Vis på internett

KYSTVERKET

ISPS-nytt

ISPS-nytt

ISPS-nytt har i en årrekke blitt sendt ut til alle sikringsledere. Alle kan enkelt melde seg av og på, eller laste ned nyhetsbrevet på **våre nettsider**. Her finner du også tidligere nyhetsbrev.

Send oss gjerne en tilbakemelding til **maritim-sikring@kystverket.no** hvis du har tips eller ønsker om innhold i fremtidige nyhetsbrev.

Kvartalsvis situasjonsorientering fra Kystverket

Avdelingen for maritim sikring inviterer til kvartalsvis situasjonsorientering 21 juni kl. 13.00-13.30. Orienteringen blir avholdt med bruk av Teams. Sikringsledere for havn og havneanlegg har mottatt invitasjon på epost. Lenken kan deles dersom andre i virksomheten ønsker å delta.

Vi vil orientere om cruise anløp og regler for dette, avdelingens kommunikasjon utad, rapporterte sikringshendelser og sikringsrisikoanalyse. Vi håper at så mange som mulig har anledning å delta nå før sommerferien slår inn for fullt.

Anløp av cruiseskip, hva gjelder?

Cruiseskip kan kun anløpe havneanlegg som har en ISPS-godkjenning som omfatter cruise. Hva det enkelte havneanlegg er godkjent for, fremgår blant annet av godkjenningsbeviset. Det er kun disse aktivitetene og operasjonene som er vurdert i havneanleggets sikringsrisikoanalyse og havneanlegget har dermed sikringstiltak tilpasset de aktivitetene de er godkjent for. Dersom havneanlegget skal starte med en ny type operasjon eller aktivitet, eksempelvis motta passasjertrafikk når de ikke er godkjent for dette, vil dette være en vesentlig endring i havneanlegget som krever en oppdatering av både sikringsrisikoanalysen og sikringsplanen.

I Kystverkets karttjeneste **Kystinfo** finnes en oversikt over godkjente cruisedestinasjoner. **Se Kystverkets nettsider** for mer informasjon om hva som gjelder ved mottak av cruise og passasjertrafikk.

Sanksjoner mot russiske skip

Kystverket har opprettet en samleside for spørsmål som kan dukke opp i forbindelse med sanksjonene som er innført mot Russland. Her finnes blant annet informasjon om havneforbudet og relevante kontaktpunkt ved spørsmål.

Les mer

Anløpsmeldinger i SafeSeaNet Norway

Skip som er omfattet av ISPS regelverket skal gi havneanlegget sikringsrelaterte opplysninger før ankomst. Informasjonen skal gis via meldingssystemet SafeSeaNet Norway (SSNN). Skipet skal innledningsvis velge hvilken havn den anløper. Deretter kan skipet, avhengig av behov, velge om havnen eller havneanlegget skal tildele kaiplass. Skip kan også sende inn en kaiforespørsel (quay request) på en konkret kai i et havneanlegg.

Forespørsel fra skip håndteres i havneanleggets «Quay request» - modul. At skipet kan velge havneanlegg, for deretter å bli tildelt kaiplass er en ny funksjon i SSNN. Hensikten med denne forbedringen er at de havneanlegg som har flere kaier selv kan tildele kaiplass. Skipet vet ikke nødvendigvis hvilken kai det skal anløpe når seilas legges i SSNN.

For at forespørselen skal bli besvart må havneanlegget velge hvilken kai som skipet skal anløpe (changed quay). Agent/skip må bekrefte endringen for at anløpet skal få status «godkjent».

Har du spørsmål eller trenger hjelp, ta kontakt med Kystverkets SSNN Support tlf 35 57 26 25 eller **support.ssnn@kystverket.no**

Tips til kvartalsvis drill

Hvordan oppfatter vi en trussel?

Sikringsplanen skal beskrive hvordan havneanlegget skal håndtere kjente trusler. Ofte omfatter dette et skjema for registrering av en bombetrussel eller andre trusler som ringes inn til havneanlegget. Denne drillen kan brukes til å teste dette skjemaet og hvordan vi opplever en trusselsituasjon.

Den som har ansvar for gjennomføring av drillen lager et lydopptak av en bombetrussel, eller annen trussel som blir ringt inn til havneanlegget. Her kan man være litt kreativ når det kommer til dialekt, tonefall og intensitet. Lydklippet blir spilt av til deltakerne som også har fått utdelt skjema for registrering av trusselmeldingen. Deltakeren blir bedt om å fylle ut skjema etter beste evne. Temaet for drillen kan gjerne være ukjent for deltakerne.

Skjemaene samles inn og resultatene gås gjennom i plenum. Resultatene kan brukes til å diskutere hvordan situasjonen ble oppfatte, og om skjema ble fylt ut likt av alle deltakere. Et annet moment for evaluering er hvor vidt alle vet hvor skjemaet er lokalisert og om det var praktisk å bruke. Det vil også være naturlig å minne deltakeren om å være årvåken ovenfor situasjoner som kan ha betydning for sikringen i havneanlegget og virksomheten. Dersom sikringsplanen beskriver håndtering av andre trusselsituasjoner kan disse også være utgangspunkt for drillen.

Husk å dokumentere gjennomført drill med tidspunkt, tema, deltakere, evaluering og evt. handlingsplan. Vurder om sikringsplan og evt. underliggende prosedyrer, instrukser, brosjyrer etc. må oppdateres. Oppdatert sikringsplan sendes Kystverket via **eDialog**

Cybersecurity – en kake?

Her er et tankeeksperiment du må gjøre før du leser resten av teksten: Lukk øynene og tenk på en kake. Ikke les videre før du ser for deg kaken.

Hva slags kake så du for deg? Var det en bløtkake med krem og bær, eller var det kanskje en sjokoladekake? Vi mennesker tenker i bilder, men tankebildene våre er ikke like. Kaken du så for deg var ikke den samme som jeg så for meg. Slik er det med risiko også. Vi oppfatter den ulikt. Skal vi bake den samme kaken gjelder det å unngå en tilfeldig røre av ingredienser.

Når man skal vurdere risiko er det viktig å beskrive hva man ønsker å beskytte. Da gjelder det å se for seg det samme risikobildet. Vi må med andre ord ha et felles sett med begreper og forståelse for hva vi mener når vi beskriver verdier, trusler og sårbarheter.

Terrortrusselen, som det maritime sikringsregelverket har som formål å begrense konsekvensene av, er fortsatt reell. Men, den sikkerhetspolitiske utviklingen det siste tiåret byr på et nytt risikobilde for ISPS-havneanlegg. Eksempler på dette er aktivitet som påvirker klima og natur og som medfører økt aktivisme mot landanlegg. Raske endringer i behov for utvikling av energiforsyning, kommunikasjonsløsninger og teknologi øker faren for kartlegging og spionasje mot maritim infrastruktur. Og, ikke minst må vi beskytte oss mot digitale trusler.

Digitale trusler er for mange et nytt og komplekst trusselbilde. Når vi kaller det cybertrusler høres det enda mer abstrakt ut. Nasjonal sikkerhetsmyndighet (NSM) har tidligere varslet om at krigen i Ukraina aktualiserer betydningen av å være årvåken om cyberhendelser, og ha gode og gjennomøvde beredskapsplaner. Nå ønsker NSM at virksomheter forsikrer seg om at de klarer å håndtere tjenestenektangrep. NSM forklarer at eksempler på tiltak kan være å ta kontakt med leverandører av internettilknytning, datasentertjenester, skytjenester og andre tjenester som kan begrense sårbarheten til virksomhetens egen IKT- infrastruktur.

Da ISPS-regelverket ble innført i Norge var det mange som ikke så nødvendigheten av å gjerde inn havneanlegg. I dag er et havneanlegg ofte avhengig av IKT-baserte systemer som har behov for egne digitale gjerder. De som leverer IKT-løsningen til havneanlegget vet ofte ikke hvilken verdi denne tjenesten har, eller hvilke funksjoner havneanlegget representerer for samfunnet. Et robust sikringssystem er derfor avhengig et felles sett med begreper mellom leverandør av tjenester, sikringslederen og den som lager sikringsrisikoanalysen.

En utfordring knyttet til den raske teknologiske utviklingen, er nettopp det at vi tenker i bilder. Sikringsrisikoanalyser (PFSA) er ofte et øyeblikksbilde, men som skal beskrive risiko inntil fem år frem i tid. Den raske teknologiske utviklingen tilsier imidlertid at fremtidens tilnærminger til sikringsrisikoanalyser bør innebære beskrivelse av verdier og verdikjeder og oppdateres ofte. Hvis ikke kan vi ende opp med en tilfeldig røre av konsepter og ideer om risiko som fører til dårlig sikkerhet.

Trøsten er at alle kan bake, det kreves bare å følge oppskriften. Og litt øvelse.

Nyttige lenker:

Port Cybersecurity - Good practices for cybersecurity in the maritime sector — ENISA (europa.eu)

Varsle Kystverket om ISPS sikringshendelser

Telefon: 35 57 26 25 (Tast 1 for å varsle ISPS-vakten)

E-post: **isps@kystverket.no**

E-postadressen til ISPS-vakten kan blant annet benyttes for å rapportere om allerede avklarte sikringshendelser, sende rapporter etter sikringshendelser eller sende forespørsler om beredskapsvaktens deltakelse ved øvelser i havneanlegg.

ISPS-nytt blir utgitt av Kystverkets avdeling for maritim sikring, og er rettet mot de som har ansvar eller interesser innenfor maritim sikring.

Formålet med nyhetsbrevet er å øke kunnskap, motivasjon og sikringsbevissthet hos sikringsledere og andre med oppgaver innenfor maritim sikring. I hovedsak gjelder dette havneanlegg som er omfattet av forskrift om sikring av havneanlegg, og havner omfattet av forskrift om sikring av havner.

Hvis du ikke ønsker å motta nyhetsbrevet i fremtiden, kan du melde deg av nederst i e-posten.

KYSTVERKET

© Kystverket

Redaktør: Beate Rødland Rabben Sperre
maritim-sikring@kystverket.no

Ønsker du å endre noe?
You can update your preferences or unsubscribe