Vis på internett

KYSTVERKET

# 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.

# Et nytt risikobilde – og sikring av havneanlegg

**Kystverket og våre godkjente sikringsrisikovirksomheter (RSO) har i møte med Etterretningstjenesten (E-tjenesten), Politiets sikkerhetstjeneste (PST) og Nasjonal sikkerhetsmyndighet (NSM) gått gjennom årets nasjonale trusselvurderinger. Her gjengir vi hovedtrekkene og kommenterer noen punkter som er relevante for sikring av havneanlegg.**

**Et nytt risikobilde**
Krigen i Ukraina har fundamentalt endret relasjonen mellom Russland og vestlige land, inkludert Norge. Dette påvirker trusselen fra russiske etterretningstjenester i Norge. Vi må forvente at den uforutsigbare sikkerhetspolitiske situasjonen vedvarer eller tilspisser seg. Sabotasje mot gassrørledningene Nord Stream 1 og 2 i Østersjøen, høy kartleggingsaktivitet mot norsk infrastruktur og flere tilfeller av alvorlig innsidevirksomhet er noen eksempler fra det siste året som belyser spennet av utfordringer vi står overfor.

I FOKUS 2023 gir E-tjenesten krigen i Ukraina og Russland mest oppmerksomhet. Men, også andre utviklingstrekk kommenteres. Rivaliseringen mellom Kina og USA tiltar, og Kinas utvikling får i økende grad betydning for Norge. Selv om terrortrusselen mot Vesten er lavere enn for noen år siden, er det tragiske angrepet i Oslo i fjor sommer en påminnelse om at trusselen fra terrorisme fortsatt er reell.

I NASJONAL TRUSSELVURDERING 2023 gir PST en vurdering av trusselbildet som det norske samfunnet står overfor. PST setter søkelys på etterretningstrusselen, med særskilt vekt på russisk og kinesisk etterretning, samt på terrortrusselen og trusler mot myndighetspersoner. Terrortrusselen vil preges av at ekstremister i større grad tilpasser ideologi, modus og valg av mål ut fra egne preferanser. Dette kan føre til at det blir mer utfordrende å avdekke terrorplanlegging.

I RISIKO 2023 peker NSM på hvordan virksomheter bør redusere sårbarheter for å gjøre trusselaktørenes jobb vanskeligere. Selv om en virksomhet har god fysisk og digital sikkerhet, så kan en trusselaktør utnytte underleverandører som er dårligere

**Risiko kan reduseres**
Sikringsrisikoanalyser (PFSA) og sikringsplaner (PFSP) må oppdateres i takt med endringer i risikobildet.

Havneanleggene må kjenne sine verdier, hvem som kan true dem og eventuell sårbarhet i sikringen. Dette gjelder også andre steder i verdikjeden. God sikring starter med tiltakene vi vet fungerer, som tetter hull der angriperne lett kommer seg inn. Vi må ta inn over oss at vi har en ny sikkerhetspolitisk situasjon, som kan utvikle seg til det verre.

NSM ser stadig utnyttelse av menneskelige, teknologiske og organisatoriske sårbarheter for å understøtte ondsinnede cyberoperasjoner mot flere norske virksomheter. Digitale trusselaktører utnytter også sårbarheter som svake passord, utdatert programvare og manglende to-faktorautentisering for å få urettmessig tilgang til IKT-systemer.

Phishingangrep vil fremdeles være den enkleste og mest brukte fremgangsmåten for å få tilgang til informasjon om en person eller virksomhet. Dette er en metode som benyttes av forskjellige trusselaktører i forbindelse med digitale angrep og svindelforsøk. Eksempel på phishing er å få deg til å klikke på en lenke i en e-post som deretter stjeler informasjon, laster ned et virus eller stenger systemet til din virksomhet.

Trusselaktørene går ikke alltid direkte på virksomhetenes nettverk. Enkeltpersoner og tredjepartstjenester som virksomhetene er avhengige av, kan bli utnyttet fordi de blir ansett som enklere å angripe enn de egentlige målene.

Spearphishing er målrettede phishingangrep mot deg eller din virksomhet. Angriperen samler inn informasjon på forhånd, for eksempel om kunde, leverandør, avtaler og samarbeidspartnere. Denne informasjonen brukes så til å bygge tillit i en e-post, ved å referere til interne ting og navn som er kjent for mottageren. Igjen må du gjerne klikke på en lenke for å bli rammet.

Næringslivets sikkerhetsråd har lansert en nødplakat for digitale angrep, med viktige telefonnumre og nyttig informasjon. Den kan skrives ut, henges på veggen, og forhåpentligvis være til nytte for virksomheter som rammes av digitale angrep. Nødplakaten er utarbeidet i samarbeid med blant annet Politiet og Nasjonal sikkerhetsmyndighet.

Sikkerhetsmyndighetene har også mye oppmerksomhet på innsiderisiko. Bakgrunnssjekk eller sikkerhetsklarering er derfor ikke et tilstrekkelig virkemiddel for å unngå innsidevirksomhet. Disse temaene er behandlet utdypende i Petroleumstilsynets rapport om Håndtering av innsiderisiko.

**Du kan bidra til å forbedre det nasjonale situasjonsbildet**
Gode trusselvurderinger krever en fungerende rapporteringskjede fra årvåkenhet hos den enkelte, gjennom rapporteringssystemer hos selskapene og videre rapportering til myndighetene.

ISPS regelverket sier at en sikringshendelse er enhver mistenkelig handling eller omstendighet som utgjør en trussel mot et skip, et havneanlegg eller en havn. Dette gjelder også for cyberhendelser, som for eksempel phishing.

**Hvordan varsler du Kystverket?**

Kystverkets døgnbemannede ISPS vakt har telefon: **35 57 26 25** eller e-post isps@kystverket.no

God sikring – og god påske!

Hilsen Richard Utne
Avdelingsleder, maritim sikring

PS!

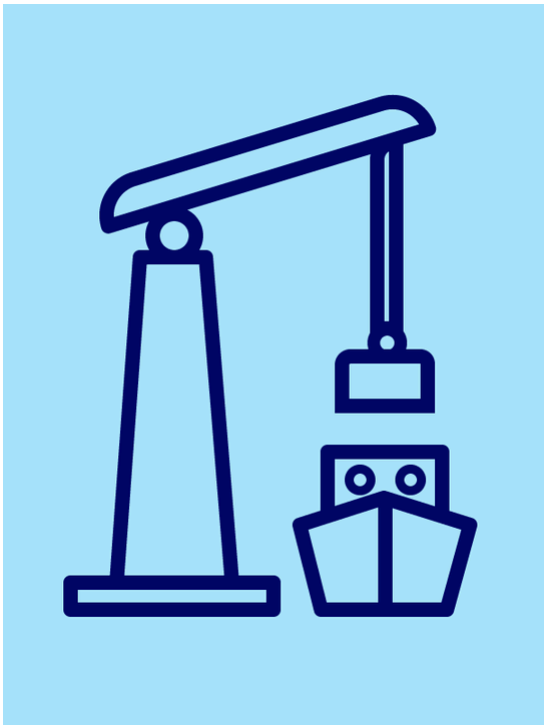
Sikkerhetstruende virksomhet og hendelser kan også varsles varsel@nsm.no eller nettsiden til PST: www.pst.no/tips-oss Vær tydelig på om det er et tips, anmeldelse eller behov for bistand. Du kan også benytte næringslivskontaktene i ditt politidistrikt for råd og bistand: https://www.politiet.no/kontakt-politiet/naringslivskontakter/

Men – husk: sikringshendelser SKAL også varsles til Kystverket!

## Resultater fra havneanleggenes rapportering i 2022

Lurer du på hvordan det står til med havneanleggenes sikringsarbeid? Nå er oppsummeringen av havneanleggenes rapportering på sikringsaktiviteter for 2022 tilgjengelig.

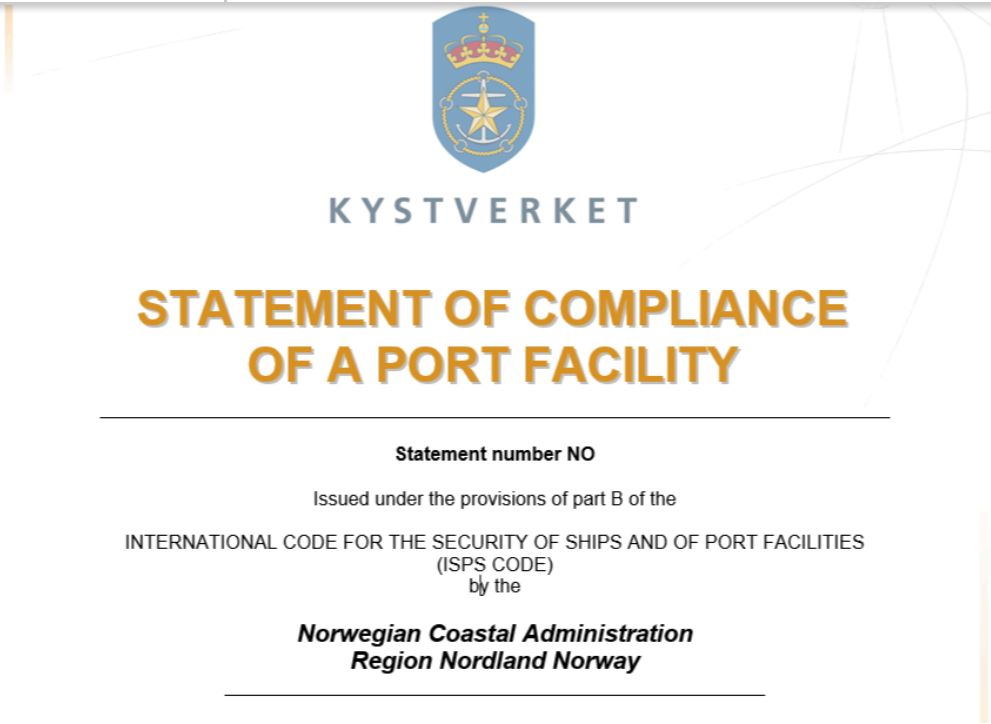
Les rapporten her



## Kvartalsvis situasjonsorientering utgår

Kystverket beklager at kvartalsvis situasjonsorientering for første kvartal 2023 utgår.

Invitasjon til neste møte med dato og innhold sendes til sikringsledere som er registrert i SafeSeaNet Norway.


KYSTVERKET

STATEMENT OF COMPLIANCE
OF A PORT FACILITY

Statement number NO

Issued under the provisions of part B of the

INTERNATIONAL CODE FOR THE SECURITY OF SHIPS AND OF PORT FACILITIES
(ISPS CODE)
by the

*Norwegian Coastal Administration*
*Region Nordland Norway*

# Forenkling av godkjenningsprosessen for havneanlegg

**Noen av dere har kanskje lagt merke til at enkelte brev fra Kystverkets avdeling for maritim sikring er betydelig kortere enn de var før. Dette har sammenheng med at vi har startet prosessen med å utarbeide nye prosedyrer med tilhørende brevmaler.**

Hensikten er tydelige og lettforståelige budskap utad, samt effektivisering og nytenkende prosesser. Dere vil derfor kunne forvente flere endringer fra Kystverket fremover.

Fra 01.01.2023 utsteder Kystverket ikke lenger Statement of Compliance (SoC). Det sendes kun ut et godkjenningsbrev der det kommer frem hvilken sikringsrisikoanalyse (PFSA) og sikringsplan (PFSP) for havneanlegget som er godkjent. Godkjenningen gis på vilkår av at havneanlegget iverksetter sikringstiltak i samsvar med PFSA og PFSP, samt at havneanlegget ikke håndterer andre skip-havn-operasjoner enn det som er beskrevet i PFSA og PFSP. Verifikasjon ved nye havneanlegg og ved fornyet godkjenning vil ikke lenger gjennomføres.

Verifikasjon av havneanlegg og utstedelse av SoC er ikke obligatoriske krav etter det internasjonale regelverket, og er heller ikke nedfelt i vår forskrift. Når vi ikke lenger skal gjennomføre verifikasjoner frigjør vi ressurser som vi heller ønsker å bruke på tilsyn.
I vår digitale hverdag er behovet for en SoC som et dokument havneanlegget kan vise fram sterkt redusert. At havneanlegget er godkjent for å ta imot internasjonal trafikk framgår både av SafeSeaNet og GISIS.

Nettsidene våre er oppdatert. Det fremkommer også her at om det er ønske om fornyet godkjenning, må havneanlegget sende inn godkjennbar sikringsrisikoanalyse og sikringsplan minimum 3 måneder før eksisterende godkjenning utløper. Dersom planverk blir sendt inn for sent eller ikke er i godkjennbar stand, vil man risikere at eksisterende godkjenning utløper før ny godkjenning er på plass.


# På tilsyn i Polen

**EMSA (European Maritime Safety Agency) er rådgivende organ for EU innenfor det maritime område. EMSA bistår EU-kommisjonen med utvikling og oppdatering av regelverk for maritim sikkerhet, samt evaluering av effektiviteten av eksisterende tiltak.**

EU-kommisjonen gjennomfører tilsyn ved havner og havneanlegg i EU- og EØS land. På disse tilsynene deltar nasjonale inspektører fra medlemslandene. Nasjonale inspektører deltar for å utveksle erfaringer og for å fremme lik praktisering av regelverket i EU og medlemslandene i EØS.

I februar ble det gjennomført tilsyn ved Swinoujscie Havn i Polen med inspektører fra Tyskland, Irland og Norge, hvor seniorrådgiver Beate Sperre fra Kystverket deltok. Tilsynsteamet bestod denne gangen av tilsynsleder fra EU-kommisjonen og 2 teamledere fra EMSA og 3 nasjonale inspektører.

Det var stort fokus på vurderingene i sikringsrisikoanalysene, for å påse at havna og havneanleggene hadde tilstrekkelige sikringstiltak og riktig grensesetting. Dette ble sett opp mot havneanleggets verdier ved skip-havn operasjoner og sannsynlige trusler for det spesifikke havneanlegget. Dersom en kritisk verdi eksempelvis er et lasthåndteringssystem forventes det at kontrollrom og servere er innenfor havneanleggets adgangsbegrenset område, samt at sikringstiltakene forhindrer uautorisert adgang, både fysisk og elektronisk.

Når det gjelder etterlevelse av sikringsplanen ble det fremhevet viktigheten av en god sikkerhetsstyring. I tillegg til opplæring, øvelser og driller, ble det presisert at periodisk internrevisjon og årlig gjennomgang av sikringsplan med involvering av ledelsen også var viktig som måleparametere for om man har gode nok sikringstiltak. Ved øvelser og driller skal det testes om sikringsplanens prosedyrer følges, og om opplæringen som er gitt er tilstrekkelig. Ved periodisk gjennomgang skal man se på konklusjoner fra øvelser, driller og internrevisjon for å vurdere om noen av sikringsplanens prosedyrer må

Beate deltok på tilsyn i 3 ulike havneanlegg, og har tatt med seg nyttige erfaringer tilbake til avdelingen for maritim sikring.

# Tips til kvartalsvis drill

## Hvilke metoder og virkemidler vil fremmede stater bruke i Norge?

Ifølge trusselvurderingene som Richard omtalte innledningsvis, vil fremmede staters etterretningstjenester benytte et bredt spekter av metoder og virkemidler i Norge. De mest tenkelige metodene er nettverksoperasjoner/cyberoperasjoner, rekruttering av kilder, digital og fysisk sabotasje, påvirkningsoperasjoner, fordekt anskaffelsesvirksomhet og ulovlig kunnskapsoverføring og overvåkning og trusler. Les mer om disse metodene på side 15 i nasjonal trusselvurdering 2023.

Drøft hvor vidt verdier i havneanlegget kan være mål for disse metodene. Sikringsplanen beskriver ulike tiltak som skal forhindre tilsiktede handlinger. Vil disse være egnet til å hindre metodene dere nettopp har drøftet? Husk at verdier i havneanlegget kan være en del av en verdikjede som kan ha betydning for sikkerheten til andre.

Husk å dokumentere gjennomført drill med tidspunkt, tema, deltakere, evaluering og forbedringspunkter.


## 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

Redaktør: Joakim Flatøy Aae
maritim-sikring@kystverket.no

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