IKT-sikkerhet i utdanningene

Anbefalinger fra arbeidsgruppen

4. november 2021

Nasjonal arbeidsgruppe for styrking av undervisning i IKT-sikkerhet[†]

[†] Medlemmene av arbeidsgruppen: *Anders Andersen (UiT-Tromsø), Tor Berre (NTNU-Trondheim), Pål Ellingsen (HVL), Olaf Hallan Graven (USN), Laurence Habib (OsloMet), Moutaz Haddara (HK), Erik Hjelmås (NTNU-Gjøvik), Mette Mo Jakobsen (UHR/UiA), Audun Jøsang (UiO), Lars Emil Knudsen (HiØ), Jingyue Li (NTNU-Trondheim), Arne Roar Nygård (Elvia/NHO), Tom Heine Nätt (HiØ), Sondre Rønjom (NSM/UiB), Hans Georg Schaathun (NTNU-Ålesund), Arild Steen (UiT-Narvik), Tor-Fredrik Torgersen (UiS).*

Kontaktperson og leder av arbeidsgruppen: Anders Andersen (Anders.Andersen@uit.no)

Innhold

Sammendrag

Denne rapporten presenterer resultatet av arbeidet til *Nasjonal arbeidsgruppe for styrking av undervisning i IKT-sikkerhet*. Arbeidsgruppen har (i) identifisert anbefalte læringsmål som forventes å bli inkludert i alle teknologi- og realfag-utdanninger, (ii) gitt anbefalinger på hvordan læringsmål i IKT-sikkerhet skal kunne realiseres i ulike utdanninger, og (iii) identifisert tilgjengelig læremateriell og vurdert dette opp mot de anbefalte læringsmål i IKT-sikkerhet og hvordan disse læringsmålene er tenkt integrert i utdanningene.

Arbeidsgruppen har identifisert seks tema innen IKT-sikkerhet som bør dekkes i alle ingeniørutdanninger, og også i høyere utdanning generelt:

1. Grunnleggende begreper og historisk utvikling
2. Bevissthet og sikkerhetskultur
3. Personvern
4. Lover, reguleringer, etikk og standarder
5. Trusselmodellering og risikostyring
6. Sikkerhetsarkitektur og innebygd informasjonssikkerhet

Å integrere disse læringsmålene i ulike utdanninger kan være en stor utfordring. Ulike utdanninger har stor variasjon i hvordan de bygges opp og hvilke tema de inneholder. I våre forslag så diskuterer vi følgende:

- Når, i hvilken form og i hvor stort omfang de ulike temaene skal introduseres
- Viktigheten av å gjøre temaet IKT-sikkerhet relevant for det spesifikke utdanningen
- Utfordringene i å få IKT-sikkerhet godt integrert i et studieløp

Vi rapporterer også kort erfaringene noen av medlemmene i arbeidsgruppen har gjort med å integrere de anbefalte læringsmålene på sitt lærested.

Å finne egnet læremateriell er også en viktig del av det å kunne integrere IKT-sikkerhet i en utdanning. Arbeidsgruppen presenter noen forslag på læremateriell og diskuterer kort hvordan disse dekker de anbefalte læringsmålene. Vi diskuterer også utfordringen i å få frem læremateriell som er relevant for ulike utdanninger. Dette innebærer blant annet læremateriell med eksempler som er kjente og relevante i fagprofilen i utdanningen til studentene. Dette er også viktig for at studentene skal være motivert til innsats på dette området.

Arbeidsgruppen har i sitt arbeide hatt spesielt fokus på ingeniørutdanningene. En av årsakene til dette fokuset er at arbeidsgruppens arbeid sammenfalt med en revisjon av Nasjonale retningslinjer for ingeniørutdanning. Vi bidro blant annet med konkrete forslag til læringsmål for IKT-sikkerhet i ingeniørutdanningene og vi brukte ulike ingeniørutdanninger som eksempel når integrasjon av læringsmål i utdanninger ble diskutert. Vi mener likevel at resultatene presentert i rapporten kan benyttes for å integrere IKT-sikkerhet i alle teknologi- og realfag-utdanninger. Vi tror også at arbeidet presentert her er et godt utgangspunkt for integrering av IKT-sikkerhet i andre utdanninger.

Kapittel 1

Introduksjon

Nasjonal arbeidsgruppe for styrking av undervisning i IKT-sikkerhet ble opprettet helt på tampen av 2018 og skulle fullføre sitt arbeid i 2020. Men så kom det en pandemi. Dette har forsinket arbeidet i denne arbeidsgruppen betydelig. En stor del av medlemmene i arbeidsgruppen har hatt sentrale roller for håndtering av koronasituasjonen lokalt i sin institusjon, og dette har gitt lite rom for avslutning av arbeidet. I tillegg ble planlagte fysiske arbeidsmøter avlyst.

Som en følge av pandemien ble det i 2020 prioritert å bruke den begrensede kapasiteten som var tilgjengelig til å bidra med læringsutbyttebeskrivelser for IKT-sikkerhet i de nye Nasjonale retningslinjer for ingeniørutdanningene [38].

1.1 Arbeidsgruppens bakgrunn

Arbeidsgruppen er et resultat av Stortingsmelding 38 (2016–2017): IKT-sikkerhet - Et felles ansvar [17]. Samfunnets behov for kunnskap om IKT-sikkerhet har vært understreket i flere tidligere utredninger og stortingsmeldinger, inklusivt i Lysneutvalgets utredning NOU 2015:13: Digital sårbarhet, sikkert samfunn [28], Stortingsmelding 27 (2015–2016): Digital agenda for Norge [24] og Stortingsmelding 10 (2016–2017): Risiko i et trygt samfunn [16]. I Stortingsmelding 4 (2018–2019): Langtidsplan for forskning og høyere utdanning 2019–2028 [26] påpekes det at det er et behov for en mer helhetlig kompetanse og tverrfaglig forståelse av sikkerhet på flere områder. Men Stortingsmelding 38 (2016-2017) går lengre ved å påpeke viktigheten av IKT-sikkerhet i alle typer høyere utdanning og foreslå tiltak for å få økt kompetanse i informasjonssikkerhet. Stortingsmeldingen ble behandlet på Stortinget 10. april 2018 med følgende vedtak [37]:

- Stortinget ber regjeringen sørge for at relevante ingeniør- og teknologiutdanninger har kurs i IKT-sikkerhet.
- Stortinget ber regjeringen sørge for at det stimuleres til bedre etter- og videreutdanningstilbud på fagskoler, universiteter og høyskoler innen IKT- og datasikkerhet.
- Stortinget ber regjeringen sørge for at digitalisering og IKT-sikkerhet prioriteres i neste Langtidsplan for forsking og høyere utdanning.
- Stortinget ber regjeringen legge fram en plan som synliggjør politiets arbeid med IKT-kriminalitet og hvordan dette skal finansieres.

I revidert statsbudsjett for 2018 tildelte Kunnskapsdepartementet midler til Universitets- og høgskolerådet (UHR) for å koordinere et arbeid for å styrke IKT-sikkerhet i teknologiutdanningene. Kunnskapsdepartementet viser til ny Forskrift om rammeplan for ingeniørutdanning [25] der læringsutbyttebeskrivelse for IKT-sikkerhet er fastsatt. I tillegg har det vært en dialog mellom Justisdepartementet, Kunnskapsdepartementet og Nasjonalt fagorgan for IKT[1] om hvordan universiteter og høyskoler kan styrke sitt tilbud om IKT-sikkerhet. Kunnskapsdepartementet ber etter denne dialogen om at UHR sin fagstrategiske enhet for matematiske, naturvitenskapelige og teknologiske fag (UHR-MNT) koordinerer et samarbeid mellom institusjonene som tilbyr ingeniør- og IKT-utdanninger for å legge mer vekt på IKT- sikkerhet i utdanningene. Samarbeidet skal bidra til tiltak som kan øke kvaliteten på, og omfanget av, IKT-sikkerhet i utdanningene.

Arbeidsutvalget til UHR-MNT behandlet tildelingen fra Kunnskapsdepartementet med utgangspunkt i et felles nasjonalt behov for å møte disse skjerpede kravene til IKT-sikkerhet i utdanningene. Arbeidsutvalget vedtok følgende:

- Arbeidsutvalget ber Nasjonalt fagorgan for IKT (UHR-NFI) om å etablere en arbeidsgruppe som planlegger og gjennomfører et prosjekt for styrking av undervisningstilbud i IKT/IKT-sikkerhet.

[1] Tidligere Nasjonalt fagråd for IKT har endret navn til Nasjonalt fagorgan for IKT.

- Arbeidsgruppen bes om å utforme forslag til hvordan det rammeplanfestede kravet om implementering av IKT-sikkerhet i ingeniørutdanningene bør gjennomføres ved utdanningsinstitusjonene.
- Arbeidsgruppen bes også gi råd om hvordan IKT-sikkerhet bør implementeres i realfag og sivilingeniørutdanning.
- Arbeidsutvalget forelegges planen til godkjenning og fungerer som styringsgruppe for prosjektet.

Alle institusjonene i UHR-NFI ble invitert til å melde inn aktuelle personer. Tekna, NHO og NITO ble også oppfordret til å stille. NHO meldte inn Arne Roar Nygård fra Eidsiva Nett, som representant fra NHO/Energi Norge. Tekna og NITO ønsket ikke å melde inn representanter til arbeidsgruppen, men ville kunne delta på seminarer for drøfting og diskusjon. Det ble også bestemt at arbeidsutvalget til UHR-NFI skulle fungere som referansegruppe for arbeidsgruppen og arbeidsutvalget til UHR-MNT skulle fungere som styringsgruppe for arbeidsgruppen. Arbeidsgruppen ble opprettet på senhøsten 2018 og hadde sitt første digitale møte 21. november 2018. I Vedlegg A.1 er det en kort presentasjon av alle medlemmene i arbeidsgruppen.

1.2 Videre føringer etter at arbeidsgruppen ble etablert

Etter at arbeidsgruppen ble etablert i november 2018 så er det kommet flere offentlige føringer og signaler relevant for arbeidet til arbeidsgruppen. I 2019 ble det utarbeidet en nasjonal strategi for kompetanse innenfor digital sikkerhet [21]. Her finner vi blant annet følgende 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 påpekes også at kompetansebehovet endrer seg hurtig på grunn av den teknologiske utviklingen. Et viktig spørsmål da er hvilke IKT-sikkerhetskompetanse det er behov for i ulike yrker og profesjoner. Dette utkrystalliserer seg i følgende mål i strategien:

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

I Stortingsmelding 5 (2020–2021): Samfunnssikkerhet i en usikker verden [20] understrekes det også at digital sikkerhet er et satsingsområde i yrkes- og profesjonsutdanninger. Og Stortingsmelding 14 (2019–2020): Kompetansereformen – Lære hele livet [27] angir en satsing for å utvikle tilbudet innen digital sikkerhet hos utdanningsinstitusjonene.

1.3 Tolkning av mandatet

Arbeidsgruppen har forsøkt å tolke sitt mandat basert på den bakgrunnen som er beskrevet ovenfor og de signaler vi har fått fra UHR-MNT og UHR-NFI. I tillegg har vi forsøkt å ta hensyn til hva som er en realistisk leveranse fra en slik arbeidsgruppe for den planlagte perioden. Dette er vår tolkning av mandatet:

- Arbeidsgruppen skal identifisere anbefalte læringsmål i IKT-sikkerhet som forventes å bli inkludert i alle teknologi- og realfag-utdanninger:
  - Arbeidsgruppen skal se særskilt på anbefalte læringsmål i IKT-sikkerhet for alle ingeniørutdanningene
  - Arbeidsgruppen skal vurdere å anbefale læringsmål i IKT-sikkerhet for andre utdanninger (ikke-teknologi- og ikke-realfag-utdanninger)
- Arbeidsgruppen skal gi anbefalinger på hvordan læringsmål i IKT-sikkerhet skal kunne realiseres i ulike utdanninger:
  - Arbeidsgruppen skal se særskilt på hvordan anbefalte læringsmål i IKT-sikkerhet kan integreres i ingeniørutdanningene
  - Arbeidsgruppen skal drøfte hvordan anbefalte læringsmål i IKT-sikkerhet kan integreres i ulike typer utdanninger
- Arbeidsgruppen skal identifisere tilgjengelig læremateriell og vurdere dette opp mot de anbefalte læringsmål i IKT-sikkerhet og hvordan disse læringsmålene er tenkt integrert i utdanningene:
  - Hvor godt dekker tilgjengelig læremateriell læringsmålene og hvor egnet er dette læremateriellet til bruk i ulike utdanninger?
  - Hvis egnet læremateriell ikke er tilgjengelig, hvordan kan man få produsert dette?

1.4 Arbeidets faser

Arbeidsgruppen har arbeidet i ulike faser. I første fase var fokus å samle inn mest mulig informasjon om området IKT-sikkerhet i utdanninger. Denne informasjon fant vi i tidligere arbeider med læreplaner i IKT-sikkerhet [13, 33], presentasjoner fra medlemmer i faggruppen fra praksis i egen institusjon, søk i offentlige utredninger og styringsdokumenter (se Vedlegg C.2), og et omfattende arbeid i å undersøke hvordan dette gjøres ved andre læresteder nasjonalt og internasjonalt. I andre fase forsøket vi å bearbeide det innsamlede materialet til konkrete forslag for læringsmål og integrasjon av disse i utdanningene. En stor utfordring i denne fasen var både å begrense seg i omfang og kompleksitet og se forslagene våre fra et ikke-ekspert perspektiv. I denne fasen så vi også at det å finne egnet læremateriell for ulike utdanninger vil bli en stor utfordring. I tredje fase var fokus på å få tilbakemeldinger på, og forbedre, våre forslag. I tillegg jobbet vi i denne fasen mye med integrering av læringsmål i ulike utdanninger og med hvordan nytt egnet læringsmateriell skal kunne bli utviklet og gjort tilgjengelig. En oversikt over alle arbeidsgruppemøtene finnes i Vedlegg A.2.

1.5 Rapporten

Rapporten er delt i tre deler. Den første delen tar for seg læringsmålene, både med konkrete læringsutbyttebeskrivelser og med en mer utfyllende og konkret diskusjon om hvilke innhold som kan inkluderes for å oppnå disse læringsutbyttene. Den andre delen har et fokus på hvordan læringsmålene kan integreres i utdanninger slik at de er relevante og inngår i en helhet i utdanningen. Den tredje delen omhandler læringsmateriell og utfordringer knyttet til det utvikle læringsmateriell relevant for ulike studieretninger og fagprofiler. Noen konkrete eksempler på læringsmateriell blir også presentert.

Med rapporten følger det også tre vedlegg. Vedlegg A beskriver arbeidsgruppens medlemmer, arbeidsgruppens møter og medlemmene i arbeidsgruppen sine deltakelser på konferanser og andre møter hvor de representerte arbeidsgruppen. Vedlegg B inkluderer andre bidrag fra arbeidsgruppen, inklusiv web-side, liste over publikasjoner og presentasjoner, bidraget til Nasjonale retningslinjer for ingeniørutdanningene og artikkel publisert på MNT-konferansen i 2019 [1]. Vedlegg C lister relevante eksterne ressurser, inklusive norske nettsider, relevante utredninger styringsdokumenter, relevante lover og reguleringer og relevante standarder og anbefalinger.

Kapittel 2

Læringsmål IKT-sikkerhet

2.1 Innledning

I et samfunn med økt digitalisering, hvor IKT er sentralt på alle områder, både i privatlivet og arbeidslivet, så er sårbarheter og risikoer som en følge av dette en stor utfordring. IKT-sikkerhet som fagområde skal bidra til å håndtere disse utfordringene. Behovet for kompetanse om IKT-sikkerhet er derfor sterkt økende, ikke bare som eget fagområde, men også som en integrert del av andre fagområder.

IKT-sikkerhet er et svært stort fagområde. Internasjonalt foregår det et betydelig arbeid med å definere hva studieprogrammer innen informasjons- og cybersikkerhet bør inneholde [13, 33]. Disse aktivitetene produserer fagoversikter innen IKT-sikkerhet som er meget omfattende og til dels overveldende. De er derfor uegnet som et direkte grunnlag for en anbefaling av hva som bør inngå av IKT-sikkerhet integrert i andre utdanninger.

En rekke offentlige utredninger og stortingsmeldinger [28, 24, 16, 17, 37] har understreket at det er et stort behov i Norge for å øke kompetanse og bevisstgjøring rundt temaene IKT og IKT-sikkerhet. I tillegg påvirker sårbarheter og risikoer, som følge av økt digitalisering, hvordan vi organiserer og regulerer alle områder av samfunnet [11].

Nasjonal Sikkerhetsmyndighet definerer i NSMs grunnprinsipper for IKT-sikkerhet[1] [31] et sett med prinsipper og underliggende tiltak for å beskytte informasjonssystemer (maskinvare, programvare og tilknyttet infrastruktur), data og tjenester mot uautorisert tilgang, skade eller misbruk. Disse grunnprinsippene er også et utgangspunkt for hvordan behovet for kompetanse er vurdert her.

På grunn av den overveldende størrelsen på fagområdet IKT-sikkerhet så vil en anbefaling som kun sier at en utdanning må inneholde minimum 5 studiepoeng IKT-sikkerhet, uten å gå inn på hva dette innebærer, være lite nyttig. Arbeidsgruppen har identifisert seks tema innen *IKT-sikkerhet* som bør dekkes i alle ingeniørutdanninger, eller i høyere utdanning generelt:

1. Grunnleggende begreper og historisk utvikling
2. Bevissthet og sikkerhetskultur
3. Personvern
4. Lover, reguleringer, etikk og standarder
5. Trusselmodellering og risikostyring
6. Sikkerhetsarkitektur og innebygd informasjonssikkerhet

En forståelse av *grunnleggende begreper* innen IKT-sikkerhet er viktig for å kunne kommunisere muntlig og skriftlig om temaet og for å kunne tilegne seg kunnskap fra ulike ressurser som bruker disse begrepene. Den *historiske utviklingen* innen IKT-sikkerhet viser at kunnskap om dette er ferskvare.

Det er nødvendig med en *bevissthet* om at bruk av IKT innebærer en sikkerhetsrisiko. En manglende *sikkerhetskultur* med fokus på slik risiko, kan få store følger for organisasjoner og for samfunnet.

Personvern handler om retten til et privatliv og selvbestemmelse over egne personopplysninger. Dette er en lovfestet rett i Norge [18] som er blitt ytterlige styrket av de nye personvernreglene som er innført i hele EU/EØS i 2018 [7]. En

[1] https://www.nsm.stat.no/publikasjoner/andre-publikasjoner/grunnprinsipper-for-ikt-sikkerhet-2-0/

forståelse av konsekvensene av personvern og bruk av personopplysninger i IKT-baserte løsninger bør være inkludert i høyere utdanning. Personvern omfatter mer enn det våre foreslåtte læringsmål inkluderer og basert på det så kunne dette temaet hatt tittelen Personopplysningsvern. Vi har valgt å beholde tittelen personvern fordi den er bedre kjent og fordi det kommer frem av vår kontekst IKT-sikkerhet hvilke område av personvern vi er interessert i.

Nært beslektet med personvern vil behovet for en kompetanse om hvordan *lover*, *reguleringer* og *etikk* påvirker bruk og utvikling av IKT-baserte systemer. Disse gir oss en ramme for hvordan vi skal agere i forhold til slike systemer. *Standarder* bidrar blant annet til å enklere kunne beskrive krav og forventninger til systemer, og de kan gi oss sjekklister for å oppfylle slike krav og forventninger.

Trusselmodellering og *risikostyring* gir oss et verktøy for å identifisere problemområder og evaluere risikoen for hvert område opp mot kostnaden for å håndtere dem. Det er viktig å kunne organisere arbeid og praksis i et utviklingsprosjekt slik at en kan sikre en helhetlig sikkerhet i produktet. Dette gjelder både programutvikling og utvikling av fysiske systemer.

Ved realisering av IKT-systemer brukes *sikkerhetsarkitektur* og *innebygd informasjonssikkerhet* for å håndtere trusler og begrense risiko. For å kunne oppnå dette, er det nødvendig med en helhetlig forståelse av sikkerhet både under utvikling (programmering), drift og avvikling av IT-systemer.

2.2 Læringsutbyttebeskrivelser

Det fins flere internasjonale retningslinjer for læringsmål i studieprogrammer som fokuserer på IKT-sikkerhet. I disse finner vi anbefalinger for studieretninger som Bachelor eller Master i informasjonssikkerhet. Det er imidlertid en relativt ny idé at informasjonssikkerhet skal inngå som en allmenndannende komponent i ingeniørutdanningene og i all annen (høyere) utdanning. De følgende læringsutbyttebeskrivelsene forsøker å beskrive hva dette bør inneholde. Læringsutbyttebeskrivelsene er gruppert etter de seks temaene identifisert ovenfor. For hvert tema er det definert et sett av læringsutbyttebeskrivelser organisert under *kunnskap (LU-K)*, *ferdigheter (LU-F)* og *generell kompetanse (LU-G)*. Disse læringsutbyttebeskrivelsene er ment brukt i læringsutbyttebeskrivelser for emner eller moduler i utdanningen. Et utvalg av disse vil enten definere nye emner i utdanningen eller de vil inngå i eksisterende emner i utdanningen. Noen er grunnleggende og bør være inkludert i alle utdanninger mens andre er spesialiserte og vil inngå i noen utdanninger.

Læringsutbyttebeskrivelser som dekker disse, men som er tenkt som læringsutbyttebeskrivelser for en konkret utdanning, er markert i fet skrift. Disse kan for eksempel brukes i beskrivelse av læringsmål i en ingeniør- eller bachelor-utdanning. Et eksempel er læringsmålene for *IKT-sikkerhet* i «Nasjonale retningslinjer for ingeniørutdanningene» [38]. Vi gjengir disse i Vedlegg B.3. I læringsutbyttebeskrivelsene under er det lagt inn en referanse til tilsvarende læringsutbytte i IKT-sikkerhet i disse retningslinjene. For eksempel, *(kunnskap a)* refererer til læringsutbytte *a)* i kategori *kunnskap*, gjengitt i Vedlegg B.3.

2.2.1 Grunnleggende begreper og historisk utvikling

Kunnskap

LU-K-1-1 Kandidaten kjenner til sentrale momenter på den historiske utviklingen innen IKT-sikkerhet

LU-K-1-2 **Kandidaten behersker de mest sentrale begrepene innen IKT-sikkerhet** *(kunnskap a)*

Ferdigheter

LU-F-1-1 Kandidaten forstår en tekst eller en presentasjon hvor grunnleggende begreper innen IKT-sikkerhet benyttes

LU-F-1-2 Kandidaten kan anvende de mest sentrale begrepene innen IKT-sikkerhet i ulike sammenhenger og kan kommunisere skriftlig og muntlig om IKT-sikkerhet

Generell kompetanse

LU-G-1-1 **Kandidaten kan delta i diskusjoner om IKT-sikkerhet** *(generell kompetanse a)*

2.2.2 Bevissthet og sikkerhetskultur

Kunnskap

LU-K-2-1 Kandidaten kan gjøre rede for samfunnets sårbarhet som konsekvens av IKT-sikkerhetsutfordringer

LU-K-2-2 **Kandidaten har en grunnleggende forståelse av trusler og sårbarhet i samfunnet, med særlig vekt på hvordan digitalisering påvirker dette i egen profesjon** *(kunnskap b)*

Ferdigheter

LU-F-2-1 Kandidaten er i stand til å identifisere og håndtere trusler og sårbarheter på ulike nivå i en organisasjon

LU-F-2-2 Kandidaten kjenner til en typisk organisering av IKT-sikkerhet i en organisasjon

LU-F-2-3 **Kandidaten kan argumentere for viktigheten av god cyber-hygiene (rutiner og oppførsel), bruker-opplæring i IKT-sikkerhet, og bevissthet rundt IKT-sikkerhetstrusler og sårbarheter** *(ferdigheter a)*

Generell kompetanse

LU-G-2-1 **Kandidaten kan samarbeide om, og utvise ansvarlighet overfor, IKT-sikkerhet** *(generell kompetanse b)*

2.2.3 Personvern

Kunnskap

LU-K-3-1 **Kandidaten har kunnskap om når behovet for personvern trer i kraft i sitt arbeid** *(kunnskap c)*

LU-K-3-2 **Kandidaten har kunnskap om typiske tilnærminger for beskyttelse og anonymisering av persondata** *(kunnskap c)*

LU-K-3-3 Kandidaten kjenner til viktige lover og regler på området (GDPR, nasjonale lover og regler)

Ferdigheter

LU-F-3-1 **Kandidaten kan vurdere om et system forvalter sensitive persondata** *(ferdigheter b)*

LU-F-3-2 **Kandidaten kan identifisere behov for beskyttelse av persondata** *(ferdigheter b)*

LU-F-3-3 Kandidaten kan anvende viktige lover og regler på området (GDPR, nasjonale lover og regler)

Generell kompetanse

LU-G-3-1 Kandidaten forstår hvorfor personvern er spesielt viktig i et samfunn med stadig økende digitalisering

2.2.4 Lover, reguleringer, etikk og standarder

Kunnskap

LU-K-4-1 **Kandidaten kan gi en oversikt over de mest relevante lover, forskrifter og standarder for IKT-sikkerhet, og deres anvendelse innenfor eget fagområde** *(kunnskap d)*

LU-K-4-2 Kandidaten kan gjøre rede for behovet for etiske retningslinjer innen IKT-sikkerhet

LU-K-4-3 Kandidaten kjenner til forholdet mellom organisasjonsinterne, nasjonale og internasjonale reguleringer

Ferdigheter

LU-F-4-1 Kandidaten kan utføre grunnleggende sjekk av etterlevelse av gjeldende lover, reguleringer, standarder og etiske retningslinjer

Generell kompetanse

LU-G-4-1 Kandidaten kan gjøre rede for de mest sentrale nasjonale, internasjonale og overnasjonale aktører innen IKT-sikkerhetsregulering

LU-G-4-2 **Kandidaten skal kunne diskutere etiske utfordringer knyttet til IKT-sikkerhet** *(generell kompetanse c)*

2.2.5 Trusselmodellering og risikostyring

Kunnskap

LU-K-5-1 Kandidaten forstår den grunnleggende sammenhengen mellom kompleksitet, risiko og sårbarhet

LU-K-5-2 Kandidaten kjenner til ulike typer IKT-angrep

LU-K-5-3 Kandidaten kan gjøre rede for de ulike stadiene og farenivåene av IKT-angrep

Ferdigheter

LU-F-5-1 **Kandidaten kan vurdere hvordan systemer innen sitt fagområde kan bli utsatt for ulike typer IKT-angrep** *(ferdigheter c)*

LU-F-5-2 Kandidaten kan gjennomføre og formidle risiko- og sårbarhetsanalyser

LU-F-5-3 **Kandidaten kan prioritere risiko og lage planer for risikoredusering** *(ferdigheter c)*

Generell kompetanse

LU-G-5-1 **Kandidaten er i stand til å gjennomføre enkle risikovurderinger** *(generell kompetanse d)*

2.2.6 Sikkerhetsarkitektur og innebygd informasjonssikkerhet

Kunnskap

LU-K-6-1 **Kandidaten er kjent med grunnleggende tekniske sikkerhetsmekanismer og deres muligheter og begrensninger** *(kunnskap e)*

LU-K-6-2 **Kandidaten er kjent med behovet for å tenke helhetlig sikkerhet under utvikling, produksjon, drift og avvikling av systemer** *(kunnskap f)*

Ferdigheter

LU-F-6-1 Kandidaten kan bistå med planer for helhetlig sikkerhet innen sitt fagområde

Generell kompetanse

LU-G-6-1 Kandidaten er i stand til å tenke helthetlig sikkerhet innen sitt fagområde

2.3 Utdyping av læringsutbyttebeskrivelsene

Læringsutbyttebeskrivelsene er et godt utgangspunkt for å få en oversikt over hvilke områder av IKT-sikkerhet som bør inngå i en høyere utdanning. Men en slik beskrivelse er ikke nok for å kunne realisere dette konkret i en utdanning. Vi vil derfor her forsøke å utdype de seks temaene og deres læringsutbyttebeskrivelser.

I Vedlegg C er det listet eksterne ressurser hvor dere blant annet finner relevante nettsider, standarder og lover og reguleringer.

2.3.1 Grunnleggende begreper og historisk utvikling

Fagområdet IKT-sikkerhet har hatt en formidabel utvikling fra tidlig 1970-tall og frem til i dag [12]. I denne perioden, har vi lært at det som var sant eller relevant innen IKT-sikkerhet i går, ikke nødvendigvis er sant eller relevant i dag eller i morgen. Risikoer, og måter å håndtere disse på, er i utvikling og de som arbeider med IKT-sikkerhet må hele tiden være oppdatert. Økende tilgjengelig regnekapasitet gjør at sikkerhetsmekanismer som tidligere var umulige eller for ressurskrevende å knekke nå blir sårbare. Dette påvirker de antakelsene som blir gjort når man forsøker å sikre IKT-systemer. I tillegg kan anerkjente verktøy og protokoller i løpet av kort tid vise seg å være problematiske og ha store svakheter. For å vite at dette er en viktig del av det å ha et bevisst forhold til IKT-sikkerhet, så er det å *kjenne til sentrale momenter på den historiske utviklingen innen IKT-sikkerhet* viktig (LU-K-1-1).

Det kan ikke forventes at nye studenter kjenner til grunnleggende begreper innen IKT-sikkerhet. Disse må læres, noe som står i kontrast til for eksempel grunnleggende begreper innen matematikk og fysikk som undervises helt fra barneskolen. Det er altså nødvendig at *de mest sentrale begrepene innen IKT-sikkerhet beherskes* (LU-K-1-2) slik at kandidaten kan *forstå en tekst eller en presentasjon hvor grunnleggende begreper innen IKT-sikkerhet benyttes* (LU-F-1-1).

Det er en utfordring at mye brukte begreper inne IKT-sikkerhet kan ha en upresis og tvetydig mening. Vi ser for eksempel at begrepet sikkerhet på norsk benyttes som en oversettelse av alle de engelske begrepen *security*, *safety* og *certainty*. En slik bruk av ordet sikkerhet gir en upresis mening og vil være en utfordring ved muntlig og skriftlig fremstilling og kommunikasjon. En mulig bedre oversettelse av disse ordene kunne henholdsvis være *sikkerhet*, *trygghet* og *visshet*. En entydig og presis anvendelse av begreper vil være viktig både for å forstå og for å bli forstått. Vi ønsker altså at studentene skal lære å *anvende de mest sentrale begrepene innen IKT-sikkerhet i ulike sammenhenger og skal kunne kommunisere skriftlig og muntlig om IKT-sikkerhet* (LU-F-1-2), og herunder kunne *delta i diskusjoner om IKT-sikkerhet* (LU-G-1-1).

Konkret hvilke begreper som bør inngå vil kunne variere avhengig av hvilke fokus eller vinkling man ønsker på IKT-sikkerhet i utdanningen. Vi vil likevel foreslå noen eksempler på begreper her. Dette er ikke er en komplett liste, men listen inkluderer eksempler på begreper som er sentrale uavhengig av fokus og vinkling på IKT-sikkerhet i utdanningen. Det er utfordrende at det ikke nødvendigvis er enighet i litteraturen om presise definisjoner av de ulike begrepene. Vi ønsker med eksemplene ikke å foreslå at disse er de rette definisjonene av begrepene. Vi ønsker kun å vise frem eksempler på slike begreper og mulige beskrivelser av disse. For eksempel vil beskrivelse av både trussel og risiko du finner her kunne avvike fra den du finner i gode lærebøker.

Selve begrepet sikkerhet, og kanskje spesifikt IKT-sikkerhet (som også kalles digital sikkerhet eller cybersikkerhet), bør diskuteres. Det er også nyttig at forskjellen mellom politikk (retningslinjer) og mekanismer innen IKT-sikkerhet diskuteres.

Den første gruppen av begreper brukes til å kunne kommunisere generelt om IKT-sikkerhet i en eller annen setting. Da trenger man å både forstå hva disse begrepene er og hvordan de beskriver situasjonen:

Begrep	*Beskrivelse*
Sårbarhet	Svakhet som kan utnyttes
Trussel	Potensiell fare (identifisere og bruke en sårbarhet)
Risiko	Sannsynlighet for at en trussel benytter sårbarhet
Eksponering	Et tilfelle av å bli eksponert for tap fra en trussel
Mottiltak	Dempe potensiell risiko

Den nesten gruppen av begreper er de ulike sikkerhetsmålene. Da er det naturlig å ta utgangspunkt i KIT (eventuelt CIA på engelsk). Nesten all litteratur som gir en introduksjon til IKT-sikkerhet inkluderer en beskrivelse av disse sikkerhetsmålene:

Begrep	*Beskrivelse*
Konfidensialitet	Unngå uautorisert tilgang til informasjon
Integritet	Sikre at informasjon ikke er endret eller manipulert
Tilgjengelighet	Informasjon er betimelig tilgjengelig og modifiserbar

I tillegg har vi to grupper med begreper som begge i litteraturen kan omtales som AAA. Det første AAA-gruppen, som også kan omtales som sikkerhetsmål, består av disse begrepene:

Begrep	*Beskrivelse*
Forsikring (assurance)	Gi og forvalte tillit
Autentisitet	Avgjøre om utsagn er genuine (oppriktige/ekte)
Anonymitet	Kan ikke tilskrives enkeltindivider

Det neste AAA-gruppen, som er den mest kjente bruken av AAA innen IKT-sikkerhet, representerer protokoller eller rutiner:

Begrep	*Beskrivelse*
Autentisering	Avgjøre om påstått identitet er ekte eller ikke
Autorisering	Avgjøre tilgang til tjeneste eller ressurs
Regnskap (accounting)	Spore aktiviteter i et system (bruk og hendelser)

I noe litteratur vil vi også finne at revisjon (audit) inkluderes i denne gruppen. Da normalt i betydningen en systematisk evaluering av sikkerheten i et system.

Begrep	*Beskrivelse*
Revisjon (audit)	Systematisk evaluering av sikkerheten i et system

Utover disse så vil mange flere begrep normalt inngå. Noen av disse kommer inn under andre læringsmål og noen vil være naturlig å ta med basert på valgt vinkling og fokus. For eksempel kan det være riktig å tidlig forklare hva som menes med prosesser og aktører (principals) i et system. Også kryptografi, kryptosystemer (både symmetriske og offentlig-nøkkel baserte), enveisfunksjoner, hash-funksjoner, digitale signaturer, digitale sertifikat og PKI vil i noen tilfeller og for noen typer studenter kunne introduseres her.

Det er ulike mulige tilnærminger for å introdusere begrepene og bruk av begrepene til studentene. I mange tilfeller vil det være naturlig å introdusere disse som en del av gjennomgangen av de andre temaene beskrevet nedendfor.

2.3.2 Bevissthet og sikkerhetskultur

Dette temaet har fokus på å lære å bruke digital teknologi på en trygg og forsvarlig måte, nettopp for å unngå å bli et lett offer for angripere, og for å ha bevissthet rundt digital hygiene og ansvarlig bruk av digital teknologi, Internett og sosiale medier.

Individuell adferd kan være avgjørende for hvor sårbart et system er, og for hvor stor risiko det er for at en slik sårbarhet utnyttes. Kultur i en organisasjon styrer mye av den enkeltes adferd, og en god sikkerhetskultur vil kunne være forbyggende mot uheldige hendelser. En sikkerhetskultur er de verdier, holdninger, antakelser, normer og kunnskaper vi har i forhold til våre (digitale) verdier. Disse styrer våre handlinger. Tydelige mål fra ledelsen og kontinuerlige prosesser er viktig for å få på plass en slik sikkerhetskultur i en organisasjon.

Kompetanse er kjernen i en god sikkerhetskultur. Det er nødvendig å kunne *gjøre rede for samfunnets sårbarhet som konsekvens av IKT-sikkerhetsutfordringer* (LU-K-2-1) og ha *en grunnleggende forståelse av trusler og sårbarhet i samfunnet, med særlig vekt på hvordan digitalisering påvirker dette i egen profesjon* (LU-K-2-2).

Slik kunnskap er ikke nok for å kunne forebygge uheldige hendelser i egen organisasjon. Det er også nødvendig å være *i stand til å identifisere og håndtere trusler og sårbarheter på ulike nivå i en organisasjon* LU-F-2-1, *kjenne til en typisk organisering av IKT-sikkerhet i en organisasjon* (LU-F-2-2) og *argumentere for viktigheten av god cyber-hygiene (rutiner og oppførsel), brukeropplæring i IKT-sikkerhet, og bevissthet rundt IKT-sikkerhetstrusler og sårbarheter* (LU-F-2-3). Det er også viktig i en organisasjon å kunne *samarbeide om, og utvise ansvarlighet overfor, IKT-sikkerhet* (LU-G-2-1). Et fokus på det ansvar den enkelte og ledelsen har til være bevisst om IKT-sikkerhet vil kunne være sentralt under dette temaet.

Konkret er det mulig innenfor dette temaet å inkludere en gjennomgang av nøkkelkomponentene i en (digital) sikkerhetskultur[2] og eventuelt en metode for å kartlegge disse [30]. Også de 10 sikkerhetsprinsippene beskrevet av Saltzer og Schroeder [34, 36] kan presenteres og diskuteres her.

[2] https://nettvett.no/digital-sikkerhetskultur/

Det finnes mange gode ressurser på nett og det er ønskelig at de viktigste er kjent og kan brukes av den enkelte. Nasjonal sikkerhetsmyndighet (NSM) er Norges ekspertorgan for informasjons- og objektsikkerhet, og det nasjonale fagmiljøet for IKT-sikkerhet. De er nasjonal varslings- og koordineringsinstans for alvorlige dataangrep og andre IKT-sikkerhetshendelser. NorSIS er en del av regjeringens helhetlige satsing på informasjonssikkerhet i Norge. Målgruppen for NorSIS sine aktiviteter er norske virksomheter i privat og offentlig sektor. Formålet til NorSIS er å bidra til at informasjonssikkerhet blir en naturlig del av målgruppens hverdag gjennom å bevisstgjøre om trusler og sårbarheter, opplyse om konkrete tiltak gjennom nyheter, råd og veiledninger, og påvirke til gode holdninger innen informasjonssikkerhet.

En oversikt over slike norske nettressurser finnes i Vedlegg C.1.

2.3.3 Personvern

Temaet *personvern* kunne vært inkludert både under temaet *bevissthet og sikkerhetskultur* og temaet *lover, reguleringer og etikk*, men fordi personvern har et spesielt fokus, og representerer en viktig problemstilling i den pågående digitaliseringsprosessen i samfunnet, så har vi valgt å organisere dette som et eget tema.

Personvern handler om retten til et privatliv og retten til å bestemme over egne personopplysninger.[3] Dette er forankret i den Den europeiske menneskerettighetskonvensjonen (EMK) og bestemmelse om personvern i Grunnloven §102. Våre anbefalte læringsmål er begrenset til håndtering av personopplysninger.

Det er derfor viktig å ha *kunnskap om når behovet for personvern trer i kraft* (LU-K-3-1) og kjennskap *til viktige lover og regler på området (GDPR, nasjonale lover og regler)* (LU-K-3-3). I tillegg må man kunne *vurdere om et system forvalter sensitive persondata* (LU-F-3-1) og *anvende viktige lover og regler på området* i en slik setting (LU-F-3-3).

I tillegg til denne bevisstheten om personvern og de lover og reguleringer som gjelder, så er det viktig å kunne *identifisere behov for beskyttelse av persondata* (LU-F-3-2) og ha en overordnet forståelse av *typiske tilnærminger for beskyttelse og anonymisering av persondata* (LU-K-3-2).

Til slutt er det viktig å forstå *hvorfor personvern er spesielt viktig i et samfunn med stadig økende digitalisering* (LU-G-3-1) og hvor man kan finne oppdatert informasjon om dette.

Også knyttet til personvern finnes det gode spesifikke ressurser på nett. En god plass å starte er hos Datatilsynet. Datatilsynet er både tilsyn og ombud. Oppgaven til Datatilsynet er å føre kontroll med personvernregelverket og medvirke til at enkeltpersoner ikke blir krenket gjennom bruk av opplysninger som kan knyttes til dem. Deres web-side er en god ressurs til alt som har med personvern å gjøre. Det er også mulig å finne mange ressurser på nett om konsekvensene for personvern som følge av GDPR [7] og Personopplysningsloven [18].

Se Vedlegg C.1 og C.3 for relevante norske nettsider og lover og reguleringer knyttet opp mot personvern.

2.3.4 Lover, reguleringer, etikk og standarder

Temaet *lover, reguleringer og etikk* vil fort kunne få et fokus på hvordan finne frem i og bruke eksisterende lovverk og andre reguleringer. Det viktigste er at studentene skal ha en overordnet forståelse av hvordan disse regulerer utvikling og bruk av IKT-systemer og at de skal kunne reflektere over etiske prinsipper for god teknologi.

Lover og forskrifter regulerer utvikling og bruk av IKT-systemer, mens standarder ofte inngår i en kravspesifikasjon i slike systemer. Det er derfor viktig å kunne *gi en oversikt over de mest relevante lover, forskrifter og standarder for IKT-sikkerhet, og deres anvendelse innenfor eget fagområde* (LU-K-4-1) og *utføre grunnleggende sjekk av etterlevelse av gjeldende lover, reguleringer* og *standarder* (LU-F-4-1).

Etikk handler om hva som er rett og galt å gjøre i ulike situasjoner, gjerne uavhengig av lover og reguleringer. Fordi IKT har en dominerende tilstedeværelse i våre liv og i vårt samfunn, så vil etikk knyttet til IKT og IKT-sikkerhet være særs viktig. Vi ønsker derfor at studenter skal lære seg å *gjøre rede for behovet for etiske retningslinjer innen IKT-sikkerhet* (LU-K-4-2) og kunne *utføre grunnleggende sjekk av etterlevelse av etiske retningslinjer* (LU-F-4-1). De skal også *kunne diskutere etiske utfordringer knyttet til IKT-sikkerhet* (LU-G-4-2).

Organisasjonsinterne, nasjonale og internasjonale reguleringer virker på ulike nivå og har forskjellig prioritet. For eksempel kan ikke en organisasjonsintern regel overprøve nasjonale lover i det landet organisasjonen har sitt virke. Det er derfor viktig å kjenne *til forholdet mellom organisasjonsinterne, nasjonale og internasjonale reguleringer* (LU-K-4-3) og kunne *gjøre rede for de mest sentrale nasjonale, internasjonale og overnasjonale aktører innen IKT-sikkerhetsregulering* (LU-G-4-1).

[3] https://www.datatilsynet.no/rettigheter-og-plikter/hva-er-personvern/

Overnasjonale aktører kan treffe avgjørelser som er bindende for alle medlemsland, også de som ikke selv stemte for avgjørelsen. EU er eksempel på en slik aktør.

De er et stort spenn av lover og reguleringer som er relevante i forbindelse med IKT-sikkerhet. GDPR [7] i Europa og Personopplysningsloven [18] i Norge er sentrale slike reguleringer som studenter bør få en viss kjennskap til. For GDPR og Personopplysningsloven er artikkel 5 fra kapittel II i GDPR som beskriver *Prinsipper for behandling av personopplysninger*, et godt utgangspunkt for å forstå hva denne reguleringen innebærer for behandling av personopplysninger. Andre lover og forskrifter som kan være relevante er Lov om nasjonal sikkerhet (sikkerhetsloven) [19], Lov om rett til innsyn i dokument i offentleg verksemd (offentleglova) [15], Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) [23] og Lov om elektronisk kommunikasjon (ekomloven) [22]. Det kommer også flere lover og forskrifter fra EU som kan være relevant, inklusiv Cybersikkerhetsforordningen [8], Forordningen om eID og elektroniske tillitstjenester [5] og NIS-direktivet (Network and Information Security) [6, 9].

I Vedlegg C.3 listes relevante lover og reguleringer.

Det finnes ulike nasjonale og internasjonale standarder som er relevante. I Norge har vi Standard Norge som er det norske medlemmet i Den europeiske standardiseringsorganisasjon (CEN) og Den internasjonale standardiseringsorganisasjonen (ISO). Norsk standard (NS) er en benevnelse på standarder fastsatt og utgitt av Standard Norge. Disse inkluderer internasjonale standarder som adoptert i Norsk Standard.

Det finnes mange standarder som er relevant for IKT-sikkerhet, inklusive standarder for risikovurderinger, kvalitetssikring, bruk av kryptosystemer og utvikling av web-applikasjoner. Noen eksempler på standarder eller anbefalinger som ofte trekkes frem er NS-ISO 31000 og NS-ISO 31010 (risikostyring), NS 5814 (risikovurdering), NS 583X-serien (tilsiktede uønskede handlinger), ISO 27000 (IT-sikkerhet), OWASP (The Open Web Application Security Project) og FIPS 140-2 fra USA (US Security Requirements for Cryptographic Modules).

I Vedlegg C.4 listes relevante standarder, anbefalinger og metoder.

2.3.5 Trusselmodellering og risikostyring

Det fins svært mange trusselaktører med motivasjon og kapasitet til å angripe IKT-systemer og infrastruktur. En grunnleggende faktor for beskyttelse er derfor å forstå og forsøke å forutsi hvordan trusselaktører vil angripe, noe som kalles trusselmodellering. Dette gir et grunnlag for å kunne håndtere relevante trusler.

Et utgangspunkt for trusselmodellering og risikostyring er å forstå *den grunnleggende sammenhengen mellom kompleksitet, risiko og sårbarhet* (LU-K-5-1). Videre vil det på et overordnet nivå å kjenne *til ulike typer IKT-angrep* (LU-K-5-2) og *de ulike stadiene og farenivåene av IKT-angrep* (LU-K-5-3) være viktig for å kunne *vurdere hvordan systemer innen sitt fagområde kan bli utsatt for ulike typer IKT-angrep* (LU-F-5-1). En slik vurdering kan være særs krevende, og for de fleste studenter vil målet her kun være å få en overordnet forståelse av området og overordnet forståelse behovet for planlegging og tiltak på dette området. Neste steg er å kunne *gjennomføre og formidle risiko- og sårbarhetsanalyser* (LU-F-5-2) og *prioritere risiko og lage planer for risikoredusering* (LU-F-5-3). Også her vil målet for de fleste studentene være å få en overordnet forståelse for temaet, gjerne gjennom eksempler relevant for deres fagområde. De er likevel ønskelig at de skal være *i stand til å gjennomføre enkle risikovurderinger* (LU-G-5-1) av eksempler fra eget fagområde. Dette vil gi en bevissthet rundt trusler, sårbarhet og risiko som er nødvendig for den digitaliserte hverdagen de senere skal virke i.

Det viktig å lære er prinsippene for trusselmodellering og risikoanalyse. Trusselmodellering forsøker å identifisere sårbarheter som kan utnyttes og bli en trussel utnyttet av en trusselaktør (angriper). Konsekvensene av at en sårbarhet utnyttes er en risiko. Et risikonivå gir uttrykk for kombinasjonen av sannsynligheten for, og konsekvensen av, en uønsket hendelse (en sårbarhet som utnyttes). Risikoanalysen brukes som grunnlag for å innføre mottiltak (det vil si å fjerne sårbarheter) som skal blokkere eller redusere de mest alvorlige truslene. Risikostyring er betegnelsen som samlet omfatter trusselmodellering, risikoanalyse og innføring av mottiltak.

NSMs grunnprinsipper for IKT-sikkerhet[4] [31] er organisert i 4 kategorier:

1. Identifisere og kartlegge
2. Beskytte og opprettholde
3. Oppdage
4. Håndtere og gjenopprette

[4] https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/

Det er naturlig å tenke at temaet trusselmodellering og risikostyring kun tilhører kategori 1. Det er ikke tilfelle. Vi må innom alle kategorier fordi vi må analysere og planlegge for aktiviteter i alle disse kategoriene. Og i tilfeller ved hendelser eller ny informasjon og kunnskap, så må vi oppdatere og vedlikeholde våre trusselmodeller og risikoanalyser.

Som nevnt under temaet *lover, regler og etikk*, så finnes det norske standarder for risikovurdering og risikostyring. I tillegg finnes det ulike modeller og metodikk som kan brukes for å gå dypere inn i problematikken. Hvilke tilnærming man velger og hvor dypt man går avhenger av studentenes fagområde og hvor omfattende fordypning innenfor temaet som er mulig og ønskelig i deres utdanninger.

I Vedlegg C.4 listes, blant annet, norske standarder for risikovurdering og risikostyring.

2.3.6 Sikkerhetsarkitektur og innebygd informasjonssikkerhet

Utvikling og bruk av IKT-systemer må foregå etter prinsippene om innebygd informasjonssikkerhet. Begrepet *innebygd* betyr simpelthen at informasjonssikkerhet må inkluderes i kravspesifikasjon, design, koding (realisering), testing, produksjonssetting, forvaltning og avvikling av alle systemer, produkter og tjenester som har IKT-komponenter. En forutsetning for at dette skal være mulig er at informasjonssikkerhet inngår i opplæring av fagfolk, ingeniører og teknologer som bygger, drifter og bruker slike IKT-systemer.

Det er derfor viktig at studentene blir *kjent med behovet for å tenke helhetlig sikkerhet under utvikling, produksjon, drift og avvikling av systemer* (LU-K-6-2), *kan bistå med planer for helhetlig sikkerhet innen sitt fagområde* (LU-F-6-1) og *er i stand til å tenke helthetlig sikkerhet innen sitt fagområde* (LU-G-6-1).

Det er umulig å tenke helhetlig sikkerhet hvis man ikke har en overordnet forståelse for eksisterende sikkerhetsmekanismer. Studentene bør altså bli kjent med de *grunnleggende tekniske sikkerhetsmekanismer og deres muligheter og begrensninger* (LU-K-6-1). Det betyr å ha en overordnet forståelse av ulike typer kryptering (ulike kryptosystemer) og deres bruksområder, inklusiv å forstå de ulike egenskapene til symmetrisk og offentlig-nøkkel basert kryptering. Det er også viktig å ha en overordnet forståelse av digitale signaturer, digitale sertifikater, PKI, sertifikatautoriteter (CA) og sikkerhetsprotokoller. Dette kan gjerne illustreres med kjente mekanismer og protokoller som HTTPS (TLS) og protokoller for autentisering. Hvor omfattende man behandler disse mekanismene vil kunne variere avhengig av studentenes bakgrunn og fagområde.

Kapittel 3

Integrasjon av læringsmål i utdanninger

3.1 Innledning

Det å utvikle læringsmål innen IKT-sikkerhet som alle teknologi- og realfag-utdanninger skal inkludere i sine utdanninger er kun en del av et større arbeid med å få disse læringsmålene inn i utdanningene. Det neste steget er å planlegge hvordan disse læringsmålene skal integreres i utdanningene. Dette er et vanskelig arbeid, spesielt for eksisterende utdanninger hvor studieplaner er etablert og hvor det er et stort press på å få inn ulike tema i utdanningene.

Et av målene med dette kapitlet er at det skal kunne være et nyttig verktøy for utdanningsinstitusjonene når de skal jobbe med integrasjon av de anbefalte læringsmålene i IKT-sikkerhet i utdanningene.

3.2 Utfordringer med å integrere IKT-sikkerhet i ulike utdanninger

Det er mange ulike faktorer som påvirker hvordan man vellykket integrerer læringsmålene for IKT-sikkerhet i en utdanning. Før vi kommer frem til noen konkrete forslag vil vi diskutere noen av utfordringene vi finner når vi forsøker å integrere IKT-sikkerhet i ulike utdanninger. Disse utfordringene må tas hensyn til i arbeidet med denne integrasjonen.

Følgende utfordringer kan man støte på når man arbeider med å integrere IKT-sikkerhet i en studieplan:

- Det er utfordrende å få plass til nye tema i en eksisterende studieplan. Skal de ulike temaene i IKT-sikkerhet gis i egne emner eller være inkludert i eksisterende emner? Er det i så fall rom for nye emner eller er det rom for nye tema i eksisterende emner.
- Ulike tema innen IKT-sikkerhet krever ulik modning og fagforståelse i eget fagområde, og det er krevende å vite når i utdanningen et tema bør introduseres. Det betyr også at det i en utdanning vil kunne være fornuftig å komme tilbake til temaene knyttet IKT-sikkerhet flere ganger i løpet av utdanningen.
- Det er utfordrende å lære IKT-sikkerhet til studenter som ikke har informatikkbakgrunn. Kunnskap om informatikk er et naturlig utgangspunkt for flere av temaene rundt IKT-sikkerhet. Det er også vanskelig å henge ny kunnskap på eksisterende knagger når studenter har begrenset med personlig erfaringer knyttet til informatikk og IKT-sikkerhet.
- Det kan være vanskelig å motivere studenter til å arbeide med de ulike temaene innen IKT-sikkerhet fordi de ikke virker relevante for eget fagområde. Det er en risiko for at studenter ikke klarer å innarbeide IKT-sikkerhet i sin fagforståelse, og i stedet pugger IKT-sikkerhet som fragmenterte kunnskapsenheter.
- IKT-sikkerhet i eget fagområde mangler ofte relevante historier og gode eksempler, blant annet fordi vi er midt inne i en rivende teknologisk utvikling, og denne teknologiske utviklingen finner vi også i fagområdet studentene studerer. En slik felles bakgrunnskompetanse, som slike historier og eksempler representerer, kan være nødvendig for å bygge ny forståelse. Offentlig kjente sikkerhetskriser kan oppfattes irrelevante og derfor overfladiske (studentene kjenner seg ikke igjen).
- Faglærere på en utdanning har nødvendigvis ikke rett kunnskap, bakgrunn eller motivasjon for å undervise temaene knyttet til IKT-sikkerhet. Det kan være nødvendig å løfte faglærernes kunnskap på området gjennom opplæring, ved å gi rom for at de selv kan tilegne seg denne kunnskapen, ved nyansettelser, eller ved samarbeid med andre enheter som kan bidra her.

En av de vanligste tilbakemelding arbeidsgruppen har fått, når vi presenterte læringsmålene for IKT-sikkerhet som bør inn i alle teknologi- og realfag-utdanninger, er at det vil være utfordrende å få plass til dette i eksisterende utdanninger. En slik tilbakemelding kan avvises, enten med å si at IKT-sikkerhet er en del av rammeplanen (som for eksempel i ingeniørutdanningene) og at det derfor *må* ryddes plass til temaene, eller ved å understreke hvor viktig IKT-sikkerhet er også i denne utdanningen som en følge av digitaliseringen av samfunnet. Vi tror likevel at en bedre tilnærming er å diskutere mulige forslag for hvordan dette kan gjøres i eksisterende utdanninger og vise at en integrasjon av IKT-sikkerhet i utdanningen vil gi kandidater med relevant og oppdatert kunnskap i eget fagområde. Vi ønsker blant annet å vise til konkrete forslag og eksempler på hvordan noen utdanningsinstitusjoner får til en vellykket integrasjon av IKT-sikkerhet i sine utdanninger. Forslagene og eksemplene vi presenterer kan være gode verktøy for en utdanningsinstitusjon som skal gjøre det krevende arbeidet det kan være å integrere IKT-sikkerhet i eksisterende utdanninger.

En annen type utfordring er tilgjengelig læremateriell. I dag er det mulig å finne generiske lærebøker som dekker de læringsmålene i IKT-sikkerhet vi anbefaler. Det er publisert flere slike lærebøker i perioden arbeidsgruppen har virket, og det er godt mulig at tilfanget vil øke ytterligere nå som disse læringsmålene er publisert. Men utfordringen er å finne læremateriell som gjør denne kunnskapen relevant for de ulike fagområdene. Denne utfordringen, og mulige tilnærminger for å løse dette, blir diskuter nærmere i neste kapittel om læremateriell.

3.3 Ulike tilnærminger til å integrere IKT-sikkerhet i utdanningene

Det er mulig å tilby de ulike anbefalte læringsmålene i IKT-sikkerhet i en utdanning, enten i egne emner eller som en del av innholdet i andre emner. For noen utdanninger vil en kombinasjon av disse tilnærmingene også være mulig. Det å etablere egne emne med IKT-sikkerhet-temaene kan være særs vanskelig i mange utdanninger. I noen utdanninger med fagkombinasjoner som er nært opp til temaene i IKT-sikkerhet, som for eksempel i informatikk- og matematikk-tunge utdanninger, så vil det være enklere å se for seg egne emner med disse temaene. Det er også mulig å se for seg utdanninger hvor noen studenter velger en fordypning som inkluder mer IKT-sikkerhet, og muligens da også med egne emner i IKT-sikkerhet.

Hvis et studiested har tilgang på fagmiljø med IKT-sikkerhetskompetanse, så kan det være ønskelig å utnytte dette. Da kan det være mulig å plukke eksisterende emner, eller deler av emner fra dette fagmiljøet til den studieplanen man utvikler. Dette er en god utnyttelse av eksisterende ressurser og man sikrer at et fagmiljø som behersker temaene har ansvaret for disse. Utfordringen med en slik tilnærming er å gjøre disse temaene relevante og fagspesifikke nok for den gitte utdanningen. Hvis ikke, så kan det være vanskelig å motivere studentene til arbeide med temaene og forstå de i sammenheng med eget fagområde.

Mange av de anbefalte læringsmålene i IKT-sikkerhet egner seg som tema i emner som vi finner i eksisterende studieplaner. Emnene må revideres slik at disse temaene er inkludert, men det er i mange tilfeller mulig uten at studieplanene bygges helt om. For eksempel vil mange ingeniørutdanninger kunne inkludere læringsmål fra de fire første temaene i IKT-sikkerhet i *Ingeniørfaglig basis* (tidligere fellesemner). Disse temaene er:

1. Grunnleggende begreper og historisk utvikling
2. Bevissthet og sikkerhetskultur
3. Personvern
4. Lover, reguleringer, etikk og standarder

Noen av disse temaene vil det også være naturlig å komme tilbake til senere i utdanningene når studentene er mer modne og har en større fordypning i eget fagområde. Eksempel på det er *Bevissthet og sikkerhetskultur* innen eget fagområde og *Lover, reguleringer, etikk og stadarder* relevante for fagområdet studentene studerer.

De to siste temaene er:

5. Trusselmodellering og risikostyring
6. Sikkerhetsarkitektur og innebygd informasjonssikkerhet

Disse vil normalt egne seg bedre senere i en utdanning. De bør knyttes sterkere opp til eget fagområde og de bør inkludere eksempler som studentene finner relevante. Det er også mulig at de vil kunne kreve læremateriell som er mer tilpasset fagområdet til utdanningen.

De er ikke bare den praktiske organiseringen av å få læringsmålene integrert i en utdanning som må vurderes. Også hvilke fokus man har, og hvor dypt man går inn i de ulike temaene, må tilpasses de ulike utdanningene. For eksempel så vil

Trusselmodellering og risikostyring i noen utdanninger inkludere metoder og verktøy for detaljerte analyser og beskrivelser av tiltak, mens det i andre utdanninger mer handler om å forstå det overordnede trusselbildet og eksempler på håndtering av risikoen dette fører med seg. I praksis betyr dette at hvor dypt man går inn i de ulike læringsmålene vil kunne variere mellom utdanninger.

3.4 Gjøre IKT-sikkerhet relevant for faget

Det er to grunner til å forsøke å gjøre temaene innen IKT-sikkerhet relevant for spesifikke utdanninger:

1. Studentene blir mer motivert for å jobbe med, og lære seg, temaene.
2. Det studentene lærer seg er mer relevant, og dermed også viktigere, for fagområdet deres.

I praksis betyr det å synliggjøre hvorfor læringsmålene fra IKT-sikkerhet er viktige på de ulike fagområdene og hvordan vi kan finne disse læringsmålene igjen i praktisering av faget. En god tilnærming for å få til dette er å hente eksempler fra faget og bruke disse i undervisning og i oppgaver og øvinger.

For å få dette til så kan det være nødvendig å sette seg inn og forstå arbeidshverdagen til utdannede kandidater, inklusiv de systemer og verktøy de blir eksponert for. En del av de systemer og verktøy de må beherske vil være generelle og gjelde for mange ulike utdanninger. I disse tilfellene kan man ha en liknende tilnærming til de relevante temaene innen IKT-sikkerhet i disse utdanningene. Andre systemer og verktøy vil være unike for spesifikke utdanninger. I slike tilfeller kan det være nødvendig å finne tilpassede eksempler og fremstillinger for å gjøre temaene relevante.

3.5 Integrere IKT-sikkerhet i ingeniørutdanningene

Arbeidsgruppen startet arbeidet sitt med utgangspunkt i retningslinjene for ingeniørutdanningene fra 2011 [39]. I disse retningslinjene er ikke IKT-sikkerhet nevnt, men vi tok utgangspunkt i utdanningens struktur for å finne plass til disse temaene i utdanningene:

- 30 studiepoeng *fellesemner* som består av grunnleggende matematikk, ingeniørfaglig systemtenkning og innføring i ingeniørfaglig yrkesutøvelse og arbeidsmetoder. Emnene i fellesemner er felles for alle studieprogram.
- 50 studiepoeng *programemner* som består av tekniske fag, realfag og samfunnsfag. Programemner er felles for alle studieretninger i et studieprogram.
- 70 studiepoeng *tekniske spesialiseringsemner* som gir en tydelig retning innen eget ingeniørfag, og som bygger på programemner og fellesemner.
- 30 studiepoeng *valgfrie emner* som bidrar til faglig spesialisering, enten i bredden eller dybden.

På tvers av inndelingen over, definerer retningslinjene flere støttefag med felles læringsmål og omfang langt utover fellesemnene. Dette gjelder særlig matematikk (10 studiepoeng i tillegg til 10 studiepoeng i fellesemne), statistikk (5 studiepoeng) og fysikk/kjemi (10 studiepoeng).

Vi startet derfor med å plassere IKT-sikkerhet innenfor dette bildet. Vi kom frem til felles læringsmål for alle ingeniørutdanninger, men som diskutert ovenfor så kan det likevel bety at man har ulik fordypning eller ulikt fokus i de forskjellige ingeniørutdanningene.

De seks temaene i IKT-sikkerhet som arbeidsgruppen har identifisert er i stor grad universelle for alle programområder i ingeniørutdanningene og kan knyttes til det som kalles «yrkesutøvelse» og «systemtenkning» under fellesemnene. I retningslinjene finner vi vedleggene *Eksempel på læringsutbyttebeskrivelse for Innføring i ingeniørfaglig yrkesutøvelse og arbeidsmetoder* (vedlegg 4) og *Eksempel på læringsutbyttebeskrivelse for Ingeniørfaglig systemtenkning* (vedlegg 5). Med utgangspunkt i disse eksemplene har vi vist at det er en naturlig og logisk sammenheng mellom sentrale læringsmål innenfor IKT-sikkerhet og eksisterende læringsmål knyttet til ingeniørdannelse i retningslinjene (se Vedlegg B.5).

I nye Nasjonale retningslinjer for ingeniørutdanning fra 2020 [38] er IKT-sikkerhet et eget punkt under delkapitlet *IKT, programmering og IKT-sikkerhet*. Dette punktet er basert på innspill fra arbeidsgruppen.

Ifølge ny Forskrift om rammeplan for ingeniørutdanning fra 2018 [25] må en kandidat for å oppnå graden bachelor i ingeniørfag ha bestått minst 180 studiepoeng bestående av:

- 30 studiepoeng *ingeniørfaglig basis* med grunnleggende matematikk, ingeniørfaglig systemtenkning og innføring i ingeniørfaglig yrkesutøvelse og arbeidsmetoder. Dette skal i hovedsak relateres til ingeniørutdanningen og legge grunnlaget for ingeniørfaget.

- 50–70 studiepoeng *programfaglig basis* med tekniske fag, realfag og samfunnsfag. Dette skal i hovedsak relateres til studieprogrammet og legge grunnlaget for fagfeltet.
- 50–70 studiepoeng *teknisk spesialisering* som gir en tydelig retning innen eget fagfelt, og som bygger på ingeniørfaglig basis og programfaglig basis. Dette skal i hovedsak relateres til studieretningen og legge grunnlaget for fagområdet. Bacheloroppgaven inngår i teknisk spesialisering.
- 20–30 studiepoeng *valgfri emner* som bidrar til videre faglig spesialisering, enten i bredden eller dybden.

I retningslinjene finner vi også følgende:

> *Ingeniørfaglig basis* skal i hovedsak relateres til ingeniørutdanningen og legge grunnlaget for ingeniørfaget. Deler av matematikken, ingeniørfaglig systemtenkning og innføring i ingeniørfaglig yrkesutøvelse og arbeidsmetoder skal sammen utgjøre en ingeniørfaglig basis som gir studentene et felles grunnlag for ingeniørprofesjonen.

For IKT-sikkerhet vil dette bety at mange ingeniørutdanninger vil kunne inkludere læringsmål fra de fire første temaene for IKT-sikkerhet i Ingeniørfaglig basis. Noen av læringsmålene fra disse temaene vil det også være naturlig å komme tilbake til senere i utdanningen når studentene er mer modne og har en større fordypning i eget fagområde.

Med hensyn på hvordan IKT-sikkerhet integreres i ingeniør-utdanningene så er det også vært å legge merke til denne formuleringen i retningslinjene:

> Ifølge studietilsynsforskriften er forventet arbeidsbelastning per studiepoeng 25–30 timer. Hvis integrering av forskjellige kvalifikasjoner er vellykket vil studiepoeng tjene mer enn ett formål. Hvis for eksempel matematikk formidles som et verktøy for å løse et bærekraftsproblem, eller IKT-sikkerhet inngår i et ingeniørfaglig prosjekt, vil samlede studiepoeng bidra til læringsutbytte både i matematikk, bærekraft, IKT-sikkerhet og prosjektarbeid.

Konsekvensen er at man ikke trenger å tenke på IKT-sikkerhet som egne autonome emner eller deler av emner. Noen av læringsmålene i IKT-sikkerhet kan oppnås som en integrert del av andre kvalifikasjoner som skal oppnås i utdanningen. Dette er også ofte en bedre måte for studentene å nå læringsmålene i IKT-sikkerhet fordi den faglige relevansen blir mer synlig når IKT-sikkerhet knyttes så sterkt opp til de andre kvalifikasjonene studentene skal oppnå.

Se også en diskusjon om IKT-sikkerhet som ingeniørdannelse i Vedlegg B.6.

3.6 Erfaringer og eksempler fra ingeniørutdanninger

Erfaringene vi har samlet her kommer fra ingeniørutdanninger som medlemmer av arbeidsgruppen enten er direkte involvert i eller hvor de har god tilgang til de som tilbyr dette i egen organisasjon. Disse erfaringene er presentert i noe ulik form, men fordi all erfaring de representerer kan være nyttig for de som skal arbeide med integrasjon av læringsmål fra IKT-sikkerhet i utdanninger, så velger vi å ikke omarbeide tekstene til en fells fremstillingsform og på den måten risikere å begrense omfanget av erfaringsdelingen.

3.6.1 UiT i Narvik

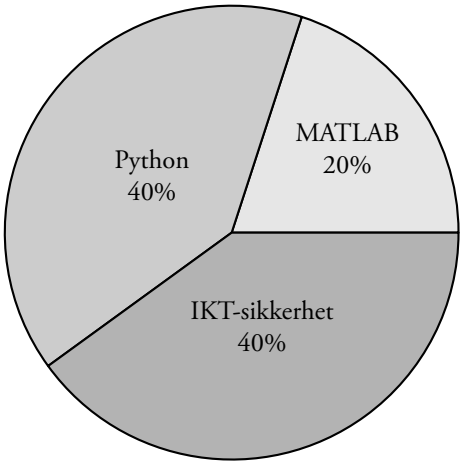
I 2014 startet Høgskolen i Narvik, nå en del av UiT Norges arktiske universitet (UiT), med emnet «Beregningsorientert programmering og statistikk» som et 10 studiepoengs emne i første semester i først år av alle bachelorutdanninger. Dette emnet var et fellesemne og ment å være starten på integrering av programmering inn i alle emner ved samtlige ingeniørdisipliner ved Fakultet for ingeniørvitenskap og teknologi (IVT). Tanken her var teknisk programmering som kunne anvendes i problemløsning for samtlige disipliner. Emnets innhold hadde klassisk statistikk på 5 studiepoeng og 5 studiepoeng med programmering hvor 2 studiepoeng av disse utgjorde programmering med bruk av regneark og 3 studiepoeng med verktøy som MATLAB og Octave.

Visjonen var at de ulike disipliner skulle bidra med problemstillinger egnet for problemløsning med verktøyene. Det ble gjort fremstøt mot de ulike disipliner for å innhente bidrag, men responsen uteble. Hensikten var å kunne illustrere relevante problemstillinger fra de ulike disipliner slik at emnet kunne være relevant for alle studenter. Videre var det også en kobling mellom statistikk og den beregningsorientert delen hvor man kunne anvende verktøyene regneark og

MATLAB/Octave til å løse statistikkutfordringer. Koblingen mellom statistikk og beregningsorientert programmering fungerte godt.

Emnet har vært under konstant forbedring siden starten. Emnet var også grunnlag for en innvilget søknad til den gang Norgesuniversitetet (DIKU) i 2016. Omkring 2018/2019 kom diskusjonen rundt endringer i utdanningene for å finne plass til IKT-sikkerhet opp til overflaten. Denne diskusjonen, sammen med oppmykning i rammeplanen for ingeniørutdanninger, ledet til at man valgte å skille statistikk ut fra den beregningsorienterte delen og tanken var å plassere grunnleggende moduler med IKT-sikkerhet i et fellesemne. Modulene med regneark ble tonet ned og noe av MATLAB/Octave ble tonet ned for å gi plass til IKT-sikkerhet. Samlet sett ble det plass til omtrent 1 til 1,5 studiepoeng IKT-sikkerhet i denne runden. «IKT-sikkerhet» ble i denne runden hentet fra et eksisterende emne på studieretning Datateknikk, «Datakommunikasjon og Sikkerhet». Utvalgte grunnleggende moduler herfra ble benyttet. Grunnet COVID-19 situasjon og utfordringer med bemanning/sykemelding har endringstakten i emnet bremset opp noe. Visjonen for emnet er fortsatt den samme.

Utviklingen går videre og nå er Beregningsorientert programmering et selvstendig emne på 5 studiepoeng. Visjonen for emnet er at det fortsatt skal inneholde beregningsorientert programmering med anvendelser fra ulike disipliner, men fra 2022 vil det være en omlegging hvor regneark erstattes i sin helhet og MATLAB/Octave tones ytterligere ned for å gi plass til grunnleggende opplæring i Python og IKT-sikkerhet. IKT-sikkerhet vil få større plass.



Tanken er nå at de grunnleggende elementene i fra IKT-sikkerhet skal ligge i dette emnet siden det er et felles emne for alle disipliner. Dette vil gi en innføring for å dekke de grunnleggende temaene for læringsutbytte: 1. Grunnleggende begreper og historisk utvikling, 2. Bevissthet og sikkerhetskultur, 3. Personvern, 4. Lover, reguleringer, etikk og standarder. For de resterende to temaene; 5. Trussel modellering og Risikostyring og 6. Sikkerhetsarkitektur og innebygde informasjonssikkerhet, er det stor forskjell mellom de ulike disipliner hvor langt man har kommet med å implementere dette. Her er det tenkt at de ulike disipliner må implementere dette i sine fagspesifikke emner. For studieretning Datateknikk vil dette allerede ligge implementert i emner som Datakommunikasjon og sikkerhet, men for disipliner som Elektroteknikk, Maskin, Prosess, Industriteknologi, Bygg er det per nå lite til ingen fokus på temaene 5 og 6. Diskusjonen om hvordan dette skal løses har begynt å komme til overflaten for disse disipliner.

3.6.2 HVL i Bergen

I 2019 og 2020 har ingeniørutdanningene på fakultet for ingeniør- og naturvitskap ved Høgskulen på Vestlandet (HVL) hatt et prøveprosjekt med integrasjon av IKT-sikkerhet i utdanningene basert på læringsmålene for IKT-sikkerhet fra Nasjonal arbeidsgrupp for styrkning av IKT-sikkerhet i utdanningene.

Utgangspunktet for prosjektet har vært å se på hvordan man kan introdusere et felles undervisningsopplegg for studentene, som blir gjennomført innenfor de eksisterende rammene for de ulike ingeniørutdanningene men uten å fortrenge eksisterende emner eller tema. Samtidig har det også vært en forutsetning at det skal være rom for å tilpasse eller relatere læringsmålene til eksempler som er relevante på hver enkelt utdanning.

Organisatorisk ble undervisningen lagt opp som en felles del av det ingeniørfaglige innføringsemnet som er obligatorisk for alle utdanningene. Undervisningen var nettbasert for å kunne tilpasses studentgrupper på flere campus og med ulike timeplaner. Det ble gjort en vurdering av omfanget av undervisningen sånn at den totale innsatsen i innføringsemnet

ikke skulle være mye større enn det som var utgangspunktet før prosjektet startet. Etter en totalvurdering ble undervisningsmodulen i IKT-sikkerhet på til sammen 3 undervisningsuker, og dette gikk parallelt med andre aktiviteteter i emnet. Det ble overlatt til hvert enkelt studieprogram å tilpasse andre aktiviteter sånn at total arbeidsmengde i perioden ble overkommelig.

Basert på de seks temaene som er foreslått av arbeidsgruppen valgte vi å lage et undervisningsopplegg som dekket over temaene slik:

- Uke 1: Grunnleggende begreper og historisk utvikling / Bevissthet og sikkerhetskultur
- Uke 2: Personvern / Lover, reguleringer, etikk og standarder
- Uke 3: Trusselmodellering og risikostyring / Sikkerhetsarkitektur og innebygd informasjonssikkerhet

Studentene fikk en flervalgstest etter at opplegget var ferdig med krav til oppnåelse for å få bestått, og denne testen representerte de felles kunnskapene vi ønsket at studentene skulle sitte igjen med.

I tillegg fikk studentene et prosjekt som skulle løses i grupper der tema var en enkel sikkerhetsanalyse av et informasjonssystem som var relevant for hver enkelt utdanning. Forslag til case ble hentet fra de ulike fagmiljøene.

Formålet med prosjektet var å få studentene til å operasjonalisere kunnskapene sine.

Erfaringene våre med dette opplegget er at det nok representerer et slags minimum i forhold til hvor mye tid man trenger for å introdusere de ulike temaene i IKT-sikkerhet. Samtidig var det et opplegg som det var mulig å få til innenfor rammene av et eksisterende emne, noe som var en stor fordel. Videre mener vi at opplegget dessverre ikke gir særlig god dybde i kunnskapene til studentene, men at mange ser ut til å sitte igjen med i det minste noe kjennskap til sentrale begreper og teknikker inennfor de ulike temaene.

Totalt sett tenker vi at prosjektet var relativt vellykket, og at vi fikk formidlet viktige kunnskaper til studentene. Samtidig erfarte vi at det er en krevende øvelse å skulle introdusere større opplegg på tvers av utdanninger som i utgangspunktet ikke har noen naturlig plass til et nytt emne. Integrasjon av IKT-sikkerhet i utdanningene blir dermed gjenstad for kompromisser med tanke på omfang og kvalitet.

3.6.3 NTNU i Ålesund

Det eneste tilbudet i informasjonssikkerhet ved NTNU i Ålesund er et valgemne ved dataingeniørstudiet. For øvrig avventer studieprogrammene nye fellesemner og retningslinjer fra det sentrale forvaltningsorganet. De eksemplene som er presentert her, ble samlet inn ved starten av komitéens arbeide for å illustrere hvor informasjonssikkerhet finner en naturlig plass som en del av ingeniørstudiet.

Eksemplene kommer fra en samtale med Terje Tvedt, koordinator for byggingeniørutdannelsen ved NTNU i Ålesund. Han understreket at IKT-sikkerhet som fag slik det er presentert av data- og elektromiljøene, er langt fra relevant for byggingeniørene. Det krever altfor mye tid å lære nok til å ha nytte av det. Derimot er vi enige om en overordnet sikkerhetskompetanse som er viktig.

Terje understrekte at IKT-sikkerheit som fag slik det er presentert av data- og elektromiljøa er langt frå relevant for byggingeniørane. Det krev alt for mykje tid å lera nok til å ha nytte av det. Derimot er me samde om ein overordna sikkerheitskompetanse som er viktig.

Scenario 1: Økonomidata, t.d. anbodsbudsjett

Byggingeniørar, som alle andre ingeniørar, er ofte med på å utvikla budsjett og anbod for nye prosjekt. Kostnadskalkylane er svært utsett for industrispionasje, fordi andre aktørar som kjenner konkurrentane sine budsjett kan tilpassa sine eigne anbod.

Behovet for å halda økonomidata konfidentielle er godt kjend blandt byggstudentane, slik at dei t.d. bruker fiktive eller sladda data i innleveringar. Kva konfidentialitet har å seia for val av programvare og lagringsløysingar og for arbeidsrutinar er derimot ikkje drøfta.

Scenario 2: Tekniske løysingar i bygg

Teikningar og annan informasjon om dei tekniske løysingane i byggkonstruksjonar kan avdekkja sårbarheiter som terroristar kan utnytta til å gjera maksimal skade. Slik informasjon vert normalt ikkje behandla som hemmeleg i dag, men er kan like fult vera eit mål for militær spionasje.

Terje kjenner ikkje til at dette vert diskutert som ein utfordring i t.d. kommunale prosessar, men det er ein potentiel trusel som studentane bør vera merksame på.

Scenario 3: Innkjøp av alarm-, overvaking- og signalsystem

Det er andre programområde (elektro og evt. data) som skal ha ansvar for utvikling av elektroniske system og dermed også dei tekniske sikkerheitskontrollane. Byggingeniørane er tek derimot del i bestillings- og innkjøpsprosessar og er gjerne problemeigar. Dette gjeld alarmsystem i bygg, overvaking av vegtrafikk og signalsystem på jernbane.

Det er lett å sjå at elektroniske innbrot kan slå ut alarmsystem og opna for fysisk innbrot, henta persondata frå overvakingssystem og utnytta signalsystem til å forårsaka togkollisjonar som terroråtak.

Trusel- og risikovurderingane høyrer i dette tilfellet til systemnivået, som byggingeniørane har naturleg eigarskap til. Dei må difor kunna identifisera truslar, estimera risiko og prioritera tiltak og kostnader.

Dette problemet gjer det òg tydleg at programområda må dela ein taksonomi for sikkherheit og risikoanalyse slik at dei kan kommunisera tydleg om kravspesifikasjonane.

Scenario 4: Persondata

Persondata er lite sentralt, men som i alle andre fag, vil kan byggingeniørar enda opp med å handsama persondata for tilsette eller kundar, og må ha grunnleggjande kjennskap til kva krav som vert stilt.

Oppsummering

Me ser eit generelt behov for ein kultur for å tenkja sikkerheit og vera merksam på truslar og sårbarheiter. Her er det kanskje etikk, meir enn informatikk, som er det viktigaste faggrunnlaget for IKT-sikkerheit. Dette gjeld alle programområde og bygg.

Scenario 3 er kanskje det dømet som krev mest systematisk og grundig opplæring i sikkerhetstenking for byggingeniørar.

Kapittel 4

Læremateriell

4.1 Innledning

Ved introduksjon av nye læringsmål i utdanninger så vil tilfanget av læremateriell som dekker disse læringsmålene kunne være en utfordring. Spesielt hvis temaene er nye. Dette er nødvendigvis ikke tilfelle for IKT-sikkerhet, men mye av læremateriellet vi finner er ikke tilpasset utdanninger med mindre søkelys på informatikk og matematikk. Spesielt mangel på informatikk-kompetanse gjør mye av eksisterende læremateriell lite egnet. I tillegg er læremateriellet ikke tilpasset de ulike fagene og det kan være vanskelig for studenter å se at temaene er relevant for deres utdanning. Det kan for eksempel være vanskelig å finne eksempler fra eget fagområde i slikt generelt læringsmateriell.

Mange utdanninger ønsker at læremateriellet skal være på norsk, spesielt for emner som undervises tidlig i utdanningen. I tillegg kan sikkerhet være såpass «fremmed» for studentene at læremateriell på norsk det vil senke terskelen for å sette seg inn i slike nye tema. Et krav om norsk språk begrenser utvalget av mulig læremateriell. Men helt håpløst er det ikke. I den senere tid har flere lærebøker på norsk blitt publisert [3, 32, 14]. Vi vil senere presentere disse med hensyn på våre anbefalinger.

4.2 Behov for læremateriell

Selv om det finnes noen lærebøker som dekker læringsmålene vi anbefaler, så er det likevel store utfordringer med hensyn på læremateriell. Disse utfordringen kommer av at en vellykket integrasjon av IKT-sikkerhet i en utdanning er avhengig av at disse temaene gjøres relevant for fagområdet. Det betyr både at læringsmålene i IKT-sikkerhet knyttes opp mot fagområdet studentene studerer og at eksemplene som brukes er relevante.

I praksis kan det bety at man trenger egne tekster, eksempler og oppgaver for ulike fagområder. Disse vil bidra til at læringsmålene i IKT-sikkerhet læres i kontekst av eget fagområde med eksempler fra eget fagområde. Disse kan kombineres med mer generelt læremateriell som til sammen dekker læringsmålene og gjør disse relevante for de ulike fagområdene.

Behovet for felles læremateriell er av kritisk karakter, av forskjellige grunner. For det første er det generelt vanskelig å finne personer med datasikkerhetsekspertise som både kan undervise på norsk og som er interessert i en jobb i akademia. For de andre kan det være utfordrende for en datasikkerhetsekspert å utvikle «delekspertise» innenfor alle de ingeniørfagfeltene som tilbys ved sin institusjon. For det tredje kan det være vanskelig timeplanmessig (og muligens også økonomisk) å ha en ressurs som bidrar til mange ulike emner på forskjellige utdanninger. Godt tilgjengelig læremateriell tilpasset utdanninger kan avhjelpe mangelen på direkte tilgang på slik datasikkerhetsekspertise.

4.3 Tiltak for å øke tilfanget av relevant læringsmateriell

I arbeidsgruppen har vi hatt et søkelys på hvordan relevant læremateriell skal bli utviklet. I et tradisjonelt marked for lærebøker vil vi fort havne i en situasjon at tekster tilpasset spesifikke utdanninger ikke har et stort nok marked for kommersiell publisering av disse. Samtidig vil det være ineffektivt og unødvendig at hver enkelt utdanning utvikler eget læremateriell tilpasset egne utdanninger. Det som er ønskelig er å finne frem til ordninger hvor liknende utdanninger kan

1. Nasjonale insentiver gjennom Dikus kvalitetsprogrammer
2. Institusjonelle policyer (blant annet for hvor læringsinnhold lagres)
3. Insentiver på institusjoner for å understøtte deling, for eksempel krav om deling når medieproduksjoner mottar støtte
4. Meritteringsordninger der den enkelte lærer får anerkjennelse for å skape og dele læringsressurser
5. Vurdering av den enkelte institusjons og lærers innsats når det gjelder å dele egenprodusert innhold
6. Kompetanseheving innen kreditering/opphavsrettslige forhold og teknisk kompetanse til lærere i sektoren eller bygge støttemiljø for bistand innen dette
7. Holdningsskapende tiltak/utviklingsprogrammer om fordeler med å dele

Figur 4.1: Tiltak for å bedre delingskulturen [40]

1. At man er redd for at det læringsinnholdet man har produsert ikke er "godt nok" til å gjenbrukes av andre eller at for mange andre får se det man har utarbeidet
2. At man er usikker på om alle opphavsrettslige forhold er godt nok ivaretatt/ at all bruk av elementer i innholdet skjer etter avtale og med kreditering av forfatter (gjelder bruk av bilder og annet materiale)
3. At det er uavklart om det er institusjonen som har eiendomsrett til innholdet eller det er den ansattes opphavsrett
4. Konkurrerende, institusjonelle/lokale satsinger
5. At det oppleves som om det er tekniske hindre for å få til å dele informasjon (mange ulike løsninger som ikke fungerer optimalt, mye "plunder og heft")
6. At man ikke vet hvordan man merker læringsressurser man deler med metadata
7. At man synes det er arbeidskrevende å registrere og merke læringsressurser for deling
8. At man kan konkurrere med andre arenaer der lærere deler innhold, som grupper på Facebook og i LMS
9. At de som ikke engster seg for å bruke innhold der opphavsrettighetene ikke er klarert, synes det er enklere å søke på nett etter ressurser enn i et LOR

Figur 4.2: Barrierer for deling av læringsressurser [40]

1. Manglende kultur for gjenbruk på lærestedet, herunder
   (a) "Not invented here"-syndrom, en innstilling i en virksomhet som gjør at man unngår å kjøpe eller bruke eksisterende produkter, forskning, standarder eller kunnskap fordi de har opphav utenfor virksomheten
2. At det er vanskelig å finne de læringsressursene man trenger fordi
   (a) taksonomien for metadata ikke er intuitiv
   (b) ressursene er dårlig merket med metadata
   (c) søk og sortering ikke fungerer optimalt
   (d) lisensiering ikke er tydelig merket
3. Manglende tillit til samlingen fordi
   (a) kvaliteten på læringsressursene er dårlig eller svært varierende
   (b) det er for få ressurser tilgjengelig til at samlingen blir attraktivt
   (c) ikke alle eller mange nok fagfelt er representert i samlingen

Figur 4.3: Barrierer for gjenbruk av læringsressurser [40]

dele på lasten med å utvikle dette. En utfordringen er å finne insentiver for å motivere en slik deling av læringsmateriell. En annen utfordring er om utdanningene selv har kompetanse nok innen datasikkerhet til å utvikle slikt læringsmateriell.

Unit (Direktoratet for IKT og fellestjenester i høyere utdanning og forskning) ga i 2019 ut en utredning om felles nasjonale løsninger for tilgang til læringsressurser på tvers av utdanningsinstitusjoner [40]. Denne utredningen har søkelys på en nasjonal løsning for tilgang til læringsressurser (Learning Object Repository, forkortet LOR), men lister også viktige tiltak for å bedre delingskulturen i universitets- og høyskolesektoren (se Figur 4.1).

Diskusjonen i Kapittel 9 i Unit sin utredning utdyper hva som må til for å få til en vellykket deling av læringsressurser i en slik nasjonal løsning. Utredningen lister også opp mulige barrierer for deling og gjenbruk av læringsressurser gjennom en slik løsning (se henholdsvis Figur 4.2 og 4.3).

Arbeidsgruppen har også diskutert slike delingsplattformer og tror at de kan være viktig for å muliggjøre slik deling. En slik nasjonal delingsplattform er ikke eneste mulighet for å bedre delingskulturen i universitets- og høyskolesektoren. Men både tiltakene og barrierene diskutert i utredningen vil være viktig å ha med seg for å få til andre vellykkede bidrag til en bedring av delingskulturen.

En velkjent motivasjon for å utføre et krevende arbeid i universitets- og høyskolesektoren er muligheter for publisering og publiseringspoeng. Vi kan allerede i dag finne interessante bidrag for å forbedre undervisning innen ulike fagområder i eksisterende tidsskrifter med søkelys på utdanning og undervisning. Et godt eksempel er tidsskriftet *Nordic Journal of STEM Education*[1]. Dette er et vitenskapelig fagfellevurdert tidsskrift som publiserer i det brede feltet pedagogisk utvikling innen vitenskap, teknologi, ingeniørvitenskap og matematikk i høyere utdanning. I tillegg har vi konferanser som MNT-konferansen[2] som har som formål å fremme MNT-utdanningenes (Matematikk, Naturvitenskap, Teknologi) kvalitet og relevans. Bidrag til denne konferansen publiseres i et eget konferanse-volum i *Nordic Journal of STEM Education* og forfattere er oppfordret til å videreutvikle sitt bidrag og sende dette inn på nytt som et tidsskriftbidrag, som da vil gjennomgå fagfellevurdering og bli publisert som en fullverdig artikkel i en kommende utgave av tidsskriftet.

Slike tidsskrifter er vel og bra, og kan bidra noe til å løse utfordringene med å utvikle læremateriell innen IKT-sikkerhet som er relevant for spesifikke utdanninger. Problemet er at bidragene er ment som innspill i en akademisk diskusjon om, eller demonstrasjon av, hvordan øke kvaliteten eller relevansen i undervisningen i en utdanning. Bidragene er ikke nødvendigvis læremateriell som andre kan ta i bruk og utvikle videre. Dette er ikke deling av læremateriell, men heller deling av erfaringer fra undervisningssituasjonen.

Et forslag fra arbeidsgruppen er å lage en publikasjonskanal hvor utviklet og videreutviklet læremateriell kan publiseres og gi uttelling for bidragsyterne, enten gjennom publiseringspoeng eller andre belønninger som kan gi positiv uttelling for den akademiske karrieren til bidragsyterne. Om dette skal organiseres som tidsskrift eller som konferanse eller som noe annet har vi ikke tatt stilling til, men det er naturlig å se dette i sammenheng med en nasjonal delingsplattform diskutert i Unit sin utredning [40]. Andre fordeler med å organisere en publiseringskanal er en mulighet for fagfellevurdering av bidragene, og på den måten sikre et minimum av kvalitet på det som publiseres i en publiseringskanal. En utfordring vi være at måten vi gjøre fagfellevurdering på i dag nødvendigvis ikke passer så godt for utviklet læremateriell, og at vi ikke nødvendigvis har noen god tradisjon for å vurdere kvalitet på læremateriell gjennom fagfellevurdering. Hvis fagfellevurderingene ikke tar tilstrekkelig hensyn til målgruppen (studentene) så kan vi fort ende opp med bidrag som skal imponere de som skal fagfellevurdere og ikke bidrag som er egnet i en utdanning. Det tradisjonelle formatet som blir fagfellevurdert er artikler, mens læringsmidler med høy kvalitet kan komme i mange ulike former og formater. Det kan være vanskelig å finne en enhetlig og god form for vurdering av slikt materiale.

Arbeidsgruppen har flere medlemmer som har vært med å utvikle læremateriell og lærebøker. Erfaringene fra disse, og andre vi har diskutert temaet med, er at det å utvikle læremateriell er tidkrevende og vanskelig i en travel hverdag som foreleser ved en utdanningsinstitusjon. Et mulig tiltak for å øke produksjonen av læremateriell er å gi rom til motiverte forelesere å bruke tid og ressurser på dette arbeidet. Dette kan gjøres ved å tilby finansieringsordninger slik at institusjonen sammen med forleser kan skaffe rom til denne for å bruke tid og ressurser på å utvikle læremateriell.

I dag utvikles mye læringsmateriell på privat initiativ av de fagansatte uten at institusjonene til de fagansette hverken oppfordrer til det eller understøtter slike aktiviteter. Vi ser ofte at utvikling av læringsmateriell har en lavere status en publisering av forskning. I de tilfeller hvor publisert læringsmateriell gir uttelling for institusjonen, i for eksempel publikasjonspoeng, så kan fagansatte rettferdiggjøre og bruke arbeidstiden på utvikling av slikt materiell. Det er likevel ofte en litt uavklart rolle mellom det å være fagbokforfatter med mulige inntekter fra dette, og det å være fagansatt som bruker tid på å utvikle læringsmateriell for egen undervisning og til gjenbruk for andre ved andre institusjoner.

Oppsummert så anbefaler læringsgruppen følgende tiltak for å øke tilfanget av relevant læremateriell:

- Opprette en felles nasjonal nasjonale løsninger for tilgang til læringsressurser på tvers av utdanningsinstitusjoner

[1] https://www.ntnu.no/ojs/index.php/njse/index
[2] https://realfagsrekruttering.no/konferanser/mnt-konferansen-2021

- Opprette fagfellevurderte publiseringskanaler for læremateriell som gir uttelling i en akademisk karriere
- Opprette nasjonale ordninger (stipend) for finansiering av ansatte i universitets- og høyskolesektoren som ønsker å utvikle tilpasset læremateriell for et fagområde
- Høyne status for utvikling av læremateriell og avklare rollen til en fagansatt i undervisningsstilling som ønsker å utvikle lærebøker og annet undervisningsmateriell

4.4 Tilgjengelig læremateriell

Det finnes i dag flere nye norske lærebøker som dekker temaene inne IKT-sikkerhet. Vi vil her presentere tre av disse lærebøkene. Disse er de vi i slutten av arbeidet til arbeidsgruppen har identifisert som mulig lærebøker på norsk for de læringsmålene vi har beskrevet. Det betyr ikke at disse er de eneste mulige lærebøkene for disse læringsmålene, men de er de vi kjenner til per dags dato.

Vi vil også henvise til nettressurser som er tilgjengelig og som kan komplementere annet læremateriell om IKT-sikkerhet. I tillegg vil vi kort presentere tre andre bøker på norsk som kan være nyttig i utdanninger som inkluderer IKT-sikkerhet. Disse er valgt fordi de representer noe annet enn en typisk læringsbok for våre anbefalte læringsmål. De kan likevel være en nyttig ressurs for noen studenter. Heller ikke her forsøker vi å være komplett i vår oversikt over slike bøker.

Det må også kommenteres at medlemmer i arbeidsgruppen inkluderer forfattere for to av de lærebøkene vi omtaler, og at arbeidsgruppen har fått tilgang på og muligheten til å gi innspill på en av lærebøkene. Boka *Digital sikkerhet – En innføring* [3] fikk arbeidsgruppen et utkast av, og muligheten til å gi tilbakemelding til, før den ble publisert. Medlem av arbeidsgruppen Tom Heine Nätt er medforfatter av boka *Datasikkerhet – Ikke bli svindlerens neste offer* [32] og medlem av arbeidsgruppen Audun Jøsang er forfatter av boka *Informasjonssikkerhet – Teori og praksis* [14]. Ingen av disse lærebokforfatterene har skrevet omtalene av disse lærebøkene.

4.4.1 Digital sikkerhet – En innføring

Digital sikkerhet – En innføring [3] er en lærebok i digital sikkerhet hvor tre redaktører har satt sammen mange bidrag over ulike tema. Hvert bidrag er et eget kapittel med egne forfattere. Boken har derfor til sammen et ganske stort antall bidragsytere.

Boka dekker de 6 tema og læringsmål som arbeidsgruppen har anbefalt:

1. Grunnleggende begreper: Kapittel 1 Introduksjon til digital sikkerhet, inkluderer mange av de grunnleggende begrepene innen IKT-sikkerhet, men andre begreper blir også introdusert i andre kapitler.
2. Bevissthet og sikkerhetskultur: Kapittel 2 Sikkerhetskultur, dekker dette temaet god. Det finnes også relevant stoff i andre kapitler, inklusiv i kapittel 3, Sikkerhet og digital etikk.
3. Personvern: Kapittel 5, Digitalt personvern, ID-tyveri og anonymitet dekker dette temaet godt. Vi finer også relevant stoff i kapittel 4, Identifikasjon, autentisering og aksesskontroll.
4. Lover, reguleringer og etikk: Kapittel 3 Sikkerhet og digital etikk, og kapittel 6 Lover og ansvar, er de kapitlene som best dekker dette temaet. Det er også mulig og finne noe relevant stoff i andre kapitler.
5. Trusselmodellering og risikostyring: Kapittel 7 Sårbarheter i IKT-systemer, kapittel 8 Trusler og etterretning, og kapittel 9 Funksjonsbasert risikovurdering, dekker dette temaet. Vi finner også stoff i andre kapitler som kan falle inn under temaet.
6. Sikkerhetsarkitektur og innebygd informasjonssikkerhet: Kapittel 11 Programvaresikkerhet, kapittel 12 Sikkerhetsovervåkning og deteksjon og kapittel 13 Hendelseshåndtering og opprydding, og noe av kapittel 1 Introduksjon til digital sikkerhet, dekker dette temaet. Vi finner også stoff i andre kapitler som kan falle inn under temaet.

Boka er naturlig nok ikke organisert basert på arbeidsgruppens oppdeling i tema, og et tema dekkes normalt over flere ulike kapitler. Angivelsene over er derfor noe omtrentlig.

Boka dekker de anbefalte læringsmålene bra og kan benyttes av studenter med ulik bakgrunn. Det meste av boka er tilgjengelig uten noen spesiell informatikkbakgrunn, men i noen kapitler er noe informatikkbakgrunn en fordel. Boka er en lærebok. På grunn av at boken har mange ulike forfattere så er boken litt mindre enhetlig enn de andre to vi omtaler her.

En komplett serie med presentasjoner fra hvert kapittel er tilgjengelig for alle forelesere til fri bruk.[3] Det er også utarbeidet digitale foredrag fra de ulike forfatteren som er spesialister i sitt området til hvert kapittel. Dette er tilgjengelig for de lærere som har behov.

4.4.2 Datasikkerhet – Ikke bli svindlerens neste offer

Datasikkerhet – Ikke bli svindlerens neste offer (andre utgave) [32] skal gi råd om hvordan du kan oppdage og forhindre farer i en digital hverdag.

Boka dekker de 6 tema og læringsmål som arbeidsgruppen har anbefalt på denne måten:

1. Grunnleggende begreper: Temaet blir presentert gjennom hele boka, og vi finner en oppsummerende liste med ordforklaringer helt til slutt i boka.
2. Bevissthet og sikkerhetskultur: Dette er på en måte hovedtema i hele boka, men da med fokus på deg personlig. I kapittel 14 Bedrifter og organisasjoner, løftes blikket ut over det personlige. Det finnes dog underveis egne informasjonsbokser i de andre kapitlene med utfordringer i forholdet mellom bedrifter og ansatte.
3. Personvern: I kapittel 9 Nettvett, diskuteres personvern. Vi finner også beslektede tema i andre kapitler.
4. Lover, reguleringer og etikk: Dette temaet omhandles først og fremst i kapittel 14 Bedrifter og organisasjoner, men vi finner relevant stoff også i andre kapitler.
5. Trusselmodellering og risikostyring: Kapittel 14 Bedrifter og organisasjoner, dekker dette temaet.
6. Sikkerhetsarkitektur og innebygd informasjonssikkerhet: Det er ikke noen spesifikke kapitler som dekker dette temaet, men vi finner noe relevant stoff i ulike kapitler.

Boka er ikke organisert på samme måte som arbeidsgruppen har inndelt læringsmålene, og det er derfor vanskelig å direkte angi hvor de ulike temaene i boka er dekket.

Vi ser at fokus i boka passer best på de fem første temaene i IKT-sikkerhet som arbeidsgruppen har anbefalt. Boka er ikke en typisk lærebok, da den ikke inkluderer oppgaver i slutten av hvert kapittel. Hele boka er mulig å lese uten noen spesiell informatikkbakgrunn. Boka har et større fokus på brukeren enn de andre lærebøkene omtalt her. Den er mer lettlest og har et fokus på praktiske tilnærminger til IKT-sikkerhet for deg personlig. Likevel inneholder boka to kapitler (kapittel 13 Når andre svikter og kapittel 14 Bedrifter og organisasjoner) som flytter fokus over i bedrifts-sammenheng.

Boka har en egen nettside og en egen sikkerhetsblogg med informasjon om boka og innlegg relevant for innholdet i boka.[4]

4.4.3 Informasjonssikkerhet – Teori og praksis

Informasjonssikkerhet – Teori og praksis [14] er en lærebok i informasjonssikkerhet spesielt rettet mot informatikkstudenter.

Boka dekker de 6 tema og læringsmål som arbeidsgruppen har anbefalt:

1. Grunnleggende begreper: Kapittel 1 Grunnleggende begreper, inkluderer mange grunnleggende begreper innen IKT-sikkerhet, men flere begreper blir introdusert i andre kapitler.
2. Bevissthet og sikkerhetskultur: Kapittel 11 Sikkerhetskultur, er det kapitlet som i hovedsak dekker dette temaet. Kapittel 9 Innebygd informasjonssikkerhet og personvern, og kapittel 10 Styring og ledelse av informasjonssikkerhet, bidrar også med stoff til dette temaet.
3. Personvern: Kapittel 8 Personopplysningsvern og kapittel 9 Innebygd informasjonssikkerhet og personvern, dekker dette temaet.
4. Lover, reguleringer og etikk: Kapittel 8 Personopplysningsvern, kapittel 9 Innebygd informasjonssikkerhet og personvern og kapittel 10 Styring og ledelse av informasjonssikkerhet, er i hovedsak de kapitlene som dekker disse temaene.

[3] https://nettressurser.no/digitalsikkerhet
[4] https://www.datasikkerhetsboka.no / https://www.datasikkerhetsboka.no/blogg

5. Trusselmodellering og risikostyring: Kapittel 12 Risikostyring for informasjonssikkerhet, dekker dette temaet. Kapittel 13 Beredskap og hendelseshåndtering, og kapittel 14 Cyberoperasjoner, bidrar også med stoff til dette temaet.

6. Sikkerhetsarkitektur og innebygd informasjonssikkerhet: Boka dekker dette temaet i svært mange kapitler i boka, inklusiv kapittel 2 Systemsikkerhet, kapittel 3 Kryptografi, kapittel 4 Nøkkelhåndtering og PKI, kapittel 5 Nettverkssikkerhet, kapittel 6 Brukerautentisering, kapittel 7 IAM – identitets- og tilgangshåndtering, og kapittel 9 Innebygd informasjonssikkerhet og personvern.

Boka er naturlig nok ikke organisert basert på arbeidsgruppens oppdeling i tema, og et tema dekkes normalt over flere ulike kapitler. Angivelsene over er derfor noe omtrentlig.

Boka dekker alle temaene i IKT-sikkerhet som arbeidsgruppen har anbefalt. Boka er lagd som lærebok. Boka passer best for studenter med noe informatikkbakgrunn, men boka forklarer grunnleggende IT-begreper, og på den måten er den selvforklarende og kan brukes innen andre studieprogrammer enn bare informatikk.

Læringsressurser i form av forelesningspresentasjoner og oppgaver med løsningsforslag til hvert kapittel er tilgjengelig fra Universitetsforlaget sine nettsider.[5]

4.4.4 Andre nyttige bøker

Håndbok i datasikkerhet – Informasjonsteknologi (fjerde utgave) [4] kan også være et alternativ til læringsmålene som arbeidsgruppen anbefaler. Boka er ikke en typisk lærebok, da den ikke inkluderer oppgaver i slutten av hvert kapittel. Men hvert kapittel avsluttes med oppsummering, kalt «Tenk over», som passer godt i en lærebok. Boka er ganske omfattende og mange av kapitlene forventer noe bakgrunn fra informatikk. Fjerdeutgaven ble utgitt i 2019 med et nytt kapittel om EU-forordningen GDPR. De andre kapitelene bærer litt preg av å være skrevet noe tilbake i tid. Blant annet refereres ikke nyere utredninger og styringsdokumenter. Boka er likevel egnet som en håndbok for personer med noe informatikkbakgrunn som trenger å sette seg inn i ulike områder innen IKT-sikkerhet.

Datasikkerhet for ledere – Hvordan beskytte din virksomhet? [2] er nok en forløper til læreboka *Digital sikkerhet – En innføring* [3], som vi omtalte over. Forskjellen er at denne boka går inn i temaene fra et ledelsesperspektiv, den er mindre omfattende og den inkluderer ikke oppgaver i slutten av hvert kapittel som normalt lærebøker har. Hvert kapittel avsluttes med oppsummering kalt «Oppsummering og tips» og den dekker våre anbefalte tema i IKT-sikkerhet ganske godt. Boka kan derfor vurderes som lærebok for noen typer studier. For noen studenter vil boka passe som tilleggslitteratur.

Kryptografi – Den hemmelige skriften [12] gir en grunnleggende forståelse av kryptografiske teknikker, med utgangspunkt i historisk materiale. Boka er ikke en typisk lærebok, og den mangler oppgaver for studentene. Den dekker også kun et lite sett av læringsmålene arbeidsgruppen har anbefalt. Den er likevel flott tilleggslitteratur fordi den dekker det komplekse temaet kryptografi på en tilgjengelig måte, med muligheter for å gå mer ned i detaljer for den interesserte leseren. Den historiske utviklingen av kryptografi er godt presentert i boka.

4.4.5 Nyttige ressurser på nett

Vedlegg C inneholder en mer komplett liste over nyttige eksterne ressurser. Spesielt nettsider listet i Vedlegg C.1 Viktige norske nettsidene, er nyttige. Disse kan være en god ressurs både for forelesere og studenter. Det er anbefalt at de som skal undervise i disse temaene kjenner til og kan finne frem på disse nettsidene og bruker de aktivt i undervisningen. Også Vedlegg C.3 Relevante lover og reguleringer og Vedlegg C.4 Relevante standarder, anbefalinger og metoder, er ressurser på nett som kan være nyttig å bruke ved undervisning om disse temaene innen IKT-sikkerhet.

[5] http://www.nettressurser.no/informasjonssikkerhet

Tillegg A

Arbeidsgruppens arbeid

Nasjonal arbeidsgruppe for styrking av undervisning i IKT-sikkerhet har vært bredt sammensatt fra utdanningsinstitusjoner, statlig sektor og næringsliv. Arbeidet i arbeidsgruppen har vært organisert på litt ulike måter i ulike faser av arbeidsgruppens virkeperiode. I arbeidsgruppens mest intense arbeidsperiode ble det gjennomført arbeidsmøter for arbeidsgruppens medlemmer. I denne perioden ble det også etablert undergrupper som fokuserte på spesifikke deler av arbeidsområdet til arbeidsgruppen. Disse undergruppene hadde egne arbeidsmøter. De fleste arbeidsmøtene ble gjennomført digitalt, men noen arbeidsmøter ble også gjennomført fysisk eller i en hybrid form.

I tillegg til arbeidsmøtene har arbeidsgruppen også arbeidet utadrettet. Dette har vært gjort både for å informere om arbeidsgruppens arbeid underveis i prosessen og for å få konkrete innspill til arbeidsgruppens arbeid. Vi har blant annet deltatt på flere konferanser og vært aktive i relevante utdanningsfaglige diskusjoner og arbeider. Nedenfor følger en oversikt over arbeidsgruppens møter og våre andre deltakelser.

A.1 Arbeidsgruppens medlemmer

Navn	*Arbeidssted*
Anders Andersen Professor	Arbeidsgruppens leder og kontaktperson. Instituttleder, Institutt for Informatikk, Fakultet for naturvitenskap og teknologi, UiT Norges arktiske universitet, Tromsø (UiT-Tromsø)
Tor Berre Bachelorstudent	Institutt for datateknologi og informatikk, Fakultet for informasjonsteknologi og elektroteknikk, Norges teknisk-naturvitenskapelige universitet, Trondheim (NTNU-Trondheim)
Pål Ellingsen Førsteamanuensis	Assisterande instituttleiar, Institutt for datateknologi, elektroteknologi og realfag, Fakultet for ingeniør- og naturvitskap, Høgskulen på Vestlandet, Bergen (HVL)
Olaf Hallan Graven Professor	Institutt for realfag og industrisystemer, Fakultet for teknologi, naturvitenskap og maritime fag, Universitetet i Sørøst-Norge, Kongsberg (USN)
Laurence Habib Professor	Instituttleder, Institutt for informasjonsteknologi, Fakultet for teknologi, kunst og design, OsloMet, Oslo
Moutaz Haddara Professor	Institutt for teknologi, School of Economics, Innovation and Technology, Høyskolen Kristiania, Oslo (HK)
Erik Hjelmås Førsteamanuensis	Institutt for informasjonssikkerhet og kommunikasjonsteknologi, Fakultet for informasjonsteknologi og elektroteknikk, Norges teknisk-naturvitenskapelige universitet, Gjøvik (NTNU-Gjøvik)
Mette Mo Jakobsen Professor	Seniorrådgiver, høgskolerådet Universitets- og høgskolerådet (UHR) / Institutt for ingeniørvitenskap, Fakultet for teknologi og realfag, Universitetet i Agder, Grimstad (UiA)
Audun Jøsang Professor	Institutt for Informatikk, Det matematisk-naturvitenskapelige fakultet, Universitetet i Oslo (UiO) / Lærebokforfatter (blant annet med boka *Informasjonssikkerhet – Teori og praksis* [14])

Navn	*Arbeidssted*
Lars Emil Knudsen	Stedfortreder for Tom Heine Nätt i perioden august–november 2019, Høgskolelektor, Avdeling for informasjonsteknologi, Høgskolen i Østfold, Halden (HiØ)
Jingyue Li Førsteamanuensis	Institutt for datateknologi og informatikk, Fakultet for informasjonsteknologi og elektroteknikk, Norges teknisk-naturvitenskapelige universitet, Trondheim (NTNU-Trondheim)
Arne Roar Nygård	Seniorrådgiver for informasjonssikkerhet og personvern Elvia / Næringslivets Hovedorganisasjon (NHO) / Energi Norge
Tom Heine Nätt Førstelektor	Avdeling for informasjonsteknologi, Høgskolen i Østfold, Halden (HiØ) / Lærebokforfatter (blant annet med boka *Datasikkerhet – Ikke bli svindlerens neste offer* [32])
Sondre Rønjom Professor II	Sjefsforsker, Nasjonal sikkerhetsmyndighet (NSM), Oslo / Bistilling, Institutt for informatikk, Det matematisk-naturvitenskapelige fakultet, Universitetet i Bergen (UiB)
Hans Georg Schaathun Professor	Institutt for IKT og realfag, Fakultet for informasjonsteknologi og elektroteknikk, Norges teknisk-naturvitenskapelige universitet, Ålesund (NTNU-Ålesund)
Arild Steen Universitetslektor	Instituttleder, Institutt for elektroteknologi, Fakultet for ingeniørvitenskap og teknologi, UiT Norges arktiske universitet, Narvik (UiT-Narvik)
Tor-Fredrik Torgersen Masterstudent	Institutt for data- og elektroteknologi, Det teknisk- naturvitenskapelige fakultet, Universitetet i Stavanger (UiS)

A.2 Arbeidsgruppens møter

Når og hvor	*Beskrivelse*
21.11.2018, 10:30–11:30 Digitalt	**Første arbeidsgruppemøte, IKT-sikkerhet i utdanningene**: En gjennomgang av bakgrunnen til arbeidsgruppen, presentasjon av medlemmene, diskusjon om hva mandatet til, og leveransen fra, arbeidsgruppen er, diskusjon om hvordan vi skal strukturere arbeidet og møteplan.
03.01.2019, 12:00–16:00 Gardermoen, Workshop – Nasjonale retningslinjer for ingeniørutdanning	**Oppstartsmøte, IKT-sikkerhet i utdanningene**: Samlokalisert med Workshop – Nasjonale retningslinjer for ingeniørutdanning. Først en presentasjon av IKT-sikkerhet i utdanningene i utdanningsinstitusjonene etterfulgt av en presentasjon av Cybersecurity Curricula 2017 [13]. Så diskusjoner om hvilke tema/områder skal med i vårt arbeid, hvordan skal vi strukturere arbeidet, og hva er minimumskunnskap om IKT-sikkerhet (læringsmål). Til slutt diskuterte vi mulig artikkel til MNT-konferansen 2019, møteplan og fordelte oppgaver til neste arbeidsguppemøte.
29.01.2019, 09:00–11:00 Digitalt	**Arbeidsgruppemøte 2, IKT-sikkerhet i utdanningene**: Diskuterte utkast til artikkel til MNT-konferansen 2019 [1] og mulig presentasjon/panel på Sikkerhetsfestivalen 2019. Lagede komplett møteplan for våren 2019 og planla det videre arbeidet frem til neste arbeidsgruppemøte.
28.02.2019, 12:00–13:00 Digitalt	**Arbeidsgruppemøte 3, IKT-sikkerhet i utdanningene**: Arbeidet med læringsmål innenfor de hovedtemaene vi er blitt enig om tidligere og diskuterte hvordan læringsmålene kan realiseres i utdanninger. Konkrete forslag for hvordan dette kan gjøres i ingeniørutdanningene ble diskutert. Diskuterte også hvordan vårt arbeid skal bli synlig slik at vi kan få tilbakemeldinger på våre forslag. Vi vil i 2019 være tilstede på og presentere oss på Sikkerhetskonferansen til NSM, MNT konferasen og Sikkerhetsfestivalen.

Når og hvor	*Beskrivelse*
29.03.2019, 13:45–15:30 Tromsø, MNT-konferansen 2019 (hybrid)	**Arbeidsgruppemøte 4, IKT-sikkerhet i utdanningene**: Etter en kort presentasjon av aktiviteter siden sist ble vi enig om å organisere det videre arbeidet i tre undergrupper: læringsmål, integrasjon av læringsmål og læremateriell. Vi ble enig om å ha fokus på ingeniørfagene frem til september i år. Vi diskuterte også når i en utdanning temane skulle gis, blant annet at man kan ha en generell komponent tidlig og spesialisering senere. Vi ønsker også å prøve ut våre forslag: UiS, HVK, UiT-Narvik og NTNU-Ålesund er mulige kandidater. Til slutt diskuterte vi hva som eksisterer og hva som mangler av læremateriell.
02.05.2019, 12:00–14:00 Digitalt	**Arbeidsgruppemøte 5, IKT-sikkerhet i utdanningene**: Kort oppdatering av hva som har skjedd siden sist: lukket web-side for arbeidsgruppen, forberedelser til Sikkerhetsfestivalen 2019 og rapportering til Nasjonalt fagorgan for IKT 8. mai (AA) og UHR-MNT 23. mai (LH). Presentasjon fra arbeidet til undergruppene, som frem til neste møte i arbeidsgruppen vil ha egne arbeidsmøter.
23.05.2019, 09:00–10:00 Digitalt	**Arbeidsmøte i undergruppen Læringsmål**: Arbeider med utkast til læringsmål og diskuterte hvordan læringsmål kan gjøres relevant i utdanninger og når i et studieløp de kan passe.
23.05.2019, 10:00–11:00 Digitalt	**Arbeidsmøte i undergruppen Læremateriell**: Arbeidet seg gjennom eksisterende (norsk) læremateriell og diskuterte hvordan relevante case/eksempler fra fagområdene kan introduseres. Diskuterte også utfordringer med at forelesere ikke kan IKT-sikkerhet godt nok og har behov for støtte. Til slutt ble ressurser til utvikling av læremateriell diskutert.
23.05.2019, 11:00–12:00 Digitalt	**Arbeidsmøte i undergruppen Integrasjon av læringsmål**: Har foreløpig fokus på ingeniørutdanningene. Tar utgangspunkt i forslag fra HGS og jobber videre med det. Bør IKT-sikkerhet være en del av introduksons- og systememnet? Mange uavklarte problemstillinger: hvilke emner, kunnskap hos forlesere.
04.06.2019, 09:00–11:00 Digitalt	**Arbeidsgruppemøte 6, IKT-sikkerhet i utdanningene**: Startet med rapportering fra undergruppene og diskusjoner rundt deres arbeid: Er en tettere kobling mellom undergruppene læringsmål og integrasjon av læringsmål nødvendig? Det kan være utfordrende med å spre temaet utover i studiene (manglende fokus). Hvordan gjøre temaene relevant i de ulike studiene? Utvikling av relevant lærermateriell og opplæring av forelesere kan være en stor utfordring. Til slutt diskuterte vi bidraget og deltakelsen på Sikkerhetsfestivalen 2019.
19.06.2019, 09:00–11:00 Digitalt	**Fellesmøte i undergruppene Læringsmål og Integrasjon av læringsmål**: Startet med en diskusjon om hvilke læringsmål som skal inn hvor i studiet, og da spesielt introduksjonsemnet og systemement i ingeniørutdanningen. Videre ble det diskutert hvordan håndterer det som er spesifikt/spesielt for studiet, og mulige vurderingsformer. Det ble også kommentert at Risiko- og sårbarhetsanalyse (ROS) er en selvsagt del av mange ingeniøremner.
27.08.2019, 16:30–19:00 Lillehammer, Sikkerhetsfestivalen 2019	**Arbeidsgruppemøte 7, IKT-sikkerhet i utdanningene**: Første tema var læringsmål og integrasjon av læringsmål i studieplaner. Tar utgangspunkt i forslag fra HGS og bruker eksisterende rammeplan som ramme for arbeidet. Baker inn tilbakemeldinger fra arbeidsgruppen. Det andre temaet var læremateriell. Dette er avhengig av de endelige læringsmålene. Er en ny publiseringskanal en mulighet for å få produsert relevant læremateriell? Både konferanse og tidskrift ble diskutert. Til slutt diskuterte vi organisering av arbeidet med en rapport om arbeidsgruppens arbeid.
10.10.2019, 12:00–14:00 Digitalt	**Arbeidsgruppemøte 8, IKT-sikkerhet i utdanningene**: Vi gikk gjennom tilbakemeldinger fra UHR-MNT-AU. Etter det gikk vi gjennom de arbeidsoppgavene som gjenstår og la en plan for å fullføre disse. Vi diskuterte også hva som bør gjøres med hensyn på læremateriell. Til slutt arbeidet vi med rapporten.

Når og hvor	*Beskrivelse*
31.10.2019, 12:00–14:00 Digitalt	**Arbeidsgruppemøte 9, IKT-sikkerhet i utdanningene**: Vi startet med status utkast til ny disposisjon og innhold for nasjonale retningslinjer til forskrift om rammeplan for ingeniørutdanning av mai 2018. Vårt bidrag hit ble også diskutert. Vi brukte noe tid på utkast til læringsutbyttebeskrivelser og status på arbeidet med integrasjon av læringsmål i studieplaner. Vi gikk også gjennom utkast til en lærebok [3] og fordelte oppgaver frem til neste møte i Narvik.
26.11.2019, 16:00–18:00 Narvik, NIKT 2019	**Arbeidsgruppemøte 10, IKT-sikkerhet i utdanningene**: Vi hadde tre hovedtema på agendaen på dette fysiske møtet: Konkrete forslag på utvikling av læringsmateriell, diskusjon rundt læringsmålene og sluttføre denne delen av arbeidet med en konkret plan for hvordan.
16.12.2019, 10:00–12:00 Digitalt	**Arbeidsgruppemøte 11, IKT-sikkerhet i utdanningene**: Fokus på dette møtet var arbeidet med å ferdigstille læringsmåldokumentet. Vi diskuterte også noe om hvordan være læringsutbyttebeksrivelser kan skrives inn i retninglinjene for ingeniørutdanningene (må være mer kompakt enn våre generelle anbefalinger).
16.01.2020, 10:00–12:00 Digitalt	**Arbeidsgruppemøte 12, IKT-sikkerhet i utdanningene**: Vi ble enig om at i det videre arbeidet skal vi produsere tre dokumenter som tilsammen vil være vår rapport fra arbeidet. Det første dokumentet presenterer og utdyper læringsutbyttebeksrivelsene vi anbefaler. Den andre dokumentet diskuterer hvordan læringsmålene kan integreres i ulike utdanninger, inklusiv et fokus på ingeniørutdanningene. Det tredje dokumentet omhandler behov for, og tilgjengelighet av, læremateriell, og en diskusjon om hvordan man skal få produsert relevant læremateriell. Avsluttet med planlegging av dette arbeidet.
13.02.2020, 10:00–12:00 Digitalt	**Arbeidsgruppemøte 13, IKT-sikkerhet i utdanningene**: I hovedsak diskusjon rundt fremdrift av arbeidet og fordeling av arbeidsoppgaver. Vi diskuterte også deltakelse og bidrag på Nasjonal konferanse om retningslinjer til forskrift om rammeplan for ingeniørutdanningene i mars (denne ble senere avlyst og erstattet av dialogmøtet 18. juni).

A.3 Arbeidsgruppens deltakelse på konferanser og andre møter

Når og hvor	*Beskrivelse*
3. januar, 2019 Gardermoen	**Workshop – Nasjonale retningslinjer for ingeniørutdanning**: Presentasjon av implementering av IKT-sikkerhet i studieprogrammer ved egen isntitusjon, presentert av et utvalg av medlemmer i arbeidsgruppen.
20. mars, 2019 Oslo	**NSM Sikkerhetskonferansen 2019**: Presentasjon av arbeidsgruppens arbeid og invitasjon til innspill og kommentarer på utkast til læringsmål.
28.–29. mars, 2019 Tromsø	**MNT-konferansen 2019**: Presentasjon av arbeidsgruppens arbeid og invitasjon til innspill og kommentarer på utkast til læringsmål.
8. mai, 2019 Gjøvik	**Nasjonalt fagorgan for IKT**: Presentasjon av status arbeidsgruppens arbeid til Nasjonalt fagorgan for IKT, som er arbeidsgruppens referansegruppe.
23. mai, 2019 Oslo	**UHR-MNT-AU**: Presentasjon av status arbeidsgruppens arbeid for arbeidsutvalget til UHR sin fagstrategiske enhet for matematiske, naturvitenskapelige og teknologiske fag (UHR-MNT-AU), som er arbeidsgruppens styringsgruppe.
26.–28. august, 2019 Lillehammer	**Sikkerhetsfestivalen 2019**: Presentajon av arbeidsgruppens arbeid og deltakelse i panledebatt om IKT-sikkerhet i utdanninger.
25. november, 2019 Narvik	**Nasjonalt fagorgan for IKT**: Presentajon av status i arbeidet til arbeidsgruppen i UHR sitt nasjonale Nasjonalt fagorgan for IKT.
23. januar, 2020	**UHRs strategiske enheter**: Presentajon av arbeidet til arbeidsgruppen for UHRs strategiske enheter.

Når og hvor	*Beskrivelse*
18. juni, 2020 Digitalt	**Dialogmøte om Nasjonale retningslinjer til forskrift om rammeplan for ingeniørutdanning**: Presentajon og utdyping av de anbefalte læringsutbyttebeskrivelsene i IKT-sikkerhet for ingeniørutdanninger fra arbeidsgruppen.
23. oktober, 2020 Digitalt	**Møte om Nasjonale retningslinjer for ingeniørutdanning**: Tilbakemelding fra ledere av fagorgan.
25. november, 2020 Digitalt	**Møte UHR-MNT**: Presentasjons av arbeidsgruppens arbeid for UHR sin fagstrategiske enhet for matematiske, naturvitenskapelige og teknologiske fag (UHR-MNT).
15.–16. mars, 2021 Kristiansand (digitalt)	**MNT-konferansen 2021**: Presentajon av arbeidsgruppens anbefalinger for styrkning av IKT-sikkerhet i utdanninger.

Tillegg B

Andre bidrag fra arbeidsgruppen

B.1 Web-siden «IKT-sikkerhet i utdanningene»

Arbeidsgruppen har lagd en web-side hvor resultatene av arbeidet til arbeidsgruppen presenteres:

`https://uit.no/project/iktsikkerhetiutdanning`

Denne siden er ment å være en ressurs for de som skal arbeide med IKT-sikkerhet i utdanninger. Her vil også eventuelle oppdateringer av arbeidsgruppens arbeidet bli gjort tilgjengelig.

B.2 Andre publikasjoner og presentasjoner

Type	*Beskrivelse*
Presentasjon	IKT-sikkerhet i utdanningene. Anders Andersen. *Sikkerhetskonferansen 2019 Nasjonal Sikkerhetsmyndighet (NSM)*, 20. mars 2019, Oslo.
Artikkel	Informasjonssikkerhet i høyere utdanning. Anders Andersen, Tor Berre, Pål Ellingsen, Laurence Habib, Moutaz Haddara, Erik Hjelmås, Mette Mo Jakobsen, Audun Jøsang, Tom-Heine Nätt, Jingyue Li, Arne Roar Nygård, Sondre Rønjom, Hans Georg Schaathun, Arild Steen, Tor-Fredrik Torgersen. *MNT-konferansen 2019*, 28.–29. mars, Tromsø. Se Vedlegg B.4 [1].
Presentasjon	Informasjonssikkerhet i høyere utdanning. Anders Andersen. *MNT-konferansen 2019*, 28.–29. mars, Tromsø.
Presentasjon og panel	Nasjonal arbeidsgruppe styrking av undervisningstilbud i IKT-sikkerhet. Anders Andersen. *Sikkerhetsfestivalen 2019*, 27. august 2019, Lillehammer.
Presentasjon	Status nasjonal arbeidsgruppe IKT-sikkerhet i utdanning. Anders Andersen. *UHR sitt nasjonale fagråd for IKT-utdanningene*, 25. november 2019, Narvik.
Presentasjon	IKT-sikkerhet i MNT-utdanning. Anders Andersen. *MNT-konferansen 2021*, 15.–16. mars 2021, Kristiansand.

B.3 Utdrag fra «Nasjonale retningslinjer for ingeniørutdanningene»

Teksten under er et utdrag fra «Nasjonale retningslinjer for ingeniørutdanningene» [38], og utdraget er hentet fra delkapitlet «IKT, programmering og IKT-sikkerhet». Teksten er også arbeidsgruppen sitt innspill til arbeidet med de nye retningslinjene for ingeniørutdanningene.

3.2.3.2 IKT-sikkerhet

Kompetanse om IKT-sikkerhet finner vi både i bredde- og spesialistutdanninger. I en ingeniørutdanning må kandidatene lære hva informasjonssikkerhet er og hvorfor ingeniører må tenke sikkerhet i hele livssyklusen av IT-systemer og teknologisystemer generelt.

I et samfunn med økt digitalisering, hvor IKT er sentralt på alle områder, både i privatlivet og arbeidslivet, er sårbarheter og risikoer som en følge av dette en stor utfordring. IKT-sikkerhet som fagområde skal bidra til å håndtere disse utfordringene. Behovet for kompetanse om IKT-sikkerhet er derfor sterkt økende, ikke bare som eget fagområde, men også som en integrert del av ingeniørutdanningene.

En utfordring ved opplæring i IKT-sikkerhet, og andre tema preget av en rivende teknologisk utvikling, er generell historieløshet på fagfeltet. Historien er en felles bakgrunnskompetanse som vi alle kan bygge ut ny forståelse fra. For eksempel, så har alle nye ingeniørstudenter et felles begrepsapparat og en felles basiskompetanse fra tidligere skolegang i fag som matematikk og fysikk. Noe tilsvarende finner vi ikke i IKT-sikkerhet i dag.

En annen utfordring ved opplæring i IKT-sikkerhet er å gjøre opplæringen relevant for studentenes fagområde. Hvis det ikke tas hensyn til dette er det en risiko for at studentene ikke klarer å innarbeide IKT-sikkerhet i sin faglige forståelse, og i stedet pugger IKT-sikkerhet som fragmenterte kunnskapsenheter uten relevans i eget fag.

Alle ingeniørutdanninger bør inkludere læringsutbytte fra følgende tema innen IKT-sikkerhet:

1. Grunnleggende begreper
2. Bevissthet og sikkerhetskultur
3. Personvern
4. Lover, reguleringer og etikk
5. Trusselmodellering og risikostyring
6. Sikkerhetsarkitektur og innebygd informasjonssikkerhet

Basert på disse temaene vil læringsutbytte innen IKT-sikkerhet for ingeniørutdanninger være som beskrevet under.

Kunnskap

a) Kandidaten behersker de mest sentrale begrepene innen IKT-sikkerhet (tema 1)

b) Kandidaten har en grunnleggende forståelse av trusler og sårbarhet i samfunnet, med særlig vekt på hvordan digitalisering påvirker dette i egen profesjon (tema 2 og 5)

c) Kandidaten har kunnskap om når behovet for personvern trer i kraft og typiske tilnærminger for beskyttelse og anonymisering av persondata (tema 3)

d) Kandidaten kan gi en oversikt over de mest relevante lover, forskrifter og standarder for IKT-sikkerhet, og deres overordnede anvendelse innenfor eget fagområde (tema 4)

e) Kandidaten er kjent med grunnleggende tekniske sikkerhetsmekanismer og deres muligheter og begrensninger (tema 6)

f) Kandidaten er kjent med behovet for å tenke helhetlig sikkerhet under utvikling, produksjon, drift og avvikling av systemer (tema 6)

Ferdigheter

a) Kandidaten kan argumentere for viktigheten av god cyber-hygiene (rutiner og oppførsel), brukeropplæring i IKT-sikkerhet, og bevissthet rundt IKT-sikkerhetstrusler og sårbarheter (tema 2)

b) Kandidaten kan vurdere om et system forvalter sensitive persondata og identifisere behov for beskyttelse av persondata (tema 3)

c) Kandidaten kan vurdere hvordan systemer innen sitt fagområde kan bli utsatt for ulike typer IKT-angrep, prioritere risiko og lage planer for risikoredusering (tema 5)

Generell kompetanse

a) Kandidaten kan delta i diskusjoner om IKT-sikkerhet (tema 1)

b) Kandidaten kan samarbeide om, og utvise ansvarlighet overfor, IKT-sikkerhet (tema 2 og 3)

c) Kandidaten kan diskutere etiske utfordringer knyttet til IKT-sikkerhet (tema 4)

d) Kandidaten er i stand til å gjennomføre enkle risikovurderinger (tema 5)

B.4 Artikkel: Informasjonssikkerhet i høyere utdanning

På de neste sidene er artikkelen «Informasjonssikkerhet i høyere utdanning» [1] lagt ved. Arbeidsgruppen skrev denne artikkelen i en tidlig fase av sitt arbeid. Artikkelen ble presentert på MNT-konferansen i Tromsø i mars 2019 og den er publisert i artikkelsamlingen til denne konferansen (Nordic Journal of STEM Education, Vol. 3 No. 1, 2019).[1] Artikkelen beskriver arbeidet som var gjort så langt og planene for det videre arbeidet.

[1] https://www.ntnu.no/ojs/index.php/njse/article/view/2992

MNT-konferansen 2019, 28.-29. mars, Tromsø

Informasjonssikkerhet i høyere utdanning

Anders Andersen[1], Tor Berre[2], Pål Ellingsen[3], Laurence Habib[4], Moutaz Haddara[5], Erik Hjelmås[2], Mette Mo Jakobsen[6], Audun Jøsang[7], Tom-Heine Nätt[8], Jingyue Li[2], Arne Roar Nygård[9], Sondre Rønjom[10], Hans Georg Schaathun[2], Arild Steen[1], Tor-Fredrik Torgersen[11]

[1]UiT Norges arktiske universitet
[2]NTNU Norges teknisk-naturvitenskapelige universitet
[3]Høgskulen på Vestlandet (HVL)
[4]OsloMet
[5]Høyskolen Kristiania
[6]Universitets- og høgskolerådet (UHR)
[7]Universitetet i Oslo (UiO)
[8]Høgskolen i Østfold (HiØ)
[9]Eidsiva
[10]Nasjonal sikkerhetsmyndighet (NSM)
[11]Universitetet i Stavanger (UiS)

ABSTRAKT: Stortingsmeldingen om *IKT-sikkerhet: Et felles ansvar* (2017) ble behandlet 10. april 2018. Et av de viktigste vedtakene som Stortinget fattet er at alle relevante ingeniør- og teknologiutdanninger skal ha informasjonssikkerhet inn i studiene. En oppfølgning av stortingsmeldingen var en revidert forskrift om rammeplan for ingeniørutdanning som ble vedtatt i mai 2018. Som følge av dette ble det opprettet en arbeidsgruppe for å utarbeide en strategi for hvordan Stortingets vedtaket bør settes ut i praksis, dvs. for å utarbeide en kompetansestrategi for IKT-sikkerhet. Denne artikkelen beskriver kort arbeidet som er gjort så langt, og planer for det videre arbeidet frem mot overlevering av rapporten om kompetansestrategien i mars 2020.

NØKKELORD: IKT-sikkerhet, ingeniørutdanninger, undervisning

1 BAKGRUNN

IT-eksperter uten kunnskap om IT-sikkerhet er som bygningsarkitekter uten kunnskap om brannsikkerhet. Det ville være uforsvarlig å utdanne bygningsarkitekter uten å gi dem kunnskap om brannsikkerhet. På samme måte er IT-utdanning uten obligatoriske moduler i informasjonssikkerhet like uforsvarlig. Likevel har det vært, og til dels fremdeles er, vanlig praksis at IT-utdanninger ikke har informasjonssikkerhet som obligatorisk del på programmet.

Det blir uttrykt fra mange hold at kunnskap om informasjonssikkerhet er en grunnleggende kompetanse som er viktig ikke bare for IT-fagene, men for all høyere utdanning, og i tillegg på lavere trinn som i videregående skole og på barne- og ungdomstrinnet.

Sammenlignbare land er også klar over mangelen på IKT-sikkerhetskompetanse. Danmark, Sverige, Nederland og Storbritannia har nasjonale strategier for å håndtere utfordringer knyttet til IKT-sikkerhet, herunder IKT-sikkerhetskompetanse. Strategiene varierer i konkretiseringsgrad og ambisjonsnivå. Den mest ambisiøse og konkrete strategien har Storbritannia, hvor NOK 16 milliarder avsettes frem til 2021 for å håndtere IKT-sikkerhetsutfordringene.

Stortingsmelding 38 (2016–2017) *IKT-sikkerhet - Et felles ansvar* [1] ble behandlet 10. april 2018. Et av de viktigste vedtakene Stortinget fattet er at alle relevante ingeniør- og teknologiutdanninger skal ha informasjonssikkerhet inn i studiene. Som følge av stortingsmeldingen ble revidert forskrift om rammeplan for ingeniørutdanning vedtatt i mai 2018 [2]. Sikkerhetskompetanse er både en bredde- og en spesialistutdanning. I bredden må alle skjønne hva informasjonssikkerhet er og hvorfor ingeniører og IT-arkitekter må tenke sikkerhet, ikke bare i designfasen, men i hele livssyklusen av IT-systemer og teknologisystemer generelt. Samtidig trengs det eksperter som har informasjons- og cybersikkerhet som spesialfelt for å kunne lede arbeidet med informasjonssikkerhet og for å kunne håndtere og respondere til alvorlige sikkerhetshendelser i organisasjoner.

MNT-konferansen 2019, 28.-29. mars, Tromsø

Denne artikkelen gir en første beskrivelse av arbeidet med å definere en kompetansestrategi for IKT-sikkerhet, som i første rekke skal gi konkrete anbefalinger for 3-årig ingeniørutdanning og andre MNT-utdanninger, men det er også relevant å se på hva som bør gjelde for høyere utdanning generelt, inkludert etter- og videreutdanning. Det diskuteres også hvorvidt strategien også skal gi anbefalinger om IKT-sikkerhet i videregående skole, og på barne- og ungdomstrinnet. Artikkelen er basert på det innledende arbeidet i en arbeidsgruppe som er opprettet for å styrke undervisningstilbud i IKT-sikkerhet.

2 STORTINGSMELDINGEN OG DENS VIDERE OPPFØLGING

2.1 Stortingsmelding 38 (2016–2017): IKT-sikkerhet - Et felles ansvar

Ovennevnte stortingsmelding [1] sier i sammendraget bl.a. at *«Regjeringen vil legge til rette for en langsiktig oppbygging av IKT-sikkerhetskompetanse gjennom en nasjonal kompetansestrategi for IKT-sikkerhet. IKT-sikkerhet gjelder alle. Ved at de unge tidlig lærer trygg bruk og forstår nødvendigheten av IKT-sikkerhet, legges grunnlaget for at oppvoksende generasjoner har med seg IKT-sikkerhetskompetanse inn i det videre utdanningsløpet og arbeidslivet.»*

Behovet for mer og bedre utdannet IKT-sikkerhetspersonell er allerede understreket i flere tidligere utredninger, bl.a. i Lysneutvalgets utredning [3], i Stortingsmelding 10 (2016–2017) *Risiko i et trygt samfunn* [4] og Stortingsmelding 27 (2015–2016) *Digital agenda for Norge* [5]. Stortingsmeldingen [1] går lenger enn de nevnte tidligere utredninger, bl.a. ved å påpeke viktigheten av IKT-sikkerhet i alle typer høyere utdanning. På den bakgrunn foreslår stortingsmeldingen [1] følgende sentrale tiltak for å økt kompetanse i informasjonssikkerhet:

- etablere en nasjonal kompetansestrategi for IKT-sikkerhet, der blant annet behovet for studieplasser og forskningssatsning vurderes,
- gjennom den påbegynte fagfornyelsen i grunnopplæringen, vurdere hvorvidt IKT-sikkerhet er tilstrekkelig inkludert i den grunnleggende digitale kompetansen elevene skal tilegne seg,
- styrke IKT-sikkerhetskompetansen i tilsyn,
- legge vekt på systematisk oppfølging og læring etter både øvelser og hendelser, også ved digitale hendelser.

2.2 Vedtak på bakgrunn av Stortingsmeldingen 10. April 2018

Stortingsmeldingen [1] ble behandlet på Stortinget 10. april 2018. Etter en diskusjon rundt ulike vedtaksforslag ble følgende vedtak faktisk gjort [6]:

1. Stortinget ber regjeringen sørge for at relevante ingeniør- og teknologiutdanninger har kurs i IKT-sikkerhet.
2. Stortinget ber regjeringen sørge for at det stimuleres til bedre etter- og videreutdanningstilbud på fagskoler, universiteter og høyskoler innen IKT- og datasikkerhet.
3. Stortinget ber regjeringen sørge for at digitalisering og IKT-sikkerhet prioriteres i neste Langtidsplan for forsking og høyere utdanning.
4. Stortinget ber regjeringen legge fram en plan som synliggjør politiets arbeid med IKT-kriminalitet og hvordan dette skal finansieres.

Vedtak 1 og 2 er relevant for arbeidet med kompetansestrategien for IKT-sikkerhet

2.3 Arbeidsgruppe for kompetansestrategien for IKT-sikkerhet

Etter Stortingets vedtak 10. april 2018 ble det bevilget midler til å utarbeide en kompetansestrategi for IKT-sikkerhet. Kunnskapsdepartementet ber om at Universitets- og høgskolerådets fagstrategiske enhet for matematiske, naturvitenskapelige og teknologiske fag (UHR-MNT) koordinerer et samarbeid mellom institusjonene som tilbyr ingeniør- og IKT-utdanninger for å legge mer vekt på IKT-sikkerhet i utdanningene. Samarbeidet skal bidra til tiltak som kan øke kvaliteten på og omfanget av IKT-sikkerhet i utdanningene. Arbeidsutvalget til UHR-MNT ber Nasjonalt fagorgan for IKT om å etablere en arbeidsgruppe med bred representasjon fra akademia, statlig sektor og næringsliv. Leder for denne arbeidsgruppen er Anders Andersen fra UiT.

Arbeidsutvalget til UHR-MNT ber om at den opprettede arbeidsgruppen planlegger og gjennomfører et prosjekt for styrking av undervisningstilbud i IKT/IKT-sikkerhet. Arbeidsgruppen bes om å utforme forslag til hvordan det rammeplanfestede kravet om implementering av IKT-sikkerhet i ingeniør-

utdanningene bør gjennomføres ved utdanningsinstitusjonene. Oppdraget inkluderer å si noe om når i studieløpet undervisning bør legges inn, hvordan (eget emne og/eller integrert i øvrige emner), omfang og faglig innhold. Arbeidsgruppen bes også gi råd om hvordan IKT-sikkerhet bør implementeres i realfag og sivilingeniørutdanning. Arbeidsutvalget til UHR-MNT er styringsgruppe for prosjektet.

21. november hadde arbeidsgruppen sitt første nett-baserte planleggingsmøte. Det første arbeidsmøtet i arbeidsgruppen ble avholdt på Gardermoen 3. januar 2019.

3 DAGENS LANDSKAP

Som premiss for arbeidet med kompetansestrategi for IKT-sikkerhet er det nyttig å ha god oversikt over landskapet der en slik strategi skal passe inn. Det første møtet i arbeidsutvalget fremla kort status for eksisterende utdanningsprogrammer for IKT-sikkerhet, og diskuterte forskriftsmessige krav til innholdet i ingeniørutdanningen.

3.1 Status for studieprogrammer innen informasjonssikkerhet

NTNU, UiB, UiO, UiA har etablert studieprogrammer som fokuserer på informasjonssikkerhet. NTNU har i mange år allerede hatt bachelor- og masterprogram for informasjonssikkerhet. UiB opprettet et bachelorprogram for informasjonssikkerhet i 2016. UiA starter et masterprogram i informasjonssikkerhet i 2019. UiO startet en masterspesialisering i informasjonssikkerhet i 2018 og planlegger et separat masterprogram i informasjonssikkerhet fra 2020. HiØ starter et bachelorprogram i informasjons-sikkerhet 2019. UiS har et masterprogram om risikostyring og beredskap. UiT starter en studieretning i IKT-sikkerhet i sitt 5-årige integrerte masterprogram (sivilingeniør) i 2020. Denne listen er ikke ment å være uttømmende. Det fins antageligvis flere studieprogrammer innen informasjons-sikkerhet som enten allerede er opprettet, eller som planlegges opprettet i nær framtid.

I tillegg fins som regel obligatoriske og/eller valgfrie emner i sikkerhet i IKT- utdanningsprogrammer i alle landets universiteter og høgskoler. Innenfor ingeniørutdanninger som følger rammeplanen er kravet om IKT-sikkerhet nytt og det er foreløpig ingen som har kommet langt i konkretisering av dette kravet. Det siste punktet er nettopp en av hovedårsakene for å utarbeide en kompetansesikkerhet for IKT-sikkerhet. Det er ikke tilstrekkelig at bare IKT-utdanninger gir kompetanse i informasjonssikkerhet, det må defineres som et krav at all (teknisk) høyere utdanning gir slik kompetanse.

3.2 Forskriftsmessige krav til innholdet i ingeniørutdanningen

Hovedretninger innen ingeniørutdanningen er: 1) byggingeniør, 2) dataingeniør, 3) elektroingeniør, 4) kjemiingeniør, 5) maskiningeniør. I tillegg kommer tverrfaglige utdanningsprogrammer som for eksempel samfunnssikkerhet (HMS), mekatronikk, produkt og produksjon.

For all treårig ingeniørutdanning gjelder forskrift om rammeplan for ingeniørutdanning. Den definerer læringsutbytte som er felles for alle fagfelt og studieprogrammer. For eksempel er det fastsatt i forskriften at 3-årig ingeniørutdanning skal inneholde minst 20 studiepoeng i matematikk og minst 5-studiepoeng i statistikk. I ny forskrift for rammeplan for ingeniørutdanning fastsatt av Kunnskapsdepartementet 18. mai 2018 [2] er en av de viktigste endringene en ny læringsutbytte-beskrivelse om IKT-sikkerhet:

> *Kandidaten kan identifisere sikkerhets-, sårbarhets-, personverns- og datasikkerhetsaspekter i produkter og systemer som anvender IKT.*

I forskriften er det definert at det skal utarbeides felles nasjonale retningslinjer for ingeniørutdanning Arbeidsgruppen ser for seg at det må legges inn i de nasjonale retningslinjene for ingeniørutdanning et krav om et minimum antall studiepoeng innen informasjonssikkerhet. Læringsutbyttebeskrivelsen over er heller ikke spesifikk og dekkende nok som en beskrivelse av IKT-sikkerhetsinnholdet i en ingeniørutdanning.

4 BASISELEMENTER FOR KOMPETANSE I IKT-SIKKERHET

Informasjonssikkerhet er et svært stort fagområde, og internasjonalt foregår betydelig arbeid med å definere hva studieprogrammer innen informasjons- og cybersikkerhet bør inneholde [7,8]. Disse aktivitetene produserer fagoversikter innen informasjonssikkerhet som til dels er overveldende og derfor uegnet som et direkte grunnlag for vår nasjonale kompetansestrategi for IKT-sikkerhet.

MNT-konferansen 2019, 28.-29. mars, Tromsø

På grunn av den overveldende størrelsen på fagområdet Informasjonssikkerhet ville det være forvirrende hvis kompetansestrategien for IKT-sikkerhet bare gir anbefaling om f.eks. minst 5 studiepoeng informasjonssikkerhet, uten en mer spesifikk beskrivelse av hva disse studiepoengene bør dekke. For å fjerne forvirring på dette området diskuterte arbeidsgruppen på arbeidsmøtet 3. januar 2019 kort grunnleggende elementer innen informasjonssikkerhet som bør dekkes uansett hovedretning innen ingeniørutdanningen, eller i høyere utdanning generelt. Utkast til liste over hovedelementer er følgende:

- Grunnleggende begreper
  - F.eks. KIT (Konfidensialitet, integritet og tilgjengelighet), autentisering og tilgangskontroll
- Bevissthet og sikkerhetskultur
  - Styring/ledelse/internkontroll av informasjonssikkerhet i organisasjoner
- Trusselmodellering og risikostyring
  - Kjennskap til angrepsmetoder og vurdering av sikkerhetstiltak
- Sikkerhetsarkitektur og innebygd informasjonssikkerhet
  - Teknisk IT-sikkerhet og sikkerhet under utvikling og drift av IT-systemer
- Innebygd personvern
  - Hensyn til personvern i alle ledd under design og drift av IT-systemer
- Lovverk / etikk
  - Relevante lovverk, krav til etterlevelse og etiske avveininger

En forståelse av grunnleggende begreper innen IKT-sikkerhet er viktig for å kunne kommunisere muntlig og skriftlig om temaet. De er nødvendig med en bevissthet i at bruk av IKT innebærer en sikkerhetsrisiko. En mangel på en sikkerhetskultur som har fokus på slik risiko kan få store følger. Trusselmodellering og risikostyring gir oss et verktøy for å håndtere dette hvor vi kan identifisere problemområder og evaluere risikoen for hvert område opp mot kostnaden for å håndtere dem. Det er viktig å kunne organisere arbeidet og praksis i utviklingsprosjekt slik at en kan sikre en helhetlig sikkerhet i produktet. Dette gjeld både programutvikling og utvikling av fysiske system. Ved realisering av IT-systemer brukes sikkerhetsarkitektur og innebygd informasjonssikkerhet for å håndtere trusler og begrense risiko. Det er nødvendig med en helhetlig forståelse av sikkerhet både under utvikling (programmering) og drift av IT-systemer for å kunne oppnå dette.

Personvern handler om retten til et privatliv og selvbestemmelse over egne personopplysninger. Dette er en lovfestet rett i Norge som er blitt ytterlige styrket av de nye personvernreglene som er innført i hele EU/EØS i 2018 [9]. En forståelse av konsekvensene av personvern og bruk av personopplysninger i IKT-baserte løsninger bør være inkludert i høyere utdanning. Og nært beslektet med dette vil behovet for en kompetanse av hvordan etikk og lover og reguleringer påvirker bruk og utvikling av IKT-baserte systemer.

5 VIDERE ARBEID

Arbeidsgruppen har nett-basert møte omtrent hver fjerde uke. I disse møtene diskuteres utvalgte og konkrete problemstillinger knyttet til gruppens leveranse. Det lages også konkrete arbeidsoppgaver frem til neste møte. Arbeidsgruppen vil også ha noen fysiske møter for å jobbe konkret med leveransen.

Arbeidsgruppens arbeid inkluderer:

- Kartlegge og dokumentere: behov, anbefalinger og relevant innhold i eksisterende studier
- Analysere, utrede og skape dialog om hvordan IKT-sikkerhet kan styrkes i utdanningene
- Utprøve og eksperimentere med konkrete studieplaner (utfordrende med hensyn på tid)
- Lage anbefalinger for å styrke IKT-sikkerhet i utdanning

Arbeidet er delt i 5 noe overlappende faser:

1. Kartlegging: Hva finner vi i dag (emner, læringsmål, anbefalinger, læremateriell)?
2. Hvilke kunnskaper og ferdigheter omfattes av arbeidsgruppens arbeid?
3. Hvilke kunnskaper og ferdigheter anbefaler vi i ulike studier (minimum, fordypning)
4. Strukturere leveransen (hvordan kan vi best mulig gi våre anbefalinger?)
5. Ferdigstille leveransen

Arbeidsgruppen er godt i gang med fase 1 og 2, og har påbegynt arbeidet i fase 3.

6 KONKLUSJON

Arbeidsgruppen har kommet i gang med sitt arbeid med å utforme forslag til hvordan det rammeplanfestede kravet om implementering av IKT-sikkerhet i ingeniørutdanningene bør gjennomføres ved utdanningsinstitusjonene. Arbeidsgruppen vil også inkludere i arbeidet sitt et forslag om hvordan IKT-sikkerhet bør implementeres i realfag og sivilingeniørutdanning og i andre utdanninger. Arbeidsgruppen diskuterer også om den skal gi anbefalinger om IKT-sikkerhet i videregående skole, og på barne- og ungdomstrinnet.

Til nå har arbeidsgruppen startet et arbeid med kartlegging av området IKT-sikkerhet. Dette inkluderer en gjennomgang av rapporter og utredninger relevant for arbeidet, en gjennomgang av eksisterende utdanninger, emner og læringsmål knyttet til IKT-sikkerhet, og en intern presentasjon i arbeidsgruppen av det erfaringsgrunnlaget vi finner her. I tillegg har arbeidsgruppen starter den første diskusjonen om hovedelementene som bør inngå bør dekkes innen informasjonssikkerhet i ingeniørutdanningene, eller i høyere utdanning generelt.

Arbeidsgruppen er åpen for innspill fra andre. Hva er de grunnleggende elementene innen IKT-sikkerhet, hva bør minimum inngå i de ulike utdanningene og hvordan bør dette organiseres?

REFERANSER

[1] Stortingsmelding 38 (2016-2017): *IKT-sikkerhet – Et felles ansvar.* Tilråding fra Justis- og beredskaps-departementet 9. juni 2017.

[2] Forskrift om rammeplan for ingeniørutdanning. Fastsatt av Kunnskapsdepartementet 18. mai 2018 med hjemmel i lov av 1. april 2005, nr. 15 om universiteter og høyskoler (Universitets- og høyskoleloven) § 3-2 annet ledd.

[3] NOU 2015:13: *Digital sårbarhet, sikkert samfunn – Beskytte enkeltmennesker og samfunn i en digitalisert verden*. Utredning fra et utvalg oppnevnt ved kongelig resolusjon 20. juni 2014. Avgitt til Justis- og beredskapsdepartementet 30. november 2015.

[4] Stortingsmelding 10 (2016-2017): *Risiko i et trygt samfunn – Samfunnssikkerhet*. Tilråding fra Justis- og beredskapsdepartementet 9. desember 2016.

[5] Stortingsmelding 27 (2015-2016): *Digital agenda for Norge - IKT for en enklere hverdag og økt produktivitet*. Tilråding fra Kommunal- og moderniseringsdepartementet 15. april 2016.

[6] Stortingstidende. Referat fra møter i Stortinget, Nr. 63 · 10. april 2018. Sesjonen 2017–2018.

[7] Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. Joint Task Force on Cybersecurity Education. (ACM, IEEE-CS, AIS-SIGSEC, IFIP-WG-11.8), 31.12.2017.

[8] Parrish, A., Impagliazzo, J., Raj, R.K., Santos, H., Asghar, M.R., Jøsang, A., Pereira, T., Sá, V.J., Stavrou, E. (2018). Global perspectives on cybersecurity education. *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE 2018)*, Cyprus, July 2018.

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR), http://data.europa.eu/eli/reg/2016/679/2016-05-04.

B.5 IKT-sikkerhet i lys av eksisterende retningslinjer

Av Hans Georg Schaathun

> *Denne teksten er skrevet tidlig i arbeidsgruppens arbeid og er tatt med her fordi den er en interessant diskusjon om integrasjon av IKT-sikkerhet i ingeniørutdanningene. Det er nyttig å lese teksten for de som arbeider med en slik integrasjon. Teksten er skrevet før de nye retningslinjene for ingeniørutdanningene var kjent.*

Dette er en innledning til diskusjon om hvordan retningslinjer for IKT-sikkerhet kan struktureres sammen med resten av retningslinjene. Utgangspunktet er retningslinjene fra 2011 sammen med de arbeidsdokumenter og opplysninger som vi har fått om den øvrige revisjonsprosessen.

Studiets struktur

Forskriften slår fast at ingeniørstudiet består av

- 30 studiepoeng fellesemner som består av grunnleggende matematikk, ingeniørfaglig systemtenking og innføring i ingeniørfaglig yrkesutøvelse og arbeidsmetoder. Emnene i fellesemner er felles for alle studieprogram.
- 50 studiepoeng programemner som består av tekniske fag, realfag og samfunnsfag. Programemner er felles for alle studieretninger i et studieprogram.
- 70 studiepoeng tekniske spesialiseringsemner som gir en tydelig retning innen eget ingeniørfag, og som bygger på programemner og fellesemner.
- 30 studiepoeng valgfrie emner som bidrar til faglig spesialisering, enten i bredden eller dybden.

På tvers av inndelingen over, definerer retningslinjene flere støttefag med felles læringsmål og omfang langt utover fellesemnene. Dette gjelder særlig matematikk (10 sp i tillegg til 10p fellesemne), statistikk (5 sp) og fysikk/kjemi (10 sp). Det faglige ansvaret for disse fagene blir gjerne delegert til fagmiljø som mangler kompetanse på programområdet og dermed ikke kan tolke læringsmålene i sammenheng med studieprogrammets mål. I praksis kan dermed realfagene lett bli oppfattet som fellesemner og sprenge rammen på 30 studiepoeng.

IKT-sikkerhet må plasseres innenfor dette bildet. Krav kan formuleres gjennom læringsmål og/eller studiepoeng. Læringsmål kan formuleres felles eller per programområde.

Felles forståelse av IKT-sikkerhet

Hittil i komitéarbeidet har vi vært enige om at IKT-sikkerhet må innebære

1. Grunnleggende begrepsforståelse
2. Bevissthet og sikkerhetskultur
3. Trusselmodellering og risikostyring
4. Personvern
5. Lovverk/etikk
6. Sikker utvikling

Disse punktene, med mulig unntak for det siste, er i stor grad universelle for alle programområder og kan knyttes til det som kalles «yrkesutøvelse» og «systemtenkning» under fellesemnene. Retningslinjene av 2011 foreslår to emner som skal dekke disse to nøkkelordene, og disse emnene har voldt store utfordringer ved utdannelsesinstitusjonene og mange studiesteder har gitt opp å implementere dem som fellesemner.

Det er nødvendig med en revisjon av denne delen av fellesemnene i forbindelse med ny rammeplan. Siden der ikke er etablert nogen sterk fagtradisjon rundt yrkesutøvelse og systemtenkning, er der rom for å komme inn med nye læringsmål, f.eks. knyttet til sikkerhet.

Forslag til LUB

Nedenfor gjengir vi LUB som foreslått i vedlegg 4–5 i retningslinjene av 2011 med utkast til endringer. Endringene er satt i kursiv. Dette er ment som et konseptprov, for å demonstrere at det er *mulig* å dekke vesentlige sider ved IKT-sikkerhet innenfor disse emnene.

Innføring i ingeniørfaglig yrkesutøvelse og arbeidsmetoder

Kunnskap

a) Kandidaten har en grunnleggende forståelse for ingeniørprofesjonen og ingeniørens rolle i samfunn og arbeidsliv.

b) Kandidaten har kunnskaper som gir grunnlag for å se teknologi både i historisk og fremtidsrettet perspektiv.

c) Kandidaten er kjent med vitenskapelig arbeidsmetode og har basiskunnskaper om prosjekt som arbeidsform, både om organisering, gjennomføring og rapportering.

d) Kandidaten kjenner de grunnleggende prinsippene i effektiv studieteknikk.

e) *Kandidaten har en grunnleggende forståelse av risiko-og sårbarhet i samfunnet, med særlig vekt på hvordan ny teknologi påvirker samfunnets sårbarhet.*

Ferdigheter

a) Kandidatenkan identifisere ingeniørfaglige problemstillinger *og sikkerhetsutfordringer,* søke nødvendig informasjon og kvalitetssikre denne som grunnlag for problemløsning.

b) Kandidaten er kjent med grunnleggende prosesser for innovasjon og nytenkning i forbindelse med prosjektarbeid.

c) *Kandidaten er kjent med grunnleggende prosesser for sikker utvikling*.

Generell kompetanse

a) Kandidaten er bevisst miljømessige, *sikkerhetsmessige* og etiske konsekvenser av teknologiske produkter og løsninger.

b) Kandidaten er kjent med hvordan han kan dele sine kunnskaper og erfaringer med andre, både skriftlig og muntlig, på engelsk og norsk, og kan samarbeide i gruppe.

c) Kandidaten er i stand til å organisere, planlegge og gjennomføre sin studietid, både individuelt og i samarbeid med andre.

Ingeniørfaglig systemtenkning (Vedlegg 5)

Kunnskap

a) Kandidaten har opparbeidet et faglig grunnlag for og forståelse av modelleringsteknikker.

b) Kandidaten har opparbeidet et faglig grunnlag for og forståelse av livsløpsanalyser.

c) Kandidaten har tilegnet seg nødvendige kunnskaper for systemdefinisjon, delsystemer, systemgrenser, systemanalyse, systemsyntese, strategianalyse og usikkerhetsananlyse.

d) Kandidaten har forstått grunnleggende sammenhenger mellom tekniske enkeltelementer og systemmessig helhet.

e) *Kandidaten har forstått den grunnleggende sammenhengen mellom kompleksitet og risiko- og sårbarhet*.

Ferdigheter

a) Kandidaten har opparbeidet ferdigheter i systemmodellering.

b) Kandidaten kan gjennomføre systemanalyse, etablere delsystemer og systemsyntese.

c) Kandidaten kan formidle resultater av systemanalyse og -syntese.

d) *Kandidaten kan gjennomføre og formidle risiko- og sårbarhetsanalyser*.

Generell kompetanse

a) Kandidaten har forståelse av at tverrfaglighet er nødvendig for gode systemløsninger.

b) Kandidaten har konsekvensforståelse (impact), *herunder risiko og sårbarhet*.

c) Kandidaten kan formidle ingeniørfag i en systemmessig kontekst.

d) Kandidaten har utviklet teamegenskaper.

Kommentar til utkastet

Utkastet over viser en naturlig og logisk sammenheng mellom sentrale læringsmål innenfor IKT-sikkerhet og eksisterende læringsmål knyttet til ingeniørdannelse i retningslinjene av 2011. Utkastet nevner ikke IKT eller informasjonssikkerhet, og understreker dermed at de mest grunnleggende læringsmålene for IKT-sikkerhet ikke er spesielle for IKT. Det kan lønne seg å være tydeligere på at IKT-sikkerhet er sentralt, uten å vanne ut kompetansens universalitet.

Ved å skrive IKT-sikkerhet inn i de to eksisterende fellesemnene, fyller vi et hull der få fagmiljø har sterke følelser for tema som blir fortrengt. Det gjør det enklere å få plass til nytt innhold i praksis.

Programvise utfordringer innen IKT-sikkerhet

Programvise læringsmål kan omfatte både kompetanseområder som er spesifikke for et fagfelt og allmenne læringsmål som krever en kontekstualisering innenfor hvert fagfelt.

Innenfor data er det lett å peke på kompetansebehov innenfor IKT-sikkerhet langt utover det som er skissert over; t.eks. sikker koding, autentiseringsløsninger, tekniske sikkerhetsløsninger, etc. Vi bør antagelig utdype læringsmål spesifikt for programområde data, men det er viktig å holde det adskilt fra felles læringsmål og se det i sammenheng med øvrige læringsmål for fagfeltet.

Selv om de felles læringsmålene som er nevnt over bør være sentrale i fellesemnene, skal de ikke nødvendigvis henvises dit alene. Det vil være naturlig å ta opp teknikker og basiskompetanse fra fellesemnene der det er relevant i program- og studieretningsemnene. Man kan endog kreve at program- og studieretningsemner eksemplifiserer sikkerhetsutfordringene for å forsterke læringen fra den ingeniørfaglige basisen.

Didaktiske utfordringer

En utfordring ved opplæring i IKT-sikkerhet og andre tema preget av rivende teknologisk utvikling, er generell historieløshet.

Vi erverver ny kunnskap og forståelse i lys av hva vi allerede kan. Det blir understreket både av Gadamers hermeneutiske filosofi og skjemalæren efter Piaget (samt matteusprinsippet Mat. 13.12-13). Historien er den felles bakgrunnskompetanse som vi alle kan bygge ny forståelse på. Innenfor matematikken er det lett å se hvordan tretusen års historikk er førende for hva og hvordan vi underviser og lærer matematikk.

Dette er antagelig bakgrunnen for at retningslinjene fra 2011 trekker frem «å se teknologi i et historisk perspektiv» som et læringsmål. Dette er ikke nødvendigvis godt ivaretatt innenfor ingeniørutdannelsene i dag, og det er gjerne heller i åndsvitenskaplige miljøer at dette blir vektlagt.

Innenfor IKT-sikkerhet mangler vi en åpenbar, felles historie å bygge faget på. Vi må også regne med at studentenes personlige erfaringer innenfor IKT-sikkerhet eller mangel på sådan er begrenset. Det gir en betydelig risiko for at studentene ikke klarer å innarbeide IKT-sikkerhet i sin fagforståelse, og i stedet pugger IKT-sikkerhet som fragmenterte kunnskapsenheter. Det gjelder spesielt dersom sikkerhetseksperter skal undervise sikkerhet med utgangspunkt i informatikken, mens studentene har sin faglige identitet innenfor t.eks. byggfaget.

Når faget mangler en historie, er vi nødt til å skape en. Det er det mulig å gjøre ved å se det nye faget i sammenheng med etablerte fag som har en viss historie. Det kan bety at datasikkerhet bare er et særtilfelle av andre sikkerhetsfag. Sikkerhetsmodeller kan begynne med å problematisere middelalderens konsentriske borger. Risikoforståelse kan ta utgangspunkt i ingeniørutfordringer preget av høy risiko, som f.eks. romfart. Der er mange muligheter, men ingen som ikke krever betydelig arbeide.

Det er òg mulig å bygge en historie, om enn kort, på offentlig kjente sikkerhetskriser. Utfordringen her er at der er lite forskning å bygge på, og de generaliseringer vi kommer opp med lett blir overfladiske. IKT-sikkerhet som kompetanseområde vil antagelig kunne tjene på om historieperspektivet i ingeniørdannelsen blir styrket, i alle fall dersom vi kan forutsette at historieperspektivet gjennomført brukes til å forstå nutiden.

Oppsummering

Det vil være nyttig å dele diskusjonen i tre, der vi separat ser på mål for fellesemnene, felles læringsmål som bør implementeres i kontekst av studieprogrammet og programspesifikke læringsmål.

Vi har antagelig ikke kompetanse til å spesifisere LUB for andre programområder enn data, men vi kan likevel peke på overfladiske eksempler og behov for videre drøfting i andre fora.

Til diskusjon

1. Er det en god idé å definere IKT-sikkerhet inn i rammen av ingeniørdannelse (yrkesutøvelse og systemtenkning) under fellesemnene?
2. Hvis vi forutsetter at IKT-sikkerhet er en del av ingeniørdannelsen, hvilke læringsmål og momenter skal vi legge vekt på der?
3. Hvilke aspekter ved IKT-sikkerhet får ikke plass i fellesemnene og må håndteres andre steder i retningslinjer? Ingeniørdannelsen, hvilke læringsmål og momenter skal vi legge vekt på?

B.6 IKT-sikkerhet som ingeniørdannelse

Dette er en konkret skisse utarbeidet av medlemmer av arbeidsgruppen med Hans Georg Schaathun fra NTNU i Ålesund i spissen. Dette arbeidet ble opprinnelig gjort tidlig i arbeidsgruppens arbeid, men er i ettertid oppdatert i henhold til de nye retningslinjene for ingeniørutdanningene. Målet med skissen er å vise hvordan IKT-sikkerhet kan integreres i eksisterende studieprogramstruktur og unngå ytterligere fragmentering

Forutsetning

Rammeplanen krever et vesentlig dannelsesaspekt i ingeniørutdannelsen [35]. Begrepet ingeniørdannelse er brukt i retningslinjene fra 2011 [39], og de nye forskriftene [25] har flere læringsmål som faller herunder. Retningslinjene fra 2011 spesifiserer to fellesemner: introduksjonsemnet, normalt første semester, og systememnet, gjerne i sjette semester, med et særlig ansvar for dannelsesaspektet. I de nye retningslinjene [38] finner vi følgende om ingeniørdannelse:

> Digitalisering av samfunnet krever digital kompetanse. Programmering, fagrelevant digital kompetanse, informasjonssikkerhet og personvern er viktige elementer i ingeniørdannelse.

Dette understreker at IKT-sikkerhet er en viktig del av dannelsesaspektet i en ingeniørutdanning.

Denne designskissen tok utgangspunkt i de to fellesemnene fra retningslinjene fra 2011. I de nye retningslinjene er begrepet *Fellesemner* erstattet med *Ingeniørfaglig basis*. Også her er ingeniørdannelse sterkt til stede. Det betyr at denne skissen likevel kan være et nyttig eksempel på hvordan IKT-sikkerhet kan integreres i en ingeniørutdanning, hvor *Introduksjonsemnet* ikke nødvendigvis er et eget emne, men det er en del av *Ingeniørfaglig basis* som kommer tidlig i utdanningen. Tilsvarende vil det *Systememnet* ikke nødvendigvis være et eget emne, men det er en del av *Ingeniørfaglig basis* som kommer litt senere i utdanningen.

Overordnet struktur

IKT-sikkerhet deles i tre:

1. Grunnleggende begrepsforståelse, bevissthet og sikkerhetskultur (Introduksjonemnet)
2. Domenespesifikk sikkerhetskomptanse (Ulike program- og spesialiseringsemner)
3. Sikkerhet i komplekse systemer (Systememnet)

Introduksjonsemnet

Jeg skal ikke gå inn i alle detaljer ved dette emnet, som må dekke alle sider ved ingeniørdannelse. Det er dog klart at sentralt i dette emnet er ingeniørrollen i forhold til resten av verden (samfunnet). Her inngår ansvaret ingeniøren har når hans systemer behandler andre menneskers data, og den risikoen man løper ved å behandle digitale data i utviklingsprosessen.

En sentral del av introduksjonsemnet er å utvikle et felles språk og begrepsapparat som kan brukes i program- og spesialiseringsemnene, slik at likhetene mellom programmene blir synlig. Når det gjelder IKT-sikkerhet kan vi altså vente at studentene lærer

1. Grunnleggende begrepsforståelse: sårbarhet, trussel, kontroll, risiko, konfidensialitet, autentisitet, tilgang, m.fl.
2. Bevissthet og sikkerhetskultur: ansvar ved bruk av institusjonens IT-utstyr, personlig sikkerhet, personvern og sikkerhetskopiering
3. Yrkesetikk, både i forhold til IKT og andre områder.

Det er vesentlig at konseptene blir situerte i ingeniørfagene og i hvert enkelt programområde. Didaktisk er det naturlig å gjøre dette gjennom case-studier, gjerne slik at studentene møter minst ett eksempel fra hvert programområde og flere eksempler fra sitt eget.

Program- og spesialiseringsemner

Program- og spesialiseringsemnene tilhører det enkelte programområde, og vi kan derfor ikke designe disse i nogen detalj. Det er derimot klart at sikkerhetsutfordringer dukker opp i alle studieprogrammer. Begrepsapparatet fra introduksjonsemnet gir et grunnlag for å diskutere utfordringene med en viss faglig tyngde når de dukker opp, uansett emne. Eksemplene i Delkapittel 3.6.3 på side 20 i rapporten illustrerer idéen med eksempler på slike utfrordringer fra byggingeniørfaget.

Når studentene lærer å utvikle systemer, enten det er maskin-, vei- eller datasystemer, må vi forvente at de lærer å identifisere sårbarheter, trusler og mulige kontroller. I noen emner vil IKT-sikkerhet være sentralt. I andre emner bruker man de samme begrepene for å diskutere andre sikkerhetsaspekter. Vi skal understreke at begrepene har samme betydning og ikke er særegne for IKT. Vi skal samarbeide om en generell sikkerhetsforståelse.

Sikker utvikling er et læringsmål som må håndteres konkret innenfor den enkelte disiplin, og som også må tolkes ulikt avhengig av hva som utvikles.

Personvern og lovverk/etikk bør nok spesifiseres som læringsmål under programemnene. Der er domenespesifikke aspekter som bør håndteres her, selv om mye av det felles grunnlaget kanskje får plass i introduksjonsemnet.

Merk at hensikten ikke er å introdusere tungt teoretisk grunnlag for IKT-sikkerhet i disse emnene. Det teoretiske grunnlaget bør i all hovedsak ligge i introduksjonsemnet, og danne grunnlaget for å studere sikkerhetsutfordringer som en naturlig del innenfor det enkelte programområdet.

Systememnet

En grunntanke i systememnet er å samle trådene fra ulike programområder og lære å håndtere utfordringene som oppstår når komponenter fra ulike ingeniørdisipliner skal bygges sammen til systemer. Vi vet at kompleksitet er den største fienden til sikkerhet, og at de største risikoene er å falle mellom to stoler.

Dette emnet må derfor ta for seg trusselmodellering og risikostyring i komplekse systemer. Dette vil selvsagt bygge på tidligere sikkerhetsforståelse.

Tillegg C

Eksterne ressurser

De eksterne ressursene inkluderer nettsider, utredninger, lover og reguleringer, standarder og andre anbefalinger. Disse har vært viktige ressurser i arbeidet til arbeidsgruppen. De er også nyttige ressurser for de som skal arbeide med å realisere IKT-sikkerhet i en utdanning eller som ønsker å arbeide med læremateriell for dette.

C.1 Viktige norske nettsider

Nettside	*URL*
Nasjonal sikkerhetsmyndighet	https://nsm.no/
Datatilsynet	https://www.datatilsynet.no/
NorSIS	https://norsis.no/
Netvett.no	https://nettvett.no/

C.2 Relevante utredninger og styringsdokumenter

Utredning	*Beskrivelse og URL*
Digital sårbarhet – sikkert samfunn (NOU 2015: 13) [28]	I denne NOUen vurderer utvalget (Lysneutvalget) digitale sårbarheter og gir anbefalinger for å redusere disse. https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/
Digital agenda for Norge (Meld. St. 27, 2015–2016) [24]	I denne stortingsmeldingen presenteres regjeringens overordnede politikk for hvordan vi i Norge kan utnytte IKT til samfunnets beste. https://www.regjeringen.no/no/dokumenter/meld.-st.-27-20152016/id2483795/
Risiko i et trygt samfunn (Meld. St. 10, 2016–2017) [16]	I denne stortingsmeldingen redegjøres det for regjeringens politikk for arbeidet med samfunnssikkerhet. https://www.regjeringen.no/no/dokumenter/meld.-st.-10-20162017/id2523238/
IKT-sikkerhet – Et felles ansvar (Meld. St. 38, 2016–2017) [17]	Dette er den første stortingsmeldingen om IKT-sikkerhet. Meldingen presenterer både status (del III) og tiltak (del II). https://www.regjeringen.no/no/dokumenter/meld.-st.-38-20162017/id2555996/

Utredning	*Beskrivelse og URL*
Cybersecurity curricula 2017 [13]	Dette er et internasjonal arbeid for å etablere dekkende og fremtidsrettede læreplaner i IKT-sikkerhet. https://cybered.hosting.acm.org/wp/
Langtidsplan for forskning og høyere utdanning 2019–2028 (Meld. St. 4, 2018–2019) [26]	Denne reviderte Langtidsplanen for forskning og høyere utdanning fra regjeringen skal sette kursen for politikk-utviklingen og investeringene i forskning og høyere utdanning i et tiårsperspektiv (med en konkretisering av mål og innsatsområder for den kommende fire-årsperioden). https://www.regjeringen.no/no/dokumenter/meld.-st.-4-20182019/id2614131/
IKT-sikkerhet i alle ledd (NOU 2018: 14) [11]	I denne NOUen vurderer utvalget behovet for rettslige og organisatoriske endringer innenfor digital sikkerhet. https://www.regjeringen.no/no/dokumenter/nou-2018-14/id2621037/
Nasjonal strategi for digital sikkerhetskompetanse [21]	Strategien angir mål og prioriteringer som skal ligge til grunn for myndighetenes arbeid med digital sikkerhet. https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhetskompetanse/id2627189/
Utredning av felles nasjonale løsninger for tilgang til læringsressurser på tvers av utdanningsinstitusjoner [40]	Utrede felles nasjonal løsning for tilgang til læringsressurser på tvers av utdanningsinstitusjoner slik at det blir mulig å forvalte læringsressurser sentralt for å stimulere til økt produksjon og deling av læringsressurser, samt gjøre åpne digitale læringsressurser for høyere utdanning tilgjengelige. https://www.unit.no/sites/default/files/media/filer/2019/06/LOR-utredning.pdf
Kompetansereformen – Lære hele livet (Meld. St. 14, 2019–2020) [27]	Stortingsmeldingen presenterer tiltak rettet mot å tette gapet mellom hva arbeidslivet trenger av kompetanse, og den kompetansen arbeidstakerne faktisk har. https://www.regjeringen.no/no/dokumenter/meld.-st.-14-20192020/id2698284/
Samfunnssikkerhet i en usikker verden (Meld. St. 5, 2020–2021) [20]	Stortingsmeldingen presenterer regjeringens politikk på samfunnssikkerhetsfeltet de neste fire årene. https://www.regjeringen.no/no/dokumenter/meld.-st.-5-20202021/id2770928/
Nordmenn og digital sikkerhetskultur 2020 [29]	Dette er en årlig rapport hvor befolkningens digitale sikkerhetskultur blir kartlagt over tid. https://norsis.no/wp-content/uploads/2020/10/Nordmenn-og-digital-sikkerhetskultur-2020-web-1.pdf
The EU's Cybersecurity Strategy for the Digital Decade [10]	EU's Cybersikkerhet-strategi sier hvordan EU vil beskytte sine mennesker, virksomheter og institusjoner mot cyber-trusler, og hvordan det vil fremme internasjonalt samarbeid og lede i å sikre et globalt og åpent Internett. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018

C.3 Relevante lover og reguleringer

Lov eller regulering	*URL*
Nasjonale retningslinjer for ingeniørutdanning [38]	https://www.uhr.no/strategiske-enheter/fagstrategiske-enheter/uhr-matematikk-naturvitenskap-og-teknologi/nasjonale-retningslinjer-for-ingeniorutdanningene/
Forskrift om rammeplan for ingeniørutdanning [25]	https://lovdata.no/dokument/SF/forskrift/2018-05-18-870

Lov eller regulering	*URL*
EU data protection rules [7]	https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en
Personopplysningsloven [18]	https://lovdata.no/dokument/NL/lov/2018-06-15-38
Sikkerhetsloven [19]	https://lovdata.no/dokument/NL/lov/2018-06-01-24
Offentleglova [15]	https://lovdata.no/dokument/NL/lov/2006-05-19-16
eForvaltningsforskriften [23]	https://lovdata.no/dokument/SF/forskrift/2004-06-25-988
Ekomloven [22]	https://lovdata.no/dokument/NL/lov/2003-07-04-83
Cybersikkerhets-forordningen [8]	https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2017/nov/cybersecurity-act
Forordning om eID og elektroniske tillitstjenester [5]	https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2012/okt/forordning-om-eid-og-elektroniske-tillitstjenester
NIS-direktivet [6]	https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2014/sep/nis-direktivet
Forslag til NIS2-direktiv [9]	https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2021/feb/nis2-direktivet

C.4 Relevante standarder, anbefalinger og metoder

Standard eller anbefaling	*URL*
Standard Norge	https://www.standard.no/
ISO 27000 (IT-sikkerhet)	https://www.standard.no/fagomrader/ikt/it-sikkerhet/
NS 5814 (risikovurdering)	https://www.standard.no/fagomrader/kvalitet-og-/risikostyring/ns-5814-krav-til-risikovurderinger/
NS-ISO 31000 (risikostyring)	https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=1002500
NS-ISO 31010 (risikostyring)	https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=1111200
NS 5830 (samfunnssikkerhet)	https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=532802
NS 5831 (samfunnssikkerhet)	https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=718201
NS 5832 (samfunnssikkerhet)	https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=718202
FIPS 140-2 (crypto)	https://csrc.nist.gov/publications/detail/fips/140/2/final
NSMs grunnprinsipper	https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/
OWASP	https://owasp.org/
LINDDUN	https://www.linddun.org/
CNIL	https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf

Referanser

[1] Anders Andersen, Tor Berre, Pål Ellingsen, Laurence Habib, Moutaz Haddara, Erik Hjelmås, Mette Mo Jakobsen, Audun Jøsang, Tom Heine Nätt, Jingyue Li, Arne Roar Nygård, Sondre Rønjom, Hans Georg Schaathun, Arild Steen og Tor Fredrik Torgersen, *Informasjonssikkerhet i høyere utdanning*, Nordic Journal of STEM Education 3 (2019), nr. 1, 267–271, ISSN 2535-4574, (MNT-konferansen 2019).

[2] Håkon Bergsjø og Ronny Windvik, *Datasikkerhet for ledere: Hvordan beskytte din virksomhet*, Universitetsforlaget, 2018, ISBN 9788215030005.

[3] Håkon Bergsjø, Ronny Windvik og Lasse Øverlier (red.), *Digital sikkerhet: En innføring*, Universitetsforlaget, 2020, ISBN 9788215034225.

[4] Torgeir Daler, Roar Gulbrandsen, Tore Audun Høie og Torbjørn Sjølstad, *Håndbok i datasikkerhet – informasjonsteknologi og risikostyring*, 4 utg., Fagbokforlaget, 2019, ISBN 978-82-450-2789-1.

[5] EU, *Regulation on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*, Regulation (EU) 910/2014, The European Parliament and of the Council, July 2014.

[6] EU, *Directive concerning measures for a high common level of security of network and information systems across the union*, Directive (EU) 2016/1148, The European Parliament and of the Council, July 2016.

[7] EU, *General data protection regulation (GDPR) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec*, Regulation (EU) 2016/679, The European Parliament and of the Council, April 2016.

[8] EU, *The EU cybersecurity act*, Regulation (EU) 2019/881, The European Parliament and of the Council, April 2019.

[9] EU, *Directive concerning measures for a high common level of security of network and information systems across the union*, Proposal for a Directive (EU) 2020/0359, The European Parliament and of the Council, December 2020.

[10] EU, *The EU's cybersecurity strategy for the digital decade*, Joint Communication to the European Parliament and the Council JOIN (2020) 18 final, European Commission, High Representative of the EU for Foreign Affairs and Security Policy, December 2020.

[11] Hans Christian Holte, Terje Wold, Håkon Grimstad, Lillian Røstad, Torgeir A. Waterhouse, Marie Moe, Lee A. Bygrave og Therese Steen, *IKT-sikkerhet i alle ledd: Organisering og regulering av nasjonal IKT-sikkerhet*, Norges offentlige utredninger NOU 2018: 14, Departementenes sikkerhets- og serviceorganisasjon, Teknisk redaksjon, 2018, ISBN 978-82-583-1373-8.

[12] Ben Johnsen, *Kryptografi: Den hemmelige skriften*, Tapir, 2001, ISBN 82-519-1683-6.

[13] Joint Task Force on Cybersecurity Education, *Cybersecurity curricula 2017: Curriculum guidelines for post-secondary degree programs in cybersecurity*, A Report in the Computing Curricula Series Version 1.0 Report, Association for Computing Machinery (ACM) / IEEE Computer Society (IEEE-CS) / Association for Information Systems Special Interest Group on Information Security and Privacy (AIS-SIGSEC) / International Federation for Information Processing Technical Committee on Information Security Education (IFIP-WG-11.8), December 2017, ISBN 978-1-4503-5278-9.

[14] Audun Jøsang, *Informasjonssikkerhet: Teori og praksis*, Universitetsforlaget, 2021, ISBN 9788215055909.

[15] Justis og beredskapsdepartementet, *Lov om rett til innsyn i dokument i offentleg verksemd (offentleglova)*, Lov 19. mai 2006 nr. 16, Det Kongelige Justis og Beredskapsdepartement, Mai 2006.

[16] Justis og beredskapsdepartementet, *Risiko i et trygt samfunn – Samfunnssikkerhet*, Melding til Stortinget 10 (2016–2017), Det Kongelige Justis og Beredskapsdepartement, Desember 2016.

[17] Justis og beredskapsdepartementet, *IKT-sikkerhet – Et felles ansvar*, Melding til Stortinget 38 (2016–2017), Det Kongelige Justis og Beredskapsdepartement, Juni 2017.

[18] Justis og beredskapsdepartementet, *Lov om behandling av personopplysninger (personopplysningsloven)*, Lov 15. juni 2018 nr. 38, Det Kongelige Justis og Beredskapsdepartement, Juni 2018.

[19] Justis og beredskapsdepartementet, *Lov om nasjonal sikkerhet (sikkerhetsloven)*, Lov 1. juni 2018 nr. 24, Det Kongelige Justis og Beredskapsdepartement, Juni 2018.

[20] Justis og beredskapsdepartementet, *Samfunnssikkerhet i en usikker verden*, Melding til Stortinget 5 (2020–2021), Det Kongelige Justis og Beredskapsdepartement, Oktober 2020.

[21] Justis og beredskapsdepartementet og Kunnskapsdepartementet, *Nasjonal strategi for digital sikkerhetskompetanse*, Strategi, Det Kongelige Justis og Beredskapsdepartement / Det Kongelige Kunnskapsdepartement, Januar 2019.

[22] Kommunal- og moderniseringsdepartementet, *Lov om elektronisk kommunikasjon (ekomloven)*, Lov 4. juli 2003 nr. 83, Det Kongelige Kommunal- og Moderniseringsdepartement, Juli 2003.

[23] Kommunal- og moderniseringsdepartementet, *Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)*, Forskrift 25. juni 2004 nr. 988, Det Kongelige Kommunal- og Moderniseringsdepartement, Juni 2004.

[24] Kommunal- og moderniseringsdepartementet, *Digital agenda for Norge – IKT for en enklere hverdag og økt produktivitet*, Melding til Stortinget 27 (2015–2016), Det Kongelige Kommunal- og Moderniseringsdepartement, April 2016.

[25] Kunnskapsdepartementet, *Forskrift om rammeplan for ingeniørutdanning*, Forskrift 18. mai 2018 nr. 870, Det Kongelige Kunnskapsdepartement, Mai 2018.

[26] Kunnskapsdepartementet, *Langtidsplan for forskning og høyere utdanning 2019–2028*, Melding til Stortinget 4 (2018–2019), Det Kongelige Kunnskapsdepartement, Oktober 2018.

[27] Kunnskapsdepartementet, *Kompetansereformen – Lære hele livet*, Melding til Stortinget 14 (2019–2020), Det Kongelige Kunnskapsdepartement, April 2020.

[28] Olav Lysne, Kristine Beitland, Janne Hagen Kristian, Åke Holmgren, Einar Lunde, Gjøsteen, Fredrik Manne, Eva Jarbekk og Sofie Nystrøm, *Digital sårbarhet – sikkert samfunn: Beskytte enkeltmennesker og samfunn i en digitalisert verden*, Norges offentlige utredninger NOU 2015: 13, Departementenes sikkerhets- og serviceorganisasjon, Informasjonsforvaltning, 2015, ISBN 978-82-583-1249-6.

[29] Bjarte Malmedal, *Nordmenn og digital sikkerhetskultur 2020*, Norwegian Centre for Information Security (NorSIS), 2020.

[30] Bjarte Malmedal and Hanne Eggen Røislien, *The norwegian cyber security culture*, Norwegian Centre for Information Security (NorSIS), 2016.

[31] Nasjonal sikkerhetsmyndighet (NSM), *NSMs grunprinsipper for IKT-sikkerhet*, April 2020, Versjon 2.0.

[32] Tom Heine Nätt og Christian F. Heide, *Datasikkerhet: Ikke bli svindlerens neste offer*, 2 utg., Gyldendal Akademisk, 2021, ISBN 978-82-05-53906-8.

[33] Allen Parrish, John Impagliazzo, Rajendra K. Raj, Henrique Santos, Muhammad Rizwan Asghar, Audun Jøsang, Teresa Pereira, Vítor J. Sá, and Eliana Stavrou, *Global perspectives on cybersecurity education*, Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE 2018), ACM, July 2018, pp. 340–341, ISBN 978-1-4503-5707-4.

[34] J.H. Saltzer and M.D. Schroeder, *The protection of information in computer systems*, Proceedings of the IEEE 63 (1975), no. 9, 1278–1308.

[35] Hans Georg Schaathun, *Ingeniørdannelse. Kva har danning i teknologifag å gjera?*, Norsk IKT-konferanse for forskning og utdanning 4 (202), NIKT-2020 UDIT Norsk konferanse for utdanning og didaktikk i IT-fagene.

[36] Richard E. Smith, *A contemporary look at Saltzer and Schroeder's 1975 design principles*, IEEE Security & Privacy 10 (2012), no. 6, 20–25.

[37] Stortinget, *Referat fra debatt sak nr. 2, Innstilling fra justiskomiteen om IKT-sikkerhet – Et felles ansvar*, Stortingstiende Sesjonen 2017–2018 (2018), nr. 63, 10. april, 3116–3124.

[38] UHR-Matematikk, naturvitenskap og teknologi (UHR-MNT), *Nasjonale retningslinjer for ingeniørutdanning*, Universitets- og høgskolerådet (UHR), 2020.

[39] UHR, Nasjonalt råd for teknologisk utdanning (NRT), *Nasjonale retningslinjer for ingeniørutdanning: På vei mot fremtiden!*, Universitets- og høgskolerådet (UHR), 2011.

[40] Unit – Direktoratet for IKT og fellestjenester i høyere utdanning og forskning, *Utredning av felles nasjonale løsninger for tilgang til læringsressurser på tvers av utdanningsinstitusjoner*, 2019.