Bevisstgjøring og ledelse - utfordringer for sikkerhetsstyring av IKT-systemer i norsk kraftforsyning

Energiberedskap 2016

NVEs beredskapskonferanse for energiforsyningen, 26.05.16

Ruth Østgaard Skotnes

Forsker, Arbeid og sikkerhet – International Research Institute of Stavanger (IRIS)

Førsteamanuensis, Risikostyring og samfunnssikkerhet – Universitetet i Stavanger

PhD-prosjekt – Risikostyring og samfunnssikkerhet (2010-2015)

› Tematisk område: Sårbarhet, teknologi og organisasjon

› Forskningstema: Utfordringer for sikkerhetsstyring av nettselskaper innenfor kraftforsyningssektoren grunnet økt bruk av IKT til å overvåke, kontrollere, og operere kraftforsyning

Bakgrunn - kraftforsyningens IKT-systemer

- Bruk av informasjons- og kommunikasjonsteknologi (IKT) for distribusjon av kraft - betydelig økning de siste tiårene
- Tidligere - ansatte på hvert større kraftforsyningsanlegg overvåket og betjente installasjonene
- I dag - anleggene fjernstyres fra et fåtall driftssentraler

Bakgrunn - kraftforsyningens IKT-systemer

- Tidligere - lukkede systemer, blokkert fra omverden
- I dag - systemene også tilknyttet kontorstøttesystemer og internett
- Sårbare for angrep i tillegg til teknisk svikt

› Foto: Ventyx

Bakgrunn - kraftforsyningens IKT-systemer

- IKT-avhengigheten utgjør en økt risiko i forbindelse med funksjonsfeil i eller dataangrep mot kraftforsyningens IKT-systemer
- Prosesskontrollsystemer (SCADA-systemer) er sårbare overfor en mengde trusler – både naturskapte og menneskeskapte (Rodal, 2001)
- Innbrudd i prosesskontrollsystemer og manipulering med fjernstyrte komponenter kan påvirke det fysiske strømnettet - alvorlige økonomiske konsekvenser, konsekvenser for liv, helse og miljøet (Stouffer, Falco, and Scarfone, 2011)
- Prosesskontrollsystemer - sårbar del av kraftforsyningssystemet

Kritisk infrastruktur - prosesskontrollsystemer

- Kraftforsyningen – en av samfunnets viktigste kritiske infrastrukturer
- IKT-systemer i seg selv blitt en kritisk infrastruktur, og er på samme tid også en viktig komponent i andre kritiske infrastrukturer (Line og Tøndel, 2012)
- Kritisk infrastruktur som styres av prosesskontrollsystemer/SCADA-systemer – i økende grad høyt profilerte mål, samtidig som det i økende grad oppdages sårbarheter og rapporteres cyberangrep (Piggin, 2014)

Trusler og sårbarhet

- NVE: Trusselen tilsvarende stor for Norge som for USA og Europa

- *”IKT en strategisk sikkerhetsutfordring. Truslene mot IKT-systemene øker, og angrepene blir stadig mer avanserte. Vi må regne med at sofistikerte sabotasje- og påvirkningsangrep vil bli rettet mot samfunnskritiske informasjonsressurser, herunder datasystemer som styrer kritisk infrastruktur”* (Nasjonal strategi for informasjonssikkerhet, 2012)

- ”Vi utsettes daglig for cyberangrep. Mange er alvorlige. Vi ser at angriper i hovedsak utnytter kjente sårbarheter. Mange av disse har vi medisin mot, men vi ser at medisinen ikke tas” (Kjetil Nilsen, NSM, 2015)

Trusler og sårbarhet

- *Norske datasystemer er generelt dårlig sikret. Datanettverksoperasjoner kan i tillegg brukes til å skade eller lamme norsk kritisk infrastruktur"* (Politiets sikkerhetstjenestes (PST) årlige trusselvurdering fra 2015)

- *"Dersom nettverksbaserte operasjoner skal kunne forebygges bedre, fordrer dette en styrking av sikkerhetskulturen og årvåkenheten i mange norske virksomheter"* (PST, 2015)

- Implementeringen av Automatiserte Målesystemer (AMS) vil også øke sårbarheten i kraftforsyningssystemet

Trusler og sårbarhet

Nyheter IT

Tidenes hacker-angrep i Norge

50 bedrifter i oljebransjen er bekreftet angrepet og ytterligere 250 varsles nå av Nasjonal Sikkerhetsmyndighet. Dette er det største hackerangrepet mot norske interesser noensinne.

Jonas Blich Bakken , Ingeborg Strand Christensen og Morten Ånestad
Publisert: 26.08.2014 – 21:59 Oppdatert: 26.08.2014 – 22:00

Les hele avisen

Norsk olje- og energibransje er i disse dager utsatt for det mest omfattende hackerangrepet mot norske interesser noensinne, ifølge Nasjonal Sikkerhetsmyndighet (NSM), som er nasjonal varslings- og koordineringsinstans for alvorlige dataangrep.

RÅD TIL BEDRIFTER

- Sørg for å holde programvare og operativsystemet oppdatert.
- Ikke tildel sluttbrukere administratorrettigheter.
- Hold brukerne bevisste.

- Omtrent 300 virksomheter får nå varsel fra oss, med konkret informasjon der vi ber dem se etter spesifikke ting i egne logger. Det er den største varslingen vi har gjennomført, sier Hans Christian Pretorius, direktør for operativ avdeling i NSM.

NSM kjenner til at minst 50 bedrifter er blitt forsøkt hacket, og grunnet usikkerhet går de nå ut og varsler

NSM

Hackertrusselen mot norsk industri øker

Hackere får mer kunnskap om industrielle datasystemer og fjernaksess gjør bedrifter mer sårbare. Det må bli større bevissthet rundt IKT-sikkerhet.

Av Joachim Seehusen

Publisert 18. september 2015 kl. 07:00

Kraftindustrien under angrep

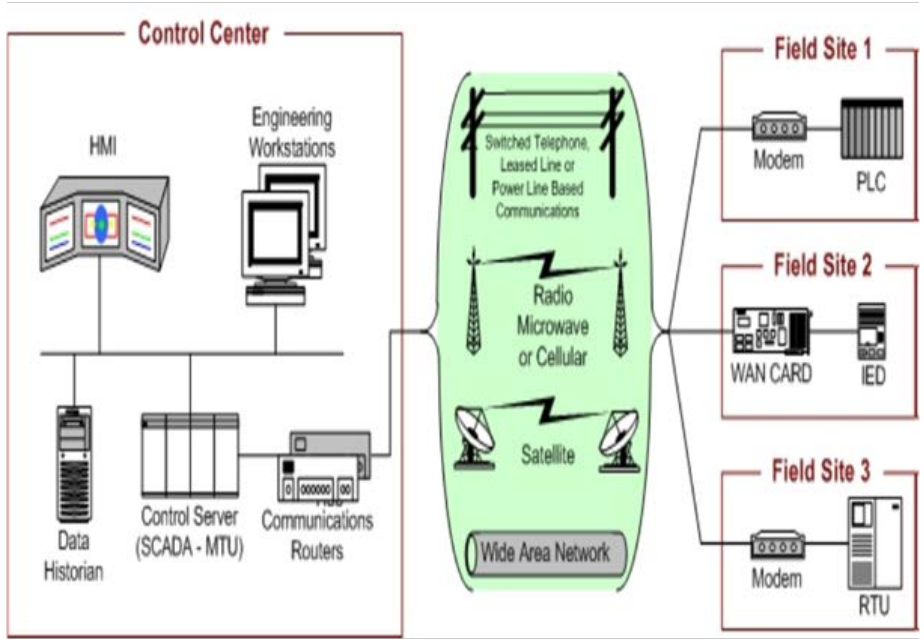
Stadig flere angrep rammer kraftproduserende industri, men det har foreløpig ikke vært alvorlige angrep i Norge

Av Joachim Seehusen

Publisert 18. september 2015 kl. 07:00 - Oppdatert 21. september 2015 kl. 15:40

Teknologi og kompleksitet

- IKT-systemene som benyttes innenfor kraftforsyningen (prosesskontrollsystemer) er mer komplekse enn tradisjonelle IKT-systemer, og har også komplekse interaksjoner med fysiske prosesser
- Stuxnet og etterfølgeren Duqu krysset en viktig grense i og med at IKT-truslene fikk fysiske konsekvenser
- BlackEnergy, Ukraina 2016 – hackere er nå i stand til å slå av strømforsyningen i et naboland



Teknologi og kompleksitet

- Samspillet mellom kompleksitet og usikkerhet er en viktig utfordring ifm. styring av IKT-sikkerhet innenfor nettselskaper

- Kompleksiteten i IKT-systemene kan gjøre det vanskelig for ledere og ansatte i selskapene å identifisere feil i eller angrep på systemene og konsekvensene av dette

- I følge ”Nasjonal strategi for informasjonssikkerhet” (2012) er det en utfordring å holde oversikt over alle gjensidige avhengigheter og potensielle sårbarheter i IKT-systemer

Mai 2016

Energiforsyningen er sårbar

Energiforsyningen må ruste seg mot nye digitale sårbarheter. (Foto: Shutterstock)

Stadig mer komplekse IKT- systemer krever at energibransjen må tenke nytt om sikkerhet. Digital sårbarhet må reduseres, og NVE varsler gjennomgang av beredskapsforskriften.

Teknologi og kompleksitet

- Den økte kompleksiteten i systemer og nett har gjort det vanskeligere for bestillere av IKT-systemer å stille klare og presise sikkerhetskrav til sine leverandører

- Systemenes kompleksitet kan være en trussel i seg selv, og kompleksiteten kan i tillegg påvirke risikopersepsjon og risikobevissthet

Datainnsamling

- Spørreskjema - 137 nettselskaper innlemmet i Kraftforsyningens beredskapsorganisasjon (KBO)
- IKT-sikkerhetsledere/-koordinatorer, beredskapsledere, IKT-medarbeidere, ansatte i driftssentraler
- Spørreskjemaet ble sendt til totalt 334 personer, og 103 respondenter returnerte skjemaet (66 ledere, 32 ansatte) – svarprosent 31 %

Datainnsamling

- På bakgrunn av skjult identitet vites ikke hvor mange av de 137 nettselskapene som representeres blant de 103 respondentene -> 29 IKT-sikkerhetsledere, 11 fra store nettselskaper og 18 fra små nettselskaper

- Intervjuer med representanter fra beredskapsseksjonen i NVE, observasjonsstudier på konferanser om IKT-sikkerhet i norsk kraftforsyning, dokumentstudier

Resultater - risikopersepsjon

Studien viste at respondentene (ledere og ansatte i norske nettselskaper) anså risikoen for feil i eller angrep på selskapenes IKT-systemer som relativt lav

Forsker Ruth Østgaard Skotnes ble overrasket da hun fant ut at nettselskapene selv opplever trusselen mot egne systemer som relativt lav. (Illustrasjonsfoto: Colourbox)

Frykter ikke hackere tross daglige angrep

Alt tyder på et reelt trusselbilde mot norske kraftdistributører. Likevel oppfatter ikke selskapene selv trusselen.

Sikkerhet blir stadig viktigere i møte med flere trusler om dataangrep mot kraftselskapene. (Foto: Jon Petter Evensen, Aftenposten / Scanpix)

Kraftselskapene trener ikke på dataangrep

Risikoen for målrettede angrep mot den norske kraftbransjen øker. Hva gjør selskapene da?

Resultater - risikopersepsjon

- Bekrefter erfaringer fra tidligere forskning -> organisasjonsstørrelse, kunnskap og bevissthet om IKT-sikkerhet, og erfaring med uønskede hendelser er faktorer som kan påvirke risikopersepsjon innad i en organisasjon

- Ledere og ansatte i store nettselskaper oppfattet risikoen for feil i eller angrep på organisasjonens IKT-systemer som noe større enn ledere og ansatte i mindre nettselskaper

- 2 ulike subkulturer innad i norske nettselskaper, avhengig av om ledere og/eller ansatte har el-faglig bakgrunn eller IKT-faglig bakgrunn

Resultater - risikopersepsjon

- Ulike tradisjoner og kultur, og ulike måter å tenke på når det gjelder bruk av teknologien -> mangel på kommunikasjon mellom disse gruppene er en faktor som kan påvirke risikopersepsjonen

- En del problemstillinger i forbindelse med IKT-sikkerhet blir tatt for gitt

- Stoler for mye på leverandørene av deres IKT-systemer og at disse vil tilby sikre løsninger som kan ta seg av alle mulige problemer

Resultater – lederskapsforankring og bevisstgjøring

- Hvis ledelsen er engasjert i IKT-sikkerhet vil de være bevisst på behovet for sikkerhetstiltak og påse at tiltakene blir implementert
- Sterk sammenheng mellom respondentenes oppfattelse av ledelsens engasjement i forbindelse med IKT-sikkerhet (lederskapsforankring) og implementering av tiltak for bevisstgjøring om og opplæring i IKT-sikkerhet
- Flertallet av respondentene i surveyen oppfattet ledelsen i deres organisasjon som engasjerte i forhold til IKT-sikkerhet
- Flertallet av respondentene svarte at i deres organisasjon fikk nyansatte særlig grundig opplæring i organisasjonens sikkerhetsregler (i informasjonssikkerhetspolicy og sikkerhetsinstruks) – 57,3% svarte positivt, 13,6% svarte negativt, og 26,2% var verken enig eller uenig

Resultater – lederskapsforankring og bevisstgjøring

- På spørsmålet om selskapene gjennomførte opplæring i IKT-sikkerhet for ledere og ansatte ettersom IKT-systemene ble oppdatert – svarte 32,3% positivt, 21,6% negativt og 43,1% var verken enig eller uenig
- Bruk av bevisstgjøringskampanjer om IKT-sikkerhet varierte mye mellom selskapene
- På spørsmålet om det i deres selskap ofte ble holdt formelle presentasjoner med informasjon om IKT-sikkerhet for å bevisstgjøre de ansatte – svarte 10,8% positivt, 54,9% negativt, og 33,3% var verken enige eller uenige
- Kun et mindretall av respondentene svarte at det i deres selskap ofte ble vist informasjonsfilmer for å bevisstgjøre de ansatte om IKT-sikkerhet

NOU 2015:13 Digital sårbarhet – sikkert samfunn

- Flere KBO-enheter er små med få ansatte, og det er en kompetanseutfordring å etablere og opprettholde nødvendige fagmiljøer

- Utvalget er gjort kjent med at kompetansen knyttet til IKT-sikkerhet er varierende blant virksomheter i bransjen - det er behov for å gjennomføre flere øvelser innenfor IKT-sikkerhet, der leverandører inviteres med

- Sektorens kritiske rolle tilsier at bransjen må ha god beredskap mot alle typer hendelser, også tilsiktede IKT-hendelser som vi ennå ikke har sett så mange av

- IKT er tett integrert i kraftforsyningen og avgjørende for å sikre en effektiv og sikker drift av systemet. Virksomhetene må selv ha evne til å håndtere hendelser

- Viktig med åpenhet og rask informasjonsutveksling om trusler, erfarte hendelser og mulige avbøtende tiltak

Teknologiskifte i energiforsyningen - Studie om muligheter og sårbarheter (Hagen, 2015)

- Trusselbildet og teknologien er i stadig endring, og det krever en aktiv holdning til sikkerhet og risiko. Ansvaret for sikkerhet ligger på ledernivå i selskapene
- Systemintegrasjon og leverandøravhengighet er en annen sårbarhet.
- I beredskapssituasjoner kan små norske sammenslutninger eller enkeltselskaper risikere å bli nedprioritert
- Utviklingen fra smarte målere til smarte nett vil kreve økt tilsyn og veiledning fra NVE. Bransjens sikkerhetskompetanse må videreutvikles
- Oppnås gjennom FSK og/ eller et partssamarbeid mellom NVE, KraftCERT og bransjeorganisasjonene om kurs og seminarer er en mulighet. Sikkerheten blir ikke bedre enn det svakeste leddet
- ”Kraftbransjen som helhet er heller ikke så langt framme når det gjelder logging og rapportering av hendelser”

Konklusjon

- Menneskelige faktorer, som grunnleggende risikoforståelse, kunnskap, kompetanse, vilje, forståelse og holdninger må være på plass for at organisatoriske og tekniske aspekter ved sikkerhetsarbeid skal fungere etter sine intensjoner

- Med dårlig risikoforståelse, lite bevissthet og engasjement blir kvaliteten på det forebyggende sikkerhetsarbeidet utilfredsstillende

- Økt fokus på IKT-sikkerhet – NVE, Forum for informasjonssikkerhet i kraftbransjen, Forum for IKT-sikkerhet og pålitelighet, KraftCERT

Konklusjon

- Behov for økt bevissthet rundt disse IKT-systemenes kompleksitet og usikkerhet, og økt fokus på IKT-sikkerhet blant både ledere og ansatte i både små og store nettselskaper
- Spesielt aktuelt i tiden fremover på bakgrunn av implementeringen av AMS
- Ledelsen må vise engasjement i forhold til IKT-sikkerhet, både gjennom handlinger og et dedikert budsjett
- Økt bruk av interaktive (ansikt-til-ansikt) presentasjoner og møter kan være et godt tiltak for å øke bevissthet om IKT-sikkerhet innad i organisasjoner
- Diskusjon av hendelser/scenarioer - involvering av de ansatte ved utforming av sikkerhetstiltak
- Informasjonsfilmer – sterke budskap

Konklusjon

- Sikkerhet først på agendaen på alle møter
- Bør forsøke å forbedre kommunikasjonen mellom de to ulike fagområdene innenfor industrielle kontrollsystemer, automasjonsteknologi og informasjonsteknologi
- Viktig at både bransjen og leverandørene av IKT-løsningene samarbeider for å gjøre prosesskontrollsystemene mer sikre
- Bestillere av IKT-systemer må stille klare og presise sikkerhetskrav til sine leverandører