Cyberkriminalitet i skipsfarten – internasjonal erfaring

Av Jan Georg Christophersen

*Title in English: Cybercrime in Shipping – International Experience

Abstract

*The shipping industry, a cornerstone of global trade, faces significant challenges in cybersecurity due to its increasing reliance on digital technologies, interconnected systems, and automation. As the sector adopts advanced technologies like the Internet of Things (IoT), cloud computing, and autonomous vessels, it opens doors to a broader range of cyber threats, putting both operational efficiency and maritime safety at risk. The industry is facing a rising tide of cyberthreats that can disrupt operation, endanger safety, and cost millions. To mitigate these risks, the industry must focus on building a more resilient cybersecurity infrastructure, improving awareness, and complying with international cybersecurity standards. Robust defenses and proactive strategies are key to ensuring the safety, efficiency, and security of global maritime operations in the digital age. The shipping industry is increasingly becoming a target for cybercriminals due to its reliance on digital systems, automation, and interconnected technologies. Cybercrime in the shipping industry ranges from financial fraud and data theft to operational disruption, and its impact is felt across global trade and logistics. Cybercriminals continue to exploit vulnerabilities in the sector, targeting everything from operational systems and vessels control to sensitive data. To combat these threats, the industry must adopt comprehensive cybersecurity strategies, improve awareness and training, and comply with emerging regulatory frameworks. Enhanced collaboration across the global shipping community is one tool to build resilience and protect the critical infrastructure that supports world trade.****

Innhold:

1. Innledning

Den digitale omdanningen representerer en stor endring i de fleste industrier, og skipsfarten er intet unntak. Fra automatiserte navigasjonssystemer og elektroniske lastedokumenter til avanserte kommunikasjonsteknologier, har digitale verktøy effektivisert driften av skip, men denne økte digitaliseringen bringer også med seg betydelige utfordringer, spesielt når det gjelder «cybersikkerhet».

Begrepet cybersikkerhet er en utvidelse av fagområdet datasikkerhet, som også tar for seg informatikk og teknologi (IT)-baserte enheter og infrastruktur. Cybersikkerhet brukes her fordi det i det vesentlig anvendes om alt som har med internett, datasikkerhet og digitale nettverk å gjøre. Cyber har ikke en direkte norsk oversettelse, men brukes i sammenhenger som cybersikkerhet, cyberangrep, cyberkriminalitet og cyberforsavar. Selv om cyber har blitt adoptert direkte fra engelsk, er det nå et vanlig uttrykk på norsk, særlig innen teknologi, IT-sikkerhet og forsvar.

Med en stadig mer sammenkoblet global skipsfartsindustri, hvor fartøy, havner, og logistikkoperatører deler informasjon i sanntid, har cyberkriminalitet blitt en voksende trussel. Hackerangrep, datainnbrudd, løsepengevirus (ransomware) og andre former for cyberangrep har potensial til å lamme operasjoner, forårsake økonomiske tap, og til og med true den fysiske sikkerheten til fartøy, last, besetning og passasjerer. Løsepengevirus, utpressingsvare, utpressingsprogramvare eller gisselvare (ofte omtalt på norsk med uoversatt engelsk term ransomware) som krypterer deler av innholdet på en infisert datamaskin slik at det er utilgjengelig for eieren for så å utpresse løsepenger.

Denne artikkelen utforsker hvordan cybersikkerhet i skipsfarten har utviklet seg i takt med den teknologiske utviklingen, hvilke trusler bransjen står overfor, og hvordan selskaper innretter sin

cybersikkerhet og derved beskytte seg mot cyberkriminalitet i en tid hvor digitale angrep er blitt en av de største risikofaktorene for den globale sjøfartsindustrien.

Cybersikkerhet og cyberkriminalitet er nært beslektede områder, der cybersikkerhet handler om å beskytte informasjon, systemer og nettverk, mens cyberkriminalitet dreier seg om de ulovlige handlingene som truer disse områdene. Sammenfattet kan man si at cybersikkerhet er det nødvendige svaret på utfordringene som cyberkriminalitet skaper. Uten effektive cybersikkerhetstiltak vil trusselen fra cyberkriminalitet kunne skade både enkeltpersoner, organisasjoner og samfunnet i stor skala. Et sentralt spørsmål blir derfor hvordan skade kan repareres.

Skipsfart, som mange andre bransjer, står overfor økende trusler fra cyberangrep. For å beskytte seg mot disse truslene iverksetter rederier og skipsoperatører en rekke tiltak som omfatter teknologiske løsninger og organisatoriske retningslinjer. Noen av de viktigste tiltakene behandles her og inkluderer brannmurer og antivirusløsninger som grunnleggende sikkerhetstiltak som beskytter skipssystemer mot kjente trusler og skadelig programvare. Dette fungerer som første forsvarslinje ved å forhindre uautorisert tilgang til skipets nettverk.

I næringen er det viktig å segmentere eller isolere ulike nettverk. Dette betyr at systemer som er kritiske for driften, som navigasjonssystemer, ikke er koblet til det samme nettverket som personlige enheter eller underholdningssystemer. Dette reduserer risikoen for at cyberangrep sprer seg mellom systemer om det skulle inntreffe.

Det er viktig å holde all programvare oppgradert med de siste sikkerhetsoppdateringer. Cyberkriminelle utnytter ofte kjente sårbarheter i utdatert programvare, og menneskelige feil er en av de viktigste årsakene til cyberangrep. Rederier bør derfor sørger for at mannskapet er trent i cybersikkerhet, inkludert gjenkjenning av nettfiske-angrep (phishing). Nettfiske er svindelangrep hvor bakmenn forsøker å lure brukeren til selv å oppgi sensitive opplysninger slik som passord, PIN-kode eller betalingskortinformasjon. Opplæring bidrar til å øke bevisstheten om gode sikkerhetsrutiner. Nettefiske baserer seg i stor grad på sosial manipulasjon.

International Maritime Organization (IMO) har innført retningslinjer for cybersikkerhet som medlemsstatene har iverksatt i nasjonal lovgivning, som skipseierselskaper derfor har plikt til å følge. Disse retningslinjene dekker alt fra risikovurderinger til innføring av tekniske tiltak for å sikre fartøy mot cybertrusler. Rederier bør gjennomfører regelmessige risikoanalyser for å identifisere sårbarheter i skipssystemer. Dette hjelper dem med å sette inn tiltak for å minimere risikoen for cyberangrep.

Skip bruker krypteringsteknologier for å sikre at kommunikasjonen mellom skip og landbaserte enheter ikke kan avlyttes eller manipuleres. Dette gjelder spesielt for viktig informasjon som rutes gjennom satellittkommunikasjon. Regelmessig sikkerhetskopiering sørger for at viktige data kan gjenopprettes i tilfelle et angrep, som løsepengevirus, der filer kan bli kryptert eller låst. Dette bidrar til å redusere skadene etter et potensielt angrep.

Mange skip har kontinuerlig overvåking av sin informasjonsteknologi (IT-systemer) for å kunne oppdage mistenkelig aktivitet i sanntid. Dette gir mulighet for rask respons på potensielle cybertrusler. Skipsfartsnæringen har utarbeidet beredskapsplaner for hva som skal gjøres dersom et cyberangrep skulle inntreffe. Dette inkluderer nødprosedyrer og samarbeid med eksterne

cybersikkehetselskaper. Disse tiltakene hjelper skipsfartsnæringen med å beskytte sine systemer og operasjoner mot det økende antallet cybertrusler som truer moderne maritim drift.

Cyberkriminalitet kan betraktes som økonomisk kriminalitet, avhenger av handlingens natur og konsekvensene den medfører. Mange cyberkriminelle handlinger har et økonomisk motiv, og målet er ofte å stjele penger, verdifull informasjon, eller å svindle individer eller organisasjoner for økonomisk gevinst. Eksempler på cyberkriminalitet som kan betraktes som økonomisk kriminalitet inkluderer: Phishing (nettfiske) for å stjele bankinformasjon eller kortopplysninger. Ransomware eller på norsk (løsepenge)-angrep, hvor kriminelle krever løsepenger for å gjenopprette tilgang til krypterte data. Identitetstyveri for å svindle til seg penger ved bruk av stjålet identiteter. Dataangrep (hacking) er uautorisert eller ulovlig tilgang til datasystemer, nettverk, eller digital informasjon. Det innebærer å manipulere, endre eller få kontroll over datasystemer uten tillatelse. Disse handlingen påvirker ofte både enkeltpersoner og selskaper økonomisk, og det kan derfor falle inn under kategorien økonomisk kriminalitet. Samtidig kan visse typer cyberkriminalitet også ha andre mål, som sabotasje eller politiske mål, og da vil det i mindre grad klassifiseres som økonomisk kriminalitet. Begrepet kan også ha en mer nøytral eller positiv betydning, særlig innen teknologi og programmering. I den positive sammenhengen snakker man gjerne om å «hacke» som en måte å finne smarte løsninger eller optimalisere teknologien på.

I lovmessige sammenhenger vil cyberkriminalitet som har økonomiske konsekvenser ofte bli behandlet under privatretten, men cyberkriminalitet kan reguleres av både strafferettslige og sivilrettslige regler, avhengig av type handling, skadeomfang og hvordan det påvirker ofrene. Den stadige økningen av cyberangrep mot skipsfarten har vært meget omfattende, det israelske cybersikkerhetsselskapet Naval Dome fant en stigning på 400 prosent det første året av pandemien 2020 – 2021 (Meland mfl., 2021).

Maritim næring består av skipseiere, leverandører av utstyr og tjenester og verft. Flere ulike tilstander som var ekstraordinær under pandemien kan være årsaken til den store stigningen. Eksemplene på utøverne av disse lovbruddene kan være hackere uten annen jobb, færre til å passe på, innskrenket reisevirksomhet for inspektører osv. Det som imidlertid er vesentlig, er at motivene er økonomiske. Krav om løsepenger er den mest alminnelig formen for krav fra hackerne, sannsynligvis på grunn av gevinsten kan innkasseres raskt. En annen begrunnelse for angrepene kan være at verdier som settes i spill i skipsfarten er store, skip og last har stor verdi. En tredje faktor er at skipsfatet ikke er den første i rekken som fornyer og sikre seg mot cyberangrep. Havner benytter for det meste standardiserte gamle teknologiske løsninger som gjør det enkelt for hackere å angripe. Skipseiere og havner må selv sikre verdier, betale for oppgraderinger av teknologien og på den måten sikre seg mot cyberangrep, fordi skipseier og havneeiere ikke er de som lider de største tapene, er de senene med å beskyttes seg. Her må lasteier som overlater sine verdier til transportøren, skipseier og havner, tas i betraktningen fordi de eier lasten. Den virkelig store risiko som kan oppstå er det lasteeierne som har, derfor er det lasteier som også er mest opptatt av oppgradert teknologi i rederier og i havner for å beskyttes seg mot cyberangrep.

De fleste av oss er vanligvis lovlydige borgere – det meste av tiden. Men vi har med stor sannsynlighet begått mindre «lovbrudd», eller brutt lover fra tid til annen, men kanskje også passivt observert at lover blir brutt. Men vi kan ikke ha unngått å observere at mer alvorlig kriminalitet

skjer i økende grad. Denne forstyrrende realitet vil det bli sett nærmer på i det følgende. Kriminaliteten øker i både industrialiserte stater og utviklingsland. Datagrunnlaget for denne artikkel bygger på alvorlig økonomisk- og organiserte internasjonale lovbrudd som relateres til cybersikkerhet, det verktøy internasjonale lovbrytere i stadig større grad søker å omgå.

Artikkelen er et forsøk på å belyse noen sider av lovbruddene, forebyggingen og håndhevingen fra et internasjonalt perspektiv. Hvilke mottiltak er iverksatt, hvem er effektive og hvem er lovende. For noen kan dette være deprimerende lesning; fordi problemet med såkalt «moderne» kriminalitet vil i mange tilfeller være utenfor området for nasjonale strafferettssystem hvor som helst i verden. Hva kan og bør gjøres for å hindre utbredelsen av cyberkriminalitet? Det vi bør innse, er at cybersikkerhet og cyberkriminalitet er fast sammenknyttet og derfor bør behandles samlet.

2. Bakgrunn

Cybersikkerhet og cyberkriminalitet har fått økt oppmerksomhet i forskningen delvis på grunn av den raske digitaliseringen av samfunnet og de potensielle trusler som følger med. Cybersikkerhet omfatter beskyttelsen av datasystemer mot uautorisert tilgang, angrep eller skade, mens cyberkriminalitet referer til kriminell aktivitet som utnytter teknologi, særlig internett, for å begå lovbrudd. Dette feltet omfatter alt av innbrudd i datasystem og identitetstyveri til mer sofistikerte angrep som løsepengevirus og digitale terrorhandlinger. En presisering av de to begrepene kan være hensiktsmessig.

Cybersikkerhet refererer til beskyttelse av systemer, nettverk og data fra digitale trusler som kan forårsake skade eller uautorisert tilgang. Forskingslitteraturen har utviklet flere definisjoner og rammeverk for cybersikkerhet, der man ofte skiller mellom tekniske, organisatoriske og lovgivende tiltak (National Institute of Standards and Technology (NIST), 2020)).

Innenfor cybersikkerhet er NIST kjent for sitt NIST Cybersecurity Framework, som er en veiledning for hvordan organisasjoner kan beskytte seg mot cybertrusler.

Cyberkriminalitet er kriminelle handlinger som involverer datamaskiner og nettverk. Dette kan inkludere innbrudd i datasystemer, nettfiske, identitetstyveri, løsepengevirus, og digitale angrep mot nasjonal infrastruktur (Brenner, 2013). I litteraturen skiller man mellom ulike former for cyberkriminalitet, som kan variere fra individualiserte lovbrudd til organiserte og stadig større angrep (Anderson & Moore, 2006).

Juridisk- og samfunnsvitenskapelig forskning på cyberkriminalitet har utviklet seg i takt med den teknologiske utviklingen. I de tidlige stadiene (1990-tallet) var cyberkriminalitet hovedsakelig knytte til hvordan virus og data angrep fungerte. Etter hvert som internett og digitale plattformer har utviklet seg, har også angrepene blitt mer sofistikerte. Dessuten har rettsutviklingen gått sin gang, lovgivningen er blitt mer direkte relevant. Samfunnsvitenskapelig forskning har fulgt opp med arbeider som viser hvordan reguleringer virker.

I henhold til norsk lov er det ulovlig å true med cyberangrep. Slike trusler kan falle inn under straffelovens bestemmelser om trusler og datakriminalitet. I Norge kan det å framsette trusler om å utføre et cyberangrep bli ansett som en straffbar handling. Spesielt hvis truslene skaper frykt

eller uro hos mottakeren. Dette kan også omfatte forsøk på utpressing eller andre former for trusler som involverer digitale systemer eller data. Strafferammene for slike handlinger kan variere avhengig av alvorlighetsgraden og omstendighetene rundet trusselen.

En gjennomgang av nyere litteratur identifiserer flere tendenser. Løsepengevirus har blitt en dominerende trussel, der angripere krypterer offerets data og krever løsepenger for å gjenopprette tilgang (Goodman, 2021).

Internet of Things (IoT) «tingenes internett», på norsk referer det til nettverket av fysiske enheter som er tilkoblet internett og kan samle inn, dele og motta data. Dette har skapt nye angrepsflater, ettersom flere enheter er koblet til internett og dermed er potensielt sårbare (Zhou mfl., 2018).

Sosial manipulering, nettfiske har økt, spesielt målrettet mot ansatte i organisasjoner, og benytter psykologiske teknikker for å få tilgang til sensitive data (Krombholz et al., 2015).

Når det kommer til økonomiske og sosiale konsekvenser har studier vist at cyberkriminalitet medfører store økonomiske tap. En global studie anslår at cyberkriminalitet vil koste verdensøkonomien over 10 billioner USD årlig inne 2025 (Morgan, 2020).

Dette inkluderer både direkte tap, som tyveri av penger eller data, og indirekte kostnader som over tid medfører, omdømmeskader og reparasjonskostnader.

Cyberkriminalitet påvirker også sosialt, ettersom den kan føre til tap av privatliv, identitet og tillit. Når informasjon blir stjålet eller lekket, kan det få alvorlige konsekvenser for individers og organisasjoners sikkerhet (Böhme, 2013).

Næringslivet, organisasjoner og myndigheter står overfor store utfordringer i å beskytte sine systemer og data. I tråd med veksten i cyberkriminalitet, har flere land iverksatt lover bygget på internasjonale konvensjoner for å bekjempe digitale trusler. Et viktig utviklingstrekk har vært etableringene av internasjonale samarbeidsfora og et rettslig rammeverk som for eksempel (Budapest Convention on Cybercrime (Budapest Convention, ETS No. 185) ant its Protocols (2001)). Budapestkonvensjonen er den første internasjonale traktaten som tar for seg cyberkriminalitet og har som mål å styrke det internasjonale samarbeidet i kampen mot cyberkriminalitet. Konvensjonen er fortsatt et sentralt verktøy for internasjonal innsats mot cyberkriminalitet og setter en juridisk og praktisk standard for samarbeid mellom stater.

Når dette er nevnt er det av betydning å vise til at EU har flere initiativer og konvensjoner som tar sikte på å forhindre cyberangrep rette mot skipsfarten. Her kan nevenes EU Cybersecurity Act. Denne lovgivningen styrker mandatet til EU Agence for Cybersecurity (ENISA) og etablerer et EU-omfattende rammeverk for cybersikkerhetssertifisering av produkter, prosesser og tjenester. Network and Information Security Directive, NIS-direktivet, er et direktivet som pålegger medlemslandene å sikre at operatører av essensielle tjenester, inkludert maritim sektor, iverksetter passende sikkerhetstiltak og rapporterer cyberhendelser. EU Maritime Security Strategy er en strategi som inkluderer tiltak for å forberede cybersikkerheten i maritim sektor, blant annet ved å fremme samarbeid mellom medlemslandene og med private aktører. I tillegg til dette har også EU etablert seg med Cybersecurity Guidelines for ships. Selv om disse ikke er en del av EU-lovgivningen, har IMO gitt ut retningslinjer for å hjelpe skipsfarten med å beskytte seg mot cybertrusler, og EU

oppfordrer til gjennomføring av disse. Tiltakene er ment som en del av EUs bredere innsats for å beskytte kritisk infrastruktur mot cybertrusler, inkludert skipsfarten.

Imidlertid er det fortsatt store utfordringer knyttet til globalt samarbeid, spesielt når det gjelder jurisdiksjons spørsmål og straffeforfølgelse. Mange cyberkriminelle opererer på tvers av landegrenser, noe som gjør det vanskelig å føre rettssaker og håndheve lovene (Deibert et al., 2019).

Cybersikkerhetsforskning har vist flere verktøy og tilnærminger for å motvirke cyberkriminalitet. Blant de mest framtredende er Kryptografi, som beskytter data ved å gjøre dem uleselig uten riktig nøkkel. Maskinlære og kunstig intelligens (KI) eller som det internasjonalt blir kalt Artificial Inteligence (AI) for å oppdage uvanlig aktivitet og forhindre cyberangrep (Chio & Freeman, 2018).

Samt sikkerhetsprotokoller for IoT, som konsentrer oppmerksomheten om å beskytte enheter i tingenes internett mot angrep (He, Chan, and Li, 2021).

I tillegg blir det lagt stadig større vekt på sikkerhet som kultur i organisasjoner. Det innebærer opplæring av ansatte for å gjenkjenne trusler som nettfiske, innføring av strenge tilgangskontroller og utvikling av robuste retningslinjer for cybersikkerhet.

Selv om det er gjort betydelig framgang på flere områder inne cybersikkerhet og bekjempelse av cyberkriminalitet er det fortsatt flere utfordringer. Etter hvert som digitale systemer blir mer komplekse, blir det vanskeligere å opprettholde sikkerheten på tvers av forskjellige plattformer og enheter. KI og automatiserte angrep gir cyberkriminelle muligheten til å gjennomføre angrep mer effektivt og i større skala (Goodman, 2021).

Økt oppmerksomhet på etikk, spesielt når det gjelder overvåkning og datahåndtering, skaper et behov for grundigere diskusjon og reguleringer rundt personvern og sikkerhet (Stahl mfl., 2020).

Forskning på cybersikkerhet og cyberkriminalitet har utviklet seg betydelig de siste årene, og vi ser en stadig økende kompleksitet både i trusler og i løsninger. Selv om det er framskritt i utviklingen av teknologiske og rettslige rammeverk for å bekjempe cyberkriminalitet, vil den framtidige forskningen måtet ta høyde for den raske teknologiske utviklingen og de stadig mer sofistikerte angrepene. Cybersikkerhet er ikke lenger kun et teknologisk spørsmål, men en samfunnsmessig utfordring som krever tverrfaglig samarbeid. Denne artikkelen søker å gi et innblikk i det omfattende og dynamiske feltet av cybersikkerhet og cyberkriminalitet som berører en del av næringslivet. Som det vil framgå, er feltet i hastig og kontinuerlig utvikling, og det krever både teknologisk innovasjon og tverrfaglig samarbeid for å møte utfordringene.

3. Økning av cyberangrep og cyberkriminalitet

Mens alle cyberangrep kan betraktes som cyberkriminalitet, er ikke alle former for cyberkriminalitet nødvendigvis cyberangrep. Cyberkriminalitet omfatter et bredere spekter av ulovlige aktiviteter som kan innebære bruk av teknologi. Forskjellen mellom cyberangrep og cyberkriminalitet ligger hovedsakelig i intensjonen og omfanget av handlingen.

Den internasjonale økningen i cyberkriminalitet har vært betydelig de siste årene. Flere faktorer bidrar til denne utviklingen, inkludert økt digitalisering, flere nettverksangrep og mer avanserte angrepsmetoder.

Ifølge rapporter fra cybersikkerhetsfirmaer og internasjonale organisasjoner har cyberkriminalitet som løsepengevirus, datainnbrudd og nettfiske-angrep økt drastisk, spesielt under pandemien COVID-19 som det er vanligst å referer til hvor den mest intense perioden var årene 2020 og 2021. I denne perioden opplevde mange stater en eksplosiv vekst i cyberangrep, da flere mennesker jobbet hjemmefra og brukte usikre nettverk.

I tillegg er det blitt mer lukrativt for kriminelle grupper å utføre angrep, noe som har ført til en profesjonalisering av cyberkriminalitet. Myndigheter, organisasjoner i næringslivet og private selskaper jobber aktivt med å forbedre sikkerhetstiltak, men utfordringen er fortsatt stor.

3.1 Det nye nivået for cyberkriminalitet

Tall som bekrefter at situasjonen er alvorlig finner vi i aktuelle rapporter om utviklingen fra organisasjoner som Europol, FBI og cybersikkerhetsfirma som Symantec og McAfee som viser endringer. Aktuelle kilder for skipsfarten er rapporteringer fra IMO og Baltic and International Maritime Council (BIMCO). Sistnevnte er verdens største medlemsorganisasjon for skipseiere, befraktere, skipsmeklere og agenter. BIMCO medlemmer dekker 62 prosent av den global handleflåten tonnasjemessig og gir derfor betydelig bredde i sine funn.

IMO har gjennomført flere tiltak for å hindre cyberkriminalitet og styrke sikkerheten i den maritime sektoren. For eksempel har IMO utviklet retningslinjer for cyberkriminalitet som anbefaler at skip og maritime organisasjoner vurderer cybertrusler som en del av deres risikoanalyser. Dette inkluderer å iverksette tiltak for å beskytte informasjonssystemer. IMO oppfordrer til at maritime aktører utvikler beredskapsplaner som inkluderer cyberkriminalitet. Dette betyr å ha prosedyrer for å håndtere cyberangrep, inkludert hvordan man kan gjenopprette systemer og data etter et angrep. For å styrke beredskapen mot cybertrusler, anbefaler IMO at ansatte får opplæring i cybersikkerhet og bevissthet om potensielle trusler. Dette inkluderer å forstå hvordan man identifiserer nettfiske-forsøk og andre angrepsmetoder.

Det er viktig å være oppmerksom på at IMO er en av FNs særorganisasjoner og således et rådgivende organ. Medlemsstatene må på grunnlag av IMOs oppfordringer iverksette oppfordringene i nasjonal lovgivning som dekker feltet. I 2021 ble det innført krav om at rederier må vurdere cyberkriminalitet i sine sikkerhetsstyringssystemer, i samsvar med The International Management Code for the Safe Operation of Ships and for Pollution Prevention (ISM-code). Dette innebærer at cybersikkerhet må være en del av den generelle risikovurderingen.

IMO arbeider med medlemsland og maritime aktører for å fremme samarbeid og deling av informasjon om cybersikkerhet og gode rutiner. Dette inkluderer partnerskap med organisasjoner som BIMCO og andre relevante aktører. IMO oppfordrer til regelmessige evalueringer av sikkerhetstiltak for å sikre at de er effektive og tilpasset utviklingen i cybertrusler. IMO tar cybersikkerhet på alvor og jobber kontinuerlig for å styrke sikkerheten i den maritime sektorene.

BIMCO har utviklet retningslinjer for cybersikkerhet som gir skipseiere og operatører verktøy for å håndtere og redusere risikoen for cyberangrep. I det vesentlige er tiltakene som organisasjonen operer med de de samme sikkerhetsregler som andre næringslivsorganisasjoner. De tilbyr kurs og seminarer om cybersikkerhet for medlemmer. Gir tilgang til verktøy og informasjon

for å hjelpe medlemmer med å sikre sine systemer. I tillegg arbeider de sammen med andre organisasjoner og myndigheter for å dele informasjon om trusler og anbefalt framgangsmåte. Og de oppfordrer til utvikling av beredskapsplaner som inkluderer cybersikkerhet for å forberede seg på mulige angrep og minske skade. Hvis nedlemmer blir utsatt for eller oppdager mistenkelig aktivitet, rapporteres dette til BIMCO og relevante myndigheter. Tidlig varsling kan hjelpe med å forhindre videre angrep. BIMCOs innsats for å bekjempe cyberkriminalitet er avgjørende for å beskytte maritime operasjoner og sikre en tryggere maritim industri

BIMCO har utgitt flere dokumenter og rapporter som omhandler cybersikkerhet og cyberangrep i skipsfartsnæringen. Cybertrusler og cyberkriminalitet har blitt stadig mer relevant i maritim industri, spesielt med økning i digitalisering og automatisering av skipsfartens operasjoner. Tiltakene er i det vesentlige de samme som beskrives i denne artikkelen og strekker seg fra å identifisere trusler til tiltak og retningslinjer via regulatoriske krav, cyberforsikring til samordning og samarbeid til hendelseshåndtering.

Eksemplet på cyberangrep i skipsfartsnæringer som det ofte vises til er Mærsk (2017), en av de mest kjente cyberhendelsene i skipsfartsnæringen. Selskapet ble rammet av NotPetya-skadelig programvare. Angrepet ført til store driftsforstyrrelser, og Mærsk estimerte at de økonomiske tapene fra angrepet var rundt 300 millioner USD.

Et annet kjent angrep var Casco (2018), som rammet det kinesiske rederiet Casco, selskapet fikk sine datasystemer ute av drift i flere dager.

Etter hvert som teknologiene om bord på skipene blir mer avansert (f.eks. autonome skip og IK-dreven systemer), vil nye cybersikkerhetsutfordringer oppstå. Her er det at internasjonalt samarbeid er viktig for å ordne opp i cybertrusler som kan ha global rekkevidde, og BILCO arbeider sammen med flere internasjonale organisasjoner for å styrke cybersikkerheten på tvers av landegrensene. Samlet sett anerkjenner BILCO cybersikkerhet som en kritisk utfordring for skipsfartsnæringen, og legger stor vekt på forebygging, beredskap og samarbeid på tvers av sektorer for å møte disse truslene.

Kunstig intelligens endret alt i 2023, og i 2024, og begynner den virkelige kampen: Hvem vil benytte kraften som befinner seg i den nye teknologien og psykologien til menneskelig atferd mer effektivt – de som bekjemper ulovligheter eller nettkriminelle.

Profesjonaliseringen av cyberkriminalitet fortsetter og gjør jevn framgang og når nye høyder i 2024, takket være oppkomsten av ny KI og nye kraftige teknologier. Av den grunn er tiden inne for organisasjoner til å investere i sikkerhet, grunnen er at det kun er begynnelsen vi har sett. Cyberkriminelle vil fortsette å utvikle mer sofistikerte metoder for å oppnå sin mål som er en enda mer profesjonell og lønnsom virksomhet (Sosafe, 2024)

Cyberkriminelle vet å utnytte de turbulente tider vi globalt lever i gjennom å bruke falske trusler for å oppnå sine målsettinger. Vi kan se det ved å betrakte en signifikant økning i antall tilfeller av desinformasjon som en form for Desktop as a Service (DaaS), det digitale landskapet er blitt en komplisert kamparena. Veksten i antall cybertrusler sparer ingen sektorer, det kan være det offentlig rom så vel som kritisk infrastruktur i konkrete utsatte posisjoner.

Cyberkriminelle vet at den største muligheten for suksess ligger i å spille på menneskelige følelser, og at sosial tilnærming er det viktigste i deres praksis. Ved å profesjonalisere

cyberkriminalitet og benytte KI, kan de skape en troverdig og komplisert sosial situasjon som gjør angrepet enklere. Dette gjør det vanskelig å skille de sanne fra de uriktige meldingene, truslene spres raskere enn noen gang. Dette skapere større utfordringer for arbeidet med cybersikkerhet en noen gang tidligere.

Lovbrytere behøver stadig færre kunnskaper og organisasjonsmessig kraft for å utvikle et høyst effektivt angrep, og det kommer til å bli et stort problem for oss alle i tiden som kommer. Når vi analyserer trusler, trenger vi å se på to forbindelse: intensjoner til den som handler og vedkommendes kapasitet. For selskaper som blir angrepet kan det oppstå en situasjon hvor motangrep kan brukes for å forsvare seg. Det kan tenkes at organisasjoner som driver former for virksomhet bygger opp kapasitet som skal være et forsvar mot konkurrenter, men ender opp med å bli brukt som våpen mot andre i næringslivet eller mot andre stater. Et eksempel kan være karteller og deres virksomhet over landegrenser. Karteller i skipsfartsnæringen refererer til samarbeid mellom rederier eller skipsfartsselskaper for å kontrollere priser, begrense konkurranse, eller markeder mellom seg. Dette er en form for prissamarbeid som kan være ulovlig i mange jurisdiksjoner, da det kan føre til høyere priser for forbrukere og begrense konkurransen i markedet. Historisk sett har skipsfartsnæringen hatt kartell-lignende struktur, spesielt gjennom såkalte «conference systems», hvor rederier samarbeider om frakter og ruteplanlegging. Dette systemet var lovlige i mange land, men har blitt gradvis avviklet eller regulert strenget for å fremme fri konkurranse.

3.2 Den overhengende trusselen og det økte presset

Den overhengende trusselen om cyberangrep er et problem som påvirker både enkeltpersoner, bedrifter og stater. Med den økende avhengigheten av teknologi og internett, har angrep blitt mer sofistikerte og vanlige.

Cyberkriminalitet som er mest vanlig er nettfiske, løsepengevirus, Distributed Denial of Service (DDoS)-angrep, og datalekkasje. Hver type har forskjellig mål og metode. Målgruppen kan være er både små og store virksomheter, offentlig sektor og privatpersoner. Konsekvensene av angrep kan føre til tap av sensitive data, økonomiske tap, omdømmetap, og i verste fall skade på fysiske systemer. For å oppnå forebyggende effekt er det viktig å iverksette steke sikkerhetstiltak, inkludert brannmurer, antivirusprogramvare, opplæring av ansatte, og regelmessige sikkerhetsvurderinger. Internasjonal samarbeid er andre tiltak som bør settes i verk når cybertrusler krysser grenser, og derfor avgjørende for å bekjempe dem effektivt. Å være proaktiv i cybersikkerhet er essensielt for å minimere risikoen og beskytte mot framtidige angrep.

Det økende cyberpresset på næringslivet er en betydelig utfordring som krever økt oppmerksomhet og handling. Antallet cyberangrep mot virksomheter har økt drastisk. Hackere benytter seg av mer sofistikerte metoder og utnytter sårbarheter i systemene. Mange angrep er målrettet mot spesifikke bransjer eller selskaper, særlig innen finans, helse, og kritisk infrastruktur. Dette gjør at konsekvensene kan være svært alvorlige. Cyberkriminalitet kan medføre betydelige økonomiske tap, både direkte (datatap, krav om løsepenger) og indirekte (tap av omdømme, kunder og muligheter). Regulatoriske krav hvor myndigheter stadig innfører strengere regler og forskrifter

for cybersikkerhet, noe som krever at virksomheter investerer i sikkerhetstiltak og oppfyller kravene. Det er nødvendig å bygge en kultur for cybersikkerhet internt i organisasjonen.

Ansatte må være opplært i å gjenkjenne trusler og håndtere dem på riktig måte. Med digitaliseringen av næringslivet kommer også nye muligheter og utfordringer. Bedriften må være i forkant med teknologi og sikkerhetsløsninger for å beskytte seg. Næringslivet bør samarbeide om informasjon om trusler og anbefalinger for sikkerhet. Samarbeid med myndigheter og bransjeorganisasjoner vil være avgjørende. Å håndtere det økende cyberpresset krever en helhetlig tilnærming der teknologiske, organisatoriske og menneskelige faktorer tas i betraktning.

3.3 Utvidelsen av mørketall

Utvidelsen av mørketallene for cyberkriminalitet referer til det økte antallet uregistrerte eller usette cyberangrep som ikke rapporteres eller dokumenteres. Mange virksomheter og enkeltpersoner velger å ikke rapportere cyberangrep av frykt for omdømmetap, juridiske konsekvenser eller kostnader knytte til krisen. Dette fører til at den faktiske forekomsten av cyberkriminalitet mest sannsynlig er vesentlig høyere enn det som er synlig i statistikkene. Manglende bevissthet kan skyldes at mange kan være uvitende om at de har blitt utsatt for cyberangrep, særlig i tilfeller av subtile angrep som data- og identitetstyveri. Dette kan bidra til en underrapportering av hendelser. Angrepene kan være vanskelig å oppdage, spesielt når de involverer avanserte teknikker som nettfiske, skadelig programvare eller løsepengevirus. Uten spesialisert verktøy og ekspertise kan det være utfordrende å identifisere angrepene. Små og mellomstore bedrifter har ofte begrensede ressurser til å håndtere cybersikkerhet, noe som kan føre til at de ikke oppdager eller rapporterer angrep. Cyberkriminelle drives av en rekke aktører, fra enkeltpersoner til organiserte kriminelle grupper. Disse aktørene blir stadig mer kreative og ressurssterke, noe som gjør det vanskelig for bedrifter å forsvare seg. Det økte mørketallet kan ha alvorlige konsekvenser for både økonomien og samfunnet som helhet. Uregistrerte angrep kan føre til tap av data, økonomiske tap, og svekkelse av tilliten til digitale tjenester. For å redusere mørketallene er det viktig å oppfordre til mer åpenhet om cyberangrep. Bedrifter bør oppmuntres til å dele informasjon og lære av hverandre, samt samarbeide med myndigheter og sikkerhetsorganisasjoner. Ved å adressere problemene rundt mørketallene kan vi får en bedre forståelse av omfanget av cyberkriminalitet og utvikle mer effektive strategier for å bekjempe det.

Mange selskaper unnlater å rapportere angrep av frykt for omdømmetap, juridiske konsekvenser eller tap av kunder. Dette kan føre til underrapportering av forekomsten av cyberangrep. Det finnes ikke alltid klare standarder for hvordan man skal rapportere og håndtere cyberangrep i skipsfarten, noe som gjør det vanskelig å samle data. Skipsfarten er ofte avhengig av eldre teknologi og systemer som kan være sårbare for angrep. Mange av disse systemene er ikke godt beskyttet eller oppdatert, noe som kan føre til flere angrep. Cyberangrepene omfatter nettfiske, løsepengevirus, DDoS-angrep og mer. Den varierte utformingen av truslene gjør det utfordrende å kartlegge og kvantifisere omfanget av angrepene. Økende spenning mellom nasjoner kan føre til mer målrettet angrep mot skipsfartsoperasjoner, som igjen kan bli underrapportert. Mange aktører

i skipsfarten har ikke tilstrekkelig kunnskap om cybertrusler, som kan føre til dårligere beskyttelse og dermed flere angrep.

For å få et klarere bilde av mørketallene, er det behov for bedre samarbeidsinitiativ mellom rederier, myndigheter og cybersikkerhetsorganisasjoner. Dette kan inkludere deling av informasjon om trusler og angrep, utvikling av retningslinjer for rapportering, og investering i opplæring og teknologi for å styrke sikkerheten.

4. Cybersikkerhet og forebyggende tiltak

Prinsippet om staters suverenitet gjelder også i cyberspace. I denne artikkelen omtales nasjonale og internasjonale forebyggende cybersikkerhetstiltak. Cyberangrepene på Stortinget i 2020 og 2021 fra russiske og kinesiske aktører viser hvor viktige det er med regulering av cyberspace på FN-nivå. To faktorer synes å være særlig avgjørende for å styrke den globale cybersikkerheten, rettssikkerheten og samarbeid mellom stater.

Det Norske Veritas (DNV) publiserte 6. Juni 2023 sin rapport «Maritime Cyber Priority 2023: Staying secure in an era of connectivity". I rapporten advarer maritime eksperter om risiko for cyberangrep og utilstrekkelig investering i cybersikkerhet. Det framgår av rapporten at mindre enn halvparten (40 %) av fagfolk innen maritime næringer mener deres organisasjon investerer nok i cybersikkerhet. Den maritime industrien har de siste tiårene hatt oppmerksomhet rettet mot å forbedre (informasjonsteknologi) IT-sikkerheten. Denne sikkerheten referer generelt til bruk av datamaskiner og informasjonssystemer for å behandle, lagre, sende og administrere data. Dette har ført til at drift er avhengig av Operational Technology (OT) som refererer til maskinvare og programvare som brukes til å overvåke og kontrollere fysiske prosesser, som produksjonslinjer, strømnettet eller transportsystemer. For skipene betyr dette teknologi og systemer som brukes i drift og kontroll av fysiske prosesser og maskiner som i denne sammenheng utgjør overvåkning, kontrollerer og automatiserer det teknologiske utstyret om bord på skip. Dette utstyret består av sensorer, brytere, sikkerhets og navigasjonsutstyr som ikke har fått tilstrekkelig beskyttelse mot risiko for angrep.

DNVs utvalgsundersøkelse viser at tre firedeler (75 %) av utvalget på 800 respondenter, mener at virksomheten prioriterer driftsteknologien høyere enn tidligere, men bare en tredel av respondentene mener at sikkerheten er like motstandsdyktig som organisasjonens IT-sikkerhet. Mye kan tyde på at den maritime industrien ikke har fulgt opp den usedvanlige hurtige sammenkobling av systemer som har funnet sted de senere år. Driftsteknologien kobles stadig tettere til omverdenen, som medfører at cyberangrep mot disse installasjoner kan få meget alvorlig konsekvenser for driften.

DNV rapporten viser et betydelig samsvar i forståelsen av at cyberangrep kan kommer til å ramme skipsfarten i tiden som kommer. (76 %) av respondentene er av den oppfatning at cyberangrep kan føre til stenging av strategiske sjøruter. (60 %) frykter for cyberangrep kan føre til skipskollisjoner, (68 %) mener at det kan føre til grunnstøtinger, som (56 %) mener kan medføre fysiske skader eller død. Kanskje ikke overraskende uttrykker fagfolkene i undersøkelse, hele 79 %, at cybersikkerhetsrisikoen er å betrakte som like viktig som helse- og sikkerhetsrisiko.

Det er hevet over enhver tvil at skipsfartssektoren i framtiden vil være helt avhengig av at teknologien er sammenkoblet i elektroniske nettverk. Sammenkoblingen av nettverk i næringen vil være av avgjørende betydning og (87 %) av respondentene svarer at skipsfartsindustrien vil være avhengig av økning i sammenkoblede nettverk. På denne måten kan sikkerheten øke, og måten det kan gjennomføres på er å samarbeide for å styrke den felles cybersikkerheten.

I tillegg til dette er det viktig å være klar over at strengere internasjonale- og nasjonale reguleringer er i rask utvikling. Det framgår også at respondentene i denne undersøkelsen, hele (84 %) var av den oppfatning at større investeringer i cybersikkerhet var nødvendig, men bare (56 %) var overbevist om at det ville skje på grunn av reguleringer. Denne manglende tiltro til at regulering og kontroll er veien å gå for å oppnå sikkerhet, finner man ofte i skipsfartsnæringen. Dette kan bero på flere hensyn, for eksempel at skipsfart over lang tid har levd sitt «frie» liv på verdenshavene.

Utviklingen har imidlertid innhentet næringens filosofi om at denne situasjon bør eller kan fortsett. Oppfatning bygger på en sterkt foreldet forståelse av samfunnsutviklingen. Skipsfartsnæringen er allerede og vil i framtiden være underlagt langt strenger regulering og kontroll. Cybersikkerhet indikerer at framtiden for skipsfartindustrien vil måtte bestå av samarbeid, deling av informasjon, åpenhet om erfaringer og derved skape felles retningslinjer for bete praksis. Derved kan verdenssamfunnet oppleve en trygger og mer bærekraftig næring, samt en renere atmosfære og mindre forurenset hav.

Dette bekreftes av funn i DNVs undersøkelse som viser at bare (31%) mener at organisasjoner i næringen på en effektiv måte deler informasjon og erfaringer knyttet til trusler og hendelser innen cybersikkerhet. Mens (60 %) mener at åpenheten ikke er tilstrekkelig og begrunnelsen som ble gitt var at maritim industri manglet standarder for å bygge en effektiv og sikker tilnærming til cybersikkerhet. Altså internasjonal regulering og kontroll vil måtte utgjøre en viktig del av cybersikkerheten (DNV, 2023).

4.1 Brannmurer og antivirusprogramvare

Brannmurer og antivirusprogrammer er to viktige verktøy for å beskytte datamaskiner og nettverk mot cybertrusler. Selv om de har forskjellige funksjoner, arbeider de sammen for å hindre angrep, skadelig programvare (søppelpost) og uautorisert tilgang.

En brannmur er en sikkerhetsenhet eller programvare som overvåker og kontrollerer inngående og utgående nettverkstrafikk. Det fungerer som en barriere mellom et internt nettverk (for eksempel et bedriftsnettverk eller en privat datamaskin) og eksterne nettverk som internett. Brannmurer kan være både maskinvare- og programvarebasert, og bruker regler for å bestemme om trafikk skal tillates eller blokkeres.

Med andre ord er funksjonen at brannmurer kontrollere data som kommer inn og går ut fra nettverket. Den blokkerer uønsket trafikk og hinder derved autorisere brukere eller skadelig programvare fra å få tilgang til nettverket. Dette fører til beskyttelse mot eksterne angrep ved å beskytte mot trusler som DDoS-angrep, innbrudd i datasystemer og spredning av skadelig programvare.

Det finnes ulke typer brannmurer som for eksempel individuelle enheter og beskytter disse spesifikke enhetene. Med maskinvarebrannmurer beskytter hele nettverk i bedrifter for å beskytte et stort antall enheter.

Et antivirusprogram er programvare som er designet for å oppdage, forhindre og fjerne skadelig programvare, som virus, trojanere, løsepengevirus og spionvareprogram. Antivirusprogrammer skanner filer og systemer på jakt etter trusler og stopper dem før de kan gjøre skade. Spionvare er programmer i form av ondsinnet kode som installeres på en datamaskin for å overvåke brukerens interaksjon med datamaskinen, uten at det foreligger informert samtykke til dette fra bruker. Skadelig programvare dekker alle typer programvare som er laget for å skade, infisere eller utnytte datasystemer og enheter. Den skadelige programvaren kan ha undergrupper som virus, ormer, trojaner, løsepengevirus og spionprogramvare.

Illusjonen er at skanningen fjerner skadelig programvare ved at antivirusprogrammet søker gjennom filer og systemer etter skadelig programvare. Dette betyr sanntidsbeskyttelse hvor systemet kontinuerlig overvåker for å oppdage nye trusler umiddelbart. Antivirusprogrammer oppdateres regelmessig for å beskytte mot nye virus og trusler.

Disse to funksjonene, brannmurer og antivirusprogrammer utfyller hverandre, hvor brannmurer hindrer eksterne brukere fra tilgang til nettverket, mens antivirusprogrammer er utformet for å oppdage og fjerne virus eller annen skadelig programvare som allerede har funnet veien inn. Med andre ord, brannmurer beskytter mot inntrengingsforsøk fra nettverket, men antivirusprogrammet kan stoppe trusler som kommer via e-post, nedlastinger eller fysiske medier som USB-minnepinner.

For optimal sikkerhet bør både brannmurer og antivirusprogram være på plass. Brannmurer stopper mange trusler fra systemet, men i tilfelle noe kommer igjennom, vil antivirusprogrammet kunne identifisere og fjerne det. Begge disse verktøyene er avgjørende for å sikre en trygg og sikker IT-infrastruktur, enten for privatpersoner eller bedrifter.

Som eksempel er det nærliggende å vise til A.P. Møller-Mærsk som har vært gjenstand for betydelige cyberangrep, spesielt det som skjedde i juni 2017. Dette var en del av en større global løsepenge-kriminalitet kjent som NotPetya, resulterte i omfattende driftsforstyrrelser for selskapet. Systemene deres ble hardt rammet, noe som førte til at flere tjenester ble stengt ned, og selskapet rapporterte om betydelige økonomiske tap.

Mærsk arbeidet raskt for å gjenopprette sine systemer og at etter dette økt forkurset på cybersikkerhet, med mål om å beskytte seg mot framtidige angrep. De har iverksatt bedre sikkerhetsprosedyrer og teknologi for å håndtere trusler og redusere risikoen for lignende hendelser.

Cyberangrep mot store selskaper som Mærsk viser hvor sårbare de mest etablerte organisasjonene er i møte med moderne trusler, og understreker viktigheten av robust cybersikkerhet i dagens digitale landskap.

NotPetya-angrepet i juni 2017 var av de mest alvorlige cyberangrepene i nyere tid, og A.P Møller-Mærsk ble hardt rammet. Angrepsmetoden som NotPetya benyttet ble først spredt via sårbarhet i Windows, kjent som EternalBlue, og utnyttet også et kompromittert oppdateringsverktøy fra det ukrainske selskapet MeDoc. EternalBlue er et datautviklet dataprogram utviklet av U.S. National Security Agency (NSA). Det er basert på sårbarhetene i Microsoft Windows

som tillater brukere å ha fordel av tilgang til et hvilket som helst antall datamaskiner knyttet til nettverket.

Dette gjorde at skadelig programvare raskt kunne spre seg i nettverk. Mærsk opplevde omfattende driftsforstyrrelser. Selskapet måtte stenge ned flere datasenter i forsyningskjeden og logistikkoperasjoner. Mærsk rapporterte at angrepet føret til et inntektsfall på mellom 250 og 300 millioner US i tredje kvartal 2017. Dette inkluderte både direkte kostnader knyttet til gjenoppretting og tapte inntekter fra forstyrrede operasjoner. Selskapet jobbet intensivt for å gjenopprette systemene. De gjennomførte omfattende sikkerhetsprosedyrer og oppgraderinger for å sikre at de kunne håndtere framtidige trusler. Etter angrepet økte Mærsk-konsernet søkelyset på cybersikkerhet. De investerte i ny teknologi og opplæring av ansatte, og utviklet strategier for bedre å håndtere risikoen ved cybertrusler.

NotPetya ble konstruer og ansett som et angrepsmiddel rettet mot Ukraina, men spredte seg raskt globalt og rammet flere store selskaper, noe som illustrerer hvordan cybertrusler kan ha vidtrekkende konsekvenser.

4.2 Segmentering av nettverk

Segmentering av nettverk referer til praksisen med å dele et nettevek opp i mindre deler eller segmenter for forbedret sikkerhet, ytelse og administrasjon. Denne prosessene brukes i IT-sikkerhet for å redusere risiko for cyberinnbrudd ved å begrense tilgangen til sensitive data og systemer. Det brukes for å optimalisere nettverksytelse ved å redusere trafikk og minimere kollisjoner.

Dersom angrepsfakten reduseres ved å dele nettverkete i segmenter, kan man begrense angrepsmulighetene. Hvis én del av nettverket blir kompromittert, vil resten av nettverket være mindre påvirket. Styret tilgang er hvor brukere av systemet får kun tilgang til segmenter de trenger, noe som reduserer risikoen for uautorisert tilgang. For å oppnå denne effekten bruker man brannmurer og andre sikkerhetsmekanismer som kan settes opp mellom nettverkssegmentene for å kontrollere hvilken trafikk som passerer.

Mindre trafikk i hvert segment får betydning for ytelsen for ved å dele opp nettverket reduseres mengden lokal trafikk i hver segment, noe som forbedrer ytelsen og reduserer forsinkelser. Nettverksressurser kan fordeles mer effektivt mellom segmentene, slik at kritiske systemer får nok båndbredde som igjen fører til bedre ressursallokering.

Hvis det oppstår feil i nettverket, kan det være enklere å identifisere og isolere problemet i et spesifikt segment, man oppnår lettere administrasjon. Segmentering gjør det enklere å legge til nye enheter eller nettverksressurser uten påvirke nettverket.

Det finnes ulike typer for fysisk segmentering ved å bruke separate fysiske nettverksenheter, svitsjer og rutere, for å dele nettverket. For å oppnå logisk segmentering bruker man virtuelle nettverk som (VLAN) eller programvaredefinerte nettverk (SND) for å dele et fysisk nettverk i flere logiske segmenter. Mer finmasket segmentering kan man oppnå der små deler av et nettverk isoleres, ofte ved hjelp av virtuelle brannmurer og programvare.

Nettverkssegmentering er en viktig komponent i Zero-Trust-arkitekturen, hvor ingen deler av nettverket automatisk stoler på hverandre uten autorisasjon.

Dette kan eksemplifiseres ved en stor tjenesteleverandør som ønsker å beskytte sensitive kundedata og interne systemer mot interne og eksterne trusler. De har et komplekst nettverk med flere avdelinger som hver har forskjellige sikkerhetskrav. Selskapet veger å benytter avdelingssegmentering hvor nettverket deles i separate soner for hver avdeling (f.eks. kundeservice, finans, IT, osv.). Hver avdeling har egne sikkerhetspolitikk. Følsomme databaser plasseres i egen segmenter med streng tilgangskontroll. Hver ansatt må autoriseres gjennom flere identitets- og tilgangskontroller. Det etableres for eksempel kontinuerlig passordovervåking. Hver sone har sin egen sikkerhetspolitikk som kan omfatte brannmurregler, datakryptering og logging av tilgang. Sist, men ikke minst innføres revisjon og oppdatering for å sikre at det til enhver tid utføres oppdateringer og tilpassinger når det skjer endringer i organisasjonen eller trusselbildet.

Ved å dele opp nettverket og utføre streng kontroll reduseres muligheten for at sikkerhetsbrudd kan spre seg. Sensitive data blir sikret gjennom kontroll og tilgang som igjen trygger både selskapet og kundene. Kontinuerlig overvåking gjør det mulig å oppdage og handel på trusler. Eksemplet vier at Zero-Trust-arkitektur i kombinasjon med nettverkssegmentering kan gi omfattende sikkerhetsløsninger og beskytte sensitive data og redusere risikoen for angrep.

4.3 Oppdatering av programvare og systemer

Oppdatering av programvare og systemer er en viktig del av vedlikeholdet av et IT-miljø, med sikte på å forbedre sikkerheten og funksjonelt ytterligere. Det innebærer installasjon av nye versjoner, sikkerhetsoppdateringer, og feilrettinger som leveres av program leverandører. Regelmessige oppdateringer bidrar til å beskytte systemene mot kjente sårbarheter og sikre at de fungerer optimalt.

Oppdateringer inkluderer ofte sikkerhetsfiksere som retter opp svakheter som kan utnyttes av hackere. Uten jevnlige oppdateringer risikerer systemet å bli kompromittert. Kjente sårbarheter kan utnyttes av ondsinnede aktører hvis de ikke rettes opp. Oppdateringer hjelper til med å holde ytelsene som selskaper er helt avhengig av som beskyttet mot nye angrep. Oppdateringer løser ofte feil og forbedrer ytelsen, noe som bidrar til at programvarene og systemer kjører jevnt og stabilt. Nye versjoner av programvare kan inneholde optimaliseringer som gjør at systemer utnytter maskinvaren bedre.

Oppdateringer kan introdusere ny funksjonalitet, verktøy og forbedringer som kan være verdifulle for brukere og virksomheter. Regelmessige oppdateringer sikrer at programvare fungerer godt sammen med andre applikasjoner og systemer i IT-miljøet (kapabilitet).

Det finnes ulike former for oppdateringer for eksempel rette opp sårbarheter som kan brukes i cyberangrep. Dette inkluderer nye funksjoner, forbedringer eller endringer i brukergrensesnittet. Rette feil (bug fixes) som kan forårsake at programvare eller systemer ikke fungerer som de skal. Oppdatering av maskinvaren, som for eksempel ruter, svitsjer (noen ganger kalt nettverksveksler, er en nettverkskomponent som styrer datatrafikk mellom ulike noder i et nettverk) eller PC-er er avgjørende for å forbedre deres ytelse eller sikkerhet.

Når det gjelder gode rutiner for oppgraderinger er det å slå på automatisk oppdateringer der det er mulig, spesielt for kritisk programvare som operativsystem, antivirus og brannmur. Et

annet hjelpemiddel er det som kalles «patch-håndtering» (en patch er en ny programkode som erstatter eller utvider deler av eksisterende programkoder i et dataprogram for å rette på feil eller legge til ny funksjonalitet), som hjelper med å identifisere og distribuere nødvendige oppdateringer på tvers av organisasjonens systemer. Før større oppdateringer rulles ut i et produksjonsmiljø, bør de testes i et testmiljø for å sikre at de ikke forårsaker problemer med eksisterende systemer. Det er viktig å ta sikkerhetskopier av systemet før oppdateringer installeres i tilfelle noe går galt under prosessen.

Noen vanlige utfordringer som en bør være oppmerksom på at oppdateringer kan forårsake inkompatibilitet med eldre systemer eller applikasjoner. Oppdateringsprosessen kan kreve at systemene må være offline midlertidig, noe som kan forårsake driftsstans. En annen vanlig utfordring kan være at bedrifter har vanskeligheter med å holde tritt med alle nødvendige oppdateringer på grunn av ressursbegrensninger. Av nevnte grunner bør sikkerhetsoppgraderinger prioriteres høyt for å holde systemer beskyttet mot dagens cybertrusler.

4.4 Opplæring av mannskap

Cyberkriminalitet har blitt en alvorlig trussel for mange industrier, og skipsfart er intet unntak. Den maritime næringen er særlig utsatt for cyberangrep på grunn av sin globale natur, avhengighet av teknologi og komplekse operasjoner. I denne sammenheng er det viktig å vurdere hvordan man kan beskytte skipsfart mot cyberkriminalitet, og hvordan opplæring av mannskapet kan bidra til å redusere risikoen.

Trusler og angrep i skipsfarten kan ta flere former og har likhet med andre angrep på næringsvirksomhet. Og består normalt av det som på dataspråket kalles løsepengevirus hvor angripere kan låse data på skipets system og kreve løsepenger for å gjenopprette tilgangen. En annen form er nettfiske-angrep hvor besetningen kan bli utsatt for e-poster eller meldinger som ser ut som legitime forespørsler, men som egentlig kar som mål å få tilgang til sensitive systemer. Hertil kommer skadelig programvare som er ondsinnede programvarer som kan installeres på skipets IT-systemer for å stjele data, forstyrre driften eller skade systemene. For skipsfarten finnes det en spesiell form som kalles Man-in-the middle (MITM) hvor angriperne kan avlytte kommunikasjon mellom skip og landbasert operasjon, og muligens manipulere informasjon. Særlig alvorlig kan angrep mot Global Positioning System (GPS) satellittnavigasjonssystemet være. Angrep rettet mot navigasjonsteknologi kan føre til at skipet mister posisjonering eller utsettes for andre sikkerhetsfarer.

De potensielle konsekvensene av cyberangrep til sjøs kan være svært alvorlig, inkludert tap av data som blir stjålet eller ødelagt kan føre til tap av kritisk informasjon som last, ruter eller operasjoner. Et vellykket angrep kan føre til at skipet blir satt ut av drift, noe som kan ha alvorlige økonomiske konsekvenser og forstyrre leveransene. Skade omdømmet til skipsfarsselskapene som kan miste tillit fra kunder, partnere og myndigheter hvis de blir utsatt for cyberangrep. Et angrep på navigasjonssystemene kan utsett mannskapet og passasjerer for fare, for eksempel ved å føre til navigasjonsfeil eller feil kommunikasjon.

En viktig forebyggende strategi mot cyberkriminalitet er å investere i opplæring av mannskapet. Skipsfartens ansatte må være klar over de potensielle truslene og ha de nødvendige ferdigheter til å håndtere sikkerhetsbrudd. Blant de grunnleggende ferdigheten er at alle ansatte, fra kaptein til dekksgutt, bør få en grunnleggende forståelse av cybersikkerhet. Dette inkluderer kunnskap om sikre passord, hvordan identifisere nettfiske-forsøk og hvordan oppdatere systemene regelmessig. De som bruker spesifikke IT-systemer på skip, som navigasjonssystemer eller kommunikasjonsteknologi, må få opplæring i hvordan de kan bruke disse på en sikker måte for å unngå uautorisert tilgang. Mannskapet bør være kjent med hvordan de skal reagere i tilfelle et cyberangrep. Dette innebærer å kjenne til prosedyrer for å rapportere og håndtere sikkerhetsbrudd, samt hvordan man kan isolere systemene for å hindre skade. Regelmessig simulering av cyberangrep på skipet kan gi mannskapet praktisk erfaring med hvordan de skal reagere på trusler. Dette kan omfatte både tekniske og organisatoriske responser. Opplæringen bør også inkludere viktigheten av å holde systemene oppdatert med de nyeste sikkerhetsoppdateringene og programvare-patchene. Mannskapet bør få opplæring i hvordan de kan samarbeide med landbaserte IT-team og sikkerhetspersonell for å oppdage og håndtere trusler på tvers av organisasjonen.

Selskaper som driver sjøfart, kan bruke en rekke teknologiske løsninger for å forbedre cybersikkerheten, blant annet brannmurer og antivirusprogramvare, som beskytter mot eksterne angrep og skadelig programvare. Kryptering for å sikre at data som sendes mellom skip og land er beskyttet mot avlytting. Intrusion Detection Systems (IDS) systemer som kan oppdage uvanlig aktivitet på skipets nettverk og varsle mannskapet om potensielle trusler. Virtual Private Network (VPN) for å beskytte kommunikasjon mellom skipet og kontorer på land, og forhindre at sensitive data blir avlyttet.

Cyberkriminalitet er en alvorlig trussel mot skipsfartsindustrien, men ved å investere i opplæring av mannskapet, iverksette robuste teknologiske løsninger og følge internasjonale sikkerhetsstandarder, kan selskapene betydelig redusere risikoen for cyberangrep. Opplæring bør være en kontinuerlig prosess som gjør mannskapet godt forberedte på å håndtere de stadig mer sofistikerte truslene som oppstår i den digitale verden.

5. Internasjonal anbefalinger

I 2018 fremmet Russland et karv om en FN-konvensjon om cyberkriminalitet og siden har diskusjonen gått. Uenigheten har vært polarisert om behovet for en slik konvensjon, og det har vært uenighet i Ad-hoc-komiteen siden 2022. Det var heller ikke mulig å oppnå enighet under Concluding Session i februar 2024.

Det ble derfor besluttet å arrangere en Reconvened concluding session som ble berammet til 29. juli – 9. august 2024 om en konvensjon: Draft United Nations convention against cybercime se:
https://www.unodc.org/unodc/encybercrime/ad_hoc_committee(ahc_reconvened_concluding_session/main (tilgang 30/09/2024).

Det ble utarbeidet et nytt forslag som til stor forundring ble akseptert med akklamasjon 8. august 2024. Draft United Nations convention against cybercrime se:

https://documents.un.org/doc/unodc/gen/v24/055/06/pdf/v2405506.pdf (tilgang 30/09/2024)

Den teknologiske utviklingen i cyberspace har vært så hurtig at samfunnene har problemer med å holde tritt med utviklingen. Derfor er en FN-konvensjon om cyberkriminalitet en nødvendighet for å oppnå globale standarder for sikkerhet, fred og rettssikkerhet i cyberspace. Nærmere om nasjonal håndheving finner en hos (Schjølberg, 2024).

Norske myndigheter har med tydelighet fått erfare at ikke bare private, men også statlige aktører går til globale cyberangrep. Sommeren 2023 ble tolv departementer utsatt for cyberangrep – truslene var mange og meget alvorlige. Alvorlig global cyberkriminalitet forårsakes av at gigantiske private IT-selskapene styrer utviklingen av cyberspace uten globale eller nasjonale reguleringer og retningslinjer. Disse selskapene gir muligheter for desinformasjon som representerer en alvorlig fare for våre demokratier. Denne vesentlige svakheten kan eventuelt rettes på når FNs konvensjon vedtas, kanskje kan den endre hensynet til nye global og nasjonale reguleringer.

5.1 Reguleringer og standarder

Flere internasjonale organer har utarbeidet retningslinjer og krav for cybersikkerhet i skipsfarten, blant annet IMO som har utgitt retningslinjer for cybersikkerhet som en del av ISPS-koden (International Ship and Port Facility Security Code). IMO anbefaler at skipsfartsselskaper utarbeider en cybersikkerhetspolitikk og risikovurderinger.

National Institute of Standards and Technology (NIST) har utviklet rammeverk for cybersikkerhet som kan tilpasses maritime operasjoner.

ISO 27001 sertifisering er standard for informasjonssikkerhet som kan brukes av skipsfartsselskaper for å gjennomføre et system for å beskytte sensitiv informasjon.

IMO er FN-organisasjonen som er ansvarlig for å utvikle og vedlikeholde internasjonale regler og standarder for skipsfart. IMOs ISPS kode ble vedtatt i 2004 og er innrettet på fysiske sikkerhetstiltak for skipsskipsfart, inkludert terrorangrep. Selv om den ikke spesifikt dekker cybersikkerhet, er det et grunnleggende rammeverk for sikkerhet i havner og skip.

IMO Res. MSC.428(98) – Maritime Cyber Risk Management er en anbefaling som ble vedtatt i 2017 og krever at skipsfartsindustriens aktører (redere, mannskap osv.) skal iverksette tiltak for å håndtere cybersikkerhetsrisiko. IMO anbefaler at skipsfartsoperatører utvikler et system for å vurdere og håndtere cybersikkerhetsrisiko som kan påvirke skipsoperasjon, både i landbaserte systemer og om bord. I tillegg ble IMOs retningslinjer for cybersikkerhet i skipsfarten ytterligere konkretisert i 2021, og kravene om cybersikkerhet skal integreres i skipsfartsoperatørenes generelle risikostyringssystemer ble styrket.

National Institute of Standards and Technology (NIST) er et amerikansk føderalt byrå som utvikler og fremmer måle- og standardiseringsløsninger for vitenskap, teknologi og industri. NIST er særlig kjent for sitt Cybersecurity Framework (NIST CFS), som gir en struktur for identifisere, beskytte, oppdage, respondere og gjenopprette cybersikkerhetshendelser. Dette rammeverket er mye brukt innen både privat og offentlig sektor, og det er spesielt nyttig for maritim industri som ønsker å etablere en robust cybersikkerhetsstrategi. Rammeverket hjelper organisasjoner med å identifisere

risiko, gjennomføre nødvendige sikkerhetstiltak og forbedre deres evne til å håndtere cybersikkerhetstrusler.

NIST SP 800-53 /NIST SP 800-82 er dokumenter som gir spesifikke retningslinjer for cybersikkerhet på tvers av ulik sektorer, inkludert den maritime sektoren. Spesielt SP 800-82 er relevant for industrielle kontrollsystemer (ICS) og Supervisory Control and data Acquisition (SCADA)-systemer som er brukt både i havner og om bord på skip, og gir veiledning for beskyttelse av kritisk infrastruktur.

ISO 27001:2013 er en internasjonal standard som stiller krav til etablering, implementering, vedlikehold og kontinuerlig forbedring av et ledelsessystem for informasjonssikkerhet, Information Security Management System (ISMS). Denne standarden gjelder på tvers av alle bransjer, inkludert skipsfart. IOS/IEC 27001 standarden definerer kraven til et informasjonssikkerhetsstyringssystem (ISMS), som kan tilpasses til enhver organisasjon for å beskytte konfidensielt, integrert og tilgjengelighet av informasjon. Innen skipsfart kan ISO 27001 hjelpe selskaper med å håndtere informasjonssikkerhet knyttet til både operasjonelle systemer om bord på skip i landbaserte IT- og kommunikasjonsinfrastruktur.

ISO/IEC 27032 – Cybersikkerhet er mer spesifikt rettet mot cybersikkerhet og gir en veiledning for å beskytte organisasjoner mot cybersikkerhetstrusler. Det er relevant for skipsfartssektoren da den kan brukes til å beskytte kritisk maritim infrastruktur mot digitale angrep.

ISO/27033 – Nettverkssikkerhet er standarden som har oppmerksomheten på sikkerhet til nettverksinfrastruktur og kommunikasjonskanaler, som er essensielt for å sikre skipsfartsoperasjoner som avhenger av pålitelige IT- og kommunikasjonssystemer.

Sammenhengen mellom IMO, NIST og ISO 27001 gir et globalt rammeverk for maritim sikkerhet og cybersikkerhet hvor IMO har oppmerksomhet på å minimere risikofaktorer som kan påvirke skipsfartens sikkerhet og operasjoner. Mens NIST gir mer detaljer, tekniske retningslinjer og rammeverk for implementering av cybersikkerhetstiltak, spesielt innen kritisk infrastruktur som også inkluderer maritim teknologi.

ISO 27001 og andre ISO-standarder gir et globalt, anerkjent rammeverk for å etablere et robust informasjonssikkerhetsstyringssystem, som kan være nyttig verktøy for maritime aktører for å sikre sine digitale ressurser.

Når det gjelder reguleringer og standarder bør EU Network and Information System (NIS) Directive nevnes fordi EU-lovgivningen setter krav til cybersikkerhet for kritisk infrastruktur, inkludert transportsektoren.

Samlet sett er disse organisasjonene og standardene kritiske for å utvikle en helhetlig og effektiv tilnærming til cybersikkerhet i skipsfartssektoren, og de hjelper både maritime aktører og myndigheter med å beskytte seg mot de økende truslene som finnes i den digitale tidsalderen.

5.2 Sikkerhetsvurderinger og risikoanalyser

Sikkerhetsvurderinger og risikoanalyse av cyberkriminalitet i skipsfartsnæringen er et kritisk tema, ettersom skip og sjøfartsinfrastruktur i økende grad blir mål for cyberangrep. Dette skylles både den digitaliseringen som skjer i bransjen og det potensielle tapet ved et vellykket cyberangrep.

Cyberkriminalitet i skipsfartsnæringen kan manifestere seg på flere måter, de vanlige truslene har vært nevnt tidligere og er skadelig programvare som infiserer skipets datasystemer og gjør det mulig for angripere å stjele data, manipulere navigasjonssystemer eller forstyrre operasjoner. Angriperne kan kryptere skipets datasystemer og kreve løsepenger for å gjenopprette tilgang. Dette kan inkludere systemer som er kritiske for navigasjon og kommunikasjon. Angriperne kan benytte nettfiske hvor man søker å lure ansatte eller ledelsen om bord til å avsløre sensitiv informasjon, som passord eller tilgangsdata. DDoS angrep gjør at skipenes kommunikasjons- og navigasjonssystemer blir utilgjengelig. Manipulering av navigasjonsdata kan angripe og forfalske GPS- eller AIS-signaler (Automatic Identification System), og potensielt føre til at skipet navigerer til farlige områder eller kolliderer med andre fartøyer. Dette skjer ved elektroniske signaler kalt «spoofing» som innebærer å sende ut falske signaler som etterligner de ekte signalene, men med modifisert informasjon. Målet er å lure mottakeren til å akseptere de falske signalene som ekte, som kan føre til feilaktig posisjonsdata eller tidsinformasjon. «Jamning» innebærer å sende ut radiostøysignaler eller signaler på samme frekvens som det målsystem bruker, med hensikt å blokkere eller forstyrre de originale signalene. Dette kan føre til at mottakeren mister signalet helt eller opplever betydelige forstyrrelser. For eksempel kan jamming av GPS-signaler gjøre at navigasjonssystemer mister posisjonsdata, som kan være kritisk for både sivil og militært bruk. Metoden benyttes for eksempel også i cyberkrigføring og rammer motstanderen, selv om angrepsvåpenet er digitalt, kan konsekvensene av angrepet, som å ramme skipsfarten få store fysiske og samfunnsmessige konsekvenser.

Sårbarheten i skipsfarten knyttes til utstyr og teknologi. Mange av systemene om bord på skipene, som er navigasjonssystemer (GPS, ECDIS – Electronic Chart Display and Information System) og kommunikasjonsutstyr, er ikke alltid designet med sikkerhet i tankene. Ofte er systemene ikke tilstrekkelig oppdaterte, noen som kan gjøre dem sårbare for angrep.

I tillegge kommer manglende cybersikkerhetskompetanse hvor mange ansatte på skipene ikke er tilstrekkelig opplært i cybersikkerhet, noe som øker risikoen for at de kan bli utsatt for nettfiske-angrep eller feilaktig håndtere sikkerhetsprosedyrer.

Sikkerheten til tredjepartsleverandører, som teknisk støtte, vedlikehold av systemer, eller programvareoppgradering, kan være et svak punkt hvis de ikke har tilstrekkelige sikkerhetsprotokoller.

De potensielle konsekvensene av et cyberangrep på skipsfart kan være svært alvorlig, både økonomisk, operasjonelt og juridisk. Her kan nevenes økonomiske tap, sikkerhetsrisiko ved manipulering av navigasjonssystemer eller kommunikasjon. Skader på omdømmet, tap av kundedata eller driftsstans, og det kan ha juridiske og regulatoriske konsekvenser, som brudd på datasikkerhet som kan føre til juridiske krav og bøter, spesielt hvis sensitive data som personopplysninger er kompromittert.

For å forstå risikoen knyttet til cyberkriminalitet i skipsfartsnæringen, kan man benytte flere metoder for risikoanalyse. FMEA (Failure Models and Effects Analysis) er en metode som kan benyttes for å indentifisere potensielle feil i systemene om bord og vurdere hvilke konsekvenser disse feilene kan ha for skipetes drift. Risikokartlegging er en systematisk vurdering av hvilke kritiske systemer som er mest utsatt for cyberangrep og hvilke konsekvenser et angrep kan ha på drift og sikkerhet. Sannsynlighet og konsekvensanalyse en vurdering av hvor sannsynlig det er at et

cyberangrep vil finne sted, og hvilke konsekvenser det vil ha hvis det skjer. Dette kan være en del av en mer omfattende risikovurdering.

For å redusere risikoen for cyberkriminalitet i skipsfartsnæringen, kan flere tiltak iverksettes. Opplæring og bevisstgjøring av ansatte, gjentagende systemer og sikkerhetsprotokoller som å gjennomføre flere lag med sikkerhet. Regelmessige oppgraderinger av alle systemer og programvare på skipet. Sikre kommunikasjonssystemer ved å bruke krypterte kanaler for kommunikasjon og sørge for at de ikke er utsatt for DDoS. I tillegge bør man inngå avtaler med leverandører og partnere som sikrer at de også følger strenge cybersikkerhetskontroller.

I den sammenheng som behandles her kan det være av verdi å forestille seg framtidige trender og utfordringer. Særlig kan det være interessant å neven økende bruk av autonome skip. Autonome og semi-autonome skip er på vei til å bli en del av framtidens skipsfart, og disse systemene vil kunne bli attraktive mål for cyberangrep. Det er viktig å utvikle robuste sikkerhetskontroller for disse teknologiene. 5G og IoT-integrasjon blir tatt i bruk av skipsfartsnæringen for å bedre effektiviteten. Denne type integrasjon referer til hvordan femte generasjon mobilnettverk (5G) brukes sammen med Internet of Things (IoT) for å skape et mer sammenkoblet og effektivt nettverk av enheter. Imidlertid kan dette øke antallet potensielle inngangspunkter for cyberangrep hvis ikke systemene er riktig sikret.

Cyberkriminalitet i skipsfartsnæringen representerer en voksende risiko som krever proaktive tiltak for å beskytte både fysiske og digitale ressurser. Sikkerhetsvurdering og risikoanalyse bør være en kontinuerlige prosesser, med oppmerksomhet på både teknologiske løsninger, opplæring og internasjonale standarder.

5.3 Kryptering av kommunikasjon

Kryptering av kommunikasjon i skipsfarten er et svært viktig aspekt for å sikre trygg og sikker drift av maritime operasjoner. I næringen er det mange typer kommunikasjon som kan være sensitive inkludert navigasjonsinformasjon er viktig for å sikre fartøysdrift og for å unngå kollisjoner. Havnefasiliteter og logistikk likeså om ankomsttider, last og annen kommersiell informasjon kan være verdifull for pirater eller konkurrenter. Håndtering av personellinformasjon om besetninger på skipene og deres helse, lønn eller sikkerhet. Kryptering hindrer uvedkommende fra å få tilgang til følsomme data. Forhindre at informasjon blir endret eller forfalsket underveis, samt hindrer at kommunikasjon kan fanges opp, og misbrukes av utenforstående parter. Det samme gjelder i høy grad i passasjerfart.

Det finnes flere typer krypteringsteknologier som kan brukes for å beskytte kommunikasjon i skipsfarten. Noen av de vanligste metodene inkluderer SSL/TSL (Secure Sockets Layer/Transport Layer Security). Disse er kryptografiske protokoller som sikrer dataoverføringer over internett og andre nettverk. Denne teknologien brukes for å beskytte kommunikasjon på internett og andre Internet Protocol (IP)-baserte nettverk. IP er en grunnleggende kommunikasjonsprotokoll som brukes for å koble enheter i nettverket og på internett. I et IP-basert nettverk blir data delt opp i små pakker, og hver pakke inneholder en IP-adresse som viser til sender og mottaker. Disse pakkene reiser gjennom forskjellige veier i nettverket for å nå sitt endelige mål, hvor de settes sammen igjen for å

rekonstruere meldingen eller informasjonen. SSL/TLS er vanlig i systemer som håndterer webtjenester og e-post.

VPN (Virtual Private Network) skaper en sikker, kryptert «tunnel» for dataoverføring over internett. Det brukes til å beskytte slipsets kommunikasjon med landbaserte operatører og andre eksterne systemer.

IPS brukes for å sikre kommunikasjon på IP-nivå, ofte brukt for å beskytte datatrafikk i private nettverk. Kan brukes i koblinger mellom skip og landbaserte systemer eller mellom skip som kommuniserer direkte med hverandre.

End-to-end kryptering sikrer at de avsenderne og mottakerne som er ment å motta data, har tilgang til informasjonen. Selv om dataene blir avlyttet, kan de ikke dekodes uten den riktige nøkkelen. Krypteringsteknologien er også viktig i kommunikasjon via satellitt, som brukes for å sende data fra skip til land, spesielt når internettforbindelsene er ustabil eller utilgjengelig. Systemer som Inmarsat og Iridium benytter kryptering for å sikre dataene som overføres. For å håndtere sikkerheten i skipsfarten på et globalt nivå finnes det flere internasjonale organisasjoner som organiserer og reguleringer, og legger føringer for kryptering og generell cybersikkerhet. Spørsmålene er behandlet under avslitt (Regulering og standarder) ovenfor.

I takt med at skipsfarten digitaliseres blir den stadig mer avhengig av teknologiske løsninger for å forbedre effektivitet og sikkerhet, derfor vil krypteringsteknologi i økende grad spiller en rolle i å beskytte maritime operasjoner. Det vil utvilsomt komme økt interesse for bruk av blokkjede-teknologi (blockchain) for å sikre integriteten av data som sendes mellom skip og havner. Etter hvert som kvantecomputere blir en trussel mot dagens krypteringsteknologi, kan skipsfartsnæringen begynne å utforske kvantekryptering for å sikre kommunikasjon. Framtidig krypteringsteknologi kan bli drevet av KI som kan tilpasse sikkerheten basert på situasjoners risiko. Blokkjedeteknologi har flere potensielle bruksområder i skipsfarten og den maritim industri. Det muliggjør en uforanderlig digital logg over alle transaksjoner og hendelser som gir bedre sporbarhet av varer (fra produksjon til levering). Økt åpenhet mellom aktører som er rederi, havnemyndigheter, og speditører. Samt at det reduserer risiko for svindel og feilinformasjon. Effektivisering og dokumenthåndtering som for eksempel konnossementer, sertifikater og forsikringspapirer kan forenkles vesentlig. Digitalisering og automatisk verifisering, sikkerhet mot forfalskning og raskere overføring mellom parter er noen eksempler. Hertil komme smartkontrakter som selvsekvenserende kontrakter med regler kodet inn i bokkjeden. Eksempler kan være automatisk betaling når varen er levert. Løpende overvåking av fartøyets stats og betingelser (f.eks. temperatur for kjølevarer). Redusert behov for mellommenn er en annen fordel. I tillegg vil vedlikehold og reservedeler til enhver tid være under full oversikt. I denne sammenheng skal etterlevelse av miljøvernregler og sikkerhet nevenes. Blokkjede kan lagre uforandrede data om utslipp, ballastvann, og valg av seilingsrute. I tillegge kommer bruk til å dokumentere overholdelse av IMO-regelverk og miljøstandarder.

Til tross for de mange fordelene som kryptering medfører, finnes det også utfordringer. Kryptering krever betydelig prosessorkraft, og eldre og mindre fartøyer kan ha problemer med å iverksette slike løsninger effektivt. Når flere forskjellige krypteringsprotokoller er i bruk, kan det oppstå mobilitetsproblemer internt, mellom systemene på ulike skip og mellom skip og havn.

Krypteringsteknologier kan være kostbare å gjennomføre og vedlikeholde, noe som kan være en utfordring for mindre aktører i skipsfartsnæringen.

Kryptering er avgjørende for å sikre trygg og pålitelig kommunikasjon i skipsfarten. Ettersom næringen blir stadig mer digitalisert og mer avhengig av informasjonsteknologi, vil kryptering være et teknologisk verktøy for å beskytte skip, havner og logistikksystemer mot cyberangrep og datalekkasje. Samtidig er det viktig at aktørene i næringen samarbeider om å utvikle og iverksette krypteringsteknologier som er både sikker og kostnadseffektive.

5.4 Kontinuerlig overvåking av systemer

Kontinuerlig overvåkning av data for å beskytte skipsfart mot cyberangrep er avgjørende for å oppdage og reagere på trusler i sanntid. Ettersom den maritime industrien er streket digitalisert, med mange systemer som er sammenkoblet via internett (IoT-enheter, navigasjonssystemer, lastestyring, osv.), er det en konstant risiko for cyberangrep som kan kompromittere sikkerheten til havs, operasjonelle prosesser og datasikkerhet.

En effektiv overvåkningsstrategi bør ha oppmerksomheten rettet mot å identifisere uregelmessigheter, reagere på potensielle trusler, og sikre kontinuitet i både systemer og dataene som er kritiske for skipsfarten. Her kan nevnes noen sentrale elementer for kontinuerlig overvåkning av data i konteksten av cybersikkerhet for skipsfart.

Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS) er begge grunnleggende verktøy for å overvåke og analysere nettverkstrafikk i sanntid for å oppdage mistenkelig aktivitet som kan indikere et cyberangrep. De kan oppdage kjente trusler som virus, skadelig programvare eller angrepsforsøk basert på signatur eller atferdsmønstre.

Deep Packet Inspection (DPI) er en teknologi som kan brukes til å analysere dataene som sendes over skipetes nettverk for å identifisere potensielt skadelige filer eller uvanlige kommunikasjonsoperasjoner som kan tyde på et angrep. DDoS eller "man-in-the-middle-angrep".

Anomalideteksjon er nok et verktøy som benytter maskinlæring og kunstig intelligens for å identifisere unormale mønstre i nettverkstrafikk. Hvis et system uventet kommuniserer med ukjent IP-adresse eller utfører uvanlige mengder dataoverføringer, kan det signalisere at angrep.

Ved overvåking av systemer og applikasjoner benytter man sikkerhetsovervåkning av Supervisory Control and Data Acquisition (SCADA-systemer) som brukes til å kontrollere og overvåke maskinsystemer om bord på skipet, som drivsystemer, elektriske systemer og brannalarmsystemer. Disse systemene kan være mål for cyberangrep, så kontinuerlig overvåkning er nødvendig for å oppdage feil eller kompromittering.

File Integrity Monitoring (FIM) overvåker filsystemene og rapporterer om endringer i kritiske systemfiler, som kan indikere uautoriserte modifikasjoner forårsaket av et angrep. Hvis en fil blir endret eller slettet uventet, kan det være et tegn på et angrep som prøver å skjule sine spor. Overvåkning bør også inkludere kontroll på at alle systemer og programvare om bord er oppdatert med nyeste sikkerhetsoppdateringene. Angripere utnytter ofte kjente sårbarheter i programvare, det er derfor avgjørende å sørge for at alle programkoder (patcher) er gjennomført i tide.

Når det gjelder overvåking av brukeraktivitet og tilgang er det brukeradferdsanalyse som kommer til anvendelse til å overvåke avvikende oppførsel fra legitime brukere. Hvis for eksempel en bruker begynner å laste ned store mengder data eller få tilgang til sensitive områder på et system

som normalt ikke brukes, kan dette være et tegn på et internetangrep eller en konto er blitt kompromittert.

Privileged Access Management (PMA) er overvåking av tilgang til privilegerte kontoer (administratorkontoer) kan bidra til å redusere risikoen for misbruk eller angrep. PAM-verktøy kan registrere og analysere alle aktiviteter som utføres av høyt favoriserte brukere, og gi en detaljert oversikt som kan brukes til å oppdage mistenkelige handlinger.

Mange skipsfartsoperatører bruker skybaserte løsninger for å lagre og håndtere data, administrere flåteinformasjon, og kommunikasjon mellom skipene og hovedkontoret. Skybasert overvåking er derfor viktig for å oppdage eventuelle sårbarheter eller angrep mot applikasjoner som «kjører i skyen».

Cloud Security Posture Management (CSPM) er et verktøy som kan overvåke og analysere konfigurasjoner i skyinfrastrukturen for å sikre at de følger de anbefalte sikkerhetspraksisene og ikke utsetter systemene for unødvendige risikoer.

Overvåkning av fysiske systemer om bord må igjen trekkes inn i denne sammenheng. Skip har som nevnt ovenfor ofte en rekke IoT-enheter som overvåker ulike aspekter ved skipets drift, fra navigasjonssystemer til miljø monitorering og maskinovervåking. Disse enheten kan utgjøre mål for cyberangrep, og det er derfor viktig å overvåke deres integritet. IoT-enheter bør konstrueres med sikkerhet i tankene, og kontinuerlig overvåking kan identifisere om de blir manipulert eller kompromittert.

Overvåking av Automatic Identification System (AIS) er et system som gjør det mulig for skip å identifisere hverandre og spore posisjoner. Angripere kan søke å manipulere AIS-data for å skjule et skips posisjon. Ved kontinuerlig overvåking av AIS-trafikk kan man oppdage uregelmessigheter som kan tyde på svindel eller angrep.

Når det gjelder Incident Response (IR) og sikkerhetshendelsesvarsling skjer det gjennom Security Information and Event Management (SIEM). SIEM-løsninger samler inn og analyserer loggfiler fra ulike kilder (nettverk, applikasjoner, operativsystemer, osv.) for å identifisere potensielle trusler. Ved å bruke korrelasjon og analyse, kan SIEM-verktøy bidra til å oppdage og varsle om potensielle cyberangrep i sanntid. Systemet kan konfigureres til å automatisk utløse en respons basert på visse trusselnivåer. For eksempel kan en uvanlig påloggingsaktivitet føre til automatisk låsing av kontoen eller valsing av sikkerhetsteamet for videre undersøkelse.

I Cybersecurity Information Sharing finnes det spesifikke initiativ for informasjonsdeling, som MARITIME Cybersecurity Operation Center (MCCOC) eller National Cybersecurity Center of Excellence (NCCoE), der aktører kan dele informasjon om cybertrusler.

Når det gjelder kontinuerlig evaluering og forbedring bør overvåkingssystemene ha innebygget redundansmekanismer (redundans betyr at noe er overflødig eller gjentakende, ofte uten å tilføre ny informasjon eller funksjonalitet) for å sikre at ingen kritiske data går tapt dersom en systemfeil oppstår. For eksempel kan redundante servere, nettverksforbindelser og strømforsyninger være nødvendige for å opprettholde kontinuitet i overvåkingen.

Regelmessig sårbarhetsskanninger er en annen viktig del av kontinuerlig overvåking som regelmessig tester av systemene (som penetrasjonstesting og sårbarhetsskanning) for å identifisere nye svakheter som kan utnyttes av angripere.

I denne sammenheng bør det presiseres at overvåkningen er av særlig betydning i samsvar med internasjonale standarder og forskrifter som vi har vært inne på ovenfor. Her neves IMOs resolusjon MSC. 428(98) om cybersikkerhet i den maritime industrien, samt nasjonale og regionale forskrifter som kan stille krav til overvåking og rapportering.

Kontinuerlig overvåking av data er en nøkkelkomponent i cybersikkerhet for skipsfart. Ved å iverksett et helhetlig overvåkingssystem som omfatter nettverk, systemer, applikasjoner, brukeratferd og fysiske enheter om bord, kan skipsoperatører oppdage og respondere på trusler i sanntid. Dette gir ikke bare beskyttelse mot cyberangrep, men også innsikt i systemenes tilstand, noe som er avgjørende for å kunne drive i skipsfartsnæringen på en sikker måte.

5.5 Beskyttelsesplan mot cyberhendelser

En effektiv plan for beskyttelse mot cyberhendelser i skipsfartsnæringen er avgjørende for både sikkerheten til maritime operasjoner og beskyttelse av sensitive data. Som en kritisk sektor for global handel, er skipsfarten i økende grad utsatt for cyberangrep som kan forstyrre både operasjonelle prosesser og økonomiske interesser. En robust cybersikkerhetsplan må ikke bare ha oppmerksomhet rettet mot forebygging, men også på oppdagelse, respons og gjenoppretting i tilfelle en hendelse inntreffer.

Det føreste som må gjøres er å etablere en ansvarlig cybersikkerhetsavdeling som har ansvar for å overvåke og beskytte både IT- og OT-systemer som benyttes om bord på skip og i havnene. Et OT-system eller operasjonsteknologisystem, referer til maskinvare og programvare som brukes til å oppdage eller kontrollere fysiske enheter, prosesser og hendelser i industrielle miljøer. OT-systemer er ofte brukt i transport og andre sektorer der det er behov for å overvåke og styre fysiske prosesser. En slik avdelingen må gjennomføre jevnlige risikovurderinger av både eksisterende systemer og potensielle trusler. Denne vurderingen bør dekke både teknologiske, operasjonelle og menneskelige sårbarheter.

Deretter bør det settes opp et Incident Response Team (IRT) en tverrfaglig gruppe bestående av både IT-spesialister og eksperter på maritime operasjoner. Denne gruppen skal være ansvarlig for å indentifisere, håndtere og respondere på cyberhendelser. Definere klare roller og ansvar for hvert medlem i cybersikkerhetsteamet, inkludert kommunikasjon med interne og eksterne aktører, for eksempel havnemyndigheter og forsikringsselskaper.

Forebyggende tiltak som bør settes i verk er i første rekke gode cyber «hygiene»-rutiner for å sikre at alle enheter og systemer er oppdaterte og beskyttet mot kjente trusler. Det betyr regelmessige oppgraderinger og sikkerhetsoppdateringer av programvare og systemer. Sterke autentiseringstiltak som flerfaktorautentisering som Multifaktorautentisering (MFA) for tilgang til kritiske systemer. Hertil kommer tilgangsstyring og rollebasert tilgangskontroll Optimize your Role-Based Access Control (RBAC) for å begrense brukernes tilgang til bare de systemer og dataene de trenger.

Information Security Management (ISMS) må iverksettes i tråd med internasjonale standarder som ISO 27001 for å sikre systematisk og helhetlig cybersikkerhet. Her bør kryptering finne stad både når det gjelder kommunikasjon og lagrede data, spesielt når det gjelder sensitiv

informasjon som last, operasjonelle data og passasjerinformasjon. På samme måte må segmentering av IT- og OT-nettverk gjennomføres for å isolere kritiske operasjonelle systemer fra mer utsatte forretningssystemer (som e-post, nettsider, osv.). Dette reduserer risikoen for sideveis eller horisontal bevegelse ved et angrep.

Andre viktige hensyn i en beskyttelsesplan er gjennomføring av regelmessig opplæring av ansatte om cybersikkerhet. Det må foreligge kunnskap om nettfiske-angrep og sosial manipulering, risikobevissthet knyttet til USB-enheter og andre eksterne medier. Bruk av sikre passord og god praksis for autentisering. Videre sikker prosedyre for håndtering av eksterne enheter (f.eks. sjekking av USB-minnepinne). Hertil kommer gjennomføring av årlige eller halvårlige sikkerhetstester og simuleringer av cyberangrep (f.eks. nettfiske-kampanjer, løsepengevirus-scenarier), både om bord på skipene og i de maritime operasjonene.

Ved leverandør- og partneravtaler må det sørges for at alle tredjepartsavtaler (inkludert teknologileverandører, havnemyndigheter og logistikkpartnere) overholder strenge cybersikkerhetskrav og integreres i virksomhetens sikkerhetsstrategi. Bruk leverandører- og kostnadsstyring for å redusere risikoen for svake ledd i leverandørkjeden. Her kommer også inn å bli medlem av relevante cybersikkerhetsforeninger og deling av trusselinformasjon med andre aktører i bransjen (The European Maritime Security Strategy (EUMSS), NIST, IMO). Dette muliggjør proaktiv oppdagelse av trusler og forbedrer sektorens samlede beredskap.

Implementering av Intrusion Detection System (IDS) for kontinuerlig overvåke både skipets og havnenes nettverk og installasjoner for tegn på uautoriserte aktiviteter og potensielle angrep er avgjørende. Her inngår å samle og analysere systemlogger fra kritiske systemer (f.eks. navigasjonssystemer, kommunikasjonssystemer) for å oppdage tidlige tegn på angrep, som unormal aktivitet eller mistenkelig trafikk. Det bør være tett integrasjon med trusseldelingssystemer for eksempel eksterne aktører, og interne kilder, for å få tidlig advarsel om nye trusler som kan påvirke skipsfarten. Det bør installeres automatiserte verktøy for å oppdage og varsle om potensielle angrep på et tidlig stadium. Her kan nevens Computer security insident response teams (CSIRTs) som forplikter seg til å forbedre sikkerheten i nettverkene som er knyttet til internett.

Å skrive en Incidet Response Plan (IRP) gjør man ved å lage en detaljert plan som spesifiserer prosedyrer som skal følges ved cyberhendelser, inkludert hvordan hendelser skal identifiseres, klassifiseres, håndteres og rapporteres. Man prøver ut IRP jevnlig gjennom øvelser for å sikre at alle involverte parter vet hvordan de skal håndtere en hendelse på koordinert og effektiv måte. I tilfelle et angrep, isolere infiserte systemer for å hindre at trusselen sprer seg til andre deler av skipet. I tilfelle av et løsepenge-angrep, iverksettes prosedyrer for å isolere berørte systemer, samle informasjon om angrepet, og kontakte relevante eksterne aktører (cybersikkerhetseksperter, myndigheter og forsikringsselskaper). Når det gjelder intern kommunikasjon under hendelen etableres en klar kommunikasjonsprotokoll som involverer relevante beslutningstakere om bord og på land, samt andre berørte parter som havnemyndigheter, kunder og leverandører. For ekstern kommunikasjon bør man ha beredskapsplaner for offentlig kommunikasjon, inkludert mediehåndtering, for å sikre at informasjon om hendelsen deles korrekt uten å skade selskapets omdømme.

For gjenoppretting og forbedring må det sørges for at man har pålitelige sikkerhetskopier av kritiske data og systemer, samt en plan for rask gjenoppretting etter et angrep. Det må dessuten sørges for at sikkerhetskopier er krypterte og regelmessig testes for å sikre at de kan gjenopprettes i tilfelle et cyberangrep. Etter hendelen, gjennomføres en grundig gjennomgang av responsen og læringsprosesser. Identifisere svake punkter i beredskapen og iverksette forbedringer for å redusere risikoen for framtidige hendelser. Også disse cybersikkerhetsplanene må gjennomgås og oppdateres jevnlig, verktøy og prosedyrer basert på de erfaringene som er gjort under faktiske hendelser eller øvelser må benyttes.

Langsiktig sikkerhetsstrategi og innovasjon kan man oppnå ved å etablere en kultur for cybersikkerhet gjennom hele organisasjonen, fra ledelse til mannskap. Ta til seg nye teknologier og holde seg oppdatert på ny teknologi og trender innen cybersikkerhet, som KI for trusseldeteksjon, blokkjede for datasikkerhet, eller avansert krypteringsteknologi. Arbeide tett med teknologiutviklere og tredjepartsleverandører for å iverksette innovative løsninger som forbedrer sikkerheten uten å gå på bekostning av andre sikkerhetsaspekter i skipsfartsnæringen.

6. Avslutning

Skipsfartens utfordringer når det gjelder cybersikkerhet og cyberkriminalitet kan oppsummeres i flere hovedpunkter. Økt digitalisering og avhengighet av teknologi gjør det lettere for skipene å operere effektivt, men øker samtidig risikoen for cyberangrep på tvers av nettverksinfrastrukturen. Hertil kommer sårbarheter i eldre systemer som ikke er konstruert for å motstå moderne cybertrusler. Eldre systemer kan være like sikre som nye, men mangler oppgradering. Manglende cybersikkerhetskompetanse om bord på skipene er en alminnelig svakhet, manglende opplæring i rederiene er ofte forekommende. Dette gjør det mulig med angrep på kritiske systemer som er navigasjon, kontrollsystemer for maskiner, lastesystemer eller kommunikasjonssystemer. Angrep kan føre til at skip kommer ut av kontrollen, blir påført skade eller at sensitive data blir stjålet eller manipulert. Trusselbildet har utviklet seg til økende bruk av løsepengevirus hvor viktige data blir kryptert av angriperne som krever løsepenger for å låse opp programvaren. I tillegg er det fare for tyveri av sensitiv informasjon som kan bruke til økonomisk vinning eller i mer alvorlige tilfeller, for å utføre terrorangrep eller sabotasje. Det finnes få enhetlige, globale regler og standarder for cybersikkerhet i skipsfarten. Men helt fritt er det ikke, IMOs retningslinjer er ofte ikke forsvarlig implementert, de er fragmentert og ikke alltid tilstrekkelig for å håndtere endringene i cybertrusselbildet. Fjernkontroll og piratkopiering av programvare er cyberkriminalitet som kan inkludere angrep på fjernstyrte systemer som brukes til å kontroller skip, eller kopiering av navigasjonsprogramvare. Dette kan føre til angriperne får tilgang til skipenes operasjoner uten at besetningen er klar over det. Cyberangrep kan også rettes mot skipsfartens forsyningskjede. Konsekvensen kan være angrep på leverandørkjedene av programvare eller teknologiske løsninger som brukes av skipene, eller i havnene og hos logistikkoperatører som er knyttet til fartøyenes operasjoner. Mange skipsfartsselskaper har ikke tilstrekkelig beredskap for å håndtere cyberhendelser. Uten klare prosedyrer for å oppdage, rapportere og håndtere cyberangrep kan konsekvensene bli store, både økonomisk og operasjonelt. Cybersikkerhet til havs krever globalt

samarbeid mellom rederier, myndigheter, havner og teknologiutviklere for å utvikle felles standarder, dele informasjon om trusler og forbedre beredskapen på tvers av landegrenser.

Cybersikkerhet i skipsfarten står overfor betydelige utfordringer som følger av økt digitalisering, eldre teknologi, manglende ekspertise og et dynamisk trusselbilde. For å møte disse utfordringene er det nødvendig med bedre opplæring av mannskap, større investeringer i sikkerhet, utvikling av universelle standarder, og et tettere samarbeid på tvers av landegrenser med globale aktører.

Referanser

Anderson, R., & Moore, T. (2006).The Economics of Information Security. *Science,* 314(5799), 610-613.

BIMCO (1905). Baltic and International Maritime Council. København, Danmark.

Böhme, R. (2013). Security Mitrics and Economics. *IEEE Security & Privacy*, 11(2), 14-22.

Brenner, S. W. (2013). Cybercrime: Criminal Threats from Cyberspace. *SAGE Publications.*

Chio, C., Freeman, D. (2018). Machine Learning and Cybersecurity. *IEEE Transaction on Security &Privacy,* 16(6), 78-86.

Cybercrime Convention (Budapest konvensjonen) (2001).

Deibert, R., Palfrey, J., & Roio, A. (2019). *Access Controlled: The Shaping of Power, Rights, and Rules in the Digital Age.* MIT Press.

Det Norske Veritas, (2023). Maritim Cyber Priority 2023: Staying secure in an era of connectivity. Oslo: *Det Norske Veritas*.

Goodman, M. (2021). *Cybersecurity and Cybercrime: The Evolving Threat Landscape.* Oxford University Press.

He, D., Chan, S., Li, Y. (2021). Internet of Things Security: A Survey. *IEEE Internet of Things Journal,* 8(3), 1518-1531.

Krombholz, K., Hobel, H.; Huber, M. and Weippl, E. (2014). Advanced Social Engineering Attacks. *Journal of information Security and Application,* 22, 113-122. https://doi.org/10.1016/j.jisa.2914.09.005

Meland, P.H., Bernsmed, K., Nesheim, D.A., og Rødseth, Ø.J. (2021). I Pandemien: Eksplosiv økning i dataangrep på skipsfarten. Hackere firedoblet sine angrep mot shippingbransjen fra februar til juni i fjor. Trondheim: *Sintef.*

Morgan, S. (2020). *Cybersecurity Ventures: Cybercrime Report 2020.* Cybersecurity Ventures.

NIST (2020). *Framework for improving Critical Infrastructure Cybersecurity.* National Institute of Standards and Technology.

Stahl, B., Timmermans, J., & Jørgensen T. (2020). Ethics of Cybersecurity. *Springer International Publishing.*

Schjølberg, S. (2024) FN-konvensjonen om cyberkriminalitet. *Lov & Data.* 3/2024: *Artikler.*

Schjølberg, S. (2023). Cyberkriminalitet – nasjonal og global utvikling. Oslo: Universitates forlaget. ISBN 9788215066394

SoSafe, report, (2024). Cybercrime Trends 2024. The latest threats and security best practices. *SoSafe* Köln, Germany.

Zhou, Y., Shi, W., & Lin, X. (2018). Securing the Internet of Things: A Survey: *IEEE Communications Surveys & Tutorials*, 20(2), 823-852.