KYSTVERKET

ISPS-nytt

4. kvartal 16. desember 2024

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 vårenettsider. 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.

Julehilsen – Maritim sikring 2024

2024 har vært et år preget av betydelige endringer og nye utfordringer innen maritim sikring. Siden vi ble samlet som en nasjonal avdeling i 2021, med ansvar for forskriftene om sikring av havn og havneanlegg, har vårt ansvarsområde utvidet seg betraktelig.

I dag har vi også ansvar for forskriften om sikker lasting og lossing av bulkskip, havneberedskapsforskriften, og fra 2025 trer den nye digitalsikkerhetsforskriften i kraft. I tillegg gjennomfører vi verdikartlegging av norske kommunale havner etter sikkerhetsloven og håndter er løpende oppdrag fra Nærings- og fiskeridepartementet. Vi er også utpekt som sektorens responsmiljø for digitale trusler.

Det sikkerhetspolitiske landskapet har blitt stadig mer komplekst. Hybride trusler, kritisk infrastruktur og behovet for bedre samarbeid mellom offentlige og private aktører står sentralt. For å møte disse utfordringene introduserer vi et nytt digitalt grensesnitt for sikringsrisikoanalyse.

Dette verktøyet, som lanseres gradvis fra vinteren 2025, vil gradvis revolusjonere måten havneanlegg vurderer og håndterer risiko på. Det er vanskelig å spå, særlig om fremtiden. Men, jeg er ganske sikker på at på samme måte som selvangivelsen

Årets hendelser har tydelig vist oss hvor sårbar maritim infrastruktur er for både fysiske og digitale trusler. Cyberangrep mot utenlandske havner og sabotasje mot undervannskabler bekrefter at scenarioer vi tidligere anså som usannsynlige, nå er høyst reelle.

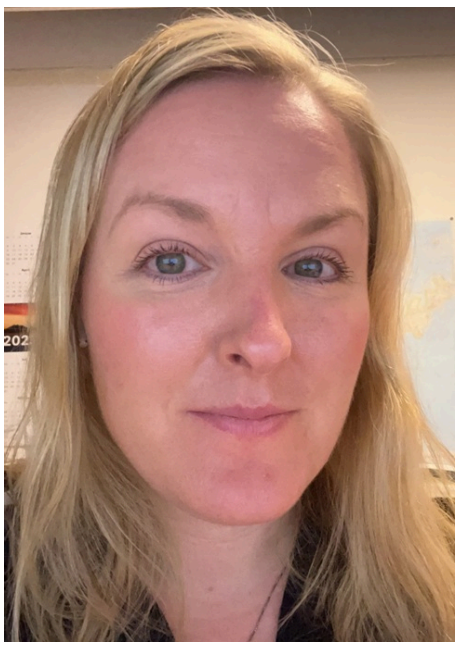
Likevel gir utviklingen av nye systemer og økt informasjonsdeling oss grunn til optimisme. Samarbeid, både nasjonalt og internasjonalt, er avgjørende, og jeg er stolt over den innsatsen som gjøres daglig av dere, våre godkjente sikringsorganisasjoner og avdelingen for maritim sikring for å styrke sikkerheten.

En spesiell takk rettes til sikringsledere og sikringsorganisasjonene i havneanleggene, som med sin innsats bidrar til økt samfunnssikkerhet og til å styrke totalforsvaret.

Vi ønsker dere alle en fredelig julefeiring og et godt nytt år!

Hilsen Richard Utne
Avdelingsleder maritim sikring

Vi har fått en ny kollega



I desember startet Astrid som seniorrådgiver i Arendal.

Hun har solid erfaring fra tilsyn innen i brannsikkerhet og har i tillegg en master med

Vi ønsker Astrid Lyngedal Rydholt velkommen til Kystverket og avdelingen for maritim sikring.

Bruk trafikklysprotokollen til å sikre informasjon i virksomheten

Trafikklysprotokollen (TLP) brukes for å legge til rette fordeling av potensielt sensitiv informasjon i, eller mellom virksomheter. TLP består av fire merker som brukes for å indikere delingsbegrensing som mottaker må forholde seg til. Trafikklysprotokollen kan være et nyttig verktøy for å ta stilling til informasjon i havneanlegget og hvordan denne kan deles.

De fire merkene defineres av sikkerhetsnettverket First og er som følger:

TLP:RED = Kun for individuelle, personlige mottakere. Ingen ytterligere formidling. Avsender kan bruke TLP:RED når informasjon ikke effektivt kan ageres på uten betydelig risiko for personvern, omdømme eller driften til de involverte organisasjonene. Mottakere kan derfor ikke dele TLP:RED-informasjon med noen andre. For eksempel i forbindelse med et møte er TLP:RED-informasjon begrenset til de som er til stede på møtet.

TLP:AMBER = Begrenset formidling. Mottakere kan bare dele dette videre ved tjenstlig behov i sin egen organisasjon og dens klienter. Merk at TLP:AMBER+STRICT begrenser deling til kun organisasjonen. Avsender kan bruke TLP:AMBER når informasjon krever støtte for å effektivt kunne ageres på, men fortsatt medfører risiko for personvern, omdømme eller drift dersom den deles utenfor de involverte organisasjonene. Mottakere kan dele TLP:AMBER-informasjon med medlemmer av sin egen organisasjon og dens klienter, men bare ved tjenstlig behov for å beskytte sin organisasjon og dens klienter og forhindre ytterligere skade. Merk: hvis avsender ønsker å begrense deling til kun organisasjonen, må de spesifisere TLP:AMBER+STRICT.

TLP:GREEN = Begrenset formidling. Mottakere kan spre dette innad i sitt miljø. Avsender kan bruke TLP:GREEN når informasjon er nyttig for å øke bevisstheten i deres bredere miljø. Mottakere kan dele TLP:GREEN-informasjon med kollegaer og organisasjoner i deres sektor eller miljø, men ikke via offentlig tilgjengelige kanaler. TLP:GREEN-informasjon kan ikke deles utenfor miljøet. Merk: når aktuelt miljø ikke er definert, antacybersikkerhets- eller cyberforsvarermiljøet.

eller ingen forutsigbar risiko for misbruk, i samsvar med gjeldende regler og prosedyrer for offentlig utgivelse. Med forbehold om opphavsregler kan TLP:CLEAR-informasjon deles uten begrensninger.

Kystverket anbefaler at havner og havneanlegg også tar i bruk trafikklysprotokollen.

Sikringsrisikoanalyser, sikringsplaner, tiltakskort, sjekklister og rapport etter sikringshendeleser er eksempler på dokumenter og informasjon man kan vurdere opp mot trafikklysprotokollen ved deling.

Bevissthet rundt informasjon og hvordan denne håndteres, vil bidra til å opprettholde et godt sikkerhetsnivå i havneanleggene. **Les mer om bruk av trafikklysprotokollen her.**

Trusselbildet for 2025

Europa går inn i 2025 med et stadig mer komplekst sikkerhetspolitisk landskap, preget av usikkerhet, rask teknologisk utvikling og økende press på kritisk infrastruktur. Her er de mest fremtredende trendene, og hva de betyr for maritim sikkerhet:

1. Hybride trusler og asymmetriske angrep
Statlige og ikke-statlige aktører intensiverer bruken av hybride trusler for å svekke europeiske land. Dette inkluderer cyberangrep, desinformasjon og sabotasje rettet mot kritisk infrastruktur som havner, undersjøiske kabler og skipsfart.

Hybride angrep, som kombinerer kinetiske- og ikke-kinetiske operasjoner, er utfordrende å oppdage og attribuere. Dette forsterker behovet for årvåkenhet, forebygging og tett samarbeid mellom private og offentlige aktører i den maritime sektoren.

2. Økende cyberrisiko
Cyberangrep mot maritim infrastruktur, maritime virksomheter og den maritime transportsektoren er økende. Både cyberkriminelle og statssponsede aktører har økt sitt søkelys på sektoren.

Phishing-angrep, ransomware og nettverksinfiltrasjoner kan lamme havners kritiske funksjoner og true både økonomisk stabilitet og nasjonal sikkerhet.

og økt digital årvåkenhet i hele den maritime næringen.

3. Geopolitisk ustabilitet
Økte spenninger mellom stormakter som USA, Kina og Russland påvirker Europas sikkerhet direkte. Kritisk maritim infrastruktur, som strategiske havneanlegg og sjøkabler, blir stadig mer utsatt for overvåkning, spionasje og påvirkningsforsøk. Dette krever løpende oppdatering av sikringsrisikoanalyser og sikringsplaner i både havner og havneanlegg. Vi understreker havneanleggs plikt til å varsle sikringshendelser (enhver mistenkelig hendelse) til Kystverket.

4. Sårbarhet i forsyningslinjene
Maritim trafikk, som håndterer en betydelig del av varetransporten, er avgjørende for både økonomisk stabilitet og samfunnets funksjonsevne. Sikkerhetstiltak må derfor være robuste på tvers av alle transportkategorier for å beskytte både fysiske og digitale transportknutepunkter.

Veien videre
Totalberedskapskommisjonen (2023) understreker viktigheten av investeringer i motstandsdyktighet, særlig i sektorer som transport, energi og kommunikasjon. For maritim sektor er dette en påminnelse om at sikkerhet ikke bare handler om å beskytte enkeltstående havneanlegg, men også om å sikre både Norge og Europas kollektive fremtid.

94 % av all norsk eksport går gjennom norske havneanlegg. Råvarer og halvfabrikata som tilsynelatende har lav verdi her hjemme, kan være av kritisk betydning når de når frem til forbrukerne som ferdige produkter; varme, lys, mat, biler, datamaskiner, telefoner - eller missiler.

Sikkerheten i norske havner er mer enn nasjonal – det er et fellesansvar som berører hele verden.

Tips til kvartalsvis drill

Jula er høysesong for cyberangrep, og hele tre av fire cyberangrep skjer utenfor normal arbeidstid. Det finnes flere former for cyberangrep, hvor phishing er blant de vanligste. Phishing er en form for nettsvindel der trusselaktører bruker ulike metoder som falske e-poster, tekstmeldinger eller falske nettsider for å lure folk til å gi fra seg sensitiv informasjon. Aktørene kan være på jakt etter brukernavn, passord eller

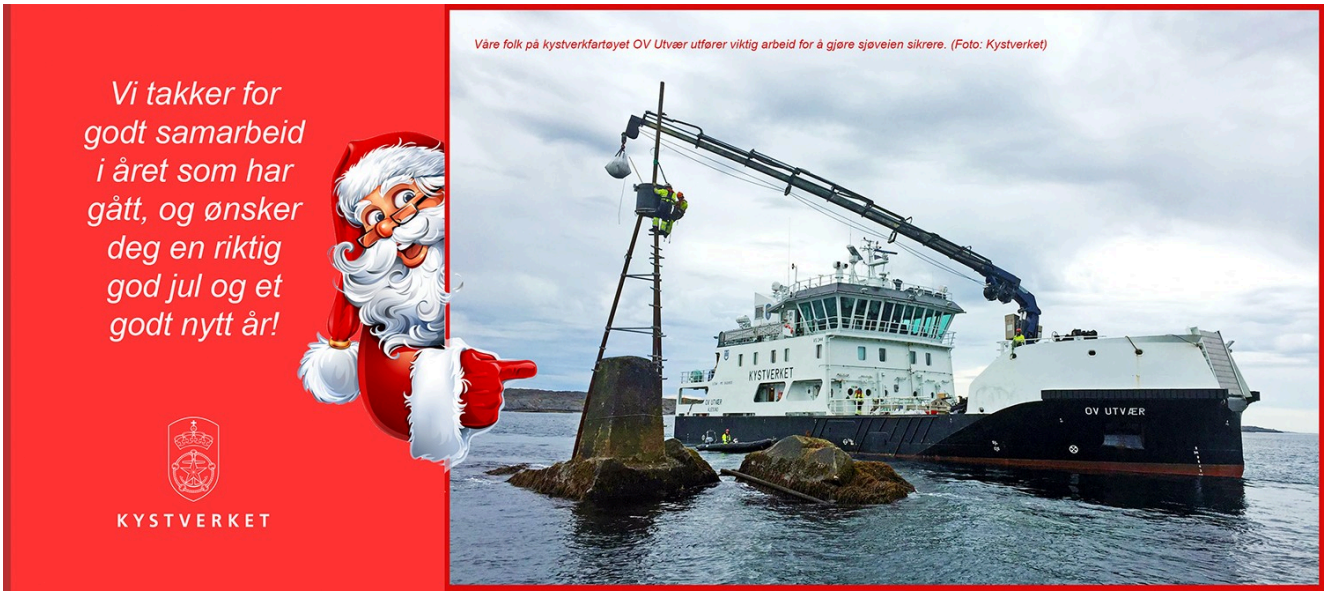
Målet er å lure mottakeren til å handle impulsivt uten å verifisere ektheten av meldingen ved å late som om det er en nødsituasjon eller en viktig melding. Phishing er en av de de mest effektive måtene å angripe virksomheter på, og kan ramme alle ansatte.

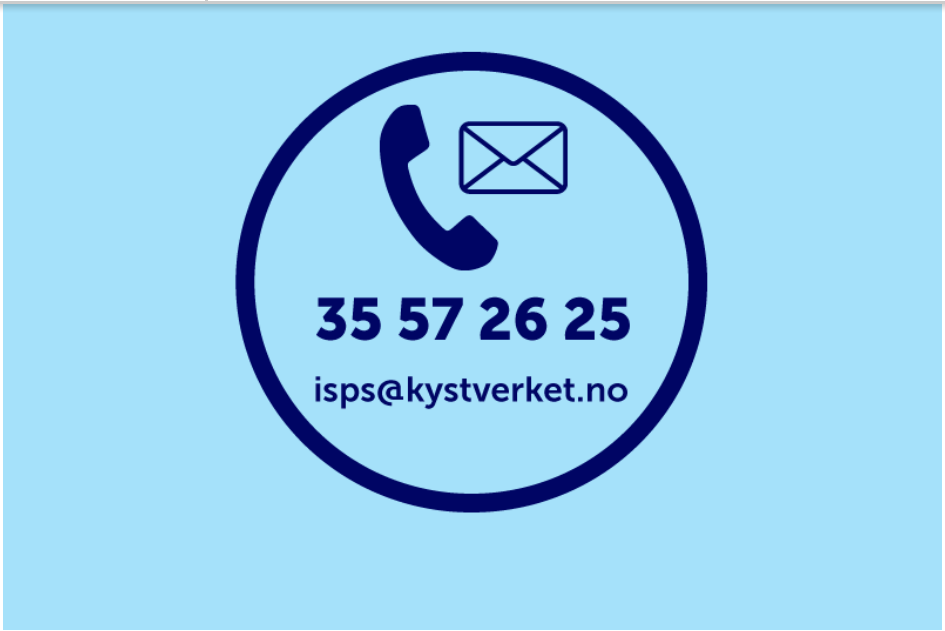
Diskuter med de ansatte; Har noen opplevd å motta en mistenkelig henvendelse i det siste? Hva var det som gjorde at du fattet mistanke? Ble hendelsen rapportert videre i virksomheten?

Hva kjennetegner en typisk phishing-melding og hva er virksomhetens retningslinjer angående slike angrep? Er alle ansatte i virksomheten kjent med disse?

Tips:
Datatilsynet har laget en veileder om hva phishing er, hvordan virksomheten best kan beskytte seg mot slike angrep og hva en bør gjøre dersom uhellet er ute og en ansatt har blitt «phishet».

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, og sende rapporter etter sikringshendelser.

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