En oppsummering av Forskningsrådets workshop 22. august 2019 om status for arbeid med cybersikkerhet i energisektoren

ENERGIX
20. september 2019

Innhold

Bakgrunn, målsetting og deltakere

Kraftnettet er en kritisk infrastruktur som både skal effektiviseres og spille en vesentlig rolle i overgangen til fornybar kraft samtidig som leveringssikkerheten opprettholdes. Økende kompleksitet og integrasjon på tvers av flere teknologiområder gir imidlertid nye utfordringer når det gjelder cybertrusler og sårbarhet.

Etter ønske fra Olje- og energidepartementet tok derfor Forskningsrådet ved Energiavdelingen initiativ til en workshop for å etablere en bedre felles forståelse av hvilke cybersikkerhetsutfordringer vi står overfor, hvor langt vi har kommet i å møte disse, aktiviteter og planer i ulike relevante fagmiljøer, og hvilke oppgaver som må løses for å møte fremtidens behov.

46 representanter for nettselskap, leverandørbedrifter, FoU-institusjoner og myndigheter var invitert (se vedlegg). Deltakerne omfattet fagfolk og ledere med ansvar og oppgaver relatert til cybersikkerhet hos myndighetene, nettselskap, leverandørindustri og akademia. Formatet var korte innlegg fra deltakerne og diskusjon i grupper.

Synspunkter og opplysninger som kom frem i presentasjonene, i diskusjonen og gruppearbeidet er oppsummert i dette notatet etter å ha vært forelagt foredragsholderne og gruppelederne.

Forskningsrådet vil benytte resultatene fra denne workshopen i vurdering av FoU-behov innenfor energisektoren som må adresseres fremover.

Resultater fra gruppearbeidet

Det var bred enighet om at konsekvensene ved store cyberangrep er alvorlige, men at risikoen for slike alvorlige angrep er begrenset. Risikoen kan imidlertid være undervurdert hvis system allerede er kompromittert uten at det er avdekket. Deltakerne fra de ulike interessentkategoriene ble plassert i hver sin gruppe og bedt om å vurdere hvor stor del av cybersikkerhetsutfordringen (gapet mellom aktuell og ønsket status) skyldes:

- Manglende kunnskapsoverføring fra andre sektorer (f.eks. forsvaret, IKT) – "*læringsgapet*"
- Manglende brukerkompetanse, rutiner og lederfokus – "*brukergapet*"
- Manglende anvendelse av grunnleggende kunnskap i systemer og verktøy – "*innovasjonsgapet*"
- Manglende lover, regler, standarder og mangler ved nettreguleringen – "*myndighetsgapet*"
- Manglende grunnleggende kunnskap – "*kompetansegapet*"

Gruppenes vurdering av cybersikkerhetsutfordringen er oppsummert i **Tabell 1**.

Størstedelen av gapet mellom aktuell og ønsket tilstand ble primært ansett å skyldes manglende brukerkompetanse, rutiner og lederfokus (*brukergapet*) og manglende grunnleggende kunnskap om cybersikkerhet (*kompetansegapet*).

Det var enighet om at gapet i mindre grad skyldes manglende kompetanseoverføring fra andre sektorer (*læringsgapet*) og mangel på myndighetsstyring i form av lover, regler, standarder og nettregulering (*myndighetsgapet*).

Gruppe/Gruppeleder	Andel av gjenstående cybersikkerhetsutfordringer som skyldes				
	Læringsgapet	Brukergapet	Innovasjons-gapet	Myndighets-gapet	Kompetanse-gapet
Myndigheter / Janne M. Hagen	Liten	Stor	Middels	Middels	Stor
FoU-institusjoner/ Marie Moe	Liten	Stor	Middels	Liten	Stor
Leverandører/ Conny Månsson	Middels	Stor	Liten	Liten	Liten
Nettselskap / Kjell Sand	Liten	Stor	Stor	Liten til middels	Stor

Tabell 1- Arbeidsgruppenes vurdering av cybersikkerhetsgapene

- ***Læringsgapet*** skyldes at bl.a. forsvaret og politi sitter på kompetanse om cybersikkerhet som i liten grad er tilgjengelig for andre sektorer som følge av nødvendig hemmelighold. Nettsektorens mest kritiske system er imidlertid ulike det man finner i andre bransjer, og det er usikkert hva som kan være overførbart. Det bør imidlertid fortsatt være noe å hente fra olje-/gassektoren mht. for eksempel SCADA og fra bank/forsikring når det gjelder datainnbrudd.

- Noen årsaker til ***brukergapet*** er at lederincentiver inklusive nettreguleringen er dårlig tilpasset trusselstrukturen, at cybersikkerhet i for stor grad overlates til IKT-avdelingene, samt at sektoren har mange små enheter med begrensede ressurser og svak, men også uutnyttet kompetanse.

- Av årsaker til ***innovasjonsgapet*** ble det nevnt at kundene ikke setter strenge nok sikkerhetskrav til leverandører og har lav betalingsvilje/-evne for sikkerhetstiltak. Mangel på lab-infrastruktur og strengere standarder ble også nevnt. Det var interessant at leverandørene vurderte manglende anvendelse av grunnleggende tilgjengelig kunnskap i systemer og verktøy, *innovasjonsgapet*, som lite, mens deres kunder, nettselskapene anså det som stort.

- ***Myndighetsgapet:*** For myndighetene er det en stor utfordring at teknologien og system-kompleksiteten utvikler seg så raskt. Sektoren er gjennomregulert, men har kanskje ikke kommet like langt mht. gode standarder. Dagens regulering er en blanding av funksjonskrav og detaljkrav, men med hovedvekt på funksjonskrav. Nylig revidert Kraftberedskapsforskrift har fått positiv tilbakemelding, men små selskap hadde gjerne sett at kravene var mer detaljerte. Noen anser at reguleringen mangler trykk fordi man undervurderer konsekvenser av et angrep, og at NSM burde tatt en mer aktivt rådgivende rolle.

- ***Kompetansegapet*** ble vurdert i hovedsak som en mangel på kompetente fagfolk på cybersikkerhetsområdet og særlig manglende kompetanse om beredskap mot angrep. God beredskap krever bl.a. grunnleggende kjennskap til den enkelte nettvirksomheten med sin blanding av nye og gamle OT- og IKT-system. *Prosjektorientert opplæring og nærings-Ph.D.'er kan være aktuelle virkemiddel for å håndtere denne utfordringen*. Bedre lab-infrastruktur for cybersikkerhet-FoU er også viktig. Representanter for leverandørene vurderte kompetansegapet

lavere enn de andre interessentgruppene, men dette ble begrunnet med at FoU-behovet primært må dekkes av FoU med sterkt brukerengasjement.

Forskningsrådet vil arbeide videre med å strukturere FoU-utfordringene og adressere disse gjennom ENERGIX, IKTPLUSS, SAMRISK, INFRASTRUKTUR programmene og Nærings-Ph.D.-ordningen.

Oppsummering av innleggene

1. Innledning

Rune Volla innledet på vegne av Forskningsrådet og William Christensen på vegne av OED:

- Kraftsystemets økende kompleksitet gjør det vanskeligere å overskue både feilkilder, faremomenter og tilstand.
- Flere eksempler på at utfall har hatt dramatiske konsekvenser for både næringsliv, forvaltning og samfunnssikkerhet.
- Hvilke utfordringer er spesielle for energisektoren og dekkes ikke av det sektoruavhengige arbeidet med cybersikkerhet.
- Å arbeide med disse utfordringene er en viktig oppgave for Forskningsrådets ENERGIX-program.
- Cybersikkerhet er også et viktig tema for programmene IKTPLUSS og SAMRISK. Temaet er også relevant for INFRASTRUKTUR (forskningsinfrastruktur).

2. Kraftnettet en grunnleggende kritisk infrastruktur

Jo De Vligher presenterte Norsk Hydros erfaringer fra cyberangrepet tidligere i år i presentasjonen "*How does a cyber attack look like? A summary of Hydro's real-life experiences*".

- Systemer ble kompromittert ved at en bestilling fra en kunde i Italia ble snappet opp av hackere og utstyrt med skadevare før den ble videresendt
- NH mottok krav om løsepenger den 18.3.19, men det er fortsatt uklart hva motivet for angrepet var
- Det ble umiddelbart iverksatt nullstilling av alle systemer inklusive 22000 PCer. Tilknyttede system som f.eks. Statnett i Norge ble også frakoplet.
- Produksjonen kunne komme i gang relativt raskt, men uten de kommersielle systemene visste man ikke hva som skulle produseres, de ansatte fikk ikke lønn mv. I Brasil ble det gjort en lønnsutbetaling til 5000 ansatte ved å kopiere forrige utbetaling og foreta manuell korreksjon for de som hadde sluttet og begynt osv.
- Gjenoppbyggingen var ekstremt arbeids- og tidkrevende. Først etter 6 uker var de første PCene i gang, men det tok 4 måneder før man igjen var i normal drift.
- Det nye systemet er sikrere enn det gamle, men man kan aldri gardere seg 100% mot innsidehjelp.
- Innbygd sikkerhet må uansett suppleres med gode beredskapsplaner hvis/når et angrep finner sted.
- Gode beredskapsplaner forutsetter en grunnleggende forståelse for alle kritiske prosesser
- De Vligher oppsummerte sine inntrykk som følger:

  - Et stort angrep krever omfattende forberedelser: Hackerne ledes til viktige systemelementer med spionvare ved å følge med på forsvarstiltakene.
  - Digitalisering er som russisk rulett: Hackerne trenger bare en kule i magasinet, men forsvarerne må være på alerten 24/365 (asymmetrisk krigføring).
  - Å rydde opp etter et stor cyberangrep er som å delta i et maratonløp for første gang: Det tar mye lenger tid og er mye mer arbeidskrevende enn ventet.

Jørgen Dyrhaug fra NSM presenterte (mis)forholdet mellom den digitale og den virkelige verden i presentasjonen "*En digital verden vs. virkeligheten*".

- Mennesker er det svake leddet i alle systemer for digital sikkerhet fordi vi ikke er konstruert for å fungere i det virtuelle rommet: Instinkter, intuisjon og følelse av fare fungerer ikke slik som i den virkelige verden.
- NSM har utviklet 23 grunnprinsipper og 123 tiltak for IKT-sikkerhet. Disse er generiske og teknologiuavhengige – det oppfordres til å sette seg godt i disse og praktisere dem.
- På sikt må vi styrke vår grunnleggende forståelse av cyberrisiko ved blant annet å få temaet inn i grunnskolen

Janne Hagen fra NVE la frem etatens betraktninger av digitalisering i kraftsektoren i presentasjonen "*Forskningsbehov på IKT-sikkerhet i energisektoren*".

- Omfattende digitalisering ansees nødvendig for å effektivisere og i det hele tatt bli i stand til å planlegge og drifte fremtidens smarte nett.
- Kraftfulle verktøy for bruk gir imidlertid også kraftfulle verktøy for misbruk.
- Løpende kartlegging av cybersikkerhet viser at mange kraftselskap har opplevd angrep mot administrative systemer, men lite mot driftssystem (SCADA).
- Bruker ca. 1 mill kr. pr. år til FoU på området; bl.a et prosjekt på risiko og beredskap, ett NFR-prosjekt sammen med Lyse m.fl. og i tillegg en egenfinansiert Dr.grad på SCADA-sikkerhet.
- NVE støtter også etablering av en labinfrastruktur for å studere cybersikkerhet ved NTNU, og anser at dette bør være et samarbeid mellom de viktige norske FoU-aktørene på området.
- Hagen ser følgende tema for FoU:
  - Kartlegging av trusselbildet og metodikk
  - Risikoforståelse ved teknologiutvikling
  - Skjerming av sensitiv informasjon
  - Sikkerhet i komplekse integrerte system
  - Sikkerhet i sanntidssystem
- Regulert kryptering skaper større ulemper enn fordeler og frarådes.
- Menneskelige aspekter er viktigst: Vekt på øvelser, rutiner, holdninger.

3. Cybersikkerhet i transmisjons- og distribusjonsnettet

Anders Granum presenterte Statnetts syn på FoU-behovet i presentasjonen "*Statnetts forskningsbehov innenfor cybersikkerhet for drift og overvåking av fremtidens sentralnett*".

- Avgjørende viktig problemstilling for at Statnett skal kunne oppfylle sin rolle
  - Langvarig brudd på strømforsyningen vil kunne føre samfunnet ut i anarki.

  - Backup er etablert, men mye tyder på at det har begrenset varighet (timer, dager) og kan være dårlig vedlikeholdt.
  - Fremtidens kraftnett vil være som et moderne jetfly – kan ikke kontrolleres uten datastøtte. Dette skyldes økende systemstørrelse og -kompleksitet og høyere grad av automatisering.
- Leverandørene ser ikke nødvendigvis direkte lønnsomhet i å utstyre sine system med det siste inne cybersikkerhet; mye av FoU-arbeidet på dette området har lav TRL.
- Kunstig intelligens (AI) og digitalisering hilses med halleluja, men cybersikkerhet og -forsvar er ikke fullt så morsomt. Dette er ikke akseptabelt! Digitalisering og cybersikkerhet må gå hånd i hånd
- FoU-tema
  - Sikkerhetsaspekter vedr. kombinasjonen IKT-system og kraftsystem, sensorer, datalagring og analyse, kommunikasjon, digitale stasjoner mv.
  - Statnett har i dag 63 FoU prosjekter hvor de fleste berører cybersikkerhet i større eller mindre grad.
  - Kapasitetsbygging: Støtter en cybersikkerhet-professor på NTNU og vil etablere nærings-Ph.D.'er hvor cybersikkerhet kan være aktuelt tema.
- Andre tiltak er løpende kartlegging av hendelser og trusler og vedlikehold av sikkerhetsholdninger blant ansatte og kunder. Statnett søker brede samarbeid med bransjen både i Norge, Norden og Europa, og mener det er avgjørende for å lykke med gode løsninger.
- «The future is electric», men forutsetter at vi håndtere cybersikkerhetsutfordringen.

Roar Nygård fra Eidsiva betraktet cybersikkerhet og "*Digital transformasjon i et HMS perspektiv*".

- Nettselskapene har over 99% tilgjengelighet for elforsyning og er svært gode på å håndtere teknisk svikt, naturskader, og arbeidsmiljø, men innen cybersikkerhet er status mye mer usikker.
- Dette aksentueres av økende digitalisering gjennom blant annet bruk av digital måleravlesning (AMS). Stadig større informasjonsmengder og ønsker om deling av informasjon på tvers av fagsystemer og mellom OT- og IT-systemer gir sikkerhetsutfordringer.
- Vi har så langt ikke blitt satt på store prøver, men skadevare kan allerede være installert på våre system som forberedelse til et angrep.
- NVEs kraftberedskapsforskrift gir kraftforsyningen et helhetlig rammeverk for å håndtere cybersikkerhet– men det må implementeres hos alle aktører!
- Utfordringen for bransjeaktørene er at systemkompleksiteten øker raskere enn kunnskapen (som er implementert i system og innarbeidet hos brukerne).
- Manglende dataintegritet kan skyldes eksterne angrep, systemfeil og brukerfeil, men kan uansett føre til personskade, hvis f.eks. en bryter er feilmerket som utkoplet.
- Det er i dag lite fokus på digital sikkerhet i HMS arbeidet: Vi må øke kompetansen vedr. digitale farer og arbeide for «cybersikkerhet for safety»; gå med «digital hjelm».
- Tiltakene må dekke en blanding av ny og gammel teknologi; dersom IKT-systemene må tas ned har man pt. ikke kapasitet/kompetanse til å bemanne alle de stedene i nettet som skal overvåkes og styres; ordonnans vil kunne bli nødvendig ved utfall av digitale tjenester.

- Koplingen av cybersikkerhet til HMS vil øke lederfokus på cybersikkerhet.
- Det er flere aktiviteter på gang for å øke digital kompetanse i kraftbransjen. NTNU CCIS har sammen med NSM og Energi Norge allerede gjennomført kurs i NSMs grunnsikringskrav for nær 100 personer i kraftbransje. Flere kurs for kraftbransjen relatert til cybersikkerhet er under planlegging.

Maria Rodahl Johansen redegjorde for Nettalliansens arbeid med cybersikkerhet i presentasjonen "*Samarbeid om håndtering av cybersikkerhet*".

- Nettalliansen eies av 43 små og mellomstore nettselskap som samarbeider om bl.a. innkjøp, kompetanse, ressursdeling og digitalisering, herunder cybersikkerhet.
- Cybersikkerhetsaktiviteter omfatter utarbeidelse av felles maler (standarder) og rammeverk, beredskapsøvelser, cybersikkerhet-fagdag, tilsynsforberedelser og et IKT-sikkerhetsforum med formål å følge opp NVEs forskrift og opprettholde digital sikkerhet gjennom bl.a.
  - Skattefunnprosjekt innen cybersikkerhet
  - Opplæring og kompetansebygging
  - Organisasjonsutvikling
- Benytter bl.a. KraftCERT som leverandør i cybersikkerhetsarbeidet.

4. Cybersikkerhet FoU-aktiviteter hos FoU-miljøene og i næringslivet

Audun Jøsang fra UiO informerte om "*Gjensidig strømbrudd: Spenningsbalanse og avskrekkingen i cyberspace*".

- Sikkerhet = Beskyttelse av ting som har verdi.
- Ulike sikkerhetsformer omfatter fysisk sikkerhet, samfunnssikkerhet, nasjonal sikkerhet, trygghet, miljø- og informasjonssikkerhet.
- Det spesielle ved informasjonssikkerhet er at den er en forutsetning for alle de andre. Man kan f.eks. ikke ha fysisk sikkerhet i en bil hvis bremsene er hacket.
- Ingen sårbarhet uten en trussel: Det var først da kjøretøyer ble tatt i bruk som drapsvåpen at Karl Johans gate ble vurdert som særlig sårbar for denne typen trusler, og fysiske sperrer ble satt opp på fortauet for å fjerne sårbarheten. Man kan si at denne sårbarheten i praksis ikke eksisterte før trusselen ble relevant. Dette eksempelet viser viktigheten av å identifisere relevante trusler for å kunne se hvilke sårbarheter man har.
- Russland har kompromittert kraftsystemet i USA. For å avskrekke Russland sier USA at de har infliltrert kraftsystemer i Russland, og at de vil gjengjelde ethvert forsøk på kraft-sabotasje fra Russland. Bruk av avskrekking er en ny utvikling innen cybersikkerhet som vi må forholde oss til.
- UiOs FoU innen cybersikkerhet omfatter alle de tre forsvarslinjene:
  - Tekniske: Prevensjon, deteksjon, korreksjon
  - Organisatoriske: Redundans, beredskap, opplæring
  - Politiske: Kjøreregler for håndtering av cybersikkerhet, cyberavskrekking (terrorbalanse), bare presumptivt vennligsinnede leverandører (ikke HUAWEI, men Facebook?)
- Hvordan avdekke opphavet til cyberangrep (attribusjon) – mange måter å skjule sporene, angrep utføres av leiesoldater osv.

Chunming Rong fra UiS belyste cybersikkerhet basert på et smartgridprosjekt i Stavangerområdet i presentasjonen "*Secure and user controlled data sharing in smart grid- Based on Blockchain*".

- Det er etablert et mikronett som er tilknyttet det lokale distribusjonsnettet.
- Mikronettet omfatter aktive brukere med lokal produksjon, lagring og laststyring og den nødvendige infrastruktur for overvåkning og styring.
- Sky- og blockchainteknologi benyttes for å oppnå dataintegritet og automatisering gjennom smarte kontrakter.
- Utfordringen er å oppnå en god balanse mellom datautnyttelse og privatliv.
- Mikronettet vil kunne fungere selv om distribusjonsnettet går ned.

Folke Haugland fra UiA belyste hvordan Lysne-rapportene vil påvirke utdannelsen innen cybersikkerhet i presentasjonen "*Lysne-rapportene: Endringer i ingeniørutdanningene*".

- All ingeniørutdannelse skal nå omfatte cybersikkerhet. Målet er at teknisk personell skal vite nok om cybersikkerhet til å overskue hva de ikke vet.
- Kapasiteten for å utdanne cybersikkerhet-spesialister skal økes, men det synes fortsatt å være begrenset etterspørsel etter disse. Alle som er utdannet ved UiA så langt har havnet i Oslo-området.
- UiA har gitt cybersikkerhet-utdannelsen en praktisk innretning (ikke forskerutdanning) og har forsøkt å tilpasse utdannelsen slik at den supplerer tilbudet fra andre universiteter.

Lilya Budaghyan fra UiB orienterte om "*Crypto research and security education at UiB*".

- Senteret har høy faglig status internasjonalt.
- Omtrent halvparten av aktiviteten finansieres gjennom prosjekter; aktuelle FoU-tema omfatter
  - Utforming og analyse av symmetriske kryptografiprimitiver
  - Kryptografiske boolske funksjoner
  - Bruk av matematisk analyse i kryptografering
  - Blockchain og anvendelse
  - Post quantum kryptografering
- Gir også en rekke kurs innen cybersikkerhet og kryptering.
- Antall professorer er nå redusert fra 4 til 2,4, men gruppen anser å ha de nødvendige ressursene til å øke FoU-aktivitetene og nasjonalt og internasjonalt samarbeid, men opprettholde fokuset på kryptologi.

Stephen Wolthausen og John Olav Tande fra henholdsvis NTNU og SINTEF understreket behovet for labinfrastruktur innen cybersikkerhetsforskning i presentasjonen "*Research infrastructure for cyber security in power systems*".

- Det foreligger et stort arsenal av cybervåpen som deles bl.a. på nettet.
- Som i Norsk Hydro eksemplet vil situasjonen ofte være at systemene allerede er kompromittert når angrepet finner sted slik at det eneste man kan gjøre er å begrense konsekvensene.

- Angriperne kan studere og teste mot virkelige system, men forsvarerne trenger en labinfrastruktur for å kunne gjøre det samme uten å forstyrre daglig drift av kritiske system.
- The Norwegian Cyber Range (NCR) er en arena for undervisning, forskning, testing av cybersikkerhet for alle typer bruker. Den er etablert i Gjøvik og Trondheim og støttes av Forsvaret, Sivilforsvaret, NorSIS, Telenor, and Evry.
- Smartgridlab 1.0 har vært viktig for å kunne tilby en testarena i bl.a. to EU-prosjekter, men fasilitetene for cybersikkerhetsforskning er begrenset.
- Den planlagte Smartgridlab 2.0 vil overkomme disse begrensningene (denne utvidelsen av Smartgridlaben er omsøkt Forskningsrådets infrastrukturprogram).

Gerd Kjølle og Marie Moe fra FME CINELDI orienterte om cybersikkerhetsaktiviteter i CINELDI forskningssenteret i presentasjonen "*Cyber security i fremtidens intelligente distribusjonsnett*".

- De senere årene har tilgjengeligheten av strømleveransene ligget på 99,98%. Hvordan vil digitaliseringen påvirke dette?
- CINELDI omfatter eldistribusjon inklusive tilknytningen til sentralnettet, men ikke transmisjon.
- For å løse sine oppgaver vil fremtidens distribusjonsnett måtte bli mye mer komplisert. CINELDI utfører FoU som skal sikre at robustheten opprettholdes med hensyn til
  - Forsyningssikkerhet
  - Personsikkerhet
  - Cybersikkerhet
- Metodikken er i stor grad basert på brukereksempler (use cases) eller i dette tilfellet 'misuse cases' som både kan omfatte utilsiktet og tilsiktet skade/angrep.
- Forskningen krever bl.a. lab.infrastruktur; ikke mulig å teste angrep i det virkelige nettet.
- Trusselbildet mot industrielle kontrollsystemer har blitt skjerpet de siste årene, flere hendelser hvor cyberangrep har påvirket fysiske systemer har blitt kjent. Et eksempel på aktuelle trusler er spionprogramvare som kartlegger prosesskontrollsystemer og laster opp informasjon til fremmede makter.

Conny Månsson fra ABB informerte om selskapets "*Cybersikkerhetsbetraktninger*" og relaterte aktiviteter i sin presentasjon.

- Store endringer i energisystemet krever store endringer i kontrollsystemene.
- Cybersikkerhet er en utfordring på flere nivåer
  - Virksomhetsnivå: Cyberangrep på kontrollsystemer for industri og elforsyning er reelle og økende.
  - Myndighetsnivå: Virksomheter må overholde forskrifter, regulativer og beste praksis.
  - Teknologi: Sammenkopling av ulike system ved hjelp av kommunikasjonsprotokoller.
  - Drift: Oppetid må opprettholdes.
- Digitale stasjoner er basert på digital kommunikasjon mellom komponenter og omverden for å redusere kostnadene, muliggjøre økt fjernovervåkning og -styring, men også dataangrep.
- Tidssynkroniseringen må være i størrelsesorden ett mikrosekund – det betyr at man ikke har tid til å kryptere og i stedet er tvunget til å autentisere.
- System- og komponentleverandørene bidrar til å møte cybersikkerhetsutfordringen gjennom

  - Sikker kommunikasjon
  - Soneinndeling og perimetersikring
  - Vern mot ondsinnet kode
  - Sikkerhetsoppdateringer
  - Sikkerhetskopiering og gjenoppretting
  - Brukerhåndtering
  - Sikkerhetslogging og monitorering
  - Produkt- og systemherding

  , *men* det er opp til kunden hva de vil kjøpe, og hva de vil ta i bruk.
- En hoveddriver for FoU er stor endringshastighet i digitaliseringen.
- Vi er bare i starten av utviklingen av cybersikkerhetstiltak.

Martin Eian fra Mnemonic informerte om "*Trusseletterretning for kraftsektoren*".

- Den dimensjonerende trusselen er statlige angripere – kan bare møtes ved at alle parter samarbeider.
- Det Russiske Ukraina-angrepet vil ha fått mye større konsekvenser hvis ikke angriperen hadde gjort to (små) feil.
- Kunnskap om trusselen er nøkkelen til å lykkes.
- Mye skjer før et angrep, truseletteretning kan detektere slik aktivitet og hindre angrepet.
- Etterretningen er både strategisk, taktisk, operasjonell og teknisk og omfatter
  - Deteksjon, respons og emulering av angrepet
  - Design av sikkerhetsarkitektur
  - Risikoanalyse
  - Fastsettelse av budsjett og prioriteringer
- Trusselbildet påvirkes av geopolitikk, intern uro, forholdet til konkurrenter og kunder, miljøkonflikter osv.
- Bør det etableres et eget senter for etterretning i kraftforsyningen, eller kan aktørene løse dette hver for seg?

Offentlig regulering og aktuelle FoU-program - Lenker

- Forskrift om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften)
- Nasjonalsikkehetsmyndighets (NSM) grunnprinsipper for ikt-sikkerhet
- https://www.forskningsradet.no/om-forskningsradet/programmer/energix/
- https://www.forskningsradet.no/om-forskningsradet/programmer/samrisk/
- https://www.forskningsradet.no/om-forskningsradet/programmer/iktpluss/
- https://www.forskningsradet.no/om-forskningsradet/programmer/infrastruktur/

Vedlegg

- Deltakerne og gruppefordeling
- Workshop program

** Presentasjonene fra workshopen kan lastes ned via aktive lenker i programmet i vedlegget.*

Forskningsrådet

Deltakere og gruppefordeling

Gruppe 1- Myndigheter	
Gruppeleder:	*Janne Merete Hagen*
William Christensen	OED
Tore Grunne	OED
Jan Magne Bae	OED
Ole Svihus	OED
Laila Berge	OED
Arne Bjørn Mildal	NVE
Janne Merete Hagen	NVE
Jørgen Dyrhaug	NSM
Sverre Aam	Energi21
Rune Volla	Forskningsrådet
Benjamin Donald Smith	Forskningsrådet

Gruppe 2- Universiteter og forskningsaktører	
Gruppeleder:	*Marie Moe*
Folke Haugland	Universitetet i Agder
Audun Jøsang	Universitetet i Oslo
Lilya Budaghyan	Universitetet i Bergen
Rong Chunming	Universitetet i Stavanger
Silje Aakre	Nord Universitet
Stephen W.	NTNU
Nils Kalstad	NTNU
Tor Olav Grøtan	SINTEF
Gerd Kjølle	FME CINELDI
Marie Moe	FME CINELDI
John Olav Tande	SINTEF
Katrine Wyller	Forskningsrådet

Gruppe 3- Leverandører/Industri	
Gruppeleder:	*Conny Månsson*
Stian Anfinsen	NORCE
Magne Granly	Smart Innovation Norway
Conny Månsson	ABB
Geir Faremo	Kongsberg Digital
Jo De Vlinger	Hydro
Eva Brekka	NC Spectrum
Erik Wold	mnemonic
Martin Eian	mnemonic
Olaug Råd	Forskningsrådet
Khanh Tuan Le	Forskningsrådet

Gruppe 4- Nettselskaper og bransjeorganisasjoner	
Gruppeleder:	*Kjell Sand*
Anders Granum	Statnett
Siv Hilde Houmb	Statnett
Jørn Egil Johnsen	Statnett
Solgun Furnes	Energi Norge
Bjørn Høiås	Hafslund Nett AS
Arne Roar Nygård	Eidsiva AS
Maria Rodahl Johansen	Nettalliansen
Berit Berg Tjørhom	Forskningsrådet
Njål Vik Medås	Hålogaland Kraft
Heidi Heggelund	Hammerfest Energi
Hanne Rodahl Johansen	Nettalliansen
Kjell Sand	Smartgridsenteret
Erland Eggen	Forskningsrådet

Workshop: Cybersikkerhet i det norske kraftnettet

09:30 – 16:00, torsdag 22. august 2019
Forskningsrådet, Drammensveien 288, Lysaker | Møterom Abel 1 & 2
Kontakt: Khanh Tuan Le (email: ktl@forskningsradet.no | Telefon: 97688824)

Forskningsrådet arrangerer en workshop om cybersikkerhet i det norske kraftnettet.

Kraftnettet digitaliseres og blir stadig mer effektivt og funksjonsrikt. Økende kompleksitet og integrasjon på tvers av flere teknologiområder gir samtidig nye utfordringer, bl.a. når det gjelder cybertrusler og sårbarhet. Det er meget viktig å ivareta cybersikkerheten til kraftnettet som er en kritisk infrastruktur.

Målsettingen for denne workshopen er å skape en felles forståelse av status for cybersikkerheten i kraftnettet og en synliggjøring av hva som må forskes på og utvikles for å møte fremtidens behov. Workshopen fokuserer på cybersikkerheten i hele kraftnettet utfra dagens situasjon og fremtidige overordnede forsknings- og utviklingsbehov. Målet er at vi kan utarbeide en skisse til GAP-analyse samt forslag til tiltak for å styrke cybersikkerheten i det norske kraftnettet.

09:00 – 09:30	*Kaffe*
09:30-09:40	Velkommen og introduksjon, *Rune Volla*, avdelingsdirektør for energi, Forskningsrådet
09:40-09:50	OEDs forventninger, *William Christensen*, avdelingsdirektør i seksjon for forskning og teknologi, Olje- og energidepartementet
09:50 – 10:30	Kraftnettet, en grunnleggende kritisk infrastruktur *Innspill fra myndighetsorganer på betydningen av og forskningsbehov på IKT-sikkerhet i energisektoren.*
09:50-10:00	How does a cyber attack look like? A summary of Hydro's real-life experiences, *Jo De Vligher*, CIO, Hydro
10:00-10:15	En digital verden vs. virkeligheten, *Jørgen Dyrhaug*, strategisk cyber-sikkerhet, Nasjonal sikkerhetsmyndighet
10:15-10:30	Forskningsbehov på IKT-sikkerhet i energisektoren, *Janne Hagen*, sjefingeniør, Norges vassdrags- og energidirektorat
10:30 – 11:00	Cybersikkerhet i transmisjons- og distribusjonsnettet Erfaring med og håndtering av cybertrusler hos TSO og DSO'er (praksis, beredskap osv.). FoU behov innen cybersikkerhet.
10:30-10:40	Statnetts forskningsbehov innenfor cybersikkerhet for drift og overvåking av fremtidens sentralnett, *Anders Granum*, assisterende FoU-direktør, Statnett
10:40-10:50	Digital transformasjon i et HMS perspektiv – Cybersecurity for Safety, *Arne Roar Nygård*, fagansvarlig informasjonssikkerhet, Eidsiva Nett

10:50-11:00	Samarbeid om håndtering av cybersikkerhet, *Maria Rodahl Johansen*, daglig leder, Nettalliansen
11:00 – 11:15	*Pause*
11:15 – 12:00	Diskusjon i grupper *Etablere en felles forståelse av cybersikkerhetsgapene i de ulike delene av energisektoren.* *Identifisere FoU-behov utfra gapene.*
12:00 – 13:00	*Lunsj*
13:00 – 14:30	Cybersikkerhet FoU-aktiviteter hos FoU-miljøene og i næringslivet *Innblikk i cybersikkerhetsaktiviteter hos FoU miljøene og i næringslivet*
13:00-13:10	Gjensidig strømbrudd: Spenningsbalanse og avskrekkingen i cyberspace, professor *Audun Jøsang*, Universitetet i Oslo
13:10-13:15	Secure and user controlled data sharing in smart grid- Based on Blockchain, professor *Chunming Rong*, Universitetet i Stavanger
13:15-13:20	Lysne-rapportene: Endringer i ingeniørutdanningene, instituttleder *Folke Haugland*, Universitetet i Agder
13:20-13:30	Crypto research and security education at UiB, professor *Lilya Budaghyan*, Universitetet i Bergen
13:30-13:45	Research infrastructure for cyber security in power systems, *John Olav Tande*, sjefsforsker, SINTEF Energi, og professor *Stephen Wolthusen*, NTNU
13:45 – 14:00	*Pause*
14:00-14:10	Cyber security i fremtidens intelligente distribusjonsnett, *Gerd Kjølle*, senterdirektør, og *Marie Moe*, forskningsleder, FME CINELDI
14:10-14:20	Cybersikkerhetsbetraktninger, *Conny Månsson*, manager gridsystem cybersikkerhet, ABB
14:20-14:30	Trusseletterretning for kraftsektoren, *Martin Eian*, forskningssjef, mnemonic
14:30 – 14:45	*Pause*
14:45 – 16:00	Fasilitert diskusjon og oppsummering *Hvordan oppfatter vi cybersikkerhetsgapene i energisektoren? Hva fungerer bra i dag?* *Hva trenger vi av forskrifter, standarder, teknologi og andre tiltak (både 'low-hanging fruits' og langsiktig/strategiske) for å håndtere fremtidens cyberutfordringene?* *Hva er FoU-behov for å møte cybersikkerhetsutfordringene i fremtidens kraftnett?* *Oppsummering av workshopen. Aksjonspunkter og plan for videarbeid.*
16:00	*Takk for i dag og vel hjem!*