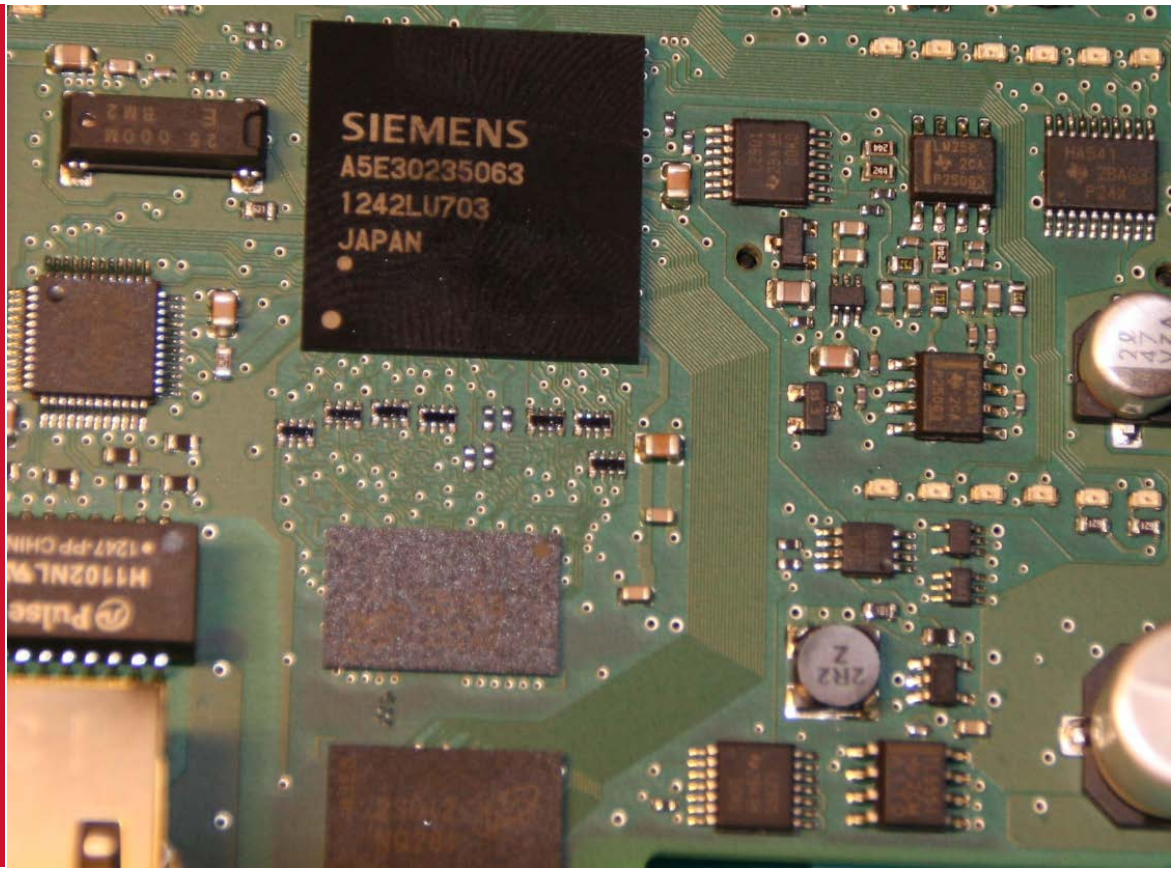
RAPPORT

Nr. 45/2020

Utvikling av cybersikkerhetskompetanse for kraftbransjen

Janne Hagen (red.), Siv-Hilde Houmb, Lars-Erik Smevold, Nils Kalstad, Arne-Roar Nygård



NVE Rapport nr. 45/2020
Utvikling av cybersikkerhetskompetanse for kraftbransjen

Utgitt av:	Norges vassdrags- og energidirektorat
Redaktør:	Janne Hagen
Forfatter:	Janne Hagen, Siv-Hilde Houmb (Statnett), Lars-Erik Smevold (KraftCERT), Nils Kalstad (NTNU), Arne-Roar Nygård (Elvia)
Forsidefotograf:	Lars-Erik Smedvold/KraftCERT
ISBN:	978-82-410-2093-3
ISSN:	1501-2832

Sammendrag: Rapporten dokumenterer resultatet av et forprosjekt initiert av NVE som hadde som mål å utvikle et forskningsprosjekt for sikkerhet i industrielle kontrollsystemer (driftskontroll) og maskinvare i kraftbransjen. I løpet av prosjektet er det blitt rekruttert to Ph.d.-kandidater fra kraftbransjen samt skaffet finansering fra Nærings-Ph.d.-ordningen i Forskningsrådet. Rapporten anbefaler en videreføring av prosjektet og at det arbeides videre med en bredere forankring i bransjen.

Emneord: Driftskontrollsystemer, IKT-sikkerhet, maskinvare

Norges vassdrags- og energidirektorat
Middelthuns gate 29
Postboks 5091 Majorstuen
0301 Oslo

Telefon: 22 95 95 95
E-post: nve@nve.no
Internett: www.nve.no

desember, 2020

Norges vassdrags- og energidirektorat
2020

Innhold

Norges vassdrags- og energidirektorat
Middelthunsgate 29
Postboks 5091 Majorstua
0301 OSLO

Telefon: 22 95 95 95
Telefaks: 22 95 90 00
Internett: www.nve.no

Forord

Kraftforsyningen digitaliseres, og digital teknologi blir stadig viktigere for å drifte en kompleks kraftforsyning og sørge for fortsatt god forsyningssikkerhet av elektrisitet og fjernvarme. Digital sårbarhet treffer også driftskontrollsystemer i kraftforsyningen. Dette er kritiske systemer som har særskilt behov for beskyttelse. De er derfor også underlagt særskilte sikkerhetskrav i kraftberedskapsforskriften.

Mange har påpekt at Norge har en kompetanseutfordring; vi trenger flere cybersikkerhetseksperter. I kraftbransjen er det behov for eksperter som har tverrfaglig kompetanse innen elkraftteknologi, digital teknologi og cybersikkerhet. Et annet aspekt som ikke er like fremtredende i den offentlige debatten er behovet for kompetanse på maskinvaresikkerhet. I bunnen av digitale løsninger ligger maskinvare, elektronikken. Vi mangler forskning og utdanning på området maskinvaresikkerhet, til tross for at sikkerhet i maskinvare er viktig for å oppnå god sikkerhet i en digitalisert kraftinfrastruktur.

NVE har derfor tatt initiativ til å bygge ny kompetanse på cybersikkerhet, med spesiell vekt på sikkerhet i industrielle kontrollsystemer (i kraftbransjen omtalt som driftskontrollsystemer) og maskinvare. Sikkerhetsutfordringene er tydelige i kraftbransjen: Kombinasjonen av utdatert og ny teknologi utfordrer eksisterende sikkerhetsregimer. Avhengigheten av leverandørene er stor, og oversikten i leverandørkjeden stopper ved første ledd. Det krever mye av virksomhetene i bransjen å ha kontroll på alle innsatsfaktorene samtidig som trusselbildet er i endring.

I løpet av 2020 har vi arbeidet i et forprosjekt for å få både finansiering på plass og for å rekruttere to kandidater fra bransjen som skal bygge kompetanse på dette området for kraftsektoren. Arbeidet har båret frukt, og i skrivende stund har Statnett og Elvia rekruttert hver sin Ph.d.-kandidat som skal gjennomføre doktorgradsstudier ved NTNU. De to kandidatene skal etter planen gjennomføre et opphold i USA ved University of Tulsa for å tilegne seg kunnskap om maskinvaresikkerhet som vi i dag ikke har i Norge.

Statnett og Elvia har fått økonomisk støtte fra Forskningsrådet gjennom Nærings-Ph.d.-ordningen og virksomhetene bidrar selv med betydelig egenfinansiering. NVE har vært en pådriver for dette tiltaket og mener det er viktig at det blir utviklet ny kompetanse sikkerhet i industrielle kontrollsystemer (driftskontrollsystemer) og maskinvaresikkerhet.

Ingunn Åsgard Bendiksen
Direktør

Elvia Holo
Seksjonsleder

Sammendrag

Det pågår en digitaliseringsprosess i kraftbransjen som også berører driftskontrollsystemer i kraftsystemet. I det framtidige kraftsystemet blir digital teknologi stadig viktigere for drift og stabilitet i kraftsystemet. Men, økt digitalisering endrer også risikobildet. Uavhengig av denne utviklingen observerer vi en endring i cybertrusler der internasjonal kriminalitet, spionasje, utpressing og sabotasje er ingredienser. For å håndtere endret risiko må kraftbransjen ha flere eksperter med praktisk og teoretisk cybersikkerhetskompetanse. Det er spesielt behov for kompetanse på helhetlig sikkerhet i industrielle kontrollsystemer inkludert maskinvare.

Helhetlig sikkerhet, som dekker alle nivåer og som også går i dybden på maskinvare, er en forutsetning for en vellykket digitalisering. Dessverre er kompetanse på særlig maskinvaresikkerhet en mangelvare i Norge. Dette er påpekt i en NVE-rapport fra 2018 som satte søkelyset på sikkerhet i leverandørkjeden. NVE tok derfor initiativ til et FOU-prosjekt som skal bygge en ny FOU-kapasitet på cybersikkerhet og maskinvaresikkerhet i samarbeid med NTNU og Universitetet i Tulsa, USA.

I løpet av prosjektets fase 1 er Statnett og Elvia blitt med i prosjektet med hver sin Ph.d-kandidat. Disse har fått støtte fra Forskningsrådet innenfor Nærings-Ph.d.-ordningen. I tillegg har prosjektet vært i kontakt med aktuelle samarbeidspartnere hos myndigheter og i bransjen. Parallelt med dette initiativet har NVE støttet NTNU med midler til å bygge en cyberfysisk lab ved NTNU der en kan sikkerhetsteste og forske på også maskinvaresikkerhet i komponenter og utstyr som benyttes i kraftforsyningen. Inspirasjon til laboratorium og kompetansebygging er hentet fra Universitetet i Tulsa og deres CyberCorps program.

Gjennom fase 1 i prosjektet er det blitt åpenbart at det bør satses målrettet over lengre tid, vi snakker år, til å bygge opp en norsk forsknings- og utdanningskapasitet på sikkerhet i teknologi som benyttes i kraftbransjen, særlig industrielle kontrollsystemer og maskinvare. I Tulsa har arbeidet pågått over mange år og under flere presidenter. Også i Norge trengs det tilsvarende langsiktig satsing.

Målet er å bygge et forskningslaboratorium og -miljø for cybersikkerhet, spesielt sikkerhet i industrielle kontrollsystemer og maskinvare der kraftbransjen kan få sikkerhetstestet komponenter og utstyr, og der ansatte kan håndtere også kraftsensitiv informasjon og sikkerhetsgradert informasjon. Dette følges av andre mål; å etablere attraktive karrieremuligheter i krysningspunktet elkraft, elektronikk og cybersikkerhet. Vi ønsker å legge til rette for å utdanne flere sikkerhetseksperter som kan arbeide i kraftbransjen, i virksomheter innen kritisk infrastruktur og hos myndigheter som krever sikkerhetsklarering.

Det arbeides med en intensjonsavtale mellom samarbeidspartnere fra bransjen, interesseorganisasjoner og myndigheter. Det er når vi løfter i flokk at vi kan nå krevende mål. Gitt at kraftbransjen skal lykkes med digitaliseringen og at forsyningssikkerheten på strøm skal fortsatt være høy, må vi investere i kompetanse og laboratoriums kapasitet. «Praktisk håndverk» må også være med skal cybersikkerhetskompetansen bli komplett.

1 Behov for kompetanse

1.1 Bakgrunn

Kraftbransjen står midt opp i en digitaliseringsbølge som følge av økt innføring av ikke regulerbar kraftproduksjon (sol- og vindkraft) og økende forbruk pga. økende elektrifisering. Vellykket digitalisering avhenger av at digital sikkerhet ivaretas. God digital sikkerhet oppnås ved en kombinasjon av programvare, maskinvare og struktur/helhetsplan herunder blant annet sikkerhetskultur. Disse elementene henger sammen og er gjensidig avhengig av hverandre ved at en god løsning på kun ett område ikke nødvendigvis gir god sikkerhet i seg selv.

Vi vet i dag at digitale sårbarheter oppdages først etter en tids bruk, og at sikkerhet i mange tilfeller er lite prioritert. Konsekvensene av datakriminalitet og digital sabotasje er stor, og cyberangrep rammer mange. Etter 2010 har trusler blitt rettet mot industrielle kontrollsystemer. I 2020, når verden står i en annen krise, Covid 19 pandemien, peker Europol i sin rapport på at kriminelle utnytter pandemien og den medfølgende sårbarheten i samfunnet (Europol, 2020). Svindel med utgangspunkt i pandemien har økt. Phishing angrep er fortsatt mest vanlig angrepsmåte nå også med svindel på SMS og simkortovertakelse, nektelsesangrep, kryptoskadevare, utpressing og trusler. Også energibransjen er utsatt for digital kriminalitet. Med referanse til norske sikkerhetsmyndighetenes trussel- og risikorapporter (PST, 2020) (NSM, 2020) er det så langt lite som tyder på at kriminaliteten på internett er på retur, eller at kraftbransjen blir mindre eksponert for cybertrusler og fremmed etterretning i tiden framover.

Sikkerhetskunnskap trengs i anskaffelser, i innovasjonsprosjekter og i digitaliseringsprosjekter. Når digital teknologi og elektronikk tas i bruk, trenger virksomhetene i kraftbransjen tilgang til kunnskap og laboratorie-kapasitet som kan undersøke sikkerheten fra maskinvare og opp til applikasjonsnivå, videre til systemnivå inklusive sikkerhet i datanettverk og sammenkoplede systemer og tjenester. Dessverre dekker ikke norske universiteter alle «sikkerhetsnivåene» i sin utdanning i informasjonssikkerhet eller cybersikkerhet. Dette er ikke bare et norsk fenomen. Hovedfokus er på programvare, nettverk, drift, styringssystem, sikkerhetsledelse og sikkerhetsarkitektur. Det er lite tilbud på utdanning i sikkerhet i maskinvare både i Norge og i andre land. Opplæring i maskinvaresikkerhet tilbys mest i industrien som produserer denne type teknologi, og i forsvarssektoren.

I dag er virksomhetene i stor grad derfor tvunget til å stole på leverandører – det er ikke mulighet til å verifisere sikkerheten, annet enn deler av den. Verifikasjon av digital sikkerhet er komplisert, som Lysne har beskrevet (Lysne, 2018). Selv om man får muligheter til å for eksempel verifisere kildekode, kan likevel kompilatoren være kompromittert, og dermed også den maskinlesbare koden. Maskinvare kan videre være modifisert i transport fra produsent til leverandør og inneholde for eksempel en bakdør, eller være en piratkopi med innebygde feil. At virksomheter i kraftbransjen ikke har innsyn og mulighet til å kontrollere sikkerheten i leverandørkjeden, særlig maskinvaresikkerheten, ble også påpekt i en NVE-rapport fra 2018 (Kirkebø & Ljøsne, 2018).

Kraftbransjen i Norge deltar aktivt inn i NTNUs Center for Cyber Security hvor industripartnere samarbeider for å avdekke ny kompetanse og delta i spissede FoU prosjekter, men bransjen ser at dette ikke dekker alle behov og at man dermed trenger både cybersikkerhetseksperter og et sikkerhetslaboratorium for reverse engineering av maskinvare og programvare, systemsikkerhet. Behovet gjelder både teknologi som benyttes i kraftbransjen i dag og teknologi som vil kunne bli utviklet og tatt i bruk i framtiden.

NVE har derfor tatt initiativ til å bygge opp en nasjonal kapasitet i samarbeid med kraftbransjen og andre myndigheter på cybersikkerhet, spesielt sikkerhet i industrielle kontrollsystemer og maskinvare. Denne rapporten skisserer veien fra idé til konsept og et gjennomførbart prosjekt.

1.2 Hva er maskinvaresikkerhet og hva er truslene mot maskinvare?

Maskinvare (elektronikk) er grunnstammen i all digital teknologi og grunnstamme også i industrielle kontrollsystemer. Derfor er tillit til maskinvaren og sikkerhet i maskinvare viktig. Ved Kungliga Tekniska Högskolan i Sverige har (Dubrova, 2014) gitt en presentasjon av temaet hardware reverse engineering, og hennes budskap er at vi ikke kan stole på at maskinvaren er sikker. Sikring av maskinvare følger samme syklus som annet sikkerhetsarbeid: beskytte, oppdage, respondere og sikre bevis. For å sikre maskinvaren benyttes teknikker som fysisk sikring, innbruddsikring, innkapsling, overdekning, elektriske sikringer, villedning av arkitekturen mm. Truslene mot maskinvaresikkerhet er for eksempel manipulasjon av maskinvare, innebygde bakdører, overspenninger mv.

Det er få forskningsartikler som forklarer metoder og verktøy for å avdekke for eksempel motstandsdyktig design mot manipulasjon og det gjør forfatterne av denne artikkelen. I forskningen har de brukt lett tilgjengelige og relativt billige komponenter som kan demonteres og splittes opp for å forstå hvordan de kommuniserer med hverandre og hvordan data flyter (T. Gordon, , Kilgore, Wylds , & Nowatkowsk, 2019).

1.3 Målsetting

Dette prosjektet har som målsetting å utvikle et nytt forsknings- og utdanningstilbud i Norge for kraftbransjen. Dette innebærer å rekruttere og finansiere to Ph.d-kandidater for at disse skal gjennomføre utdanning i cybersikkerhet ved universitetet i Tulsa i USA og bringe tilbake cybersikkerhetskompetanse som vi per i dag ikke har i Norge. Et viktig tema er maskinvaresikkerhet og reverse engineering av maskinvare.

Prosjektets målsetting er å bidra til å bygge en utdanningskapasitet som er nyttig og attraktiv for sikkerhetsarbeidet i kraftbransjen. Målet er å utdanne professorkandidater og universitetslærere med både praktisk og teoretisk kompetanse som i neste omgang vil videreføre et forskningssamarbeid mellom kraftbransjen og akademia og utdanne flere norske eksperter med praktisk kompetanse på cybersikkerhet og maskinvaresikkerhet. Siden maskinvare bærer den grunnleggende tilliten i ethvert digitalt system, vil

sikkerhetsbrudd og feil i maskinvare kunne representere en vesentlig trussel mot tilliten til digitale systemer. Dette gjelder også systemer og teknologi som i dag benyttes i kraftbransjen.

Målet er at de første PhD-kandidatene etter endt utdanning vil arbeide ved egen virksomhet og ved NTNU, og være bærebjelken i oppbygningen av et norsk fagmiljø og en lab innenfor hardware og software reverse engineering og cybersikkerhet for kraftbransjen. De vil bidra til at kraftbransjen og annen norsk kritisk infrastruktur, samt myndigheter får mulighet til å undersøke sikkerheten i produkter som i dag tas i bruk uten at vi kjenner de grunnleggende sårbarhetene i maskinvaren. Målet er at de utvalgte kandidatene blir en faglig spydspiss i reverse engineering og cybersikkerhet. På sikt vil vi kunne selv utdanne eksperter til kraftbransjen og til andre sektorer innenfor denne fagdisiplinen.

1.4 Rapportens oppbygging

Rapporten er bygget opp på følgende måte:

Kapittel 1 gir en introduksjon til bakgrunnen til prosjektet og rapportens formål.

Kapittel 2 beskriver kort prosessen fra prosjektidé til prosjektet.

Kapittel 3 omtaler prosessen med utforming av Ph.d.-prosjektbeskrivelser og søknader om finansiering fra Forskningsrådet og opptak ved NTNU.

Kapittel 4 drøfter behovet for forskningslaboratorium og utfordringer som må løses i den anledning.

Kapittel 5 omtaler internasjonalt samarbeid som er en premiss for å lykkes.

Kapittel 6 presenterer en organisatorisk løsning rundt Ph.d-kandidatene.

Kapittel 7 skisserer forslag til videre arbeid.

2 Fra idé til prosjekt

2.1 Fra idé til konsept

NVE har siden 2016 hatt et samarbeid med sikkerhetsmiljøet ved Universitetet i Tulsa og sikkerhetsmiljøet rundt professor Sujeet Shenoi. Shenoi har deltatt i flere workshops i Norge for kraftbransjen, og det har i årenes løp blitt avdekket et kompetansebehov i Norge som per i dag ikke er dekket gjennom eksisterende sikkerhetsutdanning hos norske universiteter.

Universitetet i Tulsa utdanner sikkerhetseksperter med «hands-on» kompetanse på reverse engineering og cybersikkerhet. Studentene i Tulsa får en bred og grundig utdanning i sikkerhet som dekker mange fagdisipliner -herunder elektronikk, programvare, nettverk, fysisk sikring mm. I utdanningen inngår også opplæring i reverse engineering av maskinvare for å finne sårbarheter. Slik kompetanse er nyttig for å kunne avdekke ikke kjente sårbarheter i maskinvare. Fagmiljøet ved Tulsa er USAs beste og utdanner sikkerhetseksperter til amerikanske myndigheter og til kritisk infrastruktur i USA. Norge og kraftbransjen har fått et tilbud om å sende 2-3 norske statsborgere med sikkerhetsklarering til USA og Tulsa for å ta kurs og en PhD. Det kan bemerkes at de første norske oljeingeniørene også fikk sin utdanning i Tulsa. Nå er ringen sluttet, men med cybersikkerhet som nytt tema.

NVE har derfor satt i gang et forprosjekt for å komme i gang med PhD-utdanning og oppbyggingen av forsknings- og utdanningstilbudet innenfor cybersikkerhet, sikkerhet i industrielle kontrollsystemer og maskinvare for den norske kraftbransjen ved NTNU.

2.2 Identifisering av samarbeidspartnere og interessenter

Prosjektet har identifisert flere mulige samarbeidspartnere:

- Akademia, NTNU i første omgang siden NTNU har lang tradisjon med elkraftingeniørutdanning.
- Selskap i kraftbransjen, så langt gjelder dette Statnett,Elvia og KraftCERT
- Andre myndigheter, NSM, politiet, andre sektormyndigheter
- Bransjeorganisasjoner, så langt EnergiNorge

Samarbeidet vil bli formalisert i en intensjonsavtale. Det pågår arbeid med å utforme innholdet i denne.

2.3 Kommunikasjon og informasjonsdeling

Prosjektet startet opp i januar 2020. Prosjektideen ble først drøftet med aktuelle interessenter i bransjen og med Norges Forskningsråd. Så kom Covid 19 pandemien, og samarbeidsplattformen ble utelukkende digital.

Da Norges Forskningsråd lyste ut midler til 18 doktorgradsprosjekter i IKT-sikkerhet og kryptologi for kandidater med sikkerhetsklarering, annonserte NVE på forsommeren på sin nettside dette som en etterutdanningsmulighet for bransjen. NVE oppfordret bransjen til å søke midler. Prosjektet ble presentert på møter med aktuelle samarbeidspartnere og på NVEs cybersikkerhetsworkshop i juni 2020. Sommeren 2020 hadde Elvia og Statnett meldt sin interesse. Begge selskapene hadde skaffet kandidater høsten 2020, og begge sendte søknader til Norges forskningsråd i løpet av høsten 2020.

Samtidig arbeidet prosjektet med å identifisere aktuelle fagressurser på fagområdet. I løpet av dette arbeidet fant prosjektet to tidligere ansatte i tidligere Conax. Disse hadde

kjennskap til fagfeltet reverse engineering av maskinvare med sin bakgrunn fra filmindustrien. Prosjektet gjennomførte noen møter med disse ressurspersonene som en støtte til å utforme forskningsprosjekter. Prosjektet hadde også dialog med fagmiljøet ved universitetet i Tulsa og ved NTNU.

2.4 Prosjektrisiko

Når en skal bygge ny kompetanse på et fagfelt, er det mange forhold som kan representere en risiko:

Mangel på kandidater og finansiering er den mest åpenbare. Med to NæringsPhD-kandidater hos to store selskap i kraftbransjen, er denne risikoen sterkt redusert. I skrivende stund har den ene fått positivt svar fra Forskningsrådet.

Muligheten for opphold i Tulsa/USA er en annen forutsetning. Her har pandemien satt begrensninger, men en praktisk løsning er å utsette reisen og starte opp studiet i Norge, og fortsette med forskningsoppholdet senere i USA.

Nøkkelpersoner kan bli syke slik at opplegget ikke kan gjennomføres som planlagt.

NVE har støttet NTNU med midler til å bygge en cyberfysisk lab som skal understøtte studentene og kunnskapsbyggingen. KraftCERT og NSM har donert utstyr til denne laben. Det er viktig at denne laben blir utformet slik at den understøtter prosjektet om å bygge ny kunnskap. Forskning utført ved laben kan være av sensitiv art, både i forhold til forretningshemmeligheter og kraftsensitiv informasjon. Kraftberedskapsforskriften stiller krav til beskyttelse av kraftsensitiv informasjon. I tillegg pågår det et arbeid der en vurderer om en større del av kraftbransjen skal underlegges sikkerhetsloven. I så fall er det også snakk om gradert informasjon etter sikkerhetsloven. NVE og Statnett har derfor vært i dialog med NTNU for å kommunisere behovet for sikring av laben.

PST omtaler trusler mot forskning i sin trusselrapport for 2020, se underkapittel 4.2.

3 PhD rekruttering og søknad til forskningsrådet

3.1 NæringsPhD-ordningen

Forskningsrådet gir informasjon om om Nærings-Ph.d. ordningen på sine nettsider (Norges forskningsråd, 2020). I et nærings-ph.d.-prosjekt går en virksomhet og et universitet eller høyskole sammen om et doktorgradsprosjekt. Doktorgradsprosjektet utføres av en ansatt (PhD-kandidat) i virksomheten og skal være relevant for bedriften. Dersom dette gjelder en offentlig virksomhet, heter ordningen Offentlig-Ph.d, men er ellers lik.

En Nærings-ph.d. resulterer i konkrete forsknings- og utviklingsresultater som styrker virnksomhetens kjernevirksomhet, produkter og/eller tjenester. PhD-kandidaten får en spesialistutdanning og forskerutdanning, og kandidatene arbeider like gjerne i virksomheter som i akademia etter utdanningen.

Samarbeidet med universitet eller høyskolen sikrer økt forskningskompetanse og -kunnskap for både kandidaten og bedriften som helhet.

Gjennom Nærings-ph.d.-ordningen mottar virksomheten økonomisk støtte til å styrke sin kjernevirksomhet, tjenester og produkter. Dette gir også mulighet til å bygge kompetanse i virksomheten innenfor egne rammer og behov. Nærings-ph.d. er også en fin mulighet til å starte eller opprettholde verdifulle samarbeid med akademia, og gir tilgang til forskningsorganisasjonenes kunnskap, kompetanse og infrastruktur.

Kandidaten får en doktorgrad og en forskerutdanning styrket av innsikt i næringslivets sentrale utfordringer, og forskerkompetansen til å løse disse. Gjennom prosjektet har kandidaten tilgang til uvurderlig næringslivskompetanse i egen bedrift og forskningsinstitusjonens ekspertise.

Bedrifter som får støtte til nærings-ph.d. vil i tillegg kunne søke utenlandsstipend for sin doktorgradskandidat dersom gradsgivende institusjon er norsk[1]. Forskningsrådet har en egen utlysning av utenlandsstipend[2]. På epost til NVE har Forskningsrådet opplyst at i forbindelse med behandling av utenlandsopphold er det mulig å søke om å få dekket dokumenterte utgifter til studieavgift. Beløpet må framgå i invitasjonsbrevet fra vertsinstitusjonen. Forskningsrådet har ikke definert en øvre grense. I epost til NVE sier Forskningsrådet at dette ikke må forstås som en garanti - erfaringsmessig utgjør skolepengene mellom 500 og 1500 Euro.

Forskningsrådet dekker kun "administrasjonskostnader" som vertsinstitusjonen krever. Forsikringer dekker Forskningsrådet ikke. Det må dekkes fra en eventuell bevilgning Forskningsrådet tildeler til utenlandsopphold.

Det er virksomheten som sender inn søknaden til Forskningsrådet. Intern forankring av prosjektet i virksomheten er derfor viktig. Det finnes egne skjema for slike søknader på Forskningsrådet sine nettsider.

I 2020 lyste Forskningsrådet ut 18 stipend innenfor området IKT-sikkerhet og krypto til søkere som kunne sikkerhetsklareres (Norges forskningsråd, 2020).

3.2 Nærings-PhD søknad om opptak hos universitet

I tillegg til å søke om finansiering fra Forskningsrådets nærings-Ph.d. ordning, må Ph-d.-kandidatene søke opptak hos universitet som skal utgi graden. Her kan det være ulik praksis hos ulike universiteter.

En må skaffe seg en veileder som er ansatt på universitetet eller høyskolen. Det er mulig å ha flere veiledere, også fra andre universiteter og høyskoler. I dette prosjektet blir NTNU

[1] https://www.forskningsradet.no/utlysninger/2019/narings-ph.d.--doktorgradsprosjekt-i-bedrift/
[2] https://www.forskningsradet.no/utlysninger/2019/utenlandsstipend-for-doktorgrads--og-postdoktorstipendiater/

gradsgivende institusjon. NTNU vil da være den institusjonen som godkjenner kursporteføl gen fra universitetet i Tulsa. Normalt må en nærings-Ph.d. ta en kurspakke på phd.-nivå som tilsvarer 30 studiepoeng, dvs. et halvt år på fulltid. Kandidaten utarbeider typisk en slik kursplan sammen med sin veileder. I tillegg må han/hun lage en forskningsplan for prosjektet. Kravene til Ph.d. kurspakke er regulerte, slik at man må igjennom noen obligatoriske kurs og så kan man velge andre kurs i tillegg. I dette prosjektet er planen å ta flere kurs enn normalt, for å kunne hente hjem kompetanse til Norge fra USA.

Dersom samarbeidende universitet er interessert, kan NTNU også inngå avtale med andre universiteter om dobbel grad (Cotutelle Agreement).

Universitetene har egne prosedyrer for opptak av Ph.d. studenter.

I dette prosjektet har det vært usikkerhet om hva man skal gjøre først: Søke Forskningsrådet eller søke opptak. Usikkerheten har bunnet i at begge parter henviser til hverandre. I dette prosjektet har det fungert å søke Forskningsrådet først, og deretter NTNU.

3.3 Prosjektrisiko for den enkelte kandidat

Det er også en rekke risikofaktorer for den enkelte ph.d. kandidat. Ph.d. kandidaten bør vurdere risiko for følgende forhold:

- Manglende kompetanse som må tas ved siden av gjennom tilleggskurs eller egne studier. Dette kan øke arbeidsbyrden.
- Egen utholdenhet – et ph.d. løp kan være ensomt og krevende, framdriften kan midlertidig stoppe opp, og det er viktig med gode støttespillere i virksomheten, på universitetet og i familien.
- Det er alltid en risiko at veiledningen ikke er optimal. Prosjektets innretning kan endres underveis som følge av forskningsresultater, eller sykdom kan forhindre veiledning. Det er mulig å søke om andre veiledere hvis det er behov for endring.
- Mangel på data. For en nærings-ph.d. vil datatilgangen kunne være bedre når en skriver for egen virksomhet.
- Familiesituasjonen kan bli endret og utfordre planer om utenlandsopphold.
- Sykdom eller andre forhold kan forhindre at man klarer å fullføre på normert tid. I disse dager er pandemien en utfordrer når det gjelder utenlandsopphold.

3.4 Status – to Ph.d-prosjekter

Elvia og Statnett har sendt inn søknader om støtte innenfor Nærings-Ph.d. ordningen til Forskningsrådet. Den ene søknaden legger opp til et teknologisk dypdykk i HW reverse engineering teknikker og den andre tar sikte på å sammenligne og vurdere metoder og

verktøy for sikkerhetsverifikasjon. Studentene arbeider med søknad om opptak til NTNU og Universitetet i Tulsa. Planlagt oppstart er Januar 2021.

4 Laboratorium

4.1 Cyberfysisk laboratorium hos NTNU

NVE har gjennom NVEs FOU-prosjekt *P-80401 Tverrfaglig lab for cyberfysisk sikkerhet hos NTNU* støttet NTNU økonomisk slik at NTNU kan etablere en prototype på en cyberfysisk lab, som blir en del av den nye kapasiteten på reverse engineering og cybersikkerhet. Med de ambisjoner som er lagt, er det nødvendig å videreutvikle en felles laboratorieinfrastruktur og -kapasitet – som et samarbeid mellom KraftCERT, NSM og NTNU (som en mulig del av Norwegian Cyber Range) – et Hardware Reverse Engineering laboratorium.

Det er nødvendig med utvikling og samling av laboratoriefasiliteter for å kunne drive utvikling og teste metodikk (mye kan ikke gjøres på systemer i drift), skape forståelse for og teste scenarier i samarbeid med relevante aktører og samarbeidspartnere. Arbeidet vil være grunnlag for og ledd i kompetansebygging og tidlig rekruttering av fagpersoner. Det betyr at en hensiktsmessig laboratorieinfrastruktur og -kapasitet vil være en viktig del av det praktiske grunnlaget i utdanningen innen kraftsektoren.

Det planlegges derfor med utvikling av felles laboratorieinfrastruktur mellom KraftCERT, NSM og NTNU (som en del av Norwegian Cyber Range). Flere aktører må bidra i fellesskap og dele på investeringskostnad, driftskostnad og brukstid. Det vil gjøre det mulig å dele kompetanse og erfaringer på sikt på tvers av sektorer. Rasjonale bak dette er at samme leverandører leverer teknologi til virksomheter i ulike sektorer.

Det er hensiktsmessig at laboratoriet bygges som en del av NTNUs utvikling og etablering av Norwegian Cyber Range. Dette blir en nasjonal fasilitet for øving, trening og etter hvert testing innenfor samfunnskritiske områder. Dette vil utgjøre en god omgivelse også for en spissing inn mot energisektoren.

NTNU har estimert investeringsbehovet for Hardware Reverse Engineering Laboratory til kr 14 mill og med en driftskostnad på kr 2 mill pr år over en etableringsfase på 8 år (2020 kroner). I denne forbindelse kan en se hen til Universitetet i Tulsa som utdanner sikkerhetseksperter til amerikanske myndigheter. Gjennom mange år og under ulike presidenter har professor Sujeet Shenoi arbeidet for å bygge opp et sterkt fagmiljø ved universitetet som nå er USAs beste på området. (University of Tulsa, 2020). Norge kan bygge lignende fagmiljø dersom vi får til å bygge kompetanse som senere kan vokse og utvikle et laboratorium i samarbeid med næringsliv innen kritisk infrastruktur og relevante myndigheter.

4.2 Beskyttelse av sensitiv informasjon

PST skriver følgende i sin trusselvurdering for 2020: «*Flere lands etterretningstjenester har lange tradisjoner med slik infiltrasjon av utenlandske forskningsmiljøer. Enkelte*

autoritære stater har til og med lover som krever at landets borgere bistår etterretningstjenestene ved behov. Forskningsmiljøer fra slike stater vil derfor være under sterkt press fra hjemlandets tjenester. I 2019 er det eksempler på at forskere fra land det er knyttet bekymring til har lagt til rette for og vært involvert i uautorisert bruk av norske forskningslaboratorier. Norske forskningsinstitusjoner står med andre ord i fare for å bidra til andre staters sikkerhetstruende virksomhet mot Norge og andre land. Gjennom å skaffe seg norsk flerbruksteknologi og -kompetanse vil autoritære staters militære kapasitet kunne styrkes.» (Sitat slutt).

Energiloven § 9-3 2. ledd sier «*at enhver plikter å hindre at andre enn rettmessige brukere får adgang eller kjennskap til sensitiv informasjon om kraftforsyningen»* (Olje- og energidepartementet, 1990). Kraftberedskapsforskriften § 6-1 og §-6-2 gir ytterligere detaljer om beskyttelse av kraftsensitiv informasjon og hva som utgjør kraftsensitiv informasjon. Kbf § 6-2 annet ledd definerer kraftsensitiv informasjon som «*spesifikk og inngående opplysninger om kraftforsyningen som kan brukes til å skade anlegg, system eller annet eller påvirke funksjoner som har betydning for kraftforsyningen,…*» Deretter listes noen eksempler, her nevnes «*f) forebyggende sikkerhetstiltak mot bevisst skadeverk og h) detaljerte analyser av sårbarhet som kan brukes til bevisst skadeverk».* (NVE, 2013)

Forskning på sårbarhet og sikkerhet i kraftforsyningen kan fort komme under kategorien kraftsensitiv informasjon. Forskere som får tilgang til kraftsensitiv informasjon, må undertegne taushetserklæring.

Det pågår et arbeid med å vurdere sikkerhetslovens virkeområde i kraftbransjen. Dersom flere virksomheter enn Statnett blir underlagt, kan det også bli aktuelt at forskning på sårbarhet og sikkerhet for kraftbransjen må ta hensyn til sikkerhetslovens krav til beskyttelse av informasjon.

Både laboratoriumforsøk og forskningsprosjekter må av disse grunnene være mulig å gjennomføre på en slik måte at sensitiv informasjon kan beskyttes i henhold til de krav som er stilt i lovverket. Dette vil kreve at det innføres tilgangsstyring og autorisasjon til laben, logging av tilgang, samt fysisk og logisk sikring. Det kan også være behov for sikkerhetsklarering av personell i enkelte tilfeller og dette må hensyntas i planlegging og utformingen av laboratoriumkapasitet.

4.3 Etikk

Sikkerhetsforskning krever at en tar etiske hensyn, og etikk er utfordrende (Nakashima & Soltani, 2014). Kunnskap som blir ervervet kan benyttes til både gode og dårlige formål. Da reiser følgende spørsmål seg: Er det riktig å tilby sikkerhetsutdanning som i neste omgang kan misbrukes og benyttes til å skade digitale systemer og samfunnet? Argumentet for å svare ja er at de kriminelle uansett vil tilegne seg kunnskap og fortsette med kriminell aktivitet, mens de som skal forsvare systemene vil mangle kunnskap. Et tilleggspørsmål er da om denne type spesialisert sikkerhetsutdanning skal kreve sikkerhetsklarering eller annen form for autorisasjon før opptak til kursene og tilgang til laben. Dette er spørsmål som må avklares mellom universitetet og aktuelle myndigheter, her NSM og NVE.

Ved Universitetet i Tulsa er det gjort en grundig vurdering av de studentene som får opptak til studiet. Universitetet rekrutterer aktivt og i utvalget vektlegges egnethet og verdier som samarbeid, sterkt ønske om å lære og løse problemer for fellesskapet. Vurderingen av sikkerhetsmessig egnethet og motivasjon er prioritert foran akademiske krav herunder krav til studieretning. Sikkerhetsstudiet tar inn studenter med ulik fagbakgrunn på masternivå (teknisk, økonomisk, samfunnsvitenskapelig, språkfag mm.) og gir studentene uavhengig av fagbakgrunn nødvendige tekniske ferdigheter slik at de kan fullføre en Ph.d. utdanning i cybersikkerhet. Begrunnelsen er blant annet at man ikke kjenner morgendagens teknologi og at tverrfaglighet er viktig på dette området (Carpenter, 2010).

Det er viktig at studentene som blir tatt opp ved studiet blir klar over hvor linjene går. Nulldagssårbarheter (svakheter i programvare det ikke er en løsning på ennå) som oppdages kan selges for høy pris til den som betaler mest. Store bedrifter har gjerne bounty-programmer som oppmuntrer til dette. Etisk sett er dette problematisk. Hvilken praksis som skal gjelde må avklares før studiet starter.

Ved Universitetet i Tulsa gis nyoppdaget kunnskap om nulldagssårbarheter vederlagsfritt til leverandører av produkter som er gjenstand for forskning. Slik bidrar forskningen til at sårbarhetene kan lukkes og sikkerheten bli bedre.

5 Internasjonalt samarbeid

I dette prosjektet er Universitet i Tulsa ved professor Sujeet Shenoi en sentral samarbeidspartner. Ph.d. kandidatene kan ta kurs og deltar i forskning i Tulsa. Resten av arbeidet er Ph.d.-kandidatene i Norge og jobber med prosjektet på laben og i miljøet ved NTNU.

For nærings-Ph.d. må kandidaten være 1 år hos selskapet, 1 år hos NTNU og eventuelt 1 år i utlandet. Forskningsrådet har opplyst at det ene året hos NTNU kan gjennomføres i Tulsa hvis NTNU støtter dette fordi de ikke selv har kompetanse på området.

En naturlig del av et Ph.d. løp vil innebære å identifisere kunnskapsfronten. I dette arbeidet er det en forventning at Ph.d. kandidatene vil kunne identifisere mulige samarbeidspartnere i Europa. Så langt har prosjektet identifisert et fagmiljø ved KTH i Stockholm[3], ved Ruhr Universitetet i Tyskland[4] og ved Search-Lab i Ungarn[5]. Disse miljøene er nok små sammenlignet med fagmiljøet ved University of Tulsa.

[3] https://www.kth.se/student/kurser/kurs/IS1200?l=en
[4] https://www.ei.ruhr-uni-bochum.de/studium/lehrveranstaltungen/832/
[5] https://www.search-lab.hu/about-us

6 Samarbeid og organisering

Prosjektet har identifisert og vært i dialog med følgende partnere som en start:

- NTNU
- Elvia
- Statnett
- KraftCERT
- EnergiNorge
- NSM
- NVE

NTNU inngår en separat avtale med Tulsa dersom det er behov for det.

Et utkast til intensjonsavtale (MoU) er utarbeidet og til behandling hos de mulige samarbeidspartnerne. I MoUen skisseres intensjonen med samarbeidet og en ambisjon om å videreutvikle en nasjonal kapasitet på cybersikkerhet og maskinvaresikkerhet.

Det tas sikte på å etablere en rådgivningsgruppe (Advisory Board) som støtte til kompetanse- og kapasitetsbyggingen på dette fagområdet, samt forankring i næringen. De allerede identifiserte mulige samarbeidspartnerne vil få sete i denne rådgivningsgruppen.

7 Videre arbeid

Denne rapporten har dokumentert fase 1 i NVEs FOU-prosjekt 80411 Sikkerhet i digitale verdikjeder og komponenter i kraftforsyningen. Første delmål har vært å få på plass et par Nærings-Ph.d-kandidater fra bransjen på fagfeltet cybersikkerhet, sikkerhet i industrielle kontrollsystemer og maskinvaresikkerhet (hardware reverse engineering). I løpet av forprosjektet har Elvia og Statnett kommet med i prosjektet med hver sin Ph.d-kandidat. Begge selskapene har fått positivt svar på sine Nærings-Phd.d-søknader fra Forskingsrådet. Ph.d-kandidatene søker videre opptak ved NTNU og Universitetet i Tulsa.

Et Nærings-Ph.d-prosjekt krever en god del forberedelser. Arbeidet har vært komplisert pga. pandemien som kompliserer og utsetter utveksling til USA. I tillegg er det en rekke formalkrav for opptak ved universiteter, finansiering og skatt ved utveksling. Her stiller universiteter og Forskningsrådet opp med veiledning. Det er viktig å ha både lederstøtte og kollegastøtte i slike prosesser. Resultatet fra fase 1 er en start.

Dersom dette initiativet skal lykkes, må vi løfte i flokk. «Én svale gjør ingen sommer». De to Ph.d-kandidatene er en start på å bygge opp et nytt fagmiljø i Norge på helhetlig cybersikkerhet, sikkerhet i industrielle kontrollsystemer og maskinvaresikkerhet. På sikt kan dette initiativet videreutvikles under NTNUs NORCICS-program som allerede har fått støtte fra Forskningsrådet.

Det anbefales på denne bakgrunnen å arbeide videre med prosjektet som sådan, men også å videreutvikle ambisjonsnivået sammen med samarbeidspartnere. Å bygge fagmiljøet på cybersikkerhet i Tulsa tok mange år, og tiden må også bidra i byggingen av det norske initiativet.

Et overordnet mål bør være å styrke cybersikkerheten i kraftbransjen gjennom å utdanne eksperter med praktisk og teoretisk kompetanse i grensesnittet elkraft, elektronikk og cybersikkerhet, og utvikle forskningsprosjekter og attraktive cybersikkerhets-utdanningstilbud i Norge. Samarbeidet bør utvides til å omfatte flere aktører og reguleres i en intensjonsavtale (Memorandum of understanding MoU). Arbeid med MoU er i prosess og det anbefales at samarbeidet videreutvikles i samarbeid med eksiterende og nye partnere.

Ved siden av å fullføre de to Ph.d.-prosjektene, som faglig sett komplementerer hverandre, anbefales det at et videreføringsprosjekt har som målsetning å:

- Arbeide videre med utvikling av et nasjonalt laboratorium og utdannings- og forskningskapasitet etter mal av Universitetet i Tulsa som dekker også industrielle kontrollsystemer, driftskontrollsystemsikkerhet og maskinvaresikkerhet.
- Arbeide videre med finansiering som muliggjør å invitere eksperter og gjesteprofessorer til seminarer og workshops i Norge slik at flere i det norske sikkerhetsmiljøet kan lære.
- Å arbeide med målrettet rekruttering av studenter av begge kjønn som er motiverte, kvalifiserte og sikkerhetsmessig egnet for å arbeide med kraftsensitive og graderte problemstillinger i Norge. Her bør rekrutteringsarbeidet lære av erfaringene i USA. Nærings-Ph.d. og Offentlig Ph.d. er mulige inngangsveier, slik som Forskningsrådet i 2020 har gitt muligheter til gjennom 18 stipender innen IKT-sikkerhet og krypto øremerket kandidater med sikkerhetsklarering i 2020.
- Å arbeide videre med en attraktiv trainee-ordning i energibransjen og andre kritiske infrastrukturer der en samarbeider også med sikkerhetsmiljøet i Norge, samt myndigheter. Sammen kan en skape et spennende karriereløp som kopler industri og akademia. Et slikt samarbeid gjør det mulig å bygge kunnskap i grenseflaten mellom elkraft, energiproduksjon og cybersikkerhet.

8 Referanser

Carpenter, S. (2010, 12 3). *Becoming MacGyvers*. Hentet fra www.sciencemag.org: https://www.sciencemag.org/careers/2010/12/becoming-macgyvers

Dubrova, E. (2014, 1 6). *Hardware Security.* Hentet fra www.kth.se: https://www.kth.se/social/files/59102ef5f276540f03507109/hardware_security__2017_05_08.pdf

Europol. (2020, 10 5). *Internet Organised Crime Threat Assessment IOCTA 2020.* Interpol.

Kirkebø, E., & Ljøsne, M. (2018). *IKT-sikkerhet ved anskaffelser og tjenesteutsetting, NVE-rapport 90:2018.* Oslo: NVE.

Lysne, O. (2018). *The Huawei and Snowden Questions.* Springer International Publishing.

Nakashima, E., & Soltani, A. (2014). Cybersecurity: A Special Report. The ethics of hacking 101. *Washington Post*, AA2.

Norges forskningsråd. (2020). *Nærings-ph.d. - doktorgradsprosjekt i bedrift.* Hentet fra www.forskningsradet.no: https://www.forskningsradet.no/sok-om-finansiering/midler-fra-forskningsradet/narings-phd/

Norges forskningsråd. (2020, 10 1). *Søk doktorgrad i digital sikkerhet*. Hentet fra www.forskningsradet.no: https://www.forskningsradet.no/nyheter/2020/doktorgrad-digital-sikkerhet/

NSM. (2020). *Helhetlig digitalt risikobilde 2020. Rapport.* Oslo: NSM.

NVE. (2013, 1 1). *Forskrift om sikkerhet og beredskap i kraftforsyningen*. Hentet fra www.lovdata.no: https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157#KAPITTEL_6

NVE og NSM. (2017). *Informasjonssikkerhetsilstanden i energiforsyningen, NVE-rapport nr 90: 2017.* Oslo: NVE. Hentet fra NVE.

Olje- og energidepartementet. (1990). *Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven) Kapittel 9.* Hentet fra www.lovdata.no: https://lovdata.no/dokument/NL/lov/1990-06-29-50#KAPITTEL_9

PST. (2020). *Trusselvurdering 2020*. Hentet fra politiet.no: https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2020/

T. Gordon, , T., Kilgore, E., Wylds , N., & Nowatkowsk, M. (2019). Hardware Reverse Engineering Tools and Techniques. 2019 SoutheastCon, Huntsville, AL, USA, 2019. *IEEE Xplore*, ss. 1-6.

Wiesen, C., Becker, S., Fyrbiak, M., Albartus, N., Elson, M., Rummel, N., & Paar, C. (2019, Oktober 1). Teaching Hardware Reverse Engineering: Educational Guidelines and Practical Insights. *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*. doi:10.1109/TALE.2018.8615270

NVE

Norges vassdrags- og energidirektorat

MIDDELTHUNS GATE 29
POSTBOKS 5091 MAJORSTUEN
0301 OSLO
TELEFON: (+47) 22 95 95 95

www.nve.no