Øving 2

Beskrivelse av øving

Denne øvingen teller som 10% av karakteren i faget. Besvarelsen skal være på maks seks sider, og øvingen skal leveres som pdf.

I denne øvingen skal kandidatene gjennomføre en risikovurdering av noen utvalgte hendelser. Dette innebærer vurdering av sannsynlighet og konsekvens, plotting i risikomatrise, valg av strategi for risikohåndtering og eventuelle mottiltak.

Øvingen kan gjøres i grupper på 1-2 personer, av erfaring kan samarbeid lønne seg. Hvis dere er to studenter som samarbeider så skal dere skrive opp hverandres kandidatnummer i innleveringen. **Begge kandidater må levere øvingen i Inspera**.

I denne øvingen tar vi utgangspunkt i fem uønskede hendelser. Tre av hendelsene vil påvirke "søk- og redningsoperasjoner" og to av hendelsene vil påvirke "kredittkortbetalinger".

Søk- og redningsoperasjonen (SAR):

1. Noen har montert en manipulert VDES radio som sender ut falske AIS meldinger, i området hvor søk- og redningsoperasjonen blir initiert.
2. En ansatt om bord på et av skipene har tatt med seg en flyttbar lagringsenhet som er infisert med skadevare og plugger denne inn i brunettverket på skipet. Skadevaren krypterer innholdet på PC-en hvor SAR applikasjonen er installert slik at den blir utilgjengelig.
3. GNSS antennen på et av skipene i området blir ødelagt av en storm på havet. Dette medfører at ingen av systemene på skipet har tilgang til posisjonsdata.

Kredittkortbetalinger:

4. En ondsinnet aktør bryter seg inn i lokalene hvor POS serveren er installert og stjeler med seg serveren hvor informasjonen fra kredittkortbetalingene er lagret.
5. "Jamming" på VDES sine kommunikasjonskanaler i et område utenfor norskekysten fører til redusert ytelse. Dette fører til forsinkelser ved transmisjon av data.

Oppgavetekst

1. Vurder sannsynligheten for de ulike hendelsene, ut ifra skalaen som er beskrevet nedenfor. Begrunn vurderingen din.

2. Vurder konsekvensene av de ulike hendelsene, ut ifra skalaen som er beskrevet nedenfor. Begrunn vurderingen din.

3. En risikomatrise har to akser: sannsynlighet og konsekvens. Sett opp en 4x4 risikomatrise med evalueringskriterier (grønne, gule og røde felt) og plasser hendelsene inn i risikomatrisen ut ifra dine vurderinger. (Alle de uønskede

hendelsene skal plasseres inn i samme risikomatrise.)

4. Det er fire ulike strategier for å håndtere risiko: avoid, reduce, transfer, accept. For hver av de uønskede hendelsene, velg en strategi for å håndtere risikoen og begrunn svaret ditt.

5. For to av de uønskede hendelsene, angi to mottiltak for å redusere risikoen (dvs. Fire mottiltak, to per hendelse). Spesifiser om mottiltakene er fysiske, administrative eller tekniske. For hvert mottiltak, er det sannsynligheten eller konsekvensen som reduseres?

Det er helt greit, og ofte en fordel, å gjøre antakelser om systemet når detaljer ikke er gitt i oppgavebeskrivelsen. Gjør de antakelsene du mener er fornuftig og skriv dem i besvarelsen din.

Vurderingskriterier

Øving 2 gir 10% av total karakter i TTM4185.
Det gis en poengsum fra 0-100 poeng. Poengsum gis i en skala med fem-poengere, det vil si 100, 95, 90 etc.

1. Alle de fem uønskede hendelser er beskrevet med vurdering av konsekvens og vurdering av sannsynlighet med begrunnelse- inntil 40 poeng.
2. Det er inkludert en risikomatrise der de ulike uønskede hendelsene er tydelig markert - inntil 10 poeng.
3. Alle de fem uønskede hendelsene er beskrevet med strategi for å håndtere risikoen. Det bør henvises til risikomatrisen ved valg av strategi for håndtering - inntil 30 poeng og valget må være begrunnet.
4. Mottiltak for to hendelser er beskrevet med beskrivelse av type tiltak og om tiltaket reduserer sannsynligheten eller konsekvens av den uønskede hendelsen – inntil 20 poeng.

Hver oppmerksom på at læringsassistentene kan trekke poeng hvis besvarelsen er uklar, rotete eller har dårlig språk. For full poengsum bør det komme klart frem hva kandidaten svarer på de ulike oppgavene. Bruk gjerne kursiv og fet skrift til å fremheve tekst samt bruke lister eller tabeller.

Skala for sannsynlighet

1. Usannsynlig
    a. Sjeldnere enn hvert tiende år
    b. Sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet og fungerer etter hensikten
    c. Tiltakene kan kun omgås/brytes av egne medarbeidere med gode ressurser, og god/fullstendig kjennskap til tiltakene.
    d. Eksternt personell kan ikke omgå/bryte tiltakene. Sikkerhetsbrudd kan kun skje ved at egne medarbeidere opptrer med overlegg og har spesiell kompetanse eller kunnskap.
    e. Utenforstående må ha spisskompetanse og et samarbeid med personer i virksomheten.

2. Mindre sannsynlig
    a. Årlig
    b. Sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet og fungerer etter hensikten.
    c. Tiltakene kan likevel omgås/brytes av egne medarbeidere med små til normale ressurser, som i tillegg har normal kjennskap til tiltakene.
    d. Eksternt personell trenger gode ressurser, og god/fullstendig kjennskap til tiltakene for å omgå/bryte disse.
    e. Utenforstående må opptre med overlegg og ha noe kunnskap om interne forhold (med hensikt og plan, eksempelvis ved at flere tiltak brytes i riktig rekkefølge) for å omgå/bryte sikkerhetstiltakene.

3. Mulig
    a. Flere ganger i året
    b. Sikkerhetstiltak er ikke fullt etablert, eller fungerer ikke etter hensikten.
    c. Egne medarbeidere trenger kun små til normale ressurser for å omgå/bryte tiltakene, det er ikke nødvendig med kjennskap til tiltakene.
    d. Eksternt personell trenger normal kjennskap til tiltakene (eksempelvis til hvilke rutiner som gjelder, eller hvordan sikkerhetsteknologi er implementert), i tillegg til små/normale ressurser. Inngrep forutsetter forsett (bevisst eller aktivt) for å bryte sikkerhetstiltakene

4. Sannsynlig
    a. Flere ganger pr. måned
    b. Sikkerhetstiltak er ikke etablert, eller kan omgås/brytes av egne medarbeidere og eksternt personell med små til normale ressurser.
    c. Det er ikke nødvendig med kjennskap til tiltakene.
    d. Sikkerhetsbrudd kan skje ved uaktsomhet (ubevisst eller uten forsett) av egne medarbeidere eller utenforstående.

Skala for konsekvens

1. Ubetydelig
    a. Ubetydelig stans i tjenesten (få minutter)
    b. Intet uautorisert innsyn i datasett
    c. Datasett eller andre styringsdata er komplett og riktig
    d. Ikke fare for skip eller andre fysiske elementer
    e. Ikke brudd på lovverk eller reguleringer
    f. Ubetydelig økonomisk tap
    g. Ikke tap av renommé eller rykte

2. Moderat
    a. Kort stans i tjenesten (timer)
    b. Uautorisert innsyn i lite datasett
    c. Svært små mangler i datasett slik at data som ikke er kritisk for driften blir ufullstendig
    d. Mindre fare for skade på skip eller andre fysiske elementer
    e. Mindre brudd på lovverk eller reguleringer
    f. Gjenopprettelig økonomisk tap
    g. Moderat tap av renommé eller rykte ovenfor virksomhetens omgivelser eller kunder

3. Alvorlig
    a. Moderat stans i tjenesten (inntil en dag)
    b. Uautorisert innsyn i større datasett, mulighet for endring
    c. Viktig informasjon mangler i datasett
    d. Fare for skade på skip eller andre fysiske elementer
    e. Alvorlig brudd på lovverk
    f. Fare for personskader grunnet feil i datasett
    g. Alvorlig økonomisk tap
    h. Alvorlig tap av renommé eller rykte

4. Kritisk
    a. Lang stans i tjenesten (mange dager)
    b. Fullt uautorisert innsyn eller mulighet for endring av hele datasett
    c. Kritisk informasjon mangler i datasett
    d. Fare for stor skade på skip eller i ytterste konsekvens tap av skipet
    e. Kritisk lovbrudd
    f. Tap av liv
    g. Uopprettelig økonomisk tap

Beskrivelse av case - TTM4185

Norge har alltid vært avhengig av sjøen og havet. Hoveddelen av befolkningen og næringsvirksomheten er lokalisert langs kysten, og sjøveien er avgjørende som ferdselsåre både for personer og gods [1]. Internasjonal handel er viktig for norsk økonomi, og sjøtransport er den dominerende transportformen for gods inn og ut av Norge, og i store deler av verden. Transport regnes som en av seks kritiske infrastrukturer i Norge [2].

I dag har skip begrensede muligheter til datakommunikasjon under transport på åpent hav. Hvis en tilkobling først gjøres har den som regel svært begrenset båndbredde som er upålitelig (dårlig dekning, høyt pakketap) og medfører en høy kostnad. I tillegg har mannskapet lite kunnskap om vedlikehold av de IT-systemene som er ombord på skipene i dag som kompliserer bruken av nye IT-systemer. Skip på åpent hav har liten mulighet til å anskaffe nødvendige komponenter hvis utstyr skulle feile, noe som gjør at man stiller høye krav til utstyret.

Rederibransjen har en økende grad av digitalisering som vil gi høyere tilgjengelighet, mer funksjonalitet og økt effektivitet. Dette kan samtidig introdusere nye sårbarheter som ondsinnede aktører kan utnytte. Digitaliseringen innebærer sammenkoblingen av IT-systemene på land med de datasystemene som eksisterer på et skip. Slike datasystemer finnes i mange varianter på et skip i dag. For eksempel styringssystemer med tilknytning til motor og navigering, og de systemer som hører til spesifikke formål med forskjellige skip (last, brønnboring, kranoperasjoner, containervirksomhet, etc.). Disse systemene er i stadig større grad koblet til systemene på broen (ECDIS [3], NAVTEX [4]) og til administrative systemer. I tillegg kan de fleste av datasystemene på et skip fjernstyres fra land. Dette stiller høye krav til sikkerhet og robusthet av teknologien som brukes på skipene.

Den kommende VHF Data Exchange System (VDES) [5] standarden er sentral i den kommende teknologiske utviklingen i sektoren. Teknisk Ukeblad har skrevet en artikkel om teknologien som dere kan lese her [6]. VDES vil gi skip datakommunikasjonsforbindelse med høyere hastighet, økt pålitelighet (bedre dekning, mindre pakketap), og lavere kostnad for data sendt over VDES enn hva som er mulig i dag. VDES inkluderer også en konstellasjon av satellitter som vil gi skipene Internett-tilkobling over hele verden.

VDES tilbyr tre ulike delsystemer:

- Automatic Identification System (AIS), som er en forbedret versjon av allerede eksisterende antikollisjons-hjelpemiddel for skipsfarten. Fartøyer som har utstyr for AIS om bord sender ut og utveksler informasjon om sin identitet, posisjon, fart, kurs, planlagte rute osv.
- Application Specific Messages (ASM) som er et definert meldingsformat for meldinger som sendes over VDES.
- VHF Data Exchange (VDE) som er en åpen kommunikasjonskanal som kan brukes av alle applikasjoner.

VDES kan brukes til skip-til-skip, skip-til-land og skip-til-infrastruktur kommunikasjon.

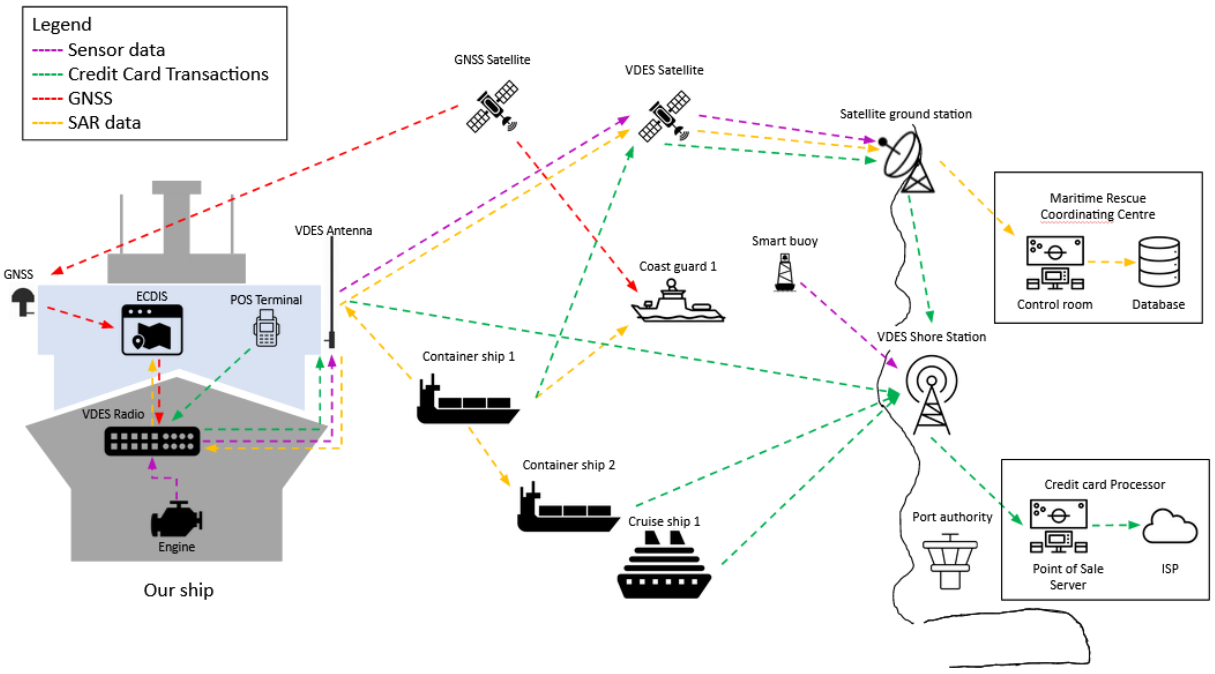
Etter hvert som VDES blir tatt i bruk av flere og flere selskaper vil behovet for sikkerhet (security) være stort. Det er fortsatt mange usikkerhetsmomenter knyttet til sikkerheten i VDES og det er grunn til å tro at systemet har forbedringspotensialer. VDES er tiltenkt å overta en rekke forskjellige applikasjoner når det blir tatt i bruk. For å begrense omfanget i denne casen har vi valgt ut to spesifikke bruksområder.
Denne casen tar for seg følgende to applikasjoner:

- **Søk- og redningsoperasjoner:**
  Koordinering og gjennomføring av søk- og redningsoperasjoner (SAR) til havs vil forbedres ved innføring av VDES. For eksempel vil redningssentralene på land automatisk kunne lokalisere og kontakte skip som befinner seg nær ulykkesplassen. I tillegg kan søkeprosessen effektiviseres, gjennom digital utveksling av søkekoordinater og visualisering av søkemønster på elektroniske kart.

- **Kredittkortbetalinger:**
  Verifisering av kortbetalinger vil bli et viktig bruksområde for VDES på passasjer- og cruiseskip. Trådløse Point-of-Sale (POS) terminaler kan kobles til et WiFi-nettverk på skipet, slik at beløpet og gyldigheten av kortet kan kontrolleres før betalingen gjennomføres. Betalingsforespørslene vil deretter sendes fra skipet til en landbasert POS server over VDES, og besvares med enten "approved" eller "rejected".

Disse to applikasjonene vil bli en integrert del av systemene om bord på skip og i de landbaserte systemene. Funksjonaliteten vil være avhengig av at systemene samhandler med flere komponenter som f.eks. utstyr og programvare om bord i skipene, satellitter og antenner.

Figuren under er et eksempel på et utsnitt av infrastrukturen til VDE. Under bildet er en kort forklaring av de ulike komponentene. Det er viktig å påpeke at figuren er ment som veiledning og at den ikke er fullstendig. Flere elementer enn de som er med i figuren kan tas med og evalueres i besvarelsen.



Beskrivelse av figuren

VDES Radio: Tilbyr datakommunikasjon til systemene på skipet. Kommunikasjon til andre båter og til land går via radio når de er innenfor rekkevidde og via satellitter når de er utenfor rekkevidde.

VDES Shore Station: Brukes for å videresende kommunikasjonen til og fra skip som er innenfor rekkevidde.

VDES Satellite: Brukes for å videresende kommunikasjon til og fra skip som ikke er innenfor rekkevidde til den landbaserte infrastrukturen (VDES shore station).

Satellite ground station: Sender og mottar data fra VDES satellitter, og kan brukes som kommandosenter for satellittnettverket.

GNSS Satellite: Global Navigation Satellite Systems. Sender signaler for avstandsbestemmelse samt blant annet bane- og klokkedata til brukerne. Brukt i globale GNSS systemer (GPS, GLONASS, GALILEO & BeiDou).

Maritime Rescue Coordinating Centre (GRCC): Mottar nødmeldinger fra skip og/eller andre aktører. Koordinerer så redningsarbeidet.

Point of Sale Server (POS server): Point of Sale serveren kommuniserer med POS terminalene på skipene. POS serveren kommuniserer videre på land til banktjenestene for å reservere beløp og gjennomføre betalinger.

Port Authority: Havnemyndighet (ikke brukt i dette caset)

ECDIS: Electronic Chart Display and Information System. Viser skipets egen og andre skips posisjoner på et elektronisk kart i sanntid. Mottar informasjon fra GNSS-antennen og VDES radio (AIS).

GNSS Antenna (On ship): GNSS-antennen tar imot GNSS signaler fra satellitter som brukes av ECDIS og VDES radioen.

VDES Antenna (On ship): VDES-antennen tar imot signaler over VDES fra andre skip, satellitter, eller infrastruktur på land.

[1] Regjeringen. Innledning, Lov om havner og farvann (havne- og farvannsloven). https://www.regjeringen.no/no/dokumenter/prop.-86-l-20182019/id2640729/?ch=3

[2] Regjeringen. 10.6 Transport, NOU 2006: 6 Når sikkerheten er viktigst — Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner, 2006. https://www.regjeringen.no/no/dokumenter/nou-2006-6/id157408/?q=kritiske%20samfunnsfunksjoner&ch=3#kap10-6

[3] International Maritime Organization. Electronic Nautical Charts (ENC) and Electronic Chart Display and Information Systems (ECDIS). http://www.imo.org/en/OurWork/Safety/Navigation/Pages/ElectronicCharts.aspx

[4] NAVTEX Navigational Telex https://www.universal-radio.com/catalog/decoders/navtex.html

[5] Blasco et al. VHF Data Exchange System (VDES): An enabling technology for maritime communications. *CEAS Space Journal,* January 2017 https://www.researchgate.net/publication/316075615_VHF_Data_Exchange_System_VDES_An_enabling_technology_for_maritime_communications

[6] Teknisk Ukeblad. VDES - VHF DATA EXCHANGE SYSTEM. https://www.tu.no/artikler/alle-storre-skip-bruker-ais-systemet-na-utvikles-neste-generasjon/276150