Departementene

Strategi

Nasjonal strategi for digital sikkerhet

Forord

Norge er blant de fremste landene i verden til å ta i bruk ny teknologi. Som politikere har vi et ansvar for å sørge for at vi får maksimalt ut av ressursene som brukes på felleskapet. Vi jobber for at både offentlige og private virksomheter skal ta i bruk digitale løsninger, fordi det gir store muligheter for effektivisering, konkurransekraft og etablering av nye arbeidsplasser.

Digitaliseringen av det norske samfunnet utfordrer oss også. Digitale infrastrukturer og systemer blir stadig mer komplekse, omfattende og integrerte. Det skapes avhengigheter og sårbarheter på tvers av ansvarsområder, sektorer og nasjoner. Det forventes at digitale tjenester skal være tilgjengelige til enhver tid. En vellykket digitalisering handler også om at løsningene ivaretar krav til sikkerhet og den enkeltes personvern på en god måte, og at vi kan ha tillit til at digitale løsninger fungerer slik de skal.

Norges første nasjonale strategi for digital sikkerhet ble lansert allerede i 2003. Med denne ble Norge et av de aller første landene i verden som fikk en nasjonal strategi på området. I takt med utviklingen av trusselbildet ble den nasjonale strategien revidert i 2007 og 2012.

I 2015 fikk vi Digitalt sårbarhetsutvalgs (Lysneutvalget) rapport om digitale sårbarheter i det norske samfunnet. Oppfølgingen av rapporten førte bl.a. til at Norge i 2017 fikk sin første stortingsmelding som utelukkende omhandler digital sikkerhet. Stortingsmeldingen har navnet «IKT-sikkerhet – et felles ansvar». Dette er ikke uten grunn – vi har alle en felles interesse av, og et ansvar for, å sikre våre verdier. Det som tidligere var et tema for spesielt interesserte er blitt noe som angår oss alle.

Denne strategien blir Norges fjerde strategi for digital sikkerhet. Strategien skal møte utfordringene som følger av en rask og gjennomgående digitalisering av det norske samfunnet. Videreutviklingen fra tidligere nasjonale strategier baserer seg på behovet for et styrket offentlig-privat, sivil-militært og internasjonalt samarbeid. Strategiens primære målgruppe er myndigheter og virksomheter i privat og offentlig sektor, herunder kommunene. Strategien skal også legge til rette for at privatpersoner får nødvendig kunnskap og risikoforståelse for å kunne ta i bruk teknologi på en trygg måte.

I utarbeidelsen av strategien er det lagt vekt på inkludering av aktører i privat og offentlig sektor, for å sikre at strategien er relevant. Strategikonferansen med over 300 deltagere, skriftlige innspill og høy deltagelse i en rekke workshops viser at det er stor interesse for å finne felles løsninger. Jeg vil rette en stor takk til alle som har bidratt med innspill i strategiprosessen.

Nå starter den viktigste jobben – oppfølgingen. Jeg håper dere tar eierskap til den nye nasjonale strategien for digital sikkerhet, setter strategien på dagsorden og bidrar til at den følges opp. Ved å møte digitale sikkerhetsutfordringer på en god måte, kan vi få større utbytte av de positive mulighetene digitaliseringen gir oss som enkeltmennesker, virksomheter og som samfunn.

Erna Solberg
Statsminister

Innhold

1 Innledning

1.1 Utfordringsbildet

Teknologien vil endre mye i årene som kommer. Robotisering, sensorteknologi, 3D-printing, stordata og kunstig intelligens er eksempler på teknologiske fremskritt som vil endre samfunnet. Vi vil få digitale tjenester vi knapt kan forestille oss, som vil være tilgjengelige hele tiden, og over alt. Vår hverdag er digital, primært til det gode for privatpersoner, virksomheter og myndighetene.

Digitaliseringen bringer også med seg utfordringer. Samfunnets sårbarhet for digitale trusler blir stadig større, og en god forståelse av samfunnets digitale avhengigheter blir viktigere. Infrastrukturer og IKT-systemer blir mer komplekse, globale og integrerte. Flere enheter kobles til internett, og bruk av skyløsninger øker. Behovet for å redusere kostnader og øke tilgangen til kompetanse gjør at flere IKT-funksjoner settes ut til tredjeparter, særlig i lavkostland. Sammensatte (hybride) trusler visker ut det tradisjonelle skillet mellom fred og væpnet konflikt, og utfordrer tradisjonell ansvarsplassering mellom sivil og militær sektor.

Den raske utviklingen gjør det krevende å forutse hvilke trusler som vil prege risikobildet fremover. Men trolig vil enkelte trusler som løsepengevirus, industrispionasje, sabotasje, personutpressing, krenkelser på nett og ID-tyveri fortsette å prege risikobildet de neste årene. Dette er trusler rettet mot privatpersoner og virksomheter, og konsekvensene kan være svært alvorlige for de som rammes.

Nasjonal sikkerhetsmyndighet (NSM) utgir årlig rapporten «Helhetlig IKT-risikobilde». Rapporten bygger på en omfattende portefølje av risiko- og sårbarhetsrapporter fra myndigheter, næringslivet, akademia og bransje- og interesseorganisasjoner. I 2018-rapporten fremgår det at digitaliseringen av samfunnet endrer verdien på eksisterende og nye digitale løsninger. For hver gang nye tjenester digitaliseres eller automatiseres øker samfunnets digitale avhengighet. Samtidig som tjenestene gjøres tilgjengelig i det digitale rom eksponeres også verdiene for trusselaktørene som opererer i domenet. Dette skaper nye sikkerhetsutfordringer og endrer risikobildet.

Trusselbildet preges av vedvarende trender fra tidligere år, samt en forsterkning av visse utviklingstrekk. Fremmedstatlig etterretningsaktivitet mot offentlige og private virksomheter samt data- og IKT-relatert kriminalitet, utgjør de fremste digitale truslene mot det norske samfunnet i 2018.

1.2 Strategi

Justis- og beredskapsdepartementet har et samordningsansvar for samfunnssikkerhet i sivil sektor. Departementet har et særlig ansvar for nasjonal digital sikkerhet i sivil sektor, og skal utforme regjeringens politikk for digital sikkerhet, herunder etablere nasjonale krav og anbefalinger for offentlige og private virksomheter.[1] Forsvarsdepartementet har ansvar for digital sikkerhet i forsvarssektoren. Myndighetene har et bredt spekter av virkemidler for å ivareta dette ansvaret, blant annet gjennom utvikling av regelverk og kunnskap, tilsynsvirksomhet og rådgivning og veiledning.

Myndighetene kan imidlertid ikke løse alle utfordringer i det digitale rom alene. Kritiske samfunnsfunksjoner og andre norske interesser er avhengige av digitale infrastrukturer som stadig øker i omfang og kompleksitet. Lange og uoversiktlige digitale verdikjeder, som spenner over flere sektorer og landegrenser, er en kjerneutfordring ved vurdering av digital sårbarhet.

De digitale sikkerhetsutfordringene skal derfor løses gjennom særlig å vektlegge samarbeid og partnerskap mellom relevante aktører, både nasjonalt og internasjonalt. Utfordringene skal løses i fellesskap, på tvers av sektorene, slik at alle interessenters sikkerhetsbehov blir ivaretatt på en god måte. Samarbeid og partnerskap skal særlig vektlegges innenfor strategiens prioriterte områder som er nærmere omtalt i kapittel 3.

1 Digital sikkerhet handler om beskyttelse av «alt» som er sårbart fordi det er koblet til eller på annen måte avhengig av informasjons- og kommunikasjonsteknologi. Brukes synonymt med begrepene IKT-sikkerhet og cybersikkerhet.

1.3 Visjon

I Norge skal det være trygt å bruke digitale tjenester. Privatpersoner og virksomheter skal ha tillit til at den nasjonale sikkerheten, den enkeltes velferd og demokratiske rettigheter blir ivaretatt i et digitalisert samfunn.

1.4 Overordnede mål

Denne strategien legger vekt på at vi i fellesskap må utvikle tiltakene som kan styrke den digitale sikkerheten i samfunnet. Med bakgrunn i sikkerhetsutfordringene, legges følgende overordnede mål til grunn:

1. Norske virksomheter digitaliserer på en sikker og tillitvekkende måte, og har bedre evne til egenbeskyttelse mot uønskede digitale hendelser.

2. Kritiske samfunnsfunksjoner er understøttet av en robust og pålitelig digital infrastruktur.

3. Styrket digital sikkerhetskompetanse i tråd med samfunnets behov.

4. Samfunnet har en bedre evne til å avdekke og håndtere digitale angrep.

5. Politiet har styrket sin evne til å bekjempe data- og IKT-relatert kriminalitet.

2 Et styrket samarbeid

Det er flere sentrale myndighetsaktører med ansvar for digital sikkerhet (se vedlegg A). Det er viktig med et godt samarbeid mellom aktørene. Et sentralt samarbeid er Felles cyberkoordineringssenter (FCKS) som består av 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.

God digital sikkerhet er imidlertid ikke en målsetting myndighetene kan nå alene. Næringslivet har kompetansen og ressursene, og er en driver for digitalisering og innovasjon. Næringslivet er derfor en sentral del av løsningen. For å beskytte det digitale samfunnet må privatpersoner, virksomheter, sektorer og nasjoner se utover seg selv. Alle virksomheter har et ansvar for å ivareta sin egen digitale sikkerhet, men samfunnets digitale avhengighet gjør det nødvendig med et styrket samarbeid og partnerskap både internasjonalt og på tvers av samfunnet.

2.1 Offentlig-privat samarbeid

Utvikling av digitale tjenester og produkter foregår ofte i private virksomheter og i forsknings- og utviklingsmiljøer. En stor andel av landets kritiske digitale infrastrukturer eies og driftes av private virksomheter. Dette betyr at viktige beslutninger om utvikling og sikkerhet i det digitale rom i stor grad blir fattet av kommersielle og ikke-statlige aktører utenfor de tradisjonelle mellomstatlige arenaene. Dette gjør at myndigheters rolle i utviklingen av det digitale rom er begrenset og det fordrer et godt offentlig-privat samarbeid.

Offentlige og private virksomheter har ulike kapasiteter, kunnskaper og kompetanse som kan utfylle hverandre. Myndighetene har en viktig rolle som lovgiver, tilrettelegger og tilsynsmyndighet, og kan etterforske og påtale data- og IKT-relatert kriminalitet. Det er også myndighetenes rolle å samle innen- og utenlandsk etterretningsinformasjon, samarbeide med internasjonale organer og dele informasjon om potensielle trusler.

Økt samarbeid gir en bedre situasjonsforståelse, bedre beslutninger og økt tilgang på ressurser. For å møte sikkerhetsutfordringer som er i stadig endring bør samarbeidet intensiveres og videreutvikles.

Styrende prinsipper:

- Myndighetene og næringslivet skal samarbeide for å identifisere, utveksle erfaringer om og drøfte digitale sikkerhetsutfordringer.
- Samarbeidet skal være forpliktende for begge parter, og være basert på åpenhet, tillit og gjensidighet.
- Myndighetene skal bidra til et næringsliv hvor det etterspørres, utvikles og tilbys digitale sikkerhetstjenester.
- Ved oppbygging av nasjonal kapasitet for digital sikkerhet skal det legges til rette for inkludering av næringslivets kapasiteter.

2.2 Sivilt-militært samarbeid

Virksomhetene i forsvarssektoren er avhengig av infrastrukturer og digitale tjenester i sivil sektor. Dette innebærer at digitale sikkerhetsutfordringer i sivil sektor også har betydning for Norges evne til å håndtere sikkerhetspolitiske kriser og å gjennomføre militære operasjoner. I ytterste konsekvens betyr dette at digitale angrep mot sivil infrastruktur kan utfordre Norges evne til å ivareta nasjonal sikkerhet.

Totalforsvarskonseptet omfatter både militær støtte til det sivile samfunn og sivil støtte til Forsvaret. Forsvarets bidrag til samfunnssikkerheten gir også bedre evne til å ivareta statssikkerheten, fordi et fungerende sivilt samfunn og en robust samfunnssikkerhet er et viktig grunnlag for et fungerende militært forsvar. For å møte utfordringer med digitale sårbarheter må militære og sivile aktører samarbeide tettere. Dette innebærer å øve på håndtering av krisesituasjoner, felles kompetanseheving, gjensidig hendelsesvarsling og å dele informasjon om trusler og sårbarheter.

NATO setter i større grad enn tidligere sivilt beredskaps-arbeid og sivilt-militært samarbeid på dagsordenen. Sivil beredskap, krisehåndtering og robuste kritiske samfunnsfunksjoner er en forutsetning for det enkelte lands, og dermed alliansens, samlede beredskap og forsvar.

Styrende prinsipper:

- Sivil støtte til Forsvaret ved digitale sikkerhets-utfordringer i kriser og væpnet konflikt skal skje innenfor rammene av totalforsvaret.
- Virksomhetene i forsvarssektoren skal samarbeide med sivil sektor for å identifisere, utveksle erfaringer om og finne løsninger på digitale sikkerhetsutfordringer som kan ha betydning for evnen til å gjennomføre militære operasjoner.
- Virksomhetene i forsvarssektoren og i sivil sektor skal kunne dra nytte av hverandres kapasiteter for å håndtere felles digitale sikkerhetsutfordringer.
- Virksomhetene i forsvarssektoren skal dele informasjon og erfaringer med sivil sektor for å øke det nasjonale sikkerhetsnivået.

2.3 Internasjonalt samarbeid

Norges internasjonale cyberpolitikk skal tjene norske interesser, sikre gode og forutsigbare rammevilkår, og bidra til forebygging og beskyttelse mot utfordringer og trusler. Det styrende dokumentet for den internasjonale innsatsen er «Internasjonal Cyberstrategi for Norge», fremlagt av regjeringen i august 2017. Strategien fastslår at et bærekraftig globalt internett er avhengig av den riktige balansen mellom åpenhet, sikkerhet, robusthet og frihet.

Digitaliseringen har på kort tid endret det globale digitale landskapet. Digitale verdikjeder krysser landegrenser. Det etableres gjensidige avhengighetsforhold som utfordrer nasjonale myndigheters kontroll. Samtidig kan data- og IKT-relatert kriminalitet i form av digitale angrep fra både statlige og ikke-statlige aktører utgjøre svært alvorlige trusler mot nasjonal sikkerhet og økonomi. For å oppnå best mulig beskyttelse, håndteringsevne og kriminalitetsbekjempelse er det viktig med målrettet norsk deltagelse på internasjonale arenaer for å styrke digital sikkerhet globalt.

Styrende prinsipper:

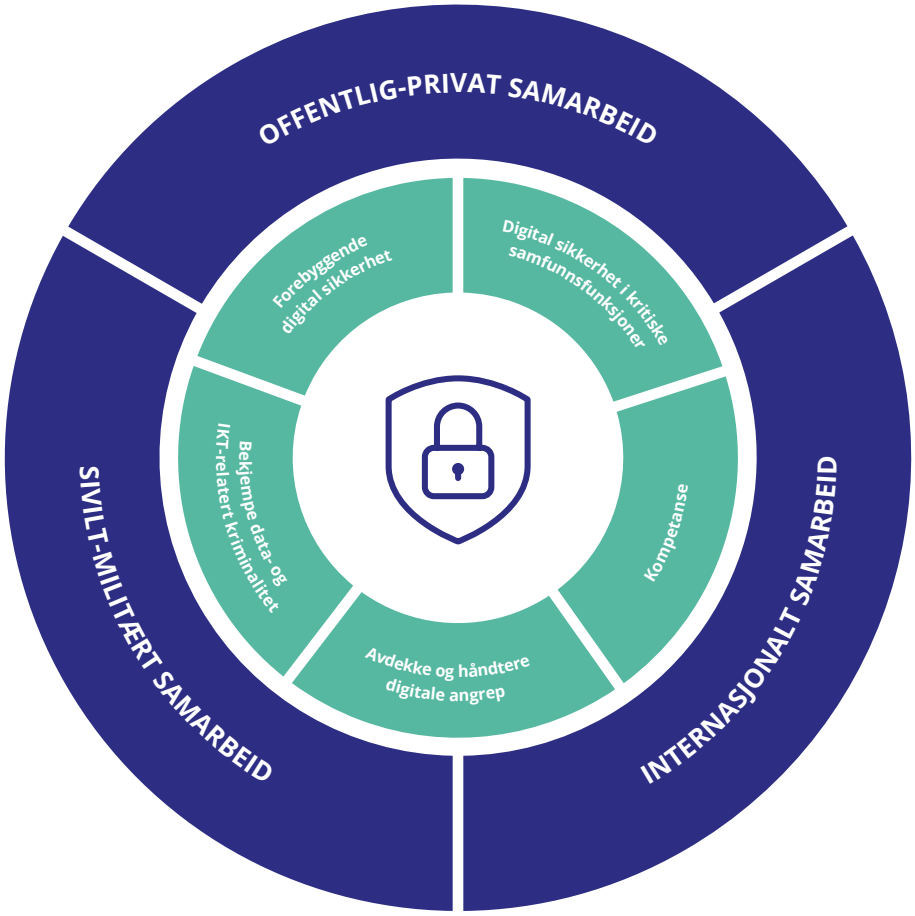
- Myndighetene vil samarbeide med andre nasjoner om å styrke vår evne til å forebygge, oppdage, varsle og håndtere digitale hendelser.
- Myndighetene vil fremme internasjonalt samarbeid om digital sikkerhet, enighet om statlig adferd i det digitale rom, og samarbeid om bekjempelse av data- og IKT-relatert kriminalitet, på internasjonale arenaer som FN, NATO, EU, OECD, OSSE. I tillegg skal det utvikles dialog med andre stater bilateralt og regionalt, herunder nordisk samarbeid.
- Myndighetene vil tilrettelegge for en aktiv norsk deltakelse på relevante internasjonale arenaer for å sikre internett som en åpen, tilgjengelig, sikker og robust plattform, basert på internasjonale standarder og samarbeid mellom myndigheter, næringsliv, akademia og andre deler av det sivile samfunn.
- Myndighetene vil tilrettelegge for tett koordinering mellom organer som representerer Norge på arenaer hvor internasjonal digital sikkerhetspolitikk og samarbeid om kriminalitetsbekjempelse og håndtering av IKT-hendelser utvikles.

3 Prioriterte områder

I et nasjonalt perspektiv er det viktig å sørge for en helhetlig tilnærming til sikkerhetsutfordringene, enten det gjelder tilsiktede (f.eks. digitale angrep) eller utilsiktede (f.eks. naturkatastrofer, tekniske feil eller uhell) digitale hendelser. Det er i samspillet mellom de forebyggende tiltakene, en robust digital infrastruktur, evnen til å håndtere digitale angrep, bekjempelsen av data- og IKT-relatert kriminalitet og tilstrekkelig digital sikkerhetskompetanse at vi oppnår en helhetlig beskyttelse mot digitale hendelser.

Digitaliseringen av samfunnet øker betydningen av digital sikkerhet. God digital sikkerhet er en særlig viktig forutsetning for å opprettholde tilliten til offentlig sektors IKT-systemer, og offentlige digitale tjenester. En digital offentlig sektor bidrar til mer effektivitet, innovasjon og økonomisk vekst i samfunnet.

Denne strategien understøttes av en to-delt tiltaksoversikt. Del 1 beskriver myndighetenes utvalgte sentrale tiltak for de prioriterte områdene som følger av dette kapittelet. Del 2 beskriver ti grunnleggende tiltak for å øke virksomheters egenevne til å beskytte seg mot og håndtere digitale hendelser.



3.1 Forebyggende digital sikkerhet

Overordnet mål:
Norske virksomheter digitaliserer på en sikker og tillitvekkende måte, og har bedre evne til egenbeskyttelse mot uønskede digitale hendelser.

Å ivareta digital sikkerhet er først og fremst et virksomhetsansvar. Virksomhetsledere er ansvarlig for å foreta risikovurderinger, og på bakgrunn av dette gjennomføre tilstrekkelige tiltak. Myndighetene skal legge til rette for at virksomheter kan beskytte seg mot uønskede digitale hendelser, både for å ivareta egen sikkerhet og for å øke samfunnets samlede robusthet. Et godt forebyggende arbeid med digital sikkerhet, og en systematisk tilnærming til håndtering av risiko, vil redusere muligheten for at uønskede digitale hendelser får konsekvenser for egen og andres virksomhet, for den enkelte privatperson og for samfunnet i stort. Prioriterte råd og anbefalinger setter virksomheter og privatpersoner i bedre stand til å finne de riktige tiltakene som hever sikkerhetsnivået i samfunnet. Del 2 i tiltaksoversikten er derfor et viktig virkemiddel for å øke virksomheters egenevne til å beskytte seg mot og håndtere digitale hendelser.

Forebyggende digital sikkerhet i samfunnet innebærer at digitale tjenester og produkter er sikre og pålitelige fra starten, og i hele tjenestens eller produktets levetid.

Delmål:

1. Virksomheter har en risikobasert tilnærming mot uønskede digitale hendelser, og bruker anerkjente rammeverk, standarder og styringssystemer for digital sikkerhet.

2. Offentlig sektor har god styring og kontroll på sin digitale sikkerhet. Virksomhetenes styringssystem for digital sikkerhet understøtter virksomhetenes hovedfunksjon, og bidrar til at sikkerhetshendelser i en offentlig virksomhet ikke medfører alvorlig skade hos andre.

3. Privatpersoner, næringslivet og forvaltningen har tillit til at offentlige digitale tjenester er sikre og pålitelige.

4. Myndigheter og virksomheter deler informasjon om trusler, sårbarheter, hendelser og effektive tiltak med relevante aktører for å øke samfunnets robusthet mot uønskede digitale hendelser.

5. Myndighetene gir råd, anbefalinger og veiledninger om digital sikkerhet for å gi virksomhetene et kunnskapsgrunnlag for sitt sikkerhetsarbeid.

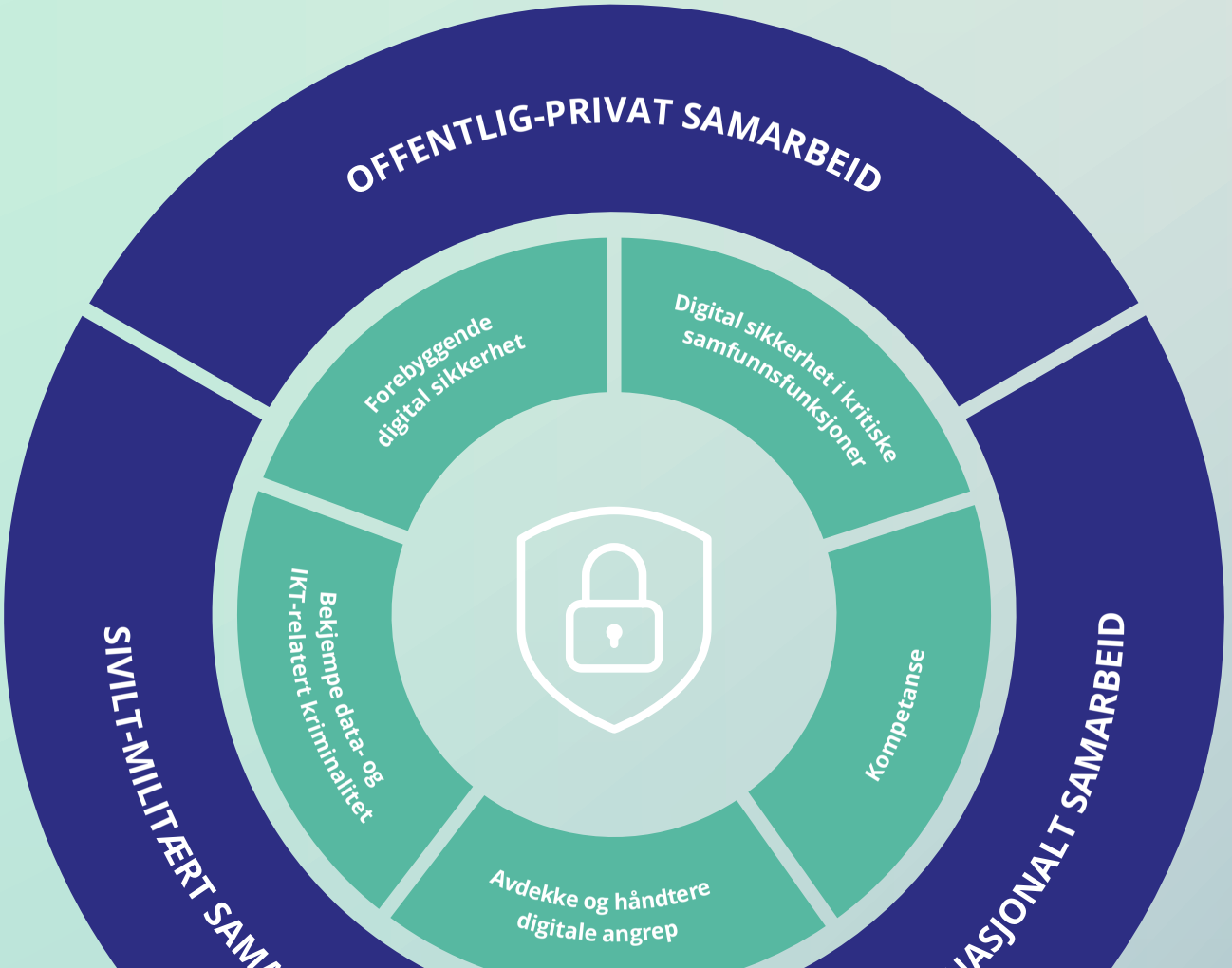
6. Myndighetene er pådriver for digital sikkerhet i digitale forbrukertjenester og produkter.

7. Myndighetene legger til rette for samarbeid i offentlig sektor og mellom offentlig og privat sektor.

8. Befolkningen har en god digital dømmekraft og god sikkerhetskultur.

Bakside av plakat – riv ut og heng opp

Nasjonal strategi for digital sikkerhet



START-TIPS	✕ ✓
Etabler tilstrekkelig systematikk for sikkerhetsstyring, og sørg for at en fagperson støtter ledelsen i arbeidet.	
Inkluder digital sikkerhet i virksomhetens risikoarbeid. Etabler tydelig ansvar i virksomheten, og effektive rapporteringslinjer til toppledelse og styre.	
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.	
Kartlegg virksomhetens sikkerhetskultur og identifiser hva som kan forbedres. Fastsett ønsket kultur og gjennomfør tilpasset, årlige treningsprogram for å fremme god sikkerhetskultur.	
Sats på god bestillerkompetanse og gjør en risikovurdering som forankres hos ledelsen.	

START-TIPS	✕ ✓
Oppgrader program- og maskinvare. Fjern unødvendig kompleksitet og ubrukt funksjonalitet. Blokker kjøring av ikke-autoriserte programmer.	
Installer sikkerhetsoppdateringer så raskt som mulig. Beskytt trådløse nettverk med sterke sikkerhetsmekanismer. Planlegg og dokumenter endringer. Slå på logging og gjennomgå viktige logger jevnlig.	
Bruk kun siste versjon av nettlesere. Beskytt e-post med DMARC. Krypter viktig informasjon når den lagres på bærbare medier og når det sendes over nettet.	
Endre standard passord og ikke tildel sluttbrukere administratorrettigheter. Bruk 2-faktorautentisering, eller som et minimum, sterke passord.	
Etabler en beredskapsplan for ulike typer hendelser og gjennomfør øvelser som tester planverket.	

Se tiltaksoversiktens del 2 for utfyllende informasjon.

Bakside av plakat – riv ut og heng opp

3.2 Digital sikkerhet i kritiske samfunnsfunksjoner

Overordnet mål:
Kritiske samfunnsfunksjoner er understøttet av en robust og pålitelig digital infrastruktur.

Samfunnet er avhengig av at kritiske samfunnsfunksjoner opprettholdes, og det forutsettes at de digitale infrastrukturene som understøtter dem virker overalt og hele tiden.[2] Gjensidige avhengigheter på tvers av ulike digitale infrastrukturer representerer en særlig utfordring. Særlig gjelder dette strømnett og elektroniske kommunikasjonsnett som er grunnleggende kritisk infrastruktur for de fleste digitale infrastrukturer. En hendelse kan oppstå i én digital infrastruktur, og ha konsekvenser i en annen. En virksomhet bør derfor vite hvilke tjenester de selv er avhengig av og hvilke potensielle konsekvenser hendelser i egen digital infrastruktur kan ha for andre.

Delmål:

1. Myndighetene sørger for at det finnes rammeverk og metoder for å identifisere kritisk digital infrastruktur, og skal veilede og sørge for at kritisk digitale infrastrukturer identifiseres.

2. Offentlige og private virksomheter som eier kritisk digital infrastruktur gjennomfører risikovurderinger for å identifisere sårbarheter og gjensidige avhengigheter mellom infrastrukturer for å sikre en helhetlig sikring av digitale verdikjeder.

3. Myndighetene har oversikt over nasjonal kritisk digital infrastruktur.

4. Myndighetene stiller krav til sikkerhet i kritisk digital infrastruktur, veileder og fører tilsyn med at sikkerheten er forsvarlig. Offentlige og private virksomheter som eier kritisk digital infrastruktur gjennomfører tiltak som sørger for forsvarlig sikkerhet i disse.

5. Offentlige og private virksomheter deltar i beredskapsøvelser knyttet til kritisk digital infrastruktur.

2 Denne strategien omfatter også kritiske samfunnsfunksjoner utover det som omfattes av sikkerhetsloven. Dette kan være funksjoner som dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse (som bank- og finanstjenester og helse- og omsorgstjenester). Se DSBs rapport «Samfunnets kritiske funksjoner» for oversikt over disse.

3.3 Kompetanse

Overordnet mål:
Styrket digital sikkerhetskompetanse i tråd med samfunnets behov.

Kompetanse og kunnskap om trusler, sårbarheter og effektive tiltak er en forutsetning for å kunne beskytte verdier mot uønskede digitale hendelser. Dette forutsetter at alle – både privatpersoner, virksomheter og myndigheter, har tilgang til informasjon om digitale sikkerhetsutfordringer og mottiltak. Spesialisering i digital sikkerhet som kreves for å ivareta vårt nasjonale sikkerhetsbehov skal gis særlig prioritet.

Nasjonal strategi for digital sikkerhetskompetanse (2019) utdyper kompetansemålene i denne strategien og skal legge til rette for en langsiktig oppbygging av kompetanse, herunder den nasjonale kapasiteten innenfor forskning, utvikling, utdanning og bevisstgjøringstiltak rettet mot befolkningen og virksomheter.

Delmål:

1. Sørge for attraktive og kompetente forskningsmiljøer som tiltrekker seg gode forskere og doktorgradskandidater.

2. Antallet spesialister innenfor digital sikkerhet dekker behovet i arbeidslivet og ivaretar hensynet til rikets sikkerhet.

3. Digital sikkerhetskompetanse skal være tilstrekkelig inkludert i utdanninger der IKT har en sentral plass, inkludert IKT- og teknologiutdanninger. Utover det bør utdanninger på andre fagområder, men med betydelige innslag av IKT, også inkludere digital sikkerhet i relevant omfang.

4. God etter- og videreutdanning innenfor IKT og digital sikkerhet på fagskoler, universiteter og høyskoler.

5. Digital sikkerhet inngår i relevante yrkesutdanninger og profesjonsutdanninger i tilstrekkelig grad.

6. Elever og lærlinger skal ha digital kompetanse, inkludert digitale ferdigheter i og kunnskap om trygg bruk og sikkerhet, som gjør dem i stand til å oppleve livsmestring og lykkes i videre utdanning, arbeid og samfunnsdeltakelse.

7. Privatpersoner har kunnskap og ferdigheter som gir dem god digital dømmekraft og som bidrar til å beskytte deres personvern og verdier på nett.

3.4 Avdekke og håndtere digitale angrep

Overordnet mål:
Samfunnet har en bedre evne til å avdekke og håndtere digitale angrep.

Digitale angrep kan utgjøre en trussel mot nasjonale kritiske funksjoner, samfunnssikkerheten generelt og norsk suverenitet. Evne til å motstå digitale angrep for å sikre egen handlefrihet vil derfor være viktige elementer i et lands forsvar. Trusselaktørene kan være andre stater, ikke-statlige grupperinger eller private rettssubjekter. Målet med angrepene spenner vidt, fra vinningskriminalitet til statlig spionasje, sabotasje og hybride operasjoner. Digitale angrep kan forstyrre, påvirke og hindre nasjonale beslutningsprosesser.

Bruk av digitale virkemidler har i økende grad blitt en integrert del av militære operasjoner. Et digitalt angrep kan, avhengig av omstendigheter som angrepets formål og legitimitet, styrke og konsekvenser, anses å utgjøre et «væpnet angrep» som utløser en stats rett til selvforsvar, (jf. FN-paktens artikkel 51).

Ansvarsprinsippet ligger til grunn for arbeidet med digital sikkerhet. Det innebærer at virksomheter som har ansvaret i en normalsituasjon, også har ansvaret for nødvendige beredskapsforberedelser og for å håndtere ekstraordinære hendelser. Myndighetene vil styrke den nasjonale beredskapen og evnen til å avdekke og håndtere digitale angrep. Dette forutsetter at roller og ansvar er avklart og at relevante aktører har god situasjons- og konsekvensforståelse. Det må være tilstrekkelig koordinering, samarbeid og deling av informasjon mellom sentrale aktører som har ansvar for å avdekke og håndtere alvorlige digitale angrep. Se pkt. 3.5 særskilt om politiets arbeid.

Delmål:

1. Norske virksomheter tar ansvar for å håndtere digitale angrep i egen virksomhet, og for å dele informasjon om disse til myndighetene og andre relevante aktører.

2. Myndighetene videreutvikler rammeverk som definerer roller, ansvar og organisering for håndtering av alvorlige digitale angrep.

3. Myndighetene har bedre kapasitet til å bistå og koordinere håndtering av digitale angrep.

4. Myndighetene legger til rette for informasjonsdeling og erfaringsoverføring mellom relevante aktører i samfunnet for å avdekke og håndtere alvorlige digitale angrep.

5. Myndighetene videreutvikler det internasjonale samarbeidet for å styrke den nasjonale evne til å forebygge, avdekke, varsle, attribuere og håndtere alvorlige digitale angrep.[3]

6. Myndighetene legger til rette for at det gjennomføres nasjonale øvelser og at Norge deltar i øvelser internasjonalt.

3 Med attribuere menes identifisering av aktør(er) som står bak et digitalt angrep.

3.5 Bekjempe data- og IKT-relatert kriminalitet

Overordnet mål:
Politiet har styrket sin evne til å bekjempe data- og IKT-relatert kriminalitet.

Politiet skal beskytte samfunnet og forebygge, avdekke, etterforske og straffeforfølge kriminalitet. Denne oppgaven er den samme i det digitale som i det fysiske rom. I en situasjon hvor bruk av ny teknologi utvikles raskt, er det utfordrende for politiet å bekjempe data- og IKT-relatert kriminalitet.[4] Trusselbildet krever at kunnskapsgrunnlaget for bekjempelse av kriminaliteten utvides og stiller nye krav til moderne IKT-utstyr og teknologisk kompetanse i politiet. Videre blir det større behov for samarbeid mellom politiet og andre aktører.

Det er viktig at befolkningen har tillit til at alle typer kriminalitet bekjempes effektivt og godt. Myndighetene vil styrke politiets forutsetninger for å utføre sine oppgaver i takt med den teknologiske utviklingen, og utviklingen i kriminaliteten.

Delmål:

1. Politiets kompetanse og kapasitet til å bekjempe data- og IKT-relatert kriminalitet er styrket.

2. Samfunnet har tillit til at politiet kan bekjempe data- og IKT-relatert kriminalitet.

4 Politiet skiller mellom datakriminalitet (kriminalitet rettet mot teknologi og datasystemer) og IKT-relatert kriminalitet (kriminelle handlinger som inkluderer bruk av IKT-verktøy, IKT-tjenester eller gjennomføres i det digitale rom).

Vedlegg A: Utvalgte aktører og kontaktpunkt

Å ivareta digital sikkerhet er først og fremst et virksomhetsansvar. Virksomhetsledere er ansvarlig for å foreta risikovurderinger, og på bakgrunn av dette gjennomføre tilstrekkelige tiltak. I tillegg har hver enkelt statsråd et overordnet ansvar for å ivareta digital sikkerhet i egen sektor. Under følger en oversikt over utvalgte sentrale aktører med tverrsektorielt ansvar.

JUSTIS- OG BEREDSKAPS-DEPARTEMENTET (JD)	FORSVARS-DEPARTEMENTET (FD)	KOMMUNAL- OG MODERNISERINGS-DEPARTEMENTET (KMD)	UTENRIKS-DEPARTEMENTET (UD)
Samordningsansvar for digital sikkerhet i sivil sektor, og et generelt samordningsansvar for samfunnets sivile sikkerhet. Forvaltningsansvar for Lov om nasjonal sikkerhet (sikkerhetsloven).	Ansvar for digital sikkerhet i forsvarssektoren.	Særskilt ansvar for å arbeide for en styrket og mer helhetlig tilnærming til digital sikkerhet i statsforvaltningen. KMD har i tillegg et samordningsansvar for regjeringens IKT-politikk og ansvar for digital sikkerhet knyttet til elektroniske kommunikasjonsnett og -tjenester, herunder internett.	Ansvar for norsk utenriks- og sikkerhetspolitikk, herunder å koordinere Norges innsats og posisjoner på internasjonale arenaer hvor globale utfordringer i det digitale rom diskuteres.

Nasjonal sikkerhetsmyndighet (NSM) er det nasjonale fagmiljøet for digital sikkerhet, og er nasjonal varslings- og koordineringsinstans for alvorlige dataangrep mot samfunnskritisk infrastruktur og andre viktige samfunnsfunksjoner. NSM driver den nasjonale responsfunksjonen for alvorlige dataangrep mot kritisk infrastruktur (NorCERT) og nasjonalt varslingssystem for digital infrastruktur (VDI). NSM leder også arbeidet i Felles cyberkoordineringssenter (FCKS). Det er nylig besluttet å etablere et nasjonalt cybersikkerhetssenter med utgangspunkt i NSM.

www.nsm.stat.no

Politidirektoratet (POD) har ansvaret for faglig ledelse, styring, oppfølging, og utvikling av politidistriktene og særorganene i politiet. Det er nylig besluttet etablering av et nasjonalt cyberkrimsenter (NC3) hos Kripos for å utvikle politiets kapasitet og kompetanse for å møte et mer digitalisert kriminalitets- og trusselbilde. Etableringen startes i 2018 og skal være ferdig innen utgangen av 2021. NC3s hovedoppgaver blir å bekjempe kriminalitet gjennom etterforskning, bevissikring, metodeutvikling og bistand til øvrige deler av politiet.

www.politiet.no

Politiets sikkerhetstjeneste (PST) har ansvar for nasjonens indre sikkerhet. PST forebygger og etterforsker lovbrudd som kan true nasjonens sikkerhet, gjennom blant annet innsamling av informasjon om personer og grupper som kan utgjøre en trussel, utarbeidelse av ulike analyser og trusselvurderinger, etterforskning og andre operative mottiltak og rådgivning.

www.pst.politiet.no

Etterretningstjenesten (E-tjenesten) er ansvarlig for å kartlegge utenlandske trusselaktører, deres motiver, kapasiteter og metoder. Formålet med etterretningsvirksomheten er å bidra til å gi norske myndigheter et solid beslutningsgrunnlag i saker som gjelder utenriks-, sikkerhets- og forsvarspolitikk.

www.forsvaret.no/organisasjon/etterretningstjenesten

Nasjonal kommunikasjonsmyndighet (Nkom) har et særskilt ansvar knyttet til sikkerhet og beredskap i elektroniske kommunikasjonsnett og -tjenester.

www.nkom.no

Direktoratet for forvaltning og IKT (Difi) er statens kompetansemiljø for informasjonssikkerhet og jobber for en styrket og mer helhetlig tilnærming til informasjonssikkerhet i statsforvaltningen gjennom å gi råd, veiledning og anbefalinger til virksomhetene.

www.difi.no

Datatilsynet er både tilsyn og ombud. Datatilsynet er et uavhengig forvaltningsorgan som har i oppgave å føre kontroll med personvernregelverket og medvirke til at enkeltpersoner ikke blir krenket gjennom bruk av opplysninger som kan knyttes til dem.

www.datatilsynet.no

Direktoratet for samfunnssikkerhet og beredskap (DSB) skal ha oversikt over risiko og sårbarhet i samfunnet og være pådriver i arbeidet med å forebygge ulykker, kriser og andre uønskede hendelser, samt sørge for god beredskap og effektiv ulykkes- og krisehåndtering.

www.dsb.no

Norsk senter for informasjonssikring (NorSIS) er en uavhengig organisasjon som arbeider for økt kunnskap om og forståelse for digital sikkerhet ved å blant annet gi råd og veiledning til privatpersoner og virksomheter (særlig SMB-virksomheter). NorSIS har redaktøransvaret for tjenestene slettmeg.no og nettvett.no. Slettmeg.no er en gratis råd- og veiledningstjeneste for de som føler seg krenket på nett, mens nettvett.no tilbyr informasjon, råd og veiledning om sikrere bruk av Internett.

www.norsis.no
www.slettmeg.no
www.nettvett.no

Vedlegg B: Relevante politiske og strategiske dokumenter

Denne strategien inngår i en større sammenheng av politiske og strategiske dokumenter som gir føringer for det nasjonale arbeidet med digital sikkerhet, blant annet:

DOKUMENT	
Meld. St. 38 (2016-2017) IKT-sikkerhet, et felles ansvar	Den første stortingsmeldingen utelukkende om digital sikkerhet.
Meld. St. 10 (2016-2017) Risiko i et trygt samfunn	Stortingsmelding om samfunnssikkerhet hvor digital sikkerhet inngår.
Meld. St. 27 (2015-2016) Digital agenda for Norge	Stortingsmelding om regjeringens digitaliseringspolitikk hvor personvern og digital sikkerhet er sentrale elementer.
Prop. 151 S (2015-2016) Kampkraft og bærekraft	Langtidsplan for prioriteringer i forsvarssektoren, herunder også digital sikkerhet.
Prop. 153 L (2016-2017) Lov om nasjonal sikkerhet	Ny sikkerhetslov som skal bidra til å trygge våre overordnede nasjonale sikkerhetsinteresser.
Instruks for departementenes arbeid med samfunnssikkerhet	Samfunnssikkerhetsinstruksen skal styrke samfunnets evne til å forebygge kriser og til å håndtere alvorlige hendelser. Digital sikkerhet er en integrert del av arbeidet med samfunnssikkerheten.
Internasjonal cyberstrategi for Norge	Strategi utgitt i 2017 som gir føringer for arbeidet med internasjonal cyberpolitikk, hvor digital sikkerhet er et av flere prioriterte områder.
Prop. 56 LS (2017-2018) Lov om behandling av personopplysninger	Ny personopplysningslov som gjennomfører EUs personvernforordning (GDPR).
Helhetlig IKT-risikobilde	Årlig rapport som skal bidra til å øke bevisstheten om og motivere til økt digital sikkerhet i norske virksomheter og i samfunnet i stort.

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-0444 B
Design og layout: Konsis Grafisk
Trykk: Departementenes sikkerhets- og serviceorganisasjon
05/2019 – opplag 500