IKT-sikkerhet i utdanningene

Læringsmål IKT-sikkerhet

22. november 2020

Nasjonal arbeidsgruppe IKT-sikkerhet i utdanningene[†]

[†] Medlemmene av arbeidsgruppen: *Anders Andersen (UiT-Tromsø), Tor Berre (NTNU), Pål Ellingsen (HVL), Olaf Hallan Graven (USN), Laurence Habib (OsloMet), Moutaz Haddara (HK), Erik Hjelmås (NTNU-Gjøvik), Mette Mo Jakobsen (UHR), Audun Jøsang (UIO), Lars Emil Knudsen (HIOF), Jingyue Li (NTNU-Trondheim), Arne Roar Nygård (Eidsiva Nett AS), Tom Heine Nätt (HIOF), Sondre Rønjom (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)

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 [1, 2]. 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 [3, 4, 5, 6, 7] 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 [8].

Nasjonal Sikkerhetsmyndighet definerer i «NSMs grunnprinsipper for IKT-sikkerhet»[1] [9] 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 6 tema innen *IKT-sikkerhet* som bør dekkes i alle ingeniørutdanninger, eller i høyere utdanning generelt:

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

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.

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 [10]. En forståelse av konsekvensene av personvern og bruk av personopplysninger i IKT-baserte løsninger bør være inkludert i høyere utdanning.

Nært beslektet med personvern vil behovet for en kompetanse av hvordan *lover*, *reguleringer* og *etikk* påvirker bruk og utvikling av IKT-baserte systemer.

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. Det er nødvendig med en helhetlig forståelse av sikkerhet både under utvikling (programmering) og drift av IT-systemer for å kunne oppnå dette.

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

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. De er gruppert etter de 6 temaene identifisert ovenfor. For hver slik 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 studiet. Et utvalg av disse vil enten definere nye emner i studiet eller de vil inngå i eksisterende emner i studiet. 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 et konkret studium, 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» [11]. Vi gjengir disse i vedlegg A. 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 A.

2.1 Grunnleggende begreper

Kunnskap

LU-K-1-1 Kandidaten kjenner til sentrale eksempler 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 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 og kjenne til en typisk organisering av IKT-sikkerhet i en organisasjon

LU-F-2-2 **Kandidaten kan argumentere for viktigheten av god cyber-hygiene (rutiner og oppførsel), brukeropplæring om 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 og sikkerhet** *(generell kompetanse b)*

2.3 Personvern

Kunnskap

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

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

LU-K-3-3 Kandidaten kjenner til de viktigste 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 et behov for beskyttelse av persondata** *(ferdigheter b)*

LU-F-3-3 Kandidaten kan anvende de viktigste 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

2.4 Lover, reguleringer og etikk

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, og bruken av, 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)*

2.5 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 stadier og farenivåer av IKT-angrep

Ferdigheter

LU-F-5-1 **Kandidaten kan vurdere systemer innen sitt fagområde 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)*

2.6 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 skal kjenne til beste praksis for helthetlig sikkerhet innen sitt fagområde

Referanser

[1] 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), Desember 2017, ISBN 978-1-4503-5278-9.

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

[3] Lysne, Olav, 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.

[4] 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.

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

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

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

[8] Holte, Hans Christian, 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.

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

[10] 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.

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

A Utdrag fra «Nasjonale retningslinjer for ingeniørutdanningene»

Teksten under er et utdrag fra «Nasjonale retningslinjer for ingeniørutdanningene» [11], 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 personvern trer i kraft og typiske tilnærminger for beskyttelse og anonymisering av data (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 om 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 systemer innen sitt fagområde 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 og 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)