Vis på internett

KYSTVERKET

ISPS-nytt

1. kvartal 22. mars 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.

Årets første ISPS-nytt

Velkommen til denne utgaven av vår kvartalsvise ISPS-nytt. Her vil vi omtale de nyeste funnene og analysene i de nasjonale trusselvurderingene fra Nasjonal sikkerhetsmyndighet (NSM), Politiets sikkerhetstjeneste (PST), og Etterretningstjenesten. Disse rapportene kaster lys over et stadig mer alvorlig og komplekst trusselbilde som havner og havneanlegg står overfor.

De årlige trusselvurderingene danner grunnlaget for vår forståelse av trusselbildet mot maritim sektor. Disse rapportene inneholder omfattende analyser av både innenlandske og internasjonale trusler, og gir verdifull innsikt i de mulige truslene og sårbarhetene som vi står overfor.

I tillegg har også politiet gitt ut to rapporter som er relevante. Politiets trusselvurdering og Politiets rapport om kriminelle nettverk peker spesifikt på økt risiko knyttet til havneanlegg og maritim infrastruktur, særlig knyttet til smugling av ulovlige varer og annen kriminalitet som utnytter sjøveien. Å forstå disse sårbarhetene er avgjørende for å utvikle effektive sikkerhetstiltak.

Vår nylige etablering av et maritimt sektorresponsmiljø, i samarbeid med Sjøfartsdirektoratet, representerer et betydelig skritt mot å styrke sikkerheten rundt våre havner og havneanlegg. Dette responsmiljøet vil være dedikert til å håndtere

Ved å kombinere innsikt fra nasjonale trusselvurderinger med konkrete tiltak, som etableringen av et sektorresponsmiljø, tar vi sikte på å styrke sikkerheten og robustheten til havner og havneanlegg. Dette nyhetsbrevet vil utforske disse temaene grundigere og gi våre lesere et dypere innblikk i de utfordringene og mulighetene som ligger foran oss i arbeidet med å opprettholde trygg og bærekraftig drift i vår maritime sektor.

Riktig god lesning!

Hilsen
Richard Utne
Avdelingsleder

Trusselvurderinger for 2024

12. februar la Etterretningstjenesten, Politiets sikkerhetstjeneste (PST) og Nasjonal sikkerhetsmyndighet (NSM) frem sine åpne trusselvurderinger for 2024. Vurderingene tar for seg den alvorlige sikkerhetspolitiske situasjonen, og gir et innblikk i hvordan Norge som småstat er utsatt. Norges posisjonering, innflytelse, konkurransedyktige industri og kompetanse er av interesse for andre land – der Kina og Russland blir trukket fram som hoved-interessenter.

Vurderingene gir et godt utgangspunkt for å analysere egen risiko og vurdere relevante forebyggende tiltak i havn og havneanlegg.

«NASJONAL TRUSSELVURDERING 2024»

sikkerhet. I deres vurdering, blir Kina og Russland trukket fram som hovedaktørene. Angrepskrigen i Ukraina, Norges NATO-medlemskap og felles grense med Russland fører til et større russisk behov for informasjon og etterretning i Norge. PST påpeker også at Kina vil kunne utgjøre en etterretningstrussel, på bakgrunn av deres ønske om økt kontroll over forsyningskjeder og posisjonering i Arktis.

PST vurderer også trusselen for terror utført av ekstreme islamister, inspirert av ideologien til IS og Al-Qaida. Trusselen vurderes som noe skjerpet sammenliknet med i fjor, grunnet det økte globale søkelyset på koranskjending og konflikten mellom Israel og Hamas.

«RISIKO 2024»

I Nasjonal sikkerhetsmyndighet sin vurdering «Risiko 2024» legges det vekt på samfunnets sårbarheter i et endret risikobilde. Her setter de søkelys på viktigheten av å kartlegge egen virksomhets verdier, avhengigheter og relevante trusler for å få en helhetlig forståelse for egen plass i verdisystemet og for samfunnet. Trusselaktører som Russland og Kina anvender ny teknologi, som i stor grad videreutvikles for å få innsikt i andre lands interesser, verdier og systemer. NSM påpeker i sine vurderinger at når truslene endrer seg må også virksomheters forståelse av sårbarheter og verdier endres i samsvar.

NSM advarer mot avhengighet av leverandørkjeder. Norge er blant mange land som er avhengig av kinesiske varekomponenter som brukes til helseteknologi, fornybar energi og forsvarsmateriell.

Trusselvurderingen advarer også mot utsatt kritisk infrastruktur, med fokus på oppkjøp og infiltrering hos underleverandører. Det påpekes at trusselaktører vil «hoppe over gjerdet der det er lavest», som betyr at underleverandører kan være inngangsporten til et større mål.

NSM tegner et komplekst bilde av hvordan trusselaktører bruker målrettede phishing-angrep for å innhente informasjon om norske virksomheter. Ondsinnede cyber-operasjoner kan gjennomføres fra hvor som helst i verden, og det er ingen fysiske begrensninger. Digitale trusselaktører vil derfor kunne ta utnyttelse av sårbarheter som svake passord, utdatert programvare og manglende to-trinns-autentisering for å få tilgang til virksomhetens IKT-systemer. Dette kan ha påvirkning på operasjoner, adgangskontroll og logistikk for å nevne noen, men også ha kaskadeeffekter ut mot forsyningskjeden.

«FOKUS 2024»

og etterretning i Norge. I sin rapport «FOKUS2024», kommer de med konkrete eksempler på hvordan disse aktørene bruker allment tilgengelig verktøy og digital infrastruktur for å kunne forstyrre forsyningskjeder, kartlegge sårbarhet og i ytterste konsekvens gjennomføre sabotasje.

E-tjenesten trekker fram at kinesiske selskaper har over lengere tid vist interesse for norske anbudsprosesser, deriblant investeringer i havner.

«FOKUS 2024» setter også søkelys på Russland sin aktivitet med kartlegging av norsk kritisk olje- og gassinfrastruktur. En slik kartlegging har foregått over lengere tid og E-tjenesten forutser at dette vil øke både i det fysiske og digitale domene. De viser til at Russland tidligere har viste vilje og evne til å ramme kritisk infrastruktur i en konfliktsituasjon.

Årets trusselvurderinger preges av et alvorlig sikkerhetsbilde med trusselaktører som er villige til å utnytte norske verdier, infrastruktur og interesser for å fremme egne mål. Felles for trusselvurderingene er allikevel at risikoen som beskrives kan reduseres. Det er derfor viktig at sikringsrisikoanalysen og sikringsplan blir oppdatert i takt med endringer i verdier, trusler og sårbarheter tilknyttet virksomheten og verdikjedene.

Styrker den digitale beredskapen

Kystverket har fått i oppdrag å etablere et «sektorresponsmiljø» (SRM) for cyber-sikkerhet i maritim sektor. Det innebærer at Kystverket, i samarbeid med Sjøfartsdirektoratet og andre relevante aktører, skal være sentral i håndteringen av alvorlige IKT-hendelser i maritim sektor.

initiativ fra Den Norske Krigsforsikring for Skib (DNK) og Norges Rederiforbund som leverer cybersikkerhetstjenester til norsk maritim næring.

Samarbeidet innebærer at NORMA Cyber vil støtte Kystverket og Sjøfartsdirektoratet i håndtering av digitale hendelser, sårbarheter og trusler innen det maritime domenet. Ansvaret for den daglige driften av maritim sektorresponsmiljøet ligger hos Kystverkets avdeling for maritim sikring.

Opprettelsen er et viktig skritt for å styrke cyber-sikkerheten i maritim sektor og sikre effektiv respons på IKT-hendelser.

Rapporterte sikringshendelser 2023

Vakt maritim sikring ble i fjor varslet om 67 sikringshendelser fra havner og havneanlegg. Vi vil i det følgende omtale hovedtrekkene blant de rapporterte hendelsene.

Nesten halvparten av rapporterte sikringshendelser er uautorisert adgang både fra landsiden og sjøsiden. Eksempel på denne typen hendelser er personer som på ulikt vis har kommet inn på adgangsbegrenset område. Intensjonen til den uvedkommende varierer fra forsøk på å komme seg om bord på fartøy til uaktsom adferd.

Mistenkelig adferd og observasjoner utgjør den andre hovedgruppen av sikringshendelser som meldes inn. Dette inkluderer droneobservasjoner og mistenkelig adferd som eksempelvis fotografering og annen mulig etterretning av havneanlegg.

Vi ser også en økning i innmeldte cyber-hendelser. Eksempler på slike hendelser er phishing-angrep og e-post-henvendelser som inneholder skadevare. Det er derfor god grunn til å beholde godt fokus på cyber-sikkerhet.

Funn fra tilsyn i 2023

Avdelingen for maritim sikring gjennomfører tilsyn ved havner og havneanlegg for å påse at regelverk og sikringsplan etterleves, og at sikringsrisikoanalysene fortsatt er relevante.

Det ble gjennomførte 6 tilsyn av havner og 89 tilsyn av havneanlegg i 2023. I havnene ble det avdekket totalt 6 avvik. Hovedsakelig ble avvik gitt på grunnlag av manglende

Ved havneanleggene ble det totalt avdekket 359 avvik, som i snitt tilsier 4 avvik per havneanlegg. Avvikene kategoriseres i alvorlighetsgrad, basert på konsekvens for havneanleggets sikring.

Svakheter i gjennomføring av øvelser og driller er noe viser at det ofte blir gitt avvik på. Det viser seg likevel at mange havneanleggene stadig blir bedre når det gjelder å sette av tid til øvelser og driller.

Mangelfull adgangskontroll og sikkerhetskontroll har en økende trend sammenlignet med tidligere år.

I tilsynsprogrammet for 2024 har vi lagt opp til en dobling av antall tilsyn som skal gjennomføres, og det vil i større grad involvere mindre havneanlegg. Det vil tas i bruk varierende tilsynsmetoder, med både stedlige tilsyn, digitale tilsyn og uvarslede tilsyn. Vi vil blant annet ha fokus på å etterse at sikringsrisikoanalyser og sikringsplaner er regelmessig gjennomgått og revidert, og at sikringsorganisasjonene er øvet og trent på relevante sikringshendelser.

Sårbarhetsvarsler formidlet av Kystverket

Kystverket samarbeider godt med andre myndigheter og organisasjoner som holder oss oppdatert om forhold som kan påvirke risikoen i den maritime sektoren. Dette kan være informasjon om kjente aktivistaksjoner eller sårbarheter i datasystem.

Vakt maritim sikring har i den siste tiden videreformidlet sårbarhetsvarsler utarbeidet av Nasjonalt cybersikkerhetssenter (NCSC). Dette er varsler om digitale sårbarheter, viktige oppdateringer eller cyber-hendelser, som er relevant for samfunnsviktige virksomheter eller funksjoner. Hver enkelt virksomhet må vurdere i hvilken grad egne systemer og verdier er relevant i forhold til varslene som formidles av Kystverket.

Dette bildet er skapt med kunstig intelligens (KI) av Kystverkets verktøy KystKI. Et årvåkent blikk er fortsatt nødvendig, slik at lastebiler ikke kjører på havet.

Tips til kvartalsvis drill

Kystverket, ved avdelingen for maritim sikring, sender fra tid til annen ut melding om digitale sårbarheter, oppfordring til økt årvåkenhet og andre hevendelser. Meldingene kan bidra til å styrke sikringen i virksomheten.

Ofte er det ikke nok at sikringsleder alene håndterer slike meldinger fra Kystverket. Eksempelvis ble det 14.03.2024 sendt ut en melding fra Kystverket om at Extinction Rebellion trolig ville gjennomføre demonstrasjoner ved industrivirksomheter med et større klimaavtrykk. Dette er relevant informasjon for personell med sikringsoppgaver.

Spørsmål som kan drøftes:
1: Har vi etablert en god praksis for å håndtere meldinger fra Kystverket eller andre relevante myndigheter?

2: Har havneanlegget rutiner for å varsle relevant personell ved utsending av melding fra Kystverket?
Dette kan være digitale sårbarheter eller oppfordring til økt årvåkenhet i forbindelse med aktivisme eller sabotasje.

forbedringspunkter.

God sikring – og god påske!

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