ARBEIDSSEMINAR OM IKT-SIKKERHET OG INTEGRERTE OPERASJONER

30. november 2006 hos Petroleumstilsynet/Oljedirektoratet, Stavanger

Referat

olf PETROLEUMSTILSYNET PETROLEUM SAFETY AUTHORITY NORWAY OLJEDIREKTORATET NORWEGIAN PETROLEUM DIRECTORATE SINTEF

Programkomité

Programkomiteen hadde ansvaret for målsetting, struktur, budsjett og oppfølging av seminaret som ble avholdt den 30/11 hos Ptil. Programkomiteen hadde sitt utspring i arrangørorganisasjonene, men var dessuten forsterket med en representant fra Statnett.

Deltakerne i programkomiteen var:

- Ellen Hagelsteen, OD
- Torleif Husebø, Petroleumstilsynet
- Stig Ole Johnsen, SINTEF
- Thore Langeland, OLF
- Siri Lunde, Petroleumstilsynet
- Tor Aalborg, Statnett

Bidragsytere

Programkomiteen spilte på en prosjektgruppe av bidragsytere som laget innhold og tematikk til konferansen, laget program, fikk inn foredragsholdere, arrangerte konferansen og laget sluttrapport. Deltakere i prosjektgruppen var:

- Eirik Albrechtsen, SINTEF Teknologi og samfunn
- Martin Gilje Jaatun, SINTEF IKT
- Stig Ole Johnsen, SINTEF Teknologi og samfunn
- Odd Helge Longva, SINTEF IKT
- Inger Anne Tøndel, SINTEF IKT

Dessuten bidro Finn Olav Sveen, University of Navarra, som referent.

Innholdsfortegnelse

1. Introduksjon

Arbeidsseminaret om IKT-sikkerhet i integrerte operasjoner ble avholdt den 30/11 2006 hos Oljedirektoratet og Petroleumstilsynet i Stavanger, i regi av Oljeindustriens Landsforening (OLF), Oljedirektoratet (OD), Petroleumstilsynet (Ptil) og SINTEF.

OLF, OD og Ptil spiller viktige roller som premissgivere for initiativer og policyutvikling mht ulike aspekter av IKT-sikkerhet. Samtidig må vi ut fra våre ulike ståsteder reagere og iverksette hensiktsmessige initiativer i forhold til den utvikling som skjer i industrien og i samfunnet for øvrig.

Arbeidsseminaret tok opp til diskusjon en rekke strategisk viktige temaer. Resultatene fra gruppediskusjonene vil dermed få innvirkning på prosesser som OLFs videre arbeid med IKT-sikkerhet, ODs arbeid og Ptils utvikling av en strategi for forvaltning og oppfølging av IKT-sikkerhet i petroleumsvirksomheten.

Målet for seminaret var å:

- Skape oppmerksomhet om informasjonssikkerhet i ulike miljøer (IKT, HMS, automasjon, drift) som er involvert i prosesskontroll- og boresystemer.
- Skape en arena for kunnskapsutveksling og nettverksbygging mellom relevante fag- og forskningsmiljøer
- Identifisere behov for tiltak, herunder forskning og kompetanseutvikling, industri- og myndighetstiltak

Seminaret samlet 46 deltakere fra olje&gass-industrien, leverandørbedrifter, kraftbransjen, offentlige etater og forskningsmiljøer.

Trondheim, 21. februar 2007

På vegne av arrangørene,

Martin Gilje Jaatun
SINTEF IKT

2. Program og arbeidsform.

Programmet for seminaret bestod av en innledning for å skape felles grunnlag for arbeidet fulgt av et gruppearbeid innen 6 forhåndsdefinerte utfordringer før lunch. Hver gruppe skulle foreslå tema knyttet til tiltak og videre arbeid for sesjonen etter lunch. Seminaret hadde fokus på gruppearbeidet.

Foredragene finnes på OD sin nettside under
http://www.npd.no/Norsk/Emner/E-drift/30.11.2006+arbeidsseminar.htm

Innledningen bestod av:

- Åpning – Oljedirektør Gunnar Berge, Oljedirektoratet
- Mål for arbeidsseminaret – Thore Langeland, OLF
- SCADA och informationssäkerhet – Robert Malmgren, Robert Malmgren AB
- SAS/SCADA-systemer til besvær – Lars Bratthall, DNV

Gruppearbeid I: Diskusjon av utvalgte utfordringer – *Eirik Albrechtsen, SINTEF*

- Kommunikasjonsgap og forskjellig kultur, holdninger og kunnskap
- Definering og klassifisering av IKT-hendelser i prosess- og boresystemer
- Indikatorer for oppfølging og måling av sikkerheten
- Hendelseshåndtering
- Sikkerhet innbygget i systemarkitektur
- Sikkerhet ved informasjonsdeling i nett (IKT og prosessutstyr)

Presentasjon av gruppearbeid I og Valg av tema for gruppearbeid II
På grunnlag av diskusjonene i gruppene ble det valgt ut noen tema som gruppene ønsket det skulle arbeides mer med i gruppearbeid II. Alle fikk lov til å stemme prosjekt på sine preferanser og etter opptelling av resultatene gikk vi videre med følgende gruppeoppgaver etter lunsj:

Gruppearbeid II: Tiltak og videre arbeid

1. Tiltak for å redusere kommunikasjonsgap, eks. prosessforståelse og opplæring. Økende krav til flerfaglighet – forståelse for hvorfor
2. How to handle legacy systems and migration path
3. Hva skal til for å nå fase 2 i IO?
4. Hvordan få til rapportering av uønskede IKT-hendelser?
5. Kategorisering av (IT-/SCADA-) systemer

Oppsummering – *Eirik Albrechtsen, SINTEF og Thore Langeland, OLF*

3. Gruppearbeid fase I

I det følgende har vi beskrevet de viktigste momentene fra gruppediskusjonen og tema som ble prioritert fra de forskjellige gruppene. I vedlegget ligger fullt referat fra alle gruppene.

3.1 Kommunikasjonsgap og forskjellig kultur, holdninger og kunnskap mellom IKT, prosess og HMS

Gruppen på seks personer ble ledet av Asbjørn Ueland fra BP.

Reelt sett er driften fjernstyrt i dag, siden prosessene jo styres av et kontrollrom som overvåker prosesser på havbunnen eller på andre deler av plattformen eller på andre plattformer.

Er kommunikasjonsgap: Gruppen påpekte at det var et vesentlig kommunikasjonsgap mellom de forskjellige fagdisiplinene offshore. Installasjonene er teknisk sett meget komplekse med mange forskjellige fagdisipliner involvert. Installasjonene har økt i kompleksitet i de senere årene med økt krav om tilgang til spisskompetanse. Ferdighetene kan også variere, noen dyktige mekanikere liker ikke å skrive, noe som gjør at en kan få dårlige rapporter om uønskede hendelser.

Komplekse prosesser: De underliggende arbeidsprosessene, f eks i SAP, er komplekse og vanskelige å forstå. Det kan være vanskelig å forstå systematikken i arbeidsordre, et viktig poeng er å forenkle og å gi god opplæring.

Rutinene fra de enkelte fagdisiplinene er ikke tilpasset virkelighetens offshore: Som eksempel ble det påpekt at en mekaniker offshore må huske 7-8 passord. Disse passordene skal sikre IKT-systemene, men mekanikerne forstår ikke hvorfor en trenger passord som sinker jobbutførelsen – alle som er offshore er jo autentisert og kontrollert. IKT-avdelingen er ofte lite synlig offshore.

DFU med IKT trengs. I forbindelse med håndtering av ulykker er det i dag laget et sett av DFU'er (definerte fare- og ulykkeshendelser) som brukes som basis for beredskap og opplæring. I dag er det ingen DFU som omfatter en uønsket IKT-hendelse, gruppen foreslo at det burde lages minst en DFU som innbefattet en uønsket IKT-hendelse, slik at organisasjonen kunne trene på det.

Mange utfordringer er knyttet opp til kulturforskjeller mellom hav og land, kvaliteten på kommunikasjon mellom hav og land blir derfor spesielt viktig. Dessuten god felles forståelse for hva man skal gjøre, hvordan og hvorfor.

Forslag til tema for Gruppearbeid II - tiltak og videre arbeid

Krav om flere ferdigheter hos hver enkelt arbeidstager, forståelse mellom hav og land og felles prosessforståelse mellom hav og land og mellom de forskjellige fagdisipliner. Foreslåtte tema fra gruppen til fase II er da:

- Interessekonflikt eller samarbeid
- **Tiltak for å redusere kommunikasjonsgapet**

3.2 Definering og klassifisering av IKT-hendelser og hendelseshåndtering

Gruppen på ni personer ble ledet av Lars Grøteide fra Norsk Hydro.

Gruppen bestod av medlemmer fra to grupper ”definering og klassifisering av IKT-hendelser” og ”hendelseshåndtering”. Gruppen fokuserte mest på hendelseshåndtering da de fleste deltakerne var fra den gruppen.

Viktig å klassifisere systemer. Gruppen så på klassifisering av systemer som viktig. Det ble nevnt en klassifisering av systemer i 4 grupperinger, 4: Instrumenterte sikkerhets-systemer, 3: Prosesstyringssystemer, 2:Vanlige interne IKT systemer brukt til administrative formål og 1: Internett, systemer utenfor bedriften.

Få på plass gode rutiner for hendelsesrapportering. Gruppen så det som viktig å få på plass gode rutiner for rapportering og oppfølging av uønskede hendelser. Rapportering av uønskede hendelser bør løftes til ledelsen. En bør følge opp alvorlighetsgraden av uønskede hendelser, slik at man får på plass risikoforståelsen av hendelsen. Det er viktig med tidlig varsling og ha oversikt over hva som har skjedd før.

Få til et samarbeid mellom HMS og IKT ifbm hendelsesrapportering. HMS avdelingen har ofte på plass gode rutiner og systemer for hendelseshåndtering. Rapportering av uønskede IKT hendelser har derfor mye å lære av HMS.

Viktig å dele uønskede IKT hendelser både eksternt og internt.
Oppmerksomheten rundt uønskede IKT hendelser innen olje og gass er lav, og en mangler gode eksempler for å skape forståelse av hva som kan gå galt. Det er derfor viktig at en etablerer rutiner for å samle og dele oversikt over uønskede IKT hendelser.

Viktig å etablere gode holdninger, eks en ”Reporting Culture” internt.
Det ble referert til en episode hvor en person fikk ”kuttet hodet” etter rapportering av en uønsket hendelse internt. Dette er ikke med til å skape god holdninger for rapportering og erfaringsdeling – det er derfor viktig at ledelsen følger opp dette systematisk.

Viktig å integrere sikkerhet med kvalitetsforbedring. Det ble påpekt at det er meget viktig å integrere sikkerheten med det totale arbeidet knyttet til kvalitetsforbedring i hele bedriften.

Forslag til tema for Gruppearbeid II - tiltak og videre arbeid

- **Hvordan få til rapportering og varsling av uønskede IKT hendelser**
- Kategorisering av systemer – struktur og metodikk
- Risikomodeller – proaktive modeller

3.3 Indikatorer for oppfølging og måling av sikkerheten

Gruppen på seks personer ble ledet av Rune Ask fra DNV. Deltakerne hadde bakgrunn fra kraft, olje og forskning.

Det er vanskelig å måle informasjonssikkerhet, det er mange ulike synspunkter på hvordan dette skal gjøres. I OLF sin arbeidsgruppe for informasjonssikkerhet (AGI) er et av målene er å finne fram til indikatorer.

Hva er formålet med indikatorer, hva skal de brukes til?
Sett fra bedriftens side er målet bedre informasjonssikkerhet og gjennom det bedre økonomi.
Indikatorer brukes

- som mål for om informasjonssikkerheten er i samsvar med policy og rammer
- til å forbedre informasjonssikkerheten og å integrere den inn i forretningspraksis
- for å måle virkningene av tiltak for å forbedre informasjonssikkerheten
- for å kunne dokumentere overfor tilsyn at informasjonssikkerheten er i samsvar med lover og regler

Det er viktig å kople samordne arbeid med informasjonssikkerhet og med HMS. Riktig valg av indikatorer kan bidra til dette

Målinger: Vi ønsker å måle i forhold til en baseline/ referanse, for eks OLF sin ISBR. I USA arbeides det med ”Baseline for security in SCADA”. ISA SP99 er i gang med en standard for "Manufacturing and Control Systems Security". Dessuten finnes NIST SP 800-53 og arbeid med "Applying NIST SP 800-53 to Industrial Control Systems". Baseline definisjoner er sentrale i dokumentene.
Trenger vi egne indikatorer for SCADA? Skal vi skille mellom prosess og administrative funksjoner? Hva slags indikatorer skal vi bruke for å måle avvik i forhold til policy?
Krav fra revisjon og tilsyn krever spesielle indikatorer
Innen oljesektoren og kraftsektoren må det tas hensyn til både bedriftsmessige og samfunnsmessige forhold. Valg av indikatorer må avspeile dette

Risiko
Indikatorene skal brukes i risikovurdering hvor risiko = sannsynlighet x sårbarhet. Ved risikovurderinger hvordan skal vi se på hendelser med store konsekvenser men med liten sannsynlighet kontra hendelser med små konsekvenser og med stor sannsynlighet? Vi kan ikke uten videre bruke statistikk, vi må legge mer ressurser i å gardere oss mot katastrofer.
Det legges alt for liten vekt på verdisetting av ”assets”

Forslag til tema for Gruppearbeid II - tiltak og videre arbeid

- Videre arbeid med ”Self Assessment ” for sikkerhet i SCADA og måling av sikkerhetsbevissthet
- Bygge erfaringsdatabaser ved direkte tekniske målinger på SCADA-systemer, eks. oppetider/nedetider/responstider ved sikkerhetsbrudd.
- Indikator/måleparameter på konsekvenser av sikkerhetsbrudd i SCADA-systemer

3.4 Sikkerhet innbygget i systemarkitektur

Gruppen på tretten personer ble ledet av Lars Bratthall fra DNV.

Innledning

Vi må ha en felles standard for bransjen. Vi må finne ut hva som faktisk er i bruk i dag (generasjon 1), og bestemme hva vi må ta i bruk for å komme til nivå 2 (generasjon 2 – se Figur 5 på s. 36).

Diskusjonspunkter

Det introduseres stadig nye løsninger i olje/gass, men det er lang turnover – **prosesskontrollutstyr har gjerne en levetid opp mot 30 år**. Bare det å finne alle tekniske systemer på en installasjon er en utfordring (ikke alle er tegnet inn).
Det er fortsatt lite investering i sikring – operatøren må tåle å betale for sikkerhet.
Er **sertifisering** av utstyr og produkter veien å gå?
Leverandører og operatører trenger felles kriterier for evaluering av komponenter og systemer. Det er mye fornuftig i **Common Criteria** (ISO/IEC 15408), men det er lite sannsynlig at vi vil se CC-evaulerte (for ikke å si sertifiserte) systemer [27] i prosessindustrien med det første.

Hvor mye kan man oppnå ved bruk av monitorering utenom sikkerhetssystemet? Er det mulig å **skille prosesskontrollsystemene** fra sikkerhetssystemene?

I **kraftsektoren** forholder man seg ikke til én leverandør. Tradisjonelt har man operert med isolerte nettverk, men disse åpnes nå; man har i stor grad informasjonsflyt mellom kontorsystemer og prosesskontrollsystemer. For å øke sikkerheten i forbindelse med IO, må man både redusere risikoen for at en inntrenging finner sted, samt redusere virkningen av de inntrengingene som slipper gjennom forsvarsverkene. Samtidig må vi ikke glemme at IO også handler om å redusere kostnader – hvis man stiller så store sikkerhetskrav at tiltakene totalt sett blir for dyre, er man dømt til å mislykkes. På den annen side burde man kunne bake inn kostnader til IT-sikkerhet i begrepet **"the cost of doing business"** – det er i dag ingen krav til IT-sikkerhet på samme måte som det er krav til HMS.

Slik sett burde **Ptil** være "eier" av en standard, gjerne med flere nivåer eller "stigetrinn" som aktørene kan forholder seg til (Ptil presiserer at de ikke lager slike standarder selv, så det er opp til næringen å ta et initiativ i denne sammenhengen). Problemet er at spesifikke krav i regelverk fort blir statiske; ved å fokusere på funksjonelle krav er det lettere å unngå at regelverket hindrer teknologiutvikling.

Forslag til tema for Gruppearbeid II - tiltak og videre arbeid

- **How to handle legacy systems and migration path**
- **Hva skal til for å nå fase 2 i IO?**

3.5 Sikkerhet ved informasjonsdeling i nett (IKT og prosessutstyr)

Gruppen på syv personer ble ledet av Chunming Rong fra UiS.

Semantisk web kommer og har et potensial innen Integrerte Operasjoner.
Det var en klar holdning om at Semantisk web kommer og at denne teknologien vil ha konsekvenser for Integrerte operasjoner. Det var litt usikkerhet knyttet til sammenhengen mellom semantisk web, web services og tjenesteorientert arkitektur (SOA) samtidig som dat var forskjellig kompetanse i gruppen..

Sertifisering/tillit i forbindelse med integrering av systemer.
Når man skal kople sammen systemer fra forskjellige leverandører slik at de kan snakke sammen vil tillit være vesentlig. Man trenger også å ha tillit til sikkerheten i systemet. En bør vurdere å bruke sertifisering av SCADA systemer.

Sikkerhetsutfordringer med Semantisk web.
Økt konnektivitet og det at systemene snakker samme språk kan gi økte/nye sikkerhetsutfordringer som må tas hensyn til. Det blir kanskje enda viktigere for de som kjøper software å ha tillit til systemutviklingsprosessen eller å vite at utviklingen har skjedd ihht etablerte standarder. Et viktig punkt som ble diskutert var sikkerheten mellom produksjonsnett og administrativt nett i en løsning der man bruker teknologi for semantisk nett.

Felles autentiseringsløsning. Etablering av en felles autentiseringsløsning slik at man kan gjenbruke autentisering gjort i et annet selskap. Det er vanskelig for et selskap å vedlikeholde informasjon for å kunne autentisere andre selskapers ansatte. Det ble foreslått å se på en løsning med en felles autentiseringshub.

Forslag til tema for Gruppearbeid II - tiltak og videre arbeid

- Integrering av webtjenester-sikkerhetsstandarder i en overordnet systemarkitektur
- Utarbeidelse av en felles tillitsarkitektur

4. Gruppearbeid fase II

Under er listet opp forslagene fra gruppearbeid I til tema for gruppearbeid II. I parentes er angitt hvilke grupper forslagene kom fra. Etter avstemning blant deltakerne ble de tema som er uthevet valgt for behandling i gruppearbeid II.

1. Integrering av web-tjenester og sikkerhetsstandarder i en overordnet systemarkitektur (gruppe 6)
2. Utarbeid en felles tillitsarkitektur (m/myndighet) for å muliggjøre adgangskontroll og rollebasert informasjonsdeling på tvers av organisasjoner (gruppe 6)
3. Interessekonflikt eller samarbeid mellom ulike miljøer (gruppe 1)
4. Indikatorer I: Videre arbeid med selfassessment skjema for sikkerhet i SCADA og måling av sikkerhetskultur (gruppe 3)
5. Indikatorer II: Etablering av erfaringsdatabaser ved tekniske målinger på SCADA-systemer ved sikkerhetsbrudd (gruppe 3)
6. Indikatorer III: Indikatorer/måleparametre for konsekvenser av sikkerhetsbrudd i SCADA-systemer (gruppe 3)
7. Risikomodellering – proaktive modeller (Gruppe 2/4)

8. **Tiltak for å redusere kommunikasjonsgap, eks. prosessforståelse og opplæring. Økende krav til flerfaglighet – forståelse for hvorfor (gruppe 1)**
9. **How to handle legacy systems and migration path (Gruppe 5)**
10. **Hva skal til for å nå fase 2 i IO? (Gruppe 5)**
11. **Hvordan få til rapportering av uønskede IKT-hendelser? (Gruppe 2/4)**
12. **Kategorisering av (IT/SCADA) systemer (Gruppe 2/4)**

I det følgende har vi beskrevet de viktigste momentene fra gruppediskusjonene. I vedlegget ligger fullt referat fra alle gruppene.

4.1 Tiltak for å redusere kommunikasjonsgap

Gruppen ble ledet av Asbjørn Ueland fra BP, med fem øvrige deltakere fra forskning og myndigheter.

Eksempel på tiltak omfatter økt prosessforståelse og opplæring. Bransjen opplever økende krav til flerfaglighet – det er økt behov for forståelse for *hvorfor* i forskjellige sammenhenger. IT-folk har gjennomgående et udekket kompetansebehov med hensyn til å forstå brukerperspektivet, betingelser og konsekvenser i "den virkelige verden". Slik sett bør man jobbe for å få en generell anerkjennelse av at fler-/tverrfaglighet er kompetanse – uten at kravene til den enkeltes spesialist-kompetanse derved blir mindre. Alle må få større forståelse for kompleksiteten i virksomheten.

Et prinsipp i informasjonssikkerhet er at man skal iverksette de billigste og raskeste tiltakene først. Således er det mye å tjene på å unngå "de dumme feilene" som skyldes at brukere misforstår eller ikke kjenner til regler og prosedyrer. Vi bør tilstrebe å finne kompetansekrav for å unngå at den enkelte ansatte blir en IKT-trussel.

Sentralt i all type læring og kommunikasjon:

- hva forventes,
- hvordan skal det gjøres, og
- hvorfor.

Når det gjelder IT, kan det av og til synes som om hvorfor-biten har falt helt ut.

Forslag til tiltak

- Det må trenes og folk må møtes sosialt for å bygge tillit – trene på kommunikasjon mellom
  1) typer mennesker og
  2) fag/profesjoner/roller

4.2 How to handle legacy systems and migration path

Gruppen på 8 deltakere ble ledet av Lars Bratthall fra DNV.

Til tross for at deltakerne ikke klarte å finne en god norsk tittel på dett temaet, er målet å få til en pålitelig integrasjon av nye og eksisterende systemer – dvs. en integrasjonsprosess som unngår at ting rakner underveis.

For å nå dette målet må vi forholde oss til:

- Tekniske utfordringer
  - identifisering av de elementer som gjør/forhindrer at vi tjener penger
- Arbeidsprosesser
  - Innvirkning av arkitektur på tvers av organisasjoner
  - Evaluering av (under)leverandører
  - Revisjon
- Organisasjon/kultur
  - Bevissthet
- Policy
  - Styring av arkitektur i organisasjonene

Det er viktig å starte i rette enden, og sørge for at sikkerhetstenkning legges til grunn for design ikke bare av sikkerhetssystemer, men også av generelle kontrollsystemer. Dette forutsetter ingeniører med mer evne til helhetstenkning en det som er normen i dag.

Prinsippet om uavhengigheten til de instrumenterte sikkerhetssystemene (SIS) utfordres i økende grad i tiden som kommer, ettersom informasjonsbehovet medfører at komponenter koples fysisk sammen.

Konsekvensen blir at man ikke lenger kan slå en ring rundt plattformen og kalle dette for en sikkerhetsperimeter, i fremtiden må også landbaserte operasjoner og leverandører regnes med i sikkerhetsperimeteren.

Sikkerheten utfordres også ved at tidligere ”dumme” enheter i stadig større grad leveres med innebygde mikroprosessorer, sensorer og kommunikasjonsmuligheter, uten at brukerne i tilstrekkelig grad er oppmerksomme på dette.

Forslag til tiltak

- Vi trenger flere ingeniører som snakker både prosesstyring og IT! Dette er en utfordring til utdanningsinstitusjonene.

4.3 Hva skal til for å nå fase 2 i IO?

Gruppen på åtte personer ble ledet av Thore Langeland fra OLF.

I fase to av IO vil man ha tettere integrasjon mellom operatør og leverandør. Viktige aspekter er deling av sanntidsinfo, linket opp slik at man kan bruke ekspertise over hele verden, mer automatisering – embedded systems og agenter.

Selskaper trenger å dele informasjon, men er også konkurrenter dette problemet er størst når konkurrenter selger tjenester til samme operatør. En utfordring er å komme frem til en felles måte å gjøre dette på slik at leverandører kan opptre på samme måte uavhengig av hvilket selskap de er inne hos.

Når det gjelder prosesskontroll, er det for mange som har tilgang og hvis man kommer inn og har nok kunnskap, har man tilgang videre. Det ble også påpekt at dagens løsninger ikke skalerer godt. Det er mye administrasjon og man må vedlikeholde regler i brannmur. Dette blir fort komplekst.

Semantisk web handler om at systemer kan snakke sammen og forstå hverandre. Man erstatter ikke nødvendigvis systemet man allerede har. Semantisk web vil gjøre det lettere med vedlikehold av systemer. Det blir mindre behov for manuelt arbeid.

Hvert enkelt oljeselskap må håndtere mye tilgang. I fremtiden kunne en løsning være å lage en hub slik at man kan benytte autentisering i andre selskaper. Det er bedre å stole på autentiseringen f.eks. Halliburton gjøre av egne ansatte, enn at man selv skal begynne å autentisere folk fra Halliburton. Det er vanskelig å ha kontroll på andres ansatte – hvem som slutter osv. Det er mye serviceselskap-personale som går igjen hos flere. Man kunne ha en felles portal for disse med gyldig autentiseringsnøkkel.

Det er et trykk på mannskapssiden hos serviceselskapene. Man har ikke lenger nok personer å utplassere i sentrene, mer må gjøres fra selskapenes egne lokaler. De trenger da tilgang til det samme som om de satt hos operatør. Det finnes teknologi for dette nå, men operatører har ulikt syn på hvordan man gjør dette. Det ville vært nyttig med felles guidelines på ansvarsforholdet, hva forventer vi at serviceselskapene stiller opp med, hvor går grenseflatene, skal de ha nettverksløsninger frem til vår brannmur, skal vi ha nettverksløsninger frem til deres brannmur, osv. Alle har de samme problemstillingene, og det burde gå an å enes om noe.

Forslag til tiltak

Det ble pekt på følgende ting man ønsket at det ble tatt tak i fremover:

- Definere hva som er god praksis. Man ønsker praktiske løsninger og svar på spørsmålet: Hva er den anbefalte måten oljebransjen gjør dette på? Dette må spres slik at man kan få kommentarer.
- Fortsette arbeid med begrepsapparat. Man legger forskjellig betydning i ordene. Ønsker forskningsprosjekter støttet av EU for å få på plass ontologi
- Kjør flere pilotprosjekter. Man opplever motvilje – mange er redde for at ting skal gå galt. Pilotprosjekter kan vise at det fungerer.

4.4 Hvordan få til rapportering av uønskede IKT-hendelser?

Gruppen på seks personer ble ledet av Lars Grøteide fra Norsk Hydro.

Informasjon om uønskede IKT hendelser må spres til egne ansatte.
Kontrollromsoperatører på offshore oljeplattformer, som sitter sentralt når et problem skal løses, var ikke kjent med virus og ormangrep. Når en uønsket IKT hendelse da inntreffer – kan det være vanskelig å få løst problemet på en god måte siten de ansatte er helt ukjent med problematikken. Gruppen foreslo en fokus på opplæring som et mulig tiltak. Man bør bruke erfaringslæring (andres erfaring) og historiefortelling. Dette gjør det mer forståelig enn en lang rekke med påbud og forbud.

Fokus på rapportering av uønskede hendelser.
Det er viktig med god rapportering av uønskede hendelser. Feil i prosesskontrollsystemer kan få store konsekvenser. Det er derfor viktig at slike hendelser blir rapportert uavhengig om de er sikkerhetsrelatert eller ikke.

Forenklede rapporteringsrutiner med god tilbakemelding.
Det er kjent at rapportering av hendelser er ekstra arbeide for den som rapporterer. Det bør derfor legges til rette for enkel rapportering. I tillegg til arbeidsbyrden er det flere faktorer som påvirker rapporteringen. Hvis rapportøren ikke blir holdt oppdatert av hva som skjer med hans rapport og om den var nyttig, så vil operatøren heller ikke se nytten med å rapportere Hvis rapportering over tid ikke fører til en forbedring av sikkerheten, så vil rapportering bli sett på som unyttig, og dermed ikke bli gjort. Og hva er vitsen med å rapportere hendelser hvis man ikke lærer noe av de?

Viktig med slakk i organisasjonen og tid til samlet refleksjon.
Det må være slakk i systemet, d.v.s. tid til refleksjon. Studier fra MIT viser at hvis man bare jobber hardt, så har man ingen tid til å forbedre seg [21]. Hard jobbing fører kortsiktig til gevinst, men man når fort en grense. Det er begrenset hvor mye hardere en person kan jobbe. Bruker man derimot tid til å utvikle verktøy som hjelper en til å jobbe smartere vil dette føre til langsiktig vinning. Det ble påpekt at det er viktig at de forskjellige aktørene i systemet snakker sammen. I forløpet til 11. september var det mange som hadde kompetansen til å forstå sammenhengen, men de hadde ikke det fulle bilde av situasjonen. Ingen hadde hele bildet. Man må snakke sammen for å legge puslespillet

Indikator som viser trusselnivået.
Det ble påpekt at en del enheter har varslingssystemer som viser trusselnivået. Man burde kanskje implementere et tilsvarende system for operatører, slik at de kan være ekstra beredt hvis trusselnivået øker.

Gruppen kom frem til tre tiltak som det bør jobbes videre med:

- **Skape en kultur for rapportering**
- **Opplysning om hendelser/erfaringslæring**
- **Samle inn god praksis mhp rapportering og håndtering av hendelser.**

4.5 Kategorisering av (IT/SCADA) systemer

Gruppen på sju personer ble ledet av Arnt Steinbakk fra Ptil.

Innledning

- Oppgaven for gruppen var å diskutere måter å kategorisere systemer med hensyn på informasjonssikkerhet og å foreslå tiltak og videre arbeid.

Formål med kategorisering er å kunne

- sette sammen systemer av ulike komponenter med gitte krav til sikkerhet for totalsystemet, kople sammen ulike systemer og oppnå gitte krav til sikkerhet for totalsystemet

Momenter fra diskusjonen

- **Tjenestene** er de som er de kritiske, ikke systemene.
- **Verdifastsetting** er viktig element i kategorisering
- Systemer kan ha både **en kritisk og en ukritisk funksjon**. Vi må ha integrasjon mellom kritiske og ukritiske systemer. Problem med **"legacy systemer"**. Både kategorisering av disse og sammenkopling med nye systemer. SKS har arbeidet med domenebeskrivelser. Sammenkoplings(inter)domene vil være de kritiske
- I SCADA systemer står konfidensialitet i dag ikke på prioritert liste, **tilgjengelighet** går foran alt
- NSM: **Objektsikkerhetsforskriften** kommer forhåpentligvis i 2007. Disse vil sette konkrete krav til sikkerhet. Kan man identifisere delsystemer etter kritikalitet?
- **Kraftsektoren** har kategorisering, oljesektoren ikke. Det er krav til robusthet og til redundans fra NVE. I tillegg kommer sikkerhetsloven og bedriftsspesifikke krav. NVE sin beredskapsforskrift gir klare sikkerhetskrav
- Selv om produktet Sannsynlighet x Konsekvens er lite må det tas alvorlig. Der konsekvensene er veldig store, **katastrofer**, må det tas spesielle forholdsregler.
- Hva med å bruke **Common Criteria** med EAL-nivåer som kategorisering?
- For kategorisering må vi ha en referansemodell og en **referansearkitektur**
- **Leverandørene** trenger spesifikke krav for å utvikle "sikre" systemer/komponenter. Ptil vil samarbeide med OD om krav

Konklusjoner

Kategorisering av sikkerhet for komponenter og systemer er i stor utstrekning upløyd mark hvor det er rom for betydelige framskritt. Samtidig er det meget komplisert og krever omforent metodikk i form i av "best practice" og /eller standarder.
Her ligger det mye arbeid for konsulenter og forskere mtp kategorisering av komponenter, forskning på arkitektur

Forslag til tiltak/områder hvor det gjøres videre arbeid:

- **Risikovurderinger på tjeneste/funksjonsnivå**
- **Referansearkitektur for å sette krav til komponenter/delsystemer**
- **Referansemodeller for grenseflatene mot andre systemer**
- **Sertifisering som en del av kategorisering**
- **Myndighetene må sette klarere krav (tre-partssamarbeidet)**

5. Forslag til tiltak fra Gruppearbeid II

Under er oppsummert de forslag til tiltak som kom fram i gruppearbeid II.

1. Det må trenes og folk må møtes sosialt for å bygge tillit – trene på kommunikasjon mellom
    a. typer mennesker og
    b. fag/profesjoner/roller

2. Vi trenger flere ingeniører som snakker både prosesstyring og IT! Dette er en utfordring til utdanningsinstitusjonene.

3. Definere hva som er god praksis. Man ønsker praktiske løsninger og svar på spørsmålet: Hva er den anbefalte måten oljebransjen gjør dette på? Dette må spres slik at man kan få kommentarer.

4. Fortsette arbeid med begrepsapparat. Man legger forskjellig betydning i ordene. Ønsker forskningsprosjekter støttet av EU for å få på plass ontologi

5. Kjør flere pilotprosjekter. Man opplever motvilje – mange er redde for at ting skal gå galt. Pilotprosjekter kan vise at det fungerer.

6. Skape en kultur for rapportering

7. Opplysning om hendelser/erfaringslæring

8. Samle inn god praksis mhp rapportering og håndtering av hendelser.

9. Risikovurderinger på tjeneste/funksjonsnivå

10. Referansearkitektur for å sette krav til komponenter/delsystemer

11. Referansemodeller for grenseflatene mot andre systemer

12. Sertifisering som en del av kategorisering

13. Myndighetene må sette klarere krav (tre-partssamarbeidet)

6. Konklusjon og forslag til videre arbeid

Målet for seminaret var å:

- Skape oppmerksomhet om informasjonssikkerhet i ulike miljøer (IKT, HMS, automasjon, drift) som er involvert i prosesskontroll- og boresystemer.
- Skape en arena for kunnskapsutveksling og nettverksbygging mellom relevante fag- og forskningsmiljøer
- Identifisere behov for tiltak, herunder forskning og kompetanseutvikling, industri- og myndighetstiltak

Målene med seminaret ble nådd. Gruppearbeidene frambrakte mange interessante synspunkter og vinklinger på IKT-sikkerhet og integrerte operasjoner fra olje&gass-industrien, leverandørbedrifter, kraftbransjen, offentlige etater og forskningsmiljøer.

Referatet gjengir dette i ubearbeidet form.

SINTEF vil nå i samarbeid med OLF lage forslag til konklusjoner og til videre arbeid, Dette kommer i en egen rapport.

APPENDIX

A. 1 Gruppe 1: Kommunikasjonsgap og forskjellig kultur, holdninger og kunnskap mellom IKT, prosess og HMS

Referent: Finn Olav Sveen

Deltakere:
Asbjørn Ueland, BP (prosessleder)
Amund Junge, IRIS
Bjørn Emil Madsen, SINTEF
Eirik Albrechtsen, SINTEF
Thore Langeland, OLF

Innledning

Innledningsvis ble det beskrevet en kultur hvor de forskjellige fagområdene holdt på med sitt og bare i liten grad samarbeidet. Telekom-avdelingen hjalp folk til å snakke sammen, elektro-avdelingen sørget for at ting fungerte og eksperter på pneumatikk og hydraulikk tok seg av boreoperasjoner og lignende. Etter hvert kom det inn noen datafolk som ikke hadde noen lang og stolt ingeniørtradisjon, men som var flinke til å få ting til. Data-avdelingen og telekom-avdelingen fikk senere mer med hverandre å gjøre og er i dag mer eller mindre slått sammen.

Kompleksitet

Redundans, tilgjengelighet på nedstengnings- og produksjonssystemer. Oljedirektør Gunnar Berge nevnte i sin innledende tale at gass er ferskvare. I oljeproduksjon kan man tåle noen dagers, kanskje ukers, stans. Når det gjelder gass så kan man ikke ha stans, i hvert fall ikke lenge, da gassen går direkte i rør til sluttbruker. Det er lite eller ingen mellomlagring.

I 1984, på en ny plattform, ønsket Phillips at all regulering skulle være i eksterne kontrollere. Hvis noe gikk ned, skulle man fortsatt ha kontroll. Man fant ut at i praksis, med over 100 sløyfer, så ble det umulig å ha uavhengige eksterne kontrollere på alt.

Integrerte operasjoner betyr ikke at man ikke kan drive hvis man mister nettforbindelse med land, men det betyr at produktiviteten blir mindre. Man er / blir avhengig av analyse og beslutningsstøtte fra land.

Safety, security og kultur

Det finnes kultur gap mellom mange forskjellige fagområder og enheter ute på plattformene og inne på land. Man skiller gjerne også mellom safety og security, selv om disse etter hvert har mer og mer med hverandre å gjøre.

I BP ble man rammet av Slammer-ormen. Det ble oppdaget at ting skjedde i systemet. Systemet det gjaldt var et drilling-supportsystem. IT-folk reagerte på ormen og var i ferd med å stenge nettverket for å hindre videre spredning. Nettverket ble til slutt ikke

stengt. Hadde det blitt stengt, hadde det ført til titalls-millioner i tap. Blant annet ville boreutstyr ha blitt kjørt fast i brønnen.

Det ble nevnt i gruppen at all drift egentlig er fjernstyring. Man sitter i et kontrollrom og overvåker en prosess som foregår langt nede i havet, eller på andre deler av plattformen. Forskjellen fra land til hav er at på plattformen kan de som jobber ute med vedlikehold, stikke innom og ta en kaffekopp med de som jobber i kontrollrommet. Dette er en fordel, men også ute på plattformene kan det være manglende kommunikasjon. Et eksempel er lang fysisk avstand mellom mekanikernes arbeidssted og kontrollrommet (kontrollrom i boligplattformen slik at man f.eks. må gjennom to plattformer for å komme dit).

Systemkunnskap

Systemene som er i bruk, og brukernes kunnskap om systemene er ikke lenger i synk. Man må i dag ha egne folk på alt. Eksempler er egne folk på spesifikke kontrollere, applikasjoner, osv. Man må ha folk med kompetanse på nettverk, fiber, protokoller, brannmur og kjernekompetanse på Windows/Linux/OS. Ueland sa det slik: ”Det som før var håndterbart for noen få, bare ekspanderer.”

IT og ulykker

Man kan ikke torpedere de skrekkscenarier som blir vist i forbindelse med IT-sikkerhet. Men man vet ikke i hvilken grad de er relevante for ens egne systemer. Det er derfor lett at man ser bort i fra dem. Det blir straks mer relevant når noe skjer med egne systemer.

Kommandolinjer i forbindelse med ulykker er laget for en gitt struktur, en viss nødssituasjon. Disse nødssituasjonene er definert i såkalte DFUer, som alle er fysisk definert. Man burde kanskje definere noen som tar utgangspunkt i IT-sikkerhet.

I dag er det krav om at et anlegg skal ha minst to uavhengige barrierer når det blir bygget.

Man er avhengig av IT for å kunne foreta analyser for å støtte produksjon. Hvis dataene blir kludret med, eller blir endret som følge av feil, vil dette føre til sub-optimal produksjon. I OLF har man foreløpig ikke sett på dataintegritet, men kun på tilgjengelighet.

Tradisjonell IT-sikkerhet og prosesskontroll

Ved en operatørkonsoll er det i praksis ikke aksesskontroll. Man er i prinsippet pålogget hele tiden, man kan ikke stenge ned systemet for å bytte operatør. Selv om man ikke har aksesskontroll til stasjonen, har man aksesskontroll til selve kontrollrommet.

IT-sikkerhets første bud er passord og avstengning av systemene hvis virus kommer inn. Det er mange tilfeller hvor man ikke kan stenge ned prosesskontrollsystemer uten at det koster mye penger.

På sykehus har man oppdaget at leger og sykepleiere ikke har tid til å logge seg inn og ut hele tiden. Førstemann om morgenen logger seg inn og forblir innlogget hele dagen. Dvs., den som logger seg på om morgenen får skylda hvis noe skjer.

Ute på plattformene må mekanikere enkelte ganger huske syv-åtte passord. Disse passordene skal sikre IT-systemene, men mekanikerne skjønner ikke hvorfor. De føler at alle passordene stjeler tid og hindrer dem i å gjøre jobben sin. Manglende informasjon og kulturforskjeller fører til gnisninger.

Det ble nevnt i gruppen at IT-sikkerhetsavdelingen noen ganger sitter og gjemmer seg i en krok. Brukere blir sett på som en trussel i stedet for en ressurs. På plattformene har man tradisjonelt hatt egne IT-folk (ofte telekom-ingeniører). Disse skal nå forholde seg til ”ekspertavdelingen” på land. IT-avdelingene på land er vant til kontormiljøer hvor nedstenging ikke er like kritisk som i prosesskontrollsystemer. Men IT-avdelingene på land er samtidig vant til et tradisjonelt høyere trusselnivå som man har vært forskånet for på plattformene. Med eDrift og integrerte operasjoner vil plattformene bli mer utsatt.

Forskjellige ferdigheter

Et annet problem er at mange veldig dyktige mekanikere ute på plattformene ikke kan skrive pga f eks lese- og skrivevansker. Dette fører til dårlige rapporter om safety-hendelser. Når rapportene er dårlige, blir det også vanskelig å finne ut hva man kan gjøre for å hindre lignende hendelser i fremtiden. Ikke bare kvantitet, men kvalitet på rapportene er viktig. Ledelsen på toppen kan tro at safety er bra, men kulturforskjellen mellom ingeniører som er dyktige til å skrive og mekanikere som ikke er det, fører til dårligere safety.

Forståelse av underliggende arbeidsprosesser

Et annet problem er hvis man ikke forstår underliggende arbeidsprosesser. Ueland fortalte at han aldri lærte seg SAP mens han jobbet på Phillips. Han forsto ikke arbeidsprosessene som ligger bak SAP. Moderne IT-systemer har mange feller i systemene, man skal dobbeltklikke her, men ikke der, osv. Man må kunne veldig mye for å unngå alle fellene.

Mekanikeren som er en god mekaniker, men som ikke behersker og forstår systematikken i arbeidsordresystemet, blir en dårlig arbeidstaker. ”Vi har pasifisert han” (Ueland).

I noen systemer er ambisjonen at de skal kunne brukes til alt. Dette fører til uoversiktlighet og enorm funksjonalitet (f.eks. SAP).

Langeland pekte på dynamikken i forbindelse med ferier. Den siste uka før du skal på ferie så tenker du på at du skal på ferie. Den første uka etter ferien bruker man på å komme i gjenge igjen. Slik har de det hele tiden ute på plattformene pga rotasjonssystemet. Dette er en sikkerhetsrisiko.

Man må kutte ut behovet for å ta snarveier i systemet. Et eksempel er å gjøre internettilgang enkelt ute på plattformen slik at driftssystemer ikke blir brukt til dette.

Kommunikasjon

Mange av problemene grunner i kulturforskjellene mellom hav og land. Dette er et problem som har vært kjent lenge. Kvaliteten på kommunikasjon mellom hav og land blir derfor spesielt viktig. Madsen pekte på tre viktige sider ved kommunikasjon: Hva man skal gjøre, hvordan man skal gjøre det og hvorfor. Hvis kun de to første er til stede og ikke den siste, så vil mekanikeren på plattformen mangle grunnleggende forståelse av prosessen. Manglende forståelse kan f.eks. føre til at man tar snarveier.

Temaer for videre arbeid

Ett gjennomgangstema er større krav om flerferdighet hos hver enkelt arbeidstager, forståelsen mellom hav-land og prosessforståelsen hav-land.

Tema:

- Interessekonflikt eller samarbeid?
- Tiltak for å redusere kommunikasjonsgap

A. 2 Gruppe 2 & 4 Hendelseshåndtering

Referent: Stig Ole Johnsen

Deltakere

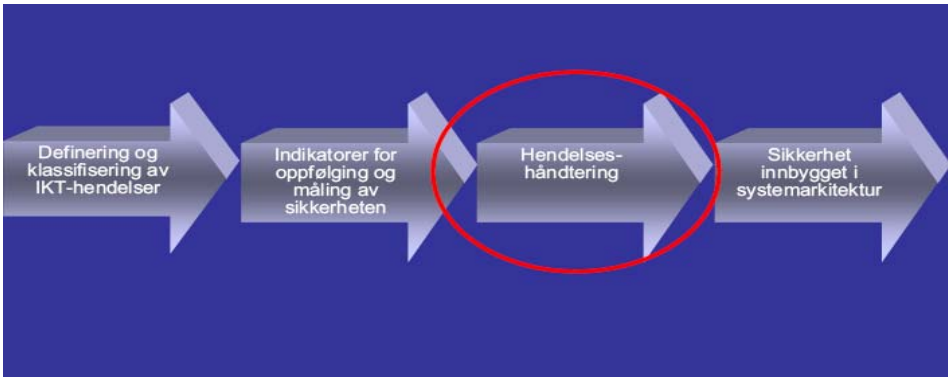
Lars Grøteide, Hydro (prosessleder)
Christophe Birkeland, NorCERT
Jose J. Gonzalez, Høgskolen i Agder
Ellen Hagelsteen, Oljedirektoratet
Maria Kjærland, Universitetet i Stavanger
Einar Oftedal, NorCERT
Arnt Steinbakk, Petroleumstilsynet
Atoosa P-J Thunem, IFE

Innledning

Innledning – fra Lars Grøteide/Hydro som dekket hendelseshåndtering, med punktene:

- Mål for hendelseshåndtering
- Håndtering av de enkelte sikkerhetsbrudd
- Læring av sikkerhetsbrudd for forebygging

Konteksten for hendelseshåndtering er forsøkt beskrevet i Figur 1.



Figur 1: Konteksten for hendelseshåndtering

Mål for hendelseshåndtering er å minimere konsekvenser knyttet til HMS, produksjonstap og økonomiske tap.

Håndtering av de enkelte sikkerhetsbrudd er delt inn i følgende trinn:

- Hva? Hvilke indikasjoner finnes?
- Klassifisering – ut fra kritikalitet og tilgjengelighet, integritet og konfidensialitet
- Løsning er å etablere/komme tilbake til normal situasjon
- Hvorfor skjedde det? Teknisk feil eller brudd på prosedyrer?
- Hvordan kan vi unngå gjentagelse? Forbedringstiltak.

Læring av sikkerhetsbrudd for forebygging er for å gi svar på spørsmålet: Hvordan kan vi unngå gjentagelse? En må da vurdere teknisk løsning, barrierer, endre prosedyrer, personell, kunnskap, holdninger, osv.

Hyppig brukte forkortelser:

- SAS: Sikkerhets- og automasjonssystemer (omfatter prosesstyring og sikkerhetssystemer)
- PCS: Process Control Systems (prosesstyringssystemer)
- SCADA: Supervisory Control and Data Acquisition Systems (begrepet brukes ofte i utlandet, i praksis det samme som PCS og SAS)
- SIS: Sikkerhetsinstrumenterte systemer

Innenfor SAS/PCS/SCADA-systemer innen olje og gass har man kanskje ikke tenkt over at det vil skje uønskede hendelser, men i telekom-industrien er det mer vanlig. Vi kan kanskje lære noe av utviklingen innen telekom?

Diskusjonspunkter

Et godt spørsmål er ”*Hvordan etablere et godt rapporteringssystem for uønskede IKT-hendelser*”.

HMS-avdelingen har gode rutiner for rapportering og oppfølging av uønskede hendelser med HMS-tilsnitt. Oppfølging av hendelser er en utfordring også innen HMS, det er ikke bare IKT som har dette problemet, men HMS har fått etablert gode rutiner. En kan derfor hente erfaringer fra HMS, for å få til læring for rapportering av uønskede IKT-hendelser. Man bør for eksempel løfte rapporteringen av IKT-hendelser til ledelsen, slik som det er gjort med rapportering av HMS-hendelser. En hendelse bør også dokumenters og følges fra A til Å. Man bør se på alvorlighetsgraden av de ulike typer hendelser slik at man får etablert risikoforståelsen av hendelsen. HMS og IKT må også ses på i en sammenheng, da en IKT-hendelse kan få HMS-konsekvenser.

Andre spørsmål som kom opp i diskusjonen var:

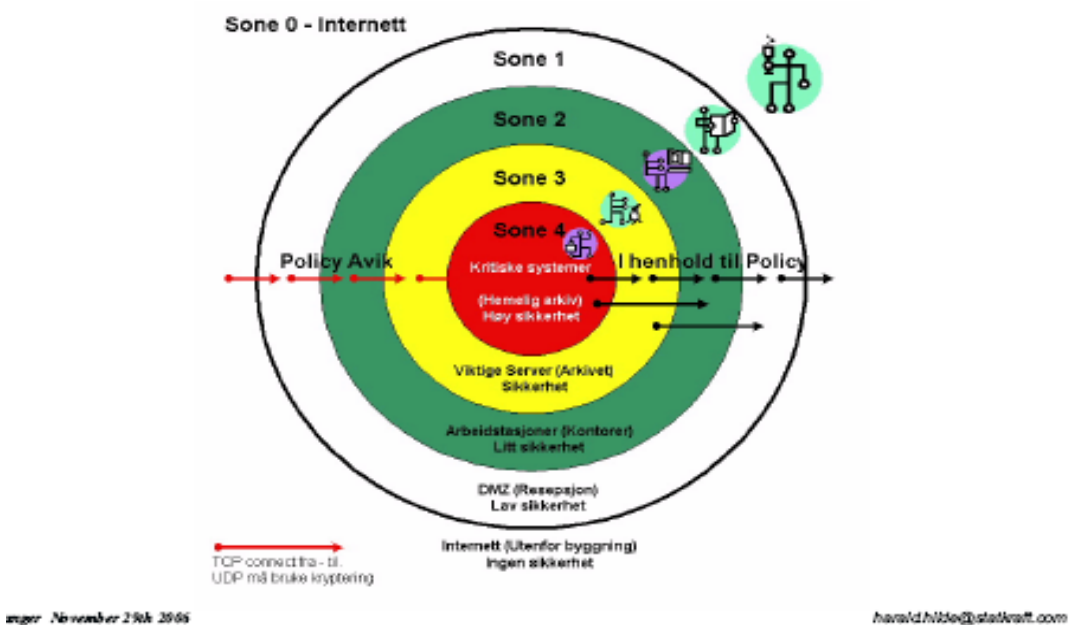
- *Hvorfor rapporteres ikke IKT-hendelser?* Rapporteringssystemene som er laget brukes ikke noe særlig for innrapportering av uønskede IKT-hendelser – hva er grunnen til det? Er det slik at rapportering stjeler tid, eller går det på oppmerksomhet? Oppmerksomheten rundt IKT-hendelser har generelt vært lav innen olje & gass. Statoil sin IKT-hendelse som ble gjennomgått i presentasjonene hos Ptil den 29/11, ble eksempelvis ikke rapportert til Ptil.
- *Hvordan gjøres hendelseshåndteringen?*
    - *Hva er rutinene for varsling?* Er rutinene kjent internt?
    - *Hva skal rapporteres til hvem?* Hvem skal vi involvere i rapporteringen, er det ledelse, er det myndigheter? (Ptil sier de bare trenger å bli involvert i ca 1 % av de viktigste hendelsene.)
    - *Hva er responsen i selskapet etter at en hendelse er rapportert?*

Forberedelse til hendelsesrapportering

En utfordring er at det ofte ikke finnes god beskrivelse av de typer systemer en jobber med, og at det kanskje er det første trinnet som bør på plass.

Det er viktig at hendelser og systemer klassifiseres. Uten klassifisering vet vi ikke hvem vi skal varsle til. I forhold til klassifisering av systemer ble det antydet en klassifisering som ble benyttet fra kraftsektoren, eks Statkraft, se Figur 2, med inndeling i tre grupperinger som grovt sett omfattet:

- 3: SIS – Sikkerhetsinstrumenterte systemer. Svikt kan ha store HMS-konsekvenser.
- 2: SAS/PCS/SCADA – Prosesstyringssystemer. Svikt kan ha økonomiske konsekvenser og mindre HMS-konsekvenser.
- 1: Administrative systemer. Svikt kan ha økonomiske konsekvenser.
- 0: Internett, verden utenfor. Sårbarheter utenfra kan påvirke hvilke hendelser som skjer i de ulike systemene.



Figur 2: Sone-modell fra Statkraft

Det er viktig at vi får til tidlig varsling og likeledes ha god oversikt over hva som historisk har skjedd. Det er viktig å kople hendelser og få fram hvilke systemer hendelsene kommer fra. Nå er det av og til for mye fokus på antall hendelser, ikke på korrelasjon mellom systemer. Vi ønsker å sammenlikne mer komplekse sammenhenger og få fram hvordan hendelser sprer seg via systemene. Vi bør ha en proaktiv holdning til hendelseshåndtering og begynne å se på trender. Det er forhåpentligvis barrierer mellom IKT- og prosessystemene.

Trinn i hendelseshåndteringen

Vi bruker MTO-perspektivet når vi skal analysere og følger trinnene som er nevnt nedenfor:

- 1. Håndtering via linje beredskap (eks plattform), eller 2. Håndtering via beredskap land,

- 3. Håndtering av hendelse via beredskapsorganisasjon,
- 4. Normalisering – komme på plass og reetablere barrierer,
- 5. Gjennomføre granskning,
- 6. Gjennomføre tiltak, tilbakeføring til installasjonen

Systematisering av historiske hendelser kan bidra til tidlig varsling av hendelser. Viktig å spre informasjon internt og eksternt fordi vi ønsker å lære av hva som skjer, vi trenger derfor erfaringsoverføring etter hendelser. 99 % håndteres internt av selskapene.

Det finnes ingen sentrale instanser for hendelseshåndtering som for eksempel et OilCERT – det er i dag rimelig store team internt i oljeselskapene som håndterer uønskede IKT-hendelser. Det synes å være den beste organisasjonsformen på nåværende stadium.

Det som bør etableres før et evt. OilCERT, er å få fram bedre og hyppigere rapportering av uønskede hendelser. I dag mangler vi rapportering.

På sikt bør vi kanskje etablere en eller annen form for OilCERT – kanskje som et nettverk mellom de som har ansvaret i dag i oljeselskapene. På denne måten kan vi finne ut hvilke trusler som skjer i forskjellige typer organisasjoner. Dette fører til at vi kan få til tidlig varsling/linking av hendelser. Et hovedmål for de foreslåtte tiltakene er å få til et tidlig varslingssystem.

Trusselbildet

Det kan være god business i å drive hacking og angrep, det er profesjonelle som driver med dette, dette kan være et område som blir utsatt for mer angrep.

Hvilke trusler har vi i vår organisasjon? Hva slags hendelser kan påvirke vår organisasjon – det finnes mange forskjellige forhold som kan påvirke dette – både tekniske løsninger, organisatoriske valg og kunnskap og holdninger i organisasjonene. Hver enkelt virksomhet må etablere en prosess for å komme fram til de viktige truslene. Noe som kan bidra til dette er innsamling av rapporterte hendelser. Tiltak mht hendelseshåndtering må skje via kategorisering og etablering av standarder på tvers.

Hva er trusselbilde:
- I forhold til integrerte operasjoner?
- I forhold til menneskelig svikt og hvor du har redundans, men svikter?

Hva er utfordringene:
- Hvordan kan man fange opp det som skjer? Må være bevisst på hva som skjer.
- Det er en terskel for å rapportere en unormal hendelse.
- Vet ikke at det var en IKT-hendelse en gang.

Begreper og definisjoner

Begreper og definisjoner brukes forskjellig mellom forskjellige bransjer – derfor viktig å lage tydelige og klare definisjoner. Klassifisering av hendelser er ulik i for

eksempel luftfart og telekom-industrien. Kategoriseringen bør standardiseres slik at vi kan få til erfaringsoverføring på tvers mellom flere bransjer.

Utfordringer ved hendelseshåndtering, samt ved definering og klassifisering av hendelser er relatert til etableringen av strukturer (taksonomier) for rapportering. Klassifisering av hendelser, for eksempel tjenestenekt osv. finnes på ulike nivå (SAS/PCS/SCADA-system, adm. system osv.). Systemer (access points) bør kategoriseres og kobles mot type angrep (methods of operation/tools). Rapporterte hendelser bør kategoriseres m.h.t alvorlighetsgrad (results) ved angrep. CERT har bl.a. laget taksonomier ut fra hendelser som har skjedd.

Risikomodeller

Det finnes mange forskjellige risikomodeller – mange av de ulike modellene kan ikke brukes i den virkelige verden – mange forsøker å modellere feil – eg det vi har kjennskap til, men hvilke trusler er det vi skal se på, dvs det som ikke har skjedd enda. Det finnes ulike risikomodeller for IKT og HMS. FFI jobber med å se på metoder for risikovurdering. Har testet ut forskjellige IKT-caser, men man mangler mye kvalitativt. BAS 5-prosjektet etablerer et rammeverk for risikovurderingsmetodikk, og forsøker også å etablere rammeverk innenfor ulike bransjer. Det er allikevel veldig vanskelig å sammenligne ulike parametere. Det er ulike kulturer og vanskelig å opprette et felles grunnlag. (Bl.a. Stoneburger [2006] ser på integrasjonen mellom HMS og IKT.)

Det har vært fokus på å modellere feil, men det er like viktig (mer viktig) å fokusere på *resilience* (robusthet), hvordan skal vi gå fram for å øke robustheten i systemene.

Hendelseshåndtering og hendelsesrapportering

Hva innebærer en IKT-hendelse i henhold til sikker drift? Hvilke hendelser er det vi prater om – vi jobber på forskjellige steder og dialektene er forskjellige.
I dag er ikke IKT-hendelser så synlige, kanskje er en av de største utfordringene at vi ikke ser dem?

Viktige hendelser kan være uten konsekvenser, men det er viktig at de blir rapportert. Vi ønsker å oppnå en erfaringsoverføring ved rapportering av hendelser. Vi må registrere alvorlighetsgrad i forhold til hendelser, eksempelvis hva hendelsene innebærer i forhold til drift. Viktig spørsmål er å avgjøre hva som er alvorlig. Flom av lavt prioriterte hendelser kan være et problem. Hendelser må bli grovkategorisert for å luke bort noe. Videre må man utvikle verktøy og tekniske løsninger for automatisk håndtering av høy-volums hendelser.

De som rapportere flest hendelser, er de som har flest og best rutiner for sikkerhetsrapportering. Gode systemer gjør at rapporteringen går opp, men at antall alvorlige hendelser går ned. Det viser seg at de som rapporterer til CERT, er de som er best på sikkerhet og er mer bevisste.

Dette dokumenteres for HMS i bl. a. [Jones 1999 og Kjellén 2000], Bjerke og Kjellén jobber hos Hydro, og Kjellén er dessuten professor II ved Institutt for industriell økonomi, NTNU.

Ingar Smedstad, jobber hos Hydro (Sandsli) og tar mastergraden i informasjonssikkerhet ved Høgskolen i Gjøvik. Han jobber med rapportering av informasjonssikkerhetshendelser (J. Gonzales er veileder og Finn Olav Sveen er medveileder). Svein Egil Sakariassen har gitt Ingar Smedstad aksess til Synergi – foreløpig lite av interesse der angående informasjonssikkerhet. Men det åpner seg for spennende muligheter tatt i betraktning at arbeidsseminaret flagget betydningen av denne problemstillingen. Dessuten ser Hydro tydeligvis problemstillingen som viktig. Hydro har jo en meget sterk stilling når det gjelder HMS takket være gode rapporteringssystemer – why not do the same in infosec?

J. Gonzalez henviste til nødvendigheten av å integrere sikkerhet med den totale kvalitetsforbedringen i organisasjonen, ref paper i SAFECOMP'2005 om rapportering av sikkerhetshendelser [Gonzalez 2005] og sammenhengen med kvalitetsforbedring. Repenning og Sterman (2001) er også en god referanse.

Etablering av gode holdninger – "Reporting Culture"

Eksempel på hvordan holdninger skapes, er "en ansatt sendte en viktig (konfidensiell) rapport til en konkurrent ved en feil. Vedkommende ble straffet for dette – men hva skjer neste gang en slik hendelse opptrer - vil han eller de som kjenner til straffen rapportere neste gang?"

Konklusjoner – Forslag til oppgaver for Gruppearbeid II

1-Hvordan få til rapportering/varsling av uønskede IKT hendelser?

- Eks opplæring, kompetanseheving. Ikke nok kompetanse der ute til å håndtere hendelser.
- Hvordan få til et godt rapporteringssystem som integreres mot HMS? Vi trenger å beskrive hendelsen, og etablere et godt rapporteringssystem.
- Få fram viktig rapportering, få bort flom av uviktig rapportering. Vær konkret på hvilken påvirking en IKT-hendelse har på resten av systemet. Vi må kjenne konsekvenser av hendelsene. Er det sammenhengen mellom IKT-hendelser og HMS-hendelser – er det det som er viktig?
- Hydro tar i bruk Synergi til rapportering av uønskede IKT-hendelser. Kanskje ikke Synergi passer til rapportering. Ingar Smestad/Hydro vil jobbe med dette. Noen mener dette systemet ikke passer for å håndtere IKT-hendelser og bruker det ikke.

2-Kategorisering av systemer – struktur, metodikker

3-Risikomodellering – Proaktive modeller

A. 3. Gruppe 3: Indikatorer

Referent: Odd Helge Longva

Deltakere

Rune Ask, DNV (Prosessleder)
Janne Hagen, Høgskolen i Gjøvik/FFI
Åge Torkildseng, SKS
Grete Løland, Petroleumstilsynet
Tor Aalborg, Statnett

Innledning

Presentasjon av deltakerne. De har bakgrunn fra kraft, olje og forskning.
Rune Ask innledet med å vise til

- at det er vanskelig å måle informasjonssikkerhet, det er mange ulike synspunkter.
- arbeidet i OLF sin arbeidsgruppe for informasjonssikkerhet (AGI) hvor et av målene er å finne fram til indikatorer. I en rapport til OLF/AGI er det foreslått seks indikatorer (KPI). Dette blir det arbeidet videre med.
- et annet tiltak i OLF/AGI for å måle informasjonssikkerhet, et ”Self Assessment” skjema. I dette stilles det 160 spørsmål med valg mellom ulike svar.
- at han deltar i ISO sitt arbeid med å lage en standard for måling av informasjonssikkerhet. Dette er teknisk fokusert.

Han påpekte ellers at han i sitt arbeid med informasjonssikkerhet i oljesektoren opplevde at det var svak ledelsesforankring, svake prosesser, mangel på risikovurderinger og på katastrofeplanlegging.

Etter denne salven startet en livlig meningsutveksling i gruppen.

Diskusjonspunkter

Målsetting

Spørsmålet var: Hva er formålet med indikatorer, hva skal de brukes til?
Momenter fra diskusjonen:

- Sett fra bedriftens side er målet bedre informasjonssikkerhet og gjennom det bedre økonomi
- Brukes som mål for om informasjonssikkerheten er i samsvar med den policy og de rammer som er satt
- Brukes til å forbedre informasjonssikkerheten og å integrere den inn i forretningspraksis
- Brukes for å måle virkningene av tiltak for å forbedre informasjonssikkerheten
- Brukes for å kunne dokumentere overfor tilsyn at informasjonssikkerheten er i samsvar med lover og regler
- Det er viktig å kople samordne arbeid med informasjonssikkerhet og med HMS. Riktig valg av indikatorer kan bidra til dette

Måling

Momenter fra diskusjonen:

- Vi ønsker å måle i forhold til en baseline/referanse, for eks OLF sin ISBR
- Indikatorene skal brukes i risikovurdering
    - sikkert nok
    - risiko = sannsynlighet x sårbarhet
- Hva slags indikatorer skal vi bruke for å måle virkningene av tiltak i forhold til baseline?
- I USA arbeides det med ”Baseline for security in SCADA”. ISA SP99 er i gang med en standard for "Manufacturing and Control Systems Security". "Part1: Concepts, Models and Terminology" er ferdig. "Part 2: Establishing a Manufacturing and Control System Security Program" er i sluttfasen. Dessuten finnes NIST SP 800-53 og arbeid med "Applying NIST SP 800-53 to Industrial Control Systems". Baseline definisjoner er sentrale i dokumentene.
- Hva slags indikatorer skal vi bruke for å måle avvik i forhold til policy?
- Innenfor kraftsektoren er det arbeidet med gapanalyse. Man har sett etter verktøy i markedet. To verktøy tas i bruk:
    - ”Self assessment” skjema
    - Direkte målinger fra SCADA som oppetider/nedetider

  Det sjekkes for
    - akseptabelt nivå
    - Hvor i prosessen var hendelsen
- En viktig indikator er mål for konsekvensene av brudd på informasjonssikkerheten
- Innen oljesektoren og kraftsektoren må det tas hensyn til både bedriftsmessige og samfunnsmessige forhold. Valg av indikatorer må avspeile dette.
- Hvor går balansen mellom å foreta ”safe shutdown” og å opprettholde produksjon?
- Ved risikovurderinger hvordan skal vi se på hendelser med store konsekvenser men med liten sannsynlighet kontra hendelser med små konsekvenser og med stor sannsynlighet? Vi kan ikke uten videre bruke statistikk, vi må legge mer ressurser i å gardere oss mot katastrofer
- Det legges alt for liten vekt på verdisetting av ”assets”
- Trenger vi egne indikatorer for SCADA? Skal vi skille mellom prosess og administrative funksjoner?
- Krav fra revisjon og tilsyn krever spesielle indikatorer

Det var delte meninger om bruk av ordet ”indikatorer”.

- Det kopler direkte til det i mange sammenhenger mye brukte ”key performance indicator”.
- Ordet ”måleparametre” er bedre på norsk

Konklusjoner – Forslag til oppgaver for Gruppearbeid II

- Videre arbeid med ”Self Assessment ” for sikkerhet i SCADA og måling av sikkerhetsbevissthet
- Bygge erfaringsdatabaser ved direkte tekniske målinger på SCADA-systemer, eks. oppetider/nedetider/responstider ved sikkerhetsbrudd.

- Indikator/måleparameter på konsekvenser av sikkerhetsbrudd i SCADA-systemer

A. 4. Gruppe 5: Sikkerhet innbygget i systemarkitektur

Referent: Martin Gilje Jaatun

Deltakere

Lars Bratthall, DNV (prosessleder)

John Aurlien, ConocoPhillips
Eivind Hage, Siemens
Bård Hauger, ABB
Kjell Arne Høyvik, Siemens
Ingve Guttorm Lode, BP
Siri Lunde, Petroleumstilsynet
Robert Malmgren, Robert Malmgren AB
Arnt Methi, Siemens
Ken Møller, Statoil
Øivind Rui, Kongsberg Maritime
Stephen Wolthusen, Høgskolen i Gjøvik

Innledning

Vi trenger å finne et ”felles multiplum” med hensyn til hvilke tiltak som skal iverksettes. Arkitektur og informasjonssikkerhet er ikke ”core business”, verken for leverandører eller operatører.

Det introduseres stadig nye løsninger i olje/gass, men det er lang turnover – prosesskontrollutstyr har gjerne en levetid opp mot 30 år.

Bare det å finne alle tekniske systemer på en installasjon er en utfordring (ikke alle er tegnet inn). Det burde vært en segmentering av nettverkene slik at man kan skille det som er ”business critical” fra alt annet. Det er i dag akseptert at man har behov for fjernaksess fra land, men sikkerhetssystemene er ikke der hvor man burde starte. Det er fortsatt lite investering i sikring – operatøren må tåle å betale for sikkerhet. Er sertifisering av utstyr og produkter veien å gå?

Det er lang levetid på prosesskontrollutstyr – kan ikke vente med å skifte ut ting ved ”naturlig avgang”. ConocoPhillips har dokumentert god praksis på dette området.

Genesis-prosjektet fra BP har bidratt til segregering og sikring av prosesskontrollssystemer. Det er viktig å sikre nett for tilgjengelighet, og å ha de nødvendige barrierer. Hvis programvarebaserte systemer svikter, skal det være en ”fysisk knapp” (på land) for å slå av det hele – er det mulig?

I kraftsektoren forholder man seg ikke til én leverandør. Tradisjonelt har man operert med isolerte nettverk, men disse åpnes nå; man har i stor grad informasjonsflyt mellom kontorsystemer og prosesskontrollsystemer. Kraftverkene har drevet og kjøpt hverandre opp, med en rekke ”multi-site” operasjoner som resultat.

Hvor skal vi – hvor er kravene – hvor er målene? Det viktigste er å begynne i det små.

Leverandører og operatører trenger felles kriterier for evaluering av komponenter og systemer – kan Common Criteria (ISO/IEC 15408 [26]) være et utgangspunkt?

Det er mye fornuftig i Common Criteria, men det er lite sannsynlig at vi vil se CC-evaulerte (for ikke å si sertifiserte) systemer [27] i prosessindustrien med det første.

Diskusjonspunkter

Hvordan kan man sikre at produkter fra Microsoft ikke påvirker sikkerheten negativ? Oljeselskapene må stille kravene!

Hvorfor ønsker vi egentlig at prosesskontrollsystemene skal ha kontakt med ”den store verden”?

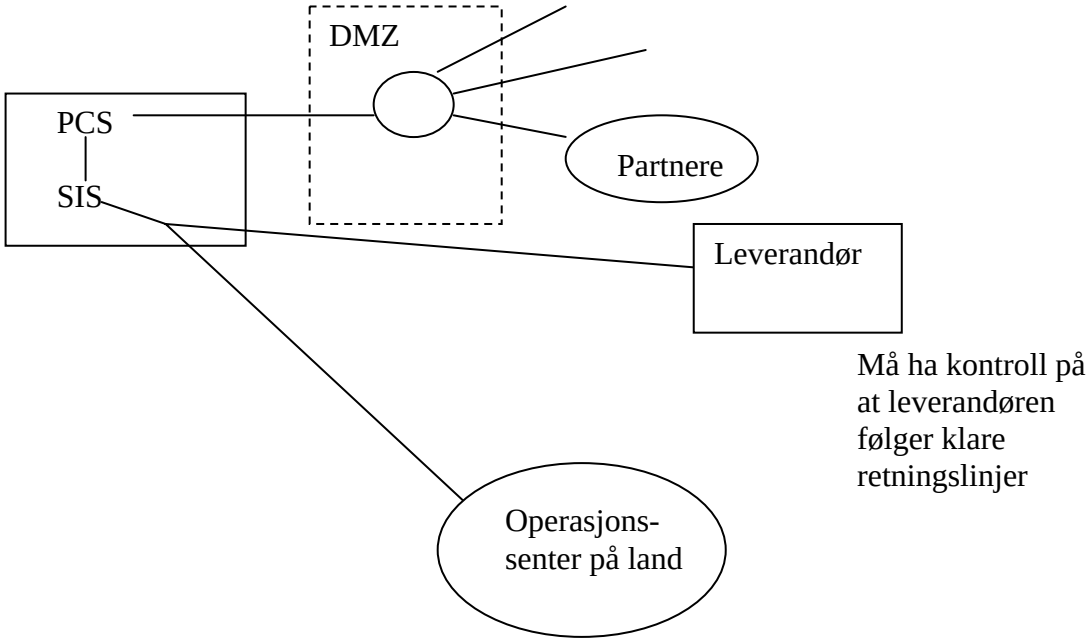
- Det er behov for sanntidsdata, bl.a. for å foreta optimalisering
- Fjernvedlikehold

Hvor mye kan man oppnå ved bruk av monitorering utenom sikkerhetssystemet? Er det mulig å skille prosesskontrollsystemene fra sikkerhetssystemene?

Hva *er* egentlig IO?

Et konkret eksempel på hvorfor man trenger kommunikasjon ut: ConocoPhillips (COP) får sanntidsdata under boring fra nedihullsinstrumentering som går til Halliburtons server i COP’s nett. Disse dataene må koordineres/kalibreres mot solobservatorium som ligger i forskjellige verdensdeler avhengig av tid på døgnet.

Må ta kommunikasjonsbehov case for case; hva trenger man i hvert enkelt tilfelle? Ukentlige møter hvor nye behov kan avklares og forhandles.



Figur 3: Skisse for å illustrere sikkerhetsutfordringer i IO

Mange operatører er ikke klare til å slippe eksterne aktører inn i ”det aller helligste”. Er det mulig å redusere usikkerheten ved en slags sertifisering av tjenester og leverandører? En løsning kan være å implementere en slags ”applikasjons-proxy” på

terminalserver i DMZ, der hver oppgave som leverandører/samarbeidspartnere skal få lov til å utføre i prosesskontrollsystemet defineres enkeltvis. Det vil da være mulig å gi tidsbegrenset adgang til å utføre oppgaven via fjernaksess. Disse ”proxyene” vil kunne evalueres/sertifiseres etter nærmere bestemte kriterier av kvalifiserte uavhengige tredjeparter (som det finnes flere av i Norge). F.eks. DNV har lang tradisjon for å foreta ”Teknologikvalifiseringsprosesser”.

Det pussige er at IO-diskusjonen later til å være en reprise av diskusjonen rundt militære nettverk for 20 år siden. I det militæret har svaret vært såkalte ”guard systems”, som har vært utviklet spesielt med hensyn på å kunne evalueres/sertifiseres etter formelle kriterier som TCSEC (og nå CC [26]).

Hvis samfunnet trenger noe, vil det bli et marked for dette. Utfordringen er eventuelt å få samfunnet til å skjønne at det trenger akkurat dette...

Den mest trivielle sensor inneholder i dag ti-tusenvis av linjer med kode. For å ta Siemens Mobile som et eksempel, hadde de direkte kontakt med hundrevis av underleverandører i forbindelse med fremstilling av sine mobiltelefoner.

For å øke sikkerheten i forbindelse med IO, må man både redusere risikoen for at en inntrenging finner sted, samt redusere virkningen av de inntrengingene som slipper gjennom forsvarsverkene. Samtidig må vi ikke glemme at IO også handler om å redusere kostnader – hvis man stiller så store sikkerhetskrav at tiltakene totalt sett blir for dyre, er man dømt til å mislykkes. På den annen side burde man kunne bake inn kostnader til IT-sikkerhet i begrepet ”the cost of doing business” – det er i dag ingen krav til IT-sikkerhet på samme måte som det er krav til HMS.

Slik sett burde Ptil være ”eier” av en standard, gjerne med flere nivåer eller ”stigetrinn” som aktørene kan forholder seg til (Ptil presiserer at de ikke lager slike standarder selv, så det er opp til næringen å ta et initiativ i denne sammenhengen). Problemet er at spesifikke krav i regelverk fort blir statiske; ved å fokusere på funksjonelle krav er det lettere å unngå at regelverket hindrer teknologiutvikling.

Det er viktig å ha kontroll på konfigurasjonsverktøy. Hensyn til HMS krever at vi alltid går til en sikker tilstand ved feil; dette omfatter også inntrenging. I teorien kan en inntrenger gjøre en mengde skade uten å bli oppdaget; dette inkluderer ting som å slå av sikkerhetskopiering, endre passord, mm. Også de lavere nivåer kan være sårbare for angrep, eksempelvis kan radiolinjeforbindelser slås av via fjernbetjening; dette vil ha konsekvenser for prosesskontrollsystemene.

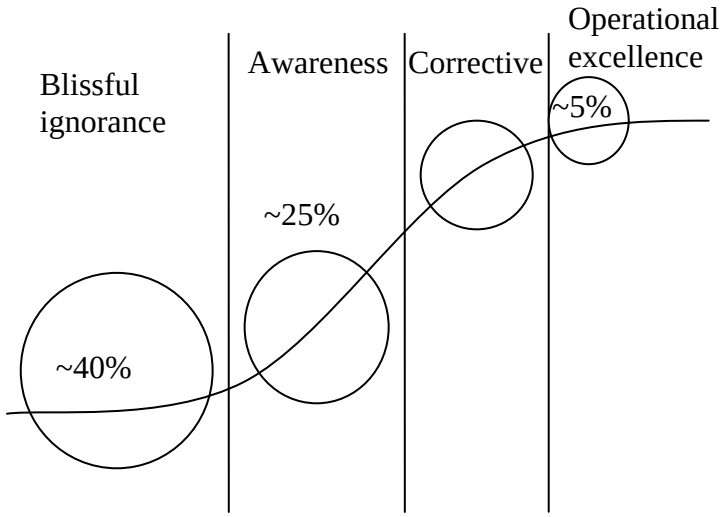
Risikoanalyse blir en utfordring, ingen har full oversikt eller kontroll med alle ledd, til syvende og sist blir det et organisasjonsspørsmål.

En typisk situasjon er at man har brannmurer etc. offshore, mens ressursgruppa som har den nødvendige kompetansen sitter på land. Hva skjer hvis man da f.eks. får et tilfelle av ”network flooding”? Tilsvarende problemstillinger vil være aktuelle ved outsourcing av IT drift. Det primære må være at man ikke må være avhengig av ekstern infrastruktur for å komme til ”sikker tilstand”.

Bransjen burde kanskje først bli enige om hvilken utvikling man *ikke* vil ha.

Det er betalingsviljen hos operatører som avgjør hva leverandørene satser på. I dag er det mest fokus på ”safe state”. En stopp kan fort koste 70 millioner; det burde derfor være god økonomi i å innføre tiltak mot informasjonssikkerhetstrusler som kan medføre stopp (men hvordan identifiserer man disse...?).

Det er et veldig fokus på HMS, i den grad at man har sett proaktiv stenging av komponenter som har feilet hos andre operatører. ”Management” tenker imidlertid ikke IT-sikkerhet. Hva slags argumentasjon, dokumentasjon eller ”beviser” trenger en operatør for å bruke 35 millioner på (f.eks.) IT-sikkerhet? Mye tyder på at forskrifter, pålegg e.l. er nødvendig – utsagn av typen ”vi IT-folk tror at dette kan komme til å bli et problem” holder i hvert fall ikke. Generelt kan man si at sikkerhetsfolkene ikke er tilstrekkelig på banen i driftsorganisasjoner.

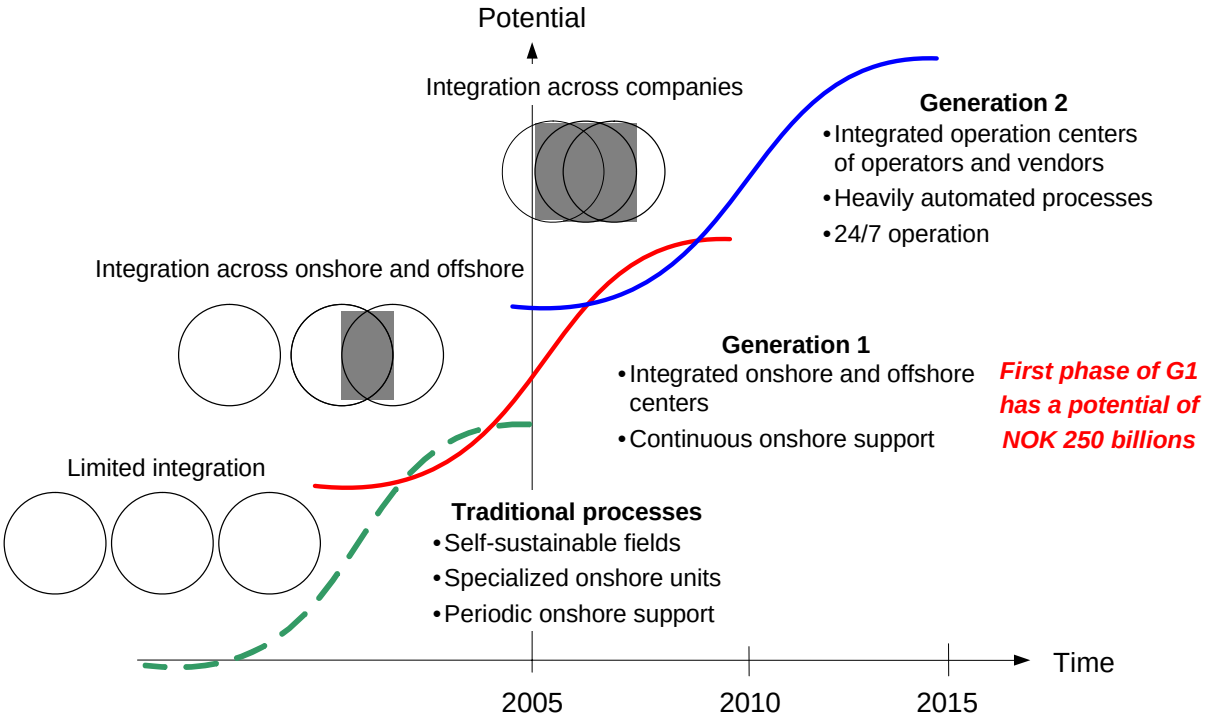


Figur 4: Kunnskap om IT-sikkerhet fra studie av Gartner Group

En undersøkelse utført av Gartner Group blant deres 2000 største kunder [28] (se Figur 4) bekrefter at IT-sikkerhet er et altfor abstrakt begrep for flertallet av beslutningstagere. Til og med i tilfeller der man får gjennomslag for sikkerhetsargumenter går det ofte galt: Man gir for mye gass, svir av masse penger, og bommer på målet. I verste fall ender det med at sikkerheten oppfattes som en hemsko av brukerne (”... folk får ikke gjort jobben sin på grunn av den #♈☠💣☹👎!! brannmuren”).

I en virksomhet følger man vanligvis gangen ”økonomi → funksjonalitet → sikkerhet”. Sikkerhet er (eller burde være) en ”enabler”.

Hva må bransjen gjøre nå? Det går ikke an å bare sitte og vente, vi må ha en felles standard for bransjen. Vi må finne ut hva som faktisk er i bruk i dag (generasjon 1), og bestemme hva vi må ta i bruk for å komme til nivå 2 (generasjon 2 – se Figur 5).

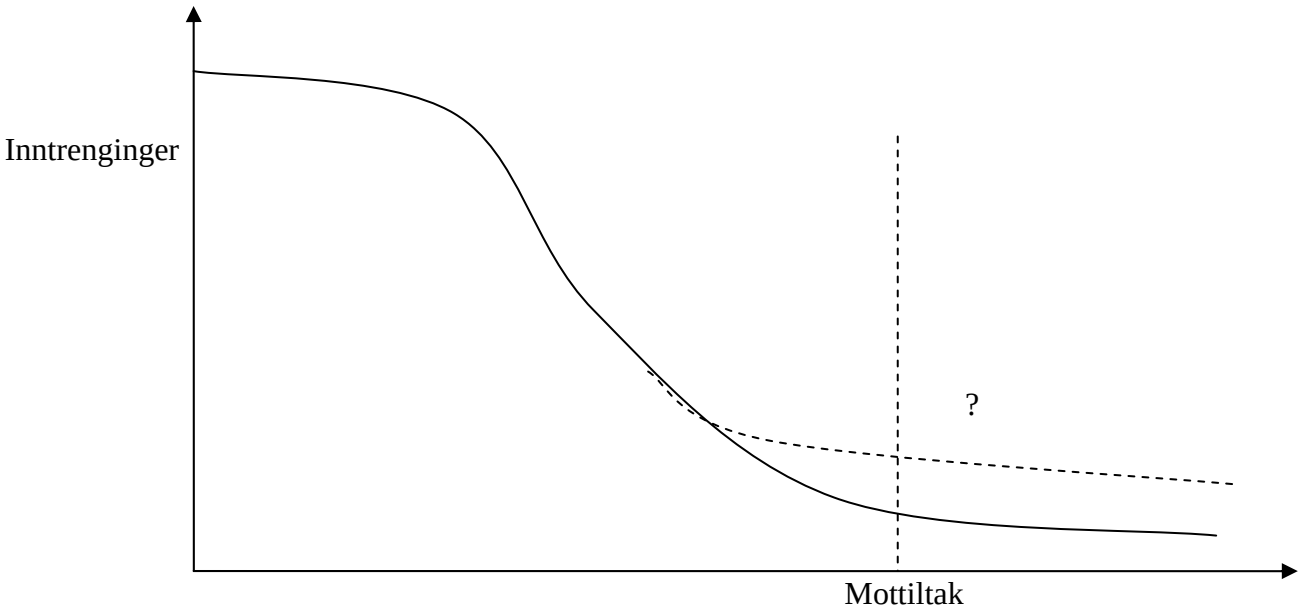


Figur 5: OLF's IO-visjon

Det er ting som tyder på at det proprietære kommer til å forsvinne på sokkelen (vi ser dette allerede, med stort innslag av produkter fra Microsoft). Dette betyr at ”noen” må gå foran for å *lage* en standard protokoll/applikasjon.

Vi må kanskje se på SIL [29] vs. sikkerhet – et innledende arbeid på dette feltet gjøres i prosjektet ”Secure Safety” som drives av SINTEF på oppdrag fra PDS-forum [30] og Forskningsrådet.

Til slutt var vi inne på en variant av problemstillingen ”the long tail” – security-hendelser er (i motsetning til safety-hendelser) ikke fordelt i henhold til en håndterbar statistisk modell. Dette betyr at vi i mye mindre grad kan si noe sikkert om effekten av tiltakene, eller om det vi beskytter oss mot faktisk kommer til å inntreffe.



Figur 6: Hva er egentlig effekten av sikkerhetstiltak?

Konklusjoner – Forslag til oppgaver for Gruppearbeid II

Følgende to tema ble foreslått til den neste gruppe-sesjonen:

- How to handle legacy systems and migration path
- Hva skal til for å nå fase 2 i IO?

A. 5 Gruppe 6: Sikkerhet ved informasjonsdeling i nett

Referent: Inger Anne Tøndel

Deltakere

Chunming Rong, UiS (prosessleder)
Kjell Olav Nystuen, FFI
Eirik Time, Statoil
Torunn Øvreås, FFI
Turid Øygard, Oljedirektoratet
Christophe Birkeland, NorCERT

Innledning

Innledningen tok for seg overordnet hvordan teknologi for semantisk web kan øke informasjonsdeling ved integrerte operasjoner, og gav en introduksjon til sikkerhetsstandarder for web services. Det ble blant annet pekt på hvordan utarbeidelse av en sikkerhetsontologi er et viktig utgangspunkt for å lage et rammeverk for sikkerhet i integrerte operasjoner. Det ble foreslått to tiltak for videre arbeid:

- Integrering av webtjenester-sikkerhetsstandarder i en overordnet systemarkitektur
- Utarbeidelse av en felles tillitsarkitektur

Diskusjoner

Syn på semantisk web

Kunnskapen om semantisk web var forskjellig blant deltakerne, og der noen hadde klokketro på at dette er fremtiden og løsningen på mange av problemene man står overfor, var andre mer forsiktige tilhengere. Det var imidlertid enighet om at semantisk web er i tiden, og har potensial innen integrerte operasoner:

- Kan lette informasjonsdeling – også mellom ulike selskaper
- Kan åpne for mer automatisk kontroll av informasjonssikkerhet

Det var noe diskusjon rundt hvordan en diskusjon rundt semantisk web bør starte – om man bør starte med teknologien og standardene, eller om man bør starte mer på den operative siden og se på behovene og hvilken informasjon som skal deles ved hjelp av teknologi for semantisk web.

Det var noe uklarhet rundt forholdet mellom semantisk web, web services og tjenesteorienterte arkitekturer (SOA). Hovedsynet var at dette er begreper som henger sammen og i stor grad blir/vil bli brukt om hverandre.

Hva en sikkerhetsontologi er og hvordan den kan brukes var også uklart for mange av deltakerne. Det ble utdypet at en ontologi ikke er et entydig regelsett, men en beskrivelse av hvordan man kan snakke sammen. Dette innebærer en definisjon av begreper og forholdet mellom dem. Hvert selskap kan definere sin egen ontologi, men for at tjenestene skal kunne snakke sammen på tvers av selskaper trenger man noe felles. Man kan se for seg en plug-in i hver enhet/tjeneste som konverterer

informasjon til et felles språk slik at man kan snakke sammen. Slik vil bruk av semantisk web ikke være det samme som å kaste gamle løsninger på båten, men legge til rette for at disse kan snakke sammen og dele informasjon. Når det gjelder sikkerhetsontologi kan en slik gjøre det lettere å håndheve policies automatisk i systemet. Målet er å gjøre det mulig å kjøre systemer uten at mennesker skal trenge å gripe inn (autopilot).

Migrasjon

Systemene i dag er komplekse, og det er lett å miste oversikten. God sikkerhet handler ofte om god oversiktlighet. Systemene er allerede uoversiktlige, og det er mange kanaler og koblinger. Nye ting vil løse noe. For eksempel så er det et problem med løsningene slik de er i dag er at leverandører ofte må ”skifte språk” på hver kontakt. Men nye løsninger klarer ikke å løse alt. Disse problemstillinger blir ofte borte i jakten på ”superløsningen”.

Det ble foreslått å bruke pilotprosjekter for å redusere problemer relatert til migrasjon.

Viktigheten av tillit
Når man nå i større grad skal koble sammen systemer slik at de kan snakke sammen vil tillit være vesentlig. Man snakker her om selskaper som kan være i sterk konkurranse med hverandre. Man trenger også å ha tillit til sikkerheten i systemene. Dette kan gjøres med avtaler på høyere nivå. En annen mulighet er i større grad å gå over til å bruke sertifisering som virkemiddel – for eksempel sertifisering av SCADA-produkter. Enda en mulighet er å bruke kode som er signert slik at man kan kjøre integritetssjekker.

Sikkerhetsutfordringer

Det ble påpekt at selv om semantisk web har mye for seg når det gjelder å få til bedre informasjonsdeling – noe som er viktig – er det ikke nødvendigvis slik at semantisk web er noe som vil løse sikkerhetsproblemer. Dette er ny teknologi for mange, og det blir viktig å tenke sikkerhet og risikostyring fra starten. En risiko som ble trukket frem var leverandører som leverer systemer som støtter ontologien, men uten at systemene er designet med god sikkerhet. Økt konnektivitet og det at systemene snakker samme språk kan gi økte/nye sikkerhetsutfordringer som må tas hensyn til. Det blir kanskje enda viktigere for de som kjøper software å ha tillit til systemutviklingsprosessen. Det ble trukket frem et eksempel der systemene ved et sykehus ble infisert av en orm. Dette førte blant annet til at dørlåssystemer og callinger ikke fungerte, og at datasystemer på akutten gikk ned. Infeksjonen fikk så store utslag siden systemene var koblet sammen.

For å vurdere sikkerheten – og hvilken sikkerhet som er nødvendig – er det viktig å vite noe om hvilken informasjon vi her snakker om å dele (sikkerhetsnivå på informasjonen) og hvem man skal dele med. Man må også vurdere hvordan man skal styre tilgang, og hvem som skal få tilgang til hva. Spesielt vil dette være viktig når man har konkurrerende leverandører inne i bildet. Man må fokusere på applikasjonen – hva som skal bruke XML-skjemaene – og det blir viktig med sikkerhet ute i enkeltkomponentene. Man må starte fra bunnen i sikkerhetskjeden slik at man får sikkerhet i alle ledd. Det er ikke nok med for eksempel tofaktorautentisering dersom det er store mangler ved sikkerheten andre steder. En stor utfordring er å vise at sikkerhet er kostnadseffektivt.

Et viktig punkt som ble diskutert var sikkerheten mellom produksjonsnett og administrativt nett i en løsning der man bruker teknologi for semantisk nett. Mange uttrykte at man, i alle fall ikke på kort sikt, kan se for seg å benytte teknologi for semantisk web på installasjoner pga sårbarheter i SCADA (spesielt gjelder dette gamle installasjoner). Disse systemene må isoleres. Data kan imidlertid pumpes inn på land og bearbeides der. På lengre sikt, etterhvert som man får bedre sikkerhet i slike systemer, kan det imidlertid bli aktuelt. Det blir viktig å se på forholdet mellom teknisk nett og det nettet der man bruker standardene. Integrering av administrativt og teknisk nett er farlig, men nødvendig. Man må intensivere sikkerhetsmekanismer i punktet der nettene må snakke sammen, og implementere barrierer og lagdeling.

Utfordringer med å få til felles løsninger
Det er en utfordring å bli enige om en standard slik at organisasjoner kan snakke sammen. Det ble diskutert om myndigheter kan ha en rolle med å stille krav. Dette ble sett på som vanskelig siden man her snakker om et internasjonalt marked med store internasjonale selskaper. Ontologi på nasjonalt nivå vil ikke fungere. Store aktører foretrekker ofte egne proprietære systemer, fordi det er dette de tjener mest penger på. OLF kan ha en rolle når det gjelder å gi råd, men kan ikke gjennomføre.

Det ble også uttrykt at det ville vært fint å bli enige om et felles sikkerhetsnivå i industrien. Det er vanskelig, men ville vært supert å få til.

Forslag til tiltak (i tillegg til det som ble foreslått i introduksjonen)
Etablering av en felles autentiseringsløsning slik at man kan gjenbruke autentisering gjort i et annet selskap. Det er vanskelig for et selskap å vedlikeholde informasjon for å kunne autentisere andre selskapers ansatte. Det ble foreslått å se på en løsning med en felles autentiseringshub.

Definere løsninger for kritiske punkter mellom produksjonsnett og administrativt nett.

B. 1 Tema 4: Kommunikasjonsgap

(Det ble ikke skrevet fullt referat fra denne gruppen, men Eirik Albrechtsen noterte stikkordene under)

Deltakere

Asbjørn Ueland, BP (Prosessleder)
Eirik Albrechtsen, SINTEF
Amund Junge, IRIS
Grete Løland, Petroleumstilsynet
Bjørn Emil Madsen, SINTEF
Turid Øygard, Oljedirektoratet

Diskusjon

- unngå de dumme feilene
- Skille IKT-systemer fra hverandre
- Robuste systemer/skall designet ift brukerbehov og – kompetanse
- Finne kompetansekrav for å unngå at den enkelte er en IKT-trussel
- Oppgradere IT-folk til å forstå bruker-perspektivet, betingelser og konsekvenser i ”den virkelige verden”
- Alle må få større forståelse for kompleksiteten i virksomheten
- Alle trenger større helhetsforståelse/ unngå parallell sub-optimalisering
- Anerkjennelse av at fler-/tverrfaglighet er kompetanse
- Det må trenes og folk må møtes sosialt for å bygge tillit – trene på kommunikasjon mellom 1) typer mennesker og 2) fag/profesjoner/roller
- Sentralt i all type læring og kommunikasjon: hva forventes, hvordan skal det gjøres og hvorfor. Når det gjelder IT, synes det som om hvorfor-biten har falt helt ut.

B. 2 Tema 8: Legacy systems

Referent: Martin Gilje Jaatun

Deltakere

Lars Bratthall, DNV (prosessleder)
Eivind Hage, Siemens
Ingve Guttorm Lode, BP
Robert Malmgren, Robert Malmgren AB
Arnt Methi, Siemens
Ken Møller, Statoil
Kjell Olav Nystuen, FFI
Torunn Øvreås, FFI

Diskusjon

Problemstilling – angrepsmåte

- Komponenter, hva kan endres
  Dekomponering av problemet
- SIS, ISO/IEC 61508[28], HAZOP, risiko
  Oversikt over systemer, arkitekturer: Hva har vi i dag?
  SIL-krav vs. oppetids-krav
  Må ha kontroll på konfigureringsverktøyene
  PCS og ”andre store grupper av systemer”
- Tjenestene du forventer fra systemene vil utvikle seg over tid
  - Trenger nye systemer
- ”Architectual erosion”
- I dag: Lappeteppe med oppgraderinger over en lav sko
- Variantbegrensning
- ”Vi skal over på IP” – uten å vurdere sikkerhet
  Mangler det helhetlige bildet
- Trenger et veikart
  Grunnen til overgang er ”end of lifecycle” for det aktuelle utstyret, f.eks. kondensatorer tørker ut, ikke lenger mulig å få tak i reservedeler.

Målet er ”Dependable integration”, som vi kan oversette som pålitelig integrasjon, eller integrasjon uten at ting rakner.

Tekniske utfordringer

”Business/mission critical”
Dvs: Hva er det som gjør (eller forhindrer) at vi tjener penger?

SIS → HMS
PCS → Business high
PCS → Business low
} Må skille disse!

Arbeidsprosesser

”Architectural impact across organizations”
Dvs: Innvirkning på arkitektur på tvers av organisasjoner
Trenger en felles måte å evaluere leverandører med hensyn til

- Arbeidsprosesser
- Teknologi/infrastruktur
- Produkter

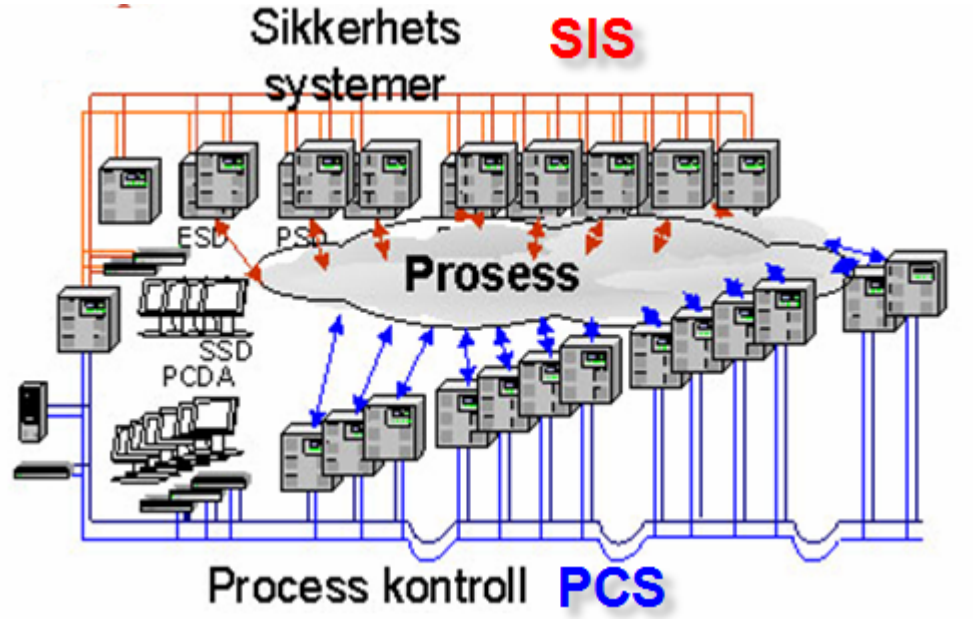
Revisjon

Organisasjon, kultur

Bevissthet (awareness)

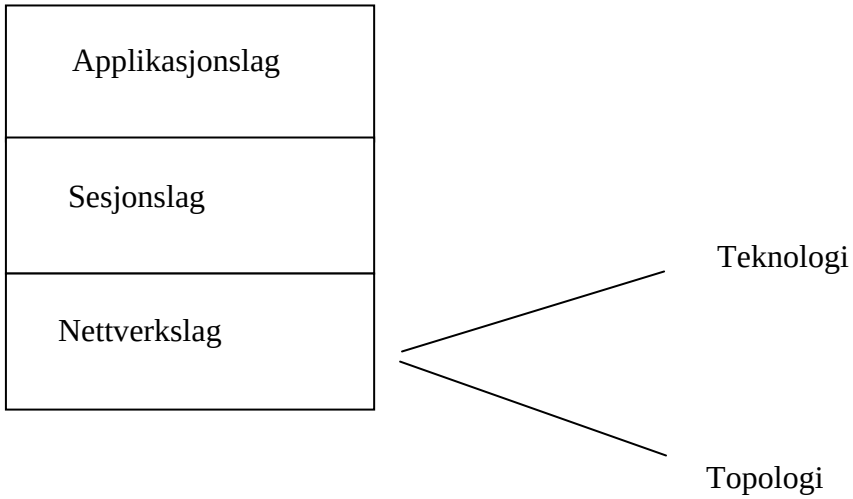
Policy

Det kommer til å bli et behov for styring av arkitektur (”architectural governance”)



Figur 7: Skille mellom PCS og SIS

Secure Engineering må legges til grunn for design av sikkerhets og kontrollsystemer. Utveksling av informasjon mellom SIS og PCS må benytte sikre metoder for informasjonsutveksling. Operatørene må kreve sikre løsninger og være villig til å betale for det. Leverandører leverer det kunden fokuserer på.



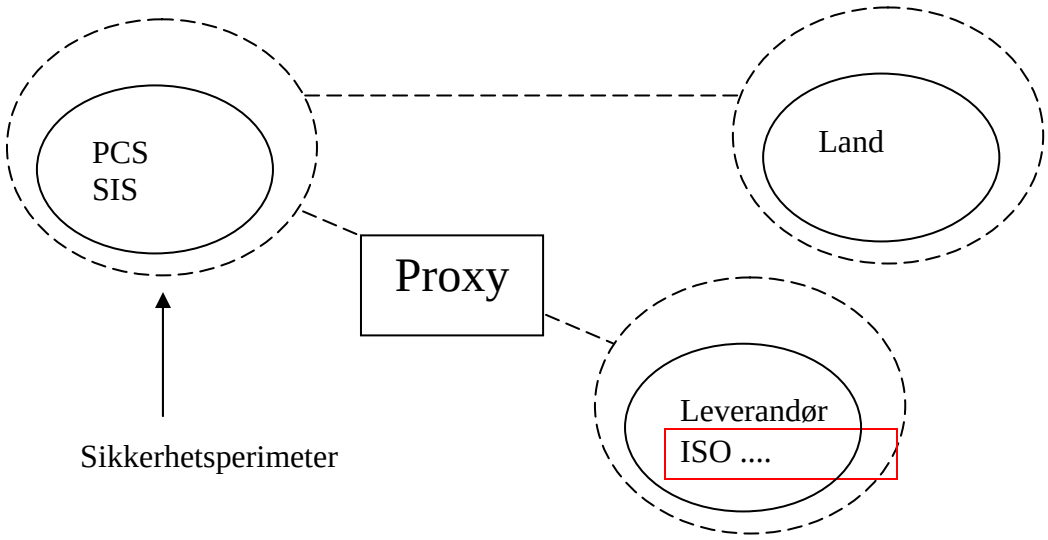
Figur 8: Et utdrag av OSI-modellen

Et ”hellig prinsipp” har vært ”uavhengighet av SIS”, men dette blir stadig vanskeligere i praksis. F.eks. vil det ofte være slik at både PCS og SIS vil ha behov for informasjon fra en gitt endebryter – da trenger vi åpenbart en ”skuddsikker” protokoll.

I Forsvaret har man lang erfaring med såkalte tonivåløsninger, der man har nett som er tillatt brukt for informasjon gradert Begrenset iht. Sikkerhetsloven men som fortsatt kan brukes for tilgang til ugraderte nett som internett. Det spørs om denne tankegangen er direkte anvendbar for IO, ettersom vi her for det meste ikke er opptatt av konfidensialitet, men integritet og tilgjengelighet.

Arkitekturen man ender opp med må være risikobasert, og må være innrettet for å kunne håndtere informasjonen på forsvarlig måte. I de fleste tilfeller vil mulighet til å lese (tappe) informasjon også gi teoretisk mulighet for å gå inn og gi styrende signaler – man har en lukket sløyfe. Endepunktene må derfor ikke ha blind tillit til data som kommer inn (”distrusting trust”).

Nok et eksempel fra virkeligheten er SAP, som er en vesentlig komponent i finanssystemet. Hvis SAP ikke skulle fungere optimalt fra starten, dytter man på med alle mulige tilleggskomponenter/moduler til man blir fornøyd. Resultatet er et informasjonsnav som alt avhenger av. Vi ønsker oss egentlig autonome systemer, men i praksis beveger vi oss mer og mer bort fra dette.

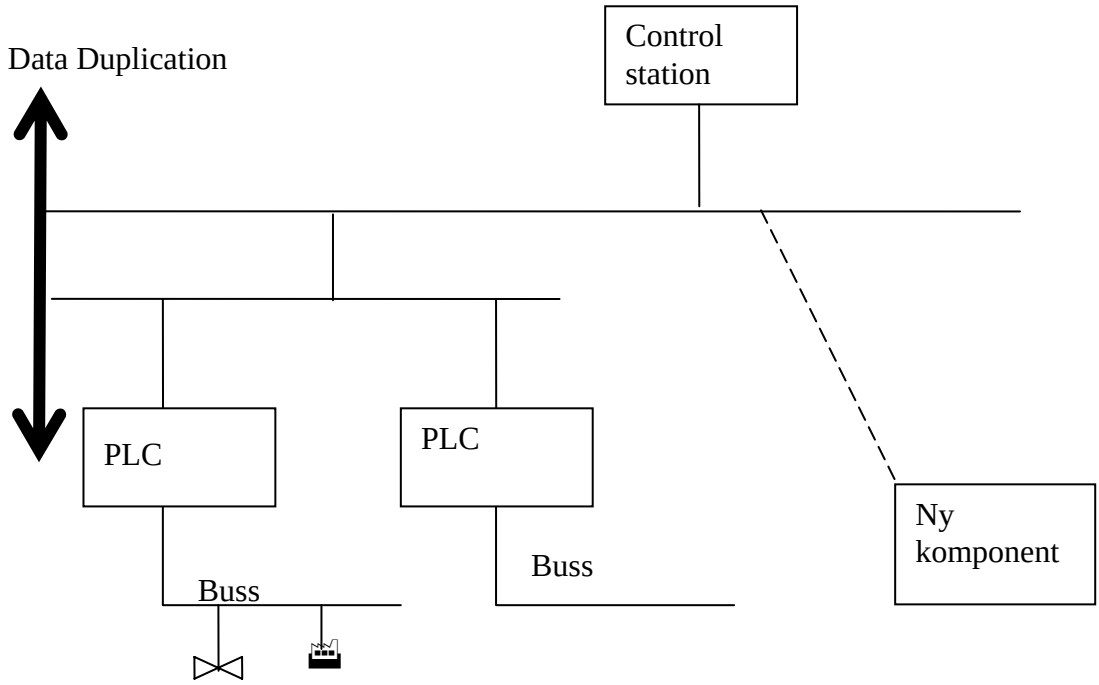


Figur 9: Sikkerhetsperimeter utvidet til å omfatte leverandører mm.

Dette betyr at man må utvide sikkerhetsperimeteren til også å omfatte landbaserte enheter og leverandører (se Figur 9). Dermed er man nødt til å ha en evaluering/sertifisering av leverandører i en helt annen skala enn det vi ser i dag. Aktuelle elementer i en slik evaluering vil være sikkerhetsfilosofi, dokumentasjon av konkrete sikkerhetstiltak og rutiner. Leverandører har tradisjon for å bli sertifisert etter ISO 9000[1], så det er mulig at f.eks. ISO/IEC 27001 [1] (tidligere BS7799) kunne være et utgangspunkt. For tiden later det til at det er inderne som er ivrigst på sertifisering, både innen 27000-serien og Capability Maturity Model (CMM 5 – se [2]).

Når vi foretar design av arkitekturen, må vi ta som utgangspunkt at *det kommer til å være feil* – alle systemer vil på et eller annet tidspunkt være sårbare.

[1] Men hvor mange slike sertifiseringer er i praksis bare støvsamlere på sjefens kontor?



Figur 10: Introduksjon av ny komponent i PCS

Det introduseres stadig mer intelligente tjenester uten at det foretas en risikovurdering, samt at man plutselig befinner seg i en situasjon der man har en stor prosentdel ny teknologi i et gitt system. Trenden med utstrakt bruk av hyllevare medfører at man i stor grad må forholde seg til enkeltkomponenter med stort prispress, noe som også må få konsekvenser for sikkerhetsmarginene. Ofte er "intelligens" i enheter noe som kommer overraskende på brukerne, som en aha-opplevelse i det øyeblikket man oppdager at det er en diagnose-port på det nye (presumtivt "dumme") utstyret.

Generasjon 2 i IO karakteriseres bl.a. av *distribuert kontroll*. Vi kommer i økende grad til å støte på problemet med "skjult programvare", som eksemplifisert i følgende anonymiserte utsagn fra en operatør: "Vi har ingen IT-systemer i vår prosesskontrollsystem". Det er åpenbart fortsatt et stort læringspotensiale til stede både i "prosess"- og "IT"-leirene. Bl.a. er det jo slik at selv om utstyret ikke er stemplet med "Dell" eller "HP", og heller ikke kjører Windows, så kan det like fullt være et IT-system!

I det militære har man tradisjonelt operert "Kommando, Kontroll, Kommunikasjon og Informasjonssystemer" (C_3I - *Command, Control, Communications & Intelligence*) som "*stovepipes*" for hver våpengren (hær, sjø, luft), med relativt lite kontakt på tvers. El-forsyning har tradisjonelt vært en manuell bransje, men som følge av deregulering og konsolidering har man nå et stort behov for automatisert kommunikasjon mellom prosess- og forretningssystemer.

Operatørene (både innen olje&gass og kraft) må vite hva de vil ha og må kunne se helheten. Det er viktig å tenke arkitektur og policy – også når man har et eksisterende system å forholde seg til. Det er viktig å finne den riktige balansen mellom funksjonalitet og sikkerhet! En nyttig øvelse kunne kanskje være å analysere hva man

kunne vunnet i forhold til et eksisterende system hvis man hadde muligheten til å bytte ut alt og starte helt på nytt.

Konklusjoner

Det finnes mange potensielle situasjoner som representerer en trussel mot sikkerhet (*security*) og HMS (*safety*).

Alt kan ikke skiftes på en gang.

Må

a) Finne en organisasjon som inneholder beslutningstakere og ”governing bodies”
b) Utvikle en risikobasert metodikk for å ivareta arkitekturen (intellektuell kontroll).

Det er klart at vi får større utfordringer ved fjernkontroll enn ved fjernlesing.

Hvilke standarder skal vi bygge på?

Det kan bli dyrt å stille for detaljerte krav.

Vi trenger flere ingeniører som snakker både prosess og IT!

B. 3 Tema 9: Hvordan nå fase to i integrerte operasjoner

Referent: Inger Anne Tøndel

Deltakere

Thore Langeland, OLF (prosessleder)
Stephen Wolthusen, Høgskolen i Gjøvik
Chunming Rong, Universitetet i Stavanger
Siri Lunde, Petroleumstilsynet
Eirik Time, Statoil
John Aurlien, Conoco Phillips
Kjell Arne Høyvik, Siemens

Diskusjon

Hva er fase to?

I fase to vil man ha tettere integrasjon mellom operatør og leverandør. Viktige aspekter er:

- Deling av sanntidsinfo
- Linket opp slik at man kan bruke ekspertise over hele verden
- Mer automatisering – embedded systems, agenter

De tjenestene som skal opp på nivå to er de som sikrer samarbeid i Nordsjøen (boring, produksjon, vedlikehold). Det blir mer og mer programvare ut av det. Mange systemer må til for å få til effektiv kommunikasjon. Man har videokommunikasjon på kryss og tvers.

Forholdet mellom konkurrenter

Selskaper trenger å dele informasjon, men er også konkurrenter. Det ble diskutert om dette er et problem, og man kom frem til at dette problemet er størst når konkurrenter selger tjenester til samme operatør. Konkurrenter sitter da i samme kontor, og må integreres inn i operatørens systemer. Datasegregering er da viktig, og dette må ligge i design av systemene.

En ting er når konkurrenter sitter fysisk sammen. En annen ting er når disse skal ha fjerntilgang til informasjon. Man trenger tillit til autentisering og til klienten, og krav til pålogging og patching.

Man har erfaringer rundt dette allerede. Leverandører er integrert inn i systemene fra sine kontorer. Men en utfordring er å komme frem til en felles måte å gjøre dette på slik at leverandører kan opptre på samme måte uavhengig av hvilket selskap de er inne hos.

Lesing vs. skriving

Det er stor forskjell på å gi lesetilgang og skrivetilgang. Skrivetilgang er kritisk, mens lesetilgang kanskje ikke trenger like store begrensninger. De fleste skal lese. Få trenger skriverett. Det ble imidlertid påpekt at lesetilgang kan være kritisk. Et eksempel er live video fra offshore-operasjon Dette ønsker man å ha kontroll med.

Dette finnes det teknologi for i dag. En begrenset mengde personer kan skrive – sende fra land og ut. Dette er det åpnet spesielt for i brannmur, og det gjelder spesifikke pc-er som står spesielle plasser. Andre kan ha tilgang til å følge med på hvordan det går. Lesing kan skje via mellomvare. Det er ingen tekniske problemer med dette – man må bare få gjort det. Det ble imidlertid påpekt at disse tingene kanskje er løst for boring. Når det gjelder prosesskontroll, er det for mange som har tilgang (logge på IMS) og hvis man kommer inn og har nok kunnskap, har man tilgang videre. Det ble også påpekt at dagens løsninger ikke skalerer godt. Det er mye administrasjon og man må vedlikeholde regler i brannmur. Dette blir fort komplekst.

Semantisk web

Semantisk web er viktig for å gjennomføre fase 2. Men det er vanskelig å komme til enighet på norsk sokkel, særlig på grunn av at det er mange internasjonale selskaper. En løsning er å plukke godbiter fra hverandre. Det ble et spørsmål om man går for langt dersom man innfører samme sikkerhetsstruktur. Blir det da enklere å bryte seg inn? Det ble påpekt at å benytte teknologi for semantisk web ikke innebærer at man ikke kan ha egne sikkerhetsløsninger. Semantisk web handler om at systemer kan snakke sammen og forstå hverandre. Man erstatter ikke nødvendigvis systemet man allerede har.

Innen integrerte operasjoner er det ofte tilfelle at datautstyr fra leverandør X kommuniserer med datasystemer fra samme leverandør (leverandør X) utenfor operatørens nett. Det ble hevdet at semantisk web ikke er relevant for dette siden dette utstyret kommer fra samme leverandør og allerede kan kommunisere. Det var imidlertid noe uenighet i at det ikke er relevant med semantisk web så lenge man er innenfor samme organisasjon. Semantisk web vil gjøre det lettere med vedlikehold av systemer. Det blir mindre behov for manuelt arbeid.

Informasjonssikkerhet

Det ble noe diskusjon rundt hvem man ser for seg som angripere og hvilke angrep man ser på. Man må anta at angriper vet like mye om nettet som oss. Spørsmålet er hvilke angripere vi må kunne anta – og fortsatt være robuste. Det ble påpekt at når man nå i større grad kobler ting sammen blir man enda mer utsatt for insidere. Disse vil nå ha tilgang til mange plattformer, og de vet hvordan ting fungerer. En mulig løsning på å bedre dette er å kreve to personer for å gjøre kritiske operasjoner. Dette fører imidlertid til behov for mer administrasjon. En annen løsning som ble skissert var å bruke semantisk web for å gjøre det lettere å overvåke ting relatert til informasjonssikkerhet. Man kan for eksempel legge inn begrensninger på antall plattformer man har tilgang til innen en viss tidsperiode.

Det ble påpekt at man har et behov for å kunne fikse feil så fort som mulig. Derfor har de som sitter på land mulighet til å fikse ting på plattform uten å måtte få lov fra plattform først. Spørsmålet er hva som er sikkert nok. Her er det ulik oppfatning mellom selskaper. Det er viktig å gjøre en vurdering av risiko.

Noen uttalte at det å hacke ikke alltid er den letteste måten å ødelegge på. Ofte vil det være enklere å slippe en bombe eller gjøre annen form for sabotasje. Det ene eksempelet som ble nevnt i presentasjonen fra DNV – der angripere tok over IT-systemene – ble imidlertid diskutert spesielt siden dette er et skrekkscenario der

angriper kan demonstrere for hele verden at han har kontroll. Spørsmålet blir da: Hvor vanskelig er det egentlig å ta kontroll? Viktige innspill relatert til dette var:

- Man trenger barrierer, og er etter hvert blitt opptatt av det i systemene.
- Det er også viktig å gå gjennom øvelser. Dette bør man gjøre i selskapene.
- Man må ha robusthet i applikasjoner som skal brukes i integrasjon. De må ikke ha bakdører og gjøre det de er tiltenkt. Man trenger motstandsdyktighet. Men det er ofte begrenset hvor mye sikkerhet som er bygd inn.
- Sertifisering.
- Det som er sikkert i dag, er ikke nødvendigvis det om en stund. Dersom man glemmer å oppgradere, kan man ende opp med mange ”åpne dører” inn i systemene.
- Validere input man får i XML, og tenke i disse baner når man designer XML-løsningene.
- Finnes tilfeller der virus går rett gjennom
- Kan ikke bruke mennesker for å overvåke denne trafikken. Må ha automatisering - i alle fall hjelpe mennesker å ta disse beslutninger.
- Det er en dynamisk industri med innovasjon og nye tekniske løsninger. Det som er normalt i dag (trafikkmønstre o.l.) er annerledes i morgen.
- Viktig å skille prosesskontrollsystemer veldig sterkt fra det andre. Envegskjøring av data derfra og ut til omverdenen.

Det er viktig å huske på at mennesker feiler. Eksempel: Man sitter hjemme og jobber. Mens man tar seg en tur på toalettet, kommer sønnen inn og gjør ting på pc-en. Det er også forskjell på kulturer.

Felles løsninger for tilgangshåndtering

Hvert enkelt oljeselskap må håndtere mye tilgang. I fremtiden kunne en løsning være å lage en hub slik at man kan benytte autentisering i andre selskaper. Det er bedre å stole på autentiseringen f.eks. Halliburton gjøre av egne ansatte, enn at man selv skal begynne å autentisere folk fra Halliburton. Det er vanskelig å ha kontroll på andres ansatte – hvem som slutter osv. En felles autentiseringshub er vanskelig å få til teknisk nå. Standarden som er mest aktuell har ikke kommet så langt enda. Men på sikt har man tro på en løsning med hub. Denne vil fungere som en ”broker”/en nøytral tredjepart, og vil ikke ha alle nøkler. Skal man logge seg på hos en operatør, vil man gå gjennom broker og få beskjed om autentiseringsnivå. Så kan operatør velge å godta eller ikke godta denne autentiseringen.

Det er mye serviceselskap-personale som går igjen hos flere. Man kunne ha en felles portal for disse med gyldig autentiseringsnøkkel. Slik det er nå, må mye persondata registreres om igjen hos flere selskaper. Hvis man kunne fått persondata som XML fra et fellessystem, ville det hjulpet mye.

Ved en fellesløsning bør man skille på ulike typer av autentisering. Eksempel: Anonyme brukere vs. registrere seg selv på Internett vs. autentisering på kvalifisert nivå.

Det ble diskutert om man kunne benytte SOIL for en slik løsning, og et spørsmål var om SOIL er sikker nok for denne type operasjoner. Det ble uttrykt at SOIL ikke er så sikker som man skulle ønske den var. Mange har tilgang, og man betrakter det som

et ”uvennlig” nett. Det er imidlertid mindre sannsynlig at man får problemer derfra enn fra Internett, og man har bedre tiltro til oppetid.

Fjerntilgang

Det er et trykk på mannskapssiden hos serviceselskapene. Man har ikke lenger nok personer å utplassere i sentrene som er bygd. Mer må gjøres fra selskapenes egne lokaler. De trenger da tilgang til det samme som om de satt hos operatør. Det finnes teknologi for dette nå, men operatører på norsk sokkel har ulikt syn på hvordan man gjør dette. Det ville vært nyttig med felles guidelines på ansvarsforholdet, hva forventer vi at serviceselskapene stiller opp med, hvor går grenseflatene, skal de ha nettverksløsninger frem til vår brannmur, skal vi ha nettverksløsninger frem til deres brannmur, osv. Alle har de samme problemstillingene, og det burde gå an å enes om noe.

En bekymring blant leverandørene når de kobles opp mot sentrene, er relatert til forretningsmodeller. De blir en del av teamet som opererer feltene, men skal ha timebetaling. Dersom de ønsker mer enn timebetaling må de da ta noe av risikoen.

Det ble også pekt på at leverandører nå i større grad må drifte utenfor sin driftsmodell. Utstyret driftes ikke lenger kun i eget nett, men på annet nett via fjerntilgang.

Aksjonspunkter

Mange av de tingene som ble diskutert har man tekniske løsninger på i dag. Det var derfor noe uklart hva som kreves for å komme på nivå to i integrerte operasjoner. Det ble pekt på følgende ting man ønsket at det ble tatt tak i fremover:

- Definere hva som er god praksis og hvordan håndtere ulike scenarier. Man ønsker konkrete, praktiske løsninger og svar på spørsmålet: Hva er den anbefalte måten oljebransjen gjør dette på? Dette må spres rundt slik at man kan få kommentarer.
- Fortsette arbeid med begrepsapparat. Man legger forskjellig betydning i ordene. Dette har også sikkerhetsmessige konsekvenser. Som et eksempel bør man være enige om de sentrale begrepene i et kontrollrom. Utfordringen er at man har leverandører fra hele verden. Det er vanskelig å bli enige om standarder. Leverandører har motforestillinger – de taper penger på det. Tror semantisk web blir viktig.
- Ønsker forskningsprosjekter støttet av EU for å få på plass ontologi
- Kjøre pilotprosjekter. Man opplever motvilje – mange er redde for at ting skal gå galt. Pilotprosjekter kan vise at det fungerer.

B. 4 Tema 10: Hvordan få til rapportering av uønskede hendelser

Referent: Finn Olav Sveen

Deltakere

Lars Grøteide, Hydro (prosessleder)
Einar Oftedal, NorCERT
Ellen Hagelsteen, Oljedirektoratet
Jose J. Gonzalez, Høgskolen i Agder
Stig Ole Johnsen, SINTEF

Bevissthet omkring hendelser

Stig Ole Johnsen fra SINTEF fortalte om funn han hadde gjort i forbindelse med intervjuer av kontrollromoperatører. Kontrollromoperatørene var helt ukjent med virus / ormangrep, slik som det som rammet Statoil i september ’06. Dette er ikke gode rutiner for hendelseshåndtering. Et utsagn som ofte gikk igjen var at ”IKT er ikke så viktig for oss fordi det ikke påvirker prosessene våre.” Intervjuene ble gjort i forbindelse med en CRIOP-analyse. Fire til fem kontrollromoperatører (alle på et skift) ble samlet og intervjuet.

Gruppen påpekte flere mulige tiltak: opplæring slik at man er i stand til å gjenkjenne symptomene på IKT-sikkerhetsproblemer og inkludering av IKT-sikkerhet i arbeidsprosessene

Hva er angrep, hva er støy?

Et problem i IKT-sikkerhet er å skille mellom angrep og støy. Tegn på angrep kan skjule seg i støy. Dette gjelder tekniske såvel som ikke-tekniske angrepsmetoder, insidere som outsidere. Det er f.eks. kjent fra insiderangrep at det er ”precursor-events”, små forhandlinger som forbereder eller tester sikkerheten før man setter inn det endelige støtet. Dette gjelder ikke alle insiderangrep, men mange. Mønstergjenkjenning (pattern recognition, signal detection) er derfor viktig for å kjempe mot uønskede sikkerhetshendelser.

Det ble foreslått at operatører og sikkerhetspersonnell (de som overvåker nett) skulle sitte i nærheten av hverandre. Fra industriens side ble dette sett på som lite praktisk gjennomførbart. Det ble allikevel påpekt at det er viktig for operatørene å ha en forståelse av det som foregår, slik at man kan redusere konsekvensen av en hendelse. Bedre situasjonsforståelse er bra ut i fra et HMS-perspektiv.

Kunnskap om problemene fører til holdninger, som igjen påvirker atferd. Dagens oljearbeidere har ikke tid og ork til å ta i mot mer generell opplæring. Man bør bruke erfaringslæring (andres erfaring) og historiefortelling. Dette gjør det mer forståelig enn en lang rekke med påbud og forbud.

Identifisering av angrep

IKT-miljøet på en plattform er komplekst. Operatører, applikasjonsleverandører og IKT-sikkerhetspersonell er alle involvert i sikring av utstyr og arbeidsprosesser. Det er ofte vanskelig å skille mellom programvarefeil og sikkerhetshendelser. Det er dog

ikke nødvendig for operatørene å finne ut av om det er en sikkerhetshendelse eller en feil. Man må uansett finne ut av hva det er. Feil i prosesskontrollsystemer kan få store konsekvenser. Det er derfor viktig at slike hendelser blir rapportert uavhengig om de er sikkerhetsrelatert eller ikke.

Svikt

Forhold som ofte fører til svikt er: 1) Tekniske feil kombinert med tilfeldigheter. 2) Insider-angrep og *social engineering*. Oljebransjen har tradisjonelt vært utsatt for den første. Den siste er per i dag ikke et problem for oljebransjen, men i morgen?

IT-feil kan være svært komplekse. Hydro hadde en bruker hos ABB som skulle kjøre opp mot Hydro. Personen fra ABB mistet fort forbindelsen. Til slutt fant man feilen som var en dårlig ruter på plattformen. Feilen var meget komplisert å finne ut av og involverte mange personer.

Forhold som påvirker rapportering

Hvis operatører skal rapportere, må det være på et nivå de forstår. Løsning og varsling av et problem er ikke det samme. Kunnskap er også her viktig. Hvis operatørene vet om virus, ormer, etc. vet de også hva som er fornuftig atferd ved tiltak. Det ble igjen påpekt fra industriens side at det er svært vanskelig for en operatør å påvise et virus.

Det er kjent i fra safety at rapportering av hendelser er ekstra arbeide for den som rapporterer. Det bør derfor legges til rette for enkel rapportering. I tillegg til arbeidsbyrden er det flere faktorer som påvirker rapporteringen. Hvis rapportøren ikke blir holdt oppdatert av hva som skjer med hans rapport og om den var nyttig, så vil operatøren heller ikke se nytten med å rapportere. Chris Johnson [9] kaller dette fenomenet “to keep the staff in the loop”. Hvis rapportering over tid ikke fører til en forbedring av sikkerheten, så vil rapportering bli sett på som unyttig, og dermed ikke bli gjort. Og hva er vitsen med å rapportere hendelser hvis man ikke lærer noe av de?

Man må ta hensyn til menneskelige faktorer. Ofte gjør vi små feil som vi kan rette opp ved å prøve igjen. Eks. shift-tasten i stedet for ctrl. Vi har en tendens til å prøve igjen selv om vi ikke forstår hva som skjer. Man må lage en kultur der hvor det er lov til å si at det er noe man ikke forstår eller at noe udefinert skjedde.

Sikkerhet som kvalitetsforbedringsprossess

Sikkerhet er en kvalitetetsforbedringsprosess. Det er ikke noe man kan gjøre en gang og så forvente at det skal fungere i fremtiden. Man må hele tiden forbedre seg for å møte nye trusler som oppstår. Calder and Watkins [4] skriver i sin bok IT Governance at sikkerhet er noe som toppledelsen ikke forstår, og noe som derfor blir delegert til personell lenger nede i organisasjonen. Sikkerhet må ikke oppleves som separat fra andre businessprosesser.

Forskning utført i USA viser at 90% av kvalitetsforbedringsprogrammer ikke gir resultatforbedring eller til og med fører til dårligere resultater [5]. Det er implementasjonsprosessen som svikter. Om man satser på for eksempel 6sigma eller TQM er mindre vesentlig, bare implementasjonen lykkes. Det må være slakk i systemet, d.v.s. tid til refleksjon. Studier fra MIT viser at hvis man bare jobber hardt, så har man ingen tid til å forbedre seg [21]. Hard jobbing fører kortsiktig til gevinst,

men man når fort en grense. Det er begrenset hvor mye hardere en person kan jobbe. Bruker man derimot tid til å utvikle verktøy som hjelper en til å jobbe smartere vil dette føre til langsiktig vinning. Ressursene man bruker til verktøyutvikling må tas fra et annet sted.

Varsling om trusselsituasjonen

Det ble påpekt at en del banker har varslingssystemer/sensorer som viser nettovervåkerne trusselnivået. Man burde kanskje implementere et tilsvarende system for operatører, slik at de kan være ekstra beredt hvis trusselnivået øker.

Mønstergjenkjenning

Det ble påpekt at det er viktig at de forskjellige aktørene i systemet snakker sammen. I forløpet til 11. september var det mange som hadde kompetansen til å forstå sammenhengen, men de hadde ikke det fulle bilde av situasjonen. Ingen hadde hele bildet. Man må snakke sammen for å legge puslespillet. ISPer (Internet Service Providers) har begynt med dette. De ser ikke kun på en maskin, men ser etter mønster over hele nettverket. ISPer har lignende krav til oppetid som det man har på en oljeplattform (100%).

Tiltak

Man bør kategorisere hva som skal rapporteres og hva som ikke skal rapporteres. For eksempel SCADA-hendelser og ikke Word-hendelser.

En kort oppsummering av det som bør undersøkes nærmere:

- Trusselbildet må bli synliggjort
- Incentiver for rapportering
- Disincentiver mot rapportering
- Keep the staff in the loop
- Mønstergjenkjennelse
- Læringssystem, man må lære fra hendelser, ikke bare rapportere de.
- Sikkerhet som et kvalitetsforbedringssystem
- Integrasjon av sikkerhetsprosesser som en del av det totale kvalitetsforbedringsprogram
- Mål, hva vil man med et rapporteringssystem?

En proaktiv holdning er ikke nok, man må hele tiden forsøke å bli bedre. En tanke er å bygge IT-sikkerhet inn i vedlikeholdstankegangen.

Gruppen kom frem til tre tiltak som det bør jobbes videre med:

- Skape en kultur for rapportering
- Opplysning om hendelser/erfaringslæring
- Samle inn god praksis mhp rapportering og håndtering av hendelser.

B. 5 Tema 11: Kategorisering av systemer

Referent: Odd Helge Longva

Deltakere

Arnt Steinbakk	Ptil	(Prosessleder)
Rune Ask	DNV	
Christophe Birkeland	NorCert	
Maria Kjærland	UiS	
Åge Torkildseng	SKS	
Tor Aalborg	Statnett	

Innledning

Deltakerne presenterte seg rundt bordet. Prosessleder viste til oppgaven som var:

- Å diskutere måter å kategorisere systemer med hensyn på informasjonssikkerhet
- Å foreslå tiltak og videre arbeid.

Diskusjonspunkter

Formål med kategorisering

- Å kunne sette sammen systemer av ulike komponenter med gitte krav til sikkerhet for totalsystemet
- Å kunne kople sammen ulike systemer og oppnå gitte krav til sikkerhet for totalsystemet

Metodikk for kategorisering

Momenter fra diskusjonen

- Kritikalitet er et viktig begrep, det angir betydning i forhold til sikker drift
- Kategorisering av komponenter av betydning for sikkerhet gir føringer for sikringstiltak
- Verdifastsetting er viktig element i kategorisering
- Kontrolltjenester er knyttet til konsekvensvurdering
- Vertikal beskrivelse av tjenester er et nyttig verktøy
- Tjenestene er de som er de kritiske, ikke systemene. Systemer kan ha både en kritisk og en ukritisk funksjon
- Vi holder oss her til SCADA-systemer
- Vi må avgrense kategoriseringene
- Vi må ha integrasjon mellom kritiske og ukritiske systemer
- Grensesnitt er kritiske områder. Et eksempel SCADA møter Admin
- SKS har arbeidet med domenebeskrivelser. Sammenkoplings(inter)domene vil være de kritiske
- I hvilken grad er det et nettverk av SCADA-systemer?
- Et interessant tilfelle er rapportering og vedlikeholdsstyring

- Problemer med systemer med ulik kultur
- I SCADA systemer står konfidensialitet i dag ikke på prioritert liste, tilgjengelighet går foran alt – kulturforskjeller
- **NSM: Objektsikkerhetsforskriften kommer forhåpentligvis i 2007. Disse vil sette konkrete krav til sikkerhet. Kan man identifisere delsystemer etter kritikalitet?**
- Fjernkontroll er en egen disiplin med store krav til sikkerhet
- SKS ønsker å bygge sikkerheten også lokalt
- Hvorfor kategorisere? Krav til sikkerhet – robusthet (minst to barrierer)
- Si SAS, ikke SCADA!!!
- Kritikalitet, måles det mot konsekvenser? Ikke bare, ta også med sannsynlighet for hendelse.
- Selv om produktet Sannsynlighet x Konsekvens er lite må det tas alvorlig. Der konsekvensene er veldig store, katastrofer, må det tas spesielle forholdsregler.
- Oppetid er ikke et tilstrekkelig mål
- Hvilke systemer inngår i styring? Risikovurdering bør gjøres av alle komponentene i forhold til funksjon.
- Mulig å kategorisere komponenter gitt arkitekturen.
- Bygge på objektsikkerhetsforskriften
- **NVE sin beredskapsforskrift gir klare sikkerhetskrav**
- Hva betyr ”sikkerhet etter klasse 3”? Den enkelte virksomhets risikovurdering i forhold til definert robusthet
- **Kraftsektoren har kategorisering, oljesektoren ikke. Det er krav til robusthet og til redundans fra NVE. I tillegg kommer sikkerhetsloven og bedriftsspesifikke krav**
- Stadig mer bruk av IKT innføres av økonomiske grunner
- Er det funksjonaliteten som er begrensningen for sikkerhet eller systemet?
- Hva med å bruke Common Criteria med EAL-nivåer som kategorisering?
- Sikkerhet i praksis må ta hensyn til andre prosesser ved kategorisering av kritikalitet. Et ”system klasse 5” vil ha interne krav og eksterne krav, krav til omkringliggende, samvirkende systemer
- For kategorisering må vi ha en referansemodell og en referansearkitektur
- Her ligger det mye arbeid for konsulenter og forskere mtp kategorisering av komponenter, forskning på arkitektur
- Problem med ”legacy systemer”. Både kategorisering av disse og sammenkopling med nye systemer
- Leverandørene trenger spesifikke krav for å utvikle ”sikre” systemer/komponenter
- Rapporten fra infrastrukturutvalget peker på kraft sektoren og olje&gass-sektoren blant topp ti mht kritisk infrastruktur. (Objektsikkerhet)
- Ptil vil samarbeide med OD.

Konklusjoner

Kategorisering av sikkerhet for komponenter og systemer er i stor utstrekning upløyd mark hvor det er rom for betydelige framskritt. Samtidig er det meget komplisert og krever omforent metodikk i form i av ”best practice” og /eller standarder.

Forslag til tiltak/områder hvor det gjøres videre arbeid:

- Risikovurderinger på tjeneste/funksjonsnivå
- Referansearkitektur for å sette krav til komponenter/delsystemer
- Referansemodeller for grenseflatene mot andre systemer
- Sertifisering som en del av kategorisering
- Myndighetene må sette klarere krav (tre-partssamarbeidet)

C. Deltakerliste

Aalborg, Tor (Statnett)	Tor.Aalborg@statnett.no
Ask, Rune (DNV)	rune.ask@dnv.com
Aurlien, John (ConocoPhillips)	john.aurlien@conocophillips.com
Birkeland, Christophe (NorCERT)	cbi@nsm.stat.no
Bratthall, Lars (DNV)	lars.bratthall@dnv.com
Gonzalez, Jose J. (Høgskolen i Agder)	jose.j.gonzalez@hia.no
Grøteide Lars (Hydro)	lars.groteide@hydro.com
Hage, Eivind (Siemens)	eivind.hage@siemens.com
Hagelsteen, Ellen (Oljedirektoratet)	ellen.hagelsteen@npd.no
Hagen, Janne (Høgskolen i Gjøvik/FFI)	janne.hagen@ffi.no
Hauger, Bård (ABB)	bard.hauger@no.abb.com
Høyvik, Kjell Arne (Siemens)	kjell.hoeyvik@siemens.com
Junge, Amund (IRIS)	Amund.Junge@irisresearch.no
Kjærland, Maria (Universitetet i Stavanger)	maria.kjarland@uis.no
Langeland, Thore (OLF)	tla@olf.no
Lode, Ingve Guttorm (BP)	lodeg@bp.com
Løland, Grete (Ptil)	grete-Irene.loland@ptil.no
Lunde, Siri (Ptil)	Siri.Lunde@ptil.no
Madsen, Bjørn Emil (SINTEF)	bjorn.e.madsen@sintef.no
Malmgren, Robert (Robert Malmgren AB)	rom@romab.com
Methi, Arnt (Siemens)	arnt.methi@siemens.com
Møller, Ken (Statoil)	KENM@statoil.com
Nystuen, Kjell Olav (FFI)	kjell-olav.nystuen@ffi.no
Oftedal, Einar (NorCERT)	
Øvreås, Torunn (FFI)	tovreas@ffi.no
Øygard, Turid (Oljedirektoratet)	turid.oygard@npd.no
Rong, Chunming (UiS)	chunming.rong@uis.no
Rui, Øivind (Kongsberg Maritime)	oivind.rui@kongsberg.com
Steinbakk, Arnt (Petroleumstilsynet)	arnt.steinbakk@ptil.no
Sveen, Finn Olav (University of Navarra)	fosveen@tecnun.es
Thunem, Atoosa P-J (IFE)	atoosa.p-j.thunem@hrp.no
Time, Eirik (Statoil)	eirik.time@statoil.com
Torkildseng, Åge (SKS)	age.torkilseng@sks.no
Ueland, Asbjørn (BP)	UelandA@bp.com
Wolthusen, Stephen (Høgskolen i Gjøvik)	stephen.wolthusen@hig.no

D. Referanser

Følgende referanser er delvis spilt inn av gruppedeltakerne, og delvis introdusert av referentene for å gi tilleggsinformasjon/bakgrunn om de diskuterte temaene.

[1] ISO/IEC 27001 "Information security management systems – Requirements"

[2] Carnegie Mellon / Software Engineering Institute: "CMMI® for Development, Version 1.2", CMU/SEI-2006-TR-008, http://www.sei.cmu.edu/pub/documents/06.reports/pdf/06tr008.pdf

[3] Anylogic er et verktøy for agent-basert, diskrete hendelser og systemdynamikk simulering: http://www.xjtek.com/

[4] Calder, A. & Watkins, S. (2005) IT Governance, London and Philadelphia, Kogan Page.

[5] Easton, G. & Jarrel, S. (1998): *The effects of total quality management on corporate performance: An empirical investigation*. Journal of Business, 71, 253-307.

[6] EuroBios -- http://www.eurobios.com/html/gb/eurobios.asp. EuroBios flagger Risk Management & Predictive analysis

[7] Gonzalez, J.J., "*Towards a Cyber Security Reporting System -- A quality improvement process, in Computer Safety, Reliability, and Security* (Lecture Notes in Computer Science 3688), B.A.G. Rune Winther, Gustav Dahll, Editor. 2005, Springer: Heidelberg.

[8] Grance T., Kent K., Kim B./ NIST "Computer Security Incident Handling Guide. Recommendations of the National. Institute of Standards and Technology. csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf. [Metodikken innebærer definering av hva som er en hendelse, samt instrukser rundt hendelseshåndtering. Men NIST er IKT orientert, og ikke HMS relatert].

[9] Grøteide, L. (Norsk Hydro). "*Presentasjon – Hendelseshåndtering*", Ptil 30/11-2006.

[10] Johnson, C. (2003) Failure in Safety Critical Systems: A Handbook of Incident and Accident Reporting, Glasgow University Press.

[11] Jones, S., C. Kirchsteiger, and W. Bjerke, *"The importance of near-miss reporting to further improve safety."* Journal of Loss Prevention in the Process Industries, 1999(12): p. 59-67.

[12] Kjaerland, M. (2005a). A Classification of Computer Security Incidents Based on Reported Attack Data, *Journal of Investigative Psychology and Offender Profiling*, 2, 105-120, (http://www3.interscience.wiley.com:83/cgi-bin/jhome/106558626). ISSN 1544-4759.

[13] Kjaerland, M. (2005b). A Differentiation between Reported Computer Security Incidents Directed towards the Bank/Finance Sector. In W. Bilsky and D. Elizur, Facet Theory: Design, Analysis & Applications (pp. 221-231). ISBN 80-86742-09-1.

[14] Kjaerland, M. (2006a). A Taxonomy and Comparison of Computer Security Incidents from the Commercial and Government Sectors, *Computers & Security*, 25, 7, 522-538, ISSN: 0167-4048. (http://www.sciencedirect.com/science/journal/01674048).

[15] Kjaerland, M. (2006d). Cyber Incident Risk Profiling: Applying Systematic Profiling for Assessing Information Systems Security Risks, *PhD Thesis* , University of Stavanger, Norway.

[16] Kjellen, U. ”*Prevention of Accidents Through Experience Feedback*” ISBN 0-7484-0925-4, Taylor&Francis, London 2000.

[17] Myrland H. ”*E-drift og sikkerhet*” UiS 2005 - (oppgaven publisert av BAS5 – på en cd)

[18] NSM ”*Sårbarheter og trusler mot informasjonssystemer”* Temahefte 1/2006 http://www.nsm.stat.no/dokumenter/Spesielle%20publikasjoner/NSM_Temahefte1_2006.pdf

[19] Nygård *”Risk management in SCADA systems”*. Master HiG 2004 http://www.hig.no/imt/file.php?id=344

[20] Orderløkken, T. L.: ”*Security Incident handling and reporting*.” Master Thesis, Gjøvik University College, 2005. http://www.hig.no/imt/file.php?id=1038

[21] Repenning, N.P. and J.D. Sterman, “Nobody ever gets credit for fixing problems that never happened.” California Management Review, 2001. 43(4): p. 64-88.

[22] Rich, E., F.O. Sveen, and M. Jager. “Overcoming Organizational Challenges to Secure Knowledge Management.” In Second Secure Knowledge Management Workshop (SKM). 2006. Brooklyn, NY.

[23] Sveen, F.O., et al.: “*Toward Viable Information Security Reporting Systems. 2007”*, International Conference on Human Aspects of Information Security and Assurance. Plymouth, UK.
[Doktorgradsstipendiat Finn Olav Sveen har som PhD-tema forbedring av hendelsesrapporteringssystemer. Han lager systemdynamiske modeller av rapporteringssystemer for HMS (”best practice”) og sanker data ang. rapportering av informasjonssikkerhetshendelser – det finnes ikke mye. Målet er dels en komparativ analyse; hvorfor fungerer en del rapporteringssystemer for HMS, mens tilsvarende for informasjonssikkerhet nesten ikke finnes og antagelig ikke fungerer særlig godt? Finn Olav har laget modellen i referanse [Rich 2006], og han har laget modellen og er førsteforfatter i ovennevnte artikkelsom nettopp ble innsendt til HAISA (International Conference on Human Aspects of Information Security and Assurance – se http://www.haisa.org/).]

[24] Stoneburner, G. (John Hopkins University): ”*Towards a Unified Security/Safety Model*” IEEE Computer, August 2006. 39(8): p. 96-97.

[25] Trcek, D. “Security models -- Refocusing on the human factor” IEEE Computer, November 2006 39(11): p. 103-104. [http://dx.doi.org/10.1109/MC.2006.399]
Thunem, Atoosa P-J (IFE) *"Modelling of Knowledge Intensive Computerised Systems Based on Capability-Oriented Agent Theory (COAT)"*, International IEEE Conference on Integration of Knowledge Intensive Multi-Agent Systems, IEEE-KIMAS'03 (proceedings: pages 58-63), September 2003, Cambridge (MA), USA.
[Trekker frem betydningen av agent-basert tankegang og teknologi til ikke minst å kunne modellere "multi-purpose"-agenter som typisk vil være i grensesnitt mellom menneske og maskin (en robot er et typisk eksempel som inneholder egenskaper av både maskin og menneske), men også "rene" tekno-agenter (er begynt å bli brukt innen datakommunikasjon).]

[26] ISO/IEC 15408 ”Information technology – Security Techniques – Evaluation Criteria for IT Security” (part 1-3)

[27] Debra S. Herrmann: “Using the Common Criteria for IT Security Evaluation”, Auerbach Publications 2003, ISBN 0-8493-1404-6

[28] Gartner Group: "Toolkit: Assessing Maturity Levels as a Key to Security Program Development", 12 July 2006, ID Number: G00141781

[29] ISO/IEC 61508 “Functional safety of electrical/electronic/programmable electronic safety-related systems”

[30] PDS-forum http://www.sintef.no/pds/
[31] OLF Guideline 104 “Information Security Baseline Requirements for Process Control, Safety, and Support ICT Systems”, 2006.
see http://www.olf.no/?35820.pdf

Vedlegg - OPPGAVER BESKREVET FRA ARRANGØRENE

- Referent skriver opp hvem som har deltatt på de ulike gruppearbeidene
- Referent sørger for å få dokumentert de viktigste diskusjonene, konklusjonene og spørsmålene fra diskusjonen, gjerne i stikkordsform

- Noen stikkord for diskusjonen i gruppearbeid I ”utfordringer”:
    - Hva er utfordringene i forhold til gitt tema?
    - Hvorfor oppstår det problemer/utfordringer?
    - Hva er mulighetene og nytteverdiene?
    - Hvorfor er temaet viktig å ta opp ifm integrerte operasjoner?
    - Hvordan ser fremtiden ut, hva er videre utvikling? Hvordan skal man følge denne utviklingen?
    - Utarbeide forslag til tiltak og videre arbeid basert på øvrige punkter (grunnlag for videre diskusjon i gruppearbeid II)
    - Annet