IT-sikkerhetspolicy for Integrerte operasjoner

av

Øistein Haaø Fossestøl

Dag Tommy Steen

Erik Krane Thvedt

Masteroppgave i informasjons- og kommunikasjonsteknologi

Høgskolen i Agder

Fakultet for teknologi

Grimstad

Mai 2007

Sammendrag

Ved å benytte IKT i alle ledd i oljeindustrien, vil man oppnå hurtigere og bedre beslutninger, og med hjelp av sanntidsdata kan man integrere arbeidsprosesser på tvers av fag og mellom organisasjoner. Denne utviklingen blir i oljenæringen kalt Integrerte operasjoner (IO). Ved hjelp av IO kan operasjoner styres uavhengig av avstand og geografisk lokasjon. Det er satt inn store ressurser på dette feltet, og allerede i dag ser man vellykkede implementeringer av Integrerte operasjoner.

Med Internett som en del av bærenettverket for data produsert i oljenæringen, vil trafikken i utgangspunktet være svært utsatt. Bruk av Internett åpner for trusler utenfra, dersom man ikke tar tilstrekkelig høyde for IKT-sikkerheten.

I dette prosjektet ser vi på trusler som er knyttet til tilpassning av SAS-systemer til IO. SAS (Safety and Automation Systems) er systemer som omhandler sikkerhet og automasjon, og inkluderer bl.a. brann- og gassdeteksjon, nødavstengning og prosesskontroll. Som et utgangspunkt for å identifisere truslene tar vi for oss hendelsesforløpet til en mislykket boreoperasjon på Snorre A-plattformen. Hendelsesforløpet er beskrevet i en granskningsrapport av Petroleumstilsynet, og vi benytter denne rapporten for å beskrive et scenario om hvordan de enkelte avvik kunne vært unngått dersom Integrerte operasjoner hadde vært inkludert i driften. Scenariet benyttes videre for å identifisere hvilke tjenester som er en del av Integrerte operasjoner, og på den måten lage en ramme rundt begrepet. Deretter avdekkes de vesentligste trusler mot disse tjenestene.

For å dekke opp om truslene presenteres et sett av IT-sikkerhetspolicyer. Disse er basert på OLFs anbefaling nr. 104, og standarden NS-ISO/IEC 17799. Policyene er delt inn i ulike temaer og teknologier, og er presentert som vedlegg i slutten av rapporten.

Videre ser vi på enkelte sikkerhetsfremmende løsninger for implementering i Integrerte operasjoner. Rollebasert aksesskontroll (RBAC) blir vurdert som aksesskontrollmetode, og vi foreslår også andre tiltak og løsninger for å øke informasjonssikkerheten ved tilpassning av SAS-systemer mot Integrerte operasjoner.

Forord

Prosjektet er utført som avsluttende oppgave for mastergradsstudium i informasjons- og kommunikasjonsteknologi ved Høgskolen i Agder, avdeling Grimstad. Oppgaven er gjennomført i tidsrommet januar til mai 2007 av Øistein Haaø Fossestøl, Dag Tommy Steen og Erik Krane Thvedt, som alle har valgt fordypning innen sikkerhet.

Oppgaven er gitt oss av Origo Engineering AS, og vi ønsker å takke Origo for muligheten til å jobbe med et spennende og fremtidsrettet prosjekt. Vi ønsker å rette en spesielt stor takk til Trond Friisø, som har vært vår kontaktperson mot Origo, og veileder for oppgaven. Han har vært en ressursperson som har kommet med gode innspill underveis, og alltid vært tilgjengelig for oss. Vi setter stor pris på hans engasjement.

Grimstad 29. mai 2007

Øistein Haaø Fossestøl

Erik Krane Thvedt

Dag Tommy Steen

Innholdsfortegnelse

Vedlegg

Figurliste

Tabelliste

1 Innledning

1.1 Bakgrunn

I dagens teknologisamfunn er det stor vekt på effektivisering ved bruk av IKT. På grunn av modne felt og fallende produksjon, har det i Nordsjøen blitt lagt mye fokus på eDrift eller Integrerte operasjoner (IO) i den senere tid. Begrepene Integrerte operasjoner og eDrift er ansett som likeverdige og vi velger å benytte Integrerte operasjoner videre i denne rapporten. IO medfører en ny driftspraksis på norsk sokkel. Man vil oppnå hurtigere og bedre beslutninger ved å bruke IKT-løsninger som inkluderer sanntidsdata til å integrere arbeidsprosesser på tvers av fag og mellom organisasjoner. Ved hjelp av IO kan operasjoner styres uavhengig av avstand.

Kort fortalt går Integrerte operasjoner ut på at data fra ulike systemer ombord på oljeinstallasjoner gjøres tilgjengelig for driftsstøttefunksjoner på land, eksperter, leverandører osv. slik at disse kan bidra til en mer optimal drift, og til å løse bestemte oppgaver i en driftssituasjon. Integrerte operasjoner er enda på et tidlig stadium og utrykket stammer fra rapporter i offentlig sektor fra 2003-2004. [1]

Ettersom man i fremtiden ser for seg at drift og operasjoner i større grad blir flyttet til landbaserte operasjonssentre, vil det være helt essensielt å sørge for at IKT-systemene som understøtter denne trenden blir tilstrekkelig sikret. Daglig oppdages det nye sikkerhetshull, og dermed nye sikkerhetstrusler i forbindelse med utbredt maskin- og programvare. Med Internett som en del av bærenettverket for data produsert i oljenæringen, vil trafikken i utgangspunktet være svært utsatt. Bruk av Internett åpner også for angrep utenfra, dersom man ikke tar tilstrekkelig høyde for IKT-sikkerheten. Norsk oljenæring vil være et yndet mål for terrorister, hvis slike en gang i fremtiden skulle finne på å skade Norge. Sett fra terroristens side, vil det være hensiktsmessig å utnytte de svakheter som finnes i IKT, versus å benytte andre terrormetoder.

Oljeindustriens Landsforening (OLF) er en landsforening i NHO (Næringslivets Hovedorganisasjon). Det er en interesse- og arbeidsgiverorganisasjon for oljeselskaper og leverandørbedrifter som er knyttet til utforsking og produksjon av olje og gass på den norske kontinentalsokkelen. [2]

Origo Engineering AS (Origo) holder til på Andøya i Kristiansand. De leverer hovedsakelig brann- og gassdeteksjonssystemer (B&G), men leverer også automasjonssystemer til

smelteverk. Origos systemer består blant annet av detektorer, PLS (Programmable Logical Sequencer) og NAS (Nødavstengningsystemer), som er knyttet til eksisterende infrastruktur. Tidligere har dette vært anlegg som i liten, eller ingen grad har hatt kommunikasjon med eksterne nettverk. Nyere installasjoner og oppgraderinger skal være tilpasset Integrerte operasjoner, etter krav fra kundene. Det er dermed en utfordring å formulere en sikkerhetspolicy for dette som er tilpasset Integrerte operasjoner. OLF har gitt en del retningslinjer som kan være et godt utgangspunkt.

1.2 Oppgaven

Studentene skal:

1. Svare på hva som er de vesentligste truslene og IT-sikkerhetsutfordringene forbundet med å tilpasse et SAS-system til Integrerte operasjoner. En mulig framgangsmåte kan være å ta utgangspunkt i et tenkt scenario, for eksempel med utgangspunkt i Snorre A hendelsen den 28.11.2004.

2. Foreslå en IT-sikkerhetspolicy tilpasset Integrerte operasjoner. Denne bør baseres på OLFs anbefaling nr. 104, og bør omfatte datamaskinsikkerhet, brukersikkerhet og fysisk sikkerhet.

3. Om tiden tillater det, vurdere noen ulike løsninger for implementering, slik som infrastrukturdesign, kommunikasjonsgrensesnitt, brukergrensesnitt, sikkerhetsmekanismer og prosedyrer/beste praksis.

1.3 Problemstilling

Oljenæringen krever at systemene som brukes på og i forbindelse med oljeplattformer skal bli bedre integrert, slik at det er mulig å samarbeide og effektivisere de forskjellige systemene. Dette stiller også krav til leverandører av utstyr til oljenæringen; utstyr som brukes på eller i forbindelse med plattformer må være tilpasset nye effektiviseringsmetoder med bruk av IKT. Origo er en leverandør av brann- og gassystemer til plattformer, og for å etterkomme de nye kravene, må systemene Origo leverer tilpasses Integrerte operasjoner. Ettersom Integrerte operasjoner i stor grad baseres på IKT og datakommunikasjon, vil det være helt nødvendig å sørge for tilstrekkelig sikring av kommunikasjonskanalene mellom de ulike enheter og systemer, både med tanke på kontinuitet i driften, og for å hindre uvedkommendes adgang til IKT-systemene. Brann- og gass-systemer går under det som kalles SAS (Safety and Automation Systems), og stiller strenge krav til sikkerhet.

Tidligere benyttet man i oljebransjen proprietære og spesialsydde systemer, disse var gjerne dyre i utvikling og lite fleksible. Idag og i fremtiden ser man tendenser til at man går over til å benytte billigere og standardiserte løsninger i forbindelse med Integrerte operasjoner. Dette medfører at også truslene knyttet til disse følger med. Når man samtidig har behov for å åpne opp systemene for å tillate en tettere integrasjon av de forskjellige nettverk og instanser, vil man også gjøre disse nettverkene mer sårbare for ondsinnede angrep.

1.4 Avgrensninger

Vi velger å ta utgangspunkt i granskningsrapporten om Snorre A hendelsen [12], slik oppgaven foreslår. Hendelsesforløpet vil utelukkende baseres på denne rapporten, og scenariene vil baseres på disse hendelsene. De vesentligste truslene og sikkerhetsutfordringene vil dermed bli utledet fra dette.

Vi forutsetter at SAS-systemene innehar samme struktur som idag, også ved overgang til G2 av Integrerte operasjoner.

IT-sikkerhetspolicyene vil baseres på OLFs anbefaling nr. 104 [10] og de trusler som avdekkes i første del av oppgaven.

I siste del av oppgaven vil vi ikke se på trivielle sikkerhetstiltak som brannmurteknologi, routere, IDS og lignende. Vi vil heller komme med nye innfallsvinkler og løsninger som kan benyttes i oljenæringen etter implementering av Integrerte operasjoner

Prosjektperioden er avgrenset til 20 uker.

1.5 Viktighet av oppgaven

Mange oljefelt har allerede, eller innen kort tid nådd punktet hvor det ikke lenger er økonomisk forsvarlig å fortsette utvinning av olje eller gass. Integrerte operasjoner kan medføre store økonomiske besparelser i form av mindre bemanning og mer effektiv drift. Videre fører dette til at man kan fortsette driften ved modne felt lengre enn man ellers kunne ha gjort.

Integrerte operasjoner krever involvering fra alle ledd, inkludert leverandører av utstyr som brukes i driften. Driftstans i produksjonen er enormt kostbart og kan medføre formidable økonomiske tap. I oljeindustrien ansees utsatt produksjon som tapt inntekt.

Det er derfor viktig at alle ledd sørger for tilstrekkelig sikkerhet innenfor sitt felt. Oppgaven tar for seg IKT-sikkerheten i forbindelse med tjenester i IO, og er derfor et viktig ledd i den videre utviklingen av Integrerte operasjoner.

1.6 Oppbygging av rapporten

Kapittel 2 tar for seg teorien rundt de emnene som blir benyttet i løsningen. I kapittel 3 beskrives metodene som er benyttet for å komme frem til løsningen, som blir beskrevet i kapittel 4. Løsningen er delt inn i tre deler, hvor første del er basert på et scenario i forbindelse med en hendelse på Snorre A-plattformen i 2004. Dette scenariets hensikt er å identifisere hvilke mulige tjenester Integrerte operasjoner kan tilby. Deretter avdekkes hvilke trusler og sikkerhetsutfordringer som eksisterer i forbindelse med de tidligere identifiserte tjenestene. Del to i dette kapitlet tar for seg mulige løsninger på de avdekkede truslene, presentert som ulike policyer. Disse policyene er vedlagt under ”Vedlegg 1”. Del tre av dette kapitlet tar for seg en del forslag til implementering, slik som sikkerhetsløsninger og prosedyrer. De tre siste kapitlene i rapporten tar for seg henholdsvis diskusjon, konklusjon og referanser.

2 Teori

2.1 Integrerte operasjoner

2.1.1 Introduksjon

Effektivisering ved bruk av IKT er blitt vektlagt mye i industrien i den senere tid. Også i Nordsjøen er dette et faktum, og Integrerte operasjoner har medført en ny driftspraksis på norsk kontinentalsokkel. IO benytter bl.a. sanntidsdata til å integrere og fordele arbeidsprosessene mellom de involverte aktører. Med dette oppnår man hurtigere og bedre beslutninger, og operasjonene kan styres uavhengig av geografiske lokasjoner.

Integrerte operasjoner gjør det mulig å distribuere data fra de ulike systemer ombord på oljeinstallasjoner til driftstøttefunksjoner på land. Disse dataene kan gjøres tilgjengelig for operatører, leverandører, eksperter med spisskompetanse på gitte områder, o.s.v. slik at disse kan bidra til å gjøre driften optimal.

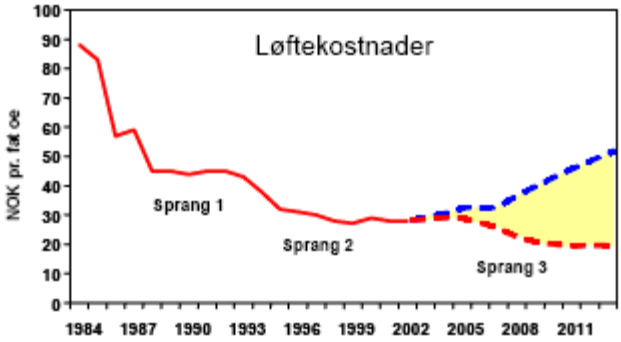
En entydig definisjon av begrepet IO finnes ikke. SINTEF har i sin rapport "Trusler og muligheter knyttet til eDrift" [3] samlet de definisjonene som betraktes som de mest refererte. Disse er:
"

- *Innebærer bruk av informasjonsteknologi til å endre arbeidsprosesser for å oppnå bedre beslutninger, til å fjernstyre utstyr og prosesser til å flytte funksjoner og personell til land (Stortingsmelding 38, 2004)*
- *Bruk av informasjonsteknologi og sanntidsdata til å optimalisere operasjonene på kontinentalsokkelen (eDrift på norsk sokkel – Det tredje effektivitetsspranget, 2003)*
- *Sanntids integrering av offshore operasjoner og onshore beslutningsstøtte med samordnet operasjonssentre (oversatt fra OG21 TTA-strategirapport "E-Operations and maintenance", 2003)*
- *"Hva er eDrift: "Nye driftsformer, IKT løsninger som inkluderer (nær) sanntidsdata, Integrerte arbeidsprosesser (tverrfaglig, hav og land, forskjellige organisasjoner) For å oppnå: Hurtigere og bedre beslutninger." (OD)*

Oljeselskaper og leverandører opererer for øvrig også med egne formuleringer, som reflekterer selskapenes visjoner for eDrift. eDrift kan omfatte bruk av fjernstøtte, fjernovervåking, fjernkontroll eller fjernstyring slik begrepene defineres. "
[3]

Mange forskjellige begrep brukes om IO. Synonymer til IO er eDrift, e-operations, Fields of the future, smarte felt (Smart fields), Instrumented fields, Digital fields og E-felt (E-field).

Rapporten "eDrift på norsk sokkel" har valgt å definere IO som "det tredje effektivitetsspranget på norsk sokkel".



Figur 1: Effektivitetssprang på den norske sokkel [4]

Sprang 1 og 2 går på forbedring av 2D seismikk (1 sprang) og 3D seismikk (2 sprang). Utbyggings- og driftskostnadene pr. fat ble, som en følge av disse sprangene, sterkt redusert. Samtidig ble oljeutvinningsgraden økt betydelig, skadelig utslipp pr. produsert enhet redusert og sikkerheten forbedret.

Utvinningsgraden i de store feltene (Ekofisk, Statfjord, Oseberg og Gullfaks) lå i 2004 rett oppunder 60 %, mens utvinningsgraden til mindre felt lå i samme periode rett oppunder 40 % [5].

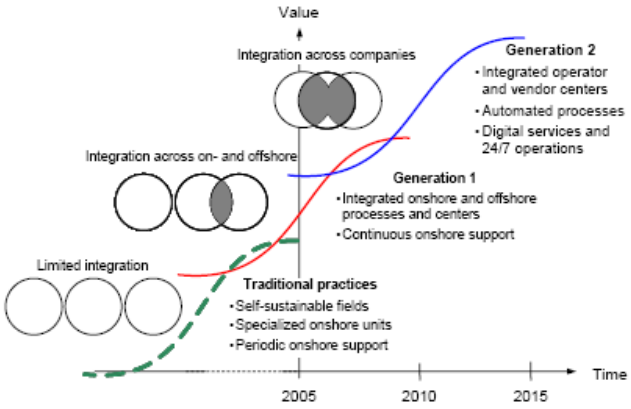
Det er forventet at utvinningsgraden vil øke med 0,5 prosentpoeng per år, men man vil ved innføring av IO kunne oppnå et løft av denne. Det forventes at man i framtiden vil kunne nærme seg en utvinningsgrad på over 70 % på de større feltene, og over 50 % samlet utvinning på norsk sokkel.

Gjennom IO har industrien mulighet til å ta enda et effektivitetssprang. Det er flere grunner til at et slikt sprang er nødvendig for norsk sokkel. Oljeproduksjonen på norsk sokkel faller mens driftskostnadene stiger. Det er lønnsomhetskrav fra eiere og kapitalmarkedet, i kombinasjon med at Norge har et høyt kostnads- og skattenivå sammenlignet med andre olje- og gassnasjoner, som gjør IO svært attraktivt for Norge. Det er også forventninger om lavere fremtidige oljepriser som har ført til et sterkt

kostnadseffektiviseringspress. Reduserte letemuligheter og mangel på utbyggingsprosjekter har ført til et lavere aktivitetsnivå de senere årene. Ved å kombinere olje- og gassteknologier med IKT kan denne trenden bli snudd. IO skaper en mindre avhengighet av geografi og øker muligheten for å optimalisere produksjon. [4]

Modne felt er oljefelt som har passert sin hovedproduksjon, og kommet inn i haleproduksjon. Dette medfører at kostnadene per produserte enhet vil øke, ettersom man ikke greier å produsere like mye som tidligere, samtidig som at kostnader knyttet til vedlikehold og produksjon stiger. Før eller senere vil ethvert felt komme inn i en tilstand hvor det ikke lengre er økonomisk forsvarlig å fortsette driften. Dette kan utsettes ved hjelp av nye produksjonsmetoder eller ny teknologi som kan være med på å redusere kostnaden forbundet med produksjon.

OLF har etablert flere arbeidsgrupper som har jobbet med spørsmål rundt IO. I et prosjekt gjennomført av en arbeidsgruppe, med navn "Integrated Work Processes" (IWP), skulle se på fremtidige arbeidsprosesser på norsk sokkel. De så for seg at IO vil bli implementert i to steg som de kaller Generasjon 1 (G1) og Generasjon 2 (G2). Dette er altså ikke det samme som det tredje effektivitetsspranget som tidligere nevnt.

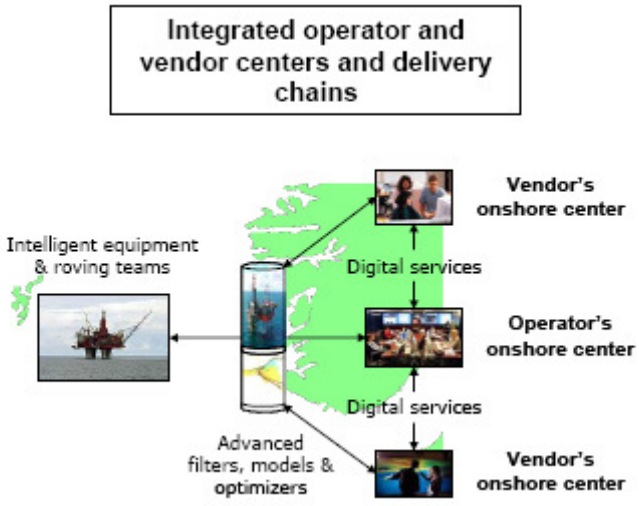


Figur 2: Integrerte operasjoners tidslinje [6]

Generasjon 1 innebærer å integrere prosesser og mennesker onshore og offshore ved hjelp av IKT-løsninger, som gjør at man kan være behjelpelig fra land. Dette krever at ansatte på land har tilgang til samme data som mannskapet offshore til samme tid (i sanntid). Her har det vært pilotprosjekter som har vist seg å være vellykkede, noe som gjør at vi allerede i dag har startet på G1. Siden dette har vært en suksess, vil det være hensiktsmessig å fortsette utbygging og integrasjon på flere installasjoner. G1 vil føre til at man kan følge med på hva som skjer samtidig og sammenligne data med simuleringer og komme med direkte hjelp og støtte fra land. Også serviceteknikere, leverandører og

lignende kan være direkte involvert i planlegging og være med under selve operasjonen, dersom det skulle oppstå komplikasjoner. Med kraftige maskiner som kan gjennomføre analyser, kan personellet også komme med anbefalinger og råd med hensyn på fakta de innehar. Dette kan være informasjon om bunnen der man borer eller råd om reservoar og hvordan disse kan utnyttes. Under prosessene som blir gjennomført, vil all planlegging og forberedelse vil bli utført på land av driftsstøttepersonell. [6]

Generasjon 2 handler om tettere integrasjon i arbeidsprosesser mellom operatører og leverandører. De fleste tjenester for å operere felt vil bli digitalisert, og de fleste operasjoner vil bli fjernstyrt. Man ser for seg at leverandører tar over mer av driften på systemene de leverer, og man har da egne kontrollsentre for både operatører og leverandører, hvor et olje- og gassfelt blir styrt fra. Leverandører kan eventuelt ha sentre på egen lokasjon til daglig drift av sine systemer. Operatørene vil fremdeles ha hovedansvaret, men vil ha en tett integrasjon og få faglig hjelp og råd fra leverandører og eksperter på de forskjellige systemene. Sentrene vil være operative 24 timer i døgnet. Avanserte filtre som filtrerer all informasjon automatisk vil være utviklet, slik at man kan få frem den informasjonen som til enhver tid er viktig. Man kan her se for seg at disse sentrene er plassert over hele kloden og at en leverandør godt kan drifte sitt system fra en helt annen del av verden. [6]



Figur 3: Illustrasjon fremtidig IO [6]

Med Integrerte operasjoner vil mengden av sanntidsdata øke i store mengder inn til land. Dette vil bidra til at miljøene onshore og offshore kan utveksle kvalitetssikrede data i sanntid, som fører til at man kommuniserer raskere og bedre. Dermed vil planleggings- og arbeidsprosessene som til nå har vært sekvensielle og tidkrevende bli effektivisert. IO vil også sørge for tettere og bedre integrasjon mellom fagområder på land. De nye

arbeidsprosessene og samarbeidsformene kan være med på å avlaste og være til støtte for arbeidet offshore. Dette vil også føre til økt sikkerhet ved at bemanningen offshore reduseres, reisevirksomheten reduseres og relasjonene mellom landsorganisasjon og plattform forbedres.

For å kunne oppnå dette er det en stor utfordring for industrien å effektivt få utnyttet den økte datamengden. Rapporten "eDrift på norsk sokkel" har kommet opp med 3 punkter for hva en effektiv utnyttelse fører til.

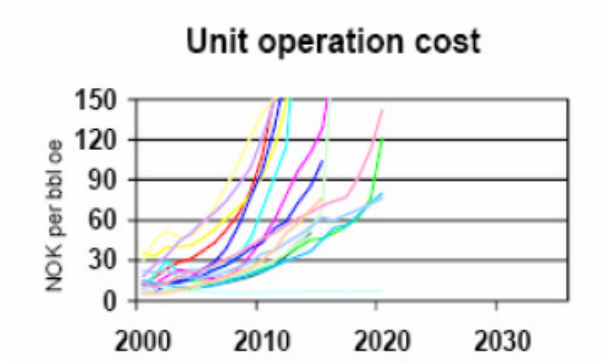
"

- *Smartere og effektive boreoperasjoner, mer optimale brønnbarrierer.*
- *Smartere utvinning, mer optimal strømningskontroll i brønner og prosessanlegg og bedre reservoarutnyttelse*
- *Smartere drifts- og vedlikeholdsprosesser*

"

[4]

Det er viktig for Norge å gripe muligheten og være tidlig ute med IO, slik at vi kan være i forkant av utviklingen, og ved hjelp av dette skape et konkurransefortrinn for norsk industri. Vi har i Norge høy kompetanse på løsninger som kan utnyttes under krevende forhold i Arktis og på store dyp. Denne kompetansen sammen med IO vil kunne skape økt konkurransekraft. [3]



Figur 4: Kostnader per produserte enhet på norsk sokkel [6]

Et annet argument for å sette av mye ressurser til IO, er at den norske sokkelen er inne i en rask modningsprosess. For at det skal være økonomisk forsvarlig å fortsette driften utover den planlagte tiden må både utvinningsgrad økes og produksjonskostnader senkes. Dette medfører at integrasjonen av G2 må akselereres, ettersom tidsvinduet er meget begrenset. Den typiske prosessen for full implementering og daglig bruk av nye konsepter og teknologier er som regel lang, samtidig som mange av feltene på den norske sokkelen nærmer seg haleproduksjon. [6]

Semantisk web og Web Ontology Language (OWL)

I Integrerte operasjoner er det mye fokus på web og webløsninger. World Wide Web har blitt det primære verktøyet for deling av informasjon, og er den viktigste globale informasjonskilden man har tilgjengelig. Trendene har vært at organisasjoner har store intranett internt, og benytter seg av internett mot andre bedrifter. Mange ønsker imidlertidig å returnere til grunnideen bak World Wide Web, som medfører at man benytter den som en et medium for interaksjon og deling av kunnskap. Dette fører til et behov for en ny metode å behandle informasjon og data på. En slik metode kalles semantisk web.

Semantisk web inneholder standarder for hvordan data skal behandles, lagres og bygges opp. Disse standardene krever at data framstår i et hensiktsmessig format, og ikke blir gjemt inni annen kode slik, at den må ekstraheres før den kan benyttes. En annen tanke bak semantisk web, er at det tillater applikasjoner og maskiner til å se sammenhengen mellom forskjellige datasett. Et eksempel på dette er semantiske linker, som tillater programmene å utføre automatisert datafangst fra flere kilder.

Semantisk webteknologien er bygd opp rundt blant annet et konsept som heter ontologi. Ontologi benyttes for å definere hvordan data er i slektskap med hverandre. Det kan også benyttes som et virkemiddel for å tvinge applikasjoner og maskiner til å behandle to forskjellige dataklasser som identiske. For eksempel kan brukerhåndboken til en enhet være definert på norsk som ”håndbok”, og alle håndbøkene til alle enheter ligger under denne klassen. På engelsk vil det hete ”manual”. Ved å innføre en ontologi som sier at brukerhåndbok er det samme som manual, vil applikasjoner behandle disse som samme klasse. Ontologiregler kan også utveksles mellom organisasjoner, og benyttes til å oppdage ny informasjon. Denne oppdagelsen av informasjon benyttes for å finne informasjon som ikke er direkte gitt i datasettene. Dette kan lettere illustreres med et annet eksempel; om vi har to fragmenter av informasjon som sier følgende: <Fido er en hund> og <Alle hunder er pattedyr> vil applikasjonen selv kunne trekke den konklusjonen at <Fido er et pattedyr> selv om denne informasjonen ikke er oppgitt.

OWL (Web Ontology Language) er et standardisert språk for publisering og deling av ontologier på World Wide Web. OWL er utviklet som en utvidelse av RDF (Resource Description Framework).

RFD er en standardmodell for datautveksling på nettet. RDF har egenskaper som tillater fusjon av data, selv om de underliggende databaseskjemaene er forskjellige, og den støtter spesifikt evolusjon av slike databaseskjemaer over tid.

Det er viktig å merke seg at ikke alle forholdene lar seg beskrive av ontologi. Enkelte datasett kan inneholde tvetydighet, og kan ikke alltid direkte bindes sammen, uten at det foreligger noe ekstra informasjon som fungerer som et slags "lim". I det første eksemplet benytter vi ontologi som knyttet sammen ordene "håndbok" og "manual". Det kan tenkes at datatypen "manual" kan inneholde informasjon om manuelle operasjoner, istedenfor brukerhåndbøker. Slike tvetydigheter kan unngås om det foreligger god kommunikasjon og klart definerte datatyper innenfor oljenæringen og alle medvirkende aktører.[17]

2.1.2 Utfordringer i Integrerte operasjoner

Integrerte operasjoner fører til en økt bruk av IKT, og nettverkssystemer åpnes opp for å bedre samarbeid over større geografiske områder. Dette fører til større avhengighet av IKT. En av tankene bak IO er at man skal kunne gi tilgang til systemene for tredjepartsaktører. Dette medfører mer åpenhet i systemene, som videre fører til større risiko og strengere krav til sikkerhet. Med IO kan næringen bli mer sårbar for feil, mer utsatt for usikkerhet, og for ondsinnede angrep. Dette betyr at man må ha et felles rammeverk for informasjonssikkerheten. Det må defineres klare retningslinjer innen sikkerheten for alle leverandører og aktører som benytter de integrerte nettverkene. Slike retningslinjer finnes ikke per i dag. [3, 6]

Sentralisering og samspill

Ved å sentralisere og integrere flere systemer øker også kompleksiteten til de teknologiske løsningene. Dette fører også til at kompleksiteten for brukere, og samspillet mellom teknologi og menneske øker. En av de største utfordringene er å få dette samspillet til å fungere. Systemene må gjøres så enkle, og opplæringen så grundig, at dette er håndterbart. Et av de viktigste tiltakene er gjennomføring av grundige risikoanalyser, eller HAZOP-studier underveis under hele utviklingen av IO. Det holder ikke å lage en risikoanalyse i dag, for så å basere framtidig integrering av IO på denne. Man må etterhvert som systemene bygges opp, og nye elementer blir lagt til, utbedre og foreta risikoanalyser, for å avdekke nye problemer som kan dukke opp på grunn av endringer i systemene. Rapporten "Trusler og muligheter knyttet til eDrift" [3] sier: *"Å håndtere kompleks og tett koblet IKT-relatert risiko gir et organisatorisk dilemma, skal man desentralisere og sentralisere på samme tid? I så måte kan eDrift (fjernstøtte) bidra positivt ved sentralisert overvåking og kontroll samtidig som enkelte drifts- og vedlikeholdsoppgaver kan desentraliseres.".*
[3]

Distribuerte systemer

Integrerte operasjoner medfører overføring av en betydelig mengde informasjon i sanntid mellom offshore- og onshoreanlegg. Dette fører til at man må utvikle standarder som definerer hvordan informasjonen lagres og sendes fra sensorer offshore til onshoresentere og motsatt. Det må avklares hvilke aktører som skal ha tilgang til denne informasjonen, og hvordan den skal deles mellom de forskjellige aktørene, slik at de blir behandlet og forstått på rett måte av alle parter [6]. Her har forskjellige leverandører og aktører sine system som de gjerne vil benytte. Rapporten "Quality Information Strategy" har kommet med forslag til hvordan dette kan standardiseres. De har tatt utgangspunkt i at informasjonen bør være lagret og distribuert på en slik måte at ikke bare én dominerende leverandør eller et system kan bearbeide og fremstille resultater. Ettersom Integrerte operasjoner bearbeider og deler informasjon mellom forskjellige organisasjonsenheter, teknologier og geografiske områder i sanntid, vil dette være viktig siden man da ikke kan være avhengig av en tilbyder [8]. Teknologiene endrer seg fortløpende, og det er derfor mest hensiktsmessig å finne en felles plattform og terminologi for informasjonsutveksling, slik at denne blir entydig og hensiktsmessig for menneskene i næringen. Den eneste standarden som er tilgjengelig i dag, er standarden ISO 15926 "Integration of life-cycle data for process plants including oil and gas production facilities". Denne standarden er relativt ny og deler av den er fremdeles under utvikling [8]. Sammen med to andre viktige standarder (POSCs EPICENTRE standard og Wellsite Information Transfer standard) vil man muliggjøre etablering av virtuelle modeller av anlegg, reservoarer og brønner [3].

Opplæring

Ofte er det bevisstgjøring og grundig opplæring som kan hindre at trusler blir til angrep på systemene. Malware og ondsinnede angrep er opplagte farer ved en slik åpning av systemene. Det som ofte er problemet er at ondsinnet kode blir plantet fra innsiden, enten av en misfornøyd ansatt med intensjon om å skade bedriften, eller av uvitende brukere som ikke er klar over hva de gjør. Dette kan være vanskeligere å sikre seg mot. Handlinger som åpning av epostvedlegg med usikkert innhold kan infisere brukerens maskin. Når denne maskinen står i et lokalnettverket vil barrierene mot eksterne nettverk ikke ha noen beskyttende effekt. Et annet problem er det som kalles "social engineering". En person kan for eksempel ringe til en ansatt og på en troverdig måte utgi seg for å være driftssansvarlig, og kan ved hjelp av dette lure den ansatte til å oppgi sitt passord eller annen sensitiv informasjon. Dette er en av de enkleste måtene for en hacker å bryte seg inn i et system på, siden man slipper tidkrevende og vanskelige angrep direkte på systemene [7]. En annen utfordring i forbindelse med informasjonssikkerhet er muligheten for teknisk svikt. Det er dermed viktig å ha

redundante systemer som gjør at nedetid og feil blir minst mulig. Faren for teknisk svikt øker med kompleksiteten og størrelsen av systemene. [3]

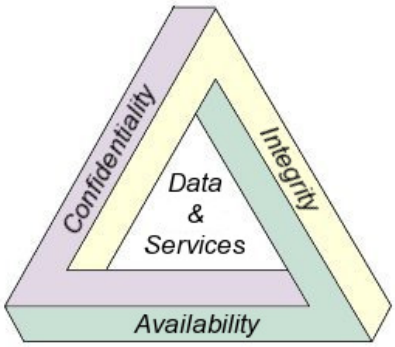
Den økte mengden informasjon som Integrerte operasjoner medfører, kan få flere negative konsekvenser og føre til risiko med hensyn på beslutninger og arbeidsforhold. Økt bruk av IKT og virtuelle samhandlinger fra forskjellige ledd kan skape stress og kommunikasjonsproblemer. Det kan fort bli for mange ledd i beslutningsprosessen og dermed bli problemer med å få fattet beslutninger. Det må derfor utvikles klare retningslinjer for hvem som har ansvar og skal ta disse avgjørelsene. I tillegg er det viktig med trening og opplæring i samarbeid med simulerte hendelser, slik at man i en virkelig hendelse vet hvem og hva man skal forholde seg til. I andre tilfeller kan økt bruk av IKT føre til at beslutninger blir tatt for fort, uten at alle faktorer er vurdert og tatt hensyn til. Dette kan igjen føre til en dårlig beslutning, grunnet forhastede konklusjoner. Igjen er det viktig med nøye opplæring og faste rutiner ved operasjoner. Integrerte operasjoner legger opp til mindre bemanning offshore og mer bemanning onshore. Dette kan føre til at man har for mange ansatte uten reell ”hands-on”-kompetanse, disse kan i noen tilfeller ta avgjørelser som virker korrekt, men som i praksis kan vise seg å være umulig, eller utgjøre en fare. Det er derfor viktig at folk på onshoresentrene får nøye opplæring, og at det finnes avanserte simuleringer som gjør det mulig for arbeidstakerne å få trening i å ta slike avgjørelser. [3]

Endring i arbeidsprosesser

Slik situasjonen er i dag, er olje- og gassnæringen hele tiden i endring og nye tiltak blir iverksatt som følge av IO. Hvis de ansatte stadig pålegges å endre sine arbeidsrutiner kan dette medføre at ansatte blir slitne og misfornøyde, som igjen kan føre til dårligere HMS klima. Innføringen av IO skaper store endringer i arbeidshverdagen, og det er derfor viktig å skape trygghet i forhold til endringsprosessen og ikke gå for fort frem. [3]

Sikkerhetstriangelet

Sikkerhetstriangelet består av konfidensialitet, integritet og tilgjengelighet. Disse tre elementene har som hensikt å sørge for at tjenester, data og ressurser er sikret, tilgjengelig og har nødvendig kvalitet. Integritet sørger for at informasjon er korrekt og ikke endret på noen måte. Tilgjengelighet sørger for at ressurser, tjenester og data er tilgjengelig når man har bruk for dem, mens konfidensialitet sørger for at kun personer som skal ha tilgang til informasjonen, får det. Hovedfokus i Integrerte operasjoner vil ligge på integritet og tilgjengelighet.



Figur 5: Sikkerhetstrianglet [9]

2.1.3 Oppsummering Integrerte operasjoner

Det er mange antydninger og teorier om fremtiden til norsk olje- og gassnæring. Det vi ser er at olje- og gassnæringen går mot en ny tidsalder i forhold til innføring av IKT. Dette skjer allerede i dag, og vil ha en større betydning i fremtiden. Det er spesielt viktig for Norge å være tidig ute i denne trenden, for å skape seg konkurransefortrinn i forhold til land som har helt andre arbeidsforhold og priser. Vi ser at trenden i denne næringen, som i andre, er at man etterhvert kan outsource deler av drift til lavkostland, slik at det blir billigere å fremstille råvarene. I tillegg vil Norge få et fortrinn lengre nord i vanskelige forhold, med IO kan man lettere utnytte disse mulighetene. IO preges foreløpig av mange spørsmål og avhenger av ny teknologi, så vel som gode strukturer rundt sikkerhet og dokumentasjon.

2.2 Hendelsen på Snorre A brukt som metode for scenario

28. november 2004 oppstod det en ukontrollert og utilsiktet situasjon under arbeid i en brønn på plattformen Snorre A. Ifølge Petroleumstilsynet (Ptil) er dette en av de mest alvorlige situasjonene som har skjedd på norsk sokkel [12]. Situasjonen oppstod under en operasjon som kalles slissegjenvinning.

Hendelsen utviklet seg med at brønnen som arbeidet pågikk i, ble ustabil da trekkingen av et sidesteg skulle foretas, og man fikk en ukontrollert gassutblåsning på havbunnen, samt gass under plattformen. Mannskap som ikke var dirkete involvert eller nødvendig for å gjenopprette stabilitet i brønnen, ble evakuert fra plattformen, da gunstige vindforhold var med på å muliggjøre dette ved hjelp av helikopter.

Det oppsto ingen skader under hendelsen, verken på mennesker eller innretning. Kostnadene hendelsen medførte omfattet utsatt produksjon og undersøkelse av sjøbunnen på senere tidspunkt. Produksjon var ikke oppe på normalt nivå igjen selv etter

tre måneder. Hendelsen kunne ha fått fatale konsekvenser. Gassen som sev opp kunne ha antent, eller medført sviktende oppdrift, som videre kunne medført tap av innretning, menneskeliv og store skader på miljøet.

2.3 IT-sikkerhetspolicy

2.3.1 Introduksjon

En IT-sikkerhetspolicy er et generelt administrasjonsdokument som skal være grunnlaget for informasjonssikkerhet i organisasjonen. Den beskriver hensikten med IKT-sikkerhet, og skal være en samlet intensjon og retning slik ledelsen formelt uttrykker den. [10] Når det i denne rapporten snakkes om sikkerhetspolicy, menes et eller flere sikkerhetsdokumenter relatert til IKT-sikkerhet i organisasjonen, også kalt informasjonssikkerhetspolicy eller IT-sikkerhetspolicy.

IT-sikkerhetspolicyen kan sies å være definisjonen av hva som ansees for sikkert innenfor IT-systemer. En sikkerhetspolicy er et sett med begrensninger, krav og regler for brukere og systemer. Den forteller *hva* som skal sikres og beskyttes, men det er viktig å merke seg at policyen aldri forteller *hvordan* dette skal gjøres i praksis. En må også merke seg at selv om policyer følges til punkt og prikke av alle involverte parter, kan de ikke garantere å hindre alle typer feilbruk eller angrep.
Det er vanlig at forskjellige deler av organisasjonen har ulikt syn på sikkerhetsbehovet. Brukere er ofte bekymret for at økte sikkerhetskrav kommer i veien for deres arbeid, systemadministratorer kan se problemer som oppstår ved drifting under streng sikkerhet, og ledelsen kan være bekymret for forholdet mellom økte kostnader kontra økt sikkerhet.

Når man implementerer en sikkerhetspolicy, bør man huske på at mennesker som affekteres av policyen ofte ikke tar imot den med åpne armer. Folk kan være negative til flere restriksjoner, spesielt hvis meningen med dem ikke kommer tydelig frem. Det er derfor essensielt at det i policyen kommer tydelig frem hvorfor den trengs og hva som er hensikten med den.

Balansen mellom sikkerhet og produktivitet må tas i betraktning når en sikkerhetspolicy blir utviklet. Er dokumentet for lite restriktivt, vil hensikten med det falle bort. Policyen er grunnlaget for informasjonssikkerheten, og er det ikke fastsatt klare og konsise regler, vil det oppstå smutthull og ”snarveier” som skaper en eller flere nye potensielle trusler.

Hvis dokumentet er for restriktivt vil det i ekstreme tilfeller være umulig å implementere og forholde seg til. I mindre ekstreme tilfeller kan de involverte parter enten ignorere policyen eller finne måter å omgå restriksjonene på. Med utgangspunkt i de overnevnte punkter, vil det være nødvendig å finne en balansegang mellom den sikkerheten som ansees nødvendig, og den produktiviteten som ønskes.

Det er essensielt at også ledelsen støtter opp under de sikkerhetspolicyer som til enhver tid er gjeldene. Hvis et sikkerhetsprogram skal være vellykket, holder det ikke at ledelsen bare gir klarsignal, de må også fremstå som gode eksempler. Ansatte må bli klar over at ledelsen anser informasjonssikkerhet som vitalt for organisasjonens drift og at de ansattes arbeidsplass kan være avhengig av sikkerhetsprogrammets suksess. [7]

2.3.2 Innhold

Policyene bør være lettfattelige og enkle å forstå, de bør ikke inneholde for mange tekniske uttrykk. Dette fordi de skal leses av alle involverte, ikke nødvendigvis bare ansatte med IKT-bakgrunn. De må også være mulig å gjennomføre og håndheve, dette medfører at de ikke kan være for restriktive. De må også være entydige og konsise for å hindre misforståelser som kan oppstå i tilfelle tvetydighet. Det bør nevnes konsekvenser for overtredelse eller forsømmelse av policyens retningslinjer.

En policy bør alltid begrunnes, begrunnelsen for restriksjonene og tiltakene bør være nevnt i hver enkelt policy. Årsaken til dette er at leseren som omfattes av policyen kan anse policyen som mindre viktig og dermed overse hele, eller deler av policyen. Dette må unngås, og det vil dermed være viktig at alle policyer får en begrunnelse.

NS-ISO/IEC 17799:2005 er en standard for informasjonssikkerhet utviklet av ISO (Den internasjonale standardiseringsorganisasjonen) og IEC (Den internasjonale elektrotekniske kommisjon), og oversatt til norsk av Norsk Standard. Den sier følgende om informasjonssikkerhetspolicy:

"Dokumentasjonen av sikkerhetspolicyen bør uttrykke ledelsens støtte og skissere virksomhetens tilnærming til administrasjon av informasjonssikkerhet. Dokumentasjon av policyen bør inneholde erklæringer om følgende forhold:

a) en definisjon av informasjonssikkerhet, dens generelle mål og omfang, og betydningen av sikkerhet for å muliggjøre deling av informasjon;

b) en erklæring om ledelsens intensjoner som støtter opp om målene og prinsippene for informasjonssikkerhet;

c) en ramme for fastsettelse av sikkerhetsmålene og sikringstiltakene, inklusive strukturen for risikovurdering og risikostyring;

d) en kort redegjørelse for sikkerhetsreglene, prinsippene, standardene og forpliktelsene som er av særlig betydning for virksomheten, f.eks.:
   1) tilpasning til juridiske, forskriftsmessige og kontraktsmessigeforpliktelser;
   2) krav til utdanning, opplæring og bevisstgjøring med hensyn til informasjonssikkerhet;
   3) kontinuitetsplanlegging;
   4) konsekvenser ved brudd på retningslinjene for informasjonssikkerhet;

e) definisjon av generelt og spesifikt ansvar for administrasjon av informasjonssikkerhet, herunder rapportering av informasjonssikkerhetsbrudd;

f) referanser til dokumentasjon som kan understøtte virksomhetens sikkerhetspolicy, f.eks. mer detaljerte retningslinjer og prosedyrer for bestemte informasjonssystemer eller utførlige sikkerhetsregler som brukerne bør rette seg etter."

[11]

Informasjonssikkerhetspolicyen kan være en del av bedriftens generelle sett av policyer [3]. Den kan videre deles inn i individuelle policyer for ulike emner. Dette kan for eksempel være:

- Fjerntilgang
- Akseptabel bruk
- Passord
- Informasjonssensitivitet
- Anti-virus
- Trådløs kommunikasjon
- Risikovurdering
- Akseptabel kryptering

Dette er bare noen få eksempler på temaer for informasjonssikkerhetspolicyer, og er ikke en fullstendig oversikt.

IT-sikkerhetspolicyer bør ikke inneholde faktaopplysninger som er tilbøyelig til stadig endring. Eksempler på dette kan være programvarers versjonsnummer, webadresser og lignende. Hvis dette ikke unngås, kan det medføre tvetydighet og misforståelser. Det medfører også at policyen tidlig blir foreldet, og må stadig oppdateres.

2.3.3 Revisjon

Informasjonssikkerhetspolicyer bør revideres med jevne mellomrom for å reflektere endringer i organisasjonen. Det er da viktig at alle policyer har en eier som står ansvarlig for den. Med eier menes her en person som har påtatt seg ansvar for policyen og dens livsløp. Ansvaret inkluderer evaluering av policyen i dens utvikling, videre om den er aktuell i forhold til organisasjonens nåværende status, og også om den har forbedringspotensial. [11]

2.4 Mulige sikkerhetsteknologier for IO

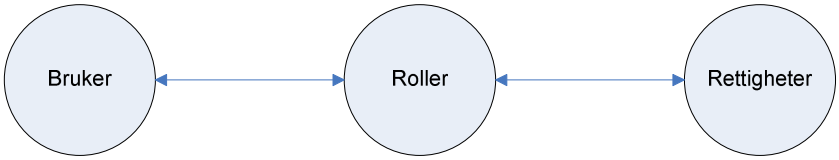
2.4.1 Role Based Access Control (RBAC)

Mange aksesskontrollmetoder krever at nettverksadministrator gis mye tillit, og mye avhenger av diskresjon og pålitelighet til denne personen. RBAC har metoder for å løse disse problemene. RBAC har vært brukt i UNIX-systemer, operativsystemer som Novell netware, Microsoft Windows NT og Solaris har en variant av RBAC ved bruk av administrerende roller. Disse har lite støtte på applikasjonsnivå. Vi ser i dag at flere RBAC elementer blir implementert inn i de nye operativsystemene. [16]

I dag er RBAC en komplett modell, utarbeidet av NIST, men ikke fullt ut standardisert. Til nå har det vært opp til utviklingsingeniørene å implementere RBAC og bruke den i applikasjoner. Tidligere har de forskjellige RBAC modellene vært veldig like, men man har blant annet brukt forskjellig terminologi, og det har dermed vært vanskelig å få de til å jobbe sammen. Dette er noe som har gjort at det er vanskelig å bytte produsent eller å integrere løsninger fra forskjellige leverandører.

RBAC kontrollerer aksess til nettverk og ressurser basert på roller. Som vist i figur 6 er rettigheter linket til roller, og brukere er igjen tildelt disse, basert på type stilling og ansvarsområde. Dette forenkler rettighetskontroll, siden det er lett å tildele eller frata roller fra brukere og tildele eller nekte rettigheter til rollene. Dette gjør systemet mer oversiktlig og lettere å holde kontroll over. Man kan også sette opp restriksjoner (constraints) som Seperation of Duty (SoD). Denne mekanismen reduserer risiko for bedrageri ved å nekte brukere mer tilgang enn de trenger for å utføre oppgaven. [16] I

vedlegg 2 følger mer inngående informasjon om aksesskontrollmetoder og den foreslåtte standarden til NIST.



Figur 6: Relasjoner mellom bruker, rolle og rettigheter

2.4.2 Digitale signaturer

Digitale signaturer kan på mange måter sammenlignes med en skriftlig signatur. Teknologien baseres på en offentlig nøkkel som er kjent for alle, og en privat nøkkel som kun er kjent for eieren. Dette er en asymmetrisk krypteringsmetode, og det man får ut av prosessen ved å kryptere en signatur med den private nøkkelen, og dekryptere den med den offentlige nøkkelen, kalles digital signatur. Den offentlige nøkkelen blir distribuert via digitale sertifikater, som knytter nøkkelen sammen med informasjon om brukeren, samt den ukrypterte signaturen. Ettersom kun eieren av den private nøkkelen kan kryptere signaturen, slik at denne kan dekrypteres med offentlig nøkkel og deretter samsvare med nøkkelen i klartekst, vil eieren dermed bli autentisert. Dette hindrer også såkalt non-repudiation, eller ikke-fornektelse. De digitale sertifikatene blir ofte garanterte av såkalte TTP (Trusted Third Party). Dette er tredjepartsaktører som går god for at sertifikatet er ekte, og faktisk tilhører den oppgitte eier.

2.4.3 Sikkerhetsenheter

Sikkerhetsenheter (eng. security tokens) har til felles at de brukes til autentisering og at de er små i størrelse, og kan som regel bæres i en lomme. Den vanligste formen for sikring innen autentisering er bruk av passord. Gode passord er ofte tilstrekkelig for en sikker autentisering i en påloggingsprosess, men i tilfeller der sesjonen innebærer pålogging til kritiske eller sensitive systemer, bør ikke passord være eneste barriere inn. Dersom passordet på en eller annen måte skulle bli kompromittert, vil sikkerhetsbarrieren være brutt. Det vil da være hensiktsmessig å innføre en ekstra barriere.

Dette kalles to-faktor autentisering, og krever to av de tre følgende faktorer;

- Noe du vet (f.eks. passord)
- Noe du har (f.eks. smartkort eller digitalt sertifikat)
- Noe du er (biometri slik som f.eks. fingeravtrykk)

Sikkerhetsenheter kommer i mange ulike utførelser. Nettbanker bruker ofte engangspassord i form av et kort med påtrykte passord, eller en digital enhet som genererer et engangspassord avhengig av tid. Denne enheten er da synkronisert med dens tilhørende konto, som genererer samme engangspassord, og sjekker disse opp mot hverandre.

Andre eksempler på sikkerhetsenheter kan være USB-penner, PCMCIA-kort, Bluetooth-baserte enheter og smartkort. Smartkort er den mest brukte typen av sikkerhetsenheter, fortrinnsvis fordi de tilbyr en relativt god sikkerhet og fordi de er svært rimelige i forhold til andre sikkerhetsenheter. Smartkort er verdens mest solgte elektroniske gjenstand, og i 2004 ble det solgt 2,3 milliarder smartkort på verdensbasis [18]

3 Metode

Målgruppen i prosjektet vårt er Origo Engineering AS som leverer brann- og gassdeteksjonssystemer til oljeplattformer, men rapporten kan i utgangspunktet benyttes av alle som ønsker en bredere forståelse av Integrerte operasjoner. Rapporten er ment som et kompetanseløft på et felt som enda er i startfasen.

Vårt problem faller inn under kategorien deskriptivt problem. Dette vil si at vi undersøker forhold som allerede er godt dokumentert og med dette som grunnlag løser oppgaven. Arbeidsmåten og bearbeidingen av informasjonen vil være kvalitativ.

Hovedteknikken for informasjonsinnsamling vil bli fra eksisterende dokumenter om emnet. Ved å benytte seg av dette er det viktig at man er kritisk til kilder, slik at fakta resultatene er basert på er validerbare og pålitelige. Vi benytter oss av dokumenter fra ulike kilder for å øke validiteten (SINTEF, OLF, Ptil etc.). Vi tar også i betraktning når dokumentene er skrevet og hvem som har skrevet de, slik at vi kan få et mest mulig korrekt bilde av situasjonen.

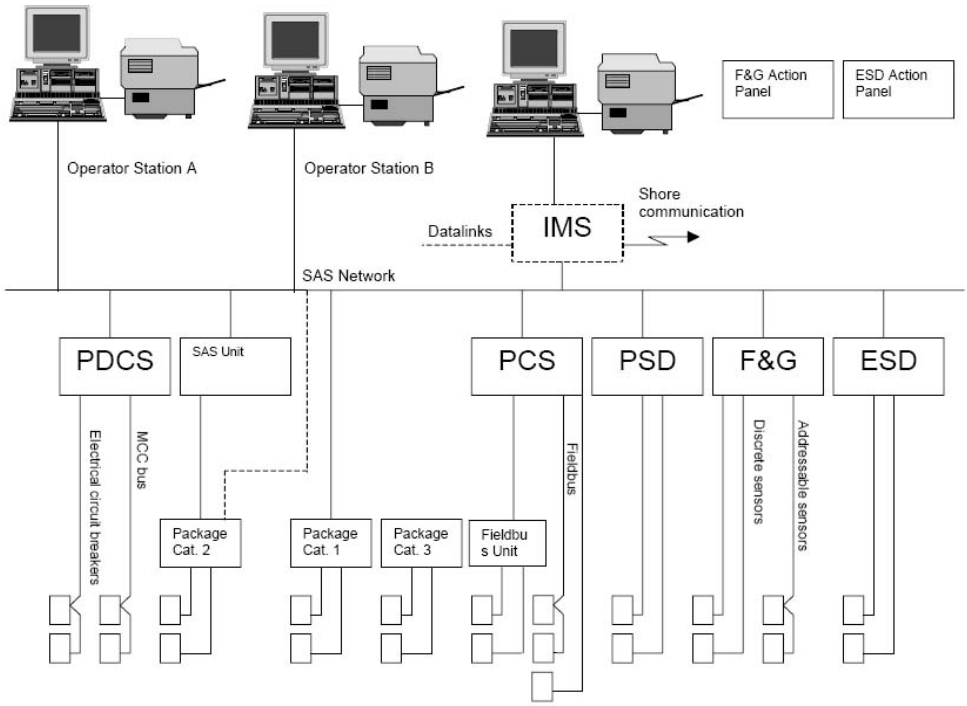
For å lettere avdekke mulige nye tjenester i Integrerte operasjoner benytter vi oss av scenarielæring. Her tar vi utgangspunkt i en rapport fra Ptil som detaljert beskriver hendelsesforløpet til en operasjon på Snorre A plattformen. *"I scenarielæring tar beslutningstakerne selv ansvar for egen fremtidstenkning og arbeider – med et spekter av metoder og verktøy – for å skape fremtidsbilder som gir bedre forståelse og perspektiver på dagens beslutninger og handlingsmønstre. Scenarielæring handler om å strekke organisasjonens egen forståelseshorisont til å ta inn mer relevant informasjon om omverdenen og fremtiden."* [19] I vår rapport lager vi et fremtidsscenario til de delene av hendelsesforløpet hvor vi mener Integrerte operasjoner kan være med på å gjøre en forandring.

4 Løsning

4.1 Integrerte operasjoner og SAS-systemer

Opprinnelig er SAS (Safety and Automation Systems) basert på isolerte systemer, hvor all kommunikasjon foregår mellom de forskjellige sløyfene og en sentral. Sikkerhetskravene som settes til slike systemer er høye, da de er helt nødvendige for å sikre ikke bare store materielle verdier i form av plattformer og installasjoner, men også menneskers liv og helse. Det er derfor særdeles viktig at slike systemer fortsatt opprettholder det høye sikkerhetsnivået som kreves av dem, selv ved tilpassning til Integrerte operasjoner. NORSOK I-002 [20] inneholder krav som skal oppfylles av slike systemer, og disse eller tilsvarende krav må fortsatt være oppfylt, selv etter overgang til IO.

De bakomliggende systemene og protokollene som idag er med på å bygge opp et SAS-system, kan benyttes selv ved videre implementering av IO (se Figur 7). Opprinnelig er operatørstasjonene plassert på installasjonen, og ved evt. oppgraderinger og vedlikehold vil det være nødvendig med utsending av mannskap.



Figur 7: Fysisk oppbygning av SAS [20]

Idet man ønsker å gjøre informasjonen som finnes på disse SAS-systemene tilgjengelig for omverdenen, vil man straks få et annet trusselbilde. Når det gjelder G1, vil informasjonen ikke forlate organisasjonens nettverk, men forbli på intern-nettverket. Dette medfører at de fleste trusler også vil bli konsentrert her. I praksis vil dette si at man tar med seg de tidligere truslene som eventuelt eksisterte i det isolerte systemet, og i tillegg får trusler på alle lag i OSI modellen.

Ved innføring av G2, ønsker man å åpne intern-nettverket for ekstern kommunikasjon. Man ønsker at blant annet leverandører av SAS-systemer skal få tilgang til systemene fra sine egne lokaler. På denne måten kan de utføre vedlikehold og oppgraderinger av systemene, uten å benytte kostnadsbelastende operasjoner, slik som utsending av mannskap. Dette tillater også leverandører å registrere og plukke opp anomalier som detekteres, og adressere disse direkte.

Ved å åpne kommunikasjonen mot omverdenen på denne måten, vil en rekke nye sikkerhetsutfordringer true systemene. Disse sikkerhetsutfordringene vil være generelle utfordringer rettet mot Integrerte operasjoner i sin helhet, og ikke mot SAS-systemer spesielt.

På bakgrunn av dette vil scenariene i det påfølgende kapittelet i hovedsak omhandle tjenester og trusler i Integrerte operasjoner generelt.

4.2 Integrerte operasjoner og Snorre A hendelsen

Dette kapittelet tar for seg deler av forløpet i hendelsen på Snorre A plattformen den 28. november 2004 og forkant av denne. Forløpet er organisert i kronologisk rekkefølge og er hentet fra Petroleumstilsynets granskningsrapport; ”Gransking av gassutblåsningen på Snorre A, brønn 34/7-P31 A” [12]. I etterkant av hver hendelse er det presentert et mulig scenario som omhandler et alternativt hendelsesforløp dersom Integrerte operasjoner hadde vært implementert på Snorre A og hos de tilhørende aktører. Deretter blir tjenestene knyttet til scenariene presentert, samt de tilhørende trusler. Det første delkapitlet er basert på ”IWP: Future Work Processes on the Norwegian Continental Shelf” [6].

4.2.1 Et fremtidsscenario

I dag er enhver offshoreinstallasjon bemannet med et gitt antall personer som har erfaringer innen ulike driftsoperasjoner, og hvordan disse håndteres og planlegges. I fremtiden ser bransjen for seg at man samler denne kunnskapen og erfaringen på et

sted, og dette kan kalles et kunnskapssenter. Senteret er en nøkkelspiller i gjennomføring, planlegging og overvåkning av drift og operasjoner som foregår ute på plattformene. Her vil kunnskap deles, og man trekker erfaringer fra de ulike miljøene og samler dem på et sted. Dette senteret har tilgang til data fra alle installasjonene i sanntid, og kan også overta styringen over store deler av plattformen om ønskelig. Styring av eksempelvis ROV (Remotely Operated Vehicle) er også mulig fra dette senteret. Kunnskapssenteret kan kjøre 3D simuleringer av f.eks. brønner, hvor sanntidsdata blir hentet inn av sensorer som er plassert både på plattformen, i utstyr og i brønnen. Kompetansen på dette senteret holder en meget høy standard, og man har også mulighet til å innkalle hjelp utenfra ved behov. Dette kan foregå i sanntids videokonferanse.

Det meste av den daglige driften foregår på land, og annen ekspertise kan kobles inn idet man støter på et problem som overgår senterets ressurser, eller trenger hjelp i en gitt situasjon. Boreentreprenører og vedlikeholdsleverandører er mer involvert i planleggingen og gjennomføringen av operasjoner, men det er fremdeles operatørene som har hovedansvaret og som godkjenner operasjoner.

Informasjonsstrømmen vil i større grad bli automatisk lagret og hentet frem når det er bruk for dem. I forkant av en operasjon vil man automatisk få opp parametere og data som er relevante og oppdaterte. Under en prosess vil man få sanntidsdata om operasjonen og disse vises i avanserte 3D-modeller.

Smarte verktøy og nevrale nettverk vil la boreoperasjoner automatisk følge en predefinert bane, og på denne måten optimalisere boreprosessen. Kunstig intelligens vil benyttes for historiske, statistiske og analytiske data, for å få en best mulig beslutningsprosess.

Muligheten til å kunne overvåke områdene i sanntid og få frem brønnens tilstand i en 3D-figur vil gi en rekke fordeler. Ved å kunne måle trykk, temperatur og strøm vil man kunne endre verdier for å utnytte ressursene best mulig. Man vil også ha alarmer som utløses dersom enkelte parametere overstiger enn gitt verdi.

Om en uforutsett hendelse skulle oppstå, har senteret mulighet til å sende speidere ut i feltet, i form av trent personell som vil opptre som senterets sanser på plassen, og har muligheten til å fungere enten som redningsmannskap eller som problemløsere. Disse har også med seg utstyr som kreves for ulike operasjoner, og bærer med seg nødvendig verneutstyr og sensorer som forteller operatørene om forholdene der de befinner seg.

Dette inkluderer opptil flere videokamera, mikrofoner og sensorer for eksempelvis gass. Disse speiderne har også med seg enheter for nedlasting av brukermanualer til alt utstyr på plattformen, og kan på denne måten til enhver tid få mest mulig informasjon om det utstyret de jobber med. Dette utstyret vil også kunne benyttes ved vedlikehold slik at man kan til enhver tid kan få relevant data mens man holder på med oppgraderinger. Ved hjelp av tilstandsbasert vedlikehold kan man også planlegge i forkant, slik at man kan gjøre flere vedlikeholdsoperasjoner samtidig. Dette kan strategisk utføres ved et tidspunkt hvor enhetene ikke er i bruk. Dersom deler av plattformen skal stanses eller utføres større vedlikeholdsoperasjoner på, kan man utføre en rekke andre vedlikeholdsoppgaver i samme tidsrom. Dette er mulig siden mange av operasjonene kan gjøres fra leverandørenes kontorer.

Hver plattform er også delt opp i sektorer, og personell som er ute på plattformen bærer med seg en brikke som inneholder personlige opplysninger, samt sender informasjon om hvor hver person befinner seg. Dette er for å raskt få oversikten over hvor mange personer som befinner seg i et område, og om man har bruk for umiddelbar assistanse, kan man påkalle personer som befinner seg i nærheten, istedenfor å vente på personell som muligens befinner seg på en annen side av installasjonen. Disse brikkene inneholder også annen relevant informasjon om personene, som f.eks. helsetilstander (allergier, plager, om personen lider av migrene, epilepsi og lignende). Dette er først og fremst for å gjøre hverdagen mer sikker for disse personene, som oppholder seg i miljøer der det er begrensede fluktmuligheter, og som kan betegnes som relativt farlige.

4.2.2 Hendelsen på Snorre A og mulig IO-scenario.

Hendelsen som skjedde på Snorre A (SNA) den 28. november 2004, er en av de mest dramatiske og potensielt største ulykkene på norsk sokkel. Dette kapittelet gjennomgår deler av hendelsesforløpet, og hvordan ting kunne vært utført dersom Integrerte operasjoner hadde vært implementert i den daglige driften. Etter hvert scenario presenteres de tjenester vi anser nødvendige og aktuelle for gjennomføringen av scenariet. Disse tjenestene forklares mer inngående i slutten av kapittelet.

Kapittelet er basert på en rapport utviklet av Petroleumstilsynet (Ptil), ”Gransking av gassutblåsningen på Snorre A, brønn 34/7-P31 A 28.11.2004” [12]. Rapporten tar for seg hendelsesforløpet i kronologisk rekkefølge og påpeker avvik fra normal prosedyre.

Operasjonen som skulle foregå på SNA kalles for slissegjenvinning og den aktuelle brønnen (P31-A) ble stengt grunnet skader i desember 2003. Ptil fikk våren 2004 informasjon om at planleggingsfasen for slissegjenvinningsoperasjonen var tatt opp.

Hendelse 1 - Planlegging

Våren 2004 ble det satt ned et prosjektlag for planlegging av operasjonen, og på det første møtet fikk programingeniøren i arbeid å hente inn historiske data angående brønnen. Dette ble presentert for SNA RESU (SNA reservoarutvinning) sammen med de tidligere problemene, og de framtidige utfordringene i henhold til planlagt operasjon. I løpet av den første halvdelen av september 2004, ble det holdt detaljplanleggingsmøter sammen med flere kontraktører. Det er verdt å merke seg at boreentreprenøren ikke var delaktig i disse møtene. Det er også verdt å merke seg at det nettopp var blitt byttet boreentreprenør. Den nye boreentreprenøren overtok 80 % av arbeidskraften til den forhenværende.

Scenario 1

Prosjektlagene til både den nye og den tidligere boreentreprenøren deltar via videokonferanse. Den tidligere boreentreprenøren er med for å bidra med erfaringsoverføring til den nye kontraktøren. Dette medfører større flyt av informasjon om brønnen, og problemene som forårsaket den tidligere stengingen. Det er også opprettet et Virtual Reality- eller virtuelt samhandlingsmiljø, hvor brønnen simuleres i 3D, og eksisterende data alt er lagt inn. Dette gjør det lettere for de involverte partene å visualisere utfordringene som teamet står ovenfor.

Tjenester 1

Tj01 - Videokonferanse

Tj02 - 3D simulering og Virtual Reality (VR)

Hendelse 2 - Kansellert møte

"*På det tredje planleggingsmøtet la SNA RESU prosjektlaget planer for:*

- *Punktering av halerør,*
- *Trekking av scab-liner i ett stykke og trekking av denne gjennom BOP*

I tillegg ble potensielle problemer med hullene i 9 5/8" fôringsrør, i forhold til punktering av halerør diskutert, uten at noe av dette ble identifisert som en risiko eller barrierebrudd." [12] Det viser seg i midlertidig senere at dette faktisk var et reelt avvik, da det kunne resultere i et maksimalt reservoartrykk på 325 bar, selv om det fra tidligere var kjent at sekundærbarrieren kun var spesifisert til et trykk på 94 bar.

En risikogjennomgang for hele programmet var også planlagt, men ble utsatt på grunn av at dette kolliderte med andre møter, og ble dermed nedprioritert. Ny dato ble satt for risikogjennomgangen, men denne gangen gikk det heller ikke å avholde møte. Dette møtet ble dermed kansellert. En annen hendelse som oppstod under denne perioden var at når alle deloperasjonene i programmet var gjennomgått og diskutert, endret boreoperasjonsleder signatursiden på det endelige dokumentet. Dette ble endret fra verifisert og godkjent til status anbefalt. Dette var heller ikke i tråd med styrende dokumenter.

Scenario 2

Et felles kunnskapssenter er operativt, og brukes under planlegging og gjennomføring av den daglige drift. Dette senteret har tilgang til 3D VR modeller av alle brønner og annen historisk og geologisk data. Eksperter for forskjellige felter er tilstede og tilgjengelige på dette senteret. Et slikt panel ville ikke godkjent og gitt klarsignal for gjennomføring, med mindre alle krav var oppfylt med hensyn på risikogjennomgang. De ville også påpekt endringene som ble foretatt i signatursiden på programdokumentasjonen. Disse signeres digitalt og lar seg vanskelig endre eller forfalske.

Historiske data vil blitt gjennomgått på senteret. Avvikene i hendelsen kunne således vært unngått, ettersom det ville blitt påpekt at sekundærbarrieren kun var verifisert til et maksimalt trykk på 94 bar.

Tjenester 2

Tj02 - 3D simulering og Virtual Reality (VR)
Tj03 - Digitale signaturer
Tj04 - Globalt tilgjengelig database over brønnhistorikk og geologi

Hendelse 3 - Oppmøteproblemer

Den 16.11.2004 ble det avholdt utreisemøte med dagskiftet, ettersom arbeidet på nabobrønnen gikk raskere enn planlagt, og arbeidet på P-31A ble dermed framskyndt i forhold til original plan. På dette møtet deltok parter som skulle delta i operasjonen, bortsett fra boresjef dag som ikke hadde muligheten til å delta på grunn av flyproblemer. Dette informasjonsmøtet ble holdt ved hjelp av powerpoint-presentasjon.

Scenario 3

Boresjef dag deltar på møtet via videokonferanse. Dette gjøres via WLAN fra flyplassen. Utstyret som kreves for dette er per idag standard i enhver bærbar pc. I det etablerte

kunnskapssenteret gjennomføres visualisering av brønnen i 3D. Potensielle problemer vil da komme tydeligere fram, enn om de ble forklart i powerpoint-slides.

Tjenester 3

Tj01 - Videokonferanse

Tj02 - 3D simulering og Virtual Reality (VR)

Hendelse 4 - Unntakssøknad

"Den 23.11.2004 sendte boreleder dag en e-post til programingeniør med kopi til boreoperasjonsleder. Henvendelsen gjaldt en forespørsel om det krevdes søknad om unntak for utrekking av 7 5/8" scab-liner uten BOP-rams. Programingeniøren svarte samme dag til boreleder: "Slik jeg tolker det slipper vi dette (unntakssøknad) så lenge vi trekker en liner som ikke er ute i åpent hull"" [12]

Scenario 4

Dette svaret vitner om enten usikkerhet i tolkning av styrende dokumenter, eller manglende forståelse av innholdet i styrende dokumenter. Dette er noe man kunne ha henvendt seg til andre personer med, siden usikkerhet rundt emnet var tilstede. Med et kunnskapssenter tilstede og i drift, vil denne feilen unngåes, da personell ved senteret døgnkontinuerlig overvåker driften og operasjoner som foregår offshore. Usikkerheten ville ikke oppstått og avviket ville vært unngått.

Tjenester 4

Tj05 - Døgnkontinuerlig overvåking fra kunnskapssenter

Hendelse 5 - Defekt pakning

"Den 25.11.2004 ble det i landorganisasjonen gjennomført risikoanalyse (HAZOP), for to deloperasjoner i programmet.

HAZOP Nr. 1: Omhandler "Dropp 5 ½" produksjonsrør med 4" straddle". Dokumentet ble godkjent og signert av SNA RESU leder, når det var ferdig.

HAZOP Nr. 2 : omhandler "Perforering og trekking av scab-liner". Dokumentet ble ikke signert/godkjent av SNA RESU leder. " [12]

Arbeidet fortsatte videre i henhold til det planlagte programmet, og den 27.11 ble scab-liner punktert, og brønnen ble dermed observert i en time for gass. Etter dette ble trekkingen av selve scab-lineren påbegynt, og en effekt kalt "U-tube" ble ikke observert,

til tross for at denne i henhold til detaljprogrammet burde gitt en trykkøkning på 32 bar. Det viste seg senere at spydet som festet strengen til scab-lineren hadde ingen eller defekt pakning, hvilket gjorde at denne effekten ikke var mulig å detektere.

Scenario 5

Kunnskapssenteret gjennomfører risikoanalyser sammen med operatørene offshore. Dersom risikoanalysen ikke blir lest, signert og godkjent, kan kunnskapssenteret på land sette en midlertidig stopper for offshoreoperasjonene. Det kreves at dokumentene som er gjeldene i henhold til en operasjon er forstått, og er dermed med på å sørge for en sikker og kontinuerlig drift. Dokumentene signeres digitalt.

Også da trekkingen av scab-lineren ble påbegynt, og de forutsette effektene ikke ble observert, kunne det blitt kjørt simuleringer på kunnskapssenteret som kunne gitt svar på hvorfor disse effektene ikke ble registrert. Man kunne da forutsett at defekt pakning i spydet kunne vært en årsak, men at effekten likevel var tilstede. Ved å simulere brønnen og kjøre mulige scenario i sanntid, kan man lettere sette i gang forbyggende tiltak på et tidlig tidspunkt, for å forhindre at situasjonen utvikler seg.

Systemet vil kunne identifisere potensielle problemer og situasjoner som kan oppstå, basert på både historiske data og logiske slutninger fra en læreprosess som maskinene utfører. De kan så trekke slutninger og komme med anbefalinger til alternative løsninger. Flere og mer nøyaktige nedihullssensorer og tilstandsbasert vedlikehold ville også kunne oppdage at pakningen var manglende eller defekt.

Tjenester 5

Tj02 - 3D simulering og Virtual Reality (VR)
Tj03 - Digitale signaturer
Tj06 - Distribusjon av sensorinformasjon
Tj07 - Fjernstyring av utvalgte deloperasjoner fra kunnskapssenter
Tj08 - AI - Kunstig intelligens
Tj12 - Tilstandsbasert vedlikehold (CBM)

Hendelse 6 - Swabbing fortsetter

"28.11.2004 i perioden fra kl. 0000 til kl. 0215 trakk boremannskapet et borerør (single) men swabbing fortsatte. Boreleder natt valgte å stoppe opp og diskuterte situasjonen med boresjef og boreleder dag. Brønnen ble da igjen forsøkt sirkulert ned gjennom scab-liner og opp ringrommet på utsiden av denne. Det ble observert lavt sirkulasjonstrykk og rask retur av borevæske til overflaten. Dette var en nytt tegn på at spydet ikke hadde

nødvendige pakninger eller at pakningene var defekte, dvs. sirkulasjonen gikk gjennom spydet og ikke gjennom scab-liner. De observerte at brønnen tok slam, dvs. at volumbalansen i brønnen virket tilfredsstillende og det gikk like mye boreslam inn i brønnen som det kom ut.

....

I tidsrommet kl. 0800 – 1530 fortsatte dagskiftet å trekke scab-liner. Swabbing med til sammen ca. 4 m3 volumøkning ble observert og det ble også målt slamtap tilsvarende 31 m3. I dette tidsrommet ble operasjonen observert i kortere og lengre perioder med flowcheck.Brønnen ble igjen tolket til å være stabil og boremannskapet fortsatte å trekke scab-liner etter hver flowcheck.

I løpet av dagen hadde boreleder løpende kontakt med plattformsjef og vakthavende boreoperasjonsleder på land for å informere om utviklingen i brønnen."
[12]

Scenario 6

Da returen av borevæsken og det lave sirkulasjonstrykket ble observert, ville dette med en gang vært en bekreftelse på manglende eller defekte pakninger i spydhodet. Nye simuleringer av væskestrømmer og mulige trykkendringer utføres på kunnskapssenteret, og man vil hele tiden ligge et skritt foran mannskapet. Sensorer på bunnen, i lineren og BOP vil gi data om slamstrømmen i sanntid. Dette vil gi operatørene mer informasjon å jobbe med for å gjøre nødvendige beregninger og mest mulig korrekte simuleringer. En nøkkelfunksjon med Integrerte operasjoner er å kunne ha muligheten til å planlegge fremover og forutse feil før de oppstår.

Kontakt med boreleder på plattformen ville hele tiden vært i sanntid via telefoni- og videotjenester som en del av de integrerte tjenestene. Man har også muligheter for å senke ned og fjernstyre en ROV fra land. Denne kan benyttes dersom man ønsker mer informasjon rundt enkelte punkter ved operasjonen, enn det som blir avdekket av informasjonen sensornettverket og målinger viser. Dette er med på å øke informasjonsflyten rundt en operasjon, og gi tidligere og mer presis informasjon om muligheter og effekter, samt advarsler ved komplikasjoner som kan oppstå.

Tjenester 6

Tj01 - Videokonferanse

Tj02 - 3D simulering og Virtual Reality (VR)

Tj06 - Distribusjon av sensorinformasjon

Tj07 - Fjernstyring av utvalgte deloperasjoner fra kunnskapssenter

Hendelse 7 - Alarmen går

Utover dagen (28.11) fortsatte problemene i brønnen, og utover ettermiddagen var det tema på det faste møtet i plattformledelsen som ble holdt kl. 17.00. Her kom de fram til at den planlagte beredskapsøvelsen, som skulle holdes samme dag, ble avlyst som følge av situasjonen som da hadde oppstått.

Drøye to timer senere, kl. 19.05, kalte plattformsjefen inn til krisemøte om situasjonen. Her ble det besluttet å igangsette en "stille alarm" for å mobilisere beredskapsledelsen.

Klokken 19.14 gikk den første gassalarmen, denne var i kjølevannet til Vigdis kompressorene.

Klokken 19.30 besluttet plattformsjefen å iverksette manuell prosessavstengning, men beholdt hovedkraften. Det ble så foretatt varsling til beredskapsfartøy, Hovedredningssentralen og Ptil i henhold til rutine. Det ble samtidig utløst generell alarm med påfølgende mønstring av personell til livbåter. Personelloversikt (POB) var klar først klokken 20.42, hvilket var langt over kravet på 25 minutter.

Scenario 7

Kontakten og informasjonen mellom plattformledelsen og land er konstant, og begge sider oppdaterer hverandre fortløpende om problemer, hendelser eller tegn på framtidige hendelser. Man har på land kjørt simuleringer over hva feilen kan være og hvordan man skal takle dette. Senteret på land har også oversikt over fartøyer og redningsfarkoster som er innenfor en akseptabel rekkevidde, og disse gis beskjed om å være i beredskap.

Plattformen er delt inn i soner, og hver person har en identifikasjonsbrikke som forteller senteret hvilken sone man er i, og hvor mange som oppholder seg der. Denne informasjonen kan også benyttes i kontrollrommet, for hele tiden å holde oversikt over hvor mange folk man har innenfor de gjeldene sonene. Dette kan brukes ved brann eller gassdeteksjoner, og man kan fastslå tryggeste vei ut for personell i en sone.

Tjenester 7

Tj01 - Videokonferanse

Tj02 - 3D simulering og Virtual Reality (VR)

Tj07 - Fjernstyring av utvalgte deloperasjoner fra kunnskapssenter

Tj09 - Fartøyoversikt i sanntid

Tj10 - Personelloversikt i sanntid

Hendelse 8 - Problemene fortsetter

Utover kvelden går det flere gassalarmer rundt omkring på plattformen, og til flere tider.

Scenario 8

Beredskapspersonellet er utstyrt med digitale ører, øyner og nese, og data sendes i sanntid til kunnskapssenteret. Dette utstyret består av videostrøm som gir direkte visning av området som personen beveger seg i. De er også utstyrt med mikrofon, slik at kommunikasjon og beskjeder kan formidles mellom senteret og personen ute i feltet. En digital nese, som består av sensorer for hydrokarboner og karbonmonoksid, samt målinger for tilstedeværende konsentrasjoner av gasser og stoffer i luften, bæres av personen i form av en vest. Med på denne vesten er også beskyttelsesutstyr og førstehjelpsutstyr, samt annet utstyr som kan brukes ute i feltet. Ved hjelp av sensorbrikken som personen til har med seg, kan man til enhver tid identifisere hvor på plattformen/installasjonen personen befinner seg.

Brann- og gassdetektorer vil være første varslingsmetode. Disse varsler om eksempelvis gass- konsentrasjonen i det området hvor detektoren er installert. Ved å utstyre beredskapspersonell med slikt utstyr, kan man få en sanntidsutforsking fra områdene som detektorene har gitt utslag på, og dermed muligheten til å kartlegge og handle mer effektivt og presist. Disse personene vil også fungere som redningspersonell dersom ulykker skulle oppstå. Ved å koordinere små grupper bestående av to eller tre personer, vil man raskt ha dannet effektive og verdifulle redningsgrupper på plattformen. Ved hjelp av kunnskapssenteret som et overordnet organ, kan data leses fortløpende, og koordinasjon mellom de forskjellige gruppene kan foregå. Samtidig blir også data hentet inn fra overvåkningskamera og detektorer.

For at dette scenariet skal kunne gjennomføres med slike rednings- og overvåkingsgrupper, må disse personene nødvendigvis få multidisiplin opplæring. De må kunne behandle alt fra mindre branner, førstehjelp og lignende. Også kunnskaper om elektroniske og mekaniske systemene på installasjonen vil være en fordel. Personene må da selvsagt også være i relativt god form både fysisk og psykisk.

Tjenester 8

Tj10 - Personelloversikt i sanntid

Tj11 - Digitalt beredskapsutstyr for rednings- og overvåkningsgrupper

4.2.3 Oversikt over IKT-tjenester og -løsninger i et fremtidsscenario

I dette kapitlet oppsummeres de tjenester og løsninger som er identifisert fra scenariet i forrige kapittel. Enkelte tjenester er ikke direkte relatert til scenariet, men vil likevel ha en indirekte innvirkning. For at tjenestene skal være funksjonelle, må enkelte punkter være oppfylt. Disse punktene blir kalt forutsetninger, og er basert på dokumentene "Digital Infrastructure Offshore" [21] og " Integrated Work Processes" [6].

Forutsetninger

F1 – Nødvendig opplæring

Tilstrekkelig opplæring for brukere av IKT systemene, slik at menneskelige feil eller usikkerhet forblir et minimum. Det er som regel uvitenhet eller usikkerhet som er årsaken til brukerfeil. Det er derfor essensielt med en rigorøs og strukturert opplæringsprosess slik at man unngår usikkerhet. Det kan være en fordel med oppfriskningskurs og faste rammer for opplæring av ansatte. De nåværende opplæringsrutinene fokuserer i mindre grad på bred kompetanse innenfor flere felt. Dette vil være nødvendig for at et operasjonssenter skal kunne fungere. Man vil trenge mer breddekompetanse og færre spesialiserte arbeidere.

F2 – Organisatoriske forandringer

Innføringen av Integrerte operasjoner fører med seg store organisatoriske forandringer. Det blir nødvendig å omdefinere ansvarsområder og beslutningsprosesser. Det vil bli en tettere relasjon til land og derfor vil flere avgjørelser bli tatt herfra. Ved innføring av G2 vil også leverandører trekkes inn i denne strukturen.

F3 – Tilgjengelig overføringskapasitet

Utstyr som benyttes må ha tilgang til tilstrekkelig overføringskapasitet, slik det kreves av tjenestene. Ved innføring av Integrerte operasjoner vil mengden av data som sendes og mottas øke formidabelt, og det er en forutsetning at overføringshastigheten for tjenestene er tilstrekkelig.

F4 – Digital infrastruktur

For at utstyr skal kunne få tilgang til den tilgjengelige overføringskapasiteten er det nødvendig at infrastrukturen er utbygd. Følgende forutsettes:

- Trådløs- og radiokommunikasjon er implementert. Trådløst på plattformene og WiMax eller fiberteknologi mellom plattformer og inn til land
- IP/VPN/MPLS basert nettverk over fiber.
- Oljeindustriens systemer er tilpasset den nye infrastrukturen.

F5 – Nødvendig og operativt utstyr

Nødvendig utstyr som benyttes i tjenestene må være tilgjengelig og være operativt. Ved innføring av nye systemer, med økt bruk av for eksempel 3D simulering og multimedia, vil det være nødvendig at datamaskiner og komponenter har tilstrekkelig kapasitet for å kunne utføre de nye tjenestene.

F6 – Tilstrekkelig redundans og stabilitet

Redundans og stabilitet i systemene må opprettholdes og fungere, for å unngå nedetid dersom deler av systemet skulle koble ut.

Tjenester

Tj01 - Videokonferanse

Videokonferanser blir brukt i stor grad idag, og har vært brukt i relativt lang tid. Med ISDNs inntog på 80-tallet, fikk man garanterte overføringshastigheter for komprimert lyd og bilde, og proprietært utstyr for videokonferanse basert på ISDN ble utviklet. Idag kreves det lite utstyr for å sette opp en videokonferanse, man trenger tilknytting til nettverk, en datamaskin, et kamera, samt programvare. Mange bærbare PC'er har idag innebygd kamera, et såkalt "webcam", slik at oppgraderingsbehovet for å få til en videokonferanse forsvinner helt. I bærbart utstyr benyttes ofte WLAN som kommunikasjonsteknologi. Dette medfører at en ikke nødvendigvis behøver noen form for kabling, og kan kommunisere nærmest hvor som helst. For videokonferanse kan det brukes flere ulike protokoller, og H.323 og SIP er de mest vanlige i dag. H.323 er en protokoll som beskriver lyd- og bildekommunikasjon på pakkesvitsjede nettverk. En underprotokoll av denne, H.239, beskriver oppsett av en todelt videostrøm. Dette kan benyttes dersom man ønsker en videokonferanse, hvor man samtidig kan vise for eksempel en presentasjon. I H.323 finnes det også muligheter for å kryptere mediestrømmen [22]. H.323 har bakgrunn fra linjesvitsjede nettverk, mens SIP er en signaleringsprotokoll basert på IP og pakkesvitsjede nettverk. SIP er transportuavhengig

og kan kjøre over UDP, TCP, ATM, osv. SIP er i utgangspunktet en enklere protokoll enn H.323, og er derfor mer brukt i det kommersielle markedet.

Tj02 - 3D simulering og Virtual Reality

3D simuleringer kan utføres ved at datamaskiner samler inn data om brønnhistorikk, geologi, og all annen aktuell data, og med hjelp av dette lager et tre-dimensjonalt bilde av området som skal simuleres. Disse simuleringene kan f.eks. brukes for å iaktta en boreoperasjon i sanntid, hvor man samtidig får informasjon om mulige komplikasjoner før de eventuelt oppstår. Simuleringer kan også brukes som en forberedende øvelse i forkant av en planlagt boreoperasjon, eller som en generell øvelse for opplæring. Her ser vi for oss at man kan plotte inn fiktive feil som skal oppstå under øvelsen, slik at man best mulig kan forberede seg dersom de faktisk oppstår.

Ved å benytte virtuelle samhandlingsmiljøer, har man mulighet til visualisering basert på VR. Her kan man for eksempel ”skape” en plattform hvor man virtuelt kan bevege seg rundt og observere. Dette kan være et samarbeidsmiljø hvor flere eksperter kan sammen løse problemer, og ved hjelp av visualiseringen kan de få et bedre bilde av de faktiske forhold, enn man kan ved å se på en statisk modell og kommunisere via telefon. Det finnes nær sagt ingen grenser for hvilke miljø man kan opprette for slike virtuelle verdener. Innenfor Integrerte operasjoner, vil f.eks. en brønn være et aktuelt miljø.

Tj03 - Digitale signaturer

Digitale signaturer brukes for autentisering, man skaper en sikkerhet mellom identitet og påstått identitet. Vi ser for oss at man her kan benytte seg av en sikkerhetsenhet, f.eks. et smartkort, samt et passord for å godkjenne og signere dokumenter. Dette vil ikke bare sørge for en sikker autentiseringsprosess, men vil også sørge for såkalt ikke-fornektelse (eng. non-repudiation). Dette vil si at man skaper en verifikasjon på at signaturen faktisk kommer fra den som står som undertegnede, slik at man ikke kan nekte for dette i ettertid. Tjenesten vil benytte seg av PKI (Public Key Infrastructure). X.509 er en standard som vil være hensiktsmessig å benytte her. Standarden beskriver bl.a. oppbygningen til sertifikatene, og er den mest brukte innen PKI.

Tj04 - Globalt tilgjengelig database over brønnhistorikk og geologi

Denne tjenesten sørger for at databaser som inneholder brønnhistorikk og andre relevante data vil være tilgjengelig fra hvor som helst i verden. Disse dataene er lagret i et standardformat, slik at man ikke er avhengig av et proprietært system for å hente ut informasjon. Mulige standarder for dette er ISO15926, POSCs EPICENTRE, WITSML og OWL. Databasene vil i hovedsak benyttes av kunnskapssenteret og personell offshore,

men kan også gjøres tilgjengelig for ekstern ekspertise, slik som f.eks. leverandører og andre aktuelle aktører.

Tj05 - Døgnkontinuerlig overvåking fra kunnskapssenter

Kunnskapssenteret er bemannet med godt opplærte og erfarne personer som til enhver tid kan bistå personene offshore. Dersom det er usikkerhet i henhold til en operasjon vil man kunne kontakte senteret med den aktuelle problemstillingen, og få en respons basert på en best mulig beslutningsprosess. Dette senteret vil kunne bistå med eksperter innen regelverk og teknisk sikkerhet. Senteret vil også overvåke operasjonene, og dersom de mener det blir gjort forhastede og dårlige beslutninger, kan de gripe inn.

Tj06 - Distribusjon av sensorinformasjon

Flere og mer avanserte sensorer vil bli plassert på installasjonen. Tidligere har informasjonen fra disse sensorene i hovedsak vært tilgjengelig for operatrørene offshore, men vil nå også distribueres til kunnskapssenteret på land og andre involverte aktører.

Tj07 - Fjernstyring av utvalgte deloperasjoner fra kunnskapssenter

Det vil være mulig å styre de fleste operasjoner fra land. Et eksempel kan være at man er usikker på status til en komponent under vann og ønsker og sende ned en ROV for å undersøke denne. For ikke å oppta ressurser fra oljeplattformen, kan man styre denne fra kunnskapssenteret. Der vil man sitte med all informasjon om komponenten som skal utforskes, noe som gjør beregninger og eventuelle skader lettere å oppdage, siden man vil ha fått en indikasjon om hva som kan være feil.

Tj08 - AI (kunstig intelligens)

Kunstig intelligens er en teknikk som brukes for å gi datamaskiner et tilnærmet menneskelig opplæringsevne. En teknikk som tilnærmer seg denne tankegangen i dag er maskinlæring. Dette vil kunne benyttes som et beslutningsstøttesystem ved komplekse situasjoner. Ved å gi en datamaskin tilstrekkelig med historiske data fra situasjoner, og løsninger på disse, vil maskinen kunne komme med et forslag til hva nye problemet kan være og hvordan disse kan løses. Å se all tidligere informasjon i sammenheng vil være tilnærmet umulig for et menneske, og i pressede situasjoner kan et slikt system være med på å finne årsak til problemene som oppstår. I fremtiden vil kunstig intelligens omfatte flere og større områder og vil sannsynligvis være mer aktivt brukt og til større hjelp i olje- og gassnæringen. De mest utbredte tilnærmingene til kunstig intelligens idag er maskinlæring og ”nevrale nettverk”. Ved maskinlæring vil man ”belønne og straffe” systemet, og systemet vil dermed bygge opp en form for erfaring, basert på den gitte straffen eller belønningen. Ved nevrale nettverk bygger man opp et datamønster som

etterlikner den som finnes i den menneskelige hjerne. Det bygger på flere noder eller nevroner som arbeider sammen for å produsere en funksjon. Dette er i motsetning til maskinlæring, hvor læreegenskapene baseres på programmeringsalgoritmer.

Tj09 - Fartøyoversikt i sanntid

På kontrollsenteret og kunnskapssenteret har man mulighet for å få opp en digital tavle som i sanntid innehar informasjon om lokasjon og tilgjengelighet på beredskapsfartøy og helikoptre, som er i nærheten. Dermed kan disse få beskjed om å holde seg klare til utrykning. Det vil også være mulig å se informasjon om hvor lang tid det vil ta for aktuelt fartøy eller helikopter å komme til unnsetning. GPS og WiMax er teknologier som kan benyttes til dette. GPS kan anvendes for å fastslå posisjonen, og når fartøyet er innenfor rekkevidde, kan WiMax benyttes for overføring av informasjon om posisjonen og andre data, slik som f.eks. drivstoffmengde, last, o.l.

Tj10 - Personelloversikt i sanntid

Personell som befinner seg på plattformen bærer en identifikasjonsbrikke som sender informasjon om hvilken sone personen befinner seg i. Denne informasjonen kan brukes til å opplyse om hvor mange og hvem som befinner seg i hver sone. Dersom det skulle bli brann eller gasslekkasjer, kan man få kvalifisert personell i nærheten til å undersøke området. Man kan også lettere fastslå tryggeste vei ut for personell som befinner seg i utsatte områder. Identifikasjonsbrikken kan baseres på RFID (Radio Frequency Identification). Her vil det være hensiktsmessig å benytte seg av såkalte aktive brikker i VHF-båndet. Disse har en relativt lang rekkevidde, og kan lagre en del informasjon. Aktive RFID-brikker har, i motsetning til passive, en egen strømkilde, slik at rekkevidden øker betraktelig. ISO 18000-7 er en standard for aktive RFID-brikker, og vil kunne være et utgangspunkt for denne typen løsninger.

Tj11 - Digitalt beredskapsutstyr for rednings- og overvåkingsgrupper

Tjenesten består av en vest beredskapspersonell tar på seg. Denne vesten kommuniserer med kunnskapssenteret, og gir visuelle bilder via et kamera, lyd og kommunikasjonsmuligheter gjennom mikrofon og øreprop, og sensorer som gir informasjon om konsentrasjon av gass eller lignende. Dette fører til at kunnskapssentrene får et mer detaljert innblikk til de faktiske forhold. Sensorene vil kunne gi mer informasjon om situasjonen, enn en vanlig person kan gi. Kunnskapssenteret har mulighet til å fortløpende gi instrukser til beredskapspersonell om reparasjoner og skadebegrensende arbeid. Det vil også være mulighet til å sende beredskapspersonell digitale manualer og instruksjoner, som disse kan få fram på en skjerm tilknyttet beredskapsutsyret. Et prosjekt som har tatt for seg de grunnleggende

funksjonene (kamera, radiokommunikasjon og trådløs nettverk) er alt tilgjengelig i et produkt som heter visiWEAR som leveres av Monitor System Scotland Limited [23].

Tj12 - Tilstandsbasert vedlikehold (CBM)

CBM står for "Condition Based Maintenance", oversatt til norsk benyttes ofte utrykket tilstandsbasert vedlikehold. Ved kalenderbasert vedlikehold vil utstyr enten repareres eller byttes ut ved feil, eller ved gitte serviceintervaller. Ved tilstandsbasert vedlikehold benytter man sensorer for å registrere bestemte parametere ved utstyr. I dag benyttes CBM hovedsakelig ved større roterende utstyr, eksempelvis turbiner, kompressorer og pumper. I framtiden ser man for seg at CBM også kan benyttes ved andre typer utstyr. Eksempler på parametere som måles ved utstyret kan for eksempel være temperatur, vibrasjoner, lyd og slitasje. System1 fra Bently Nevada [25] er et CBM-system som allerede idag overvåker en rekke parametere på norsk sokkel. [26]

Tj13 - Aksesskontroll

Aksesskontroll benyttes for å delegere tilgang til ressurser i systemet. Det dekker både autentisering, som forteller hvem som har tilgang, og autorisering som sier noe om hvilke ressurser man har tilgang til. I hovedsak skal aksesskontroll hindre uautorisert tilgang til ressurser. Det vil si at brukere ikke skal ha tilgang til mer enn det man trenger for å utføre den aktuelle jobben. For Integrerte operasjoner vil det være hensiktsmessig å benytte seg av RBAC. RBAC definerer roller med hensyn på hvilken stilling man har og hvilken oppgave man skal utføre, og er dermed enklere og administrere og kontrollere i større distribuerte nettverk.

Tj14 - Programvare for håndtering av distribuert informasjon

Ved innføring av IO, vil programvaren som håndterer distribuert informasjon spille en viktig rolle for fremføring og presentasjon av data. Siden mengden data kan være formidabel, og mye av denne er irrelevant for normal drift, må man unngå at operatørene "drukner" i informasjon. Det man derimot ønsker er at operatøren skal ha oversikt over sensordata, f.eks. hvor sensoren er plassert, om verdiene over- eller understiger gitte predefinerte kriterier, eller om en alarm utløses. I krisesituasjoner vil det være nødvendig å kunne hente ut data som omhandler krisen, slik at denne blir håndtert på best mulig måte.

Tj15 - Sikkerhetstiltak i nettverk

Nettverkssikkerhet er ikke en tjeneste alene, men heller et sett med tjenester, tiltak og kontrollmetoder i forbindelse med kommunikasjonsnettverk. Tjenestene inkluderer

brannmurteknologi, IDS/IPS (Intrusion Detection/Prevention System), VLAN (Virtual Local Area Network), anti-virus programvare, o.s.v.

4.2.4 Sikkerhetstrusler

Med utgangspunkt i de overnevnte tjenestene, har vi kunnet identifisere de vesentligste truslene knyttet opp mot disse. Tabell 1 viser sammenhengen mellom trusler og tjenester.

Tr01 - Avlytting av datatrafikk

Begrepet benyttes om en person med uærlige hensikter som fanger opp elektromagnetiske signaler som sendes via kommunikasjonskabler eller i luft.

Tr02 - Man-in-the-middle

En inntrenger kan maskere seg som et nettverkselement mellom to kommuniserende parter og avlytte eller endre datatrafikken imellom dem.

Tr03 - Identitetstyveri/maskerade

En inntrenger kan benytte seg av en annen persons identitet for å tilegne seg eller endre informasjon som vedkommende i utgangspunktet ikke har tilgang til.

Tr04 - Fysisk tyvlytting/tyvtitting

En person med uærlige hensikter kan f.eks. avlytte videokonferanser som foregår i det offentlige rom, eller tyvtitte på terminaler ved for eksempel bedriftsbesøk.

Tr05 - Malware

Malware er ondsinnet kode som kan gi tilgang til informasjon og data som man normalt ikke har tilgang til. Dette kan gjøres ved at malwaren inneholder kode som enten åpner for utvendig tilkobling, eller sender data tilbake til inntrengeren. Malware kan også endre data, eller gjøre data eller ressurser utilgjengelig.

Tr06 - Forfalskning av sikkerhetsenhet

Sikkerhetsenheter kan stjeles eller forfalskes og benyttes slik som den originale enheten. Dette kan gi tilgang til ressurser og konfidensiell informasjon som uautoriserte personer kan tilegne seg eller endre.

Tr07 - Social engineering

Teknikker brukt for å manipulere mennesker til å utføre visse handlinger, eller oppgi informasjon.

Tr08 - Smugling av stjålne data

Autorisert personell med uærlige hensikter kan smugle ut konfidensiell informasjon fra sin arbeidsplass.

Tr09 - Manipulering av data

Data som er produsert kan endres eller slettes av autoriserte personer med uærlige hensikter.

Tr10 - Tjenestenektangrep

Tjenestenektangrep benytter seg av metoder for å oppta ressurser, slik at disse blir utilgjengelige for brukere eller maskiner.

Tr11 - Fysisk sabotasje

Personer med uærlige hensikter kan fysisk sabotere IKT-utstyr med intensjon om å gjøre ressursene utilgjengelige.

Tr12 - Brukerfeil

En autorisert bruker kan utføre utilsiktede handlinger som er skadelige.

Tr13 - Misbruk av privilegier

En autorisert bruker med privilegier kan utføre ondsinnede handlinger med intensjon om å skade eller ødelegge systemer. Vedkommende kan stjele konfidensiell informasjon, endre eller gjøre denne utilgjengelig.

Tr14 - Logisk innbrudd

En inntrenger kan bryte seg inn i systemer v.h.a. ulike angrepsmetoder, og tilegne seg konfidensiell informasjon, endre eller gjøre denne utilgjengelig.

Liste over tjenester:

Tj01	Videokonferanse
Tj02	3D simulering og Virtual Reality
Tj03	Digitale signaturer
Tj04	Globalt tilgjengelig database over brønnhistorikk og geologi
Tj05	Døgnkontinuerlig overvåking fra kunnskapssenter

Tj06	Distribusjon av sensorinformasjon
Tj07	Fjernstyring av utvalgte deloperasjoner fra kunnskapssenter
Tj08	AI (kunstig intelligens)
Tj09	Fartøyoversikt i sanntid
Tj10	Personelloversikt i sanntid
Tj11	Digitalt beredskapsutstyr for rednings- og overvåkingsgrupper
Tj12	Tilstandsbasert vedlikehold (CBM)
Tj13	Aksesskontroll
Tj14	Programvare for håndtering av distribuert informasjon
Tj15	Sikkerhetstiltak i nettverk

Tabell 1: Relasjon mellom trusler og tjenester

Trussel	Navn	Tjenester
Tr01	Avlytting av datatrafikk	Tj01, Tj04, Tj05, Tj06, Tj07
Tr02	Man-in-the-middle	Tj01, Tj04, Tj05, Tj06, Tj07
Tr03	Identitetstyveri	Tj01, Tj03, Tj13
Tr04	Fysisk tyvlytting	Tj01
Tr05	Malware	Indirekte alle
Tr06	Forfalskning av sikkerhetsenhet	Tj03, Tj13
Tr07	Social Engineering	Tj13
Tr08	Smugling av stjålne data	Tj04, Tj14, Tj15
Tr09	Manipulering av data	Tj04, Tj06, Tj12, Tj14
Tr10	Tjenestenektangrep	Indirekte alle
Tr11	Fysisk sabotasje	Indirekte alle
Tr12	Brukerfeil	Tj02, Tj05, Tj07, Tj11, Tj12, Tj14, Tj15
Tr13	Misbruk av privilegier	Tj03, Tj05, Tj07, Tj13, Tj15
Tr14	Logisk innbrudd	Tj04, Tj13, TJ15

For å få en oversikt over truslene, og hvordan de representerer farer, har vi valgt å kategorisere de i konfidensialitet, integritet og tilgjengelighet. Av tabell 2 fremgår det hvilken kategori truslene primært er brudd på.

Et brudd på konfidensialitet vil si at inntrengeren vil få tilgang til data som han i utgangspunktet ikke ville hatt tilgang til. Dette kan medføre lekkasje av f.eks.

bedriftshemmeligheter, som videre kan medføre svikt i grunnlaget for bedriftens eksistens.

Brudd på integritet medfører at data blir ugyldige og ukorrekte, f.eks. ved at en inntrenger endrer data. Denne type brudd kan blant annet medføre feil beslutningsgrunnlag for avgjørelser.

Brudd på tilgjengelighet medfører at data, tjenester og ressurser ikke lengre er tilgjengelige. Dette kan eksempelvis forårsakes av overbelastning av nettverk som følge av tjenestenektangrep.

Tabell 2: Klassifisering av trusler

Trusler	Brudd på konfidensialitet	Brudd på integritet	Brudd på tilgjengelighet
Tr01 - Avlytting av datatrafikk	✓		
Tr02 - Man-in-the-middle	✓	✓	
Tr03 – Identitetstyveri/ maskerade	✓	✓	
Tr04 – Fysisk tyvlytting/ tyvtitting	✓		
Tr05 – Malware	✓	✓	✓
Tr06 – Forfalskning av sikkerhetsenhet	✓	✓	
Tr07 – Social Engineering	✓	✓	
Tr08 – Smugling av stjålne data	✓		
Tr09 – Manipulering av data		✓	✓
Tr10 – Tjenestenektangrep			✓
Tr11 – Fysisk sabotasje			✓
Tr12 – Brukerfeil	✓	✓	✓
Tr13 – Misbruk av privilegier	✓	✓	✓
Tr14 – Logisk innbrudd	✓	✓	✓

Tabell 3 viser sammenhengen mellom truslenes sannsynlighet og konsekvens. Sannsynlighet er hvor hyppig en hendelse inntreffer, og konsekvensen er alvorlighetsgraden dersom hendelsen faktisk inntreffer. Tabellen er basert på egen vurdering og tar utgangspunkt i at policyene er fulgt. Vi har definert kategoriene på følgende vis:

Sannsynlighet:

Liten

Forekommer sjeldent og estimeres til et tilfelle per år eller sjeldenere

Kan forekomme

Begrenset antall, estimert til 2-4 tilfeller i året.

Vanlig

Forekommer relativt ofte, estimert til et tilfelle i måneden eller oftere.

Konsekvens

Liten

Medfører minimale og opprettelige skader på aktiva.

Middels

Medfører moderate og opprettelige økonomiske tap.

Alvorlig

Medfører tap av sensitive data og bedriftsomdømme. Kan medføre store økonomiske tap.

Katastrofal

Medfører tap av menneskeliv eller betydelige og uopprettelige økonomiske tap.

Tabell 3: Sannsynlighet og konsekvens

		Sannsynlighet		
		Liten	Kan forekomme	Vanlig
Konsekvens	Liten			Tr04
	Middels	Tr01, Tr02	Tr07, Tr09, Tr12	
	Alvorlig	Tr03, Tr06, Tr10, Tr11, Tr14	Tr05, Tr08	
	Katastrofal	Tr13		

4.3 IT-sikkerhetspolicy

Sikkerhetspolicyene er inkludert i vedlegg 1, og er delt inn i temaer for ulike teknologier og områder. På denne måten vil policyene være enklere å vedlikeholde og oppdatere, og den overordnede informasjonssikkerheten vil bedre kunne ivaretas.

Policyene er produsert i henhold til NS-ISO/IEC 17799, som er en informasjonssikkerhetsstandard utviklet av ISO (Den internasjonale standardiseringsorganisasjonen), og IEC (Den internasjonale elektrotekniske kommisjon). Den ble fastsatt som norsk standard i 2005, og den norske oversettelsen ble utgitt i februar 2006. Fremtidige utgaver av ISO/IEC 17799 er forslått innarbeidet i en serie av internasjonale standarder for informasjonssikkerhet, og utgaven i 2007 vil i såfall bli hetende ISO/IEC 27002:2007. [11]

Det er tatt hensyn til OLFs anbefaling nr. 104, ”Information security baseline requirements for process control, safety and support ICT-systems” [10], og sikkerhetspolicyene er i all hovedsak basert på denne anbefalingen. I dette dokumentet har OLF utarbeidet retningslinjer og anbefalinger for å forbedre den generelle informasjonssikkerheten i oljenæringen. Med dette ønsker OLF å øke sikkerhet og kontinuitet i operasjonene på norsk sokkel. [10]

Policyene i dette vedlegget er ikke nummerert i henhold til viktighet, men det er viktig å merke seg at enkelte policyer er mer relevant i forhold til vår oppgave, enn andre. Mindre relevante policyer er likevel utarbeidet og vedlagt, ettersom vi mener dette bedre vil kunne skape et helhetlig bilde av den overordnede IKT-sikkerheten. Uten disse vil det kunne oppstå mangelfulle forestillinger om hva som kan ansees sikkert innenfor IKT.

Uttrykkene informasjonssikkerhet og IT/IKT-sikkerhet blir i policyene benyttet om hverandre, og bygger på konfidensialitet, integritet og tilgjengelighet av informasjon. I policyene omtales også SAS-systemer (Safety and Automation System). Som tidligere nevnt er dette systemer som foretar monitorering, logisk kontroll og vernetiltak ombord på installasjonen [20]. Brann- og gass-systemene Origo leverer tilhører SAS.

Tabell 4 viser policyenes dekningsgrad i forhold til truslene Tr01 - Tr14

Liste over policyer:

P01. Akseptabel bruk policy
P02. Akseptabel kryptering policy
P03. Elektronisk post policy
P04. Passord policy
P05. Policy om aksesskontroll
P06. Policy om antivirus
P07. Policy om fjerntilgang
P08. Policy om fysisk sikring
P09. Policy om logisk sikring
P10. Policy om nettverkssikkerhet og –topologi
P11. Policy om sensitiv informasjon
P12. Policy om sikkerhetskopiering
P13. Policy om trådløs kommunikasjon
P14. Sikker drift policy

Tabell 4: Dekningsgrad i policyer

Trussel	Navn	Policy
Tr01	Avlytting av datatrafikk	P02, P04, P07, P08, P10, P11, P13
Tr02	Man-in-the-middle	P02, P04, P07, P08, P10, P11, P13
Tr03	Identitetstyveri/ maskerade	P02, P04, P08, P11
Tr04	Fysisk tyvlytting/ tyvtitting	P01, P04, P08, P11
Tr05	Malware	P01, P03, P06, P07, P12, P14
Tr06	Forfalskning av sikkerhetsenhet	P01, P02, P08
Tr07	Social Engineering	P01, P03, P04, P11
Tr08	Smugling av stjålne data	P08, P11
Tr09	Manipulering av data	P12, P14
Tr10	Tjenestenektangrep	P10
Tr11	Fysisk sabotasje	P08, P12, P14
Tr12	Brukerfeil	P09, P14
Tr13	Misbruk av privilegier	P05, P08
Tr14	Logisk innbrudd	P02, P04, P05, P10, P11, P13

4.4 Forslag til løsninger for implementering

4.4.1 RBAC

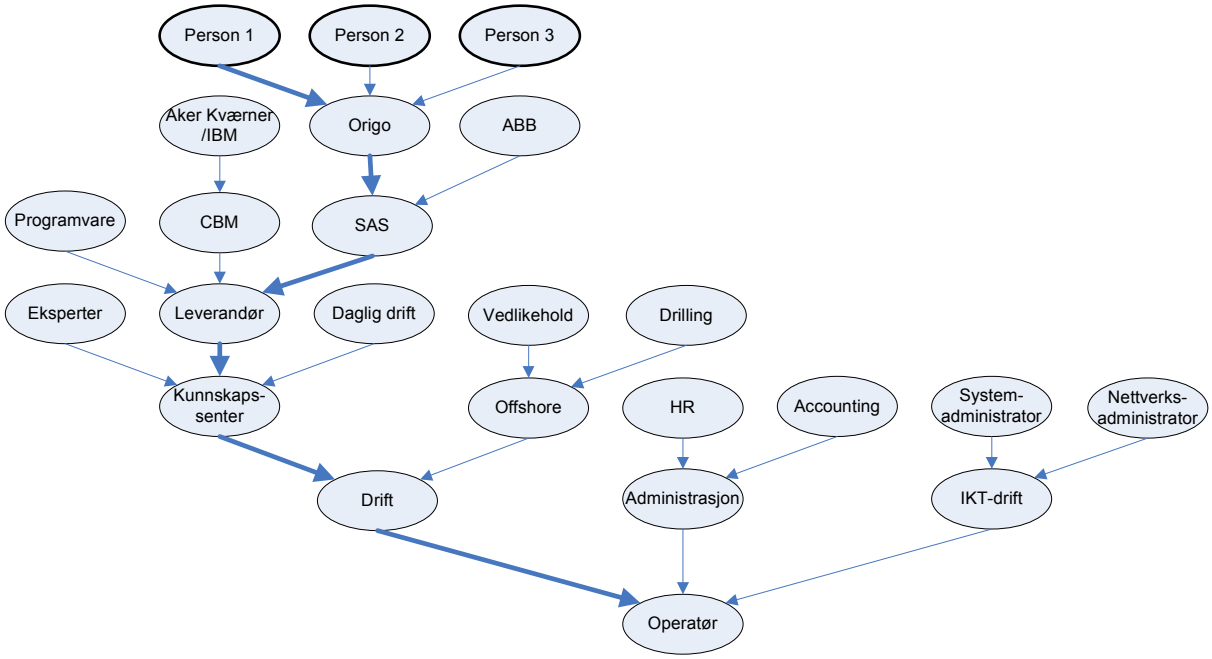
En av de store utfordringene ved implementering av Integrerte operasjoner vil være å kontrollere rettighetene til ressurser for brukerne. Dette er en ressurskrevende jobb når omfanget blir så stort som Integrerte operasjoner tilsier. Det vil være essensielt at dette kontrolleres på en slik måte at man ikke mister oversikt og at brukere ikke får tilgang til mer enn de har behov for. Ved å benytte seg av RBAC vil man ha mulighet til å definere roller, gi disse rollene rettigheter og videre tilegne brukerne roller. Det vil dermed bli lettere å holde kontroll over hvilke rettigheter de forskjellige brukere har.

RBAC støtter muligheten for å arve rettigheter fra underliggende roller, det betyr at man kan definere færre roller enn ellers. For eksempel kan man definere en rolle som heter leverandører og her gi generelle rettigheter som gjelder for alle leverandører. Deretter kan man videre spesifisere mer konkrete roller ut i fra hva denne leverandøren leverer. Dette muliggjør at man senere kan tildele eller frata leverandører rettigheter kun ved å endre denne ene rollen.

Muligheten for å kunne begrense antall roller en bruker kan ha samtidig er med på å sikre at man ikke skal ha tilgang til mer enn man har behov for. RBAC kan forhindre konflikter ved to motstridende roller, og gjør i disse tilfellene at man bare kan være tilegnet flere roller dersom de ikke er motstridende.

Case studiet "The Role Based Access Control System of a European Bank: A Case Study and Discussion" [24] beskriver et RBAC-system brukt i en hovedbank i Europa. Her var det i 2001 ca. 40000 brukere og 1300 definerte roller. Dette systemet behandler i gjennomsnitt 42000 roller hver dag og bruker ca. 85ms for å kunne avdekke en individuell rolle, og systemets tilgjengelighet er 99 % per år. Systemet har vært brukt i over et tiår, og viser at det er sannsynlig at et slikt system vil kunne benyttes i Integrerte operasjoner.

Figur 8 viser en begrenset RBAC struktur og gir et innblikk i mulighetene ved å benytte seg av rollehierarki i oljenæringen etter innføringen av Integrerte operasjoner.



Figur 8: En begrenset RBAC struktur

Figuren leses slik at person 1 er medlem i Origo, Origo er medlem i SAS, SAS er medlem i Leverandør osv. Medlemskap går nedover mens rettighetene går oppover.
Når person 1 får rollen Origo vil den automatisk arve rettigheter og roller nedover. Dette forenkler måten å behandle aksesskontrollen på. Man kan også tenke seg at en person i Origo blir kalt inn som ekspert i en gitt sak og man kan da lett gi denne personen rollen Eksperter slik at han får rettigheter som er tilegnet denne rollen.

4.4.2 Semantisk web

For at andre generasjon av Integrerte operasjoner skal kunne implementeres og benyttes mest mulig effektivt og i henhold til visjonene, må standarder for elektronisk deling av informasjon mellom selskaper og disipliner etableres [4]. Dette er for å oppnå at informasjonen blir delt på en effektiv og sikker måte. Om informasjon er tilgjengelig, men vanskelig å oppdrive, vil dette medføre at den ikke vil bli benyttet i like stor grad som er ønskelig. Ifølge rapporten ”eDrift på norsk sokkel år 2010” [4] fra OLF, ligger utfordringene i innføring av slike systemer i en felles etablering av syntakser og semantikk. Det har i de senere årene blitt utviklet standarder innenfor industrien både for språk og arbeidsprosesser. Disse har bidratt betydelig til standardisering av semantikken, men har vist seg vanskelige å implementere og ført til uheldige frysninger av arbeidsprosesser.

Ved å kombinere disse standardene fra industrien selv, med de foreslåtte standardene for semantisk web og ontologier fra W3C, mener vi at systemene kan implementeres på

en lettere måte. Man vil kombinere velkjente teknologier, og gjøre muligheten for å bygge en database over relasjoner til arbeidsprosesser, teknologier og utstyr som eksisterer på norsk sokkel per idag og i fremtiden. OLFs rapport påpeker et par problemer. Det ene problemet identifiseres som " *ISO-standarden må utvides til å inkludere begrepene i POSCs EPICENTRE- og WITSML- standardene*" [4]. Dette er mulig å løse ved å implementere begrepene alt idag under et temporært datasett, for så å benytte seg av ontologier for å linke dette datasettet til de standariserte med en gang det foreligger en slik felles standard.

En slik implementasjon for distribusjon og regler for relasjoner, vil kunne benyttes på mange områder. Eksempelvis kan det benyttes i tjenesten Tj12 - Tilstandsbasert vedlikehold (CBM), hvor det kan være et verktøy for å skape relasjoner mellom komponenter, produsenter og leverandører. Et annet sted det kan implementeres, er Tj04 - Globalt tilgjengelig database over brønnhistorikk og geologi. Her vil man kunne benytte den eksisterende informasjonen om brønner som et referansepunkt. Om man eksempelvis søker etter en spesifikk brønn, vil man også enkelt kunne finne informasjon om egenskapene til brønnen. Hva slags sensorer som er tilstede, hvem leverandørene av disse sensorene er, hvor lenge de har vært i drift og hva slags problemer som har blitt rapportert, er eksempler på slik informasjon. Ved full implementering av G2 vil man også ha muligheten til å gå motsatt vei. Om en leverandør finner en feil ved noe av sitt eksisterende utstyr, og anser dette som kritisk, vil man ha muligheten til å søke etter f.eks. utstyrets versjonsnummer, og se hvor utstyret som inneholder denne feilen er installert, og hvor det er planlagt installert i nær framtid. På denne måten kan leverandøren selv rapportere til driftorganisasjonen om hvilke komponenter som krever utskiftning.

4.4.3 Digitale signaturer i Integrerte operasjoner

I tjeneste Tj03 - Digitale signaturer, kreves det en type sikkerhetsenhet i kombinasjon med et passord for å bl.a. signere dokumenter. Dette gjøres for hindre såkalt "repudiation", eller nektelse på norsk. En må sørge for at dokumenter er signert og godkjent av den rette vedkommende, og at denne ikke kan nekte for å ha gjort dette i ettertid. Ved bruk av tjenesten "digitale signaturer", vil dokumenter som er signert av en person kunne bevises å være signert av denne personen, ettersom det kun er han eller hun som innehar sikkerhetsenheten og passordet. På denne måten kan man hindre ansvarsfraskrivelse, og en sørger også for å skape forsikring om hvem som har skrevet under.

Smartkort vil være et godt alternativ som sikkerhetsenhet, da disse tilbyr relativt god sikkerhet, de er små og lette å bære med seg, og ikke minst, de er billige. Vi ser for oss at ved å benytte smartkort for signering og godkjenning av dokumenter innenfor Integrerte operasjoner, vil man samtidig kunne benytte smartkortet for en rekke andre sikkerhetsrelaterte oppgaver. Som adgangskort vil smartkort fungere fullgodt, idag får man også kombinerte smartkort og RFID-kort (Radio Frequency Identification), som mange eksisterende adgangskort er basert på. Smartkort vil også kunne benyttes i påloggingssituasjoner for terminaler og arbeidsstasjoner, eller for godkjenning av utført vedlikehold eller reparasjoner.

4.4.4 Distribusjonstjeneste for policyer

Vi foreslår en tjeneste for å kunne distribuere policyer til brukere som har fått tildelt roller i RBAC. Policyer vil bli linket opp mot de eksisterende rollene i RBAC, og når en bruker får tildelt en ny rolle, vil brukeren automatisk motta policyen(e) relatert til den gitte rollen, hvis dette eksisterer. Enkelte policyer gjelder for alle brukere uansett rolle, og disse vil distribueres ved førstegangs inntreden i systemet.

Metoden for distribusjon vil vi ikke gå inn i detalj, men det finnes mange måter å løse dette på. En metode kan være å benytte en meldingstjeneste som gir beskjed straks en eller flere nye policyer er aktuelle. Personen får da beskjed om å gå inn i bedriftens intranett via en webleser. Her vil alle tidligere policyer også ligge til enhver tid for senere opplysning. Brukeren vil her få beskjed om å lese igjennom og gjøre seg forstått med policyen, og deretter signere den ved hjelp av passord og smartkort i den tidligere nevnte tjenesten ”digitale signaturer”. Ved signering bekrefter brukeren at denne har lest og forstått policyen, og at han eller hun forplikter seg til å følge den. Først når dette er gjort vil brukeren få tilgang til eventuelle nye tjenester og privilegier tilknyttet rollen. Dersom policyer blir revidert og oppdatert, vil disse distribueres til alle som var omfattet av den tidligere policyen.

4.4.5 Felles kontaktpunkt for rapportering av sikkerhetshendelser

Et felles kontaktpunkt for rapportering av sikkerhetshendelser og -brudd vil gjøre det lettere for ansatte å gi beskjed, dersom de oppdager brudd på informasjonssikkerheten. Dette kan være en e-postadresse og et telefonnummer. Det kan også implementeres i den tidligere nevnte distribusjonstjenesten for policyer. Mange sikkerhetshendelser vil ignoreres på grunn av usikkerhet om hvor man skal henvende seg angående dette. Kontaktpunktet bør informeres til samtlige ansatte med jevne mellomrom, og de ansatte bør opplyses om viktigheten av rapportering og at dette gjøres umiddelbart.

5 Diskusjon

5.1 Metodekritikk

Vi tar utgangspunkt i et hendelsesforløp og baserer scenariene våre på dette. Dette kan medføre at man får et begrenset innblikk i boreoperasjonen, og dermed ikke tar høyde for alle deler av et hendelsesforløpet. Her kunne det vært hensiktsmessig å trekke inn rapporter og beskrivelser av andre operasjoner, for å få et mer fullstendig bilde. Det kunne også vært hensiktsmessig med innspill fra personer som jobber i oljenæringen offshore, og som dermed har en god forståelse av hvordan slike operasjoner gjennomføres.

Et alternativ til scenariometoden kunne vært å basere løsningen kun på dokumenter skrevet om emnet. Dette ville muligens kunne avdekket flere av truslene, men ved å kombinere denne kunnskapen med scenarier fikk vi identifisert enkelte tjenester som ikke er omtalt tidligere. Intervjuer kunne også vært benyttet for å innhente informasjon. Dette ville vært en omfattende prosess og ville krevd mer tid eller andre avgrensninger i oppgaven. Vi ser også for oss at en grundig risikoevaluering vil være nødvendig for å kunne få et komplett bilde av trusler ved tilpassning av SAS-systemer til Integrerte operasjoner.

Med dette utgangspunktet mener vi at det viste seg hensiktsmessig å benytte seg av scenario som metode for å avdekke trusler, slik vi har gjort i denne rapporten. Tatt i betraktning tidsbegrensningen og vår kunnskap om emnet før oppstart, mener vi scenariometoden har gitt oss et godt utgangspunkt for identifiseringen av trusler. Ved hjelp av scenario fikk vi avdekket hvilke tjenester vi har sett for oss er en del av Integrerte operasjoner, og på denne måten var det mulig å lage en ramme rundt det noe diffuse begrepet IO. Da tjenestene var avdekket, ble det ut fra dette mulig å identifisere trusler som utgjør en risiko mot de avdekkede tjenestene. Her er det viktig å merke seg at det i fremtiden mest sannsynlig vil komme en rekke nye tjenester i forbindelse med Integrerte operasjoner, og derfor også nye trusler som ikke er omtalt i denne rapporten.

5.2 SAS

Oppgaven vil ha svar på hva som er de vesentligste truslene og sikkerhetsutfordringer forbundet med å tilpasse et SAS-system til Integrerte operasjoner. Vi har kommet fram til at siden SAS-systemer er relativt lukkede systemer som kommuniserer med felles kontaktpunkt på plattformen, så vil det være lettere å kunne identifisere trusler mot SAS,

ved å se på Integrerte operasjoner som en helhet. Dette medfører at enkelte trusler kan oversees, ettersom vi i denne rapporten ikke har tatt høyde for trusler som kan ligge innenfor SAS-systemets grenser. Dersom tiden hadde tillatt det, ville vi gått dypere inn i SAS-systemet, og sett på eventuelle trusler som kan ligge her.

Vi forutsetter i denne oppgaven at SAS-systemet ikke endres ved overgangen til G2. Her bør man være klar over muligheten for at SAS-systemene åpnes mer opp enn slik de er idag, slik at kommunikasjon kan foregå direkte til de enkelte enhetene i SAS-systemet. Dette vil kunne føre til at trusselbildet endrer seg, og skape nye utfordringer i forbindelse med IKT-sikkerheten. Dette er en situasjon vi ikke har omtalt i denne rapporten.

5.3 Drøfting av trusler

Vi har avdekket de vesentligste truslene og IT-sikkerhetsutfordringene forbundet med å tilpasse et SAS-system til Integrerte operasjoner. Truslene vi har identifisert er beskrevet på et overordnet nivå, og siden faktiske sikkerhetsbrudd alltid er nyanserte og spesifikke, vil det kunne eksistere et gap mellom antatte trusler og faktiske brudd på informasjonssikkerheten. Det er svært viktig å merke seg det faktum at flere trusler kombinert kan utgjøre en mye større risiko enn "summen" av truslene hver for seg.

Oljenæringen bør være åpen om sikkerhetshendelser som oppstår, slik at alle aktører kan dra nytte av erfaringen. Dette bidrar til en økt IKT-sikkerhet totalt, og vil være en vinn-vinn situasjon for alle legitime parter.

Generelt om alle trusler

Rapportering av sikkerhetshendelser er særdeles viktig, slik at en kan iverksette tiltak mot disse umiddelbart. P09 - "Policy om logisk sikring" sier i punkt 3.0.3: "Prosedyrer for rapportering av sikkerhetshendelser og sikkerhetsbrudd skal dokumenteres og implementeres i organisasjonen. Sikkerhetshendelser skal alltid håndteres umiddelbart, før de utvikler seg til å bli sikkerhetsbrudd". Policyen definerer også retningslinjer for håndtering av sikkerhetshendelser og -brudd. Selv om disse tiltakene ikke nødvendigvis hindrer at sikkerhetshendelser oppstår, vil tiltakene være med på å øke den generelle informasjonssikkerheten.

Tr01 - Avlytting av datatrafikk

Avlytting av datatrafikk går på konfidensialitet, og kan forekomme ved alle typer datakommunikasjon, deriblant videokonferanser, overføring av data fra databaser, sensorer, samt overvåkningstrafikk og fjernstyringsdata. Avlytting av datatrafikk er noe

som oppstår relativt sjeldent, ettersom angrepet krever inngående kunnskap om nettverksprotokoller og teknologier, i tillegg vil man ikke kunne hente ut leselig sensitiv data, ettersom P11 "Policy om sensitiv informasjon" sier i punkt 3.5: "All sensitiv informasjon (...) skal til enhver tid lagres kryptert, og overføres i kryptert form". Dette skal gjøres i henhold til P02 - "Akseptabel kryptering policy".

For å sikre mot kompromittering av passord, sier P04 "Passord policy" i 3.3.4: " Passord må aldri sendes i klartekst i noen form for elektronisk kommunikasjon". Alle fjerntilkoblinger skal utføres i henhold til P07 "Policy om fjerntilgang". I punkt 3.2.8 står det: "Fjerntilkoblingen skal krypteres ved bruk av f.eks. VPN". For å vanskeliggjøre selve avlyttingen, sier P08 - "Policy om fysisk sikring" i punkt 3.6.2: "Kabler som brukes til dataoverføring eller telekommunikasjon må være sikret mot avlytting og skade.", dette er også påpekt i P10 - "Policy om nettverkssikkerhet og -topologi" i punkt 3.3.5.

Trådløs kommunikasjon er i utgangspunktet svært utsatt for avlytting, derfor sier P13 - "Policy om trådløs kommunikasjon" i 3.2.2: "Alle datamaskiner på det trådløse nettverket må benytte seg av bedriftens VPN-oppsett for å sikre at minst mulig av trafikken er uautorisert og ukryptert." og i punkt 3.2.3: "Bedriftens trådløse nett skal ikke benyttes for fjerntilkobling til SAS-systemer."

Tiltaket som omfatter sikring av kabler mot avlytting vil ikke ha noen effekt utenfor organisasjonens lokaler. De andre tiltakene medfører at sensitiv informasjon vil være kryptert, derfor vil trusselen bare kunne føre til moderate tap. Disse tapene omfatter data som ikke er kryptert p.g.a. lav sensitivitet, denne informasjonen kan imidlertid benyttes i social engineering, jfr. Tr07. I tillegg vil det eksistere en sannsynlighet for at de valgte krypteringsmetoder inneholder svakheter som ikke er kjent, slik at avlyttet trafikk i ettertid kan dekrypteres.

Tr02 - Man-in-the-middle

Man-in-the-middle angrep vil nødvendigvis omfatte de samme tjenestene som Tr01 "Avlytting av datatrafikk". Forskjellen her er at dette angrepet er aktivt og angriperen kan også endre data mellom to kommuniserende parter, og derfor går trusselen både på konfidensialitet og integritet. De samme policyer og punkter i disse vil være gjeldende her.

Dersom policyene følges, vil endring av data som følge av denne trusselen være begrenset til ukryptert og åpen informasjon, derfor vil trusselen bare kunne medføre middels alvorlige konsekvenser. Sannsynligheten for at trusselen blir til et

sikkerhetsbrudd vil være mindre enn Tr01, ettersom kompleksiteten av angrepet er større.

Tr03 - Identitetstyveri/maskerade

Identitetstyveri er en trussel mot autentiseringsmekanismer. Dette inkluderer både logiske, slik som digitale signaturer og aksesskontroll, og fysiske ved f.eks. videokonferanse. Det viktigste mottiltaket mot denne trusselen vil være P04 - "Passord policy", der alle punktene i policyen er svært viktig for beskyttelse mot kompromittering av passord, som videre beskytter mot trusselen. Ved bruk av f.eks. digitale signaturer brukes ofte smartkort, disse kan stjeles eller kopieres. Dette medfører to-komponent autentiseringsmekanismen vil falle bort. Derfor er P04 særdeles viktig, i tillegg sier P02 - "Akseptabel kryptering policy" i punkt 3.2.2: "Utstyr som benyttes for å generere eller oppbevare nøkler skal fysisk sikres". Dette gir ingen garanti for tap eller kopiering av smartkort, men vil ha en forebyggende effekt.

I verste tilfelle kan en person med ondsinnede intensjoner få tak i begge komponentene (passord og smartkort) til en person med høy sikkerhetsklarering og mange privilegier. Dette kan medføre alvorlige konsekvenser, da inntrengeren kan tilegne seg og endre all informasjon som identiteten han har stjålet har tilgang til. Konsekvensene vil imidlertid begrenses av P08 - "Policy om fysisk sikring" som definerer sikre soner hvor sensitiv informasjon oppbevares, jfr. P11 - "Policy om sensitiv informasjon". I de tilfeller hvor inntrengeren ikke fysisk er tilstede ved lokasjonen, vil P08 ikke ha noen forebyggende effekt, men dette går på Tr14 - "Logisk innbrudd".

Den fysiske delen av identitetstyveri har policyene ingen dekning for. Hvis en person med uærlige hensikter overtar en persons identitet ved videokonferanse, f.eks. ved å forstyrre bildet, eller på annen måte skjuler sin identitet og oppgir seg for å være en annen, vil ikke regler gitt i policyer dekke opp om dette. Det vil imidlertid være liten sannsynlighet for at dette skjer, da det ville krevd mye planlegging og vært en omfattende prosess. Sensitiv informasjon skal uansett ikke deles over videokonferanse uten tilstrekkelig sikring, derfor vil konsekvensen her isolert sett vært liten og kun medføre minimale skader. Ettersom trusselen også omfatter logisk identitetstyveri, vil den samlet sett kunne få alvorlige konsekvenser.

Tr04 – Fysisk Tyvlytting/tyvtitting

Fysisk tyvlytting er noe som kan oppstå relativt ofte. Man kan tenke seg at en person deltar på et møte ved hjelp av videokonferanse, og denne personen befinner seg i det offentlige rom. Da vil det være en stor sannsynlighet for at bruddstykker av tale og blikk

på skjermen kan forekomme. For majoriteten av de som får noe informasjon på denne måten, vil informasjonen være uforståelig og uinteressant. Om derimot en person med ondsinnede intensjoner aktivt går inn for tyvlytting/-titting, kan vedkommende i verste fall ekstrahere hele konferansen. Dette vil være brudd på konfidensialitet, men vil kun medføre opprettelige skader, da sensitiv informasjon ikke skal deles via videokonferanser uten tilstrekkelig sikring. Også blikk på terminalskjermer kan forekomme, og uvedkommende kan på denne måten oppta informasjon ved f.eks. bedriftsbesøk. P01 - "Akseptabel bruk policy" sier;

- 3.2.6. "Alle datamaskiner skal ha passordbeskyttet skjermsparer eller utlogging, med automatisk innkobling etter en viss tid uten aktivitet".
- 3.3.2. Uakseptabel bruk: "Spredning av konfidensiell informasjon til uvedkommende".

Punkt 3.2.6. dekker ikke opp trusselen fra den tid den ansatte forlater terminalen til skjermsparerfunksjonen trer i kraft. Derimot sier 3.3.2. at det er den enkelte ansattes ansvar at informasjonen her ikke kommer på avveie. Når det gjelder videokonferanser kan man tenke seg situasjoner hvor det er viktigere at en person deltar i konferansen, enn at absolutt ingen konfidensiell informasjon spres til uvedkommende. I en slik situasjon vil man muligens bryte enkelte regler fastsatt i policyene.

Tyvtitting ved inntasting av passord kan forekomme, men P04 - "Passord policy" sier i punkt 3.3.7: "Inntasting av passord skal skjules". I tillegg sier den i punkt 3.3.5: "Passord skal endres umiddelbart ved mistanke om kompromittering".

P08 - "Policy om fysisk sikring" definerer såkalte sikre soner. Dette vil si at soner hvor sensitiv informasjon er tilgjengelig, skal være fysisk adskilt fra evt. besøkende og uvedkommende. Dette tiltaket vil begrense muligheten for tyvtitting av sensitiv informasjon. Her må man ta høyde for klarerte ansattes tyvtitting, men dette vil gå under Tr08 - "Smugling av stjålne data".

Tr05 - Malware

Malware er et svært omfattende begrep og vil kunne være en trussel mot alle IKT-tjenester i Integrerte operasjoner. Virus, ormer o.l. kan angripe systemer relativt ofte og dette er ikke nødvendigvis angrep rettet direkte mot organisasjonen. P06 - "Policy om antivirus" sier i punkt 3.2.1: "Alle maskiner skal ha oppdatert og operativ beskyttelse mot malware". Dette tiltaket vil stoppe den kjente typen malware. Ukjent eller spesielt utviklet malware vil kunne slippe forbi beskyttelsen, og dette vil kunne medføre brudd på konfidensialitet, integritet og tilgjengelighet. Dette vil ikke være vanlig og antall

hendelser vil være begrenset. Konsekvensen kan likevel være alvorlig og føre til tap av sensitive data, utilgjengelige tjenester og store økonomiske tap.

P07 - "Policy om fjerntilgang" og P14 - "Sikker drift policy" sier begge at utstyr brukt til fjerntilkobling skal ha adekvat malware-beskyttelse. Dette er svært viktig for å hindre spredning av malware til sensitive systemer. P01 – "Akseptabel bruk policy" og P03 - "Elektronisk post policy" påpeker tiltak for å forhindre infisering og spredning av malware. P03 sier f.eks. i 3.1.3: "Vedlegg som følger innkommende epost skal ikke åpnes med mindre avsenderen og innholdet er kjent for mottakeren". Dette er tiltak som vil begrense muligheten for infisering.

Total beskyttelse mot malware er umulig å oppnå, og dersom infeksjon er et faktum, vil P12 - "Policy om sikkerhetskopiering" ha lagt retningslinjer for kopiering av viktig data, og man vil kunne oppnå status quo. Dette vil likevel kunne føre til nedetid av IKT-tjenester, men vil begrense skadeomfanget.

Tr06 - Forfalskning av sikkerhetsenhet

Sikkerhetsenheter benyttes bl.a. i tjenesten "digitale signaturer". Slike enheter kan også benyttes for tilgangskontroll, både logisk og fysisk. Trusselen forutsetter fysisk tilgang til originalenheten, og dette alene tilsier en liten sannsynlighet for forfalskning, ettersom P01 - "Akseptabel bruk policy" sier under punkt 3.3.3: Uakseptabel bruk: "Skjødesløs bruk eller sikring av (...) sikkerhetsenhet". Dette underbygges av P02 - "Akseptabel kryptering policy", punkt 3.2.2 "Utstyr som brukes for å generere eller oppbevare nøkler skal fysisk sikres". Disse retningslinjer garanterer ikke forfalskning eller stjeling, men vil redusere sannsynligheten betraktelig. I tillegg vil forfalsking av slike enheter være vanskelig, og kreve inngående kunnskap og avansert utstyr. Dersom noen faktisk gjennomfører angrepet og er i besittelse av en sikkerhetsenhet med mange privilegier, vil det i de fleste tilfeller også eksistere en ekstra barriere i form av passord. I verste tilfelle vil inntrengeren også tilegne seg dette, og da vil konsekvensene være alvorlige og kan medføre tap av sensitive data, utilgjengelige ressurser og store økonomiske tap.

Når det gjelder fysiske adgangsbarrierer hvor sikkerhetsenheter benyttes, vil det i enkelte tilfeller kunne gis tilgang til området med en sikkerhetsenhet alene, altså uten et passord i tillegg. Dette vil kunne gi full tilgang for en inntrenger, dersom sikkerhetsenheten forfalskes eller stjeles. Likevel vil sannsynligheten for skade begrenses som følge av P08 - "Policy om fysisk sikring" som sier bl.a. i punkt 3.2.2. "Adgang til områder hvor sensitiv informasjon lagres og/eller behandles skal holdes til et minimum".

Tr07 - Social engineering

Social engineering er en trussel mot aksesskontrollmekanismer, fordi det er en teknikk for å omgå disse. Trusselen er vanskelig å beskytte seg mot, og det er opplæring som er det viktigste tiltaket mot angrep. Opplæring utenfor IKT-systemer dekkes ikke opp av policyene. P01 - "Akseptabel bruk policy" sier i punkt 3.3.2: Uakseptabel bruk: "Spredning av konfidensiell informasjon til uvedkommende". Dette er et svært lite dekkende tiltak mot trusselen, ettersom det her vil bli opptil den enkelte innehaver av informasjons ansvar å avgjøre om forespørselen er legitim. Dette kan være vanskelig, spesielt med informasjon som i utgangspunktet virker triviell. Igjen er det opplæring som gjelder. En social engineer kan bygge videre på triviell informasjon for å tilegne seg mer sensitiv informasjon. Ingen av policyene dekker trusselen direkte, men f.eks. P03 - "Elektronisk post policy", punkt 3.1.8, "Det skal utøves kritisk sans til innholdet i e-postmeldinger. Avsenderadresser kan lett forfalskes", bygger opp rundt viktigheten av å være kritisk når det gjelder spredning av informasjon. Dette tas også opp i P04 - "Passord policy" i punkt 3.3.1: "Passord skal aldri deles med andre". P11 - "Policy om sensitiv informasjon" handler om klassifisering av sensitiv informasjon og er et viktig tiltak mot social engineering, ved at man unngår usikkerhet rundt sensitiviteten av informasjon.

Trusselen kan forekomme relativt ofte i medmenneskelig kommunikasjon, men konsekvenser av slike hendelser vil som regel kun medføre opprettelige skader. De alvorligste bruddene krever dyktighet og overbevisende fremtreden, og vil også kreve en god del planlegging og innsikt. Disse vil forekomme sjeldent, men kan medføre moderate skader på aktiva.

Tr08 - Smugling av stjålne data

Smugling av stjålne data er en trussel mot lagret informasjon innad i organisasjonen. Databaser over f.eks. brønnhistorikk og geologi inneholder informasjon som kan ansees viktig for organisasjonen. Dersom disse data kommer på avveie ved at ansatte smugler den ut, vil det ikke nødvendigvis få alvorlige konsekvenser. Derimot ved å smugle ut data som er vitalt for organisasjonen, vil konsekvensene bli mer alvorlige. Dette kan føre til tap av bedriftsomdømme og økonomiske tap og kan forekomme i et begrenset antall tilfeller. Informasjon om nettverkskonfigurasjon og -oppsett kan også smugles ut, og dette vil være en alvorlig trussel, ettersom den kan gjøre det lettere for gjennomføringen av f.eks. Tr14 - "Logisk innbrudd".

P08 - "Policy om fysisk sikring" inneholder tiltak som hindrer adgang for uvedkommende til områder hvor sensitiv informasjon oppbevares og behandles. P11 - "Policy om sensitiv

informasjon" forteller hvordan sensitiv informasjon skal behandles. Disse retningslinjene vil være effektive tiltak mot trusselen, men vil ikke dekke opp fullstendig. Årsaken til dette er at enkelte ansatte kan allerede inneha informasjonen på legitimt vis, og deretter smugle denne ut med ondsinnede intensjoner. Dette er nærmest umulig å sikre seg mot.

P08 sier også i punkt 3.1.5: "Medbrakt foto/videoutstyr, lydutstyr eller andre metoder for opptak er ikke tillatt i sikre soner, med mindre det er spesifikt autorisert". Dette vil være med på å begrense muligheten for å smugle ut informasjon om hvor f.eks. kamera, alarmer og andre sikringstiltak er plassert.

Tr09 - Manipulering av data

Manipulering av data kan forekomme relativt ofte i form av endring av triviell informasjon. Dette forårsaker brudd på integritet, som videre fører til at den opprinnelige informasjonen ikke lenger er tilgjengelig. Slike hendelser kan utføres for å justere informasjonen i brukerens favør. Dette vil kun medføre minimale og opprettelige skader. Om endringen utføres på kritisk data som har betydning for drift og HMS, vil derimot konsekvensene bli betraktelig større. Likevel vil det i slike situasjoner som regel være flere ansatte med i beslutningsprosessen, slik at de alvorligste konsekvenser vil unngås.

P14 - "Sikker drift policy" sier bl.a. i punkt 3.0.1: "Brukere av IKT-systemer skal ha adekvat opplæring i gjeldende informasjonssikkerhetskrav og akseptabel bruk av IKT-systemene". Dette vil sørge for at de ansatte vil få innblikk i konsekvensene som følger av denne trusselen. Likevel vil ingen av policyene direkte dekke denne trusselen, da den går på den enkeltes vilje til å følge etiske retningslinjer.

Dersom store mengder data manipuleres og dette oppdages, vil man kunne hente ut den opprinnelige informasjonen ut ifra sikkerhetskopier, jfr. P12 - "Policy om sikkerhetskopiering". Dette vil imidlertid ikke være tilfellet i tidsrommet fra forrige sikkerhetskopiering til manipulering foregår.

Tr10 - Tjenestenektangrep

Tjenestenektangrep går ut over tilgjengeligheten av data i ulike tjenester. Trusselen forekommer relativt sjeldent, ettersom det krever motivasjon og ressurser. P10 - "Policy om nettverkssikkerhet og -topologi" sier i punkt 3.3.1: "All trafikk mellom eksterne og det interne nettverket skal routes gjennom en eller flere brannmurer", og i punkt 3.3.2: "All trafikk inn mot bedriftens nettverk skal overvåkes v.h.a. IDS". Ingen policyer vil hindre angrep direkte, men disse tiltakene vil begrense alvorligheten av dem. Hvis et omfattende tjenestenektangrep er vellykket fra angriperens ståsted, vil konsekvensene

kunne være alvorlige. Tjenester som er vitale for operasjonell drift vil kunne gjøres utilgjengelige, og dette kan videre føre til store økonomiske tap.

Tr11 - Fysisk sabotasje

Fysisk sabotasje kan i utgangspunktet sette alle IKT-tjenester ut av spill og gjøre disse utilgjengelige. Trusselens konsekvenser strekker seg fra ubetydelige skader til store økonomiske tap og tap av sensitiv informasjon.

Alvorlighetsgraden er delvis avhengig av klareringen til sabotøren, fordi P08 - ”Policy om fysisk sikring” sier i 3.1.1: ”Sikkerhetssoner innenfor bedriften skal klart defineres” og i 3.2.3: ”Sikre områder bør beskyttes med hensiktsmessig adgangskontroll for å sikre at bare autorisert personell får tilgang”. Dette hindrer ikke fysisk sabotasje, men vanskeliggjør dette mot sensitive systemer. P08 definerer også regler for å sikre andre IKT-komponenter, slik som f.eks. kabling i punkt 3.6.2: ”Kabler som brukes til dataoverføring eller telekommunikasjon må være sikret mot (...) skade”. Disse tiltakene går hovedsaklig ut på å begrense tilgangen til komponenter som kan saboteres, og hindrer ikke trusselen direkte. Ved f.eks. påsatt brann eller oversvømmelse, vil det kunne få alvorlige konsekvenser. P08, punkt 3.3, ”Beskyttelse mot eksterne og miljømessige trusler” definerer retningslinjer for å beskytte viktig data mot f.eks. brann og oversvømmelse. Dette hindrer heller ikke fysisk sabotasje, men er med på å begrense skadeomfanget ved en slik hendelse.

Det er viktig å merke seg at fysisk sabotasje er en trussel som er svært vanskelig å sikre seg mot. Dersom noen aktivt går inn for å sabotere IKT-komponenter, vil det være en sannsynlighet for at vedkommende lykkes i større eller mindre grad. Policyenes regler er i hovedsak gitt for å begrense skadeomfanget, og P12 - ”Policy om sikkerhetskopiering” definerer regler for sikkerhetskopiering og gjenoppretting av data som kan gå tapt ved fysisk sabotasje. Ved alvorlig sabotasje som kan klassifiseres som en katastrofe, sier P14 - ”Sikker drift policy” i punkt 3.0.2: ”Planer for katastrofegjenoppretting skal dokumenteres og testes for kritiske systemer (...)”.

Fysisk sabotasje er en trussel mot tilgjengelighet, og dersom en hendelse først inntreffer vil disse tiltakene redusere tiden tjenestene er utilgjengelige. Det er likevel en liten sannsynlighet for at en hendelse inntreffer, ettersom vinningsgraden vil være liten, og de juridiske konsekvensene for sabotøren vil være omfattende.

Tr12 - Brukerfeil

Så lenge mennesker er involvert i prosesser og beslutninger, vil brukerfeil alltid kunne oppstå. Det er dette som kalles "den menneskelige faktor". Opplæring vil være det viktigste tiltaket og P14 - "Sikker drift policy" sier i 3.0.1: "Brukere av IKT-systemer skal ha adekvat opplæring i gjeldende informasjonssikkerhetskrav og akseptabel bruk av IKT-systemene. (...) For å opprettholde både informasjonssikkerhet og operasjonell drift, er det viktig at all personell får opplæring i korrekt bruk av IKT-systemene". Så lenge god opplæring av ansatte finner sted, vil antallet tilfeller være begrenset, samtidig som alvorlighetsgraden vil være moderat. P09 - "Policy om logisk sikring" nevner også opplæring i punkt 3.0.5: "IKT-systemene skal ha utpekte eiere. (...) Eieren skal sørge for at (...) opplæring blir gitt".

Enkelte brukerfeil kan få alvorlige konsekvenser, men ettersom viktige beslutninger sjeldent foretas av enkeltpersoner, vil de alvorligste konsekvenser unngås. Policyene dekker ikke opp trusselen direkte, men ved å sørge for tilstrekkelig opplæring, vil de ansatte unngå brukerfeil som skaper alvorlige og uopprettelige skader.

Tr13 - Misbruk av privilegier

Misbruk av privilegier har man lite direkte beskyttelse mot, og konsekvensen av trusselen kan være katastrofal. Ansatte med privilegerte tilgangsrettigheter kan endre konfigurasjonsdata ved særdeles viktige sikkerhetskomponenter. Sammen med å sørge for at kun ansvarsfulle og erfarne mennesker får tildelt betydningsfulle privilegier, vil den beste forsvarsmekanismen mot en slik trussel være splittelse av ansvar og privilegier. Policyene definerer ikke hvordan dette skal utføres, og overordnede retningslinjer for dette burde vært definert. P05 - "Policy om aksesskontroll" sier i punkt 3.1.3: "Tildeling av privilegier skal ikke utføres uten en fullstendig autorisasjonsprosess." og P08 - "Policy om fysisk sikring", punkt 3.2.2. sier: "Adgang til områder hvor sensitiv informasjon lagres og/eller behandles skal holdes til et minimum". Disse tiltakene begrenser antall personer med privilegerte tilgangsrettigheter og vil redusere sannsynligheten for at trusselen blir et sikkerhetsbrudd.

Misfornøyde ansatte er noe ethvert større selskap vil oppleve, men at ansatte vil misbruke eventuelle privilegier for å skade sin arbeidsgiver i katastrofalt omfang, vil være lite sannsynlig, ettersom konsekvensene for den ansatte vil være formidable i ettertid.

Tr14 - Logisk innbrudd

Logisk innbrudd kan ramme stort sett alle IKT-systemer, dersom tilstrekkelige sikringstiltak ikke iverksettes. Policyenes oppgave er å definere regler som forhindrer eller begrenser muligheten for at logiske innbrudd kan gjennomføres. Trusselen vil hovedsaklig være brudd på konfidensialitet, men kan også være brudd på både tilgjengelighet og integritet, dersom data slettes eller endres under innbruddet. Ved logisk innbrudd kan dårlige passord være en svakhet, og derfor definerer P04 - "Passord policy" i punkt 3.2 og 3.3 regler for oppbygning og beskyttelse av disse, og hindrer bruk av dårlige passord. P05 - "Policy om aksesskontroll" uttrykker i 3.4.1: "Sikre påloggingsprosedyrer skal benyttes for tilgang til operativsystemer. Prosedyren skal ikke avsløre noe om systemet før pålogging er gjennomført. Antall mislykkede påloggingsforsøk skal loggføres og begrenses til 3". P10 - "Policy om nettverkssikkerhet og -topologi" sier i punkt 3.3.1 og 3.3.2 at både brannmurteknologi og IDS skal beskytte nettverket. I tillegg uttrykker den i 3.3.4: "Alle nettverkstjenester som ikke er nødvendig for driften skal være deaktivert". Samtlige av disse tiltakene vil være med på å begrense muligheten for logiske innbrudd, men ingen av dem vil garantere beskyttelse mot trusselen, ettersom logiske innbrudd ofte benytter allment ukjente svakheter.

Trådløs kommunikasjon er spesielt utsatt for logisk innbrudd, ettersom signalene er tilgjengelig overalt i dekningsområdet. P13 - "Policy om trådløs kommunikasjon" definerer derfor følgende regel i 3.2.2: "Alle datamaskiner på det trådløse nettverket må benytte seg av bedriftens VPN-oppsett for å sikre at minst mulig av trafikken er uautorisert og ukryptert."

Dersom disse tiltakene skulle feile, og logisk innbrudd er et faktum, vil det være viktig å begrense skadeomfanget. P11 - "Policy om sensitiv informasjon" og P02 - "Akseptabel kryptering policy" definerer retningslinjer for klassifisering av sensitiv informasjon, og hvordan denne skal behandles og krypteres. Dersom logisk innbrudd inntreffer, vil sensitiv informasjon som stjeles være uleselig, ettersom den er tilstrekkelig kryptert. Dette er tiltak som ikke dekker opp om trusselen, men som vil være skadebegrensende dersom et brudd inntreffer.

Logisk innbrudd vil ikke være et vanlig fenomen, ettersom sikringstiltakene vil stoppe de fleste forsøk. Likevel vil muligheten alltid være tilstede, spesielt innenfor allment ukjente sårbarheter i maskin- og programvare. Dette er det svært vanskelig å dekke opp om, og aktiv IDS-overvåkning med anomali-deteksjon vil her være hensiktsmessig. Konsekvensene ved logisk innbrudd kan medføre tap av sensitive data og store

økonomiske tap. Det kan også føre til juridiske konflikter i forhold til f.eks. personvernloven.

5.4 IT-sikkerhetspolicy

Det vil være problematisk å utvikle sikkerhetspolicyer for Integrerte operasjoner som en helhet, ettersom sikkerhetspolicyer må ha et bestemt publikum som målgruppe. Med utgangspunkt i vår oppgave var det hensiktsmessig for oss å velge leverandører av SAS-systemer som målgruppe for policyene. I tillegg er vår oppdragsgiver, Origo, en leverandør av slike systemer.

Ettersom vi har valgt å kategorisere policyene ut fra teknologier og områder, og ikke ut ifra de enkelte truslene, vil det nødvendigvis være flere policyer som er aktuelle for hver enkelt trussel. En annen fremgangsmåte ville vært å ta for seg den enkelte trussel, og utvikle et slags tiltaksdokument for å dekke opp om denne. Denne metoden har vi ikke benyttet, da vi mener det vil gjøre helheten mindre oversiktlig. Oversiktlighet og entydighet er viktige momenter i sikkerhetspolicyer for å unngå misforståelser og potensielle sikkerhetshull.

ISO 17799, som er et av utgangspunktene for våre policyer, er av mange akseptert som ”beste praksis” innenfor IKT-sikkerhetsadministrasjon. Standarden tar utgangspunkt i tradisjonelle organisasjonsstrukturer, hvor majoriteten av informasjonsflyten foregår internt i organisasjonen. Det kan derfor være et problem å benytte denne standarden som utgangspunkt for informasjonssikkerhet i Integrerte operasjoner, da IO ikke vil ha noen klare og tydelige organisasjonsgrenser. SINTEF anbefaler i sitt dokument ”Trusler og muligheter knyttet til eDrift” utvikling av en variant av ISO 17799 som er spesielt rettet mot olje- og gassektoren. En slik standard ville vært et bedre utgangspunkt for våre policyer.

Ettersom oljeindustrien går mot mer fragmentering og økt bruk av outsourcing og underleverandører, vil det være mange mer eller mindre selvstendige ledd som utgjør helheten i Integrerte operasjoner. Dette fører til at det kan bli et problem å utforme IT-sikkerhetspolicyer ved en overgang til G2 av Integrerte operasjoner, og videre problematiserer det oppgaven med å definere et felles rammeverk for IKT-sikkerhet. Hvem som har ansvaret for at tilstrekkelig IKT-sikkerhet inkluderes i alle leddene, er et spørsmål som bør tas opp.

5.5 Forslag til videre arbeid

Våre forslag til løsninger er ikke ment som noe ferdig oppsett, men heller som et innblikk i noen av de teknologier og fremgangsmåter som kan benyttes i Integrerte operasjoner. Dersom tiden hadde tillatt det, ville vi gått dypere inn i emnene vi har omtalt.

RBAC

En av de største utfordringene ved implementering av Integrerte operasjoner er administrasjon av aksesskontroll. RBAC er en aksesskontrollmetode som egner seg i større distribuerte systemer, og vi foreslo en begrenset struktur som viste hvordan et slikt system kunne vært bygd opp mot SAS-systemer i IO. Denne figuren er på ingen måte fullstendig og er ikke ment som noe fullgodt svar for implementering. Likevel vil man ved å illustrere det på denne måten få en ide om hvordan et slikt system kan settes opp.

Her ville det nok vært hensiktsmessig å gå enda dypere inn i RBAC og sett på restriksjoner og rettigheter til enkelte roller for å bedre kunne se sammenhengen. Case-studiet som vi omtaler i denne rapporten diskuterer løsningen brukt i den nevnte banken opp i mot mulighetene som ligger i RBAC. Dette kan være verdifull informasjon som bør tas i betraktning ved eventuell videre utvikling av RBAC i Integrerte operasjoner.

Trust Based Management er en metode for å kontrollere tilgangskontroll som ved videre utvikling kan benyttes i distribuerte systemer. Dette er noe vi ville undersøkt nærmere dersom tiden hadde tillatt dette. Metoden baserer seg på at man unngår å måtte identifisere ulike brukere under autentiseringsprosessen. Denne funksjonen vil heller bli inkludert inn som en del av serverprogramvaren, og de forskjellige applikasjoner inneholder enkle koder for å sjekke om brukeren skal få tilgang til en ressurs eller ikke.

Semantisk web og OWL

Implementering av semantisk web kan medføre store fordeler i form av tidsbesparelser. Likevel kan det også medføre enkelte problemer dersom man ikke aktivt går inn for å motarbeide disse. Et av problemene er igjen overflod av informasjon til den enkelte bruker. En person risikerer å ”drukne” i informasjon, ettersom store deler av all informasjonen er linket sammen på en eller annen måte. Dette krever igjen opplæring og bedre forståelse av hvordan man skal jobbe effektivt med store informasjonsmengder. Der brukerne tidligere måtte benytte mye tid på å finne relevant informasjon, vil denne tiden nå betraktelig reduseres.

Kontrakter mellom leverandører og operatører bør oppdateres for å inkludere nye krav om leverandørenes plikter ved feilrapportering, registrering av modeller og innlegging av informasjon i databasene som benyttes av hele organisasjonens semantiske webtjenester.

Også fullstendig definisjon av språk og arbeidsprosesser vil være en utfordring for implementasjon av semantisk web. Dette kan løses, som tidligere nevnt, ved at man benytter seg av midlertidige dataklassetyper under konstruksjonen, og bygger så ontologier med de standardiserte klassetypene så snart de er definerte. Man risikerer riktignok ved denne løsningen, at det vil forekomme tvetydighet av klasser, og dette er et problem som må adresseres.

Digitale signaturer

For å unngå ansvarsfraskrivelse foreslår vi bruk av digitale signaturer og smartkort. Ved å signere f.eks. godkjenningsdokumenter og vedlikeholdsrapporter med en slik løsning, unngår man tvil om dette i ettertid. På en annen side kan denne metoden føre til at godkjenningsprosesser tar lengre tid enn tidligere, ettersom man er avhengig av smartkortleser, noe som ikke nødvendigvis finnes ved alle terminaler. Et alternativ til bruk av smartkort er biometri. Her kunne man benyttet f.eks. fingeravtrykkgjenkjenning og skanning av iris. Når det gjelder fingeravtrykk ansees ikke dette spesielt sikkert, da en slik metode lett kan forfalskes eller forbigås. Med irisskanning vil man oppnå relativt god sikkerhet, men dette medfører nødvendigvis relativt dyrt utstyr.

Distribusjonstjeneste for policy

Hvis sikkerhetsbrudd oppstår, vil det ofte være manglende etterlevelse av sikkerhetspolicyer som er årsaken. Vi valgte derfor å foreslå et system som distribuerer policyer med hensyn på roller personen innehar. Vi mener at ved å påkreve signering, og med dette bekrefter at man har lest og forstått gjeldende policyer, vil det føre til en bedre etterlevelse av disse. Policyer skal revideres og oppdateres med jevne mellomrom. Ved en slik tjeneste vil man lettere kunne formidle og sørge for at oppdaterte versjoner blir distribuert og lest, enn ved en papirbasert løsning. Vi har i rapporten ikke beskrevet metoder for å utvikle denne tjenesten.

Det er viktig å presisere at selv om denne løsningen vil føre til en større bevisstgjøring av sikkerhetspolicyene, kan den ikke ta høyde for at de blir fulgt. Man kan ikke sikre seg mot f.eks. at personer i en stresset arbeidssituasjon signerer og godkjenner uten at de egentlig har lest og forstått dokumentene. Her er det viktig med en god informasjonssikkerhetskultur og opplæring i viktigheten av slike policyer.

Felles kontaktpunkt

Et felles kontaktpunkt for rapportering av sikkerhetshendelser ble foreslått som et tiltak for forbedring av informasjonssikkerheten. Dersom sikkerhetshendelser ikke blir rapportert til personell med ansvar for slike, vil heller ikke sikkerhetshullet bli tettet, og faren for gjentagelse vil eksistere. Denne tjenesten gir ingen garanti for formidling av slike hendelser, men så lenge et slikt felleskontaktpunkt blir godt opplyst hos de ansatte, vil det mest sannsynlig føre til en økt rapportering av sikkerhetshendelser og -brudd.

6 Konklusjon

Vi har i denne rapporten tatt for oss det vi anser som den trolige utviklingen av Integrerte operasjoner, og truslene knyttet til dette. Da IO ennå ikke er et fullstendig definert og rammebestemt utrykk, åpnes det for en forandring i tjenester og infrastruktur. Dette vil kunne medføre endringer i trusselbildet, og er en direkte årsak til at IKT-sikkerhet alltid må tas hensyn til i videre uvikling av IO.

Truslene vi har avdekket er blitt vurdert i forhold til sannsynlighet og konsekvens. Videre har vi diskutert i hvilken grad våre forslag til sikkerhetspolicyer dekker opp om truslene. Det ble dermed mulig å se hvilke trusler som er dekket og hvilke trusler som har mangelfull dekning, eller som sikkerhetspolicyer vanskelig kan sikre mot.

Policyene vi har utviklet i dette prosjektet gir et godt grunnlag for informasjonssikkerhet, slik hensikten med sikkerhetspolicyer er. Sikkerhetspolicyer er et svært viktig ledd i informasjonssikkerheten, men de er verdiløse dersom de ikke blir fulgt. Opplæring og god sikkerhetskultur er derfor like viktige faktorer som policyene selv. Integrerte operasjoner krever en forbedring av kompetanse, holdninger og forståelse for informasjonssikkerhet.

En av de største utfordringene ved å oppnå en sikker overgang til IO Generasjon 2, vil ligge i å omdefinere ansvarsområder. Alle som er brukere av de nye tjenestene, vil ha et ansvar for at systemet er og forblir sikkert. Integrerte operasjoner fører med seg et formidabelt antall mennesker som benytter de integrerte systemene, og dette understreker viktigheten av ansvarsdelegering.

Uten hensyn til IKT-sikkerhet, er Integrerte operasjoner et dødfødt prosjekt. Å sørge for sikring av IKT-systemene innenfor IO, spesielt med tanke på integritet og tilgjengelighet, vil være en oppgave det bør legges mye arbeid i. Integrerte operasjoner er fremtiden i norsk oljeindustri, og skal man nå målet, må alle ledd i utviklingen oppnå konsensus om viktigheten av informasjonssikkerhet.

7 Referanser

[1] Stortingsmelding nr. 38, "Stortingsmelding 38 – Om petroleumsvirksomheten", 2003-2004
http://www.regjeringen.no/nb/dokumentarkiv/Regjeringen-Bondevik-II/Olje--og-energidepartementet/233575/234258/alt_om_stortingsmelding_nr-38_2003-2004.html?id=253901&epslanguage=NO
Hentet: 13.04.07

[2] Oljeindustriens landsforenings webside
http://www.olf.no/om
Hentet: 15.01.07

[3] SINTEF; Johnsen, Lundteigen, Albrechtsen, Grøtan, "Trusler og muligheter knyttet til eDrift", 2005
http://www.sintef.no/upload/Teknologi_og_samfunn/Sikkerhet%20og%20pålitelighet/Rapporter/STF38%20A04433.pdf
ISBN: 92-14-03138-9
Hentet: 15.01.07

[4] Arbeidsgruppe OLF, "eDrift på norsk sokkel – Det tredje effektivitetsspranget", 2002
http://www.olf.no/nyheter/aktuelt/?15204.pdf
Hentet: 07.02.07

[5] Oljedirektoratet, "Petroleumsressursene på norsk kontinentalsokkel", 2005
http://www.npd.no/NR/rdonlyres/62E91556-1E80-4475-BA65-9EDB5B2E33E9/0/Ressursrapporten2005.pdf
Hentet: 24.04.07

[6] Arbeidsgruppe OLF; Integrated Work Process, "Integrated Work Processes; Future work processes on the Norwegian Continental Shelf", 2005
http://www.olf.no/?28867.pdf
Hentet: 15.01.07

[7] Kevin D. Mitnick & William L. Simon, "The art of deception" , 2002
ISBN: 9-780-76454280-0

[8] Arbeidsgruppe OLF; Quality Information, "Quality Information Strategy of Integrated Operations on The Norwegian Continental Shelf"
http://www.olf.no/?29218.pdf
Hentet: 15.01.07

[9] Wikipedia, "Information Security",
http://en.wikipedia.org/wiki/Information_security
Hentet: 03.05.07

[10] Steering Group Integrated Operations, OLF's Guideline No. 104, "Information Security Baseline Requirements for Process Control, Safety and Support ICT Systems", 2006
http://www.olf.no/hms/retningslinjer/?32544.pdf
Hentet: 10.01.07

[11] NS-ISO/IEC 17799, "Informasjonsteknologi, Sikkerhetsteknikk, Administrasjon av informasjonssikkerhet (ISO/IEC 17799:2005)", 2005
ICS 35.040

[12] Petroleumstilsynet; Brattbakk, Østvold, van der Zwaag, Hiim, "Gransking av gassutblåsning på Snorre A, brønn 34/7-P31 A 28.11.2004", 2004
http://www.ptil.no/NR/rdonlyres/82A30AD3-2F43-46F0-9378-4911175E1554/7408/SNAEndeligrapport_utennavnkomprimert.pdf
Hentet: 15.01.07

[13] Matt Bishop, "Computer Security: Art and science", 2002
ISBN: 0-201-44099-7

[14] Matt Bishop, "Introduction to Computer Security", 2004
ISBN: 0-321-24744-2

[15] Camelot, "Differentiation between access control terms", 2001
http://www.windowsecurity.com/uplarticle/2/Access_Control_WP.pdf
Hentet: 21.03.07

[16] National Institute of Standards and Technology (NIST), "Proposed NIST Standard for Role-Based Access Control", 2001
http://csrc.nist.gov/rbac/rbacSTD-ACM.pdf
Hentet: 16.03.07

[17] W3C Semantic Web; Frequently Asked Questions
http://www.w3.org/2001/sw/SW-FAQ
Hentet: 03.05.07

[18] Hubert Vigneron, "Shaping the future: Role of Smart Cards", 2005
http://www.items.fr/IMG/pdf/Hubert_Vigneron.pdf
Hentet: 24.04.07

[19] Per Espen Stoknes, "Lær av fremtiden; Norske organisasjoner erfaringer med scenariobasert strategi", 2004
ISBN: 82-05.33086-7

[20] NORSOK standard I-002, "Safety and automations systems (SAS)", 2001
http://www.standard.no/pronorm-3/data/f/0/01/34/3_10704_0/I-002.pdf
Hentet: 15.01.07

[21] Arbeidsgruppe OLF; Digital Infrastructure Offshore, "Common Network Operation Management for Digital Infrastructure Offshore on The Norwegian Continental shelf", 2005
http://www.olf.no/?29220.pdf
Hentet: 15.01.07

[22] International Telecommunication Union, "H323 - Packet-Based Multimedia Communications Systems", 2006
http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-H.323-200606-I!!PDF-E&type=items
Hentet: 25.04.07

[23] Monitor Systems Scotland Limited - visiWEAR
http://www.monitor-systems.co.uk/
Hentet: 30.04.07

[24] Schaad, Moffett, Jacob, "The Role-Based Access Control System of a European Bank: A Case Study and Discussion", 2001
https://fronter.com/hia/links/files.phtml/904577785$676998757$/Fagstoff/RBAC/EuropeanBankACaseStudy.pdf
Hentet: 17.04.07

[25] GE Energy (Norway) AS, Bently Nevada "System 1; Optimization and Diagnostic Platform", 2005
http://www.ge-energy.com/prod_serv/products/oc/en/downloads/sys1_brochure.pdf
Hentet: 25.04.07

[26] Teknisk Ukeblad, "Tilstandsovervåking på et meget høyt nivå!", 2007, Nr. 11 s. 59

Vedlegg 1 - IT-sikkerhetspolicyer

P01 - Akseptabel bruk policy

1.0 Formål

Det vil være nødvendig for enhver bedrift å legge ned retningslinjer og regler for akseptabel bruk av IT-systemene. Formålet med denne policyen er å beskytte IT-systemer brukt i og mot Integrerte operasjoner mot tilsiktet og utilsiktet skade, og sette grunnlaget for akseptabel bruk av IT-systemene. Uakseptabel bruk kan eksponere bedriften for farer, slik som malware-angrep, uautorisert bruk av nettverkstjenester og -ressurser, tap av sensitive data, materiell- og personskade, samt juridiske konflikter.

2.0 Omfang

Denne policyen gjelder for all personell ved bedriften med tilgang til IT-systemene, samt alt utstyr som benyttes i bedriften eller mot SAS-systemer. Det er enhver bruker av IT-systemenes ansvar å gjøre seg forstått med og følge disse reglene.

3.0 Policy

3.1 Generelt

1. Data som blir produsert på bedriftens datasystemer forblir bedriftens eiendom.
2. All sensitiv informasjon skal behandles i henhold til ”Policy om sensitiv informasjon”. Se også ”Akseptabel kryptering policy”.
3. Bedriftens datasystemer skal i minst mulig grad benyttes til private formål, og hver enkelt ansatt står ansvarlig for å utøve god dømmekraft i.f.t. hva som ansees resonnabelt privat bruk. Ved usikkerhet angående dette punktet, skal ledelsen konsulteres.
4. Autorisert personell innenfor bedriften kan når som helst overvåke nettverk og systemer, for å bekrefte at denne policyen overholdes. Dette blir gjort i henhold til Datatilsynets reglement.

3.2 Sikkerhet

1. Passord skal håndteres varsomt og aldri deles med andre. Se ”Passord policy”.
2. Kryptering av informasjon skal gjøres i henhold til ”Policy om akseptabel kryptering”.
3. E-postvedlegg skal håndteres med varsomhet. Se ”E-post policy”.

4. All informasjon som er lagret eller produsert på bedriftens datasystemer bør klassifiseres som konfidensielt eller ikke konfidensielt. Se "Policy om sensitiv informasjon".
5. Bærbart utstyr er spesielt utsatt for tyveri, derfor skal spesielle sikkerhetshensyn tas til dette.
6. Alle datamaskiner skal ha passordbeskyttet skjermsparer eller utlogging, med automatisk innkobling etter en viss tid uten aktivitet.
7. Alle datamaskiner koblet til bedriftens nettverk eller nettverk tilknyttet SAS-systemer skal ha oppdatert antivirus/anti-malwareprogramvare installert. Se "Policy om antivirus".

3.3 Uakseptabel bruk

Det følgende regnes som uakseptabel bruk, og skal ansees ikke tillatt.

1. Utvikling eller spredning av malware.
2. Spredning av konfidensiell informasjon til uvedkommende.
3. Skjødesløs bruk eller sikring av passord eller sikkerhetsenheter. Passord skal aldri oppgis til andre eller skrives ned.
4. Alle former for angrep mot eller fra bedriftens nettverk. Dette inkluderer tjenestenektangrep, nettverkssniffing, adressespoofing, samt alle andre handlinger som kan ansees skadelig for bedriftens nettverk, eller nettverk tilknyttet SAS-systemer.
5. Distribusjon av spam.
6. All distribusjon av informasjon som inneholder trakassering, mobbing, eller nedlatende kommentarer.
7. All bruk som er skadelig for bedriften, dens ansatte, SAS-systemer bedriften har tilknytning til, eller som strider mot norsk lovgivning.

4.0 Konsekvenser ved forsømmelse

Enhver som forsømmer regler gitt i denne policy vil risikere sanksjoner, inkludert økonomisk ansvar og oppsigelse. Forsømmelser som strider mot norsk lov vil bli anmeldt til gjeldende myndighet.

5.0 Definisjoner

Malware

- All programvare ment for å infiltrere, overvåke, skade eller ødelegge et datasystem uten brukerens samtykke eller viten. Eksempler på malware er virus, ormer, trojanere, spyware, adware, etc.

E-post

- Elektronisk overføring av informasjon gjennom mail-protokoller som f.eks. IMAP eller SMTP

Adressespoofing

- Forfalskning av avsenderadresse.

Tjenestenektangrep

- Forsøk på å overbelaste en nettverksressurs slik at denne blir utilgjengelig for dens brukere. Bedre kjent som DoS (Denial of Service).

Nettverkssniffing

- Avlytting av pakketrafikk som foregår på nettverket.

Spam

- Distribusjon av tilnærmet identiske meldinger til en stor mengde mottakere. Meldingene er som regel uønsket av mottakerne og inneholder ofte reklame eller malware.

6.0 Referanser til dokumentasjon

NS-ISO/IEC 17799:2005, kapittel 7.1.3 ”Akseptabel bruk av aktiva”

NS-ISO/IEC 17799:2005, kapittel 10.10 ”Overvåking”

NS-ISO/IEC 17799:2005, kapittel 11.3 ”Brukeransvar”

OLF Guideline No.104, ISBR #6

P02 - Akseptabel kryptering policy

1.0 Formål

Hensikten med denne policyen er å beskytte sensitiv og konfidensiell data mot uautorisert tilgang. Det er også denne policys hensikt å begrense benyttede krypteringsmetoder til de som ansees sikre nok til å utføre den førstnevnte oppgave. Om konfidensiell bedriftsinformasjon kommer uvedkommende i hende, kan det medføre skade på bedriftens omdømme, drift og fremtid. I verste fall kan det føre til formidable økonomiske tap og juridiske konsekvenser.

2.0 Omfang

Denne policyen gjelder for all personell ved bedriften, samt alt utstyr som benyttes i bedriften eller mot SAS-systemer. Policyen gjelder også for tredjepartsaktører med tilknytning til bedriften. Det er enhver bruker av IT-systemenes ansvar å gjøre seg forstått med og følge disse reglene.

3.0 Policy

3.1 Generelt

1. Kun standardiserte krypteringsmetoder skal brukes for kryptering, eksempler på dette kan være 3DES, AES, RSA.
2. Kun standardiserte metoder skal benyttes for nøkkelutveksling i symmetriske kryptosystemer, f.eks. Diffie-Hellman.
3. Nøkkellengden i symmetriske kryptosystemer skal ikke være mindre enn 128 bits.
4. Enhver bruk av ikke-standardiserte krypteringsmetoder er ikke tillatt.

3.2 Beskyttelse

1. Alle kryptografiske nøkler skal beskyttes mot endring, tap eller ødeleggelse.
2. Utstyr som benyttes for å generere eller oppbevare nøkler skal fysisk sikres. Se "Policy om fysisk sikring".
3. Kryptografiske nøkler skal ha en begrenset levetid, og skal bare kunne benyttes innenfor et definert tidsrom.

4.0 Konsekvenser ved forsømmelse

Enhver som forsømmer regler gitt i denne policy vil risikere sanksjoner, inkludert økonomisk ansvar og oppsigelse. Forsømmelser som strider mot norsk lov vil bli anmeldt til gjeldende myndighet.

5.0 Definisjoner

Symmetrisk kryptering

- Krypteringsmetode som benytter samme nøkkel for både kryptering og dekryptering, til forskjell fra asymmetrisk kryptering.

Asymmetrisk kryptering

- Krypteringsmetode som benytter et nøkkelpar for hver deltaker, en offentlig og en privat nøkkel. Ved kryptering brukes offentlig nøkkel, ved dekryptering brukes privat nøkkel.

6.0 Referanser til dokumentasjon

NS-ISO/IEC 17799:2005, kapittel 12.3 ”Kryptografiske sikringstiltak”

P03 - Elektronisk post policy

1.0 Formål

Elektronisk post (e-post, e-mail) er idag en av de viktigste former for kommunikasjon for bedrifter. Av den grunn er det også et utsatt medium for angrep som kan skade bedriften. E-post blir mye brukt for spredning av malware, og datamaskiner kan lett bli infisert, dersom man ikke utøver forsiktighet og kritisk sans til innkommende meldinger sendt via dette mediet. E-post blir også brukt av angripere i det som kalles ”social engineering”, hvor angriperen utgir seg for å være en person i behov for opplysninger og informasjon. Angriperen kan på denne måten få tak i potensielt sensitiv data som vedkommende videre kan benytte for å skade bedriften, eller for egen vinning.

2.0 Omfang

Denne policyen gjelder for all personell som innehar en e-postkonto hos bedriften.
Det er enhver bruker av e-post sitt ansvar å gjøre seg forstått med og følge disse reglene.

3.0 Policy

3.1 Generelt

1. All innkommende e-post skal kontrolleres for malware ved nedlastning/åpning
2. All utgående e-post skal kontrolleres for malware før sending
3. Vedlegg som følger innkommende e-post skal ikke åpnes med mindre avsenderen og innholdet er kjent for mottakeren.
4. E-post skal regnes for et usikkert medium, og derfor skal ikke sensitiv informasjon sendes i klartekst over dette mediet.
5. Bedriftens e-postkontoer skal i minst mulig grad benyttes til privat bruk. Se ”Akseptabel bruk policy”.
6. Bedriftens e-postkontoer skal ikke benyttes for spredning av spam eller malware.
7. Innloggingsinformasjon for e-postkontoer skal holdes hemmelig.
8. Det skal utøves kritisk sans til innhold i e-postmeldinger. Avsenderadresser kan lett forfalskes.
9. Bedriftens e-postkontoer blir overvåket i henhold til Datatilsynets reglement.

3.2 Bedriftens omdømme

1. Bedriftens e-postkontoer skal ikke benyttes for opprettelse eller distribusjon av informasjon som kan virke støtende eller fornærmende på andre. Dette inkluderer kommentarer om rase, kjønn, etnisk opphav, religion, politiske meninger, seksuell legning, alder, osv.
2. Enhver som mottar e-post med innhold nevnt under punkt 1 fra en bedriftskonto, skal straks melde ifra til sin overordnede.

4.0 Konsekvenser ved forsømmelse

Enhver som forsømmer regler gitt i denne policy vil risikere sanksjoner, inkludert økonomisk ansvar og oppsigelse. Forsømmelser som strider mot norsk lov vil bli anmeldt til gjeldende myndighet.

5.0 Definisjoner

E-post

- Elektronisk overføring av informasjon gjennom mail-protokoller som f.eks. IMAP eller SMTP

Malware

- All programvare ment for å infiltrere, overvåke, skade eller ødelegge et datasystem uten brukerens samtykke eller viten. Eksempler på malware er virus, ormer, trojanere, spyware, adware, etc.

Social engineering

- Teknikker brukt for å manipulere mennesker til å utføre visse handlinger eller oppgi informasjon.

Klartekst

- Tekst uten noen form for kryptering. Kan leses uten tilleggsinformasjon.

Spam

- Distribusjon av tilnærmet identiske meldinger til en stor mengde mottakere. Meldingene er som regel uønsket av mottakerne og inneholder ofte reklame eller malware.

6.0 Referanser til dokumentasjon

NS-ISO/IEC 17799:2005, kapittel 10.8.1 ”Prosedyrer for utveksling av informasjon”

NS-ISO/IEC 17799:2005, kapittel 10.8.4 ”Elektronisk meldingsformidling”

NS-ISO/IEC 17799:2005, kapittel 10.4.1 ”Sikringstiltak mot ødeleggende kode”

P04 - Passord policy

1.0 Formål

Denne policyens formål er å sette krav til passord, deres oppbygning, lagring og endringsfrekvens. Passord er ofte eneste barriere mot brukerkontoer, og det er derfor svært viktig å benytte passord med tilfredsstillende sikkerhetskrav. Et dårlig passord kan bli gjenstand for kompromittering, og kan sette datasystemer i fare for innbrudd og uautorisert bruk av ressurser. Dette kan videre føre til tap av sensitiv og konfidensiell data, skade på bedriftens omdømme, materiell- og personskade, samt juridiske konflikter.

2.0 Omfang

Denne policyen gjelder for all personell hos bedriften, som har noen form for aksess beskyttet av passord. Dette inkluderer, men er ikke begrenset til brukerkontoer, administratorkontoer, nettverksressurser, kryptert lagring, etc.

3.0 Policy

3.1 Generelt

1. Alle passord på brukernivå må endres minst hver sjette måned, anbefalt er hver fjerde måned.
2. Alle passord på systemnivå må endres minst hver fjerde måned, anbefalt er hver andre måned.
3. Passordbrukere skal underskrive en erklæring om at reglene i denne policy overholdes.

3.2 Oppbygning

1. Passord skal inneholde 8 eller flere tegn
2. Passord skal inneholde minst 3 av de 4 nevnte tegnkategorier; store bokstaver, små bokstaver, tall, spesialtegn slik som f.eks; !”#%&/\()=?[]{}+-_’*@£$€
3. Passord skal ikke være ord som kan finnes i noen ordbøker.
4. Passord skal ikke være tegn som naturlig påfølger hverandre, slik som f.eks. 123456, abcde, qwerty, osv.

5. Passord skal ikke være vanlige bruksord, eller varianter av disse. Dette inkluderer:
    - Navn på familie, venner, kjæledyr, kolleger, firma, geografiske steder ol.
    - Fødselsdatoer, bryllupsdatoer, andre merkedager
    - Telefonnumre eller adresser, inkludert e-postadresser eller brukernavn
    - Typiske IT-ord, slik som kommandoer, URL, navn på programvare/maskinvare, osv

3.3 Beskyttelse

1. Passord skal aldri deles med andre. Unntak fra denne regel, er førstegangspassord som må endres ved første innlogging.
2. Samme passord skal aldri benyttes på mer enn èn konto.
3. Passord skal aldri skrives ned i klartekst.
4. Passord må aldri sendes i klartekst i noen form for elektronisk kommunikasjon.
5. Passord skal endres umiddelbart ved mistanke om kompromittering.
6. Passord skal ikke lagres i "husk passord" -funksjoner i noen applikasjon.
7. Inntasting av passord skal skjules.

Passord skal aldri deles med noen. Hvis noen krever et passord oppgitt, skal vedkommende henvises til dette dokumentet.

4.0 Konsekvenser ved forsømmelse

Enhver som forsømmer regler gitt i denne policy vil risikere sanksjoner, inkludert økonomisk ansvar og oppsigelse. Forsømmelser som strider mot norsk lov vil bli anmeldt til gjeldende myndighet.

5.0 Definisjoner

Passord

- Et sett med tegn som benyttes for å autentisere en bruker.

Brukerkonto

- Konto på lavere nivå enn systemkonto, typisk innlogging på arbeidsstasjoner, e-postkontoer, osv

Systemkonto

- Konto for administrative oppgaver, f.eks. root, administratorkonto, osv.

Klartekst

- Tekst uten noen form for kryptering. Kan leses uten tilleggsinformasjon.

6.0 Referanser til dokumentasjon

NS-ISO/IEC 17799:2005, kapittel 11.2.3 ”Administrasjon av brukerpassord”

NS-ISO/IEC 17799:2005, kapittel 11.3.1 ”Bruk av passord”

P05 - Policy om aksesskontroll

1.0 Formål

Aksesskontroll innebærer all kontroll av tilgang til informasjon. Hensikten med denne policyen er å definere retningslinjene for hvordan kontroll av aksess til informasjon skal gjennomføres og håndheves. Uautorisert aktivitet i IKT-systemene kan medføre tap av sensitiv informasjon, økonomiske tap, tap av omdømme og juridiske konflikter.

2.0 Omfang

Denne policyen gjelder for alt personell i bedriften med tilgang til bedriftens IKT-systemer, samt all personell med ansvar for gjennomføring av sikkerhetstiltak. Policyen gjelder også for tredjepartsaktører som har noen forbindelse med de førstnevnte

3.0 Policy

3.1 Administrasjon

1. Alle tilgangsrettigheter skal nektes, med mindre de er eksplisitt tillatt. IKT-systemer skal være konfigurert slik at alle aksessrettigheter er fjernet, med mindre brukeren eksplisitt er autorisert.

2. Det skal utvikles formelle prosedyrer for brukerregistrering, brukersletting og tildeling av passord. Alle brukernavn skal være unike og tilgangsrettigheter skal ikke overstige brukerens behov. Brukerlisten skal regelmessig gjennomgås for å vurdere brukernes tilgangsrettigheter, og for å fjerne overflødige konti.

3. Tildeling av privilegier skal ikke utføres uten en fullstendig autorisasjonsprosess. Autorisasjonsprosessen og registeret over alle tildelte privilegier skal holdes ved like. Privilegier skal kun tildeles på grunnlag av behov. Register over brukere med spesielt privilegerte tilgangsrettigheter skal gjennomgås minst hver tredje måned for å sørge for at ingen har tilegnet seg uautoriserte rettigheter

3.2 Brukeransvar

1. Passord skal holdes hemmelig og behandles i henhold til "Passord policy".

2. Ubevoktet utstyr skal sikres, alle aktive sesjoner og innlogginger skal avsluttes om man forlater utstyret/arbeidsplassen.

3.3 Nettverk

1. All tilgang til SAS-systemer skal kun gis til personell som ettertrykkelig har behov for det.

2. Kun sterke og godkjente autentiseringsmetoder skal brukes for å autentisere fjernbrukeres tilgang til SAS-systemer. Autentisering med passord mot SAS-systemer skal suppleres med bruk av fysiske sikkerhetsenheter, slik som smartkort. Se også "Policy om fjerntilgang".

3. Registeret over brukere med tilgang til SAS-systemer skal oppdateres og vedlikeholdes på lik linje med punkt 3.1.3.

3.4 Programvare

1. Sikre påloggingsprosedyrer skal benyttes for tilgang til operativsystemer. Prosedyren skal ikke avsløre noe om systemet før pålogging er gjennomført. Antall mislykkede påloggingsforsøk skal loggføres og begrenses til 3. Passordet som tastes inn skal ikke vises, og det skal ikke overføres i klartekst over nettverk.

2. Alle sesjoner skal avbrytes etter maksimum 30 minutter uten aktivitet. I lavrisikoområder kan dette begrenses til utlogging eller skjermsparer med passord. I høyrisikoområder er tidsavbruddet begrenset til 10 minutter, alle nettverkstilkoblinger og kjørende applikasjoner skal da stenges ned.

4.0 Konsekvenser ved forsømmelse

Enhver som forsømmer regler gitt i denne policy vil risikere sanksjoner, inkludert økonomisk ansvar og oppsigelse. Forsømmelser som strider mot norsk lov vil bli anmeldt til gjeldende myndighet.

5.0 Definisjoner

Privilegier

- Spesielle tilgangsrettigheter som muliggjør endring og konfigurasjon av systemparametere.

Smartkort

- Kort med mikroprosessor som tilbyr elektroniske sikkerhetstjenester. Mye brukt for autentisering.

6.0 Referanser til dokumentasjon

NS-ISO/IEC 17799:2005, kapittel 11 ”Aksesskontroll”

OLF Guideline No.104, ISBR #14

P06 - Policy om antivirus

1.0 Formål

IT-systemer er sårbare for angrep av malware, og det er denne policyens hensikt å legge ned retningslinjer for beskyttelse mot slike angrep. Infiserte IT-systemer kan være gjenstand for videre spredning av malware, og det er derfor viktig å få stoppet problemet øyeblikkelig, eller aller helst unngå infeksjon i utgangspunktet.

Malware kan komme fra utsiden og inn i bedriftens nettverk, f.eks. i e-postvedlegg, eller bli fysisk transportert dit ved hjelp av f.eks. eksterne lagringsenheter. Det er derfor viktig å ikke legge alle sikringstiltak i de logiske barrierene mot eksterne nett, men også ta hensyn til interne enheter og nettverk.

2.0 Omfang

Denne policyen gjelder for all personell som benytter seg av IT-systemene hos bedriften. Det er enhver bruker sitt ansvar å gjøre seg forstått med og følge disse reglene.

3.0 Policy

3.1 Generelt

1. Det skal utøves streng kritisk sans til nedlastningene fra nettet. Filer fra ukjente eller mistenkelige områder skal ikke lastes ned.

2. Det er brukerens ansvar at programvare for antivirus er oppdatert med de seneste tilgjengelige oppdateringer til enhver tid.

3. E-post spam skal slettes uten å åpne vedlegg. Se også ”Akseptabel bruk policy” og ”Elektronisk post policy”.

4. Når sikkerhetsoppdateringer til programvare er tilgjengelig, skal disse hentes ned og installeres umiddelbart. Spesielle hensyn skal tas til sensitive systemer.

3.2 Krav

1. Alle maskiner skal alltid ha oppdatert og operativ beskyttelse mot malware. Der hvor ikke kritiske sanntidssystemer benyttes, skal denne beskyttelsesprogramvaren konfigureres slik at definisjonsfiler for malware lastes ned automatisk.

2. Nye enheter som introduseres til IT-systemet eller nettet skal skannes og sjekkes for malware før de kobles til nettverket.

4.0 Konsekvenser ved forsømmelse

Enhver som forsømmer regler gitt i denne policy vil risikere sanksjoner, inkludert økonomisk ansvar og oppsigelse. Forsømmelser som strider mot norsk lov vil bli anmeldt til gjeldende myndighet.

5.0 Definisjoner

Virus

- Programvare med destruktiv hensikt, som kan kopiere seg selv og infisere datamaskiner og datautstyr uten brukerens tillatelse eller viten.

Malware

- All programvare ment for å infiltrere, overvåke, skade eller ødelegge et datasystem uten brukerens samtykke eller viten. Eksempler på malware er virus, ormer, trojanere, spyware, adware, etc.

Spam

- Distribusjon av tilnærmet identiske meldinger til en stor mengde mottakere. Meldingene er som regel uønsket av mottakerne og inneholder ofte reklame eller malware.

6.0 Referanser til dokumentasjon

NS-ISO/IEC 17799:2005, kapittel 10.4 ”Beskyttelse mot ødeleggende og mobil kode”

OLF Guideline No.104, ISBR #13

P07 - Policy om fjerntilgang

1.0 Formål

Denne policyens hensikt er å definere retningslinjer for fjerntilgang til SAS-systemer for bedriften. Disse retningslinjene er definert for å begrense potensiell eksponering av nettverket, da dette kan medføre skade på aktiva, skade på omdømme, økonomiske tap og personskader.

2.0 Omfang

Denne policyen gjelder for alle ansatte med fjerntilgang til SAS-systemer. Policyen omhandler enhver form for fjerntilgangsprivilegier til SAS-systemer. Med fjerntilgang menes alle tilkoblinger til enheter fra et nettverk utenfor det nettverket enheten er tilkoblet.

3.0 Policy

3.1 Generelt

1. Det er alle ansatte med fjerntilgangsprivilegier sitt ansvar å sørge for at enhver fjerntilkobling til SAS-systemer holder påkrevde sikkerhetskrav.

2. Alle tilkoblinger skal ha et hensiktsmessig mål og skal dokumenteres. Enhver form for unødvendig tilkobling er ikke tillatt.

3. Det skal alltid foreligge arbeidstillatelse før en fjerntilgangssesjon settes opp. Se ”Sikker drift policy”

4. Kun sterke og godkjente autentiseringsmetoder skal brukes for å autentisere fjernbrukeres tilgang til SAS-systemer. Autentisering med passord mot SAS-systemer, skal suppleres med bruk av fysiske sikkerhetsenheter, slik som smartkort. Se også ”Policy om aksesskontroll”.

3.2 Krav

1. Fjerntilkobling må være strengt beskyttet. Fjerntilgangsforbindelser må aldri, under noen omstendigheter opprettes uten påkrevd autentisering og kryptering.

2. Utstyr brukt til fjerntilkobling skal være i henhold til gjeldene regler angående antivirusbeskyttelse, oppdatering og patching.

3. Ikke under noen omstendigheter skal ansatte oppgi innloggingsinformasjon/ passord til noen. Innloggingsinformasjon skal behandles strengt konfidensielt.

4. Enhver som oppretter en fjerntilkobling til SAS-systemer må sørge for at utstyret ikke er koblet til noe annet nettverk samtidig. Unntak fra denne regel er lokalnettverk som er under brukerens totale kontroll.

5. Bruk av ustandardisert utstyr for fjerntilkobling må godkjennes av nettverksansvarlige.

6. Trådløse nettverk skal ikke benyttes for fjerntilgang til SAS-systemer. Se ”Policy om trådløs kommunikasjon”.

7. Fjerntilkoblingen skal krypteres ved bruk av f.eks. VPN.

4.0 Konsekvenser ved forsømmelse

Enhver som forsømmer regler gitt i denne policy vil risikere sanksjoner, inkludert økonomisk ansvar og oppsigelse. Forsømmelser som strider mot norsk lov vil bli anmeldt til gjeldende myndighet.

5.0 Definisjoner

Fjerntilgang

- Tilkobling til enhet fra et nettverk utenfor nettverket enheten er tilkoblet.

Smartkort

- Kort med mikroprosessor som tilbyr elektroniske sikkerhetstjenester. Mye brukt for autentisering.

Aktivum

- Alt som har verdi for bedriften.

VPN

- Virtual Private Network, sikkerhetsteknologi for beskyttelse av informasjonsoverføring.

6.0 Referanser til dokumentasjon

NS-ISO/IEC 17799:2005, kapittel 11.4 ”Aksesskontroll i nettverk”

OLF Guideline No.104, ISBR #14

P08 - Policy om fysisk sikring

1.0 Formål

Fysiske sikkerhetsbarrierer må benyttes for å beskytte informasjon og data som bedriften har i sin besittelse. Denne policyens hensikt er å legge retningslinjer for hvordan soner av sikkerhet skal defineres, og hva slags tiltak som må være på plass for å sikre bedriftens aktiva. Om de fysiske sikkerhetsbarrierene feiler, vil det kunne medføre uautorisert tilgang til IKT-systemene. Dette kan videre føre til tap av sensitiv informasjon, økonomiske tap, tap av omdømme, samt juridiske konsekvenser.

2.0 Omfang

Denne policyen gjelder for alle ansette ved bedriften, for besøkene og for tredjepartsaktører som er tilstede hos bedriften. Policyen omhandler alt utstyr og alle bedriftens avdelinger og kontorer.

3.0 Policy

3.1 Generelt

1. Sikkerhetssoner innenfor bedriften skal klart defineres. Disse sonene må defineres ut i fra hva slags rolle de fyller for bedriften, utstyr og data som lagres der, og hvordan de er plassert i forhold til andre soner.

2. Soner skal være klart avgrenset ved hjelp av vegger eller andre fysiske barrierer. Det må ikke herske tvil om hva slags sone man til enhver tid befinner seg i og hva slags regler som gjelder der.

3. Antall ulike soner bør begrenses til et minimum. Ved innføring av mange typer soner vil det kunne skape usikkerhet og misforståelser.

4. Enhver sone skal ha klare regler som alle brukere skal være inneforstått med. Disse reglene bør inneholde informasjon om hvem som har tilgang, tidspunkt man har tilgang og eventuelle særskilte regler og prosedyrer som er gjeldene for den enkelte sone.

5. Medbrakt foto/videoutstyr, lydutstyr eller andre metoder for opptak er ikke tillatt i sikre soner med mindre det er spesifikt autorisert.

3.2 Adgangskontroll

1. Besøkene må registrere seg med navn, tid for ankomst og avreise, og tildeles besøkskort som skal oppbevares synlig under hele besøket. Den besøkende skal også gjøres kjent med eventuelle krav og prosedyrer i soner som arbeidet skal utføres i.

2. Adgang til områder hvor sensitiv informasjon lagres og/eller behandles skal holdes til et minimum. Til slike områder bør personen få utdelt adgangskort/koder, og systemet må være konstruert slik at det til enhver tid lagres informasjon om innlogging/utlogging og spor som kan benyttes til å følge adgangen til forskjellige soner. Operatører fra tredjepartskontraktør som må ha tilgang til sikre soner, må også være under oppsikt til enhver tid.

3. Sikre områder bør beskyttes med hensiktsmessig adgangskontroll for å sikre at bare autorisert personell får tilgang.

3.3 Beskyttelse mot eksterne og miljømessige trusler

1. Viktig data og informasjon skal oppbevares på rom som er sikret mot spesielle miljømessige situasjoner som kan oppstå. Dette inkluderer også bygningsmessige problemer som kan forekomme, eksempel vannlekkasje i gulv, vegger og tak. Brennbart materiale må heller ikke oppbevares i slike rom.

2. På områder hvor det lagres og oppbevares sensitiv data, må det være installert røykdetektor som er operasjonell til enhver tid. Også nødvendig sikkerhetsutstyr må være hensiktmessig plassert til slike soner (f.eks. brannslokkingsutstyr).

3.4 Offentlig tilgang. Områder for lasting og levering

1. Disse områdene skal fysisk sikres i form av mulighet for avlåsing. Tilgang til disse sonene kan kun gjøres av autorisert personell, som igjen kan åpne for uautorisert personell ved behov.

2. Området bør være slik utformet at det kan benyttes uten at det gir adgang til andre områder. Det skal også isoleres fra informasjonsbehandlingsområder.

3. Dører til laste- og lossingsområder skal være låst når området ikke er i bruk.

3.5 Plassering og sikring av informasjonsbehandlingsutstyr

1. Utstyr som behandler sensitiv data må være plassert slik at de ikke er tilgjengelig innenfor de lavere sikkerhetssonene. Områder hvor slikt utstyr opererer eller lagres må være av sikker karakterer, hvor kun autorisert personell har tilgang.

2. Adgang til sikre soner bør holdes til et minimum.

3. For kritisk informasjonsbehandlingsutstyr må UPS være installert og fungerende. Disse skal sjekkes regelmessig for feil eller mangler, og behandles ifølge produsentens servicekrav og instruksjoner.

3.6 Sikkerhet for kabling

1. Alle kabler som strekkes må merkes godt, slik at det til enhver tid aldri er tvil om hvor kabelen er tilkoblet. Denne informasjonen må også følge med som en del av nettverkstopologien, se også ”Policy om nettverkstopologi”.

2. Kabler som brukes til dataoverføring eller telekommunikasjon må være sikret mot avlytting og skade. De bør også være fysisk adskilt for strømkabler for å holde forstyrrelser på et minimum.

3. Om reparasjon på kabler utføres, må dette dokumenteres og registreres. Om dette på noen måte medfører endring i tilkoblingspunkter eller nettverkstopologi må endringene registreres og/eller merkingen oppdateres.

3.7 Sikring av kontorer, rom og utstyr

1. Bedriftens eiendeler skal ikke fjernes fra bedriften med mindre det er spesifikt autorisert. Om utstyr skal fjernes, må det foreligge skriftlig tillatelse.

2. Interne telefonlister, adresselister, og registre som angir plassering av informasjonsbehandlingsutstyr skal ikke være offentlig tilgjengelig.

3. Kontorer som har mulighet for fysisk sikring må lukkes når disse ikke er i bruk. Når brukeren(e) forlater kontoret for dagen, låses dette.

4.0 Konsekvenser ved forsømmelse

Enhver som forsømmer regler gitt i denne policy vil risikere sanksjoner, inkludert økonomisk ansvar og oppsigelse. Forsømmelser som strider mot norsk lov vil bli anmeldt til gjeldende myndighet.

5.0 Definisjoner

Aktivum

- Alt som har verdi for bedriften.

UPS

- Uninterruptable Power Supply, enhet som sørger for videre drift i et gitt tidsrom ved strømbrudd.

6.0 Referanser til dokumentasjon

NS-ISO/IEC 17799:2005, kapittel 9 ”Fysisk og miljømessig sikkerhet”

OLF Guideline No.104, ISBR #11

P09 - Policy om logisk sikring

1.0 Formål

Logisk sikring omfatter alle informasjonssikkerhetstiltak innenfor programvare og logisk system- og nettverkskonfigurasjon. Hensikten med denne policyen er å definere retningslinjene for hvordan informasjonssystemer og nettverk logisk skal sikres, og hvordan sikkerhetshendelser og -brudd skal håndteres. Uautorisert aktivitet i IKT-systemene kan medføre tap av sensitiv informasjon, økonomiske tap, tap av omdømme og juridiske konsekvenser.

2.0 Omfang

Denne policyen gjelder for alt personell i bedriften med tilgang til SAS-systemer, samt all personell med ansvar for gjennomføring av sikkerhetstiltak. Policyen gjelder også for tredjepartsaktører som har noen forbindelse med de førstnevnte

3.0 Policy

1. Tiltak for å kontrollere aksess til informasjon skal innføres, se ”Policy om aksesskontroll”.

2. Prosedyrer for rapportering av sikkerhetshendelser og sikkerhetsbrudd skal dokumenteres og implementeres i organisasjonen. Sikkerhetshendelser skal alltid håndteres umiddelbart, før de utvikler seg til å bli sikkerhetsbrudd. Prosedyrene skal inneholde entydige fremgangsmåter for rapportering, og mal for utfylling av informasjon. Det skal gis tilbakemelding til vedkommende som rapporterte sikkerhetshendelsen eller -bruddet. Et felles kontaktpunkt for rapportering skal opprettes.

3. Det skal aldri foretas noen form for etterforskning av sikkerhetshendelser og -brudd uten ledelsens samtykke. Alle sikkerhetshendelser og -brudd skal behandles konfidensielt, og det skal aldri endres på noe som kan forspille bevis.

4. IKT-systemene skal ha utpekte eiere. Med eier menes her en person som står ansvarlig for systemet, dets konfigurasjon, oppbygning og sikkerhet. Eieren skal sørge for at:
    - kun godkjente applikasjoner og tjenester blir installert
    - risikovurdering blir utført regelmessig
    - gjeldene sikkerhetskrav er implementert
    - all dokumentasjon for systemet er oppdatert, tilgjengelig og tilstrekkelig sikret
    - opplæring blir gitt
    - sikkerhetshendelser og -brudd blir gjennomgått, og at nødvendige tiltak blir gjennomført

5. Utstyr som brukes til kommunikasjon med SAS-systemer skal kun brukes til spesifikke formål. Alle tjenester, applikasjoner og systemparametere som ikke er nødvendig for driften skal være deaktivert.

4.0 Konsekvenser ved forsømmelse

Enhver som forsømmer regler gitt i denne policy vil risikere sanksjoner, inkludert økonomisk ansvar og oppsigelse. Forsømmelser som strider mot norsk lov vil bli anmeldt til gjeldende myndighet.

5.0 Definisjoner

IDS

- Intrusion Detection System, benyttes for å detektere og rapportere uønsket og ondartet nettverkstrafikk.

6.0 Referanser til dokumentasjon

NS-ISO/IEC 17799:2005, kapittel 13 ”Administrasjon av informasjonssikkerhetsbrudd”

NS-ISO/IEC 17799:2005, kapittel 7.1 ”Ansvar for aktiva”

OLF Guideline No.104, ISBR #3, ISBR #6, ISBR #16

P10 - Policy om nettverkssikkerhet og –topologi

1.0 Formål

Hensikten med denne policyen er å beskytte informasjonsflyten på bedriftens interne og eksterne nettverk. IT-nettverket er en svært viktig del av bedriftens IT-systemer, og det er derfor viktig at nettverkets konfigurasjon og struktur sørger for optimal drift til enhver tid. Sikkerheten i nettverket må ivaretas for å unngå uautorisert tilgang til nettverksressurser og -tjenester. Innbrudd og uautorisert tilgang i nettverket kan få alvorlige konsekvenser, deriblant tap av sensitiv informasjon, tap av markedsposisjon og omdømme, økonomiske tap og juridiske konsekvenser.

2.0 Omfang

Denne policyen gjelder for nettverksansvarlige ved bedriften, samt alt personell med ansvar for gjennomføring av sikkerhetstiltak. Policyen gjelder også for tredjepartsaktører som har noen forbindelse med de førstnevnte. Policyen omhandler alle enheter som er tilkoblet nettverket og alt nettverksutstyr.

3.0 Policy

3.1 Generelt

1. All trafikk mellom eksterne og det interne nettverket skal routes igjennom en eller flere brannmurer.

2. Nettverkets utstyr og grensesnitt skal alltid være oppdatert og merket. Det skal til enhver tid finnes oppdaterte nettverksdiagrammer som viser hvordan nettverket er oppbygd og konfigurert.

3. Det skal til enhver tid finnes dokumentasjon på nettverksutstyr. Denne dokumentasjonen skal inneholde informasjon om fysisk plassering av nettverksutstyr, arbeid utført på utstyr, eierskap til utstyr, samt feillogger.

3.2 Fysisk og logisk adskillelse av nettverk

1. Nettverksinfrastrukturen skal gi mulighet for å segmentere nettverk slik at utstyr som har ulike sikkerhetsnivåer eller har behov for spesielle krav (sanntidssystemer, garantert responstid, etc) har mulighet for logisk eller fysisk adskillelse.

2. Utstyr for kommunikasjon med SAS-systemer bør være installert på et logisk eller fysisk adskilt nettverk fra IKT-systemer som kjører administrative oppgaver, testing og utvikling, etc. Dette må gjøres med mindre det er installert sikkerhetstiltak som garanterer at systemene ikke påvirker hverandre.

3.3 Sikkerhet

1. Nettverkets grensesnitt mot eksterne nettverk skal alltid beskyttes av en eller flere brannmurer.

2. All trafikk inn mot bedriftens nettverk skal overvåkes v.h.a. IDS. Denne skal ha oppdaterte regler og være operativ til enhver tid.

3. Nettverkskonfigurasjon skal kun utføres av nettverksansvarlige.

4. Alle nettverkstjenester som ikke er nødvendig for driften, skal være deaktivert.

5. Nettverkskabler skal beskyttes mot avlytting ved å skjule disse i vegg, eller ved å benytte kabelgater. Nettverkspunkter skal deaktiveres dersom disse ikke er i bruk.

4.0 Konsekvenser ved forsømmelse

Enhver som forsømmer regler gitt i denne policy vil risikere sanksjoner, inkludert økonomisk ansvar og oppsigelse. Forsømmelser som strider mot norsk lov vil bli anmeldt til gjeldende myndighet.

5.0 Definisjoner

IDS

- Intrusion Detection System, benyttes for å detektere og rapportere uønsket og ondartet nettverkstrafikk.

6.0 Referanser til dokumentasjon

NS-ISO/IEC 17799:2005, kapittel 10.6 ”Nettverksadministrasjon”

NS-ISO/IEC 17799:2005, kapittel 11.4.5 ”Oppdeling av nettverk”

NS-ISO/IEC 17799:2005, kapittel 11.6.2 ”Isolering av sensitive systemer”

NS-ISO/IEC 17799:2005, kapittel 9.2.3 ”Sikkerhet for kabling”

OLF Guideline No.104, ISBR #4, ISBR #11

P11 - Policy om sensitiv informasjon

1.0 Formål

Hensikten med denne policy er å gi retningslinjer og regler for hva slags informasjon som skal regnes for sensitiv og som må behandles konfidensielt, samt hvilken informasjon som kan regnes som ikke-sensitiv eller offentlig.

Det er essensielt for bedriften at konfidensiell bedriftsinformasjon blir unntatt uvedkommende. Hvis dette ikke unngås, kan informasjon som er vital for bedriftens fremtid komme på avveie, og bedriftens markedsposisjon og omdømme kan skades. Dette kan også medføre juridiske konflikter og materielle tap.

Alle spørsmål som gjelder klassifisering av informasjon skal rettes til den enkeltes overordnede.

2.0 Omfang

Denne policyen gjelder for all personell hos bedriften, samt alle tredjepartsaktører med innsynsrett i konfidensiell bedriftsinformasjon. Policyen gjelder for all informasjon lagret eller distribuert digitalt, all nedskrevet eller utskrevet informasjon, samt all informasjon delt muntlig.

3.0 Policy

All informasjon produsert i bedriften skal enten klassifiseres konfidensielt eller offentlig. På denne måten vil alt som ikke eksplisitt er klassifisert som offentlig informasjon, være konfidensielt, og skal behandles deretter. Det er eieren av informasjonen som står ansvarlig for at den får korrekt klassifisering. Uklassifisert informasjon skal antas å være konfidensielt med mindre andre opplysninger eksplisitt er gitt.

Informasjon bør merkes med ulik type klassifisering ut fra hvor sensitiv informasjonen er. I det følgende er definert tre ulike typer sensitivitetsklassifiseringer i tillegg til klassifiseringen ”åpen” som regnes for offentlig informasjon.

3.1 Åpen

Offentlig publisert bedriftsinformasjon, dette kan være åpen informasjon om bedriften, lokasjoner, kontaktinformasjon, etc. Det trengs ikke ta spesielle forhåndregler ved håndtering av denne typen informasjon.

3.2 Lite sensitiv

Generell bedriftsinformasjon, slik som generell personelldata og annen informasjon som ikke påvirker bedriften i særlig stor grad ved offentliggjøring. Selv om informasjonen er klassifisert "lite sensitiv", skal den behandles konfidensielt.

3.3 Middels sensitiv

Konfidensiell finansiell, teknisk og personellinformasjon som faller utenfor punktene 3.2 og 3.4. Kun autorisert personell skal ha tilgang til denne typen informasjon.

3.4 Høyst sensitiv

Informasjon som vil falle under denne kategorien er f.eks. bedriftshemmeligheter, kildekode, ikke patenterte produkter, og informasjon som er vitalt for bedriftens fremtid og suksess. Tilgang til slik informasjon skal bare gis autorisert personell med behov for informasjonen. All informasjon som går under kategorien "høyst sensitiv" skal merkes med dette, eller tilsvarende navn.

3.5 Behandling av sensitiv informasjon

All sensitiv informasjon, jfr. 3.2, 3.3 og 3,4 skal til enhver tid lagres kryptert, og overføres i kryptert form, se "Akseptabel kryptering policy".

4.0 Konsekvenser ved forsømmelse

Enhver som forsømmer regler gitt i denne policy vil risikere sanksjoner, inkludert økonomisk ansvar og oppsigelse. Forsømmelser som strider mot norsk lov vil bli anmeldt til gjeldende myndighet.

5.0 Definisjoner

Eier

- En person som står ansvarlig for systemet, enheten eller informasjonen.

Kryptering

- Bruk av algoritmer og logiske nøkler for å skjule informasjon. En må inneha korrekt nøkkel for å dekryptere og lese informasjonen.

6.0 Referanser til dokumentasjon

NS-ISO/IEC 17799:2005, kapittel 7.2 ”Klassifisering av informasjon”

NS-ISO/IEC 17799:2005, kapittel 10.7 ”Håndtering av datamedier”

P12 - Policy om sikkerhetskopiering

1.0 Formål

Hensikten med denne policyen er å legge retningslinjer for sikkerhetskopiering, hvordan denne skal gjennomføres, hva som skal kopieres og testintervaller. Sikkerhetskopiering er nødvendig for å opprettholde tilgjengelighet av informasjon, og sørge for kontinuitet i driften. Om sikkerhetskopiering ikke gjennomføres korrekt, kan det medføre økonomiske tap i form av tapt arbeid og informasjon. Dette kan også få fatale konsekvenser for bedriften, ettersom informasjon som er viktig for bedriftens fremtid kan gå tapt, slik som kunderegistre, kundeinformasjon, viktige bedriftsprosedyrer, prototyper, osv. Bedriftens omdømme kan skades, og med det kan inntektsgrunnlaget forsvinne.

2.0 Omfang

Denne policyen gjelder for all personell med ansvar for gjennomføring av sikkerhetstiltak. Policyen omfatter all produsert informasjon i bedriften, samt alt data som ansees viktig for bedriften.

3.0 Policy

3.1 Frekvens for gjennomføring

1. Det skal som et minimum tas inkrementell sikkerhetskopi hver kveld i ukedagene.

2. Det skal en gang i uken tas full sikkerhetskopi av alle data.

3. En gang i måneden skal det tas en sikkerhetskopi som skal lagres i henhold til datatilsynets reglement. Denne kopien skal også lagres på et sted fysisk separert fra de ukentlige sikkerhetskopiene på et sted hvor den er beskyttet mot brann, oversvømmelse og lignende.

4. Det skal gjennomføres test av sikkerhetskopier minst en gang hvert år eller når systemer for sikkerhetskopiering endres.

3.2 Generelt

1. Servere som brukes i den daglige driften skal til enhver tid kjøre speiling av harddisker som brukes til lagring av data.

2. Sikkerhetskopiering skal utføres på et sikkert og stabilt medium, som til enhver tid skal være merket med tidspunkt for kopiering. Mediene skal også byttes ut så snart de viser tegn på slitasje eller har fått en synlig skade, eller når produsentens oppgitte levetid er nådd.

3. De daglige sikkerhetskopiene skal lagres på et sikkert sted, og skal være lagret slik at de er beskyttede mot fysiske og miljømessige farer.

4. De ukentlige sikkerhetskopiene skal lagres fysisk adskilt fra de daglige sikkerhetskopiene. Disse skal også være beskyttet mot fysiske og miljømessige farer. Lagring i brannsikker skap er påkrevd.

4.0 Konsekvenser ved forsømmelse

Enhver som forsømmer regler gitt i denne policy vil risikere sanksjoner, inkludert økonomisk ansvar og oppsigelse. Forsømmelser som strider mot norsk lov vil bli anmeldt til gjeldende myndighet.

5.0 Definisjoner

Speiling

- Lagring av samme data på to eller flere harddisker samtidig.

Inkrementell sikkerhetskopi

- En sikkerhetskopi av data som er forandret siden siste fulle sikkerhetskopi eller inkrementelle sikkerhetskopi.

6.0 Referanser til dokumentasjon

NS-ISO/IEC 17799:2005, kapittel 10.5 ”Sikkerhetskopiering”

OLF Guideline No. 104, ISBR #15

P13 - Policy om trådløs kommunikasjon

1.0 Formål

WLAN og andre trådløse overføringsteknikker blir mye brukt til nettverksforbindelser. Siden mediet benytter radiobølger som kan fanges opp av alle innenfor dekningsområdet, regnes mediet for usikkert med mindre forhåndsregler benyttes for tilkobling. Hensikten med denne policyen er å legge retningslinjer for bruk av trådløse nettverk hos bedriften.

2.0 Omfang

Denne policyen gjelder for alle ansatte, besøkende og tredjepartsaktører med utstyr for tilkobling til bedriftens trådløse nettverk. Denne policyen gjelder alle former for trådløs kommunikasjonsutstyr.

3.0 Policy

3.1 Generelt

1. Alle aksesspunkter/basestasjoner som er tilkoblet til bedriftens nettverk skal være registrert og godkjent av sikkerhetsansvarlig hos bedriften

2. Alle aksesspunkter/basestasjoner skal til enhver tid være dokumentert med deres plassering, konfigurasjon, SSID og hvilke nettverk den er tilkoblet. Om det gjøres forandringer, skal disse dokumentene oppdateres. Se ”Policy om nettverkstopologi”.

3. SSID skal være konfigurert slik at den ikke avslører noe informasjon om bedriften, avdeling, ansatte eller lignende. Den skal heller ikke inneholde informasjon om type eller produsent av basestasjonen/aksesspunktet.

3.2 Tilkobling og teknologi

1. Alle produktene som brukes for trådløs kommunikasjon må være godkjent av bedriften, og ikke inneholde kjente svakheter.

2. Alle datamaskiner på det trådløse nettverket må benytte seg av bedriftens VPN-oppsett for å sikre at minst mulig av trafikken er uautorisert og ukryptert. Dette medfører at trådløse enheter må ha en punkt til punkt hardware kryptering. Se "policy om akseptabel kryptering".

3. Bedriftens trådløse nett skal ikke benyttes for fjerntilkobling til SAS-systemer. Se også "Policy om fjerntilkobling".

4.0 Konsekvenser ved forsømmelse

Enhver som forsømmer regler gitt i denne policy vil risikere sanksjoner, inkludert økonomisk ansvar og oppsigelse. Forsømmelser som strider mot norsk lov vil bli anmeldt til gjeldende myndighet.

5.0 Definisjoner

SSID

- Service Set IDentifier, navn på spesifikt trådløst nettverk.

VPN

- Virtual Private Network, sikkerhetsteknologi for beskyttelse av informasjonsoverføring.

6.0 Referanser til dokumentasjon

NS-ISO/IEC 17799:2005, kapittel 10.6 "Nettverksadministrasjon"

NS-ISO/IEC 17799:2005, kapittel 11.7.1 "Bærbart datautstyr og kommunikasjonsutstyr"

OLF Guideline No. 104 ISBR #11

P14 - Sikker drift policy

1.0 Formål

Formål med denne policyen er å legge retningslinjer for sikring av kontinuitet og operasjonell drift. Hvis det oppstår uforutsette hendelser, skal det være mulig å oppnå status quo innen kort tid, og det er derfor viktig å ha veldokumenterte og testede prosedyrer for hvordan dette oppnås. Forsømmelse av regler gitt i denne policy kan medføre omfattende materielle og økonomiske tap for bedriften, samt juridiske konflikter.

2.0 Omfang

Denne policyen gjelder for alt personell i bedriften med tilgangsrettigheter til SAS-systemer, samt all personell med ansvar for gjennomføring av sikkerhetstiltak. Policyen gjelder også for tredjepartsaktører som har noen forbindelse med de førstnevnte.

3.0 Policy

1. Brukere av IKT-systemer skal ha adekvat opplæring i gjeldende informasjonssikkerhetskrav og akseptabel bruk av IKT-systemene. De fleste problemer knyttet til IKT-systemer kan spores tilbake til feil bruk av disse. For å opprettholde både informasjonssikkerhet og operasjonell drift, er det viktig at all personell får opplæring i korrekt bruk av IKT-systemene. Dette gjelder nye ansatte og eksisterende ansatte når nye systemer innføres. I tillegg skal det minst en gang i året gjennomføres oppfriskningskurs.

2. Planer for katastrofegjenoppretting skal dokumenteres og testes for kritiske systemer og utstyr for kommunikasjon med SAS-systemer. Katastrofeplaner skal ha entydige definisjoner på hva som ansees som en katastrofe. Disse skal evalueres minst en gang i året, og testes minst en gang hvert annet år. Evaluering av katastrofeplaner skal også gjennomføres ved større forandringer i infrastruktur og systemer. Etter testing skal resultatene evalueres og planene oppdateres i henhold til resultatene.

3. Krav til informasjonssikkerhet for IKT-komponenter skal integreres i utviklings-, innkjøps- og oppstartsprosessene. Alle kontrakter og avtaler med tredjepartsaktører skal inneholde opplysninger om gjeldende krav til informasjonssikkerhet i utstyr, programvare og tjenester.

4. Utstyr for kommunikasjon med SAS-systemer skal ha definerte og dokumenterte retningslinjer for vedlikehold og support. Det skal foreligge dokumentasjon for hvordan vedlikehold skal gjennomføres, samt dokumentasjon på hvordan håndtering av problemer i forbindelse med IKT-systemene skal utføres.

5. Prosedyrer for endringsadministrasjon og arbeidstillatelser skal alltid følges for alle tilkoblinger til og endringer i SAS-systemer og -nettverk. Endringer i informasjonssystemer skal kun utføres under streng kontroll av endringsadministrasjon. Aldri skal det gjøres endringer i SAS-systemer uten at arbeidstillatelse er utgitt.

6. IKT-systemer skal være oppdatert og patchet når de er koblet til SAS-systemer. Sikkerhetsoppdateringer skal alltid installeres når de er tilgjengelige og godkjente i henhold til punkt 5.

7. Utstyr for kommunikasjon med SAS-systemer skal ha adekvat, oppdatert og aktiv beskyttelse mot malware. Se også ”policy om antivirus”.

8. Påkrevd operasjons- og vedlikeholdsprosedyrer skal være dokumentert og oppdatert. Alle prosedyrer i forbindelse med operasjon og vedlikehold skal dokumenteres og dokumentasjonen skal kun være tilgjengelig for autorisert personell. Endringer i prosedyrene skal kun utføres i henhold til punkt 5. Sikkerhetskopiering skal dokumenteres og gjennomføres, se ”Policy om sikkerhetskopiering”.

4.0 Konsekvenser ved forsømmelse

Enhver som forsømmer regler gitt i denne policy vil risikere sanksjoner, inkludert økonomisk ansvar og oppsigelse. Forsømmelser som strider mot norsk lov vil bli anmeldt til gjeldende myndighet.

5.0 Definisjoner

Malware

- All programvare ment for å infiltrere, overvåke, skade eller ødelegge et datasystem uten brukerens samtykke eller viten. Eksempler på malware er virus, ormer, trojanere, spyware, adware, etc.

6.0 Referanser til dokumentasjon

NS-ISO/IEC 17799:2005, kapittel 6.2.3 ”Sikkerhetshensyn i avtaler med tredjepart”

NS-ISO/IEC 17799:2005, kapittel 8.2.2 ”Bevisstgjøring, utdanning og opplæring”

NS-ISO/IEC 17799:2005, kapittel 10 ”Kommunikasjons- og driftsadministrasjon”

NS-ISO/IEC 17799:2005, kapittel 12.6 ”Administrasjon av teknisk sårbarhet”

NS-ISO/IEC 17799:2005, kapittel 14 ”Kontinuitetsplanlegging”

OLF Guideline No.104, ISBR #5, ISBR #7, ISBR #8, ISBR #9, ISBR #10, ISBR #12, ISBR #13, ISBR #15

Vedlegg 2 - Aksesskontrollmetoder og RBAC

Aksesskontrollmetoder

Aksesskontroll er et verktøy for å tillate eller nekte bruken av ressurser. Det finnes et stort utvalg av forskjellige måter å løse denne oppgaven på. Operativsystemene bruker flere av dem for å fastslå tilgangsrettigheter for brukerne. I større distribuerte systemer som Integrerte operasjoner, vil det være essensielt å benytte seg av en aksessmetode som enkelt kan gi eller nekte brukere aksess til ulike deler av nettet. Siden det i IO hele tiden vil være forandringer i struktur, f.eks. at ansatte skifter stilling og skal ha forskjellige rettigheter til ulike tider, er det viktig at dette er oversiktlig og intuitivt organisert. Man må sørge for at brukere ikke får tilgang til ressurser utover det som er nødvendig for å utføre arbeidet og også at nødvendige ressurser blir tildelt.

Innenfor aksesskontroll finnes det en metode som egner seg til større distribuerte systemer. Role Based Access Control (RBAC) er en aksesskontrollmetode som egner seg i større organisasjoner som er i konstant endring, med mange brukere som skal ha forskjellige rettigheter til ulike tider. Denne metoden har vært kjent i lang tid, men har ikke vært en standard og har derfor blitt implementert på forskjellige måter med ulike terminologier og funksjoner. National Institute of Standards and Technology (NIST) har utarbeidet en komplett modell som er foreslått som en standard. Ved å standardisere RBAC vil det være enklere å implementere den, siden det er et felles rammeverk for hvordan terminologi og teknologi er integrert.

Access Control Matrix (ACM)

Access Control Matrix er det grunnleggende og enkleste rammeverket for å beskrive aksess og sikring av systemer [13]. ACM bygger på en enkel tabell for å gi rettigheter.

Tabell 5: Access Control Matrix

	Fil 1	Fil 2	Prosess 1	Prosess 2
Prosess 1	Lese, skrive, eier	Lese	Lese, skrive, kjøre, eier	Skrive
Prosess 2	Tilføye (append)	Lese, eier	Lese	Lese, skrive, kjøre, eier

Ut fra denne kan man lese at prosess 1 eier fil 1 og kan lese og skrive til fil 1 mens den kun kan lese fil 2. Prosess 1 kan også kommunisere med prosess 2 og dette kan prosess

2 lese. I teorien er dette en enkel og oversiktlig metode for å kontrollere aksess til objekter. Problemet er at ved mange objekter blir tabellene veldig store, vanskelige å opprettholde og bruker store mengder plass.

ACL og Capabilities er to varianter av Access Control Matrix.

Access Control List (ACL)

ACL lagrer hver kolonne med objektet det representerer. Tabell 5 ved bruk av ACL vil bli som følger:

Acl(fil 1) = { (prosess 1, {lese, skrive, eier)}), (prosess 2, {tilføye}) }
Acl(fil 2) = { (prosess 1, {lese}), (prosess 2, {lese, eier}) }
Acl(prosess 1) = { (prosess 1, {lese, skrive kjøre, eier}), (prosess 2, {lese}) }
Acl(prosess 2) = { (prosess 1, {skrive}), (prosess 2, {lese, skrive, kjøre, eier}) }

Et av problemene med ACL er at dersom et objekt ikke er nevnt i ACL så har det heller ingen rettigheter. På et system med mange subjekter vil ACL bli veldig stor og dersom mange har samme rettigheter til en fil kan man definere et ”wildcard” for å gi et hvilket som helst ikke-navngitt subjekt et sett med standardrettigheter. I teorien er ACL enkel, lett forståelig og krever lite endring og implementering av utstyr. Men når det blir mange brukere og objekter blir det fort uoversiktlig å vanskelig å administrere. Det vil være vanskelig å få en oversikt over hvem som har tilgang til hvilke ressurser og man kan fort oppleve at folk får tilgang til mer enn de skal. [13, 14]

Capabilities

I ACL benyttet vi oss av kolonnene for å lage listene, med capabilities lister man ut radene. Eksempel som brukt i tabell 5 vil da se slik ut:

Cap(prosess 1) = { (fil 1, {lese, skrive eier}), (fil 2, {lese}), (prosess 1, {lese, skrive, kjøre, eier}), (prosess 2, {skrive}) }
Cap(prosess 2) = { (fil 1, {tilføye}), (fil 2, {lese, eier}), (prosess 1, {lese}), (prosess 2, {lese, skrive, kjøre, eier}) }

Når en prosess forespør en capability på vegne av en bruker, leter operativsystemet gjennom de forskjellige capabilities for å bestemme hvilke rettigheter prosessen har. Selv om dette gjør den er sikrere enn ACL, og at man har større kontroll over prosessene, viser det seg at ACL er den mest brukte metoden. Dette kan være fordi det i de fleste tilfeller er snakk om aksessrettigheter for subjekter på objekter, dette er lettere og mer

effektivt behandlet av ACL, siden man i capabilities må søke gjennom alle subjektene for å kunne ta en avgjørelse.
[13, 14]

Andre aksesskontrollmetoder

Det har blitt utviklet et stort antall forskjellige aksesskontrollmetoder. Disse er utviklet ut fra samme prinsipp som forklart over og er spesialisert til forskjellig bruk og komponenter. Det vil være andre krav og behov for sikkerhet i en brannmur, enn i for eksempel en database. Det er derfor utviklet forskjellige aksesskontrollmetoder som er tilpasset de forskjellige komponentene. Ofte kan man også bruke flere av dem sammen.

I en brannmur benyttes gjerne Content Based Access Control (CBAC) som ser på ressursene og kan begrense tilgang til en ressurs med hensyn på sekvens. Det vil si at en bruker bare kan tilkoble en ressurs et visst antall ganger. I databaser har man andre aksesskontrollmetoder som Content Dependent Access Control (CDAC) og View Based Access Control (VBAC). VBAC er et eksempel som kun kan benyttes til databasesystemer og ikke til å kontrollere filer eller andre applikasjoner. Her vil brukere som logger seg på få tilgang til ulike skjermbilder utifra hva de har behov for. For eksempel skal en sykepleier ikke ha tilgang til de samme opplysningene som en lege, men begge to vil få et vindu som for dem ser fullstendig ut. [15]

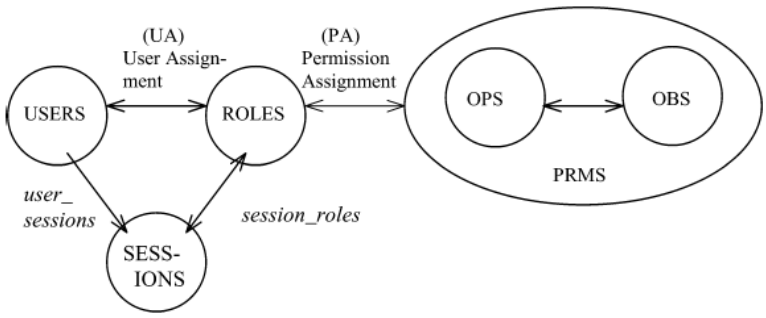
Mandatory og Discretionary Access Control (MAC og DAC) beskriver to forskjellige måter å klassifisere aksessmetoder på. MAC er, som navnet tilsier, obligatorisk og kan ikke overstyres av brukere. Et klassisk eksempel på dette er e-postserveren som gjerne setter faste grenser på hvor store e-postene kan være for å komme gjennom serverne og har i dag typisk en maksgrense på 10MB for vedlegg. DAC derimot, lar brukerne selv ta den endelige avgjørelsen om hvilke rettigheter et objekt skal ha. Eieren av filen kan selv velge om andre skal ha rettigheter til å lese, skrive, kjøre og slette. Dette gir flere muligheter for brukerne, men man er da avhengig av å stole på brukerne, og at de kjenner til bedriftens retningslinjer for sensitiv data, og behandler dette deretter. Ofte er aksesskontroll løst v.h.a. samhandling av disse to metodene ut ifra hva slags type objekt det er snakk om. Egenskrevne dokumenter kan man for eksempel selv få lov til å sette rettigheter til, men det kan ligge en overordnet MAC som gjør at de ikke kan publiseres og deles utenfor bedriften. [15]

Det finnes også flere andre metoder som retter seg mot ulike komponenter, men fellesnevneren for alle sammen er at de ikke er beregnet til å styre og kontrollere store distribuerte systemer slik som Integrerte operasjoner er.

Role Based Access Control (RBAC)

For å få entydig terminologi og få en oversikt over omfanget av RBAC, begynner standarden med en modell som definerer grunnleggende RBAC elementer og relasjoner av funksjoner som er inkludert i standarden. Denne modellen blir kalt RBAC Reference Model. Referanse-modellen har to formål: " *It rigorously defines the scope of RBAC features that are included in the standard. This covers the core set of features to be encompassed in all RBAC systems, aspects of role hierarchies, aspects of static constraint relations, and aspects of dynamic constraint relations. In addition, the reference model provides a precise and consistent language, in terms of element sets and functions for use in defining the functional specification.*"[16]

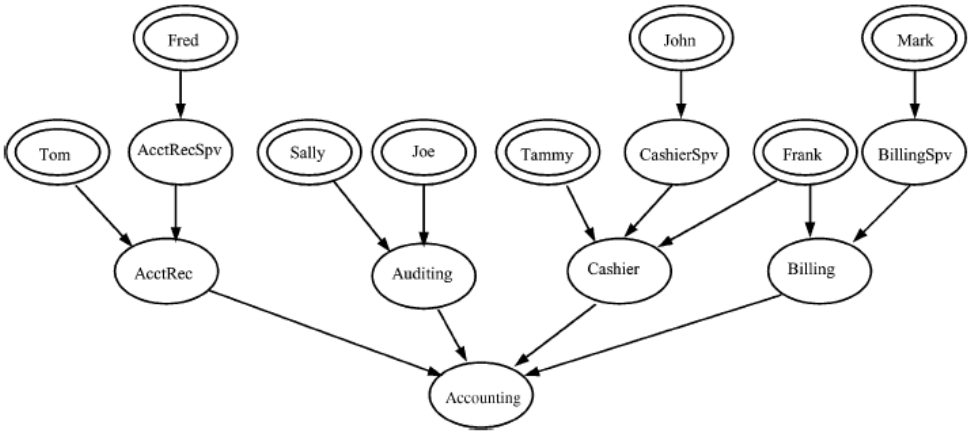
Modellen er delt opp i 4 hovedelementer; Core RBAC, Hierarkisk RBAC, Static seperation of duty (SSD) og Dynamic seperation of duty (DSD).
Core RBAC er den grunnleggende modellen som er obligatorisk i alle implementeringer av RBAC. Den består av fem forskjellige dataelementer som er brukere (USERS), roller (ROLES), objekter (OBS), operasjoner (OPS) og tillatelse (PRMS). I tillegg har modellen sesjoner som blir aktivert når man bruker rettigheter man er tilegnet. Hver sesjon er assosiert med en enkelt bruker og hver bruker er assosiert med en eller flere sesjoner. Den viktigste funksjonen til Core RBAC er UA (User Assignment) og PA (Permission Assignment) som vist i figur 7. Core RBAC beskriver hvordan man oppretter og sletter brukere (UA) og rettigheter (PA). [16]



Figur 9: Core RBAC [16]

Hierarkisk RBAC er en utvidelse av Core RBAC som gir støtte for rollehierarki. Dersom det er en stor organisasjon med mange objekter og brukere kan en slik implementering gjøre administrasjonen av roller enklere og systemene mer intuitive. Rollehierarkier definerer relasjoner av arv mellom roller.

Ved å benytte seg av arv vil rettigheter som mange brukere trenger tilgang til, kunne arves fra predefinerte roller, og man slipper å ha mange roller med akkurat de samme rettighetene gjentatte ganger. Et eksempel på et hierarki som er bygd opp som dette er vist i figur 8.



Figur 10: Eksempel på hierarki i regnskap [16]

Rollehierarkier er i standarden delt opp i to typer av rollehierarki. *General Role Hierarchies* tillater at man kan være tilkoblet flere roller på samme nivå i bedriften. I figur 8 vil Frank som har tilgang til rollene innen både *Cashier* og Billing, vil være et typisk eksempel på dette. I *Limited Role Hierarchies* ville ikke dette være tillatt. Her setter man begrensninger ved at en bruker bare kan være tilegnet en rolle på samme nivå. Hvis vi ser bort ifra Frank kan vi si at figur 8 ville vist en *Limited Role Hierarchy.*

Separation of duty relasjoner blir brukt for å håndheve motstridende interesser. I RBAC kan et eksempel på motstridende interesser være at man har to roller som gir ulike rettigheter til samme område eller fil.

Static seperation of duty (SSD) gjør dette ved å sette opp restriksjoner mot at man kan tilegne seg to roller som er motstridende. Det vil si at dersom man har tilgang til begge roller, vil man ikke kunne benytte begge roller samtidig. SSD er i standarden laget både med og uten rollehierarki. I rollehierarki vil SSD også gjelde for arvede roller.

Dynamic seperation of duty (DSD) relasjoner, har samme prinsipp som SSD, og begrenser tilgangen til motstridende roller. Mens SSD begrenser bruk av samtidige og motstridende roller, gjør DSD det mulig at en bruker benytter flere motstridende roller samtidig så lenge brukeren benytter rollene uavhengig. Hvis brukeren prøver å gjøre to oppgaver samtidig som har motstridende rettigheter i forhold til rollene, vil DSD hindre dette. [16]