Departementene

Strategi

Nasjonal strategi for digital sikkerhetskompetanse

Nasjonal strategi for digital sikkerhetskompetanse

Samarbeid og målrettet innsats
– nøkkelen til digital sikkerhetskompetanse

Forord

Digital sikkerhetskompetanse er en viktig forutsetning for at Norge skal lykkes med digitalisering. Dette er av betydning for vekst, velferd og kunnskapsutvikling. Kompetanse i digital sikkerhet bidrar til tryggere digitale løsninger og at personvernet til den enkelte blir ivaretatt.

Justis- og beredskapsdepartementet har i samarbeid med Kunnskapsdepartementet utarbeidet en nasjonal strategi for digital sikkerhetskompetanse som grunnlag for å utvikle kompetanse i tråd med samfunnets, arbeidslivets og den enkeltes behov.

Digital sikkerhetskompetanse er en knapp ressurs nasjonalt og internasjonalt. Strategien følger opp regjeringens ønsker om å styrke den nasjonale kompetansen innenfor forskning og utdanning samt bevisstgjøringstiltak rettet mot befolkningen og virksomheter. En forutsetning for trygg bruk av IKT er tilstrekkelig digital sikkerhetskompetanse på alle samfunnsnivåer, fra vanlige brukere til yrkesutøvere og spesialister innenfor utvalgte og særlig kritiske områder.

Denne kompetansestrategien er en utdypning og komplettering av Nasjonal strategi for digital sikkerhet hvor kompetanse er et av fem prioriterte områder. Strategien er et ledd i prosessen med å styrke den digitale sikkerhetskompetansen. Tiltakene vil igangsettes og/eller videreutvikles innenfor en fireårsperiode.

Vi har prioritert å øke antallet spesialister og å styrke forskningen. Vi vil spesielt vise til kompetansemiljøene innenfor forskning og høyere utdanning som aktivt har tatt utfordringen med utvikling av kompetanse og kunnskap innen feltet digital sikkerhet.

Vi lever i et samfunn der det digitale brer om seg i privatliv, utdanning og arbeidsliv. Digitale ferdigheter har blitt grunnleggende på linje med lesing, skriving, regning og muntlige ferdigheter. Ikke uten grunn peker Stortingsmeldingen om *IKT-sikkerhet – et felles ansvar* på at vi må starte tidlig, vi må starte allerede i grunnskolen. Ved å starte tidlig kan vi bygge en kultur for digital sikkerhet som omfatter alle.

Alle må ha tilstrekkelig kunnskap om digital sikkerhet, enkeltindivider som institusjoner. Vi oppfordrer derfor alle, offentlige og private institusjoner, til å ta denne strategien i bruk.

Vi takker for alle gode og konstruktive innspill vi har fått i arbeidet med denne strategien fra både private og offentlige aktører.

Oslo, 30. Januar 2019

Ingvil Smines Tybring-Gjedde

Samfunnssikkerhetsminister

Iselin Nybø

Forsknings- og høyere utdanningsminister

Innhold

1 Innledning

I Stortingsmelding 10 (2016-2017) *Risiko i et trygt samfunn* og Stortingsmelding 38 (2016-2017) *IKT-sikkerhet – et felles ansvar*, ligger det politiske grunnlaget for tiltak for økt kompetanse på digital sikkerhet[1], og for en kompetansestrategi som legger til rette for langsiktig oppbygging av kompetanse.

Justis- og beredskapsdepartementet (JD) har samordningsansvar for regjeringens politikk for digital sikkerhet i sivil sektor. Dette innebærer også et overordnet nasjonalt ansvar for at kompetansebygging innenfor digital sikkerhet møter fremtidens behov.

Kunnskapsdepartementet (KD) har det overordnede ansvaret for norsk utdannings- og forskningspolitikk. Stortingsmelding 4 (2018-2019) *Langtidsplan for forskning og høyere utdanning* 2019-2028 legger grunnlaget for fremtidig prioritering og ressursinnsats innenfor høyere utdanning og forskning. Læreplanverket styrer innholdet i grunnopplæringen (grunnskole og videregående opplæring).

Det enkelte departement har et overordnet ansvar for digital sikkerhet innenfor sin sektor. I dette inngår også et ansvar for å tilrettelegge for at man i egen sektor/egen virksomhet har adekvat kompetanse.

Nasjonal strategi for digital sikkerhetskompetanse retter seg både mot myndigheter og offentlige og private virksomheter. Utdanningssektoren og forskningsinstitusjoner har betydelige oppgaver på dette området. Tiltakene som presenteres i kompetansestrategien er i hovedsak tiltak i regi av myndighetene. Flere av tiltakene er allerede under arbeid. Regjeringen forutsetter at utdanningssektoren, forskningsinstitusjonene og private virksomheter følger opp med egne prioriteringer som støtter opp om strategien. Det er gjennom en felles innsats vi kan nå det

[1] Begrepet digital sikkerhet handler om beskyttelse av «alt» som er sårbart fordi det er koblet til eller på annen måte avhengig av informasjons- og kommunikasjonsteknologi.

overordnede målet om *styrket digital sikkerhetskompetanse i tråd med samfunnets behov.*

En nasjonal strategi for digital sikkerhet er ferdigstilt parallelt med denne kompetansestrategien. Her inngår kompetanse som et av fem prioriterte områder. Kompetansestrategien er en videre utdyping av de mål som følger av den nasjonale strategien for digital sikkerhet. Det fremheves her at digitale sikkerhetsutfordringer skal håndteres gjennom samarbeid og partnerskap mellom relevante aktører, både nasjonalt og internasjonalt.

2 Utfordringer

Lysneutvalgets utredning (NOU 2015: 13) *Digital sårbarhet – sikkert samfunn* belyser utfordringene for digital sikkerhetskompetanse både i utdanning og forskning. Utvalget påpekte at forskningsmiljøene er små og fragmenterte, at det er en generell mangel på kunnskap om de økonomiske tapene som følger av digital sårbarhet og hva forebyggende sikkerhet koster. Videre var utvalget opptatt av at det er en langsiktig prosess å bygge opp og vedlikeholde kompetanse- og forskningsmiljøer. Blant utvalgets forslag var å styrke nasjonal forskningskompetanse i kryptologi og opprette øremerkede stillinger til stipendiater som kan sikkerhetsklareres.

Undersøkelser fra Nasjonal sikkerhetsmyndighet (NSM) viser at mange virksomheter har betydelige forbedringsbehov knyttet til sikkerhetsbevissthet og sikkerhetskompetanse. Arbeidet med sikkerhet blir ikke prioritert som del av den totale styringen av virksomheten. Ledelsen vet heller ikke hvilken risiko de tar på vegne av virksomheten (NSM 2017[2]). En internasjonal undersøkelse (2016 og 2018[3]) i regi av KPMG, og utdyping ved samtaler med norske toppledere, viser et tilsvarende bilde. Norske toppledere[4] synes det er krevende å overvåke risikolandskapet. Undersøkelsen viser kompetanseutfordringer, spesielt når det kommer til kombinasjonen mellom teknologiinnsikt, erfaring fra ledelse og risikohåndtering.

Undersøkelser[5] som Norsk senter for informasjonssikring (NorSIS) gjennomførte i 2016, 2017 og 2018 om digital sikkerhetskultur, viser lav forståelse for netthygiene i befolkningen, dvs. konsekvenser av egen adferd på nett og betydningen av sikring av maskinvare. NorSIS har også publisert en rapport om ungdom og digital

2 Nasjonal sikkerhetsmyndighet 2017: *Helhetlig IKT-risikobilde 2017*.
3 KPMG: Global CEO Outlook 2018.
4 KPMG: Vilje til endring – samtaler med norske toppledere. Topplederundersøkelsen 2016 og 2018.
5 Malmedal, Bjarte og Røislien, Hanne Eggen (2016): The Norwegian Cyber Security culture. NorSIS, Norsk senter for informasjonssikring.

sikkerhetskultur i 2017[6]. En konklusjon er at opplæringen som gis ungdom om digital sikkerhet er for lite strukturert og tydelig, både i form og innhold. Ungdom lærer i større grad enn andre aldersgrupper gjennom prøving og feiling, og langt færre lærer på kurs eller utdanning.

På oppdrag fra JD har NIFU[7] utarbeidet rapporten *IKT-sikkerhetskompetanse i arbeidslivet – behov og tilbud* (Mark m.fl. 2017). Her anslås at det i 2030 vil mangle 4.100 personer med digital sikkerhetskompetanse sett i forhold til behovet. Modellen for beregning av tilbud bygger på tidsserier som ikke tar med de seneste årene med økning i studenter. På den annen side vil framskrivning av etterspørselssiden også undervurdere fremtidens behov. Forskerne fremhever at det er vanskelig å anslå behovet presist, selv i dag. Selv om tallet er usikkert, peker rapporten, basert på ulike datakilder, på et fremtidig kompetansegap og tegner et bilde av økende utfordringer. Rapporten trekker også frem en potensiell mangel på undervisningsressurser i digital sikkerhet i universitets- og høyskolesektoren pga. en økning i antall studenter.

6 Malmedal, Bjarte og Røislien, Hanne Eggen (2017): Ungdom og digital sikkerhetskultur. NorSIS Norsk senter for informasjonssikring.

7 Mark, Michael Spjelkavik, C. Tømte, T. Næss og T Røsdal (2017): IKT-sik kerhetskompetanse i arbeidslivet – behov og tilbud. Rapport 2017:32, Nordisk Institutt for studier av innovasjon, forskning og utdanning (NIFU).

3 Satsingsområder

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

Utfordringsbildet tilsier et bredt perspektiv på læring og kompetanse for å nå kompetansestrategiens overordnede mål. Tiltak må omfatte både teknisk kompetanse og kompetanse knyttet til organisering, ledelse og trygg bruk. Strategien må videre dekke hele bredden, fra forskning og ekspertkompetanse til bygging av god sikkerhetskultur i befolkningen.

På denne bakgrunn er strategiens satsingsområder:
- Langsiktig forskning av god kvalitet
- Tilstrekkelig nasjonal spesialistkompetanse
- Digital sikkerhet som del av IKT-relaterte utdanninger og tilgrensende fag
- Etter- og videreutdanning (EVU) innenfor IKT og digital sikkerhet
- Digital sikkerhet i yrkes- og profesjonsutdanninger
- God grunnkompetanse
- Bevisstgjørende tiltak og bedret digital sikkerhetskultur

På et overordnet nivå har KD ansvar for å styre og følge opp underliggende institusjoner og virksomheter innenfor de rammer som er trukket opp av Stortinget. Universitets- og høgskoleloven har også bestemmelser til vern om akademisk frihet og ansvar, for å sikre akademiske verdier og institusjonenes og den enkelte vitenskapelig ansattes faglige uavhengighet. Selv om institusjonene er faglig uavhengige og selv fastsetter sine studieplaner og det faglige innholdet i utdanningene, er det etablert sentrale rammeplaner for en rekke profesjonsutdanninger.

Tiltakene som presenteres i kompetansestrategien er i hovedsak tiltak i regi av offentlig sektor. Regjeringen forventer at utdanningssektoren, forskningsinstitusjoner og private virksomheter også framover følger opp med egne prioriteringer. Relevante personvernemaer må inngå i fremtidige kompetansetiltak innenfor digital sikkerhet.

HOVEDTILTAK FOR Å STYRKE KOMPETANSEN INNENFOR DIGITAL SIKKERHET

Regjeringen har prioritert å styrke kompetansen på digital sikkerhet og myndighetene har alt startet arbeidet med flere relevante kompetansetiltak innenfor utdanning, inkludert etter- og videreutdanning, forskning og bevisstgjøring rettet mot befolkningen. Dette er tiltak som gradvis vil bidra til betydelig økt kompetanse innenfor digital sikkerhet.

I regi av KD og utdanningssystemet pågår prosesser som er viktige for å styrke den digitale kompetansen framover. Det pekes spesielt på følgende:

- *Langtidsplan for forskning og høyere utdanning (2019-2028).* I den reviderte planen lanserer regjeringen en opptrappingsplan på 800 mill. kroner over fire år til utdanning og forskning innenfor teknologi, herunder IKT og digital sikkerhet. Oppfølging av Langtidsplanen innebærer fra 2019 minst 57 mill. kroner årlig til forskning om digital sikkerhet, inkludert styrket forskning i kryptologi.

- *IKTPLUSS* er Forskningsrådets store satsing på IKT-forskning og innovasjon. I regi av NFRs IKTPLUSS er det bevilget til sammen minimum 350 mill. kroner ved utlysninger i 2015 og 2018 til «Et trygt informasjonssamfunn».

– *Stortingets bevilgninger i statsbudsjettene til nye studieplasser og rekrutteringsstillinger (stipendiater) innenfor IKT og digital sikkerhet 2016-2018.* Satsingen innebærer til sammen et varig økt årlig opptak av 1500 studenter. Regjeringen har i 2017 og 2018 øremerket totalt 62 rekrutteringsstillinger til digital sikkerhet, inkludert kryptologi.

– *Ny kompetansereform – Lære hele livet.* Det skal legges til rette for å ta utdanning og være i jobb samtidig, og etter- og videreutdanningstilbudet må møte arbeidslivets behov for relevant og fleksibel utdanning. Det legges opp til kontinuerlig oppdatering av kompetanse, blant annet som følge av digitalisering. I RNB (Revidert nasjonalbudsjett) i 2018 ble det bevilget 10 mill. kroner til utvikling av fleksible videreutdanningstilbud i digital kompetanse. I statsbudsjettet for 2019 ble det bevilget 37 mill. koner til dette tiltaket.

– *Fagfornyelsen og arbeidet med nye læreplaner i grunnskole og videregående skole.* Samfunnsfag får særskilt ansvar for grunnleggende digitale ferdigheter, mens programmering kommer inn i flere fag. I den teknologiske skolesekken inngår bl.a. 48 mill. kroner i støtte til skoleeiere til innkjøp av digitale læremidler fra 2019.

Langsiktig forskning av god kvalitet

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

For å styrke kjernemiljøene innenfor digital sikkerhet er det behov for å bygge forskningskapasitet og -kvalitet. Ved å styrke kjernemiljøene legger man et bedre grunnlag for deltagelse i nasjonalt og internasjonalt forskningssamarbeid, herunder å styrke nasjonale program som samspiller med EU-forskningen (Horisont 2020).

Et viktig delmål for Norges forskningsråds programmer IKTPLUSS og SAMRISK er å bygge norsk kompetanse innenfor samfunnssikkerhetsforskning om digital sikkerhet, som gjør at norske forskere i større grad konkurrerer internasjonalt og deltar i prosjekter i Horisont 2020 i samarbeid med forskere fra andre land.

CyberSec4Europe – et pilotprosjekt som del av den fremtidige etableringen av et felles europeisk kompetansenettverk for digital sikkerhet:

Pilotprosjektet startet ved årsskiftet 2018/2019. Formålet med pilotprosjektet er å bidra til at EU ivaretar og blir ledende i neste generasjon av digital sikkerhet og teknologi. I løpet av 3,5 år skal prosjektet utvikle et veikart med anbefalinger for hvordan både nasjonale og felleseuropeiske kompetansenettverk bør drives.

CyberSec4Europe består av totalt 43 partnere fra 22 europeiske land, hvor SINTEF og NTNU deltar fra Norge. Av det totale prosjektbudsjettet på 15 mill. Euro fra EU's forskningsprogram Horisont 2020, går vel 700 000 Euro til Norge.

Det utdannes for få kryptologer i Norge i dag. Den nasjonale forskningskompetansen innenfor kryptologi skal styrkes. Det er tildelt midler til 24 stipendiatstillinger for søkere som kan sikkerhetsklareres. Sterkere fagmiljøer er nødvendig da kryptologien hele tiden er i utvikling og det gjøres et stort arbeid for å omgå de mekanismene som er i bruk. Spesielt bør utviklingen av kvantedatamaskiner nevnes, da dette vil få en avgjørende effekt på fundamentet for kryptologien i framtida.

Langtidsplanen for forskning og høyere utdanning 2019-2028 er regjeringens viktigste verktøy for å prioritere investeringer i forskning og høyere utdanning. Langtidsplanen legger fra 2019 opp til en bred teknologisatsing. Satsingen innen teknologi skal sees i sammenheng med perspektiver fra blant annet humanistisk, samfunnsvitenskapelig og juridisk forskning og utdanning. Langtidsplanen er utvidet med en ny langsiktig prioritering kalt «samfunnssikkerhet og samhørighet i en globalisert verden», som inkluderer digital sikkerhet. Utdanning er også et område som gis økt oppmerksomhet i revidert plan.

Tiltak
Prioritering av digital sikkerhet i revidert langtidsplan for forskning og høyere utdanning Den reviderte langtidsplanen inneholder en opptrappingsplan på 800 mill. kroner over fire år til utdanning og forskning innenfor teknologi, herunder grunnleggende forskning innenfor IKT, inkludert digital sikkerhet.
Prosjekter i regi av IKTPLUSS v/Norges forskningsråd I 2015 ble det igangsatt prosjekter av 3-4 års varighet – innenfor satsingen «et trygt informasjonssamfunn», med en ramme på mer enn 150 mill. kroner. Det pågår prosjekter om temaer som kryptologi og personvern. Utlyste midler i 2018 på 196 mill. kroner går til prosjekter om kritisk infrastruktur
Styrke digital sikkerhet som del av SAMRISK-programmet v/Norges forskningsråd Digital sikkerhet har inngått som tema i SAMRISK II (2013-2018). I programplanen for 2018 – 2027 er teknologi og samfunnssikkerhet en faglig prioritering. Det ble i 2018 utlyst midler til temaene teknologi og samfunnssikkerhet og organisering/ansvar innenfor samfunnssikkerhetsområdet. SAMRISK-programmet styrkes fra 2019 med 7 mill. kroner årlig til forskningstemaer om digital sikkerhet.
Fyrtårnprosjekt i regi av IKTPLUSS v/ Norges forskningsråd Fyrtårnprosjekt er prosjekter med en tydelig problemstilling om å bidra til å løse samfunnsutfordringer. Prosjektene skal i tillegg ha en bredde i kompetanse om den gjeldende forskningsfronten, organisasjonsstruktur, tjenesteyting og anvendelsessiden. Dette fyrtårnprosjektet er et samarbeid mellom brukere og forskere om tverrsektorielle tema som personvern – digital sikkerhet og sikkerhetsøkonomi på 10 mill. kroner årlig fra 2019.

Arena for forskningsformidling innenfor digital sikkerhet, større årlig konferanse

JD vil etablere en arena for å formidle brukerrettede forskningsresultater om utvalgte temaer innenfor digital sikkerhet. JD vil vurdere nasjonalt og internasjonalt samarbeid eller partnerskap om konferansen.

Styrke kjernemiljøene ved en kryptologisatsing fra 2018

Basisbevilgningen fra JD til NTNU CCIS (fra 2016) er på 5 mill. kroner årlig til områder som personvern, digital etterforskning og biometri. HOD bidrar til grunnbevilgningen med 2 mill. kr årlig. I tillegg kommer bidrag fra partnerne og inntekter fra andre kilder. Fra og med 2018 tildeler JD, som del av regjeringens kryptologisatsing, 5 mill. kroner til Simula@UiB for spesielt å styrke forskningen innenfor kryptologi. I tillegg bidrar KD, SD og NFD til grunnbevilgningen som til sammen er på mer enn 50 mill. kr. Videre tildelte KD i 2018 midler til 24 rekrutteringsstillinger til NTNU og Simula@UiB for å styrke forskningen på kryptologi, midler som videreføres og trappes opp til helårsbevilgninger i 2019 (jf. satsingsområdet tilstrekkelig nasjonal spesialistkompetanse).

Tilstrekkelig nasjonal spesialistkompetanse

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

Det må utdannes et tilstrekkelig antall spesialister innenfor digital sikkerhet, inkludert kryptologi. For å ivareta rikets sikkerhet må en høy nok andel av disse spesialistene kunne sikkerhetsklareres.

Utdanningsinstitusjonene oppfordres til å benytte tilgjengelige virkemidler for å gjøre ph.d. til en attraktiv karrierevei, og å fange opp gode kandidater på et tidlig tidspunkt. JD vil ha dialog med Universitets- og høyskolerådet (UHR) om fremtidens behov og virkemidler for å arbeide for tilstrekkelig nasjonal spesialistkompetanse.

Regjeringens satsing på studieplasser til IKT-relaterte utdanninger i 2016, 2017 og 2018 innebærer tilsammen et varig økt årlig opptak på 1500 studenter. Det vil gradvis medføre en betydelig økning av tilgangen på godt kvalifiserte IKT-kandidater. Mange institusjoner melder også at de utvikler spesialiserte moduler og temaer i digital sikkerhet både på bachelor- og masternivå for å møte etterspørselen fra arbeidslivet og myndighetene. Dette innebærer til sammen et betydelig løft for å dekke arbeidslivets økte etterspørsel etter kandidater, som anslått i NIFU-rapporten.

NIFU-rapporten peker på en spesiell utfordring med å rekruttere kvinner til fag innen digital sikkerhet. Kvinneandelen er langt lavere enn for naturvitenskapelig og tekniske fag generelt og noe lavere enn for IKT-studier. Det er heller ikke noen tegn til at andelen kvinner øker. Ca. 13 pst. av studentene innenfor digital sikkerhet er kvinner.

Tiltak
Utdanning innenfor IKT og digital sikkerhet Flere studieplasser i 2016, 2017 og 2018 innenfor IKT-relaterte utdanninger, bl.a. rettet mot digital sikkerhet, innebærer til sammen et økt årlig opptak på 1500 studenter. I tillegg har styrene ved institusjonene innenfor sine rammebevilgninger ansvar for å prioritere sine studietilbud i samsvar med samfunnets behov for kompetanse. Innenfor opptrappingsplanen «Teknologiløft» i den reviderte langtidsplanen for forskning og høyere utdanning, vil regjeringen vurdere å øke antall studieplasser innenfor IKT-relaterte utdanninger.
Øke antall personer med ph.d. utdanning i digital sikkerhet inkludert kryptologi Flere rekrutteringsstillinger i 2017 og 2018 (16 + 46 stillinger) øremerket til digital sikkerhet og kryptologi vil videreføres og trappes opp til helårsbevilgninger.
Stimulere til bruk av nærings ph.d. og offentlig sektor ph.d. i regi av Norges forskningsråd Offentlige og private virksomheter får støtte til at ansatte kan gjennomføre en doktorgrad. Forskningsrådet gir tilskudd til doktorgradsarbeidet med inntil 50 prosent av kostnadene. Virksomhetene oppfordres til å benytte dette tilbudet i større grad til prosjekter om digital sikkerhet.
Likestillingstiltak for flere jenter til studier innenfor digital sikkerhet JD vil samarbeide med NTNU ved Nasjonalt senter for realfagsrekruttering om å oppsummere et kunnskapsgrunnlag om tiltak for å motivere flere jenter til å velge MNT-fag, herunder IKT-fag.

Digital sikkerhet som del av IKT-relaterte utdanninger og tilgrensende fag

Mål: 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.

Det varierer i hvor stort omfang digital sikkerhet inngår i IKT-relevante utdanninger. Kompetansen på dette området bør styrkes. Som Lysneutvalget påpekte, bør alle systemutviklere og programmerere ha et visst minimum av digital sikkerhet for å bidra til at digital sikkerhet bygges inn ved design og utvikling av IKT-systemer.

I tildelingen fra KD til nye studieplasser innenfor IKT er det lagt til grunn at institusjonene skal prioritere studietilbud rettet mot digital sikkerhet. Satsingen har gradvis, i tillegg til flere studieplasser i digital sikkerhet, også medført et økt omfang av emner i digital sikkerhet i ulike IKT-studier både på master og bachelornivå.

Det er løpende dialog mellom myndighetene og utdanningsinstitusjonene om digital sikkerhet i IKT- og teknologiutdanningene. Digital sikkerhet må forsterkes som del av tilgrensende fag, dvs. relevante teknologiske utdanninger hvor digital sikkerhet hører naturlig hjemme. Det er viktig at utdanningsinstitusjonene på studieprogramnivå har god dialog med samfunns- og arbeidslivet om utdanningene.

Tiltak
Kartlegge behov og tilbud av kurs i digital sikkerhet som del av IKT og tilgrensende fag Det skal foreligge et oppdatert tall- og faktagrunnlag for digital sikkerhet som del av IKT og tilgrensende fag. JD vil sørge for oppdatert statistikk og analyser for å følge med på kompetansegapet innen digital sikkerhet, jf. rapporten fra NIFU og Lysneutvalget.
Styrke arbeidet med digital sikkerhet i ingeniør- og teknologiutdanningene Universitets- og høgskolerådet er tildelt 1 mill. kroner i 2018 for å koordinere et samarbeid mellom institusjonene som tilbyr ingeniør- og IKT-utdanninger for å legge mer vekt på digital sikkerhet i utdanningene. Samarbeidet skal bidra til tiltak som kan øke kvaliteten på og omfanget av digital sikkerhet i utdanningene. KD vil også i 2019 tildele midler til tiltaket.

Etter- og videreutdanning (EVU) innenfor IKT og digital sikkerhet

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

NIFU-rapporten rettet søkelys mot et akutt behov for digital sikkerhetskompetanse og at etter- og videreutdanningstilbudet innenfor digital sikkerhet samtidig synes å være begrenset.

Etter- og videreutdanning kan være kortsiktige treffsikre tiltak for å dekke deler av kompetansegapet på digital sikkerhet. Et premiss for vellykkede tilbud er dialog mellom arbeidsliv og utdanningsinstitusjonene. Tilbudene bør være fleksible og utvikles for ulike utdanningsgrupper.

Tiltak
Regjeringens kompetansereform – lære hele livet Regjeringen vil gjennomføre en kompetansereform slik at ingens kompetanse skal gå ut på dato. I forbindelse med arbeidet med kompetansereformen vil regjeringen se på insentiver for individer og virksomheter for å styrke sin kompetanse, og hvorvidt utdanningssystemet er rigget for å levere etter- og videreutdanning som dekker arbeidslivets behov.
Markussen-utvalget om udekkede behov for etter- og videreutdanning Regjeringen har satt ned et utvalg for å undersøke udekkede behov for etter- og videreutdanning, og i hvilken grad utdanningssystemet er i stand til å møte arbeidslivets behov for fleksible kompetansetilbud.
Midler til utvikling av fleksible videreutdanningstilbud i digital kompetanse Regjeringen har som en start på kompetansereformen satt av 10 mill. kroner til utvikling av fleksible videreutdanningstilbud i digital kompetanse i 2018. I statsbudsjettet for 2019 ble det bevilget 37 mill. kroner til dette tiltaket. Høyskoler, universitet og fagskoler kan søke på midlene sammen med bedrifter og næringsliv.

Digital sikkerhet i yrkes- og profesjonsutdanninger

Mål: Digital sikkerhet inngår i relevante yrkesutdanninger og profesjonsutdanninger i tilstrekkelig grad.

Kompetansebehovet i ulike yrker endrer seg hurtig i møte med teknologisk utvikling. Det er derfor nødvendig å undersøke hvilke spesifikke digitale sikkerhetskompetanser det er behov for i yrker og profesjoner. Dette gjelder både for høyere utdanning og fag- og yrkesopplæringen.

Våren 2018 ble det besluttet at man skal gjøre endringer i den yrkesfaglige tilbudsstrukturen i videregående opplæring. Utdanningsdirektoratet arbeider fram til 2020 med å endre og tilpasse innholdet i de nye yrkesfaglige utdanningsprogrammene.

Ut fra en vurdering av hvordan digitaliseringen påvirker risikobildet og behovene for digital kompetanse, inkludert personvern, må de ansvarlige for de ulike yrkes- og profesjonsutdanningene vurdere hvordan og i hvilken grad digital sikkerhet kan integreres i utdanningene. Noe arbeid har allerede blitt lagt ned i både videregående opplæring og i universitets- og høyskolesektoren. Disse danner gode eksempler og kan være forbilder for andre.

Tiltak
Gjennomgang av relevante læreplaner i fag- og yrkesopplæringen KD vil gjennom arbeidet med nye yrkesfaglige læreplaner vurdere hvor det er relevant å innlemme digital sikkerhet i kompetansemålene i læreplanene. Digital sikkerhet kan for eksempel inngå som et element i det nyopprettede utdanningsprogrammet IKT og medieproduksjon.
Politiutdanning – kurs innenfor IKT-kriminalitet/digital sikkerhet, som del av bachelor- og masterutdanning JD arbeider med en melding om endringene i kriminalitetsbildet. Meldingen vil gjennomgå og drøfte konsekvenser for politiets kapasitet og kompetanse.
Digital sikkerhet i helsefagutdanninger Styrke digital sikkerhet i helsefagutdanningene.

Rammeverk for lærerens profesjonsfaglige digitale kompetanse

Rammeverk for lærerens profesjonsfaglige digitale kompetanse (PfDK) er et retningsgivende dokument som politikkutviklere, instituttledere, lærerutdannere, lærere, lærerstudenter og andre kan bruke som referanse i arbeidet med å øke kvaliteten i lærerutdanning og systematisk etter- og videreutdanning av lærere.

Etikk

En profesjonsfaglig digitalt kompetent lærer kjenner skolens verdigrunnlag i forhold til digitalisering i samfunnet. Læreren har innsikt i lovverk så vel som etiske problemstillinger knyttet til digital dannelse og deltakelse i det digitale og demokratiske samfunnet. Læreren bidrar til å utvikle elevenes digitale dømmekraft, forståelse og evne til å handle i tråd med dette.

God grunnkompetanse

Mål: 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.

Barn og unge lever i en digitalisert virkelighet og trenger kunnskap og ferdigheter for å kunne bruke teknologien på en sikker måte. Grunnleggende digitale ferdigheter inkluderer utvikling av god digital dømmekraft og strategier for å beskytte digitalt utstyr og informasjon.

Stortingsmelding 28 (2015-2016) *Fag – Fordypning – Forståelse, en fornyelse av Kunnskapsløftet,* beskriver mål og prinsipper for fagfornyelsen. Elevene skal få en kompetanse som forbereder dem på framtidens arbeids- og samfunnsliv. Derfor endres læreplanene slik at de får mer relevant innhold, tydeligere prioriteringer og bedre sammenheng mellom fag. Læreplanene skal legge bedre til rette for dybdelæring og forståelse.

Fra skoleåret 2020-2021 skal de nye læreplanene tas i bruk. Det er da viktig med et mangfold av gode og innovative digitale læremidler. Programmering inngår i flere fag som følge av fagfornyelsen. Programmering er også innført som valgfag på ungdomstrinnet.

Bedre teknologiforståelse gjennom grunnopplæringen og mer oppmerksomhet om digital sikkerhet i befolkningen kan på sikt bidra til bedre søkning til relevante studieprogram i høyere utdanning.

Tiltak

Første fase av fagfornyelsen er utvikling av kjerneelementer i fagene

Kjerneelementene gir retning og prioriteringer for læreplanene som skal være ferdige høsten 2019. Av kjerneelementene, som ble fastsatt juni 2018, framgår det at naturfag vil få en tydelig teknologidel, programmering kommer inn i flere fag og algoritmisk tenking blir fremhevet i matematikkfaget. Samfunnsfag får et spesielt ansvar for digitale ferdigheter.

Videreutdanning for å styrke lærernes digitale kompetanse

Det er tilbud om videreutdanning i programmering og profesjonsfaglig digital kompetanse for lærere gjennom videreutdanningsstrategien Kompetanse for kvalitet.

Den teknologiske skolesekken inneholder flere tiltak for teknologiforståelse og digitale læremidler[8]

Den teknologiske skolesekken skal bidra til elevenes kunnskap om og forståelse for teknologi, algoritmisk tenkning og programmering og gi tilgang på gode digitale læremidler. I 2018 etableres en tilskuddsordning for utvikling av digitale læremidler. Skoleeiere vil fra 2019 få økonomisk støtte til innkjøp av digitale læremidler på til sammen 48 mill. kroner. Det vil blant annet gis tilskudd til vitensentrenes arbeid med programmering for elever og lærere og tilskudd til utstyr til skoleeiere som prioriterer kompetanseheving i programmering for lærere.

[8] https://www.udir.no/kvalitet-og-kompetanse/nasjonale-satsinger/den-teknologiske-skolesekken/.

Bevisstgjørende tiltak og bedret digital sikkerhetskultur

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

Den nye teknologien har skapt store endringer i hvordan folk behandler informasjon, og hvordan vi har gjort oss avhengig av at nettjenester er tilgjengelige til enhver tid. Tilstrekkelig opplæring/bevisstgjørende tiltak er sentralt for å bidra til bedre «netthygiene». Dette omfatter betydningen av å sikre egen datamaskin for sikkerheten på nettet generelt. NorSIS undersøkelser i 2016, 2017 og 2018 for å måle digital sikkerhetskultur viser at befolkningen ikke har nok kunnskap om digital sikkerhet.

Digital sikkerhet bør inngå som del av bevisstgjørende tiltak innenfor IKT generelt. Det bør videre utvikles tilpasset opplæring om digital sikkerhetskultur til utsatte grupper i befolkningen.

Det skal videreutvikles et kunnskapsgrunnlag om den norske sikkerhetskulturen, som kan brukes som beslutningsgrunnlag for sikkerhetstiltak i norske bedrifter og kommuner. Større virksomheter bør vurdere egne undersøkelser for å få bedre oversikt over den digitale sikkerhetskulturen som grunnlag for tiltak.

Tiltak
Undersøkelse om digital sikkerhetskultur NorSIS gjentar undersøkelsene fra 2016, 2017 og 2018 om digital sikkerhetskultur, i små og mellomstore virksomheter, kommuner og befolkningen. Som ledd i prosjektet inngår forskningssamarbeid for å utvikle ny kunnskap om hvordan digital sikkerhetskultur utvikles og påvirkes. Det vektlegges bred spredning av resultatene fra prosjektet. JD bidrar til delfinansiering.
Måle grunnskoleelevenes digitale ferdigheter KD vurderer om den digitale kartleggingsprøven på 4. trinn skal videreutvikles og gjøres obligatorisk.
Folkeopplysningskampanje JD vil vurdere å etablere en folkeopplysningskampanje, evt. som del av Nasjonal sikkerhetsmåned. Innretningen av kampanjen vil skje i samarbeid med NorSIS. Dette kan eksempelvis være «Fjellvettregler», kreativ informasjon tilpasset ulike befolkningsgrupper, inkludert grupper som befinner seg utenfor arbeidsmarkedet.
European Cyber Security Challenge i regi av ENISA Dette er en nasjonal og internasjonal konkurranse for å synliggjøre unge talenter. En juniorgruppe 16-20 år og en seniorgruppe 21-25 år. NTNU CCIS står for den norske konkurransen. Slike tiltak kan bidra til å skape blest og medieoppmerksomhet om kompetanse på digital sikkerhet blant ungdom og unge voksne.

En pilot om opplæring av barn og ungdom i regi av NSM, NVE, NorSIS, NTNU, UiO og Abelia i Oppegård, Ski og Rogaland.

Piloten er finansiert gjennom et spleiselag fra norske myndigheter, frivillig dugnad fra universiteter, private selskap og økonomisk støtte fra den amerikanske ambassaden. Piloten skal utvikle og teste et opplæringskonsept tilpasset norske forhold etter modell av amerikanske GenCyber[9]. Formålet med piloten er å utdanne lærere og elever i digital sikkerhet, følgende elementer inngår:

- Sommerskole, få ukes-lange sommerleirer for barn/ungdom.
- Utvikle et opplæringskonsept i informasjonssikkerhet som vektlegger praktisk læring og som treffer ulike aldersgrupper og ferdighetsnivåer
- Evaluere og lære og bruke erfaring fra piloten til å utvikle flere utdanningstilbud.

[9] National Science Foundation (NSF) og National Security Agency, jf URL https://www.gen-cyber.com/about/

Ordliste:

NTNU CCIS	Norges teknisk naturvitenskapelige universitet, Center for Cyber and Information Security,
ENISA	European Union Agency for Network and Information Security
GenCyber	The GenCyber program: summer cybersecurity camp experiences for students and teachers at the K-12 level.
Grunnopplæringen	Betegnelse for det 13-årige opplæringsløpet som omfatter 10-årig grunnskole og 3-årig videregående opplæring
EVU	Etter- og videreutdanning
NFR	Norges forskningsråd
NIFU	Nordisk Institutt for studier av innovasjon, forskning og utdanning
NorSIS	Norsk senter for Informasjonssikring
NSM	Nasjonal sikkerhetsmyndighet
UHR	Universitets- og høgskolerådet

Utgitt av:
Justis- og beredskapsdepartementet

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-0446 B
Trykk: Departementenes sikkerhets- og serviceorganisasjon
01/2019 – opplag 600