ISPS-NYTT

OM MARITIM SIKRING I NORGE

KYSTVERKET

NUMMER 4 – 2021
22 DESEMBER

I DENNE UTGAVEN:

Trusselaktører tar ikke hensyn til smitteverntiltak

Begrepet samfunnssikkerhet handler om vår kollektive evne til å verne oss mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og som setter liv og helse i fare. Slike hendelser kan være utløst av naturen, være et utslag av tekniske eller menneskelige feil, eller bevisste handlinger.

Direktoratet for samfunnssikkerhet og beredskap (DSB) beskriver samfunnets kritiske funksjoner som funksjoner samfunnet ikke kan klare seg uten i syv døgn eller kortere, uten at dette truer befolkningens sikkerhet og/eller trygghet. Disse samfunnsfunksjonene, mener DSB, ivaretar grunnleggende verdier og kan derfor betraktes som «grunnpilarer for samfunnets robusthet». Grunnpilarene er delt i tre overordnede kategorier som igjen består av totalt 14 underkategorier vi kjenner som samfunnets kritiske funksjoner.

Pandemien har demonstrert hvordan avhengigheter i samfunnssikkerhetskjeden kan påvirke samfunnets funksjonalitet. Pandemien har ført til knapphet på råvarer og begrenset produksjon.

Samtidig er etterspørselen rekordhøy og forsyningskjedene er overbelastet.

Dette gjenspeiles særlig i containerterminaler. Når tilbud og etterspørsel påvirkes, endrer varer verdi. Tollvesenet melder om økning i kriminell virksomhet i europeiske havneanlegg, og havnearbeidere tilbys opp mot 100 000 Euro for å plassere last slik at kriminelle nettverk får tilgang. Slik smugling er et eksempel på finansiering av kriminell- og terror relatert virksomhet.

Eksempelet viser at sikring av verdikjedene er viktig, og at samfunnssikkerhet er avhengig av sikre havner og havneanlegg. Trusler tar ikke hensyn til smitteverntiltak. Avdelingen for maritim sikring vil derfor ha fokus på tilsynsaktivitet gjennom 2022. Vi skal gripe momentet og utnytte digitale flater for å gjennomføre oppdraget vårt. I våre tilsyn forventer vi at havneanlegg gjennomfører øvelser og driller innenfor mulighetsrommet de er gitt, og at sikringstiltak etterleves.

Hilsen
Richard Utne
avdelingsleder
avdelingen for maritim sikring

Bildet: Samfunnets kritiske funksjoner (DSB 2016)

Tid for havneanleggenes årlige rapportering i SafeSeaNet Norway

Den årlige rapporteringen i SafeSeaNet Norway (SSNN) åpnes 3. januar 2022.

I en tid med pandemi og færre gjennomførte myndighetstilsyn er den årlige rapporteringen viktig for å danne et bilde av sikringstilstanden i norske havneanlegg. Resultatet vil avdekke om det er områder innen sikring som Kystverket bør ha økt fokus på. Kystverket oppfordrer alle havneanlegg til å sende inn utfylt rapporteringsskjema.

Det skal lønne seg å være god. Ut fra en risikobasert tilnærming vil Kystverket prioritere ressurser der risikoen for at sikringshendelser kan oppstå er størst. Havneanlegg som ikke utfører sikringstiltak, som beskrevet i egen sikringsplan, vil ha en høyere sårbarhet. Årlig rapportering gir et bilde av hvordan havneanleggene jobber med å forebygge sikringshendelser, noe som vil ha betydning for Kystverkets tilsynsplan.

De havneanleggene som har en enklere implementering av ISPS regelverket etter § 11 i forskrift om sikring av havneanlegg vil motta et eget rapporteringsskjema. Rapporteringen via SSNN erstatter rapporteringsskjema som det vises til i sikringsplaner for § 11 havneanlegg.

Sikringslederne vil motta en epost når rapporteringen åpnes. Kontroller derfor at kontaktinformasjon til havneanleggets sikringsleder er korrekt i SSNN. Sikringsleder må være bruker av SSNN og ha tilgang til «sitt havneanlegg». Om sikringsleder ikke har opprettet bruker må vedkommende registreres seg så raskt som mulig. Ved spørsmål om SafeSeaNet Norway, ta kontakt med Kystverket, support.ssnn@kystverket.no.

Fortsatt må hvert enkelt havneanlegg rapportere individuelt og det er ikke mulig å melde inn en rapport for flere havneanlegg. Siste frist for å rapportere inn er 31. januar 2022. Ved spørsmål som selve rapporteringen ta kontakt med seniorrådgiver ved avdelingen for maritim sikring, Grethe Westre, grethe.westre@kystverket.no.

SafeSeaNet Norway

Julen er også høytid for cyberangrep

De fleste havneanlegg har på en eller annen måte en avhengighet til datastyrte funksjoner. I følge NSM (Nasjonal Sikkerhetsmyndighet) er tiden fremover også høytid for angrep i det digitale rom. Dette henger sammen med at trusselaktører utnytter at det ofte er lavere beredskap på fridager.

NSM har tre råd for digital beredskap gjennom julen:

- Sjekk at kriseplanene dine holder mål og finn ut hvilke ansatte som kan være tilgjengelige gjennom julen hvis du må kalle inn personell. Du trenger både ansatte med teknisk kompetanse, kommunikasjonsmedarbeidere, og ledelse i tilfelle en digital krise.
- Gå gjennom grunnleggende sikkerhetstiltak i virksomheten, og dobbeltsjekk at totrinnsbekreftelse og sterke passord er på plass. Se NSMs nettsider for detaljer.
- Minn ansatte om at julen er høysesong for forsøk på digital utpressing, phishing og andre dataangrep.

Les hele artikkelen fra NSM her

Tips til kvartalsvis drill

Test om sikringsorganisasjonen har tilgang til nødvendige deler av sikringsplanen. Gjør dette ved å spørre personer på ulike nivå i organisasjonen om de har tilgang til relevante prosedyrer, tiltakskort, instrukser og skjema. Det er viktig at sikringsleder har satt seg inn i dette før testen gjennomføres.

Eksempler på relevante dokumenter kan være:

- Ansvar og oppgaver for vedkommende
- Prosedyre for adgangskontroll
- Instruks for visitasjon
- Instruks for gjennomsøkning av biler
- Instruks for godskontroll (tilpasset aktuell godstype)
- Tiltakskort ved eskalering av sikringsnivå
- Tiltakskort ved sikringshendelse
- Skjema for klargjøring av kai før ISPS-anløp
- Skjema for hendelsesrapport
- IT-løsninger

Drillens mål er å belyse om sikringsplanen er tilgjengelig og kjent for sikringspersonellet i tråd med ansvar og oppgaver til den enkelte. Skriv en rapport etter drillen med dato, tema og deltakere, samt oversikt over resultat og nødvendig oppfølging.

Vi i avdelingen for maritim sikring ønsker alle en sikker jul

Foto: Torstein Gamst pixlight.no

KYSTVERKET

Sentral postadresse: Kystverket, postboks 1502, 6025 ÅLESUND

Telefon: +47 07847

Internett: www.kystverket.no

E-post: post@kystverket.no

Varsling om ISPS sikringshendelser: +47 35 57 26 25