications (BEREC). Samferdselsdepartementet gjennomførte en høring sommeren 2010 for ytterligere å oppdatere ekomregelverket med henblikk på nasjonale behov. Resultatet vil bli fremmet i proposisjon til stortinget.

Tiltak: Ekomloven er under revisjon og Samferdselsdepartementet vil i lovendringen endre kravene til sikkerhet i de offentlige ekomnettene for om nødvendig å kunne stille strengere krav til nett og tjenester.

Ansvarlig departement: SD

Tiltak 0.7: Videreføring av bruken av Standard Norge

Bakgrunn: Standard Norge (SN) deltar aktivt i det internasjonale standardiseringsarbeidet på IKT-sikkerhet innenfor den anerkjente ISO-standarden. Flere norske virksomheter i offentlig og privat sektor bruker disse IKT-sikkerhetsstandardene aktivt i sitt IKT-sikkerhetsarbeid. SN har over flere år bidratt aktivt til utviklingen av disse IKT-sikkerhetsstandardene slik at norske interesser blir ivaretatt i forbindelse med utformingen.

Tiltak. Årlig tilskudd til SN vil bli videreført i 2013.

Ansvarlig departement: FAD

Ivareta informasjonssikkerheten på en mer helhetlig og systematisk måte

Tiltak 1.1: Styringssystem for informasjonssikkerhet i statsforvaltningen basert på standarder

Bakgrunn: Flere departementer har, og flere arbeider med å innføre, krav om styringssystem for informasjonssikkerhet i egen sektor. Direktoratet for forvaltning og IKT (Difi) har anbefalt statsforvaltningen å benytte standarden ISO/IEC 27001 ved etablering av styringssystem for informasjonssikkerhet (Referansekatalogen 3.1). I arbeidet med å implementere relevante kontroller anbefales det å følge strukturen i ISO/IEC 27001 appendiks A og innholdsmessig støtte seg på ISO/ IEC 27002. Det heter videre i anbefalingen at dersom en virksomhet allerede har et operativt styringssystem på andre områder, vil det i de fleste tilfeller være mest hensiktsmessig å oppfylle ISO27001-kravene innenfor rammene av det eksisterende styringssystemet. Anvendelsesområdet gjelder sikker offentlig behandling av beskyttelsesverdig informasjon. Innføring av styringssystem på informasjonssikkerhetsområdet skal ses i sammenheng med styringssystem og rammeverk for risikostyring i andre deler av virksomheten. Dette gjelder andre krav om styringssystem og internkontrollsystem som ligger i økonomiregelverket, internkontrollforskriften (HMS), eforvaltningsforskriften, personopplysningsloven og -forskriften m.v.

Tiltak: FAD har bedt Difi om en vurdering av mulig pålegg om bruk av standardene i statlige virksomheter

Ansvarlig departement: FAD

Tiltak 1.2: Etablering av retningslinjer for informasjonssikkerhet og cyberoperasjoner for forsvarssektoren

Bakgrunn: Ansvaret for informasjonssikkerhet og cyberoperasjoner er plassert på mange aktører i forsvarssektoren. Ansvaret er delvis regulert gjennom instrukser og regulativer, men området er i stadig utvikling og det er behov for å foreta en helhetlig gjennomgang. Det er derfor besluttet å gjennomføre et arbeid for å utvikle en overordnet, helhetlig og integrert tilnærming til forsvarssektorens arbeid innen det digitale rom. Forsvarsdepartementets cyberretningslinjer for forsvarssektoren skal fastsette ansvar, oppgaver og myndighet for departementet og underlagte etater, og bidra til danne rammene for den videre planlegging og utvikling av forsvarssektorens kapabiliteter, struktur og organisering på området.

Tiltak: Det utarbeides og implementeres retningslinjer for informasjonssikkerhet og cyberoperasjoner for forsvarssektoren.

Ansvarlig departement: FD

Tiltak 1.3: Styrke ledelsen av informasjonssikkerhetsarbeidet i Forsvaret

Bakgrunn: Det er viktig å identifisere planlagte og ikke planlagte aktiviteter og prosjekter innen informasjonssikkerhet, for videre å lage en plan for når aktivitetene skal og bør gjennomføres. Dette vil synliggjøre avhengigheter mellom aktiviteter og bidra til å skape et godt beslutningsgrunnlag for Forsvarets prioritering av aktiviteter innen informasjonssikkerhet. Det bør videre etableres en «Sikkerhetsportal» på egnet plattform for å legge til rette for deling av informasjon om trusler, sårbarhet, rutiner og prosedyrer. En slik portal bør også være egnet til å utveksle erfaringer om god praksis med hensikt å kunne etablere Forsvarets «beste praksis» innen sikkerhet.

Tiltak: Det skal etableres en plan for videreutvikling av informasjonssikkerhetsarbeidet i Forsvaret og etableres en sikkerhetsportal med tanke på utvikling og kommunikasjon av beste praksis i etaten.

Ansvarlig departement: FD

Tiltak 1.4: Organisasjonsmessige tiltak i universitets- og høyskolesektoren

Bakgrunn: Det er viktig at sikkerhetsarbeidet ved den enkelte institusjon i universitets- og høyskolesektoren er tilstrekkelig robust. En forutsetning er en felles tilnærming til informasjonssikkerhet.

Tiltak: Kunnskapsdepartementet har gitt UNINETT i oppgave å etablere og lede et sekretariat for informasjonssikkerhet i universitets- og høyskolesektoren. I tillegg til sekretariatet har UNINETT etablert et sikkerhetsforum for universiteter og høyskoler. Forumet skal være rådgivende innenfor området informasjonssikkerhet, beredskap og kontinuitet. Her skal sektoren kunne dele erfaringer og skaffe seg kunnskap om hvordan man kan jobbe effektivt og praktisk innenfor informasjonssikkerhet og beredskap/kontinuitet.

Ansvarlig departement: KD

Styrke IKT-infrastrukturen

Tiltak 2.1: Styrke arbeidet med objektsikkerhet iht. sikkerhetsloven

Bakgrunn: God informasjonssikkerhet krever egenbeskyttelse av datasentre, kabler og kritiske digitale knutepunkt (noder) i fysiske og logisk distribuerte systemer. Denne beskyttelsen må være av både fysisk, administrativ og teknisk art. Forskrift om objektsikkerhet trådte i kraft 1. januar 2011 og skal implementeres over en treårsperiode. Departementene skal utpeke objekter i egen sektor innen 2012, og objekteiere (virksomhetene) skal iverksette egenbeskyttelsestiltak innen utløpet av 2013. Regelverket bidrar til en tverrsektoriell tilnærming til utvelgelse og beskyttelse, og skal sikre at man også tar hensyn til avhengigheter på tvers av sektorer i samfunnet. NSM skal i samarbeid med fagdepartementene ivareta nødvendig koordinering i utvelgelsesprosessen, gi råd og veiledning, og føre et overordnet tilsyn. Sektormyndigheter skal ta initiativ for konkretisering av de funksjonelle krav i sektorregelverket og føre tilsyn med etableringen av nødvendige sikkerhetstiltak for objekter innen sektoren som er utpekt som skjermingsverdige.

Tiltak: NSMs rådgivnings- og veiledningskapasitet styrkes for å tilrettelegge for at sikkerhetslovens krav om utvelgelse og klassifisering av objekter gjennomføres som forutsatt, og at nødvendige egenbeskyttelsestiltak implementeres i samarbeid med sektormyndighetene.

Ansvarlig departement: FD og JD

Tiltak 2.2: Politiets og Forsvarets planlegging av objektsikring

Bakgrunn: Politiets og Forsvarets sikring av objekter er viktige elementer i den helhetlige tilnærming til sikring av samfunnskritisk infrastruktur, herunder IKT-infrastrukturen. I motsetning til objekteiers defensive og forebyggende sikring, består politiets sikring av offensive tiltak og om nødvendig bruk av makt for å hindre eller begrense anslag mot objekter. Forsvaret har, dersom riket er i krig, krig truer, eller rikets selvstendighet eller sikkerhet står i fare, et selvstendig ansvar for objektsikring av objekter som har avgjørende betydning for forsvarsevnen og det militære forsvaret og som er lovlige mål i krise og krig, såkalte nøkkelpunkter. I 2012 ble det vedtatt en ny instruks som tydeliggjør politiets og Forsvarets ansvar for objektsikring ved bruk av sikringssystemer fra politiet eller Forsvaret.

Tiltak: Beredskapssystemet og de etatsvise regelverk for politiet og Forsvaret vil bli gjennomgått og ajourført iht. ny overordnet instruks om objektsikring med sikringsstyrker. Forsvaret og politiet skal med grunnlag i nytt regelverk gjennomgå hvilke objekter som skal sikres. Etatene må også planlegge og øve på denne sikringen. Forsvaret og politiet skal i arbeidet med objektsikring med sikringsstyrker ta hensyn til om objektene er underlagt forebyggende grunnsikringsregler etter sikkerhetsloven og annet regelverk.

Ansvarlig departement: JD og FD

Tiltak 2.3: En robust og pålitelig ekominfrastruktur

Bakgrunn: En robust og pålitelig ekominfrastruktur er en nøkkelfaktor for å levere den informasjonssikkerheten som samfunnet forventer. Den gjensidige avhengigheten mellom infrastrukturen for elektronisk kommunikasjon og infrastrukturen for elektrisk kraft utgjør en sårbarhet som bør følges opp med god risikostyring og regelmessig vurdering av kostnadseffektive sikkerhetstiltak. NVE og PT må sammen fortsette arbeidet med å avdekke felles trusler mot infrastrukturene for ekom og elektrisk kraft og regelmessig gjennomføre felles øvelser for å sikre et tilfredsstillende beredskapsnivå mot hendelser. Et slikt samarbeid mellom NVE og PT er etablert.

Tiltak: Samarbeidet mellom NVE og PT skal videreutvikles. De regionale øvelsene vil fortsette også etter 2013.

Ansvarlig departement: SD

Tiltak 2.4: Begrense konsekvensene ved utfall i ekomsektoren

Bakgrunn: I 2011 ble det gjort erfaring med hendelser som fikk store konsekvenser for infrastrukturen og produksjon av tjenester. Hendelsene har vist at aktører som er avhengig av ekom for å kunne levere nødvendige tjenester i større grad må være forberedt på bortfall av ekom og gjøre nødvendige beredskapsmessige tiltak (som for eksempel alternativ telefoni).

Tiltak: Aktørene i ekomsektoren skal i løpet av 2013 gjennomføre tiltak som begrenser konsekvensene av utfall i forsyningen av elektrisk kraft, og konsekvensene av skade på egen infrastruktur. Dette omfatter oppgradering av løsninger for reservekraft, bedre sikring av transmisjon og beredskapstiltak for å redusere reparasjonstid etter skader.

Ansvarlig departement: SD

Tiltak 2.5: Kommunikasjonssikkerhet i mobilnettene

Bakgrunn: Alle offentlig tilgjengelige ekomnett vil kunne være utsatt for forsøk på avlytting og manipulasjon av kommunikasjonen. Den mest brukte standarden for mobiltelefoni (GSM) var lenge kjent for å ha en høy sikkerhetsgrad. Dette har endret seg over tid, og i dag kan GSM avlyttes med billigere og mer tilgjengelig utstyr. Samtidig har nettverkene blitt mer avanserte med langt flere nettverkselementer levert av ulike produsenter. Utviklingen gjør at ekommyndighetene må vurdere tiltak for å øke sikkerheten i ekomnettene.

Tiltak: PT skal vurdere de eksisterende tekniske løsninger for kommunikasjonskonfidensialitet i de offentlige mobilnettene, og om nødvendig foreslå kostnadseffektive tiltak for å øke sikkerheten på dette området. Dette tiltaket omfatter flere aktiviteter som allerede er påbegynt og hvor arbeidet vil fortsette også etter 2013. Enkelte tiltak vil gjennomføres ved pålegg, og andre tiltak følger av klassifiseringsforskrift hvor selve klassifiseringen skal være gjennomført 1. april 2013 og tiltakene senest 1. juli 2014.

Ansvarlig departement: SD

Tiltak 2.6: Prioritetsordning i mobilnettene for brukere med samfunnsviktige oppgaver

Bakgrunn: Enkelte hendelser kan føre til et skadeomfang som vil gi redusert kapasitet i ekomnettet i en periode. Det er derfor viktig å ha en prioritetsordning som gir brukere med ansvar for samfunnsviktige oppgaver bedre framkommelighet i mobilnettene i en krisesituasjon hvor mobilnettene er overbelastet. Det er særlig i forbindelse med ulykker, strømutfall og uvær at en slik prioritetsordning er viktig.

Tiltak: Tilbydere av mobiltelefoni skal innføre tekniske løsninger for prioritet slik at samfunnskritiske funksjoner kan understøttes best mulig. Ordningen er i første omgang tenkt å gjelde for offentlige telefonitjenester. Andre ekomtjenester kan på et senere tidspunkt bli vurdert for prioritetsordningen. Post- og teletilsynet er gitt i oppdrag å sørge for at det innføres en slik ordning i løpet av 2013. Det er bevilget 30 millioner kroner for å iverksette ordningen. Regjeringen foreslår å dimensjonere ordningen for inntil 10 000 brukere fordelt på nasjonal og regional

kriseledelse, operative beredskapsaktører og diverse støttefunksjoner. Ansvaret for å identifisere brukere av en slik ordning vil ligge innenfor den enkelte sektor. En årsavgift fra prioritetsabonnementene skal finansiere mobiltilbydernes driftskostnader knyttet til ordningen.

Ansvarlig departement: SD

Tiltak 2.7: IKT-infrastrukturen i universitets- og høyskolesektoren

Bakgrunn: IKT-infrastrukturen i universitets- og høyskolesektoren er utviklet og driftet av UNINETT, i samarbeid med sektoren. Forskningsnettet er internettforbindelsen for forskning, undervisning og formidling i Norge og sikrer universitets- og høyskolesektoren høy kapasitet og stor driftssikkerhet. Dette gjelder også IKT-løsningene på campus som i stor grad ble standardisert gjennom Giga-Campusprosjektet.

Tiltak: Forskningsnettet har meget god tilgjengelighet gjennom redundans. I det videre arbeidet med å styrke denne infrastrukturen vil Kunnskapsdepartementet i samarbeid med UNINETT vurdere hvordan integritet og konfidensialitet blir ivaretatt i bruken av forskningsnettet.

Ansvarlig departement: KD

Sørge for en felles tilnærming til informasjonssikkerhet i statsforvaltningen

Tiltak 3.1: Etablere ny IKT-løsning for departementene

Bakgrunn: I lys av dagens risikobilde er det avgjørende at departementene har IKT-løsninger som både ivaretar informasjonssikkerheten og samtidig er effektive og dekker departementenes ulike behov. Departementene har et økende behov for sikre IKT-tjenester som en konsekvens av økt bruk og avhengighet av IKT.

Tiltak: Det er igangsatt et internt prosjekt i FAD som vurderer ulike systemløsninger som kan møte fremtidig trusselbilde samtidig som det utnytter teknologiske nyvinninger som gjør at brukerne i departementene kan behandle, lagre og dele informasjon av forskjellig sensitiv karakter (unntatt høygradert).

Ansvarlig departement: FAD

Tiltak 3.2: Innføring av evne til høygradert datakommunikasjon mellom departementene, underliggende etater og andre sentrale beredskapsaktører i sektorene

Bakgrunn: Under kriser og i beredskapsplanlegging vil det være behov for å dele gradert informasjon med hverandre, og innføring av et slikt system for høygradert datakommunikasjon innebærer at sivile aktører vil kunne motta og formidle viktig, sensitiv og gradert informasjon som ivaretar leveransegaranti, sporbarhet og reell prioritering av informasjonstrafikk.

Tiltak: Regjeringen har bestemt at det skal innføres et nytt system for høygradert datakommunikasjon mellom departementene og sentrale beredskapsaktører i sektor. En

arbeidsgruppe ledet av Justis- og beredskapsdepartementet skal vurdere hvilke aktører i sivil sektor som har behov for høygradert datakommunikasjon. Gammel infrastruktur vil snarest bli erstattes med nytt system hos eksisterende brukere, og dagens løsning holdes i drift frem til dette er gjennomført.

Ansvarlig departement: JD og FD

Tiltak 3.3: Løsninger for sikker mobil kommunikasjon

Bakgrunn: Departementene har lenge vært koblet sammen i et kablet gradert telefonsystem som muliggjør tale på sensitivt og lavgradert nivå. Det er et udekket behov for en mobil løsning som favner informasjonsutveksling på det samme nivået.

Tiltak: Det arbeides for å få på plass en løsning for mobilkommunikasjon av lavgradert og sensitiv informasjon for statsforvaltningen.

Ansvarlig departement: JD og FD

Tiltak 3.4: Elektronisk ID

Bakgrunn: Ved å etablere flere tjenester med høy sikkerhet kan forvaltningen jobbe mer effektivt og frigjøre ressurser. Kost-/nytteanalyser av Altinn (2010) og eID-programmet (2009) viser at det er mange milliarder å spare på å lage elektroniske tjenester med sikker identifisering. Direktoratet for forvaltning og IKT (Difi) har utviklet MinID, som er en eID på mellomhøyt sikkerhetsnivå, for pålogging til offentlige tjenester på nett. MinID har per 2012 over 2,8 millioner brukere. For at innbyggerne skal få tilgang til offentlige tjenester med personsensitivt innhold på nett er det en forutsetning med eID på høyt sikkerhetsnivå. Til slike tjenester kan innbyggerne bruke privat eID fra BankID, Buypass og Commfides. BankID har per 2012 rundt 2,8 millioner brukere, mens Buypass og Commfides samlet har om lag 400 000 brukere. Innbyggerne kan velge mellom disse ulike eID-ene gjennom Difis felles innloggingstjeneste ID-porten, som gjør at innbyggerne møter det samme innloggingsbilde på tjenester fra mer enn 270 offentlige virksomheter.

Tiltak: FAD vil følge utviklingen i markedet for eID-løsninger. Samtidig arbeider JD med å utstede et nasjonalt ID-kort med eID på høyt sikkerhetsnivå, som et offentlig alternativ til de private eID-løsningene på høyt sikkerhetsnivå. FAD vil følge opp at fellesløsningene kan benyttes mot alle relevante offentlige, elektroniske tjenester. For å sikre standardisering og mulighet for fellesløsninger vil FAD fortløpende vurdere hvorvidt gjeldende rammeverk og retningslinjer for bruk av elektronisk ID er i tråd med den tekniske utviklingen og de statlige behovene.

Ansvarlig departement: FAD og JD

Tiltak 3.6: Videreutvikling av håndteringen av kryptonøkler for gradert informasjon

Bakgrunn: For å beskytte mot uønsket tilgang til sikkerhetsgradert informasjon blir informasjonen kryptert. Det er viktig at krypteringen understøtter en sikker og effektiv informasjonsutveksling.

Tiltak: Systemet for elektronisk produksjon og distribusjon av kryptonøkler i sikkerhetsgraderte systemer skal videreutvikles.

Ansvarlig departement: FD

Sikre samfunnets evne til å oppdage, varsle og håndtere alvorlige IKT-hendelser

Tiltak 4.1: Styrke NorCERT

Bakgrunn: NorCERT ble etablert fast i 2006. Virksomheten fikk nye lokaler i 2012, men har vært på samme ressursmessige nivå siden etableringen, til tross for en jevn stigning i oppgavevolumet.

Tiltak: NorCERT skal videreutvikles som operativt nasjonalt koordineringspunkt for arbeidet med å oppdage, varsle om og håndtere alvorlige dataangrep. Styrkingen innebærer døgnkontinuerlig drift, forbedret deteksjonsevne i varslingssystemet for digital infrastruktur (VDI), økt nasjonal evne til effektivt å håndtere alvorlige IKT-hendelser, økt kapasitet til analyse av skadevare og strategisk analyse av IKT-risikobildet, samt tilrettelegging for intensivert koordinering av det nasjonale og internasjonale samarbeid innen informasjonssikkerhet. Særlig viktig vil være å få på plass gode koordineringsrutiner knyttet til Forsvarets bistand til det sivile samfunn, hvordan Post- og teletilsynets fullmakter etter ekomloven skal kunne benyttes, og generell utarbeidelse av et nasjonalt rammeverk for ledelse, styring og samarbeid med de sektorvise responsmiljøene. Det nordiske samarbeidet mellom nasjonale CERTer skal styrkes.

Ansvarlig departement: JD og FD

Tiltak 4.2: Etablering av sektorvise responsmiljøer

Bakgrunn: Hendelser i kritiske IKT-systemer som rammer en virksomhet kan ha betydning for andre virksomheter i sektoren, men også for andre sektorer. Virksomhetenes administrative og operative systemer er ofte bundet sammen gjennom internett. Det er viktig med rask og systematisk varsling ved alvorlige hendelser mellom berørte virksomheter og offentlige myndigheter, på tvers av sektorene. En viktig forutsetning for effektiv håndtering av IKT-hendelser er at det etableres sektorvise responsmiljøer, eller såkalte CSIRT'er (Computer Security Incident Response Team) som kan stå i kontakt med responsmiljøer i de enkelte virksomheter i sektoren, andre sektor-CSIRT'er og under nasjonal faglig koordinering og veiledning av NSM (NorCERT). NSMs rolle vil ikke gripe inn i sektordepartementenes konstitusjonelle ansvar. Det siste året har justissektoren og helsesektoren, energisektoren m.fl. arbeidet med dette. Fra før har universitets- og høgskolesektoren egne responsmiljøer. Forsvaret har sitt sentrale responsmiljø plassert i Cyberforsvaret.

Tiltak: I tiden fremover skal det arbeides for å systematisk etablere responsmiljøer i de ulike sektorene og utvikle prosedyrer, rutinebeskrivelser og planer for hvordan responsmiljøene skal samhandle med virksomhetene, hverandre, sektormyndigheter og NorCERT. Sektorene må selv

vurdere hva slags behov de har for å håndtere IKT-kriser og hvordan de mest effektivt kan etablere sine responsmiljøer. NSM/NorCERT vil være tilgjengelig for veiledning i prosessen. Norge vil med et slikt nett av sektor-CSIRT'er, under koordinering fra NorCERT, bli bedre i stand til å møte og takle nettbaserte trusler. Det må etableres en tydelig ansvarslinje til sektordepartementene fra CSIRT'ene.

Ansvarlig departement: JD og samtlige sektordepartementer

Tiltak 4.3: Sikkert kommunikasjonsnettverk mellom de nordiske nasjonale CERT-funksjoner

Bakgrunn: Etter oppdrag fra de nordiske utenriksministre overleverte tidligere utenriksminister Thorvald Stoltenberg i februar 2009 en rapport om fremtidig nordisk utenriks- og sikkerhetspolitisk samarbeid. Rapporten inneholdt flere konkrete forslag som berører samfunnssikkerhet og beredskap, og har bidratt til økt oppmerksomhet om nordisk samarbeid på dette området. Det er også avgitt en felles nordisk solidaritetserklæring.

Tiltak: Et første viktig tiltak for å styrke samarbeidet innen IKT-sikkerhet er å etablere et gradert kommunikasjonsnettverk mellom de nordiske nasjonale CERT-funksjonene. Formålet med et slikt gradert kommunikasjonsnettverk vil være å varsle, analysere og respondere på en sikker og effektiv måte på tvers av landene ved digitale angrep. Ambisjonen er at kommunikasjonsnettverket skal være på plass ved utløpet av 2012 og med et juridisk rammeverk som fundament. Landene vil da ha et viktig instrument for å kunne videreutvikle det praktiske nordiske samarbeidet om digital sikkerhet. Som et neste skritt sees det nærmere på hvilke utenriks- og sikkerhetspolitiske aspekter knyttet til digital sikkerhet som kan gi en merverdi gjennom nordisk samarbeid.

Ansvarlig departement: JD, FD og UD

Tiltak 4.4: Varsling av hendelser og utfall av ekominfrastruktur og -tjenester

Bakgrunn: Tilbyderne av elektronisk kommunikasjon driver i dag en kontinuerlig kontroll med drift av egne nett. Tilbyderne er pålagt å varsle Post- og teletilsynet ved større hendelser i nettene. Tilsynet vurderer hvor alvorlig hendelsene er og varsler videre til Samferdselsdepartementet.

Tiltak: PT skal i 2013 teste ut og evaluere en teknisk løsning for varsling av hendelser og utfall av ekominfrastruktur og -tjenester. Løsningen må legge til rette for at også NorCERT mottar relevante varsler.

Ansvarlig departement: SD

Sikre samfunnets evne til å forebygge, avdekke og etterforske datakriminalitet

Tiltak 5.1: Styrking av politiets arbeid med forebygging og bekjempelse av internettrelatert kriminalitet

Bakgrunn: For å møte de utfordringer internettrelatert kriminalitet innebærer, er det nødvendig med en rekke tiltak innen justissektoren. Generelt er innsatsen mot datakriminalitet på Kripos styrket gjennom at Stortinget i 2012 har bevilget 15 mill. kroner til forebygging og bekjempelse av internettrelatert kriminalitet. Det er nylig etablert et prosjekt på Kripos knyttet til internettrelatert etterforskingsstøtte.

Tiltak: Den påbegynte satsingen på internettrelatert kriminalitet i politiet skal videreføres. Det skal foretas en løpende vurdering av behovet for ytterligere styrking av politiet i planperioden.

Ansvarlig departement: JD

Tiltak 5.2: PSTs ansvar og rolle ved nettverksangrep

Bakgrunn: PST har gjennomført første del av et prosjekt som ser på eget ansvar og egen rolle ved nettverksangrep og er nå i ferd med å gjennomføre anbefalingene i prosjektrapporten. Hovedelementene i rapporten er knyttet til avklaring av et arbeidskonsept for PSTs arbeid med nettverksetterretning og gjennomføring av en gjennomgående styrking av PSTs evne til å håndtere nettverksetterretning mot Norge og norske interesser gjennom å øke bemanningen i alle ledd fra etterretningsinnsamling og ledelse, teknisk håndtering, strategisk analyse og etterforsking. Deltagelse i NorCERT på permanent basis gjennom en rotasjonsordning og en økning av kompetansen knyttet til nettverkstrusler og håndteringen av disse, samt en videre utredning av spørsmål knyttet til informasjonsinnhenting og forebyggende tiltak i det digitale rom er andre elementer i rapporten.

Tiltak: PST følger opp tiltakene i rapporten.

Ansvarlig departement: JD

Tiltak 5.3: Oppfølging av kartlegging vedrørende politiets håndtering av datakriminalitet

Bakgrunn: Det er i 2012 utført et kartleggingsarbeid i POD i samarbeid med Riksadvokaten vedrørende politiets håndtering av datakriminalitet, politioppgaver på nett og behandling av elektroniske spor. Kartleggingen har resultert i rapporten, "Politiet i det digitale samfunn". Den anbefaler en rekke forbedringspunkter.

Tiltak: Det skal vurderes tiltak på bakgrunn av rapporten.

Ansvarlig departement: JD

Tiltak 5.4: Forebygge og avdekke kriminalitet på internett – utredning av tipstjeneste

Bakgrunn: Publikum kan være en viktig ressurs for kunnskap om uønskede hendelser i samfunnet.

Tiltak: Det skal utredes om dagens ordning med Rød Knapp kan utvides til å omfatte all internettrelatert kriminalitet.

Ansvarlig departement: JD

Tiltak 5.5: Utrede mulighet for bedre sanntidsposisjonering av mobile kommunikasjonsenheter

Bakgrunn: Mer nøyaktig posisjonering av mobile kommunikasjonsenheter er nødvendig i situasjoner hvor det er viktig å gripe inn raskt. Politiet kan i dag få tilgang til posisjoneringsdata med hjemmel i straffeprosessloven § 216b. Det er behov for en lovendring som gir adgang til å spore mobile kommunikasjonsenheter på en mer nøyaktig måte, også på tidspunkter der kommunikasjonsenheten ikke aktivt benyttes til kommunikasjon.

Tiltak: Det skal foretas en utredning om bruk av sanntidsposisjonering for etterforsking av alvorlige straffesaker og i redningsoperasjoner der liv og helse er i fare. Utredningen skal også vurdere om tilbyderne skal pålegges en leveringsplikt av posisjoneringsdata og hvilke type data som skal utleveres. Både hensynet til kriminalitetsbekjempelse og personvern skal ivaretas.

Ansvarlig departement: JD

Tiltak 5.6: Effektiv lokal forebygging av datakriminalitet

Bakgrunn: Flere aktører må samarbeide for å bidra til forebygging av datakriminalitet i det enkelte lokalsamfunn. Etablerte samarbeidsstrukturer innenfor kriminalitets-forebygging, som politiråd og samordning av lokale kriminalitetsforebyggende tiltak (SLT), kan benyttes også til dette formålet.

Politiråd er et formalisert samarbeid mellom lokalt politi og kommunale myndigheter som har som mål å bidra til kriminalitetsforebygging og trygghet i lokalsamfunnet. SLT er spesielt rettet mot forebygging av kriminalitet blant barn og unge. Politiet har etablert et politirådssamarbeid med de fleste kommuner i Norge. Når det gjelder SLT har i underkant av halvparten av kommunene organisert det kriminalitetsforebyggende arbeidet overfor barn og unge i henhold til denne modellen.

Tiltak: Politiet bør bruke politiråd for å styrke kunnskapen om datakriminalitet i lokalsamfunnet, formidle råd om hvordan man lokalt kan beskytte seg selv mot denne formen for kriminalitet, samt for å initiere forebyggende tiltak som involverer flere aktører i lokalsamfunnet. Likeledes er SLT en aktuell samarbeidskanal når det gjelder forebygging som retter seg direkte mot barn og unge enten som gjerningspersoner eller som offer for denne typen av kriminalitet.

Ansvarlig departement: JD

Kontinuerlig innsats for bevisstgjøring og kompetanseheving

Tiltak 6.1: Videreføre nettvett.no

Bakgrunn: Post- og teletilsynets tjeneste nettvett.no er en av mange aktører som driver informasjonsarbeid rettet mot brukere av elektroniske kommunikasjonstjenester.

Tiltak: Dette arbeidet skal videreføres og tilsynet vil i 2013 gå i dialog med andre aktører for å sikre at aktørene samlet dekker behovet for bevisstgjøring og informasjon.

Ansvarlig departement: SD

Tiltak 6.2: Videreføre tilskuddet til NorSIS

Bakgrunn: I FADs arbeid med forebyggende IKT-sikkerhet er tilskudd til foreningen Norsk senter for informasjonssikring (NorSIS) et virkemiddel. NorSIS er en uavhengig forening for formidling av råd og veiledning vedrørende informasjonssikring. I følge foreningens vedtekter er NorSIS overordnede mål å bevisstgjøre om trusler, opplyse om tiltak og påvirke til gode holdninger innen informasjonssikkerhet. NorSIS er en viktig pådriver på informasjonssikkerhetsområdet. NorSIS drifter også Slettmeg.no, en rådgivningstjeneste for dem som føler seg krenket på nett.

Ansvaret for å følge opp tilskuddet til NorSIS overføres fra FAD til JD ifm. overføringen av ansvaret for forebyggende IKT-sikkerhet.

Tiltak: JD vil videreføre det årlige tilskuddet til NorSIS på 6,86 mill. kr i 2013.

Ansvarlig departement: JD

Tiltak 6.3: Støtte til personvern og informasjonssikkerhet i grunnopplæringen

Bakgrunn: Senter for IKT i utdanningen jobber med personvern og informasjonssikkerhet for å bistå skoler og skoleeiere i arbeidet med å ivareta de rettslige krav som stilles til behandling av opplysninger som kan knyttes til bestemte enkeltpersoner i skolen (ansatte, elever og foreldre/foresatte). Disse kravene skal ivareta personvernet til den enkelte ansatt, elev eller foreldre/foresatt når opplysninger om dem behandles ved bruk av elektroniske hjelpemidler eller når de inngår i manuelle personregistre.

Tiltak: Senter for IKT i utdanningen vil videreføre en rekke tiltak for personvern og informasjonssikkerhet, bl.a. Personvernskolen.no (i samarbeid med Senter for rettsinformatikk (SERI)) og Du bestemmer (i samarbeid med Datatilsynet, Teknologirådet og Medietilsynet). Senteret har også ansvaret for FEIDE i grunnopplæringen. Feide hjelper skoleeier og skoler med å ivareta personvernet til brukerne, og bidrar til at personopplysninger blir håndtert på en trygg og lovmessig måte.

Ansvarlig departement: KD

Høy kvalitet på nasjonal forskning og utvikling innenfor informasjons- og kommunikasjonssikkerhet

Tiltak 7.1; Systematisk utnytte resultatene av satsningen på sikkerhet, personvern og sårbarhet gjennom Forskningsrådets store IKT-program VERDIKT

Bakgrunn: VERDIKT har «sikkerhet, personvern og sårbarhet» som prioriterte fagområder gjennom hele programperioden (2005-2014). Dette har gitt en god portefølje av forskningsprosjekter av høy kvalitet ved forskjellige forskningsmiljøer. Disse har resultert i spennende forskningsresultater i form av kunnskap og kompetanse. I løpet av programperioden har VERDIKT også støttet et Ressursnettverk (NISNet) og nå et Verdinettverk (FRISC) innen fagområdet informasjonssikkerhet.

Tiltak: Det skal skapes møteplasser og arena for deling og utnyttelse av forskningsresultater fra VERDIKT og stimulere forskningsmiljøene til å utnytte sin kompetanse og konkurrere på EU sin forskningsarena (security for society)

Ansvarlig departement: Alle relevante fagdepartementer

Tiltak 7.2: Innspill til Forskningsrådets neste IKT-satsning

Bakgrunn: Norges Forskningsråd har startet prosessen med planleggingen av en ny IKT-satsning fra 2015. Første utkast for et dokument som beskriver grunnlaget for veien videre foreligger. I dette dokumentet trekkes samfunnssikkerhet frem som et viktig samfunnsområde der forskning på IKT- og informasjonssikkerhet kan bidra med nye løsninger. I tillegg defineres «Et trygt informasjonssamfunn» som et eget forskningstema som omfatter problemstillinger innen personvernproblematikk, sikring og utvikling av robust infrastruktur (systemer og nettverk), trygg og sikker dataoverføring etc. Forskningsinnsatsen innenfor informasjonssikkerhet må evne å kombinere høy kunnskap om teknologi med høy kunnskap om behov hos brukere, organisatoriske-/systemeffekter og virkning på samfunnet. Etiske og juridiske problemstillinger er sentralt.

Tiltak: Det tas initiativ til en kartlegging og konkretisering av forskningsbehov innen IKT-sikkerhet med utgangspunkt i de ulike sektorenes ansvarsområder.

Ansvarlig departement: JD med innspill fra sektordepartementer

Tiltak 7.3: Støtte til SIMULA

Bakgrunn: Målet med statens eierskap i Simula Research Laboratory AS er å bidra til grunnleggende langsiktig forskning på utvalgte områder innen programvare- og kommunikasjonsteknologi. Dette bidrar til å sikre et høyt internasjonalt nivå på forskningen i Norge, samtidig som det utdannes høyt kvalifiserte forskere. Etter beslutning fra Kunnskapsdepartementet har det i regi av Norges forskningsråd vært gjennomført evaluering av Simula. Evalueringen, som ble lagt frem i 2010, bekrefter at selskapet leverer meget gode vitenskapelige resultater og har utviklet seg til en inspirerende nyskapning i det norske forskningssystemet. Simula hevder seg også svært godt internasjonalt. Både KD, NHD og SD er inne med midler til grunnbevilgning til SIMULA på totalt 50 mill. kroner. SD gir også tilskudd til forskningsprosjektet *Robuste nett*. Dette prosjektet arbeider med arkitekturer og mekanismer som gjør nettverk og brukere av nettverk bedre rustet til å møte avvik fra normal drift. Resultatene blir brukt til å finne avhengigheter og foreslå tiltak for å øke robustheten i de offentlige ekomnettene.

Tiltak: Støtten til prosjektet Robuste nett via VERDIKT-programmet skal søkes videreført ut prosjektperioden.

Ansvarlig departement: SD

Tiltak 7.4: Etablering av programmet *Samfunnssikkerhet* i regi av Forskningsrådet

Bakgrunn: Samfunnets evne til å opprettholde viktige samfunnsfunksjoner og ivareta borgernes liv, helse og grunnleggende behov under ulike former for store påkjenninger omfatter også tiltak og kunnskap om kontinuitet i IKT-systemer. Økt kunnskap og kompetanse på området vil kunne bidra til bedre beredskap og mer robuste systemer.

Tiltak: Det nye programmet Samfunnssikkerhet skal bidra til ny kunnskap og forståelse om farer og trusler mot samfunnets evne til å opprettholde viktige samfunnsfunksjoner og ivareta borgernes liv, helse og grunnleggende behov under ulike former for store påkjenninger og bidra til bedre motstandskraft, forebygging, beredskap, redningsarbeid, krisehåndtering og læring. Programmet viderefører det avsluttede programmet Samfunnssikkerhet og risiko (SAMRISK) skal bidra til å utvikle tverrfaglig kapasitet og kompetanse både innenfor samfunnsvitenskapene, inkludert jus, og mellom disse og humanistiske fag, teknologi og naturvitenskap. Forskningen skal rekke over flere sektorer i samfunnet. IKT-sikkerhet vil være et relevant tema inn i forskningsprogrammet.

Ansvarlig departement: JD, FD og SD

Tiltak 7.5: FoU i regi av Nasjonal sikkerhetsmyndighet

Bakgrunn: NSM har i mange år initiert og selv drevet FoU knyttet til spesielle områder av informasjonssikkerhetsfeltet. Forskning har til nå i for stor grad vært reaktiv, og forutsatt at brukere har presentert sine behov.

Tiltak: Det vil bli utviklet en langsiktig plan for NSMs forsknings- og utviklingsaktiviteter, hvor NSM vil endre innretning fra å respondere reaktivt på behov fremmet av brukerne til selv å ta initiativ til FoU-aktiviteter.

Ansvarlig departement: FD og JD