Bacheloroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for ingeniørvitenskap
Institutt for havromsoperasjoner og byggteknikk

Robert Arnesen
Mathias Dimmen Andersson
Sondre Ytterland

Maritim cybersikkerhet

Bacheloroppgave i Nautikk
Veileder: Marie Haugli Larsen
Mai 2020

NTNU
Kunnskap for en bedre verden

Robert Arnesen
Mathias Dimmen Andersson
Sondre Ytterland

Maritim cybersikkerhet

Bacheloroppgave i Nautikk
Veileder: Marie Haugli Larsen
Mai 2020

Norges teknisk-naturvitenskapelige universitet
Fakultet for ingeniørvitenskap
Institutt for havromsoperasjoner og byggteknikk

NTNU
Kunnskap for en bedre verden

NTNU

Kunnskap for en bedre verden

Bacheloroppgave

Hovedprosjekt TN303212

Maritim Cybersikkerhet

10003, 10007, 10020

Totalt antall sider inkludert forsiden: 57

Innlevert Ålesund, 27.05.2020

Obligatorisk egenerklæring/gruppeerklæring

Den enkelte student er selv ansvarlig for å sette seg inn i hva som er lovlige hjelpemidler, retningslinjer for bruk av disse og regler om kildebruk. Erklæringen skal bevisstgjøre studentene på deres ansvar og hvilke konsekvenser fusk kan medføre. **Manglende erklæring fritar ikke studentene fra sitt ansvar**.

Du/dere fyller ut erklæringen ved å klikke i ruten til høyre for den enkelte del 1-6:		
1.	**Jeg/vi erklærer herved at min/vår besvarelse er mitt/vårt eget arbeid, og at jeg/vi ikke har brukt andre kilder eller har mottatt annen hjelp enn det som er nevnt i besvarelsen.**	☒
2.	**Jeg/vi erklærer videre at denne besvarelsen:** • ikke har vært brukt til annen eksamen ved annen avdeling/universitet/høgskole innenlands eller utenlands. • ikke refererer til andres arbeid uten at det er oppgitt. • ikke refererer til eget tidligere arbeid uten at det er oppgitt. • har alle referansene oppgitt i litteraturlisten. • ikke er en kopi, duplikat eller avskrift av andres arbeid eller besvarelse.	☒
3.	**Jeg/vi er kjent med at brudd på ovennevnte er å betrakte som fusk og kan medføre annullering av eksamen og utestengelse fra universiteter og høgskoler i Norge, jf. Universitets- og høgskoleloven §§4-7 og 4-8 og Forskrift om eksamen.**	☒
4.	**Jeg/vi er kjent med at alle innleverte oppgaver kan bli plagiatkontrollert i Ephorus, se Retningslinjer for elektronisk innlevering og publisering av studiepoenggivende studentoppgaver**	☒
5.	**Jeg/vi er kjent med at høgskolen vil behandle alle saker hvor det foreligger mistanke om fusk etter NTNUs studieforskrift.**	☒
6.	**Jeg/vi har satt oss inn i regler og retningslinjer i bruk av kilder og referanser på biblioteket sine nettsider**	☒

Publiseringsavtale

Studiepoeng: 15

Veileder: Marie Haugli Larsen

Fullmakt til elektronisk publisering av oppgaven

Forfatter(ne) har opphavsrett til oppgaven. Det betyr blant annet enerett til å gjøre verket tilgjengelig for allmennheten (Åndsverkloven §2).
Alle oppgaver som fyller kriteriene vil bli registrert og publisert i Brage med forfatter(ne)s godkjennelse.
Oppgaver som er unntatt offentlighet eller båndlagt vil ikke bli publisert.

Jeg/vi gir herved NTNU i Ålesund en vederlagsfri rett til å gjøre oppgaven tilgjengelig for elektronisk publisering:	☒**ja**	☐**nei**
Er oppgaven båndlagt (konfidensiell)? (Båndleggingsavtale må fylles ut)	☐**ja**	☒**nei**
- Hvis ja: **Kan oppgaven publiseres når båndleggingsperioden er over?**	☐**ja**	☐**nei**
Er oppgaven unntatt offentlighet? (inneholder taushetsbelagt informasjon. Jfr. Offl. §13/Fvl. §13)	☐**ja**	☒**nei**

Dato: 27.05.2020

Forord

Etter tre år på studieprogrammet Bachelor i nautikk ved NTNU i Ålesund, Institutt for havromsoperasjoner og byggteknikk, avslutter vi studiet ved å presentere vår bacheloroppgave om maritim cybersikkerhet.

Som gruppe ønsker vi å rette stor takk til veileder Marie Haugli Larsen, for å ha gitt oss god oppfølgning og raske tilbakemeldinger. Vi vil takke respondentene for at de tok seg tid til å delta slik at vi kunne skrive denne oppgaven. Til slutt vil vi takke Kjell Inge Tomren ved institutt for IKT og realfag i Ålesund. Han har kommet med gode tips og innspill, selv om han ikke har hatt noe tilknytning til vår oppgave.

Tiden vi har arbeidet med denne oppgaven har vært svært lærerik. Vi gikk inn i dette prosjektet med ingen erfaring som forskere og med blandede datakunnskaper. Likevel hadde ingen av oss større IT-kunnskaper enn en «vanlig» person i midten av tjueårene. Kunnskapsnivået innen cybersikkerhet har økt betraktelig og vi vil spesielt trekke frem intervjuene vi hadde med penetrasjonstesterene som særdeles givende for vår forståelse av temaet og viktigheten av kunnskapen vi nå besitter.

Sammendrag

Hensikt: Målet med studiet var å kartlegge kunnskapsnivået til offiserer om bord, samt komme frem til en konklusjon som kan være med å gjøre det lettere å øke bevisstheten, og bedre holdningene mot cybersikkerhet om bord.

Bakgrunn: Cybertrusler mot IT- og OT-systemer er høyst aktuelt i 2020, og mannskapet om bord i et fartøy burde ha kjennskap til slike system for å sikre seg selv og rederiet mot angrep. IMO oppfordrer skipseiere til å ta cyberrisikostyring inn i sitt sikkerhetsstyringssystem innen 01.01.2021.

Metode: Gjennom å foreta kvalitative forskningsintervjuer av tre offiserer og to penetrasjonstestere, forsøkte vi å svare på problemstillingen vår. Ved å velge denne metoden fikk vi et innblikk i respondentenes erfaringer og kunnskapsnivå om cybersikkerhet.

Funn: Studiet har vist at offiserenes inngående kjennskap til sårbare systemer om bord ikke er nok til å sikre et skip og dets selskap mot trusler, enten truslene er utilsiktet eller ei. Det kom frem at offiserene selv ikke føler de får nok trening på området, og penetrasjonstesterene underbygger dette med sin ekspertise.

Konklusjon: Vi kan se at viktigheten av øvelser vektlegges som et preventivt tiltak, samt for å vedlikeholde kunnskap. Øvelser vil gjøre at mannskapet får testet prosedyrene sine og får kjenne på hvordan det er når for eksempel deler av systemer blir lammet av et angrep. Det ser likevel ut til at cyberøvelser nesten ikke eksisterer om bord i fartøy i dag

Vi kan også se at god teknisk planlegging er essensielt når det kommer til å kunne vedlikeholde systemer ombord. Blant de enkleste tiltakene for å sikre seg mot angrep er å oppdatere programvare for å tette kjente sikkerhetshull, men dette hjelper ikke om systemet er utgått og ikke støttes av produsenten lenger.

Engelsk sammendrag (abstract)

Purpose: The goal of the study was to determine the level of knowledge which officers holds, to make a conclusion which can make it easier to raise awareness and to better the attitude towards cyber security on board.

Background: Cyber threats against the IT- and OT-systems are most relevant in 2020. The crew on board a vessel should have knowledge about these systems and how they work to decide fitting measures to make sure that both themselves and the shipowners are protected against such attacks. IMO encourages shipowners to implement cyber risk management in their safety management system by 01.01.2021.

Method: Through choosing a qualitative design and making in-depth interviews with three officers and two penetration testers, we tried to answer our main issue. By choosing this method we got an insight in our respondent's experiences and the level of knowledge about cyber security.

Findings: The study has shown that the officer's in-depth knowledge about vulnerable systems on board is not enough to secure a ship and its owners against threats, given they are intentional threats or not. It also shows that the officers themselves feel as though they have not been given sufficient schooling or training when it comes to cyber security, and the penetration testers substantiates this with their expertise.

Conclusion: We can see the importance of drills to be emphasized as a preventive measure and to retain knowledge. Drills will make sure that the crew gets to test their procedures and that they get first-hand experience in how it feels when for example parts of their systems are paralyzed from a cyber-attack. Although it does not look like cyber drills exist on board vessels today.

We can see that good technical planning is essential when it comes to making sure you are able to maintain systems on board. Among the simplest of measures to make sure you are sufficiently protected against attacks is to update software to fix known security breaches. Although this does not help if the systems are expired and are no longer supported by the manufacturer.

Terminologi

ARPA	Automatisk radarplotting
BIMCO	Baltic and International Maritime Council
Bro	Området fra der et fartøy blir kontrollert, også kalt styrhus.
Bro-PC	Datamaskin i styrhuset på et fartøy
BWM systemer	Ballast water management (kontrollsystem for ballast)
CBT-kurs	Computer based training
Cyber	Noe som har med kybernetikk, cyberspace e.l.
Datanettverk	Nettverk som gjør det mulig for flere enheter å kommunisere
Datasikkerhet	Sikring av digital informasjon eller digitale system
DP	Dynamisk posisjonering
ECDIS	Electronic Chart Display and Information System
GMDSS	Global maritime distress and safety system
GNSS	Global Navigation Satellite System
IMO	International Maritime Organization
Informasjonssikkerhet	Sikring av informasjon eller informasjonsteknologi
ISM-koden	Internasjonale norm for sikkerhetsstyring
IT	Informasjonsteknologi
Kompatibelt	Går sammen med/kan brukes sammen
Kontrollsystem	System utformet på en slik måte at det har tilgang til å kontrollere andre systemer
NotPetya	Kryptert angrepsmetode

OT	Operasjonell teknologi
Protokoll	Konvensjonelt eller standardisert sett med regler som bestemmer tilkobling, kommunikasjon og dataoverføring mellom to endepunkter.
Risikostyring	Kartlegging av risiko og tiltak for å minimere sannsynlighet av forekomst
Segregering	Adskille systemer
Server	Programvare som tilbyr en eller flere tjenester til andre datamaskiner over et datanettverk
SMS	Sikkerhetsstyringssystem
VDR	Voyage Data Recorder
Voice-Over-IP	Internett telefoni

Innhold

Sammendrag ..... **IV**

Engelsk sammendrag (abstract) ..... **V**

Terminologi ..... **VI**

1 Innledning **1**

1.1 Problemstilling og avgrensning 1

1.2 Oppgavens oppbygning 2

2 Teoretisk grunnlag **3**

2.1 Maritim cybersikkerhet 3

2.1.1 IT og OT 3

2.2 Mennesket 4

2.3 Trusselbildet 5

2.3.1 Hva er et cyberangrep 5

2.3.2 Sikring av system 8

3 Metode **12**

3.1 Forskningsmetode 12

3.2 Intervju som datainnsamling 12

3.2.1 Intervjuguide 13

3.2.2 Utvalgsbeskrivelse 13

3.3 Gjennomføring av intervjuene 14

3.4 Validitet og reliabilitet 15

3.5 Etikk 17

3.6 Bearbeiding av data 17

3.7 Feilkilder 18

4 Presentering av funn **20**

4.1 Offiserer 20

4.1.1 Kunnskap 20

4.1.2 Bevisstgjøring om bord 21

4.1.3 System, prosedyrer og tiltak 21

4.2 Penetrasjonstestere 22

4.2.1 Trusler og konsekvens 23

4.2.2 Segregering og sikring 24

4.2.3 Bevisstgjøring og trening 24

4.2.4 Utdaterte programvarer 25
5 Drøfting 26
5.1 Ansvar krever kompetanse 26
5.1.1 Øvelser 27
5.2 Rutiner 29
5.2.1 Passordbruk 29
5.2.2 Teknisk sikring 30
5.3 Systemet om bord 31
5.4 Oppsummering 31
6 Avslutning 33
Bibliografi 35
Vedlegg 37
Vedlegg 1 – Intervjuguide Offiserer 37
Vedlegg 2 – Intervjuguide Penetrasjonstestere 39
Vedlegg 3 – Samtykkeskjema 41
Vedlegg 4 – Vurdering fra NSD 44
Vedlegg 5 – Bevisstgjøringsplakat 46

Figurliste

Figur 1 Bevisstgjøringsplakat - punkt 1. Passord..... 33
Figur 2 Bevisstgjøringsplakat - punkt 2. Oppdater programvare..... 33
Figur 3 Bevisstgjøringsplakat - punkt 3. Segregering..... 34
Figur 4 Bevisstgjøringsplakat - punkt 4. Utsette kritiske system..... 34
Figur 5 Bevisstgjøringsplakat - punkt 5. Vær forsiktig..... 34

1 Innledning

I 2017 ble Maersk utsatt for et stort cyberangrep forårsaket av NotPetya-skadevaren, som også påvirket andre organisasjoner globalt. Dette resulterte i at Maersks containerskip stod stille, og deres 76 havneterminaler stoppet opp. Gjenopprettingen av systemene gikk fort, men allikevel tapte selskapet opp imot 300 millioner USD, for blant annet tap av inntekter, IT-gjenoppretting og ekstraordinære kostnader knyttet til drift (SAFETY4SEA, 2018). Det hele startet da en tilfeldig bankansatt i Ukraina svarte på en e-post som inneholdt NotPetya-skadevaren (SAFETY4SEA, 2018).

Som en konsekvens av angrep som eksempelvis ovenfornevnte skriver Kibar (2018) at «den internasjonale maritime organisasjonen IMO har erklært at bransjen må komme à jour med gode nok løsninger for cybersikkerhet innen 2021». Kibar (2018) sier videre at «truslene kan være alt fra innblanding i navigeringssystemer og fjernstyrte prosesser, til at data lekkes eller låses, eller at angripere overtar autonome skip digitalt. Sabotasje, skadevareangrep, utpressing og ren informasjonsuthenting er andre farer i horisonten».

1.1 Problemstilling og avgrensning

Ut fra vårt ønske om å finne ut hvordan kompetansenivået til norske offiserer er med hensyn til maritim cybersikkerhet, har vi formulert følgende problemstilling:

"Hvordan er kompetansen blant norske dekksoffiserer innenfor cybersikkerhet, og hva kan gjøres for å imøtekomme IMOs oppfordring om innføring av cyber risk management?"

Ved å foreta kvalitative forskningsintervju ønsker vi å se nærmere på kunnskapsnivået til seilende offiserer om håndteringen av cybersikkerhet. Vi ønsker også å intervjue to penetrasjonstestere som har den tekniske erfaringen og innsikten til å kunne gi oss deres perspektiv på hvordan situasjonen er, og hvordan den bør håndteres.

Dalland (2012) skriver at ved å avgrense problemstillingen vil det bli lettere for oss å finne litteratur som er relevant for oppgaven. Derfor har vi valgt å avgrense problemstillingen vår til å gjelde den maritime sektoren med minst en norsk offiser om bord. Videre avgrenses oppgaven til å omhandle passasjer og cruisefart, samt transport av olje og kjemikalier, men denne avgrensningen vil ikke bli referert til videre i oppgaveteksten.

1.2 Oppgavens oppbygning

I denne oppgaven vil det først bli presentert relevant teori for å skape en forståelse av hva cybersikkerhet innebærer samt identifisering av trusler. Det teoretiske grunnlaget i oppgaven er basert på litteratur utarbeidet av shippingindustrien og allerede innhentet statistikk. Deretter presenteres hvilken metode som er benyttet for innsamling og bearbeiding av data under metodekapittelet. Videre kommer oppgavens hoveddel hvor det presenteres funn gjort i studiet som deretter drøftes i lys av problemstillingen. Til slutt utledes en avslutning av oppgaven hvor det også vil bli presentert et forslag til en bevisstgjøringsplakat.

2 Teoretisk grunnlag

I dette kapittelet skal vi presentere teori som beskriver maritim cybersikkerhet, og trusselbildet med tanke på den menneskelige interaksjonen om bord i et fartøy. I denne delen legges det vekt på fagtekster utarbeidet av shippingindustrien, herunder retningslinjer skrevet i regi av blant andre Baltic International Maritime Council (BIMCO).

Det vil i løpet av kapittelet bli forklart og gjennomgått definisjoner, trusselbildet, menneskets ansvar, anbefalinger og retningslinjer, sårbare systemer og sikring av systemer.

2.1 Maritim cybersikkerhet

Den internasjonale sjøfartsorganisasjonen (IMO) vedtok i 2017 en forskrift som omhandler cybersikkerhet i et forsøk på å få bedrifter i det maritime miljøet til å øke bevisstheten og ta grep for å sikre seg mot trusler. Forskriften oppfordrer skipseiere til å ta cyberrisikostyring inn i sitt sikkerhetsstyringssystem (SMS) innen den trer i kraft 01.01.2021 (IMO, 2017).

Den Internasjonale norm for sikkerhetsstyring (ISM-koden) del A, punkt 7 og 8 (2014) legger vekt på at et selskap skal ha iverksatt slike tiltak for å sikre viktige operasjoner om bord, herunder øke sikkerheten for skip og personell og miljøvern, samt at et selskap skal kunne identifisere nødsituasjoner, og allerede ha en beredskapsplan til slike situasjoner. ISM-koden sier også at et selskap skal ha innført prosedyrer for trening og øvelser for å være forberedt i en nødsituasjon (Forskrift om sikkerhetsstyringssystem for skip m.m., 2014).

Cybersikkerhet, herunder datasikkerhet og informasjonssikkerhet, er begreper som brukes om hverandre og beskriver det samme; å sikre at informasjon og informasjonssystemer opprettholder konfidensialitet, integritet og tilgjengelighet (Daler, Gulbrandsen, Høie, & Sjølstad, 2019). Von Solms (2013) definerer cybersikkerhet slik:

> *The protection of cyberspace itself, the electronic information, the ICTs that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace.* (s.101)

2.1.1 IT og OT

På grunn av den hurtige teknologiutviklingen om bord på fartøy vil IT- og OT-systemer flettes mer sammen, og stadig oftere være tilkoblet internett. BIMCO et al. (2018) forklarer forskjellen mellom operasjonell teknologi (OT) og informasjonsteknologi (IT) som at «OT-

systemer kontrollerer den fysiske verden og IT administrerer data». OT beskrives som all maskin- og programvare som direkte påvirker fysiske enheter og prosesser, som for eksempel navigasjonssystemer, last/ballast og ulike sensorer. IT er all annen teknologi om bord som har med informasjonsbehandling å gjøre, både maskin- og programvare og kommunikasjonsteknologier (BIMCO et al., 2018).

Systemene om bord i fartøy kan ofte være intrikate og vanskelig for en offiser uten IT-kompetanse å holde kontroll på, likevel er det viktig at offiserer om bord i et fartøy er klar over sårbarheten til systemene (BIMCO, ICS, Witherby, 2019). Potensielle sårbare systemer kan være:

Bro- og navigasjonssystemer: ECDIS, GNSS, AIS, VDR, radar/ARPA og DP

Lastestyringssystemer: lastekontrollrom, ballastsystemer, kraner og lastesporing

Kommunikasjonssystemer: satellittkommunikasjon, trådløse nettverk, satellittelefon og voice-over-IP (VOIP)

Støttesystemer: ballast, anker, slepevinsj og fortøyningsvinsjer som kan styres automatisk

Sikkerhetssystemer: som brannvarsling, overvåking og sikkerhetsalarmer for øvrig

Administrasjonssystemer: både på land og på sjøen

Velferdssystem: passasjerer eller mannskap kobler seg på nettverk med private utstyr, gjestenett

Styringssystemer: herunder fremdrifts-, strøm- og maskinsystem

Hvilket som helst av disse systemene er sårbare for et angrep på grunn av at de ofte er tilkoblet hverandre indirekte eller direkte, og et angrep på et av systemene kan spre seg hurtig til resten av systemene via fartøyets nettverk (BIMCO et al., 2019).

2.2 Mennesket

I 2018 publiserte Future Nautics en rapport fra spørreundersøkelsen *crew connectivity* hvor deltakerne var 6000 sjøfolk fra 30 ulike nasjoner (Future Nautics , 2018). Blant funnene som ble rapportert kan en se at bare 20% av deltakerne mente at cybersikkerhet var ansvaret til

alle om bord, og at ikke flere enn 49% var klar over selskapets cyberpolitikk. BIMCO et al. (2019) sier at dette er et gap i sikkerheten som en angriper kan komme til å utnytte.

Det tyske bank- og forsikringskonsernet Allianz sier i sin *safety and shipping review 2019* at de estimerer mellom 75-96% av alle ulykker til sjøs involverer menneskelige feil. Det kan da også hevdes at menneskelig feil vil være en faktor for hvor vellykket et cyberangrep vil være. For eksempel så vil mennesket i et angrep basert på sosial manipulasjon være angriperens vei inn i systemet (Allianz, 2019).

2.3 Trusselbildet

Stadig flere systemer er bygd opp rundt digitalisering, integrering og automatisering, og det kreves derfor at det er risikostyring for cybersikkerhet om bord (BIMCO et al., 2018). Daler et al. (2019, s. 43) skriver at selv om informasjonsteknologien har hatt en kraftig økning de siste tiårene så ligger sikkerheten allikevel ofte etter. I rapporten til Future Nautics (2018) kommer det frem at hele 47% av deltakerne i undersøkelsen har vært på et fartøy som har blitt utsatt for et angrep. Ifølge Daler et al. (2019, s. 43) kunne de fleste saker tilknyttet angrep ha vært unngått om det hadde vært etablert enkle sikrings- og kontrolltiltak.

2.3.1 Hva er et cyberangrep

Et cyberangrep er et hvilket som helst forsøk på å forstyrre, skade eller overbelaste skipssystemer, herunder IT- og OT-nettverk, datanettverk og mannskapets personlige datamaskiner for å få tilgang til systemer og data som tilhører selskapet og skipet for øvrig (BIMCO et al., 2019).

Det finnes flere former for angrep, og denne oppgaven tar utgangspunkt i hva slags angrep som kan komme til å påvirke hverdagen til offiserer om bord i fartøy. Generelt sett kan angrepene som påvirker rederier og skip settes inn i to kategorier:

Tilfeldige angrep: Hvor et rederi eller et skips systemer og data er ett av mange potensielle mål.

Målrettede angrep: Hvor et rederi eller et skips systemer og data er et tiltenkt mål.

I følge BIMCO et al. (2018) vil tilfeldige angrep mest sannsynlig bruke metoder som er tilgjengelig via internett, og kan som kan brukes til å lokalisere, oppdage og utnytte sårbarheter som allerede eksisterer hos et rederi eller om bord et fartøy. BIMCO et al. (2018) identifiserer tilfeldige angrep som følger:

Malware (skadevare) er en type programvare som er designet for å infiltrere og/eller gjøre skade på systemer uten at eier er klar over det. Det finnes flere forskjellige typer skadevare og den mest brukte metoden er via e-post;

- Ransomware: Er en skadevare som låser maskinen for bruk eller krypterer data på disken. Ofte brukt av svindlere for å holde maskinen din eller dine data som gissel. Frigjøres ikke før du har betalt løsepenger (ransom), eller gjort en spesifikk handling.

- Trojan: Er en skadevare som utgir seg for å være et nyttig program. Navnet stammer fra fortellingen om den store hule hesten som ble brukt av grekerne for å smugle soldater inn i Troja.

- Virus: Er en type skadevare som kjennetegnes ved at det sprer seg hver gang en infisert fil blir åpnet av brukeren eller systemet. Et datavirus kan opprette, flytte eller ødelegge filer og forstyrre en datamaskins minne eller oppstartssystem.

- Worms (Ormer): Er en type skadevare som på egenhånd er i stand til å finne nye ofre og spre seg til disse via internett.

- Spyware: Er en skadevare for å spionere på en bruker i håp om å få tak i eksempelvis graderte e-poster, brukernavn og/eller passord eller kredittkortinformasjon.

Water holing er å opprette en falsk nettside eller å infiltrere en eksisterende nettside for å utnytte besøkende.

Scanning er å tilfeldig angripe en stor del av internett.

Målrettede angrep bruker ofte mer sofistikerte metoder. Typiske metoder er (BIMCO et al., 2018):

Social engineering (sosial manipulering) er en form for dataangrep som har svært lite med teknologi å gjøre. I motsetning til "tradisjonell" teknisk hacking hvor målet gjerne er ettertraktede og kompliserte med høy teknisk sikkerhet, er målet her selve brukeren som sitter bak skjermen.

Angriperen går ut ifra at den menneskelige faktoren er sikkerhetens svakeste ledd og teknologien er altså ikke målet i seg selv, men derimot bare et virkemiddel for å svindle brukeren til å eksempelvis gi fra seg informasjon (Nätt & Heide, 2015, s. 29).

Informasjon som ikke bare kan gi angripere tilgang til nettverk og systemer, men også fysiske rom om bord. Dette kan være eksempelvis kontrollrom eller motorrom (BIMCO et al., 2019).

Den kanskje mest vanlige formen for sosial manipulering er **phishing**. Phishing er å forsøke å få sensitiv informasjon fra en bruker ved å sende ham/henne en e-post eller lure ham/henne inn på en falsk nettside som ser ekte ut. Det kan for eksempel være en kopi av nettsidene til en nettbank eller en kopi av påloggingssiden til facebook. Dette kan kalles nettfiske på norsk (Nätt & Heide, 2015, s. 44).

Spear phishing er en variant av phishing der bakmennene på forhånd samler inn data om personer eller bedrifter. Denne dataen benyttes for å gjøre e-post og nettsider mer troverdige ved at de inneholder informasjon tilhørende offeret.

Brute force (ren styrke) er en metode som går ut på å prøve mange passord med håp om å gjette riktig.

Denial of service (tjenestenekt) er en metode som gjør at brukere ikke får adgang til tjenester ved å overbelaste nettverk.

Motivasjon

Motivene for å utføre et cyberangrep varierer, og BIMCO et al. (2018) har delt angriperne inn i fire kategorier med hensyn til motivasjon:

- *Aktivister*, inkludert misfornøyde ansatte sin motivasjon er å skade omdømme til selskapet eller å forstyrre driften. Målet til denne gruppen kan være å ødelegge data, lekkasje av sensitiv informasjon, medieoppmerksomhet, eller nektelse av adgang til systemer eller tjenester.

- *Kriminelle* sin motivasjon er økonomisk gevinst, kommersiell spionasje eller industriell spionasje. Målet til de kriminelle er ofte å selge stjålet data eller kreve løsepenger for stjålet data og for systemers operasjonelle drift. Målet kan også være å tilrettelegge for uredelig transport av last som å samle informasjon til en mer sofistikert kriminell handling; nøyaktig posisjon til lasten, hva slags skip som transporterer, handlingsplaner og lignende.

- *Opportunister* har selve utfordringen som motivasjon, og målet er å komme seg igjennom sikkerhetsnettet eller økonomisk vinning.

- *Stat/organisasjoner/terrorister* har politisk vinning og spionasje som motivasjon, og målet deres er å samle informasjon eller å forstyrre økonomi og kritisk nasjonal infrastruktur.

BIMCO et al. (2018) nevner i tillegg at det er en mulighet for at ansatte kan komme til skade for å blottlegge cybersystemer og data. Som hovedregel er det utilsiktet, men oppstår som følge av menneskelige feil skapt mens håndteringen av IT- og OT-systemer foregår, eller mangel på å følge prosedyrene.

National Cyber Security Centre (2016) skriver at selv om angripere har motivasjon og kapasitet til å utføre et angrep, er de avhengige av at det finnes en mulighet for et angrep. Med dette mener de at selv om det ikke er mulig å ha kontroll over angriperne, kan det gjøres vanskeligere for dem å lykkes.

2.3.2 Sikring av system

Selv om det er umulig for et rederi eller et selskap å sikre seg helt mot et angrep, er det likevel viktig at programvarene om bord holdes oppdatert for at systemene skal være sikret mot sikkerhetshull. Likeså er det viktig med brannmurer og virusprogrammer (BIMCO et al., 2019). Ifølge National Cyber Security Centre (2016) finnes det billige og effektive løsninger for å sikre seg mot angrep over internett. Disse er som følger:

- *Skadevarebeskyttelse*: etablerer og vedlikeholder skadevarebeskyttelsen som oppdager og reagerer på kjente angrepsmetoder.

- *Oppdateringssystem*: oppdaterer programmer som er mest utsatt og sårbare med siste tilgjengelige versjon av programmet, for å unngå angrep som utnytter programvarefeil.

- *Passordrutiner*: sørger for at en god passordrutine er på plass og forståelig for bruker.

- *Brukertilgang*: sørger for at brukere har begrenset tilgang til systemer, og begrenset mulighet til å utføre handlinger.

- *Utførelseskontroll*: hindrer at en ukjent programvare kan installere eller kjøre seg selv, inkludert USB og CD.

Videre utdypes noen av punktene ytterligere.

Passord

I boken *Datasikkerhet, ikke bli svindlerens neste offer* blir viktigheten av gode passord tungt vektlagt. Nätt & Heine (2015) forteller at hjernen ikke er konstruert for å lage tilfeldige tegnsammensetninger, og derfor velger folk ofte passord som er lette å knekke.

Nätt & Heine (2015) forklarer videre typiske feil som kan unngås når passord skal opprettes:

Unngå personlig informasjon: Ved hjelp av social engineering, sosiale medier eller annen offentlig informasjon finner angripere personlig informasjon om deg som hjelper de å knekke passord.

Unngå vanlige passord: Selv om passord ikke bør ha personlig informasjon, bør de ha personlig preg. National Cyber Security Centre i Storbritannia publiserte i april 2019 en liste over de 100 000 mest hackede passordene. Øverst på denne listen er passord som "123456", "qwerty", "password" m.m (National Cyber Security Centre, 2019).

Unngå ordlistepassord: Videre forteller Nätt & Heine (2015) at dersom angripere ikke lykkes i å finne et passord basert på metodene nevnt ovenfor så kan vanlige ord og begrep testes ved hjelp av automatikk. Denne type angrep kalles for "ordlisteangrep". Her blir det brukt programmer som tester ord og uttrykk fra ordlister og nettsider for å knekke et passord.

Nasjonal sikkerhetsmyndighet (2018) anbefaler å bruke 16 tegn i passord og sier at dette vil gi akseptabel beskyttelse. De skriver også at det de ser på som best og mest brukervennlig er å lage passfraser/passetninger i stedet for ord, og aller helst dialekt, slang eller feilstavede ord. Dette kan gjøre det lettere for folk å huske passordet, samtidig tilfredsstilles anbefalingen om lengde og kompleksitet.

Oppdatering

BIMCO et al. (2019) skriver at oppdatering av programvare eller *patching* er viktig siden dette er regelmessig utstedt for å tette sikkerhetshull. Dette gjelder alt av datamaskiner og alle programmer som omhandler endepunktbeskyttelse. Enheter som kan kobles til det sentrale nettverket ombord er å anse som et endepunkt. Disse enhetene kan være

inngangspunkt for datasikkerhetstrusler og trenger derfor sterk beskyttelse. Dette fordi de ofte er det svakeste leddet i nettverkets sikkerhet. En slik type beskyttelse kan være:

- Anti-virus
- Brannmur
- System for å oppdage innbrudd i nettverket
- Data input/output-kontroll
- Program- og brukeradministrasjon (BIMCO et al., 2019)

Segregering

Ofte vil det enten være rederiets interne IT avdeling eller eksterne innleide konsulenter som har ansvar for å segregere nettverk. Uansett er det nyttig for en offiser å ha tilstrekkelig kunnskap for å verifisere at segregeringen av nettverk har blitt gjort ordentlig (BIMCO et al., 2019, s. 78)

BIMCO et al. (2018) sier at tradisjonelt sett har datanettverk vært åpne på en slik måte at alle enheter som er koblet til kan se hverandre. Å sette opp et nettverk på denne måten er veldig lettvint, men fører også til at konsekvensene av et vellykket angrep kan bli større. For dersom alle enheter kan se hverandre på samme nettverk og bare en av de blir infisert, kan dette spre seg til andre enheter fort. I ytterste konsekvens kan dette føre til at angripere får tilgang til skipets kontrollsystem, og da kunne eksempelvis kontrollere fremdrift, ballast, strømstyring eller andre ombordbaserte integrerte system (BIMCO et al., 2018).

BIMCO et al. (2019) skriver at prinsipielt burde nettverkstilgangen til et system holdes til et minimum, altså det tilgangsnivået et system trenger for å minimum kunne utføre tiltenkt handling. Som forklart ovenfor burde for eksempel ikke en datamaskin på et kontor om bord ha tilgang til bro- eller maskinroms-nettverket.

Videre skriver BIMCO et al. (2018) at for å oppnå segregering av nettverk kan det være greit å bruke flere V-LAN (virtuelle lokale områdenettverk). Disse kan bli satt opp på en slik måte at de grupperer enheter etter hvilken tilgang de skal ha, ettersom formålet med et V-LAN er å få låst av tilgangen til enheter seg imellom. For eksempel mellom datamaskiner og servere.

En datamaskin som blir brukt i jobbsammenheng trenger sannsynligvis bare tilgang til e-post serveren (IT) og ikke serveren til strømstyringen om bord (OT) (BIMCO et al., 2018).

En korrekt segregering kan betydelig hindre en angripers tilgang til et skipssystem, og er en av de mest effektive metoder for å forebygge cyberhendelser og forhindre spredning av skadevare (BIMCO et al., 2018).

Opplæring

Fra 2012 til 2018 økte antall sjøfolk som hadde tilgang til internett ombord med over en halv million (520 000), og ser man bare på tallet kan det være lett å glemme at dette er 520 000 forskjellige mennesker (Future Nautics , 2018). For å komme á jour med IMO sin oppfordring om at alle rederi skal ha adressert cyberrisiko i sikkerhetsstyringssystemet før 01.01.2021, skal også alle disse 520 000 menneskene ha opplæring i håndtering av cybertrusler i henhold til ISM-koden Del A, punkt 1.2.2.3 (2008). Dette punktet sier at selskapets mål for sikkerhetsstyring skal være «stadig å forbedre ferdighetene til personell i land og om bord med hensyn til sikkerhetsstyring, herunder forberedelse på nødssituasjoner som omfatter både sikkerhet og miljøvern».

BIMCO et al. (2018) sier at cybersikkerhetstrening burde være tilrettelagt for de individuelle rollene om bord, men viser også til at de burde dekke følgende generelle prinsipp:

- E-post og internettbruk
- Bruken av personlige enheter om bord
- Programvare, datasikkerhet-praksiser og back-up protokoller
- Oppbevaring av passord og sensitiv personlig/rederi informasjon
- Identifisering av mistenkelig aktivitet eller enheter
- Gjenkjenning av malware og phishing-forsøk
- Bruken av preventive midler som sikkerhetsoppdateringer, systemoppdateringer, samt anti-virusprogramvare.
- Cyberrisikoen tredjeparter utgjør (slik som eksterne leverandører og ingeniører)
- Hvordan planlegge for vedlikehold av programvare når en serviceoperatør kommer om bord.

3 Metode

I dette kapittelet skal vi redegjøre hvordan vi kom frem til en problemstilling og hvordan vi valgte metode for innsamling av data. Videre blir det presentert hvordan intervjuene ble gjennomført og tankene bak intervjuguiden, samt en presentasjon av utvalgsbeskrivelsen. Deretter fremstilles en gjennomgang av selve arbeidet og validiteten til undersøkelsen. Videre behandles analysemetoden valgt for bearbeiding av den innsamlede datamengden, og til slutt en gjennomgang av feilkilder

3.1 Forskningsmetode

Metoden vi har valgt er kvalitativ metode i form av intervjuer, som følge av oppgavens art. Dalland (2012, s. 112) sier at «de kvalitative metodene tar sikte på å fange opp mening og opplevelse som ikke lar seg tallfeste eller måle». Vi ønsker å se på offiserenes kunnskapsnivå rundt cybersikkerhet, hvilke rutiner de har på området og i det hele tatt hvordan sikringen av informasjon og operasjon praktiseres om bord i et fartøy.

Maritim cybersikkerhet er et komplisert tema som er veldig aktuelt i dag, men som også er et ukjent fagområde for oss. Derfor har vi i tillegg til offiserene valgt å intervjue penetrasjonstestere som har arbeidet med å teste og kvalitetssikre den maritime cybersikkerheten, for å gi oss et mer nyansert og nøyaktig innblikk i den maritime cybersikkerheten.

I motsetning til kvantitativ metode hvor det samles data gjennom undersøkelser og spørreskjema, samler vi her data i form av intervju hvor respondentene kan få prate åpent rundt nøkkelspørsmålene, dele sine erfaringer og gi oss et mer personlig innblikk i deres oppfatning av sikkerheten rundt både IT- og OT-systemer om bord. Når vi stiller spørsmål om hvordan noe er i virkeligheten, er det et empirisk spørsmål (Dalland, 2012, s. 115).

3.2 Intervju som datainnsamling

Kvale & Brinkmann referert i Johannessen, Tufte og Christoffersen (2015, s. 135) karakteriserer det kvalitative forskningsintervjuet som en samtale med en struktur og et formål. Oppbygningen er avhengig av hvilken rolle deltakerne har i intervjuet. Partene er ikke likestilte i intervjuet siden det er intervjuer som stiller spørsmål og kontrollerer situasjonen. Slike intervjuer kan ofte oppfattes mer som en samtale heller enn rene spørsmål og svar, da målet er å forstå eller tolke noe.

Vi gjennomfører intervjuene over telefon, som vi mener er mest praktisk siden respondentene enten er på sjøen eller befinner seg på andre siden av landet. Når vi intervjuer har vi en intervjuguide som vi tar utgangspunkt i [vedlegg 1-2]. Vi tar opptak av samtalen, slik at vi på et senere tidspunkt kan transkribere, og lar respondenten styre samtalen. Vi har også muligheten til å grave dypere i enkelttema om respondenten har kunnskap eller sterke meninger om et spesielt felt.

3.2.1 Intervjuguide

Når dataene skal samles inn via et kvalitativt forskningsintervju, vil første bud være en godt gjennomarbeidet intervjuguide. Før intervjuet settes i gang skal kunnskap være på plass og en teoretisk forståelse for fenomenet som undersøkes, slik at det kan stilles relevante spørsmål (Kvale & Brinkmann, 2017, s. 141). Det første vi gjorde før vi opprettet spørsmål og tema til intervjuguiden var å sette oss inn i konteksten rundt problemstillingen, som i denne sammenhengen betydde å lese seg opp på cybersikkerhet i bøker og artikler. Under utarbeidingen av spørsmålene ville vi ikke teste kunnskapen til respondentene, men stille mer åpne spørsmål for å lære om respondentenes erfaringer og syn på cybersikkerhet. En åpen situasjon under intervjuet vil også gi større sjanse for spontane og uventede svar (Dalland, 2012, s. 167).

Vi drøftet i gruppen om intervjuguiden skulle sendes i forkant til respondentene for å forberede seg, men kom frem til at det ikke ville være gunstig om vi ønsket oss en åpen samtale og spontane svar. Respondentene fikk likevel en samtykkeerklæring [vedlegg 3] på forhånd som inneholdt formuleringen av problemstillingen vi jobbet med.

Videre måtte vi ha informanter med relevans for oppgaven. Vi kom frem til at vi behøvde to forskjellige utvalg. Dette betydde at vi måtte utforme to intervjuguider ettersom de satt på ulik erfaring og det var ulike data vi ønsket å hente. Vi delte opp intervjuguiden etter tema som vi mente var relevante, i tillegg til noen forslag til spørsmål for hver enkelt kategori. Vi brukte disse spørsmålene relativt fritt ettersom intervjuguiden bare skulle være behjelpelig med å lede oss gjennom intervjuet, slik at samtalen forble så åpen som mulig slik Dalland (2012, s. 167) forklarer.

3.2.2 Utvalgsbeskrivelse

Da oppgavens omfang ble bedre kjent for oss, ble det diskutert hvor mange informanter vi trengte for å få nok svar og tilstrekkelig bredde i resultatene, samt hvilke grupper som måtte intervjues. Valget av intervjupersoner var strategisk, fordi vi skulle ha to forskjellige utvalg

der noen skulle dele erfaring fra sjøen, og noen skulle forklare sikkerhetsaspektet ved problemstillingen. Vi fant det derfor hensiktsmessig å utføre to forskningsintervjuer med eksperter innenfor cybersikkerhet, penetrasjonstesterene, og deretter også tre intervju med offiserer på ulike skip, både styrmenn og kapteiner

Intervju med penetrasjonstesterene ble bestemt fordi de arbeider med maritim cybersikkerhet som sikkerhetskonsulenter, og kan gi oss en innsikt i temaet som ikke offiserene kan. Penetrasjonstesterene jobber i ulike selskap og har ulik erfaring med sikkerhetstesting av nettverk om bord på skip, og de har erfaring med å arbeide for norske og utenlandske rederi. Vi kontaktet penetrasjonstesterene direkte via e-post hvor de sa seg villig til å hjelpe oss ved stille til intervju.

Ved valg av offiserene ønsker vi å få en innsikt i deres forhold og prioritering av cybersikkerhet, deres kunnskapsnivå og hva som faktisk blir praktisert ute på sjøen. Det ble bestemt at vi ville intervjue norske offiserer i forskjellige næringer. Dette for å se om intervjupersonene har ulikt kunnskapsnivå og holdninger til temaet.

3.3 Gjennomføring av intervjuene

«Formålet med det kvalitative forskningsintervjuet er å få tak i intervjupersonens egen beskrivelse av den livssituasjonen hun eller han befinner seg i» (Dalland, 2012, s. 153). På forhånd hadde vi utarbeidet en intervjuguide inndelt i forskjellige temaer for å holde en «rød tråd» gjennom intervjuet. I diskusjonen om hvorvidt det var nødvendig å møte intervjuobjektene ansikt-til-ansikt måtte vi ta følgende i betraktning: tilgjengelighet, tid og relevans for oppgaven.

Da vi skulle prøve å avtale et tidspunkt for intervju om bord med de forskjellige offiserene, viste det seg til slutt at det kom til å bli vanskelig å tilordne, da lastehavnene lå et godt stykke unna studiested, og timeplanen var utilregnelig. Det ble da bestemt at vi skulle utføre intervjuene over telefon, og siden vi ville ha det samme utgangspunktet for alle intervjuene, ble penetrasjonstesterene også intervjuet over telefon.

Vi kontaktet alle intervjupersonene på samme måte over telefon. Vi forklarte dem hvordan intervjuet kom til å foregå, og når opptaket skulle til å starte. Intervjuene ble utført av to studenter i vår gruppe, men alle var til stede ved alle intervjuene.

Ved oppringning ble intervjupersonen satt på høyttaler slik at vi kunne ta opp samtalen med opptakere. Vi brukte to opptakere for å sikre redundans om noe skulle skje med en av opptakerne.

Spørsmålene ble stilt systematisk etter intervjuguiden, og på samme måte til alle intervjupersonene. Da intervjuene nærmet seg slutten åpnet vi opp for egne tanker og innspill fra intervjupersonene, i tilfelle de hadde komt på noe underveis.

Helt til slutt i intervjuet ble det anledning for at de andre i gruppen som ikke stilte spørsmål kunne komme med innspill som de hadde notert seg.

Etter endt intervju fordelte vi opptakene likt på gruppen, slik at alle deltok likt ved transkripsjonen. Vi sørget for at transkripsjonen skulle foregå innen rimelig tid etter intervju, slik at vi minsket faren for å miste informasjon.

3.4 Validitet og reliabilitet

Validitet og reliabilitet er to ting som må evalueres for om man kan si at forskningsarbeidet har gitt troverdig kunnskap, og det er flere vitenskapelige metoderegler og kunnskapskrav for å oppnå dette. Med validitet mener vi at dataene vi har samlet inn har relevans og gyldighet, og med reliabilitet må vi evaluere påliteligheten av dataen (Dalland, 2012, s 52).

I all forskning vil det bli stilt spørsmål om dataens pålitelighet eller reliabilitet, altså hvorvidt dataene som er samlet inn er nøyaktige og gode nok. Når man skal evaluere reliabiliteten bør man da gå gjennom metoden for innsamling, bearbeidingen, og hvilke data som blir brukt (Johannessen et al., 2015, s. 40). Når vi har intervju over telefonen slik som vi har, vil problemstillingene i våres tilfelle være; om spørsmålene vi stiller er oppfattet korrekt av respondent, at vi transkriberer og noterer riktig, lyden i opptakene er gode nok. Disse kravene krevde godt forarbeid av oss som forskningsgruppe (Dalland, 2012, ss. 120-121).

Videre vil vi gå gjennom prosessen fra vi startet datainnsamlingen til vi var ferdige med å bearbeide den, samt evaluere metoden vi brukte.

Vi begynner med å se på påliteligheten ved innsamlingen av data, altså intervjuene, og hva som kunne påvirke denne. Ettersom det er intervjuet og samtalen som bestemmer kvaliteten på datainnsamlingen, vil det være vanskelig for en annen forsker å få samme resultat, siden vår unike erfaringsbakgrunn også vil gi en unik tolking (Johannessen et al., 2015, s. 229). Det betyr at intervjuprosessen vil være viktig å gjennomføre tilfredsstillende, samt å gi en

åpen og presis beskrivelse av prosessen. Vi brukte god tid på å lage to intervjuguider, en til offiserene og en til penetrasjonstesterene, som var delt opp i tema for å holde samtalen relevant og for å få de data vi var ute etter. Intervjuene ble gjennomført over telefonen. Opptaket av samtalene vil da være den viktigste komponenten til å styrke påliteligheten. En faktor som kan redusere påliteligheten videre er om transkriberingen av opptaket blir feil eller misforstått. Vi løste dette ved å velge et sted med lite støy og sjekket at utstyret fungerte før vi ringte, og som en ekstra forsikring brukte vi to opptakere slik at vi kunne velge det beste opptaket og oppnå redundans. I tillegg gikk vi gjennom transkriberingen som gruppe for å forsikre oss om at det vi hadde notert var korrekt og at vi hadde forstått alle informantene korrekt.

Før vi ringte informantene fikk de et samtykkeskjema vi laget ut fra en mal fra NSD, slik at de var innforstått med vilkårene i deltakelsen, herunder opptak, lagring av informasjon og bruken av data fra oppgaven vår. Skjemaet forklarte tema for intervju, anonymitet og annen informasjon om hva dette innebar, samt at før vi startet opptak forklarte vi de igjen om hvordan de skulle anonymiseres. Dette mener vi ga en ro og trygghet for informantene til å svare ærlig.

Ettersom vi har gått gjennom alle data felles som gruppe, detaljert forklart metoden for innhentingen av data, samt at vi må gå ut ifra at informantene har vært ærlige, håper vi at dette har bidratt til å styrke påliteligheten til oppgaven. Det betyr likevel ikke at andre forskere med ulikt erfaringsgrunnlag enn oss ikke ville fått en annen tolking av dataene og fremstilt andre funn.

Med validitet i en kvalitativ forskningsoppgave som vi har er spørsmålet om det er sammenheng mellom problemstillingen vi har utarbeidet og dataene vi samler inn. Det betyr at vi med god validitet oppnår troverdighet (Johannessen et al., 2015, s. 230). Altså at vi ikke bare har valgt ut det vi ser på som relevante og gode kilder eller informanter, men at dataene vi får ut ifra dem gjennom intervju vil være relevante (Dalland, 2012, s. 120). Vi har i tidligere delkapittel forklart intervjuguiden og prosessen under datainnsamlingen, og med dette mener vi at dataene våre svarer på problemstillingen vår.

3.5 Etikk

Ettersom dette er en stor læringsmulighet for oss, i tillegg til de som eventuelt måtte lese og bruke oppgaven i fremtiden, var det viktig at vi gjør alt på en korrekt måte analytisk og etisk.

Da dette er første gang vi går frem i rollen som forskere med egen data, var det flere problemstillinger å tenke over. For eksempel hvordan vi skal opptre som forskere og hvordan behandler vi data. Når det kommer til notatskriving og koding av dataene er det viktig at vi har forstått respondentene riktig. Vi sikret oss mot dette med å stille oppfølgingsspørsmål og ved å diskutere imellom oss for å være sikre på at alle hadde samme oppfatning.

Det er flere etiske problemstillinger når man skal skrive en slik forskningsoppgave. En av dem vil være det som omhandler anonymiteten til informantene.

Vi som forskere hadde noen utfordringer klare før vi tok kontakt med intervjuobjektene. Vi startet med å søke til Norsk Senter for forskningsdata (NSD), og fikk prosjektet godkjent [vedlegg 4]. Etter at vi hadde bestemt oss for hvilke informanter vi skulle intervjue, sendte vi dem et samtykkeskjema fra NSD med informasjon om hvem som var ansvarlige, hva det innebar for dem å være med og hvordan vi oppbevarer data. Da vi tok kontakt over telefon forklarte vi hvordan og hvor lenge vi ville oppbevare opptakene, samt fikk muntlig samtykke. Personopplysningene vi har på informantene, blir erstattet med en kode som vi lagret på navneliste adskilt fra andre data. Vi nevner ikke navn på personer, arbeidssted eller organisasjoner som er nevnt i samtalene.

3.6 Bearbeiding av data

I arbeidet med analysen av intervjuene brukte vi tematisering med meningsfortetting. Dette blir beskrevet av Kvale & Brinkmann (2017, s. 232) som en «forkortelse av intervjupersonenes uttalelser til kortere formuleringer. Lange setninger gjøres kortere, hvor den umiddelbare mening i det som er sagt, gjengis med få ord». Vi vil altså analysere svarene vi får av intervjupersonene og rette fokus mot hvilke svar som går igjen. Ved å gjøre det på denne måten mener vi at vi ville komme frem til det mest sentrale i problemstillingen.

Selve tematiseringen består av fem trinn: Det første trinnet vil være å lese over alle intervjuene for å få en oversikt over helheten, før vi deler det opp i naturlige enheter etter innhold i trinn nummer to. Det tredje trinnet består av å uttrykke det sentrale temaet i enheten så enkelt som mulig. Deretter skal vi i løpet av trinn fire se innholdet i enheten i lys av

problemstillingen. Dette gjøres før vi i femte og siste trinn binder sammen de viktigste emnene i intervjuet til et mest mulig fortettet uttrykk for meningsinnholdet (Kvale & Brinkmann, 2017, s. 232).

Da det ble brukt to forskjellige intervjuguider, en til penetrasjonstesterene og en til offiserene, ble de splittet opp i to grupper og analysert hver for seg, likevel ble det gjort med samme metode. Intervjuene ble tematisert etter hvilke svar vi fikk, dette ble gjort i plenum for å sikre oss mot tap av informasjon, før vi begynte å kategorisere.

Penetrasjonstesterene sine svar ble kategorisert som følgende: trussel og konsekvens, segregering, sikring, bevisstgjøring, trening og planlegging. Offiserenes svar ble kategorisert som: kunnskap, lærevillighet og prosedyrer. I intervjuet med en av penetrasjonstesterene ble det også stilt et tilleggsspørsmål. Dette for å tette egne kunnskapshull, og ble derfor behandlet i en egen kategori; hacking av segmenterte nettverk.

Ved tolkingen av våre bearbeidede data ble det lagt vekt på om svarene vi fikk var gjentagende, altså om vi fikk samme svar fra ulike respondenter på samme spørsmål. Svarene vi fikk kan utenom å være ulike, også ha ulik mening eller varierende grad av viktighet for vedkommende. Derfor anså vi det som svært viktig dersom svar gjentok seg under intervjuene, da svarene får en annen tyngde når dataene skal ilegges en dypere mening.

3.7 Feilkilder

Vi har tatt med en del feilkilder under kapittel 3.5 og 3.6, men vi vil ta for oss noen flere her.

Da materialet vi jobber med er samlet inn selv gjennom datainnsamling i form at intervjuer må vi ta hensyn til ulike feilkilder som kan høre med. Det kan for eksempel være at vi tillater oss selv å være forutinntatte, tillater oss å forvente et visst svar eller at vi på forhånd har bestemt oss for et utfall og bare leter etter vinklinger for å argumentere for det. Vi ønsker i stedet å fokusere på informasjonen gitt av informantene under intervjuet og la fakta bestemme utfallet av oppgaven.

Da intervjuene ble gjennomført over telefon kan det argumenteres for at vi mister noe informasjon vi kunne fått ved å eksempelvis gjøre det ansikt til ansikt.

Ansiktsuttrykk og mimikk, kroppsspråk og andre ikke-verbale reaksjoner er eksempel på noe vi ikke får med. Det kan også argumenteres for at ved å ha et utvalg på tre offiserer får

man ikke et stort nok representativt grunnlag til å kunne danne fakta eller ved å stille litt andre spørsmål kunne en fått andre svar som kanskje kunne endret utfall av oppgaven.

Under utførelsen av intervjuene var vi alle tre til stede, samt at alle tre analyserte intervju etter transkripsjon. Vi var klar over vi kunne miste en del informasjon ved å gjøre det over telefon, og derfor var vi ekstra påpasselige med å lytte etter endringer i tonefall, da vi mener dette kan være indikasjoner på hvordan folk oppfatter spørsmål.

4 Presentering av funn

I dette kapittelet skal vi presentere de viktigste funnene på vår analyse av de kvalitative forskningsintervjuene. Funnene vil bli presentert etter de ulike kategoriene brukt i analysen.

4.1 Offiserer

For å finne ut hvordan kompetansen er blant norske dekksoffiserer innenfor cybersikkerhet, behøvde vi et innblikk i hvilken kunnskap intervjupersonene satt inne med om retningslinjer, systemer om bord og hvordan de forholder seg til det i det daglige. Tematiseringen av intervjuene ble utarbeidet med tanke på dette, og ble delt inn i følgende kategorier: kunnskap, bevisstgjøring om bord og system, prosedyrer og tiltak.

Offiserene blir referert til som følgende, med erfaring i parentes: O1(2år), O2 (30år) og O3 (40år)

4.1.1 Kunnskap

Intervjuene startet med et generelt spørsmål om offiserenes forhold til cybersikkerhet for å få et innblikk i hva slags holdninger offiserene hadde til temaet, og om de hadde noe kunnskap om emnet. Vi forventet få svar som bar preg av likhet, da dette var et ganske åpent og lite konkret spørsmål.

O1 sa at hos dem hadde de en egen designert IT-gruppe som tok seg av det meste, og det forholdet han hadde til temaet var som en bruker av datamaskiner på bro, men at alt som hadde med sikring, installering og oppdateringer ikke var hans ansvarsområde. O2 var veldig bevisst og bekymret angående temaet og ga uttrykk for at dette var en prioritet hos dem. O3 fortalte at cybersikkerhet var noe han ikke hadde noe særlig forhold til, og var klar over at det var noe han måtte passe på, men ikke noe utover det.

Videre ble offiserene spurt om de hadde opplevd noen form for cyberangrep, for å innlede til litt mer teknisk reflektering rundt temaet. Her svarte O1 at de stadig vekk får e-post i fra kontoret om at det er forsøk på angrep via phishing, og at de må opptre varsomt. O2 hadde opplevd virus på en mannskaps-PC for noen år tilbake. O3 hadde ikke opplevd noen angrep personlig eller mot fartøyet, men også han mottok til stadighet e-post fra ledelsen på land hvor de informerte om forsøk på svindel som var blitt fanget opp av rederiet.

Ved utarbeidelse av intervjuguiden stilte vi oss spørsmålet om hvilket kunnskapsnivå vi kunne forvente at intervjupersonene hadde om maritim cybersikkerhet. Ut fra svarene på

spørsmålene som krever litt refleksjon og systemforståelse, utviste alle intervjupersonene en viss form for kunnskap. De hadde ikke forståelse for systemene på et datateknisk nivå, men generell kunnskap om hva som er viktig i forhold til maritim cybersikkerhet.

4.1.2 Bevisstgjøring om bord

På spørsmål om hvordan mannskapet blir orientert om nettverkssikkerhet var det ingen som svarte at de hadde aktivt orienterte mannskapet, men en fellesnevner var at alle offiserene på et eller annet tidspunkt hadde gjennomført en CBT (computer based training) om bord som var blitt pålagt av rederiet.

Det kom frem i intervjuet at de alle kunne ønske seg mer kursing som ikke foregår via en PC-skjerm, men hvor de aktivt kan delta i undervisningen og stille spørsmål underveis, for eksempel et landbasert kurs. Det ble gitt uttrykk for at et CBT-kurs ombord ikke var like hensiktsmessig som et landbasert kurs da det alltid var en stressfaktor til stede når de var på jobb, i form av at det alltid er noe de skal rekke eller være klar for, og at dette da ikke nødvendigvis var et gunstig miljø for læring.

4.1.3 System, prosedyrer og tiltak

Komponenter som er koblet til nettet kan være uoversiktlig, så i et forsøk på å definere offiserenes inngående kjennskap til det generelle systemet om bord, spurte vi dem om de visste hvilke komponenter som er tilkoblet internett på bro. O1 svarte at det ikke var veldig lett å ha oversikt over systemene, men mente at alle datamaskinene på bro var tilkoblet internett. O2 fortalte at siden det er nettverk om bord så er det ganske mye som er koblet til, men at på broen var det ikke så mye som var koblet til. Han forteller også at de har tilgangskontroll på USB-innganger. O3 påpekte at det bare er bro-PC som er tilkoblet internett, resten er tilkoblet innad i skipet.

Siden det er viktig at offiserene er klar over mulige sårbarheter ved systemene om bord, ble de spurt om de var klar over hvem som har tilgang til nettverket som den operasjonelle teknologien er koblet til. O1 fortalte at det kun var den designerte IT-gruppen som har tilgang til det, og at de selv ikke kunne utføre noen handlinger på det nettverket. O2 derimot svarte at alle offiserene hadde tilgang til nettverket, men at også øvrige mannskap kan få tilgang når de skal føre inn hviletid. Mannskapet er da under oppsyn. Han nevner også at det er forbud mot å koble til usertifiserte USB-stikker. O3 sa at det kun er offiserene som har tilgang til den operasjonelle teknologien på bro, og at det er et hierarki om bord som hindrer øvrige mannskap i å kunne få tilgang.

BIMCO et al (2019) sier at cyberrisikostyring bør være en viktig del av sikkerheten og sikkerhetskulturen, og bør håndteres på alle nivåer i selskapet. Vi spurte derfor om offiseren kunne fortelle oss om hvilke tiltak og prosedyrer som er innført mot cyberangrep. O1 var usikker på dette, men påpekte igjen at IT-gruppen tar seg av slikt. Han sier også at passord blir oppdatert hver 2. måned, samt hver gang en nyansatt offiser kommer om bord, men siden de er et stort team på broen har alle rollene sin egen designerte arbeidsstasjon som de deler med kollega av samme stilling. Han nevner også at mannskap har sitt nett, gjestene har sitt, og så er de operasjonelle systemene separat. O2 svarer at det å begrense bruken og tilgangen til mannskapet om bord er et tiltak, og sier videre at ingenting skal installeres på PC-ene uten godkjenning. Det skal bli gjort av IT-gruppen på land. Han sier også at han selv er opptatt av å bytte passord og mener det ikke er retningslinjer eller prosedyrer fra rederiet angående passordbytte. O3 forteller at rederiet har et innleid firma som tar seg av det meste, slik at man ikke kan gjøre endringer uten at det godkjennes. Han nevner videre at mannskapet har et eget nettverk de kan bruke til private formål som er separat fra båtens operasjonelle system, men at det er sperre på enkelte nettsider.

Mot slutten av intervjuet åpnet det opp for egen tolkning og reflektering. For å få høre hva offiserene faktisk tenkte og følte rundt temaet ble de bedt om å fortelle hva slags tiltak de selv kunne ha tenkt seg når det gjelder maritim cybersikkerhet. Det ble her nevnt at det var ønskelig med mer passordbruk, da de kunne se for seg at mulighetene for uvedkommende å ha tid alene med PC-er på bro ved landligge var for store til å ikke bli tatt på alvor. Det ble derimot ikke nevnt noe systemteknisk under denne reflekteringen, som kan være en pekepinn på at offiserene ikke hadde noe inngående systemforståelse for IT- og OT-systemene.

4.2 Penetrasjonstestere

For å kunne bidra med fremtidig kunnskapsløft, samt få en bredere forståelse av holdningene som offiserene har til temaet, trengte vi aktuelle svar fra personer som jobber med cybersikkerhet innenfor maritim sektor. Svarene vi fikk i intervjuet ble kategorisert med tanke på dette, og ble delt inn i følgende: trusler og konsekvens, segregering og sikring, bevisstgjøring og trening, samt utdaterte programvarer.

Penetrasjonstesterene blir referert til som følgende: P1, P2

4.2.1 Trusler og konsekvens

Vi spurte penetrasjonstesterene om hvordan de opplevde cybersikkerheten om bord fartøy i dag, og fikk vite at både P1 og P2 var samstemte i at cybersikkerheten om bord i skip generelt sett var for dårlig. En av penetrasjonstesterene ga uttrykk for at det var bedring, men at det går sent, og påpeker videre at dårlig sikkerhet vil naturligvis føre til større sannsynlighet for at angrep lykkes.

Da de ble spurt om det var noen trusler mot IT-systemene som var mer utbredt enn andre svarte begge to at den vanligste formen for angrep var med metoden phishing, og da ofte akkompagnert av en ransomware. Videre ble vi fortalt at phishing veldig ofte ikke var tilsiktet et fartøy eller et rederi, men ble sendt ut til så mange som mulig ved hjelp av et automatisert program. Grunnen til dette var ifølge P2: «Det er det letteste å gjøre, og det som gir mest penger med minst mulig innsats». P1 forteller at målrettede angrep også kan forekomme, og at angrepene mot maritim sektor kan være alt i fra kriminelle til statlige aktører.

På spørsmål om mannskapets private enheter kunne utgjøre en trussel, var det konsensus om at mobiltelefoner i dag var ganske sikre, men at de absolutt ikke måtte lades rett i en PC på bro. Dette for at dersom mobiltelefonen eksempelvis var koblet til nett, så var bro-PC nå også koblet til nett og hvis denne tok inn en skadevare eller var infisert med en programvare som ikke var bra, så ville dette spre seg til bro-PC.

Vi ble også fortalt at private bærbare PC-er var å betrakte som en sikkerhetstrussel. Eksemplet som ble vist til var som følger; dersom denne PC-en var blitt infisert med noe når en var hjemme og man uvitende om dette tok med seg denne ombord og plugget den i et nettverk hvor kritiske systemer også var koblet til så kunne dette spre seg til disse systemene.

Vi spurte videre om hvilke tenkelige scenarioer som kunne utspille seg dersom et skip ble angrepet. Her ble det sagt av både P1 og P2 at konsekvensene av et angrep vil være avhengig av tiltak man har på plass før skaden er skjedd, da spesielt segregering. Men at det i verste fall kunne bety at de kom seg så langt inn i systemene at broen gikk i svart, at navigasjon og kommunikasjon ble tatt ned, som er fullt mulig for en angriper å gjøre ifølge P1: «Du kan stenge ned alt hvis du vil, hvis du har et reelt stort angrep».

4.2.2 Segregering og sikring

Penetrasjonstesterene ble spurt om hvilke tiltak som kunne bli iverksatt for å sikre skip online. Det som ble nevnt hyppigst var viktigheten av å segmentere nettverk. P1 forklarte at det ikke bare er viktig med segregering inn til kritiske system, men også at det segmenteres fra skip og inn til kontorene, og fra kontorene ut til skip. P2 påpekte også hvor viktig det var med et segmentert gjestenett. De var begge spesielt opptatt av å få frem skadebegrensningen som kan oppnås ved å ha segregering under et angrep. P2 forklarte at hvor langt en angriper kan komme seg inn i systemene om bord, beror i stor grad på hvor god segregering som er opprettet i forkant.

Sett bort i fra segregering ble det også lagt stor vekt på passordbruk og oppdatering. P1 mente på at «hovedproblemet er at det blir brukt veldig mye dårlige passord» og sa at en mulig årsak til dette er at det ofte ikke er hver enkelt bruker om bord som har sitt personlige passord, men at det er rollen sin bruker, og rollen rullerer. For eksempel at styrmann har en bruker, kapteinen har en bruker osv. Det kan resultere i at man tar i bruk passord som er lette å bruke for flere. P1 sa videre at «Det går mye fortere å knekke et passord hvis det er et dårligere passord» og nevner at «en passfrase på 20 små bokstaver kan være lettere for en bruker å huske og vil være vanskeligere å knekke enn et passord på 8 tilfeldige tegn»

Viktigheten av å ta sikkerhetskopier for å sikre seg ble også nevnt her. For å sette det i perspektiv fortalte P2 oss at: «da Maersk ble angrepet i 2017, så hadde de ikke sikkerhetskopi. Hell i uhell hadde de en server som ikke var koblet til strøm og var offline under angrepet, dette var de ikke klar over selv engang. Denne serveren endte opp med å være sikkerhetskopien til Maersk»

4.2.3 Bevisstgjøring og trening

Som videre svar på vår leting etter tiltak for sikring ble bevisstgjøring brakt frem som noe av det aller enkleste og viktigste som kan gjøres. Det ble også sagt at bevisstgjøring var begynt å bli ganske allment utbredt, da mange rederi allerede hadde startet med å informere/kurse mannskap om nettsikkerhet ved å sende ut infoskriv og e-læringskurs. Vi fikk vite at på den ene siden var de glad for at de ulike selskapene hadde begynt å bevisstgjøre mannskap, men på den andre siden så ble det ikke gjort nok, da det for eksempel svært sjeldent forekom noen form for praktiske øvelser.

Videre da vi spurte om tiltak for å sikre skip online fikk vi vite at de mente noe av det beste man kunne gjøre var å kjøre phishing-kampanjer, hvor det leies inn eksterne konsulentfirma

for å gjøre dette. P2 var spesielt opptatt av viktigheten praktiske øvelser har, hvor mannskapet selv får kjenne på hvordan det er å få tilsendt noe i e-posten som de ikke er klar over kommer og at man får se hvordan det håndteres. Dette kan da spores videre og trening kan bli mer skreddersydd for enkeltindivider. Formålet med dette vil være å få folk til å begynne å tenke seg ekstra nøye om, da de selv har erfart hvordan angrepene foregår.

P2 informerte oss også om at i olje og gassektoren pleide de å kjøre en del cyberøvelser, men at dette ikke hadde kommet helt til maritim sektor enda. "Dette er som en brannøvelse, bare med cyber". I en slik øvelse får man beskjed om at man er under angrep. Ingen får røre PC og folk har heller ikke hverandre sine telefonnummer. Hensikten med en slik øvelse vil være å se hvor gode prosedyrene er ombord ved et eventuelt angrep.

4.2.4 Utdaterte programvarer

Det ble også stilt spørsmål om penetrasjonstesterene hadde sett noen svakheter som gikk igjen om bord i fartøy. Det ble som tidligere nevnt sagt dårlig segregering av nettverk, svake passord og slurv med oppdateringer, men det ble også fortalt at de hadde sett mye utdaterte system som Windows XP og Windows 7. Disse skal ikke oppdateres fra leverandørens side lenger og vil da bli veldig sårbare. Det ble også ytret ønske om at man skulle begynne å behandle cybersikkerhet i et sikkerhetsperspektiv og ikke "sånn som IT-avdelingen driver med". Da særlig med tanke på planlegging og bygging av nye fartøy.

Det ble fortalt at det har vært vanlig å kjøpe kontrollsystem helt i startfasen, som gjør at når skipet var ferdigstilt og klar for å seile så var kontrollsystemet allerede 4-5 år. Dette fordi oppdateringene var gjort ved byggestart og ikke når skipet var klart til å seile. Vi ble opplyst om at dette medførte at det ikke var mulig å oppdatere flere datamaskiner som drev ulike kontrollsystem, da programvarene var blitt så utdaterte at de ikke lenger var kompatibel med nyere maskinvare. Noe som igjen medførte at man må få bukt med forskjellige svakheter ved hjelp av ulike brannmurer, segregering og prosedyrer, i stedet for å kunne løse problemet med å oppdatere programvare.

5 Drøfting

Ved å intervjue tre seilende offiserer og to penetrasjonstestere med erfaring som sikkerhetskonsulenter, var hensikten å belyse problemstillingen som er beskrevet i kapittel 3.

I denne delen skal det som ble presentert i forrige kapittel, drøftes opp mot teori og våre egne refleksjoner. Ved å koble sammen kategoriene fra analysen, ønsker vi å se på ulike årsakssammenhenger som kan fortelle oss hvilket kunnskapsnivå offiserene har angående cybersikkerhet, og hva som kan gjøres for å imøtekomme IMOs krav innen 2021.

5.1 Ansvar krever kompetanse

Under intervjuene med penetrasjonstesterene kom det frem hvor viktig det var å bevisstgjøre mannskap om risikoen ved bruk av cybernett og informasjonsteknologi. At det var særdeles viktig å være klar over farene slik at preventive tiltak kunne bli satt i gang i hele organisasjonen om bord. Etter intervjuet med offiserene satt vi igjen med et inntrykk av at rederiene hadde startet med å informere mannskap gjennom nettbaserte kursmoduler og brosjyrer de var blitt tilsendt. Dette tolker vi som at fokuset mot denne risikoen øker og at det eksisterer et ønske om å få satt i gang tiltak for å øke kunnskapen blant offiserene utover det som «Ola Nordmann» besitter. Like fullt ble det presisert for oss av penetrasjonstesterene at å bare informere og la det være med dette, var på langt nær godt nok, da dette ikke er en særlig effektiv metode for å få med alle. Det kan argumenteres for at ved å for eksempel dele ut informasjon gjennom brosjyrer og nettbaserte kurs vil bare de mest ivrige og gjerne de som har litt datainteresse fra før sette seg inn i dette.

I cybersikkerhet finnes det et uttrykk: «et forsvar i dybden» som illustreres ved at det finnes et lag av barrierer som må brytes ned for at et angrep skal være vellykket (Forcepoint, 2018). Skal man oppnå en sikring med flere lag som må penetreres for at et angrep skal være vellykket, er det kritisk at alle som håndterer teknologi knyttet til cybernett er klar over trusler som kan forekomme. De må også vite hva de skal gjøre dersom et angrep forekommer da de ofte vil være det første ledd som må knekkes for å komme seg inn på systemene. På bakgrunn av dette kan det argumenteres for at det ikke er holdbart med å bare informere, det burde også trenes på slike situasjoner.

Da offiserene ble spurt om hvorvidt de visste hvilke komponenter på bro som var tilkoblet internett kunne alle svare etter litt betenkningstid, men det ble gitt uttrykk for at det var

vanskelig å ha oversikt over alle systemene, hvor de var koblet til og hvorfor. På bakgrunn av dette kan det tenkes at det hadde vært hensiktsmessig med en plansje over koblingene til systemene, en plansje som kartla hvor alle system hentet info fra, samt sendte info til. Dette for å gjøre det enklere for offiserer å holde kontroll på hvilke system som er koblet til hva, samt for å bidra til enklere risikovurdering og risikostyring.

5.1.1 Øvelser

Da offiserene ble spurt om hvilket forhold de hadde til cybersikkerhet var det bare en av dem som ga uttrykk for at dette var noe han var bekymret for med tanke på konsekvensene dette kunne medføre. De andre svarte at de hadde fått e-post fra rederiet hvis rederiet hadde vært utsatt for angrep, for å informere om trusselen, og ga også uttrykk for at dette var noen andre sitt ansvar. De sa også at de ikke hadde han noe førstehånds erfaring med dette selv. Det kan tenkes at nettopp en slik erfaring på kloss hold ville økt offiserens bevissthet rundt temaet, samt øke villighet til å utføre øvelser mot cybersikkerhet. En kan argumentere for at dersom en person ikke har sett/opplevd noe på kloss hold, så vil det være vanskelig å få et ordentlig forhold til dette.

På den ene siden kan det argumenteres for at å pålegge folk øvelser mot cyberangrep, kan virke litt mot sin hensikt dersom de ikke har et skikkelig forhold til dette. Øvelsene kan bli utført halvhjertet på bare noen få minutter for at de skal kunne kvittere ut på utført øvelse, og det kan bli sett på mer som en byrde enn som det viktige preventive tiltaket det kan være.

På den andre siden kan det hevdes at om man virkelig skal øke bevisstheten rundt temaet kan det være lurt å leie inn eksterne selskap for å kjøre eksempelvis phishingkampanjer om bord. P2 fortalte oss at dersom mannskapet om bord i et fartøy skal få et skikkelig forhold til dette så må de nesten få «kjenne det på kroppen» hvordan det er å få noe i e-posten som de ikke er klar over skal komme, men som gjør skade dersom de trykker på koblingen. Det kan for eksempel være en uskyldig e-post kamuflert som rederiet, men som gir angripere kontroll over datamaskinen dersom man trykker på linken vedlagt. Dette underbygger også BIMCO et.al (2018) hvor de sier det er viktig at relevant personell utfører cybersikkerhetsøvelser på jevnlig basis for å kunne respondere effektivt dersom et angrep skulle forekomme.

Blant tiltakene for å sikre skip online fortalte penetrasjonstesterene at phishingkampanjer var noe av det som hang høyest hos dem. Dette ble lagt frem som særdeles effektivt, da dette ville være en form for praktisk øvelse. Ingen av de intervjuede offiserene fortalte oss at de

hadde hatt noe som kunne minne om dette. Særlig P2 presiserte for oss viktigheten av å ha praktiske treninger på dette området, og trakk frem eksempel fra olje og gass sektoren hvor de pleide å kjøre "cyber drills". Dette ble uansett ikke nevnt blant offiserene, og den eneste formen for trening vi ble fortalt de hadde fått var enten databaserte kurs eller å ha fått utlevert infoskriv. Så sant man kan definere dette som trening.

I ISM-koden Del A, punkt 1.2.2.2-1.2.2.3 (2014) står det at et selskaps mål skal være å identifisere alle risikoer for skip, personell og miljø, samt at de stadig skal forbedre ferdighetene til personell ombord med hensyn til sikkerhetsstyring, herunder forberedelse på nødsituasjoner som omfatter sikkerhet og miljøvern. Tatt i betraktning at ytterste konsekvens av et cyberangrep kan være at angripere får tilgang til operasjonell teknologi, og kan overstyre systemer som er kritiske for driften av skipet, kan man kategorisere risikoen et cyberangrep utgjør for særs stor. Sett fra et sikkerhetsperspektiv kan man derfor argumentere for at en slik trussel burde få tilsvarende oppmerksomhet som andre trusler som utgjør en fare for sikker navigering og generelt drift av skipet.

Videre kan man se til ISM-kodens punkt 8 hvor det står skrevet at et selskap skal identifisere mulige nødsituasjoner og innføre fremgangsmåter for å reagere på dem. Det står også at selskapet skal opprette programmer for trening og øvelser i å forberede seg på handling i nødssituasjoner (Forskrift om sikkerhetsstyringssystem for skip m.m., 2014).

Det kan argumenteres for at cybersikkerhet er et relativt nytt tema i den maritime bransjen og at det ikke har vært nødvendig med fokus på det enda. IMO har også som kjent sagt at fristen for deres oppfordring for implementering av tiltak i SMS er 01.01.2021, så på den ene siden kan det hevdes at en ledelse som ikke har presset på for å få lært opp mannskap og som ikke har presset på for at det skal avholdes øvelser bare har "handlet i tiden" og ikke gjort noe mindre preventivt enn mange andre i lignende situasjoner. Uansett står det klart i ISM-koden hvilke tiltak som er forventet av et selskap dersom man oppdager nye trusler, og tatt i betraktning at ingen av de intervjuede offiserene kunne vise til noe praktisk trening, kan man anta at forbedringspotensialet fremdeles er til stede blant norske rederi og på norske fartøy.

Viktigheten av øvelser burde ikke undervurderes, likevel er dette tiltak for å vedlikeholde allerede tillært kunnskap. Derfor kan det hevdes at første prioritet for rederi burde være å få kurset mannskap, og da gjerne holde landbaserte kurs slik det ble ytret ønske om fra offiserer

under våre intervju. Det ble fortalt at de så CBT-kurs som lite hensiktsmessige, da det var noe som ofte ble skummet gjennom, da man gjerne hadde andre oppgaver i tillegg, samt at man ikke satt i gruppe og fikk diskutere tanker med andre deltakere og foredragsholdere, slik man gjør på et landbasert kurs. For en kan hevde at nettopp det å lære et mannskap hvordan angripere opererer er nøkkelen til å kunne beskytte seg mot trusler.

5.2 Rutiner

Som vi nevnte i teorikapittelet så vil menneskelig feil være en av faktorene til et vellykket cyberangrep, og videre stod det også at med enkle tiltak kunne de fleste saker vært unngått. Slike enkle tiltak kan da være gode rutiner. Rutinene som går oftest igjen blant penetrasjonstesterene og i teoridelen er passord og oppdatering, samt opplæring og trening som er nevnt over.

Viktigheten av å ha gode passord har vi dokumentert både under teori og funn. Likevel er det kun en av offiserene som nevner at det finnes rutiner i rederiet på bytte av passord. Samtidig sier offiserene at de er opptatt av å bytte passord og ønsker mer passordbruk ettersom de forstår konsekvensene om uvedkommende får tilgang til PC-en. På tross av dette sier en av penetrasjonstesterene at dårlige passord er hovedproblemet som angår cybersikkerhet på skip. Ut ifra funnene oppfattes offiserene positive til å måtte bruke mer tid på å bytte og lage gode passord. Likevel er erfaringen fra penetrasjonstesterene at bruken av passord på skip er for dårlig, ettersom det heller blir brukt passord som er lette å huske.

Patching eller oppdatering av programvare har vi tidligere skrevet at er viktig med tanke på å tette sikkerhetshull. Offiserene hadde lite å komme med her annet enn at O1 sa at IT-gruppen om bord tok seg av slikt og O3 nevnte at de hadde et innleid firma som tok seg av det meste. En kan håpe på at de rederiene med et dedikert IT-team om bord eller som har tatt seg bryet med å utkontraktere en IT-avdeling ikke vil slurve når det kommer til oppdateringer. For andre rederier derimot sier penetrasjonstesterene at det er en del utdaterte systemer på norske fartøy, inkludert operativsystem som ikke lenger blir oppdatert.

5.2.1 Passordbruk

Fra penetrasjonstesterene ble det vist til at et stort problem var at det fantes veldig mye dårlige passord, P1 gikk så langt som å kalle dette for et hovedproblem. Samtidig så fikk vi antydninger fra offiserer om at noen syntes "Det begynte å gå litt langt" og at det kunne være en plage. Skal et "forsvar i dybden" bli en realitet er det viktig at ingen sluntrer unna, og da spesielt på passordbruk. Imidlertid er det en fare for at brukere av et system som ber

deg om å bytte passord hver 6. uke, til slutt kommer til å synes det blir travelt, så vil de søke mot minste motstands vei. Det vil i slike tilfeller resultere i mye korte og dårlige passord, fordi de er lette å huske på.

På den ene siden er det viktig at passord er så sikre som mulig. Ofte vil man av få beskjed fra et system om at et passord burde være minst 6-8 tegn og ha en blanding av små og store bokstaver + spesialtegn. Nätt & Heide (2015, s. 89) hevder at om man klarer å lage et passord med tilfeldige bokstaver og spesialtegn og med en lengde på 8, vil kombinasjonene gjøre at det tar cirka 2287 år å knekke passordet dersom man forsøker med 100 000 forsøk pr. sekund. Nätt og Heide (2015) skriver videre at med nyere grafikkort og kraftigere prosessorer er det lett å oppnå over 10 millioner forsøk pr. sekund. Dette vil senke tiden på å knekke et passord betydelig.

På den andre siden vil det virke mot sin hensikt å endre passord ofte dersom folk ender opp med å ta snarveier og lage enkle passord fordi de ikke klarer å huske nye avanserte passord som de må lage nye av flere ganger i året. P1 la vekt på at «et passord på 20 bokstaver med kun små bokstaver er bedre enn et på 8 bokstaver som er helt tilfeldige». P2 svarte likt under sitt intervju og sa at «et passord på 20 tegn, der mellomrom er et godkjent tegn, vil teoretisk sett være umulig å knekke. Forståelig nok så vil det være lettere for folk å huske passfraser bestående av bare små bokstaver, en det vil være å huske tegn og tall i en helt tilfeldig rekkefølge.

5.2.2 Teknisk sikring

Da vi stilte penetrasjonstesterene spørsmål om hvilke tiltak som var best for å hindre angrep og spredningen av et angrep ble segregering brakt frem som det mest effektive. Også i teoridelen beskrives det viktigheten av et godt segmentert nettverk og hvordan det kan begrense konsekvensen av et angrep. I tillegg til segregering finnes det andre viktige former for sikring; skadevarebeskyttelse, brukertilgang og oppdateringssystem.

Offiserene hadde lite å komme med her, likevel kan det argumenteres for at det sjelden er offiserene som setter opp datanettverket og segregeringen, da dette ofte er innleide konsulenter. Samtidig kan kunnskap om temaet gjøre det lettere å verifisere kvaliteten av segregeringen og sikkerheten på nettverket. Det som kan være uheldig er om det utvikler seg en kultur hvor offiserene rett og slett ikke tar trusselen på alvor på grunn av manglende forståelse for trusselen. Dette baserer vi på intervjuene vi har gjennomført hvor vi ser muligheter for at det noen steder kan utvikle seg en kultur hvor offiserene ikke tar trusselen

på alvor. Dette mener vi kan forhindres dersom rederiene for eksempel leier inn konsulentfirmaer for å bevisstgjøre og kurse mannskapet.

5.3 Systemet om bord

Fra våre intervju med penetrasjonstesterene kom det frem at de anså det som svært viktig at hele organisasjonen begynte å se cybersikkerhet i et sikkerhetsperspektiv. Altså at man måtte behandle temaet på lik linje som andre sikkerhetstrusler som utgjør en stor risiko for fartøyet, og ikke noe som "IT-avdelingen driver med". Hos en av de intervjuede offiserene ble det uttrykt skepsis til hvorvidt trusselen virkelig var så reell som vi skulle ha det til, og at "ting var begynt å gå litt langt". Det ble altså gitt uttrykk for at offiseren synes systemdesign og preventive tiltak ble for tungvint i forhold til hvor kritisk han anså situasjonen til å være.

Skal en lykkes med å få en hel organisasjon til å jobbe sammen for å best mulig sikring, kan det argumenteres for at den drivende kraften for å skulle gjennomføre dette burde komme fra den øverste delen av organisasjonshierarkiet. For det er nettopp dette BIMCO et al. (2018) sier; cyberrisikostyring burde starte på et ledelsesnivå, i stedet for å bli delegert videre til en IT-avdeling eller skipssikkerhetsoffiser (SSO).

Det burde da fra ledelsen av rederiet settes fokus på sikring av systemene om bord helt i fra planleggingsfasen av nye skip til flåten. Ser man til våre intervju med penetrasjonstesterene kommer det frem at kanskje den største og mest hyppige svakheten som går igjen, er hvor penetrasjonstesterene har vært på testing og systemene har vært utdaterte. Og i mange tilfeller programvaresystem som ikke lar seg oppdatere lenger, som har kjente sikkerhetshull og ikke lenger er kompatibelt med nyere maskinvare.

På den ene siden kan det argumenteres for at når rederiet bestilte nybygget for 10 år siden med tilhørende programvare-pakke, så var de ikke klar over at for eksempel Windows ville slutte å oppdatere systemet bare noen år senere. På den andre siden så kan en se til historikken til programvaresystem og argumentere for at levetiden ikke har vært i nærheten av levetiden for et fartøy noensinne, og at man derfor i planleggingsfasen av nybygg kanskje burde prøve å legge opp til at systemer kan byttes ut relativt enkelt og uten for store utskiftninger av vitale deler i fartøyet når den tid kommer.

5.4 Oppsummering

Hensikten med dette studiet har vært å få et innblikk i kompetansenivået til norske dekksoffiserer når det kommer til cybersikkerhet, samt forsøke å kartlegge hva som kan bli

gjort for å komme á jour med IMO sin oppfordring om implementering av cybersikkerhet i sikkerhetsstyringssystemer før 01.01.2021. Dette har blitt gjort ved hjelp av kvalitative forskningsintervjuer som baserte seg på fagfolk sine erfaringer og kunnskap.

ISM-koden legger vekt på at et selskaps mål skal være å identifisere risikoer og forbedre ferdighetene til mannskapet med hensyn til sikkerhetsstyring. Når det er sagt kan vår studie tyde på at risikoen et cyberangrep utgjør ikke er innforstått alle plasser.

Begge penetrasjonstesterene fortalte at cybersikkerheten om bord i fartøy i dag er for dårlig. Uten tilstrekkelig opplæring og kursing kan det være vanskelig å bedre cybersikkerheten. Vår studie viser at det forekommer lite kursing i cybersikkerhet, og at det er ønskelig med landbasert kursing, og ikke CBT. Lykkes man med å øke kunnskapsnivået og bevisstgjøre mannskapet vil det kunne føre til en jevnere fordeling av ansvaret for cybersikkerheten om bord, som vil gjøre organisasjonen bedre rustet for å møte et angrep.

Videre kan vi se at viktigheten av øvelser vektlegges som et preventivt tiltak, samt for å vedlikeholde kunnskap. Øvelser vil gjøre at mannskapet får testet prosedyrene sine og får kjenne på hvordan det er når for eksempel deler av systemer blir lammet av et angrep. Ikke desto mindre ser det ut til at cyberøvelser nesten ikke eksisterer om bord i fartøy i dag.

Vi har også sett at god teknisk planlegging er essensielt når det kommer til å kunne vedlikeholde systemer ombord. Blant de enkleste tiltakene for å sikre seg mot angrep er å oppdatere programvare for å tette kjente sikkerhetshull, men dette hjelper ikke om systemet er utgått og ikke støttes av produsenten lenger.

6 Avslutning

Avslutningsvis vil vi med alt tatt i betraktning, og med et mål om å finne gode løsninger for å komme á jour med IMO sin oppfordring, få presisere det som ble sagt av penetrasjonstesterene: "Første bud er bevisstgjøring". Videre burde det kurses, og da gjerne på land for å optimalisere læreforhold. Til slutt burde det trenes i form av ombordbaserte øvelser, slik at organisasjonen står best mulig rustet for potensielle angrep.

Som en hjelpende hånd og for å få startet med bevisstgjøring har vi på bakgrunn av oppgaven utarbeidet en plakat med fem punkter som kan henges opp om bord. Denne plakaten ble laget med moduler og verktøy fra nettsiden designcap.com. Punktene i plakaten tar utgangspunkt i nøkkelelement som kan hentes ut fra teorien og drøftingen som er presentert, og med den hensikt å bevisstgjøre et mannskap. Plakaten kan sees i sin helhet i vedlegg 5.

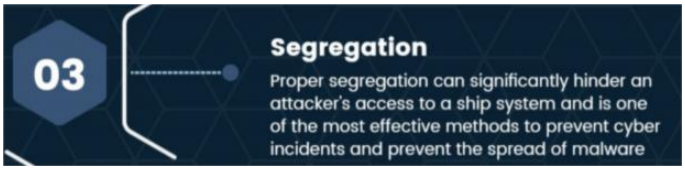
Første punkt omhandler passord, og tips til hvordan et passord kan lages i henhold til det som har blitt presentert.

Figur 1 Bevisstgjøringsplakat - punkt 1. Passord

Det andre punktet forteller om oppdatering av programvarer samt kort om hvorfor man bør passe på å oppdatere forskjellige utstyr.

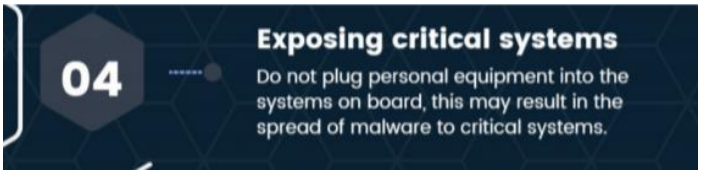
Figur 2 Bevisstgjøringsplakat - punkt 2. Oppdater programvare

Videre omhandler det tredje punktet segregering, og viktigheten av å skille de forskjellige systemene fra hverandre.



Figur 3 Bevisstgjøringsplakat - punkt 3. Segregering

Det fjerde punktet handler om å passe på at personlige enheter ikke kobles til systemene om bord, for det kan resultere i spredning av skadevare til systemene.



Figur 4 Bevisstgjøringsplakat - punkt 4. Utsette kritiske system

Til slutt handler det femte punktet om at man skal være forsiktig med hva man trykker på, da med tanke på phishing.

Figur 5 Bevisstgjøringsplakat - punkt 5. Vær forsiktig

Denne plakaten er på ingen måte perfekt, eller tilstrekkelig som et tiltak mot cybertrusler, men det kan være starten på å bevisstgjøre et mannskap om bord i et fartøy. Ved å inkludere nevnte punkter i en slik bevisstgjøringsplakat vil man rette fokuset mot elementer som kan være viktig å ta tak i innledningsvis i et bevisstgjøringsprogram.

Bibliografi

Allianz. (2019). *Safety And Shipping Review 2019.* Hentet fra https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/AGCS-Safety-Shipping-Review-2019.pdf

BIMCO, CLIA, ICS, Intercargo, Intermanager, Intertanko, (...) World shipping council. (2018). *The Guidelines on Cyber Security Onboard Ships*. Hentet fra https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

BIMCO, ICS, Witherby. (2019). *Cyber Security Workbook for On Board Ship Use* (1. utg.). Witherby Seamanship International.

Daler, T., Gulbrandsen, R., Høie, T. A., & Sjølstad, T. (2019). *Håndbok i datasikkerhet* (4. utg.). Bergen: Fagbokforlaget.

Dalland, O. (2012). *Metode og oppgaveskriving* (5. utg.). Oslo: Gyldendal Norsk forlag.

DESIGNCAP. (u.d.). Hentet 2020 fra www.designcap.com

Forcepoint. (2018). *What is Defence in Depth?* Hentet 05 02, 2020 fra https://www.forcepoint.com/cyber-edu/defense-depth

Forskrift om sikkerhetsstyringssystem. (2008). *Forskrift om sikkerhetsstyringssystem på norske skip og flyttbare innretninger, FOR-2008-03-14-306*. Hentet fra https://lovdata.no/dokument/LTI/forskrift/2008-03-14-306

Forskrift om sikkerhetsstyringssystem for skip m.m. (2014). *Forskrift om sikkerhetsstyringssystem for norske skip og flyttbare innretninger, FOR-2014-09-05-1191*. Hentet fra https://lovdata.no/dokument/SF/forskrift/2014-09-05-1191/KAPITTEL_1#KAPITTEL_1

Future Nautics . (2018). *Crew connectivity.* Hentet fra http://www.crewconnectivity.com/?product=2018-crew-connectivity-survey-report

IMO. (2017, 08 08). *Maritime cyber risk management in safety management systems.* Hentet fra www.imo.org/en/OurWork/Security/WestAfrica/Documents/Resolution%20MSC.428(98)%20-%20Maritime%20Cyber%20Risk%20Management%20in%20Safety%20Management%20Systems.pdf#search=cyber

Johannessen, A., Tufte, P., & Christoffersen, L. (2015). *Introduksjon til samfunnsvitenskapelig metode* (4. utg.). Oslo: Abstrakt Forlag AS.

Kibar, O. (2018, 10 03). Vil beskytte skip mot digitale pirater. Hentet 02 14, 2020 fra https://www.dn.no/teknologi/cyberangrep/kongsberg-digital/hacking/vil-beskytte-skip-mot-digitale-pirater/2-1-429565

Kvale, S., & Brinkmann, S. (2017). *Det kvalitative forskningsintervju* (3. utg.). Oslo: Gyldendal Norsk Forlag.

Nasjonal Sikkerhetsmyndighet. (2018, 10 04). *Passordanbefalinger fra Nasjonal Sikkerhetsmyndighet.* Hentet fra https://www.nsm.stat.no/aktuelt/passordanbefalinger-fra-nasjonal-sikkerhetsmyndighet/

National Cyber Security Centre. (2016, 01). *Common cyber attacks: reducing the impact*. Hentet fra https://www.ncsc.gov.uk/files/common_cyber_attacks_ncsc.pdf

National Cyber Security Centre. (2019, 04 21). *Passwords, passwords everywhere.* Hentet fra https://www.ncsc.gov.uk/blog-post/passwords-passwords-everywhere

Nätt, T. H., & Heide, C. F. (2015). *Datasikkerhet; ikke bli svindlerens neste offer* (1. utg.). Oslo: Gyldendal akademisk.

Rossouw Von Solms, J. (2013, 04 11). *From information security to cyber security*. Hentet fra https://www.sciencedirect.com/journal/computers-and-security

SAFETY4SEA. (2018, 05 31). Maersk Line: Surviving from a cyber attack. Hentet 05 08, 2020 fra https://safety4sea.com/cm-maersk-line-surviving-from-a-cyber-attack

Vedlegg

Vedlegg 1 – Intervjuguide Offiserer

Hva vi ønsker å vite noe om	Forslag til spørsmål (Intervjuguide)
Informasjon før opptak	Si litt om temaet for samtalen (bakgrunn, formål) Forklar hva intervjuet skal brukes til, og forklar taushetsplikt og anonymitet Spør om noe er uklart og om intervjupersonen har noen spørsmål Informer, få samtykke til og start opptak
Personalia	Utdanning Års erfaring på sjøen Nåværende stilling
Generelt	Hva er ditt forhold til cybersikkerhet? Har du opplevd noen form for cyberangrep? Hvis ja: Hvor, når, hvordan ble det håndtert, hvor mange, omfang/konsekvens
Opplæring	Hvordan briefer dere mannskapet om nettverkssikkerhet?
Kunnskap	Har du fått kursing i cybersikkerhet? Hvis ja: nyttig? Hvis nei: er det ønskelig? Hvilke komponenter er koblet til internett? Kan du si noe om hvem som har tilgang til nettverket som OT er koblet til?
Rutiner	Hvilke tiltak/prosedyrer er innført mot cyberangrep? Hva slags tester/øvelser blir utført med hensyn på cybersikkerhet? Blir passord jevnlig oppdatert? Har dere restriksjoner på mannskapets tilkoblingsmuligheter? Om du kunne valgt; hva slags tiltak kunne du tenkt deg? Forslag

Oppsummering	Er det noe du er spesielt opptatt av i forhold til det vi har snakket om? Hvorfor er dette viktig? Hva kan/burde gjøres? Oppsummere hva som er gjennomgått Har jeg forstått deg riktig? Er det noe du vil tilføye?

Vedlegg 2 – Intervjuguide Penetrasjonstestere

Hva jeg ønsker å vite noe om	Forslag til spørsmål (Intervjuguide)
Informasjon før opptak	Si litt om temaet for samtalen (bakgrunn, formål) Forklar hva intervjuet skal brukes til, og forklar taushetsplikt og anonymitet Spør om noe er uklart og om intervjupersonen har noen spørsmål Informer, få samtykke til og start opptak
Personalia	Utdanning Nåværende stilling
Trusler	Hvordan opplever du den maritime cybersikkerheten i dag? Hvilke interne/eksterne trusler mot IT-systemet finnes det? Hvordan har trusselbildet rundt cyberangrep på maritime systemer endret seg de siste årene? Hvorfor kan mannskap sine personlige telefoner/datamaskiner utgjøre en trussel ved å være tilkoblet nettverk om bord?
Systemet	Basert på din erfaring: Hvordan angriper hackere? Er det noen svakheter du ser som går igjen om bord i fartøy? (Hvilke? Har du noen formening om hvorfor?) Ser du noen tiltak som kan bli iverksatt for å sikre skip online? Hvorfor øker sårbarheten til IT-systemene?

Trening	Hvilket inntrykk har du av rederi/ansattes prioritering av cybersikkerhet? Vil du tro det er sannsynlig at de fleste fartøy vil komme ajour med IMO sitt krav om gode løsninger for cybersikkerhet? (På hvilken måte burde de fleste klare det?) Rederiene burde drive god opplæring om bord i sine fartøy, hvordan tenker du at man kan trene mannskapet til å opptre varsom rundt interne system?
Når skaden har skjedd	Dersom skaden har skjedd, hvilke tiltak burde iverksettes? I ytterste konsekvens; dersom man er infiltrert og ikke er klar over det, finnes det begrensinger på hvor langt en inntrenger kan komme?
Fremtiden	Hva kan man gjøre bedre for å beskytte kritisk infrastruktur mot cyberangrep? Hvordan kan vi best lære fra cyberhendelser? På hvilken måte tror du trusselen vil endre seg fremover? Hvorfor øker sårbarheten til cybersikkerheten?
Oppsummering	Hvordan vil du definere cybersikkerhet? Er det noe du er spesielt opptatt av i forhold til det vi har snakket om? Hvorfor er dette viktig? Hva kan/burde gjøres? Oppsummere hva som er gjennomgått Har jeg forstått deg riktig? Er det noe du vil tilføye?

Vedlegg 3 – Samtykkeskjema

Vil du delta i forskningsprosjektet

"Maritim cybersikkerhet"?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å finne ut om hvordan kompetansen blant norske sjøfolk er i forhold til maritim cybersikkerhet. Dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål
Formålet med prosjektet er å beskrive kompetansen til norske sjøfolk innenfor cybersikkerhet, og drøfte hvilke tiltak som kan bli gjort for å imøtekomme IMOs krav om innføring av cyber risk management
Dette prosjektet er en bachelor skrevet ved NTNU i Ålesund.

Hvem er ansvarlig for forskningsprosjektet?
NTNU er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?
Vi trenger informasjon fra fagfolk og anser deg som en ekspert på området.

Hva innebærer det for deg å delta?
Hvis du velger å delta innebærer det å være med på et intervju hvor lydopptaket blir tatt opp og analysert for å brukes i vår oppgave. Intervjuet vil vare i 30-60 min.
Opptaket blir slettet etter sensurfrist av oppgaven vår. (utgangen av Juni)

Det er frivillig å delta
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykke tilbake uten å oppgi noen grunn. Alle opplysninger om deg vil da bli anonymisert. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger
Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

- *De som vil ha tilgang til informasjonen vi innhenter er vi tre studentene (Mathias Andersson, Sondre Ytterland og Robert Arnesen) og veileder (Marie Haugli Larsen)*
- *Personopplysninger om deg vil bli erstattet med en kode som lagres på egen navneliste adskilt fra øvrige data.*

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?
Prosjektet skal etter planen avsluttes *20.05.2020.Personopplysninger og opptak blir slettet etter sensurfrist 15.06.2020.*

Hva gir oss rett til å behandle personopplysninger om deg?
Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra *NTNU* har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter
Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke personopplysninger som er registrert om deg,
- å få rettet personopplysninger om deg,
- få slettet personopplysninger om deg,
- få utlevert en kopi av dine personopplysninger (dataportabilitet), og
- å sende klage til personvernombudet eller Datatilsynet om behandlingen av dine personopplysninger.

Hva gir oss rett til å behandle personopplysninger om deg?
Vi behandler opplysninger om deg basert på ditt samtykke.

Hvor kan jeg finne ut mer?
Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:

- *NTNU i Ålesund* ved *Marie Haugli Larsen.*
  - *marie.h.larsen@ntnu.no*
  - *Tlf* +47 450 61 300
- Vårt personvernombud: *Thomas Helgesen*
- thomas.helgesen@ntnu.no
- Tlf: 930 79 038
- NSD – Norsk senter for forskningsdata AS, på epost (personverntjenester@nsd.no) eller telefon: 55 58 21 17.

Med vennlig hilsen

Marie Haugli Larsen
Veileder

Mathias D. Andersson
Student

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *Maritim Cybersikkerhet*, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ☐ å delta i *intervju*
- ☐ *at opptaket lagres frem til 15.06.2020*

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet, ca. *15.06.2020*

(Signert av prosjektdeltaker, dato)

Vedlegg 4 – Vurdering fra NSD

NSD NORSK SENTER FOR FORSKNINGSDATA

NSD sin vurdering

Prosjekttittel

Maritim cybersikkerhet

Referansenummer

161219

Registrert

24.01.2020 av Mathias Dimmen Andersson - mathiada@stud.ntnu.no

Behandlingsansvarlig institusjon

Norges teknisk-naturvitenskapelige universitet NTNU / Fakultet for ingeniørvitenskap / Institutt for havromsoperasjoner og byggteknikk

Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)

Marie Haugli Larsen, marie.h.larsen@ntnu.no, tlf: 45061300

Type prosjekt

Studentprosjekt, bachelorstudium

Kontaktinformasjon, student

Mathias Dimmen Andersson, mathiasdimmenandersson@hotmail.com, tlf: 41364206

Prosjektperiode

09.01.2020 - 30.06.2020

Status

13.02.2020 - Vurdert

Vurdering (1)

13.02.2020 - Vurdert

Det er vår vurdering at behandlingen av personopplysninger i prosjektet vil være i samsvar med personvernlovgivningen så fremt den gjennomføres i tråd med det som er dokumentert i meldeskjemaet 13.02.2020 med vedlegg, samt i meldingsdialogen mellom innmelder og NSD. Behandlingen kan starte.

MELD VESENTLIGE ENDRINGER
Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være

nødvendig å melde dette til NSD ved å oppdatere meldeskjemaet. Før du melder inn en endring, oppfordrer vi deg til å lese om hvilke type endringer det er nødvendig å melde: https://nsd.no/personvernombud/meld_prosjekt/meld_endringer.html

Du må vente på svar fra NSD før endringen gjennomføres.

TYPE OPPLYSNINGER OG VARIGHET
Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til 30.06.2020.

LOVLIG GRUNNLAG
Prosjektet vil innhente samtykke fra de registrerte til behandlingen av personopplysninger. Vår vurdering er at prosjektet legger opp til et samtykke i samsvar med kravene i art. 4 og 7, ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse som kan dokumenteres, og som den registrerte kan trekke tilbake. Lovlig grunnlag for behandlingen vil dermed være den registrertes samtykke, jf. personvernforordningen art. 6 nr. 1 bokstav a.

PERSONVERNPRINSIPPER
NSD vurderer at den planlagte behandlingen av personopplysninger vil følge prinsippene i personvernforordningen om:

- lovlighet, rettferdighet og åpenhet (art. 5.1 a), ved at de registrerte får tilfredsstillende informasjon om og samtykker til behandlingen
- formålsbegrensning (art. 5.1 b), ved at personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke viderebehandles til nye uforenlige formål
- dataminimering (art. 5.1 c), ved at det kun behandles opplysninger som er adekvate, relevante og nødvendige for formålet med prosjektet
- lagringsbegrensning (art. 5.1 e), ved at personopplysningene ikke lagres lengre enn nødvendig for å oppfylle formålet

DE REGISTRERTES RETTIGHETER
Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: åpenhet (art. 12), informasjon (art. 13), innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18), underretning (art. 19), dataportabilitet (art. 20).

NSD vurderer at informasjonen som de registrerte vil motta oppfyller lovens krav til form og innhold, jf. art. 12.1 og art. 13.

Vi minner om at hvis en registrert tar kontakt om sine rettigheter, har behandlingsansvarlig institusjon plikt til å svare innen en måned.

FØLG DIN INSTITUSJONS RETNINGSLINJER
NSD legger til grunn at behandlingen oppfyller kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1. f) og sikkerhet (art. 32).

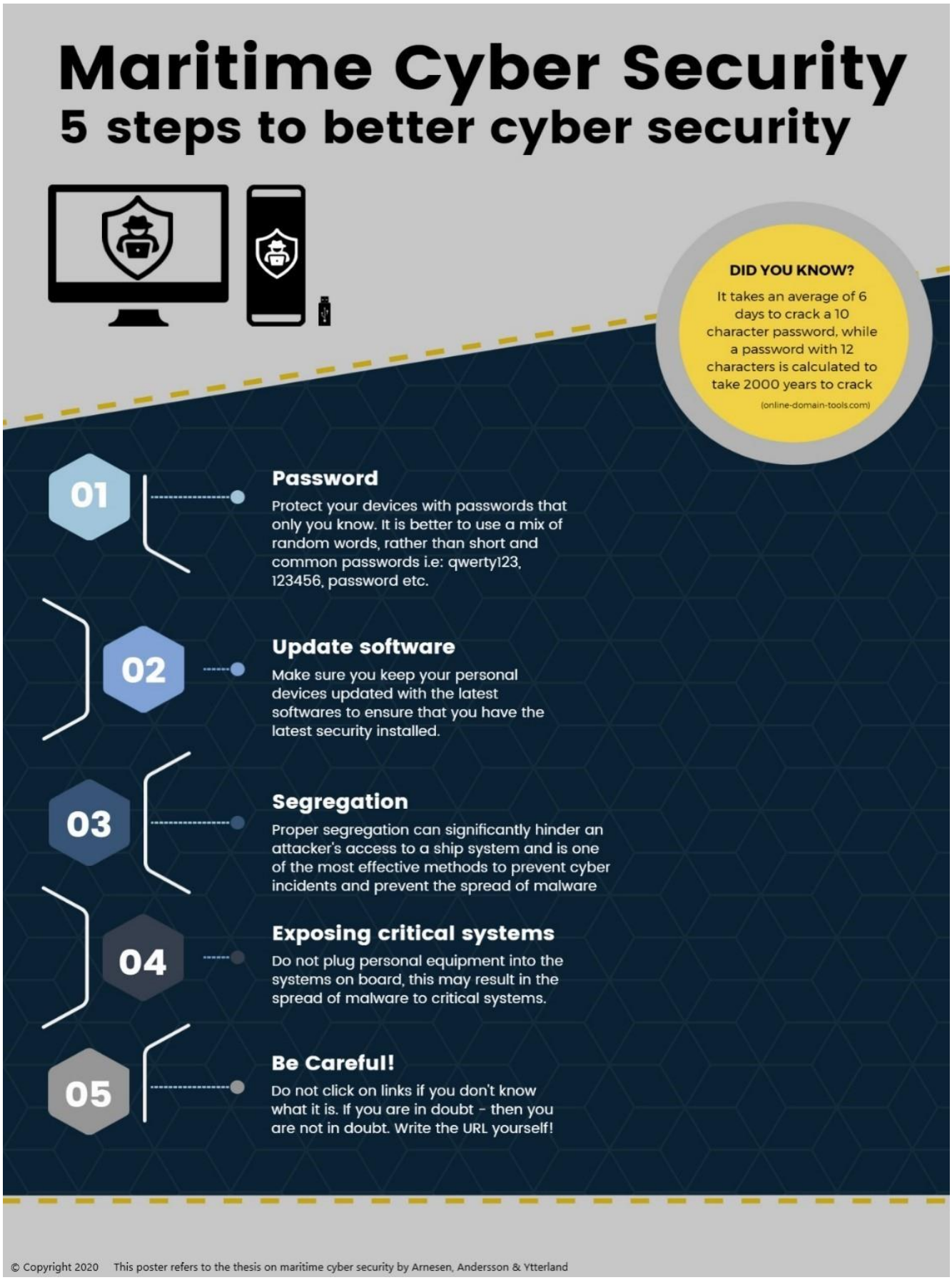
For å forsikre dere om at kravene oppfylles, må dere følge interne retningslinjer og eventuelt rådføre dere med behandlingsansvarlig institusjon.

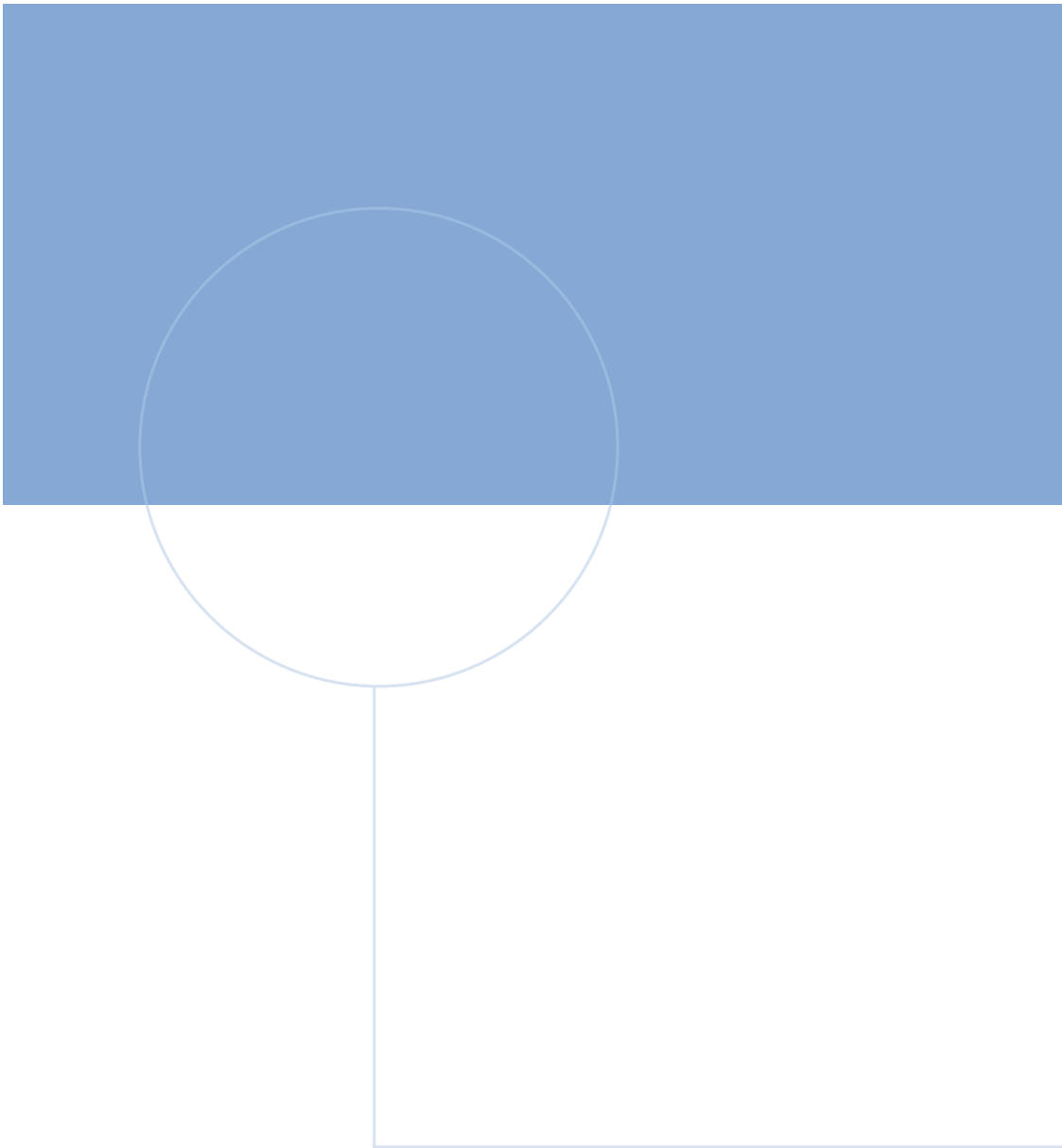
OPPFØLGING AV PROSJEKTET
NSD vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Lykke til med prosjektet!

Tlf. Personverntjenester: 55 58 21 17 (tast 1)

Vedlegg 5 – Bevisstgjøringsplakat





NTNU

Kunnskap for en bedre verden