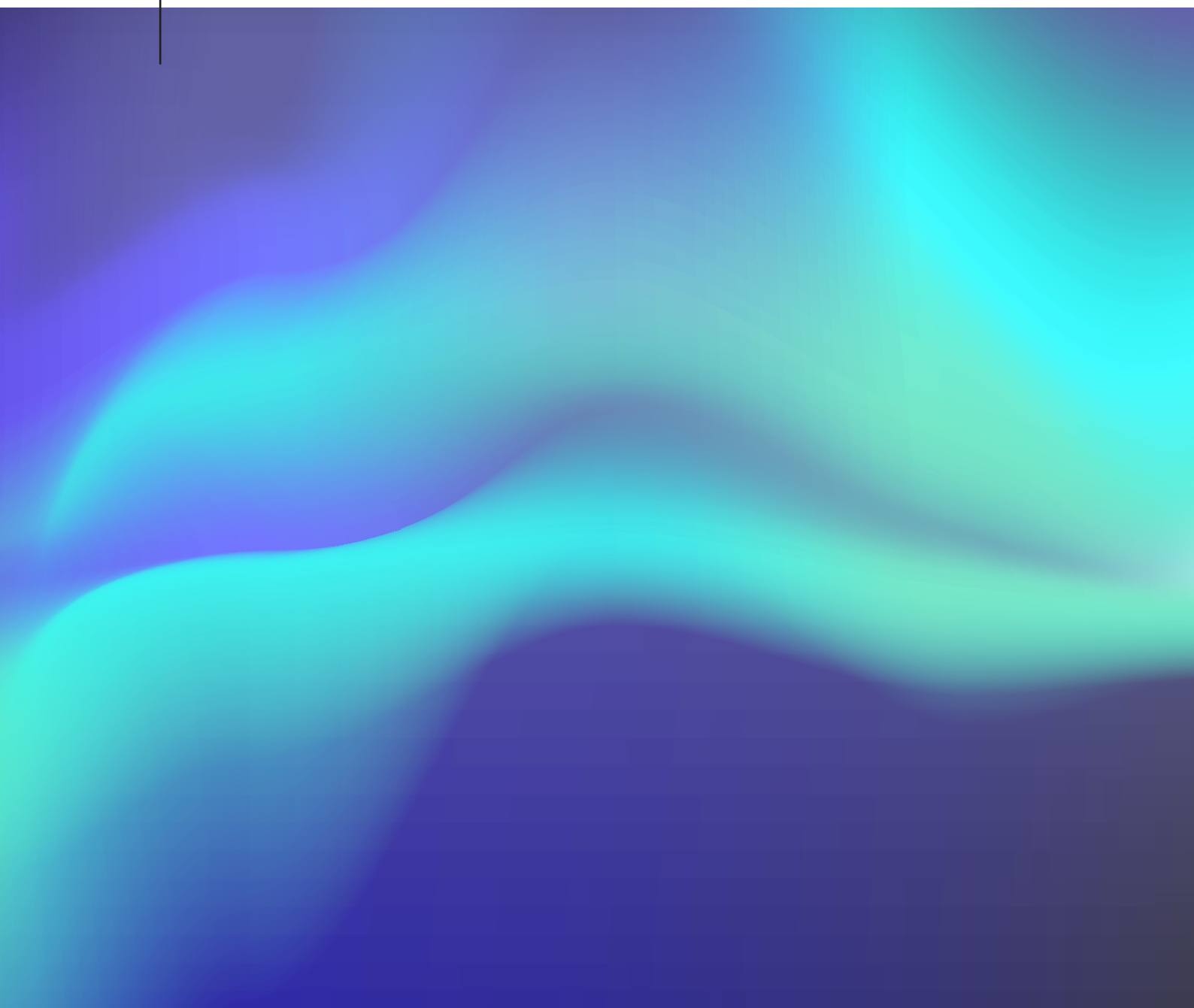
Tiltaksoversikt til nasjonal strategi for digital sikkerhet



Innhold

1. Innledning 7

1.1. Rapportering og oppfølging av tiltaksoversikten 7

2. DEL 1 – Sentrale tiltak for økt digital sikkerhet 8

2.1. Utvalgte tiltak som støtter flere av de strategiske prioriteringene 8

Tiltak 1: Nasjonale tekniske sikkerhetstiltak – en større nasjonal sikkerhetspakke 8

Tiltak 1.1: Ny sensor for varslingssystem for digital infrastruktur (VDI) 8

Tiltak 1.2: Neste generasjons deteksjonskapasitet 8

Tiltak 1.3: Allvis NOR, kartlegging og sårbarhetsundersøkelse 9

Tiltak 1.4: DNS servertjeneste til offentlig sektor 9

Tiltak 1.5: Sikker e-posttjeneste for departementene 9

Tiltak 2: Nasjonal strategi for digital sikkerhetskompetanse 9

Tiltak 3: Nasjonalt cybersikkerhetssenter 10

Tiltak 4: NC3 (Politiets nasjonale cyberkrimsenter) 10

Tiltak 5: Sikker digitalisering i offentlig sektor 10

2.2. Forebyggende digital sikkerhet 11

Tiltak 6: IKT-sikkerhetsutvalget 11

Tiltak 7: Oppfølging av IKT-sikkerhetsmeldingen og Digitalt sårbarhetsutvalg 12

Tiltak 8: Nasjonale anbefalinger og rådgiving 12

Tiltak 8.1: Nasjonale anbefalinger og rådgivningsaktiviteter i regi av NSM 12

Tiltak 8.2: Grunnprinsipper for IKT-sikkerhet 12

Tiltak 8.3: Nasjonalt IKT-risikobilde 12

Tiltak 8.4: Forsknings- og utviklingsaktiviteter i regi av NSM 13

Tiltak 8.5: Difis kompetansemiljø og veiledningsmateriell – sikkerhet i IKT-anskaffelser 13

Tiltak 8.6: NorSIS (Norsk senter for informasjonssikring) 13

Tiltak 8.7: Nettvett.no 13

Tiltak 8.8: Slettmeg.no 14

Tiltak 9: Offentlig-privat samarbeidsforum 14

Tiltak 10: Interdepartementalt fagnettverk 14

Tiltak 11: Samhandlingsarena for sentrale tilsynsmyndigheter 14

Tiltak 12: Kvalitetsordning for leverandører 15

Tiltak 13: Inntrengingstester 15

Tiltak 14: ENISA 16

Tiltak 15: Informasjonsdeling og operativt situasjonsbilde for digital hendelseshåndtering 16

Tiltak 16: Standardisering 16

Tiltak 17: Standard Norge 17

Tiltak 18: Statens standardavtaler (SSA) 17

Tiltak 19: Gradert datakommunikasjon mellom departementene, underliggende etater og andre sentrale beredskapsaktører i sektorene 17

Tiltak 20: Sikret offentlig nett (SON) 17

Tiltak 21: Nasjonal sikkerhetsmåned 18

Tiltak 22: Nasjonal kryptopolitikk 18

Tiltak 23: NATO Cooperative Cyber Defence Centre of Excellence 19

Tiltak 24: European Centre of Excellence for Countering Hybrid Threats 19

Tiltak 25: Kapasitetsbygging internasjonalt 19

Tiltak 26: Kapasitetsbyggingstiltak på digital sikkerhet i utviklingsland 20

Tiltak 27: Norwegian Cyber Range (NCR) 20

Tiltak 28: Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner for forsvarssektoren 20

2.3. Digital sikkerhet i kritiske samfunnsfunksjoner 21

Tiltak 29: Ny sikkerhetslov 21

Tiltak 30: NIS-direktivet 21

Tiltak 31: Nasjonal kjerneinfrastruktur 22

Tiltak 32: Fiberføringer til utlandet 22

Tiltak 33: Økt sikkerhet i ekomnett 22

Tiltak 34: Forslag til ny lov om Etterretningstjenesten og tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon 23

Tiltak 35: Nasjonalt rammeverk for helhetsvurdering av verdikjeder 23

Tiltak 36: NATO Cyber Defence Pledge 24

Tiltak 37: Neste generasjon nødnett 24

2.4. Kompetanse – oversikt over tiltak i nasjonal strategi for digital sikkerhetskompetanse 24

2.5. Avdekke og håndtere digitale angrep 26

Tiltak 38: Sektorvise responsmiljøer 26

Tiltak 39: JustisCERT 27

Tiltak 40: Rammeverk for håndtering av IKT-sikkerhetshendelser 27

Tiltak 41: IKT-sikkerhetsøvelse 27

Tiltak 42: Internasjonale øvelser 28

Tiltak 43: Felles cyberkoordineringssenter (FCKS) 28

Tiltak 44: Tverrsektoriell cyberreserve 29

Tiltak 45: Åpenhet og evaluering av uønskede digitale hendelser 29

2.6. Bekjempe data- og IKT-relatert kriminalitet 29

Tiltak 46: Stortingsmelding om politiets kapasitet og kompetanse 29

Tiltak 47: Politiets sikkerhetstjeneste (PST) 30

Tiltak 48: Støtte FNs innsats for å bekjempe data- og IKT-relatert kriminalitet globalt 30

Tiltak 49: Nasjonalt elektronisk identitetsbevis (eID) 30

Tiltak 50: Internasjonalt samarbeid om data- og IKT-relatert kriminalitet 31

Tiltak 51: Politiets nasjonale innbyggerundersøkelse 31

3. DEL 2 – Anbefalte tiltak for å øke virksomheters egenevne 32

1. Innledning

Nasjonal strategi for digital sikkerhet ble lansert av regjeringen januar 2019. I strategien utpekes det mål for fem prioriterte områder. Strategien understøttes av denne todelte tiltaksoversikten, hvor del 1 beskriver utvalgte sentrale tiltak som støtter opp under strategien, og del 2 lister ti grunnleggende tiltak som virksomheter i offentlig og privat sektor anbefales å gjennomføre. Tiltakene i del 2 skal legge til rette for å øke virksomheters egenevne til å beskytte seg mot og håndtere digitale hendelser.

1.1. Rapportering og oppfølging av tiltaksoversikten

Justis- og beredskapsdepartementet (JD) og Forsvarsdepartementet (FD) har det overordnede ansvaret for å følge opp strategien. Det enkelte departement er ansvarlig for at strategiens prioriteringer og tiltaksoversikten blir fulgt opp innenfor sin sektor. Departementene må i denne forbindelse samarbeide tett med underlagte virksomheter og berørte aktører i sektorene slik at planlagte sikkerhetstiltak i nødvendig grad blir koordinert med andre departementer.

Hvert departement skal aktivt involvere berørte parter i privat sektor i utarbeidelsen av tiltak. Departementene skal sørge for å kartlegge hvorvidt de iverksatte tiltakene i egen sektor bidrar til at målformuleringene under de strategiske prioriteringene nås.

I forbindelse med departementenes oppfølging forutsettes det at betydningen av god digital sikkerhet blir formidlet til underlagte etater. Dette kan med fordel inngå som del av etatsstyringen.

Tiltaksoversikten utgis separat, og skal revideres ved behov. Tiltak som berører næringslivet forutsettes gjennomført i nært samarbeid med næringslivets egne organer. Tiltak som berører forbrukerne bør gjennomføres i samarbeid med forbrukerorganisasjonene. Før innføring av nye tiltak bør det alltid foretas en vurdering av hvordan tiltaket berører personvernet, og om nødvendig må personvernmyndighetene involveres ved planlegging og gjennomføring.

For å kartlegge status i oppfølgingen av strategiens prioriteringer, vil JD og FD følge utviklingen på sikkerhetsområdet gjennom å innhente status fra departementenes oppfølging av strategien. Det vil bli innhentet status på departementenes arbeid ca. to år etter lansering av strategien.

Oppfølgingen av strategien vil også foregå gjennom en interdepartemental gruppe, og gjennom et offentlig-privat samarbeidsforum. Disse gruppene skal blant annet følge utviklingen når det gjelder sikkerhetsutfordringer og trender, og fortløpende vurdere om dette utløser et behov for å revidere hele eller deler av innholdet i den nasjonale strategien og tilsvarende i tiltaksoversikten.

2. DEL 1 – Sentrale tiltak for økt digital sikkerhet

2.1. Utvalgte tiltak som støtter flere av de strategiske prioriteringene

Tiltak 1: Nasjonale tekniske sikkerhetstiltak – en større nasjonal sikkerhetspakke

Digitale angrep blir stadig mer sofistikerte. Nye angrepsteknikker, økt brukt av kryptering og komplekse angrepsinfrastrukturer, gjør at vi må tenke nytt for å opprettholde nasjonal deteksjonsevne. Bruk av kunstig intelligens, maskinlæring og stor grad av automatiserte prosesser blir kritiske faktorer som må nyttiggjøres. Prosjektet «P2950» skal gå over flere år og har en betydelig kostnadsramme. Som del av prosjektet skal det utvikles ny sensorteknologi til bruk i blant annet Varslingssystem for digital infrastruktur (VDI). Prosjektet etablerer økt teknisk kapasitet for å ta i bruk kunstig intelligens og maskinlæring. Prosjektet skal også ta frem graderte og ugraderte automatiske delingsplattformer, mobile kapasiteter, samt dynamisk datainnsamling og dataanalyse som vil kunne videreutvikles og skaleres i tråd med fremtidige behov.

Tiltak 1.1: Ny sensor for varslingssystem for digital infrastruktur (VDI)
Dagens VDI-løsning har gjennom snart 20 år stadfestet vår evne til å oppdage målrettede digitale angrep uten at det har gått på bekostning av personvernet. En større spredning av VDI-sensorer hos eiere av samfunnskritisk infrastruktur og samfunnsviktige funksjoner vil øke den nasjonale deteksjonsevnen betydelig. Det skal utvikles ny sensorteknologi som skal bygge videre på og erstatte dagens VDI-sensor. Neste generasjons VDI-sensor skal ha mulighet til å støtte graderte signaturer og indikatorer.

Ansvarlig virksomhet: FD og Nasjonal sikkerhetsmyndighet (NSM)
Gjennomføres: 2018-2021

Tiltak 1.2: Neste generasjons deteksjonskapasitet
Det skal utvikles ny nasjonal deteksjonskapasitet som skal ta i bruk kunstig intelligens og maskinlæring på innsamlet data. Plattformen som skal utvikles skal gi muligheter for automatisk skadevareanalyse og automatisk deling av resultater.

Ansvarlig virksomhet: FD og NSM
Gjennomføres: 2018-2021

Tiltak 1.3: Allvis NOR, kartlegging og sårbarhetsundersøkelse
«Allvis NOR» er en tjeneste NSM tilbyr for å øke sikkerheten i offentlige virksomheter og eiere av kritisk infrastruktur. Tjenesten består i hovedsak av regelmessig kartlegging og sårbarhetsundersøkelse av utvalgte IP-adresser som er tilgjengelige på internett. Informasjon om sårbare tjenester blir delt med systemeier. Tjenesten skal videreutvikles og oppskaleres slik at den kan avdekke flere sårbarheter i flere virksomheter enn den gjør i dag.

Ansvarlig virksomhet: NSM
Gjennomføres: 2018-2021

Tiltak 1.4: DNS servertjeneste til offentlig sektor
NSM tilbyr i dag en DNS-tjeneste til utvalgte virksomheter. Gjennom bruk av tjenesten kan man stoppe trafikk mot uønskede nettsider. DNS-tjenesten skal videreutvikles og oppskaleres til å tilbys til offentlig sektor.

Ansvarlig virksomhet: NSM
Gjennomføres: 2018-2021

Tiltak 1.5: Sikker e-posttjeneste for departementene
E-post er den foretrukne digitale kommunikasjonskanalen for norske offentlige og private virksomheter, selv om ny teknologi muliggjør andre metoder for å kommunisere elektronisk. Det store flertallet av uønskede hendelser rettet mot nasjonal kritisk digital infrastruktur starter med en forfalsket e-post. Det eksisterer i dag en rekke forbedringer til e-post-standarden. Flere av disse forbedringene har til hensikt å begrense mulighets-rommet for å motta forfalsket e-post. Det skal etableres et felles mottak og en analysetjeneste av uønskede e-poster for departementene.

Ansvarlig virksomhet: FD
Gjennomføres: 2019

Tiltak 2: Nasjonal strategi for digital sikkerhetskompetanse

Nasjonal strategi for digital sikkerhetskompetanse (2019) skal påvirke retning, innhold, samt synliggjøre ansvar for tiltak innenfor utdanning og forskning. I tillegg omhandler strategien bevisstgjørende tiltak rettet mot befolkningen, kommuner og virksomheter. Strategien er et ledd i en pågående prosess med å utvikle tiltak for økt sikkerhetskompetanse i samarbeid med målgruppene, som er myndigheter, offentlig og private virksomheter, utdanningssektoren og forskningsinstitusjoner.

Langtidsplan for forskning og høyere utdanning vil legge føringer for forsterket forskningsinnsats innenfor digital sikkerhet. Det legges til rette for styrket samarbeid for mer vekt på digital sikkerhet som del av ingeniør- og teknologiutdanninger.

Det rettes i strategien et spesielt søkelys mot kunnskapsgrunnlaget for tilstrekkelig digital sikkerhetskompetanse. JD vil sørge for oppdatert statistikk og analyser for å følge med på kompetansegapet innenfor digital sikkerhet. Videre skal det legges til rette for

et forbedret kunnskapsgrunnlag om sikkerhetskultur for befolkningen og virksomheter. Prioriteringer innenfor kompetanseområdet er på over 800 mill. kroner. I tillegg kommer studieplassene på IKT som har blitt tildelt de siste tre årene, hvor det har vært til dels sterke føringer på digital sikkerhet. Budsjettmessige satsinger som følger av den reviderte Langtidsplan for forskning og høyere utdanning inngår heller ikke i beløpet.

Ansvarlig virksomhet: JD og Kunnskapsdepartementet (KD)
Gjennomføres: 2019

Tiltak 3: Nasjonalt cybersikkerhetssenter

NSM skal etablere Nasjonalt cybersikkerhetssenter. Senteret vil bygge på allerede besluttede og etablerte tiltak og bygger på en lignende struktur som andre toneangivende land med tilsvarende sentre. Senteret representerer en styrking av det arbeidet NSM allerede utfører. Senteret skal styrke samarbeidet mellom de ulike IKT-sikkerhetsmiljøene slik at ulike aktører opererer i et felles risikobilde og med samme situasjonsforståelse. Etableringen er et viktig steg i videreutviklingen av det privat-offentlige samarbeidet innenfor IKT-sikkerhetsområdet. For å sikre tydelig ansvars- og rollefordeling er det viktig med et godt samarbeid mellom det nasjonale cybersikkerhetssenteret og politiets NC3-senter (se tiltak 4) for best mulig utnyttelse av samfunnets ressurser på området. IKT-sikkerhetsutvalgets anbefalinger (se tiltak 6) vil kunne ha betydning for den videre utviklingen av senteret.

Ansvarlig virksomhet: FD, JD og NSM
Gjennomføres: Oppstart 2018

Tiltak 4: NC3 (Politiets nasjonale cyberkrimsenter)

Politidirektoratet (POD) startet i 2018 etableringen av et nasjonalt cyberkrimsenter (NC3) ved KRIPOS. Flere land har allerede etablert et slikt senter. NC3 skal være et ekspertorgan som skal gjøre politiet bedre rustet til å håndtere data- og IKT-relatert kriminalitet.

JD vil påse at POD har en helhetlig tilnærming der kompetansen og kapasiteten ved NC3 inngår i PODs samlede styring og oversikt over politiets kompetanse og kapasitet.

Ansvarlig virksomhet: POD og JD
Gjennomføres: Oppstart 2018

Tiltak 5: Sikker digitalisering i offentlig sektor

Direktoratet for forvaltning og IKT (Difi) evaluerte i 2018 arbeidet med informasjonssikkerhet i statlige virksomheter. Evalueringen viser behovet for fortsatt styrking av arbeidet med styring og kontroll med informasjonssikkerhet i virksomhetene. Videre kommer det fram at alle departementer i sin etatsstyring bør bli bedre på oppfølging av sikkerhetsarbeidet i underliggende virksomheter.

- Difis arbeid med styring og kontroll på informasjonssikkerhet skal utvides til å omfatte både statsforvaltningen og kommunene fordi utfordringene i statsforvaltningen gjelder også for kommunene.
- Virksomhetene i offentlig sektor skal få et mer samordnet og helhetlig tilbud om veiledning om digital sikkerhet.
- Difi skal videreutvikle sin rolle innen veiledning og anbefalinger på området.
- Etatsstyringen av digital sikkerhet skal være tilpasset vesentlighet og risiko. Difi skal i samarbeid med Direktoratet for økonomistyring (DFØ) tilby veiledning til etatsstyrere for å kunne følge opp området digital sikkerhet på en god måte.
- Difis arbeid på området skal også avstemmes med berørte myndigheter med spesiell vekt på NSM og Datatilsynet.
- Direktoratet for samfunnssikkerhet og beredskap (DSB) skal tilrettelegge for og gjennomføre kurs i planlegging og gjennomføring av øvelser for offentlige virksomheter. Difi bidrar til arbeidet med å utvikle øvelser innenfor digital sikkerhet.
- Anbefalingene fra evalueringen i 2018 skal følges opp i et samarbeid mellom Difi, DFØ, DSB, NorSIS og NSM.

Ansvarlig virksomhet: Kommunal- og moderniseringsdepartementet (KMD) og Difi
Gjennomføres: 2019-2024

2.2. Forebyggende digital sikkerhet

Under følger sentrale tiltak som skal understøtte målet om at norske virksomheter skal digitalisere på en sikker og tillitsvekkende måte, og ha bedre evne til egenbeskyttelse mot uønskede digitale hendelser.

Tiltak 6: IKT-sikkerhetsutvalget

IKT-sikkerhetsutvalget ble oppnevnt i statsråd 15. september 2017. Utvalget skulle vurdere om dagens regulering av IKT-sikkerhet er hensiktsmessig, og om det er hensiktsmessig fordeling og organisering av tverrsektorielt ansvar på etatsnivå innenfor nasjonal IKT-sikkerhet. Utvalget hadde også mandat til å foreslå konkrete rettslige og organisatoriske endringer. Utvalget leverte sin utredning til JD 3. desember 2018. Utvalgets NOU ble sendt på høring i desember 2018 og JD vil deretter vurdere videre oppfølging.

Ansvarlig virksomhet: JD
Gjennomføres: 2019

Tiltak 7: Oppfølging av IKT-sikkerhetsmeldingen og Digitalt sårbarhetsutvalg

Digitalt sårbarhetsutvalg (Lysneutvalget) la frem flere anbefalinger for å redusere digitale sårbarheter i samfunnet. Meld. St. 38 (2016–2017) «IKT-sikkerhet - et felles ansvar» (IKT-sikkerhetsmeldingen) gir en oversikt over status på oppfølgingen av utvalgets anbefalinger. JD vil benytte oversikten til å følge opp departementene i det videre arbeidet med digital sikkerhet. Det vil bli innhentet ny status på oppfølgingen i 2019.

Ansvarlig virksomhet: JD
Gjennomføres: 2019

Tiltak 8: Nasjonale anbefalinger og rådgiving

Tiltak 8.1: Nasjonale anbefalinger og rådgivningsaktiviteter i regi av NSM
NSM skal videreutvikle nasjonale anbefalinger og gjøre disse tilgjengelig gjennom nettsider, kurs og annen rådgivingsaktivitet. Anbefalingene skal tas frem basert på erfaringer fra operative avdelinger, reelle hendelser, gjeldende trusselbilde, forskning og utvikling innenfor teknologi og endrede bruksområder, samt erfaringsutveksling med nasjonale og internasjonale, offentlige og private aktører.

Ansvarlig virksomhet: NSM
Gjennomføres: Løpende

Tiltak 8.2: Grunnprinsipper for IKT-sikkerhet
NSMs «Grunnprinsipper for IKT-sikkerhet» definerer et sett med prinsipper og underliggende tiltak for å beskytte informasjonssystemer (maskinvare, programvare og tilknyttet infrastruktur), data og tjenestene de tilbyr mot uautorisert tilgang, skade eller misbruk. Produktet skal være levende og tidsaktuelt, og vil oppdateres jevnlig basert på innspill fra brukere og fagmiljøer fra offentlig og privat sektor.

Ansvarlig virksomhet: NSM
Gjennomføres: Løpende

Tiltak 8.3: Nasjonalt IKT-risikobilde
Rapporten «Helhetlig IKT-risikobilde» som årlig utgis av NSM, skal bidra til å skape et felles situasjonsbilde som gjør virksomheter og myndigheter i stand til å treffe riktige tiltak. I tillegg skal rapporten være et verktøy for virksomhetene i deres risikovurderingsarbeid. Produktet skal evalueres og videreutvikles.

Ansvarlig virksomhet: NSM
Gjennomføres: Årlig

Tiltak 8.4: Forsknings- og utviklingsaktiviteter i regi av NSM
Den raske utviklingen innenfor teknologi, endrede bruksmønster og endret risikobilde, gir økt risiko for uønskede digitale hendelser og medfører økt behov for forskning og utvikling for å ta frem effektive forebyggende sikkerhetstiltak. Digital sikkerhet er ett av de prioriterte områdene i NSMs FoU-aktivitet. NSM skal drive forskning og bidra til utvikling av forebyggende tiltak, herunder i kryptografi og sikkerhet i virtuelle systemer.

Ansvarlig virksomhet: NSM
Gjennomføres: Løpende

Tiltak 8.5: Difis kompetansemiljø og veiledningsmateriell – sikkerhet i IKT-anskaffelser
Difi skal videreutvikle sitt kompetansemiljø og sine veiledningsressurser knyttet til vurdering av IKT-sikkerhet ved ugraderte offentlige IKT-anskaffelser. Veiledning knyttet til anskaffelse av skytjenester og tjenesteutsetting av IKT skal prioriteres spesielt. Dette inkluderer vurderinger knyttet til sikkerhet og risiko. NSM og Difi skal samarbeide for å sikre en helhetlig tilnærming til veiledning på IKT-sikkerhetsområdet, herunder om anskaffelser og tjenesteutsetting av IKT.

Ansvarlig virksomhet: Difi
Gjennomføres: Løpende

Tiltak 8.6: NorSIS (Norsk senter for informasjonssikring)
NorSIS mottar årlig driftstilskudd fra JD, og er del av regjeringens satsing på digital sikkerhet innenfor samfunnssikkerhetsfeltet. NorSIS bidrar til de overordnede målene for samfunnssikkerhetsarbeidet, gjennom å øke virksomheters og privatpersoners forståelse for, kunnskap om og aktivitet for styrket digital sikkerhet. Målet for tilskuddet til NorSIS er å gjøre samfunnet mer robust mot uønskede digitale hendelser. Tilskuddet skal benyttes for å nå målgruppen norske virksomheter i privat og offentlig sektor, herunder kommunesektoren. Små og mellomstore virksomheter skal prioriteres. NorSIS skal også bidra med råd og veiledning til befolkningen.

Ansvarlig virksomhet: JD og NorSIS
Gjennomføres: Løpende

Tiltak 8.7: Nettvett.no
Tjenesten nettvett.no ble lansert i 2005 og har som formål å bidra til å bygge sikkerhetskultur hos både forbrukere, viktige samfunnsaktører og i virksomheter, ved å være en portal med informasjon til forbrukere og små og mellomstore bedrifter om sikker bruk av internett. Siden 2017 er det etablert et samarbeid om tjenesten mellom flere sentrale aktører: NorSIS har redaktøransvaret og driver siden på vegne av NSM og Nasjonal kommunikasjonsmyndighet (Nkom), og skal bidra til en mer koordinert og bedret informasjonsflyt til målgruppen.

Ansvarlig virksomhet: NorSIS, med støtte fra NSM og Nkom
Gjennomføres: Løpende

Tiltak 8.8: Slettmeg.no
Slettmeg.no er en råd- og veiledningstjeneste for de som føler seg krenket på nett. Tjenesten drives av NorSIS. For å sikre veiledning til befolkningen om risiko knyttet til aktivitet og atferd på nett, skal tjenesten Slettmeg.no videreutvikles.

Ansvarlig virksomhet: NorSIS
Gjennomføres: Løpende

Tiltak 9: Offentlig-privat samarbeidsforum

Regjeringen etablerte et samarbeidsforum i 2018 («Forum for nasjonal IKT-sikkerhet») som består av representanter fra myndigheter, næringslivet, interesse- og bransjeorganisasjoner og akademia. Partene representerer virksomheter som enten eier eller forvalter kritisk digital infrastruktur eller kritiske samfunnsfunksjoner, eller som har sentrale roller innenfor forskning og utdanning.

Forumet skal sikre at strategiske spørsmål knyttet til digitale sikkerhetsutfordringer og internasjonalt samarbeid blir diskutert mellom private aktører og myndighetene. Forumet skal bidra til åpenhet, tillit og samhandling mellom offentlige og private aktører når det gjelder å dele informasjon og diskutere problemstillinger relatert til digital sikkerhet. Forumet etablerer en ny samarbeidsrelasjon mellom myndighetene på departementsnivå og utvalgte virksomheter og skal evalueres etter en oppstartsperiode for å sikre en best mulig fungerende arena.

Ansvarlig virksomhet: JD
Gjennomføres: 3-4 ganger årlig, evalueres innen 2020

Tiltak 10: Interdepartementalt fagnettverk

«Nettverk for nasjonal IKT-sikkerhet» skal sikre at strategiske spørsmål knyttet til digitale sikkerhetsutfordringer og internasjonalt samarbeid relatert til dette, blir diskutert og koordinert mellom departementene. For 2018 har fagnettverket blitt videreutviklet for å styrke offentlig-privat, sivil-militært og internasjonalt samarbeid knyttet til digital sikkerhet. Nettverket skal evalueres innen 2020 for å sikre en best mulig fungerende arena.

Ansvarlig virksomhet: JD
Gjennomføres: Møtes 3-4 ganger årlig, evalueres innen 2020

Tiltak 11: Samhandlingsarena for sentrale tilsynsmyndigheter

NSM har fått i oppdrag å utrede, etablere og lede en felles samhandlingsarena for de ulike sektorenes mest sentrale tilsynsmyndigheter. Hensikten er å sikre informasjonsutveksling og kompetanseoverføring, og på den måten øke kvaliteten på sektorenes tilsyn med digital sikkerhet.

NSM inviterte i 2017 DSB og Nkom til et samarbeid om å utrede og etablere samhandlingsarenaen. Utredningen ble levert 2017 og første møte i

samhandlingsarenaen ble gjennomført i mars 2018. Her var DSB, Nkom, Petroleumstilsynet, Finanstilsynet og NVE invitert. Det er stor interesse for arenaen, og mange tilsyn ønsker å delta. Samhandlingsarenaen skal fremover utvides med flere tilsyn, og det arbeides videre med følgende hovedpunkt som grunnlag for samarbeid:

- Erfaringsutveksling mellom tilsynsmyndighetene både før og etter ny sikkerhetslov som trådte i kraft fra 1. januar 2019
- Enhetlige tilsyn med mest mulig felles tilsynsmetodikk
- Kunnskapsoverføring og kompetanseheving
- Samarbeidsavtaler mellom NSM og sektortilsynene

Ansvarlig virksomhet: NSM
Gjennomføres: Løpende

Tiltak 12: Kvalitetsordning for leverandører

I 2017 lanserte NSM en kvalitetsordning for leverandører som tilbyr tjenester for håndtering av digitale angrep. Formålet med ordningen er å gjøre det mulig for virksomheter å velge leverandører som etter NSMs vurdering har tilfredsstillende tjenestekvalitet, samt bidra til å øke den generelle sikkerhetskompetansen i Norge. Ordningen er en pilot og har blitt evaluert i løpet av 2018. Foreløpige erfaringer av ordningen er positive. En utvidelse av ordningen til andre typer tjenester skal vurderes basert på evalueringen. Tjenester som vil bli vurdert som del av ordningen er blant annet sårbarhetstesting og rådgiving.

Ansvarlig virksomhet: NSM
Gjennomføres: 2019

Tiltak 13: Inntrengingstester

Inntrengingstesting er et svært effektivt virkemiddel for å avdekke sårbarheter og legge til rette for risikoreduserende tiltak. Inntrengingstesting som verktøy blir stadig viktigere for å sikre at den digitale kritiske infrastrukturen er tilstrekkelig trygg og robust. I ny sikkerhetslov åpnes det for en økning i bruken av private tilbydere til blant annet inntrengingstester i skjermingsverdige IKT-systemer. Det kan også være aktuelt å stille krav om slike tester før system som krever godkjenning, får dette. Dersom det private markedet skal kunne tilby slike tjenester også for kritiske og/eller graderte IKT-system, legges det opp til å etablere en godkjenningsordning av tilbydere. For 2019 er NSMs kapasitet til inntrengingstesting styrket med 10 mill. kroner for å øke sikkerheten og gjøre samfunnskritisk digital infrastruktur mer robust.

Ansvarlig virksomhet: NSM
Gjennomføres: 2019

Tiltak 14: ENISA

EUs byrå for nettverks- og informasjonssikkerhet (ENISA) er et kompetansesenter for cybersikkerhet. ENISA utvikler anbefalinger, bidrar til utvikling av regelverk og retningslinjer, og samarbeider med operative enheter i Europa. Norge deltar i ENISA gjennom EØS-samarbeidet.

Gjennomføringen av NIS-direktivet (se tiltak 30) vil styrke ENISA ved at byrået får tildelt rollen som faglig knutepunkt for det nettverket av nasjonale fagmyndigheter som NIS-direktivet etablerer. Det er også lagt frem forslag til forordning (jf. KOM/2017 477 «Cybersecurity Act») som vil styrke ENISA sitt mandat, samt innføre et felleseuropeisk rammeverk for sikkerhetssertifisering av IKT-produkter og IKT-tjenester.

Internasjonalt samarbeid er helt avgjørende for utvikling av globale retningslinjer og for å redusere og bekjempe digitale trusler. Norge deltar aktivt i ENISA sitt arbeid, men uten stemmerett. I takt med ENISAs styrkede rolle og økt kapasitet vil Norge prioritere samarbeidet med ENISA og øke den nasjonale anvendelsen av ENISA sine leveranser.

Ansvarlig virksomhet: JD og Samferdselsdepartementet (SD)
Gjennomføres: Løpende

Tiltak 15: Informasjonsdeling og operativt situasjonsbilde for digital hendelseshåndtering

Informasjonsdeling er avgjørende for å avdekke og håndtere digitale angrep. Det er behov for å øke samarbeidet og informasjonsflyten generelt, men spesielt i forhold til de virksomhetene som i dag ikke fanges opp av rammeverket for håndtering av IKT-sikkerhetshendelser (se tiltak 40). I denne sammenheng nevnes to sentrale tiltak:

- Etablering av verktøy for deling av tekniske indikatorsett. Private og offentlige virksomheter som knytter seg til løsningen skal kunne dele egne indikatorsett med andre, og motta indikatorsett fra NSM NorCERT.

- Videreutvikle et ugradert nasjonalt operativt situasjonsbilde som er tilgjengelig via en portal med påloggingsmulighet for sektorvise responsmiljøer og nasjonale beslutningstakere.

Ansvarlig virksomhet: NSM
Gjennomføres: Løpende

Tiltak 16: Standardisering

Difi skal fortløpende utrede bruk av sikkerhetsstandarder i statsforvaltningen. Alle IT-standarder i offentlig sektor er kategorisert som anbefalte eller obligatoriske avhengig av bruksområde, norske og europeiske lover, forordninger og forskrifter. Obligatoriske standarder inngår i forskrift om IT-standarder i offentlig forvaltning. Standardene er samlet i en referansekatalog som forvaltes av Difi. Referansekatalogen gir oversikt over anbefalte og obligatoriske IT-standarder for offentlig sektor.

Ansvarlig virksomhet: KMD og Difi
Gjennomføres: Løpende

Tiltak 17: Standard Norge

Norge skal være til stede på internasjonale arenaer hvor standarder for digital sikkerhet utvikles. I 2016, 2017 og 2018 har Standard Norge fått tilsagn om bevilgning til programmet «Standardisering innen IKT-sikkerhet». Det er reetablert en norsk speilkomite 1/SC 27, under ledelse av NSM, som skal bidra til å avklare behov for standarder innenfor IKT-sikkerhetsområdet. Videre skal det prioriteres deltakelse i en nystartet komite 1/SC 41 «Internet of Things». Det skal engasjeres eksperter og samarbeid med forskningsmiljøer inngår i prosjektet.

Ansvarlig virksomhet: JD og NSM
Gjennomføres: Løpende

Tiltak 18: Statens standardavtaler (SSA)

Statens standardavtaler brukes i stort omfang, ikke bare ved offentlige anskaffelser, men også mellom næringsdrivende. Nærings- og fiskeridepartementet har det overordnede ansvaret for standardavtalene. Mer utfyllende sikkerhetsklausuler, i første omgang i avtalene som brukes ved IKT-drift og skytjenester, kan potensielt ha stor positiv innvirkning på mange avtaler om tjenesteutsetting av IKT-tjenester. JD og KMD vil, i samarbeid med underlagte fagmiljøer, vurdere behovet for revisjon av sikkerhetsklausulene relevante for tjenesteutsetting.

Ansvarlig virksomhet: JD og KMD, i samarbeid med Difi og NSM
Gjennomføres: 2019

Tiltak 19: Gradert datakommunikasjon mellom departementene, underliggende etater og andre sentrale beredskapsaktører i sektorene

FD har ansvaret for drift og forvaltning av Nasjonalt BEGRENSET nett (NBN). NBN er en lavgradert IKT-plattform for utveksling av lavgradert informasjon. NBN er rullet ut til samtlige departementer, og relevante offentlige og private virksomheter tilkobles NBN fortløpende.

FD har fått i oppdrag å utvikle Nasjonalt HEMMELIG nett (NHN) for høygradert kommunikasjon i statsforvaltningen. NHN er under utvikling og det planlegges med utrulling til departementene i 2019. NHN bygger på samme arkitektur som NBN.

Ansvarlig virksomhet: FD
Gjennomføres: 2019

Tiltak 20: Sikret offentlig nett (SON)

Sikret offentlig nett (SON) er et høyhastighets datanett mellom deltakende aktører. Hovedformålet er at deltakerne skal få økt grad av beskyttelse mot tilsiktede uønskede hendelser fra internett. Ved bortfall av internett, kan deltakerne likevel kommunisere seg imellom over SON. Ved et pågående digitalt angrep mot én deltaker, kan virksomheten koble fra internett og benytte en annen deltakers internettlinje. SON kan også benyttes for å stoppe trafikk mot internettadresser som benyttes i angrep eller leverer virus og skadevare.

Ved etablering av SON som bærenett er det mulig å etablere fellestjenester mellom alle eller mellom enkelte av deltagerne. Eksempler på tjenester er SharePoint-løsninger, felles sikkerhetsløsninger, telefoni og epost. SON er også vurdert som mulig bærer for nasjonale graderte nett, for Forsvarets og politiets IKT-systemer og politiets alarm- og varslingssystem. Deltagerne i SON kan også benytte sikkerhetsgraderte sensorer (se tiltak 1), noe som vil styrke nasjonal deteksjonsevne.

SON er et pilotprosjekt under utvikling i et samarbeid mellom JD, FD, politiet og NSM. NSM skal lede videreutviklingen hvor SON er tiltenkt som en sentral komponent i NSMs nye sentraliserte VDI-løsning (se tiltak 1) og som et viktig beredskapstiltak for alle deltakende virksomheter. Det skal også utredes et forslag til mandat og eierskap, med en drifts- og styringsmodell som inkluderer de nødvendige forhold som følger av et slikt nasjonalt tiltak, herunder økonomi.

Ansvarlig virksomhet: NSM
Gjennomføres: 2018-2021

Tiltak 21: Nasjonal sikkerhetsmåned

Et av de større enkeltstående tiltakene som gjennomføres for å øke kunnskapen og kompetansen på digital sikkerhet er «Nasjonal sikkerhetsmåned». Tiltaket er en offentlig-privat dugnad for å skape oppmerksomhet om digital sikkerhet. Nasjonal sikkerhetsmåned gjennomføres i oktober hvert år, og ble i 2018 gjennomført for åttende gang. I 2018 ble det gitt opplæring til 250 000 ansatte i 330 virksomheter. NorSIS koordinerer gjennomføringen av nasjonal sikkerhetsmåned på oppdrag fra JD.

Ansvarlig virksomhet: NorSIS og JD
Gjennomføres: Årlig

Tiltak 22: Nasjonal kryptopolitikk

«Norsk kryptopolitikk» ble utgitt av daværende Nærings- og handelsdepartementet i 2001, og er basert på OECDs retningslinjer for kryptopolitikk publisert i 1997. Kryptering som tiltak bidrar til å beskytte informasjonens konfidensialitet, integritet og autentisitet, og er selve grunnlaget for sikker elektronisk databehandling og kommunikasjon. Det er et stort potensiale for å øke sikkerheten i tjenester som skal behandle sensitive data gjennom bruk av kommersielle løsninger. Å sørge for å opprettholde nødvendig nasjonal kryptokompetanse og å stimulere til innovasjon og produktutvikling, er andre årsaker til at det er behov for å revidere den nasjonale kryptopolitikken.

Det er nedsatt en arbeidsgruppe under ledelse av FD som reviderer kryptopolitikken. Sentrale tema som behandles er blant annet teknologisk utvikling, kryptokompetanse, rikets sikkerhet, næringsinteresser, eIDAS-forordningen og regulering av bruk av krypto.

Ansvarlig virksomhet: FD og JD
Gjennomføres: 2018-2019

Tiltak 23: NATO Cooperative Cyber Defence Centre of Excellence

NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) i Tallinn Estland, ble formelt etablert som et multinasjonalt NATO-akkreditert faglig cybersenter i 2008. NATO CCD COE har over 40 medarbeidere og arbeider med rettslige, politiske og operasjonelle cyberproblemstillinger, og publiserer arbeid som nyter global anerkjennelse. Norge har søkt om medlemskap i senteret. Det forventes en formell innlemming i løpet av 2019.

Ansvarlig virksomhet: FD, JD og Utenriksdepartementet (UD)
Gjennomføres: Etablering i løpet av 2019 (følges deretter opp løpende)

Tiltak 24: European Centre of Excellence for Countering Hybrid Threats

Det sikkerhetspolitiske landskapet preges av stadig mer sammensatte utfordringer og komplekse aktørbilder. Bruk av hybride virkemidler blir stadig mer utbredt. Flere land opplever desinformasjon, påvirkningskampanjer knyttet til valg og digitale angrep mot kritisk infrastruktur. Effekten av disse og andre hybride virkemidler forsterkes av samfunnets økte avhengighet av det digitale rom.

Det er nødvendig å møte disse utfordringene med en helhetlig tilnærming og god koordinering både nasjonalt og internasjonalt. Derfor har UD, FD og JD sammen gått inn for å forsterke innsatsen på dette området, blant annet ved å knytte Norge til det finskledede hybridsenteret (European Centre of Excellence for Countering Hybrid Threats). Her vil Norge samarbeide med allierte og nære partnere for å bedre kunne forstå og håndtere hybride trusler.

Ansvarlig virksomhet: UD, FD og JD
Gjennomføres: Løpende

Tiltak 25: Kapasitetsbygging internasjonalt

Norge støtter i dag prosjekter for å kartlegge behov for styrking av digital sikkerhet i utviklingsland. Som et ledd i dette skal Norge videreføre sin deltakelse i «Global Conference On Cyberspace» (GCCS). GCCS ble arrangert første gang i London i 2011 og omtales som Londonprosessen. GCCS er en diskusjonsarena der både statlige og ikke-statlige aktører fra næringslivet, akademia og sivilsamfunn møtes for å diskutere ulike aspekter av utfordringene i det digitale rom, med særskilt fokus på kapasitetsbygging og erfaringsutveksling.

Fokus hva gjelder kapasitetsbygging har gått fra fastsetting av prinsipper til implementering av disse. I 2015 ble «Global Forum On Cyber Expertice» (GFCE) etablert som oppfølging av Londonprosessen. Det er et konkret tiltak for samarbeid om kapasitetsbygging og deling av mønsterpraksis. Norge er medlem av GFCE og deltar i deres arbeid i ulike ekspertgrupper. Andre myndigheter og akademia oppfordres til å stille fageksperter til rådighet for å delta inn i ekspertgrupper internasjonalt for å bistå med kompetanseoverføring og kapasitetsbygging. Deltagelse inn i slike grupper må dekkes innenfor den enkelte virksomhets eksisterende rammer.

Ansvarlig virksomhet: UD og JD – andre virksomheter oppfordres til å bidra
Gjennomføres: Løpende

Tiltak 26: Kapasitetsbyggingstiltak på digital sikkerhet i utviklingsland

UD gir støtte til ulike aktører for å bidra til kapasitetsbygging i utviklingsland. Kapasitetsbygging innenfor digital sikkerhet skal styrke evnen til å beskytte kritisk infrastruktur og bekjempe digitale trusler, som en del av den bærekraftige utviklingsagendaen.

Ansvarlig virksomhet: UD
Gjennomføres: Løpende

Tiltak 27: Norwegian Cyber Range (NCR)

Norwegian Cyber Range (NCR) er den første nasjonale test- og øvingsarenaen for cyber- og informasjonssikkerhet på tvers av alle samfunnssektorer. NCR skal både være en akademisk og kommersiell øvingsarena, og på sikt også tilby kommersielle tjenester mot ulike markedssegmenter både privat og offentlig.

Testing, trening og øving er virkemidler for å eksponere virksomheter og mennesker for hendelser i realistiske, men trygge omgivelser. NCR sikrer effektiv og virkelighetsnær kompetansebygging, og kobler sammen samfunnsmodeller, digitale verdikjeder og digital infrastruktur i ett eller flere definerte miljøer. I tillegg vil man ut fra en slik øvingsarena kunne legge til rette for målrettet etter- og videreutdanningstilbud innenfor nasjonal IKT-sikkerhet.

NTNU har fått støtte fra fylkeskommunen i Oppland på 20 mill. kroner fordelt over tre år til å bygge opp NCR. Dette gjøres som en del av et samarbeid med Cyberforsvaret, Sivilforsvaret, Telenor Norge, EVRY, NorSIS, NSM og mnemonic gjennom NTNUs Center for Cyber and Information Security (NTNU CCIS).

Samarbeidet inkluderer også et felles prosjekt med Estland. Denne delen av prosjektet kalles «Open Cyber Range». Estland og Norge har fått 32 mill. kroner av EØS-midlene for å bli bedre til å bekjempe cyberkriminalitet. Prosjektet ledes av Estlands forsvars-departement, med deltagelse fra Teknologiuniversitet i Tallinn og NTNU sitt Institutt for informasjonssikkerhet og kommunikasjonsteknologi.

Ansvarlig virksomhet: NTNU
Gjennomføres: Lansert 2018

Tiltak 28: Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner for forsvarssektoren

FDs retningslinjer for informasjonssikkerhet og cyberoperasjoner i forsvarssektoren ble gitt ut i 2014. Siden 2014 har det blant annet skjedd endringer i etatsstrukturen under FD, begrepsbruken, i hjemmelsgrunnlag med videre. Det er derfor behov for å foreta en revisjon av retningslinjene.

Ansvarlig virksomhet: FD
Gjennomføres: 2018-2019

2.3. Digital sikkerhet i kritiske samfunnsfunksjoner

Vårt samfunn består av en rekke kritiske samfunnsfunksjoner, som energiforsyning, finansielle tjenester og satellittbaserte tjenester. Dette er funksjoner som må opprettholdes til enhver tid av hensyn til samfunnets grunnleggende behov. Flere av samfunnsfunksjonene forutsetter at man har en digital infrastruktur som virker nær sagt overalt og hele tiden. Under følger sentrale tiltak som skal understøtte målet om at kritiske samfunnsfunksjoner er understøttet av en robust og pålitelig digital infrastruktur.

Tiltak 29: Ny sikkerhetslov

FD la i juni 2017 frem forslag til ny lov om nasjonal sikkerhet (sikkerhetsloven) for Stortinget. Stortinget har vedtatt loven, som trådte i kraft 1. januar 2019.

Lovens virkeområde er utvidet fordi avhengighetene på tvers av sivil-militær, offentlig-privat og mellom samfunnssektorer øker. Loven inneholder også krav om sikring av alle skjermingsverdige informasjonssystemer, ikke bare systemer som behandler sikkerhetsgradert informasjon. Regler om eierskapskontroll gir mulighet til å kontrollere og eventuelt stanse oppkjøp av strategisk viktige selskaper underlagt sikkerhetsloven. Loven gir mer tilpassede regler om sikkerhetsgraderte anskaffelser. Det arbeides med å lage veiledere til den nye sikkerhetsloven.

Departementene skal kartlegge og identifisere tjenester, produksjon og andre former for virksomhet som er av en slik betydning at helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser (grunnleggende nasjonale funksjoner). Departementene skal videre fatte vedtak om hvilke virksomheter som loven skal gjelde for.

NSM styrkes i 2019 med 38 mill. kroner for å settes i stand til å implementere og starte utøvelsen av nye og utvidede oppgaver som sikkerhetsmyndighet i henhold til ny sikkerhetslov, herunder også for å forbedre kapasiteten til å gjennomføre inntrengingstester.

Ansvarlig virksomhet: FD
Gjennomføres: 2019

Tiltak 30: NIS-direktivet

NIS-direktivet pålegger EUs medlemsland å sørge for et minimumsnivå for den nasjonale digitale sikkerheten ved at de plikter å utarbeide en nasjonal strategi, etablere et nasjonalt responsmiljø for digitale hendelser (CSIRT), utpeke en nasjonal kompetent myndighet og å pålegge leverandører av samfunnsviktige tjenester og noen digitale tjenester IKT-sikkerhetskrav og varslingsplikt ved alvorlige IKT-sikkerhetshendelser. Medlemslandene plikter også å delta i samarbeidsgruppene som er etablert under NIS-direktivet, det vil si NIS samarbeidsgruppe for strategisk styring og CSIRT-nettverk.

Norge er foreløpig ikke forpliktet til å gjennomføre NIS-direktivet fordi direktivet ikke er innlemmet i EØS-avtalen. Den norske regjeringen besluttet i desember 2016 å anse direktivet som EØS-relevant og akseptabelt, og Island har inntatt samme posisjon. Liechtenstein har foreløpig ikke inntatt en endelig posisjon. EØS-prosessen er dermed ikke avsluttet ennå.

Regjeringen legger til grunn at direktivet blir bindende for Norge. Derfor er arbeidet med en eventuell gjennomføring av direktivet i norsk rett påbegynt. Høringsnotat om gjennomføring med utkast til lov som gjennomfører direktivet ble sendt på høring i desember 2018.

Direktivet gir på flere områder nasjonalt handlingsrom til å stille mer omfattende sikkerhetskrav til virksomhetene som blir berørt av direktivet og til flere enn det som følger av direktivet. Regjeringen legger foreløpig opp til at de norske reglene skal ligge så tett opptil direktivets virkeområde og krav som mulig. Det legges også foreløpig opp til å benytte eksisterende myndighetsstruktur i størst mulig grad. Dette vil kunne endres som følge av anbefalingene fra IKT-sikkerhetsutvalget (se tiltak 6).

Ansvarlig virksomhet: JD
Gjennomføres: 2019

Tiltak 31: Nasjonal kjerneinfrastruktur

For ekomsektoren er det særlig viktig å fortsette arbeidet med å øke diversitet og robusthet i ekomnettene innenlands og til viktige punkter i utlandet. I «Nasjonal Transportplan 2018-2029» er det lagt inn en satsing på en pilot som skal stimulere markedet til å øke redundansen i transportdelen av ekomnettene innenlands. Det ble bevilget 40 mill. kroner i 2018. Denne bevilgningen er videreført i 2019. Nkom har i 2018 på oppdrag fra og i samråd med SD jobbet med å spesifisere og igangsette pilotprogrammene.

Ansvarlig virksomhet: SD og Nkom
Gjennomføres: 2018-2020

Tiltak 32: Fiberføringer til utlandet

Fiberinfrastrukturen mot utlandet er en kritisk del av den moderne, nasjonale infrastrukturen. Ensidig ruting av norsk internettrafikk gjennom Sverige er en betydelig nasjonal sårbarhet. Nye utlandsforbindelser og alternativ ruting av trafikk vil bidra til å øke den samlede nasjonale kapasiteten, redundansen og sikkerheten i ekomnettene.

Det ble i 2018 bevilget 40 mill. kroner for å legge til rette for fiberkabler mellom Norge og utlandet. Denne bevilgningen er videreført i 2019, samt en tilsagnsfullmakt på 20 mill. kroner, slik at total ramme for satsningen er 100 mill. kroner. Nkom har i 2018 på oppdrag fra og i samråd med SD forberedt en utlysning av midlene.

Ansvarlig virksomhet: SD og Nkom
Gjennomføres: 2018-2020

Tiltak 33: Økt sikkerhet i ekomnett

Ekomnett bærer stadig større samfunnsverdier. Et utfall i ekomnett kan få alvorlige konsekvenser på de aller fleste samfunnsområder og for kritiske samfunnsfunksjoner. SD har igangsatt et arbeid med å utrede ulike tiltak for å øke sikkerheten i norske ekomnett. Det skal blant annet vurderes om det bør tydeliggjøres krav til eierne

av nettene, herunder om det bør stilles tydeligere krav til sikkerhet knyttet til utstyrsleverandører av ekominfrastruktur som bærer av kritiske samfunnsfunksjoner.

Ansvarlig virksomhet: SD og Nkom
Gjennomføres: Oppstart 2018

Tiltak 34: Forslag til ny lov om Etterretningstjenesten og tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon

FD nedsatte i 2016 et utvalg (Lysne II-utvalget) for å utrede de prinsipielle sidene ved en eventuell tilgang for Etterretningstjenesten til grenseoverskridende elektronisk kommunikasjon. Utvalget leverte sin rapport 26. august 2016, og anbefalte innføring av et digitalt grenseforsvar med klar innramming og strenge kontrollmekanismer for å ivareta personvernet. Rapporten ble sendt på høring og skapte bred offentlig debatt.

I 2017 bestemte regjeringen at FD skulle utrede hvordan en form for digitalt grenseforsvar kunne lovreguleres og etableres i Norge. Utredningen er foretatt på bakgrunn av utviklingen i trusselbildet, styrkingen av menneskerettighetenes stilling i norsk rett og digitaliseringen av samfunnet. Den teknologiske utviklingen har ført til at nesten all kommunikasjon er flyttet fra radio og satellitt til digitale signaler i kabler. Etterretningstjenesten har ingen egen tilgang til informasjonen som flyter i disse kommunikasjonskablene. Behovet for slik aksess aktualiseres av fremtredende utviklingstrekk i samfunnet, herunder fremveksten av grenseoverskridende trusler og den økte forekomsten av digitale trusler rettet mot statlige og private aktører.

Parallelt med utredningen om Etterretningstjenestens tilgang til grenseoverskridende elektronisk kommunikasjon er det foretatt en fullstendig gjennomgang av gjeldende lov om Etterretningstjenesten. Utredningene fremgår av høringsnotat som sendt på alminnelig høring 12. november 2018 med høringsfrist 12. februar 2019.

Ansvarlig virksomhet: FD
Gjennomføres: 2018-2019

Tiltak 35: Nasjonalt rammeverk for helhetsvurdering av verdikjeder

Lysneutvalget anbefalte å etablere et nasjonalt rammeverk for å ivareta en helhetsvurdering av verdikjeder. Utvalget begrunner dette blant annet med at lange og uoversiktlige verdikjeder som spenner over flere sektorer, nivåer og landegrenser, er en kjerneutfordring ved vurdering av digital sårbarhet. Komplekse digitale verdikjeder pekes på som et vesentlig hinder for å kunne fastslå hvilken digital sårbarhet vi har. Utvalget finner dette igjen i alle sektorer som de omhandler i rapporten. Som en oppfølging av anbefalingen er det nedsatt en arbeidsgruppe som skal foreslå et nasjonalt rammeverk for å ivareta en helhetsvurdering av verdikjeder.

Ansvarlig virksomhet: JD og DSB
Gjennomføres: 2019

Tiltak 36: NATO Cyber Defence Pledge

NATOs stats- og regjeringssjefer sluttet seg til en felles cybererklæring under NATO-toppmøte i 2016. Bakgrunnen var nye sikkerhetstrusler mot NATO, og behovet for å fremheve og prioritere arbeid for styrket digital sikkerhet i nasjonale nettverk og infrastrukturer på tvers av sektorer i samfunnet og mellom land.

Norge skal følge opp forpliktelsene som ligger i cybererklæringen. Landene har gjennom erklæringen forpliktet seg til å gjøre forbedringer på en rekke områder nasjonalt, siden det er medlemslandene selv som har ansvar for å sikre seg mot digitale trusler i nasjonal infrastruktur. Forpliktelsene omfatter områder som ressursallokering, samarbeid, forståelse og informasjonsdeling og kompetanseutvikling.

Ansvarlig virksomhet: FD og øvrige relevante departementer
Gjennomføres: Løpende, med årlig rapportering til NATO

Tiltak 37: Neste generasjon nødnett

I desember 2017 ble det besluttet at frekvensressurser i 700 MHz-båndet skulle gjøres tilgjengelig for interesserte kommersielle ekom-tilbydere i Norge. Frekvensene har gode dekningsegenskaper, og er viktige for å sikre utbredelse av avanserte mobiltjenester i hele Norge. 700 MHz-båndet er en av de utpekte ressursene for fremtidig utbygging av 5G, som er neste generasjons mobilnett og som er viktig for en vellykket digitalisering i privat og offentlig sektor.

Fremtidige kommunikasjonsløsninger for nød- og beredskapsetater og Forsvaret skal kunne leveres av de kommersielle mobiltilbyderne. Det vil derfor gjennomføres tiltak for å legge til rette for at disse samfunnsviktige brukernes behov kan bli ivaretatt gjennom en kombinasjon av myndighetspålegg og kommersielle anskaffelser.

JD og SD, sammen med DSB og Nkom, er i gang med utredninger knyttet til etablering av neste generasjon nødnett i de kommersielle nettene. Det skal i første omgang utarbeides en konseptvalgutredning om temaet.

Ansvarlig virksomhet: JD, SD, DSB og Nkom
Gjennomføres: Utredningsarbeid pågår. Kvalitetssikring planlegges gjennomført når konseptvalgutredning foreligger.

2.4. Kompetanse – oversikt over tiltak i nasjonal strategi for digital sikkerhetskompetanse

Kompetanse om digital sikkerhet er en knapp ressurs nasjonalt og internasjonalt. Regjeringen har de siste årene lagt til rette for bedre utdanningskapasitet og økt forskning på digital sikkerhet. En egen strategi skal legge til rette for en langsiktig oppbygging av kompetanse på digital sikkerhet, spesielt den nasjonale kapasiteten innenfor forskning, utvikling, utdanning og bevisstgjøringstiltak rettet mot befolkningen og virksomheter. Tabellen under lister tiltak som følger av nasjonal strategi for digital sikkerhetskompetanse.

TILTAK I NASJONAL STRATEGI FOR DIGITAL SIKKERHETSKOMPETANSE
Satsningsområde: Langsiktig forskning av god kvalitet
Prioritering av digital sikkerhet i revidert langtidsplan for forskning og høyere utdanning
Prosjekter i regi av IKTPLUSS v/Norges forskningsråd
Styrke digital sikkerhet som del av SAMRISK-programmet v/Norges forskningsråd
Fyrtårnprosjekt i regi av IKTPLUSS v/ Norges forskningsråd
Arena for forskningsformidling innenfor digital sikkerhet, større årlig konferanse
Styrke kjernemiljøene ved en kryptologisatsning fra 2018
Satsningsområde: Tilstrekkelig nasjonal spesialistkompetanse
Utdanning innenfor IKT og digital sikkerhet
Øke antall personer med ph.d. utdanning i digital sikkerhet inkludert kryptologi
Stimulere til bruk av nærings ph.d. og offentlig sektor ph.d. i regi av Norges forskningsråd
Likestillingstiltak for flere jenter til studier innenfor digital sikkerhet
Satsningsområde: Digital sikkerhet som del av IKT-relaterte utdanninger og tilgrensende fag
Kartlegge behov og tilbud av kurs i digital sikkerhet som del av IKT og tilgrensende fag
Styrke arbeidet med digital sikkerhet i ingeniør- og teknologiutdanningene
Satsningsområde: Etter- og videreutdanning (EVU) innenfor IKT og digital sikkerhet
Regjeringens kompetansereform – lære hele livet
Markussen-utvalget om udekkede behov for etter- og videreutdanning
Midler til utvikling av fleksible videreutdanningstilbud i digital kompetanse
Satsningsområde: Digital sikkerhet i yrkes- og profesjonsutdanninger
Gjennomgang av relevante læreplaner i fag- og yrkesopplæringen
Politiutdanning – kurs innenfor IKT-kriminalitet/digital sikkerhet, som del av bachelor- og masterutdanning
Styrket digital sikkerhet i helsefagutdanningene

Satsningsområde: God grunnkompetanse
Første fase av fagfornyelsen er utvikling av kjerneelementer i fagene
Videreutdanning for å styrke lærernes digitale kompetanse
Den teknologiske skolesekken inneholder flere tiltak for teknologiforståelse og digitale læremidler
Satsningsområde: Bevisstgjørende tiltak og bedret digital sikkerhetskultur
Undersøkelse om digital sikkerhetskultur
Måle grunnskoleelevenes digitale ferdigheter
Folkeopplysningskampanje
European Cyber Security Challenge i regi av ENISA
En pilot om opplæring av barn og ungdom i regi av NSM, NVE, NorSIS, NTNU, UiO og Abelia i Oppegård, Ski og Rogaland

2.5. Avdekke og håndtere digitale angrep

Digitale angrep kan være krevende å oppdage og kan i ytterste konsekvens utgjøre en trussel mot nasjonale interesser eller krenkelse av norsk suverenitet. Å øke vår nasjonale evne til å avdekke og håndtere digitale angrep er derfor viktig. Under følger sentrale tiltak som skal understøtte målet om at samfunnet har en bedre evne til å avdekke og håndtere digitale angrep.

Tiltak 38: Sektorvise responsmiljøer

En nasjonal satsning på det digitale sikkerhetsområdet er etablering av sektorvise responsmiljøer, og styrking av den nasjonale modellen for hendelseshåndtering. Ambisjonen med de sektorvise responsmiljøene er at disse skal kunne bistå sin sektor med kompetanse og være knutepunkt for informasjon og informasjonsflyt mellom virksomheter i sektoren, mellom sektorer og mellom sektor og nasjonalt nivå (NorCERT). NorCERTs koordinering og bistand til håndtering innebærer blant annet å dele informasjon med de sektorvise responsmiljøene, politiet, samfunnskritiske virksomheter og andre aktuelle aktører. NSM bistår også i etableringen og oppfølgingen av de sektorvise responsmiljøene. Som en minimumsløsning skal det etableres et kontaktpunkt i sektoren for alvorlige IKT-hendelser og prosedyrer for varsling internt i sektoren og opp mot NSM NorCERT. Utover dette må sektorene selv vurdere hva slags behov de har for å håndtere alvorlige IKT-hendelser og hvordan de eventuelt skal skalere opp sine responsmiljøer.

Det skal arbeides videre med implementering av nasjonal struktur for håndtering av hendelser i tråd med rammeverk for håndtering av IKT-sikkerhetshendelser. De sektorvise responsmiljøene skal ha departementsforankring.

Ansvarlig virksomhet: JD, med oppfølging av samtlige departementer
Gjennomføres: Løpende

Tiltak 39: JustisCERT

I tråd med nasjonale føringer etablerte JD tidligere et responsmiljø på minimumsnivå for varsling i sektor og opp mot NSM NorCERT. JD har sammen med sektor vurdert merbehovene, og det er besluttet å etablere JustisCERT som erstatning for tidligere minimumsløsning. Etableringen vil være i tråd med rammeverket for håndtering av IKT-sikkerhetshendelser. JustisCERT vil ha kapabilitet til å detektere, analysere, varsle, koordinere og håndtere alvorlige digitale hendelser i Justissektoren, samt aktivt bidra gjennom ulike tiltak til å redusere sårbarheten i Justissektoren. JustisCERT vil betjene over 19 enheter i justissektoren, samt flere større underenheter av disse. Uavhengig av størrelse, vil alle enheter i justissektoren kunne nye godt av kapabiliteten til JustisCERT, og tiltaket finansieres av samtlige deltagende virksomheter.

Ansvarlig virksomhet: JD, Politidirektoratet (POD) og tilknyttede virksomheter
Gjennomføres: 2018-2019

Tiltak 40: Rammeverk for håndtering av IKT-sikkerhetshendelser

Det er behov for bedre og mer effektiv samhandling ved håndtering av hendelser som påvirker flere virksomheter og sektorer. Det vil arbeides videre med implementering av nasjonal struktur for håndtering av hendelser i tråd med beslutning av rammeverk fra 2017. Rammeverket skal videreutvikles gjennom blant annet:

- Formalisering og forankring av sektorvise responsmiljøer på departementsnivå i alle sektorer for beskyttelse av nasjonale grunnleggende funksjoner.
- Formalisering av sektorvise responsmiljøers rolle i krisehåndteringsplanverk og øvelser.
- Etablering av verktøy og prosesser for effektiv deling av informasjon om hendelser.
- Inkludering av private aktører.
- Få på plass en struktur for kommunenes og fylkesmennenes rolle i responsmiljøene og i rammeverk for håndtering av IKT-sikkerhetshendelser.

Ansvarlig virksomhet: JD og FD (eiere) og oppfølging av samtlige departementer
Gjennomføres: Løpende

Tiltak 41: IKT-sikkerhetsøvelse

Det skal gjennomføres en ny nasjonal IKT-sikkerhetsøvelse med formål å styrke sivil-militært, offentlig-privat og internasjonalt samarbeid for hendelseshåndtering. En ny nasjonal øvelse vil spesielt ta utgangspunkt i et styrket offentlig-privat samarbeid, og vil derfor inkludere private virksomheter i planlegging, utforming og gjennomføring av øvelsen.

Sentrale eiere av kritisk digital infrastruktur og andre utvalgte private virksomheter, vil inviteres med i tidlig fase for sammen med myndighetene definere øvingsbehov, -form, -mål og rammer for øvelsen. Øvelsen skal også øve sivilt-militært samarbeid, og benyttes for å videreutvikle det nasjonale rammeverket (se tiltak 40) til å inkludere

private virksomheter. JD, FD og SD er oppdragsansvarlige for øvelsen. DSB vil lede planleggingsprosessen og gjennomføringen av øvelsen i nært samarbeid med blant annet NSM, Nkom og private aktører.

Ansvarlig virksomhet: JD, FD og SD
Gjennomføres: 2020

Tiltak 42: Internasjonale øvelser

Bruk av øvelser på alle nivåer er et viktig virkemiddel for å øke evnen til krisehåndtering og for å avdekke behov for kompetanse. Norge deltar i en rekke internasjonale øvelser:

- NATOs Cyber Coalition: NATOs største og viktigste Cyber Defence-øvelse, med deltakere fra en rekke allierte, partnerland, EU, industri og akademia. Formålet med Cyber Coalition er å øve evnen til å beskytte NATOs og nasjonale nettverk mot ulike former for digitale angrep.

- Locked Shields: NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) sin årlig øvelse rettet mot teknisk personell og de teknisk operative miljøene herunder CERT-miljøer. Hensikten med øvelsen er å styrke og komme tettere på kompetanse- og fagutviklingen innenfor NATO-alliansen. NSM NorCERT sikrer og koordinerer den norske deltakelsen i øvelsen med både egne ressurser og med ressurser fra andre sektorer.

- Cyber Europe: EUs store cyberøvelse som ENISA arrangerer hvert andre år. Øvelsen simulerer omfattende og alvorlige uønskede hendelser og inkluderer både tekniske oppgaver og kommunikasjon/samarbeid. NSM deltok i 2016 og 2018.

- NATOs CMX: CMX er NATOs årlige krisehåndteringsøvelse for politisk og strategisk nivå. Hensikten er å øve krisehåndtering i samspill med nasjonale og allierte myndigheter.

Ansvarlig virksomhet: FD, JD og NSM
Gjennomføres: Løpende

Tiltak 43: Felles cyberkoordineringssenter (FCKS)

FCKS er et permanent, samlokalisert fagmiljø med representanter fra NSM, E-tjenesten, PST og Kripos. FCKS skal bidra til å øke den nasjonale evnen til å motstå alvorlige digitale angrep og understøtte strategisk analyseproduksjon og vedlikeholde et helhetlig trussel- og risikobilde for det digitale rom. FCKS er ikke et selvstendig organ med egen beslutningsmyndighet, og etableringen innebærer ingen endringer i rettsgrunnlag, fullmakter, roller eller oppgaver.

For å sikre at formålet med etableringen av FCKS oppnås skal E-tjenesten, PST, NSM og Kripos foreta en evaluering av senteret etter to års drift.

Ansvarlig virksomhet: FD og JD
Gjennomføres: 2019

Tiltak 44: Tverrsektoriell cyberreserve

NSM skal i perioden 2018-2019 utrede en tverrsektoriell cyberreserve for hendelseshåndtering ved spesielt store kriser som krever innsats utover ordinær bemanning. I utredningen skal det sees på hvilke krav som må stilles til personell i en slik modell, og hvilke miljøer eller personer det er naturlig å knytte til et slikt tiltak. Andre momenter som må avklares er blant annet juridiske forhold, behov for klarering av personell, og øvelser og trening for å opprettholde kompetanse.

Ansvarlig virksomhet: NSM
Gjennomføres: 2018-2019

Tiltak 45: Åpenhet og evaluering av uønskede digitale hendelser

NSM har tidligere på oppdrag fra JD utarbeidet anbefalinger for hvordan offentlige og private virksomheter bør vurdere åpenhet om uønskede digitale hendelser. Anbefalingene er laget i samarbeid med Difi, NorSIS, POD og Næringslivets sikkerhetsråd (NSR). Offentlige og private virksomheter oppfordres til å følge disse anbefalingene.

Videre følger det av instruks for departementenes arbeid med samfunnssikkerhet, at det ved større hendelser ligger til lederdepartementet å sørge for evaluering av hendelseshåndteringen. Formålet med evalueringen er å identifisere læringspunkter, foreslå tiltak og påse at de følges opp.

Det er bestemt at det etter datainnbruddet i Helse Sør-Øst i 2018, skal gjennomføres evalueringer i helsesektoren, NSM og JD. Videre bør større uønskede digitale hendelser evalueres. Myndighetene anbefaler at også private virksomheter evaluerer større hendelser og deler erfaringer.

Ansvarlig virksomhet: Alle
Gjennomføres: Løpende

2.6. Bekjempe data- og IKT-relatert kriminalitet

Regjeringen vil sørge for at politiet har de forutsetningene som er nødvendige for å bekjempe data- og IKT-relatert kriminalitet. Kapasitet og kompetanse står særlig sentralt. I tillegg til tiltakene nedenfor vises det til tiltak 4 om etablering av NC3.

Tiltak 46: Stortingsmelding om politiets kapasitet og kompetanse

Regjeringen vil legge frem en melding om endringene i kriminalitetsbildet og konsekvenser for politiets oppgaver og tjenester. Meldingen vil gjennomgå og drøfte utviklingstrekkene og konsekvenser for politiets kapasitet og kompetanse.

Ansvarlig virksomhet: JD
Gjennomføres: 2019

Tiltak 47: Politiets sikkerhetstjeneste (PST)

For 2019 økte PSTs bevilgning med 25 mill. kroner til arbeid med hybride trusler og cybertrusler, slik at PST får personell og teknologi som gir bedre kapasitet i det digitale rom til å avdekke, forhindre, håndtere og etterforske de mest alvorlige forsøkene på spionasje, sabotasje, påvirkningsoperasjoner og sammensatte (hybride) trusler. Bevilgningen vil blant annet gi grunnlag for videre utvikling av PSTs samarbeid med E-tjenesten, NSM og Kripos i FCKS.

Ansvarlig virksomhet: JD
Gjennomføres: 2019

Tiltak 48: Støtte FNs innsats for å bekjempe data- og IKT-relatert kriminalitet globalt

Norge bidrar i 2018-2021 med 35 mill. kroner i støtte til FNs kontor for narkotika og kriminalitet (UNODC) for bekjempelse av data- og IKT-relatert kriminalitet. UNODC bistår utviklingsland i å gjennomføre relevant lovgivning, lære opp politiet i etterforskning og påtalearbeid, og domstolene i å sikre bevis, samt forfølge digitale spor og evne til å dele informasjon mellom land. Prosjektet gjennomføres i perioden frem til 2021 i land i Vest-Afrika, Midtøsten, Nord-Afrika og Sørøst-Asia. Ambisjonen er å nå ut til så mange dommer-, påtale- og politifunksjoner som mulig. Målet er at den norske støtten kan bidra konkret til å redde liv og ta bakmenn, også i saker med forgreninger til Norge. Norge bidrar fra før med en ekspert til UNODCs arbeid mot data- og IKT-relatert kriminalitet.

Ansvarlig virksomhet: UD
Gjennomføres: 2018-2021

Tiltak 49: Nasjonalt elektronisk identitetsbevis (eID)

De nasjonale ID-kortene som etter planen vil bli lansert i 2020 skal inneholde elektronisk identitetsbevis (eID). Med dette vil sikkerhetsnivået for elektronisk identifisering bli det samme som for pass, og en person kan kun ha én nasjonal eID. eID-en vil tilbys både norske og utenlandske borgere som kvalifiserer til nasjonalt ID-kort. IKT-tjenester som har behov for samme sikkerhetsnivå som identifisering med pass kan med dette ta i bruk nasjonal eID og med det redusere faren for misbruk. Nasjonal eID vil kunne brukes både på offentlige og private tjenester, og skal være et supplement til eID-er i markedet. Sikkerhetsnivået i offentlige tjenester er definert i «Rammeverk og autentisering og uavviselighet i offentlig kommunikasjon».

Ansvarlig virksomhet: JD
Gjennomføres: 2020

Tiltak 50: Internasjonalt samarbeid om data- og IKT-relatert kriminalitet

JD skal fremme internasjonalt samarbeid og deltakelse i internasjonale fora hvor det pågår arbeid med relevans for norsk forebygging og bekjempelse av data- og IKT-relatert kriminalitet. Dette omfatter samarbeid i bl.a. FN, Europarådet og EU.

Ansvarlig virksomhet: JD
Gjennomføres: Løpende

Tiltak 51: Politiets nasjonale innbyggerundersøkelse

POD gjennomfører årlig innbyggerundersøkelser der befolkningens tillit til politiet står sentralt. Befolkningens inntrykk av politiets håndtering av ulike hendelser, bla kriminalitet på nett, inngår i undersøkelsen. Innbyggerundersøkelsen gir verdifull informasjon om befolkningens opplevelse av trygghet og politiets evne til å håndtere data- og IKT-relatert kriminalitet.

Ansvarlig virksomhet: POD
Gjennomføres: Årlig

3. DEL 2 – Anbefalte tiltak for å øke virksomheters egenevne

Offentlige myndigheter har kommet med flere råd og anbefalinger de siste årene for å øke virksomheters egenevne til å beskytte seg mot og håndtere uønskede digitale hendelser. Blant disse er NSMs «Grunnprinsipper for IKT-sikkerhet» og Difis «Internkontrollveileder»[1].

Denne delen består av 10 anbefalte tiltak som virksomheter i offentlig og privat sektor bør gjennomføre. Tiltakene er hentet frem gjennom et samarbeid bestående av virksomheter fra både offentlig og privat sektor. Tiltakene bygger på de råd og anbefalingene som er nevnt over, og gir norske virksomheter et godt utgangspunkt for hva de bør tenke på, uavhengig av størrelse, modenhet og kompetanse om digital sikkerhet.

En nasjonal innsats for å øke grunnsikringen

God styring og effektive virksomhetsprosesser er vesentlig for å opprettholde ønsket kvalitet, utvikling og for å levere etter fastsatte mål. Styring og involvering fra ledelsen bidrar til at de riktige tiltakene blir iverksatt og at ressursene brukes riktig. Samtidig oppnås det ikke digital sikkerhet kun med etablerte prosesser og involvering fra ledelsen. Det er de faktiske sikkerhetstiltakene som implementeres, som konfigurering av IKT-systemene, bygningsbarrierer og handlinger til den enkelte ansatte, som setter det reelle sikringsnivået.

For å opprettholde ønsket sikkerhetsnivå må digital sikkerhet være en integrert del i alle virksomhetens fagområder og virksomhetsprosesser. Det avhenger av at man har kontroll på hva man gjør, og at beslutninger tas på et tilstrekkelig informasjonsgrunnlag. God sikkerhetsstyring er en forutsetning for å lykkes. For å få til dette må styret og ledelsen ha eierskap til sikkerhetsprosesser og -aktiviteter. Digital sikkerhet må inkluderes i risiko- og rapporteringsprosesser og virksomheten må ha personell med tilstrekkelig fagkompetanse og kjennskap til egen virksomhet. Et godt utgangspunkt for å få til dette er Difis internkontrollveileder og NSMs veileder i sikkerhetsstyring.

Virksomheter må i tillegg gjennomføre nødvendige tiltak for å sikre IKT-systemene. NSMs grunnprinsipper for IKT-sikkerhet beskriver tiltak som alle virksomheter bør implementere for god grunnsikring. De definerer et sett med prinsipper og underliggende tiltak for å beskytte IKT-systemer (maskinvare, programvare og tilknyttet infrastruktur), data og tjenestene de tilbyr mot uautorisert tilgang, skade eller misbruk.

For mange virksomheter kan veien til god virksomhetsstyring og implementering av de riktige tiltakene virke lang. Punktene under beskriver 10 viktige tiltak for å starte sikkerhetsarbeidet.

1 https://www.nsm.stat.no/grunnprinsipper-ikt
http://internkontroll.infosikkerhet.difi.no/

Anbefaling 1: Ledelse

Digital sikkerhet må være en integrert del av virksomhetens IKT-systemer og tjenester. Det avhenger igjen av gode prosesser for styring og ledelse. Det bør etableres aktiviteter for sikkerhetsstyring, som del av virksomhetsstyringen, hvor det er tydelige krav og forventninger til sikkerhet. Dette inkluderer å tilføre nødvendige ressurser med tydelig ansvarsbeskrivelse og oppfølging. Omfanget må tilpasses virksomhetens størrelse og behov. Dette kan tilrettelegges svært enkelt, med få roller og enkel gjennomføring, i en liten virksomhet. Motsatt settes det større krav til virksomheter som har et større beskyttelsesbehov.

Start-tips: Etabler tilstrekkelig systematikk for sikkerhetsstyring, og sørg for at en fagperson støtter ledelsen i arbeidet.

Anbefaling 2: Risikostyring

Etabler en prosess for risikostyring i virksomheten som er en del av en helhetlig styringsstruktur. Prosessen for risikostyring må være kjent i virksomheten. Målet er at ansatte kjenner virksomhetens risikostyring, hvordan beslutninger tas og hvilket risikonivå som er akseptabelt.

Det er viktig å ha gode føringer for hvordan man skal forstå og vurdere risiko, hvilke kriterier som gjelder for å akseptere risiko, og hvem som skal ta beslutninger basert på identifisert risiko. Dette er viktig for å sikre at avgjørelser om risiko tas på riktig nivå og grunnlag. Risikostyring for digital sikkerhet bør inngå som del av den helhetlige risikostyringen i virksomheten. Etabler derfor prosesser for å evaluere og kvalitetssikre sikkerhetstiltak, hvor resultatene rapporteres til ledelsen.

Start-tips: Inkluder digital sikkerhet i virksomhetens risikoarbeid. Etabler tydelig ansvar i virksomheten, og effektive rapporteringslinjer til toppledelse og styre.

Anbefaling 3: Kartlegg verdikjeder, informasjonsverdier, utstyr og brukertilganger

Å kjenne sin egen virksomhet er viktig for å drive effektivt og levere gode tjenester. Kartlegging av mål, leveranser og tjenester vil bidra til at viktige verdikjeder, informasjon og avhengigheter blir identifisert og vurdert. Det er viktig å kartlegge virksomhetens leveranser og verdikjeder, hvilke enheter og programvare virksomheten støtter seg på, og hvilke brukere og brukertilganger som eksisterer. Dersom en virksomhet ikke har god nok oversikt kan enkelte deler av IKT-systemene være godt sikret, mens andre, vitale deler er åpent eksponert og sårbart for digitale angrep.

Start-tips: Lag en oversikt over virksomhetens sentrale mål, hvilke verdier og verdikjeder som inngår, hvor viktige data lagres og hvem som har tilgang til disse dataene.

Anbefaling 4: Inkluder digital sikkerhet i virksomhetskulturen

Ansattes kunnskaper og holdninger er vesentlig for at virksomheter kan operere sikkert. Virksomheter må derfor sørge for at ansatte har nødvendig informasjon, kunnskap og ferdigheter til å opprettholde ønsket sikkerhetsnivå. En virksomhetsledelse må kommunisere mål og prioriteringer for digital sikkerhet tydelig og effektivt, og fremstå som gode rollefigurer. Alle ansatte, fra øverste ledelse til nyansatte fra skolen, bør følge tilpassede spor for opplæring, kompetansebygging og bevisstgjøring om sikkerhet. Ansatte som opererer og støtter sentrale tjenester må ha tilstrekkelig kunnskap og erfaring for å opprettholde sikker drift av IKT-systemene.

Start-tips: Kartlegg virksomhetens sikkerhetskultur og identifiser hva som kan forbedres. Fastsett ønsket kultur og gjennomfør tilpasset, årlige treningsprogram for å fremme god sikkerhetskultur.

Anbefaling 5: Leverandørkontroll

Ved kjøp av IKT-tjenester og IKT-produkter er det viktig at sikkerheten blir ivaretatt på et nivå som virksomhetens ledelse er komfortabel med. Det må stilles krav til produkter og leverandører slik at sikkerheten er ivaretatt i hele produktets eller tjenestens levetid. Det er viktig med god bestillerkompetanse, oversikt og kontroll på hele livsløpet, gode risikovurderinger, riktige og gode krav til IKT-tjenesten og til leverandør, og at beslutningen tas på riktig nivå.

Start-tips: Sats på god bestillerkompetanse og gjør en risikovurdering som forankres hos ledelsen.

Anbefaling 6: Sikker konfigurasjon

For at ansatte skal jobbe effektivt og ha tillit til arbeidsverktøyene, må IKT-systemene kunne stoles på. Dette gjøres ved å etablere tillitsverdige systemer og tjenester, konfigurere og tilpasse maskin- og programvare og verifisere at konfigurasjonen er riktig. Svake ledd i oppsett og konfigurering av IKT-systemer kan utnyttes av trusselaktører og gir økt risiko for uforutsette hendelser. Konfigureringen må oppdateres kontinuerlig, i takt med endringer i teknologi, bruksmønster og trusselbilde.

Start-tips: Oppgrader program- og maskinvare. Fjern unødvendig kompleksitet og ubrukt funksjonalitet. Blokker kjøring av ikke-autoriserte programmer.

Anbefaling 7: Kontroll på nettverk og systemkomponenter

Virksomhetens nettverk og systemkomponenter vil være utsatt for ytre og indre påvirkninger. Dette kan være skadelig programvare som kan skade maskiner og nettverk, eller planlagte endringer som følge av et nytt regnskapssystem som skal innføres. Det vil uansett være en del hensyn virksomheten må ta slik at IKT-systemene opprettholder ønsket robusthet. Virksomheten må innføre tiltak for beskyttelse mot skadevare, overvåkning og analyse av IKT-systemet og håndtering av endringer. For å undersøke om korrekte sikkerhetsmekanismer er på plass, vil det i mange tilfeller lønne seg å gjennomføre tester og øvelser hvor man forsøker å oppnå tilgang til ressurser og data som man ikke skal ha tilgang til.

Start-tips: Installer sikkerhetsoppdateringer så raskt som mulig. Beskytt trådløse nettverk med sterke sikkerhetsmekanismer. Planlegg og dokumenter endringer. Slå på logging og gjennomgå viktige logger jevnlig.

Anbefaling 8: E-post og websikkerhet

Alle virksomheter må ha kontroll på egne data og tjenester for å ivareta behov for kvalitet og sikkerhet. E-post og websikkerhet bør ha et særskilt fokus da mange av truslene fra internett kommer inn via disse kanalene. Direktørsvindel, nettfiske (phishing) eller skadevare som kryptovirus er eksempler på slike trusler. Vedlegg i e-post er en av de vanligste inngangsveiene for å distribuere datavirus, ormer og annen type skadevare. Vedlegg i e-post bør derfor alltid behandles varsomt, spesielt hvis avsender ikke er kjent.

Virksomheten bør ha kontroll på informasjonsflyten som går til og fra eget nettverk, samt innad i eget nettverk. Data og tjenester må beskyttes både når det ligger lagret hos virksomheten, eller hos en tjenesteleverandør, og når data formidles over ulike informasjonskanaler som over internett.

Start-tips: Bruk kun siste versjon av nettlesere. Beskytt e-post med DMARC. Krypter viktig informasjon når det lagres på bærbare medier og når det sendes over nettet.

Anbefaling 9: Tilgangskontroll

Tilgangen til virksomhetens data og tjenester må kontrolleres slik at det ikke blir misbrukt av uvedkommende. Dette gjøres ved å ha kontroll på kontoer, kontrollere bruk av administrative privilegier, sørge for sikker pålogging og jevnlig gjennomgå tilgangsrettigheter.

Fysisk tilgang til nettverk og informasjonssystemer, inkludert datarom, bør tilgangsstyres på lik linje med logiske tilganger.

Start-tips: Endre standard passord og ikke tildel sluttbrukere administratorrettigheter. Bruk 2-faktor autentisering, eller som et minimum, sterke passord.

Anbefaling 10: Hendelsesberedskap

Alle virksomheter må være forberedt på å håndtere hendelser når dette oppstår ved å utvikle og implementere effektive prosesser for hendelseshåndtering. Dette gjøres ved å oppdage hendelser hurtig, kontrollere og fjerne hendelsesårsaken effektivt, og gjenopprette tilliten til systemer og nettverk. Prosessene inkluderer planverk, definerte roller, øving, kommunikasjon og ledelsesoversikt. En viktig del av dette er muligheten for gjenoppretting av data dersom det blir nødvendig. Hendelseshåndtering og beredskap er en sentral del av virksomhetens helhetlige plan for virksomhetskontinuitet.

Start-tips: Etabler en beredskapsplan for ulike typer hendelser og gjennomfør øvelser som tester planverket.

Notater

Notater

Utgitt av:
Departementene

Bestilling av publikasjoner:
Departementenes sikkerhets- og serviceorganisasjon
www.publikasjoner.dep.no
Telefon: 22 24 00 00
Publikasjoner er også tilgjengelige på:
www.regjeringen.no
Publikasjonskode: G-0445 B
Design og layout: Konsis Grafisk
Trykk: Departementenes sikkerhets- og serviceorganisasjon
01/2019 – opplag 2000