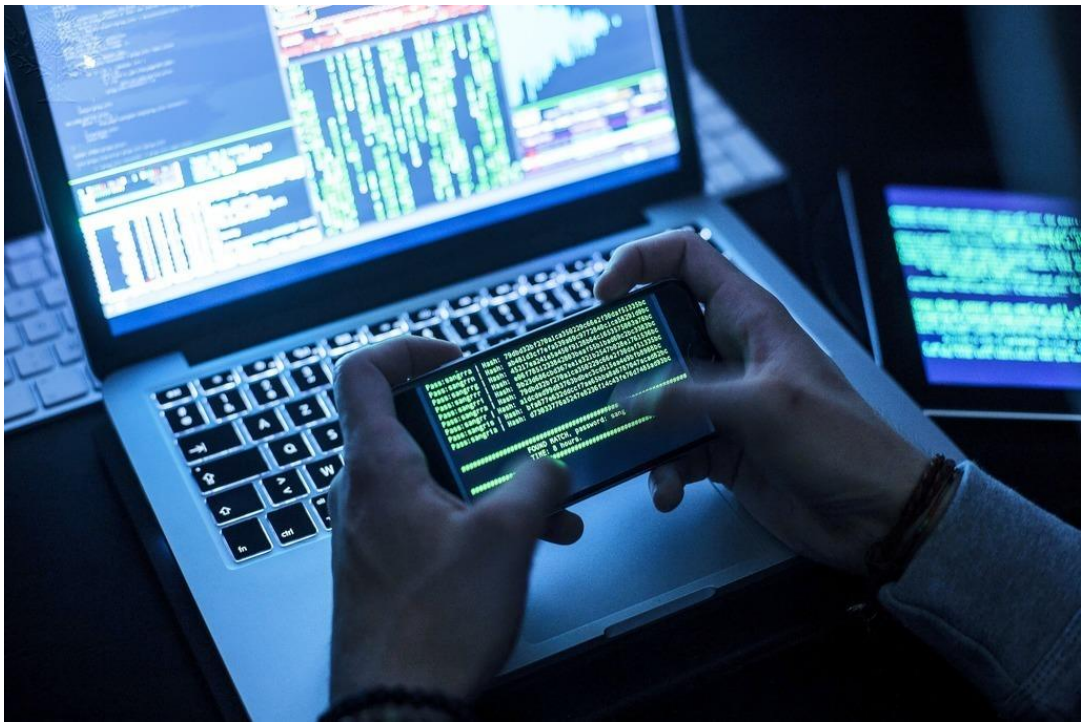
CHALMERS



En studie av cybersäkerhet i svenska hamnar

En undersökning av organisationernas motståndskraft och ställningstagande till cybersäkerhetsriktlinjer i hamnar

Kandidatarbete inom internationell logistik

WILLIAM GREGORSON
ADAM SIBGÅRD

INSTITUTIONEN FÖR MEKANIK OCH MARITIMA VETENSKAPER

CHALMERS TEKNISKA HÖGSKOLA
Göteborg, Sverige, 2023

En studie av cybersäkerhet i svenska hamnar

En undersökning av organisationernas motståndskraft och ställningstagande till cybersäkerhetsriktlinjer i hamnar

Kandidatarbete inom internationell logistik

WILLIAM GREGORSON
ADAM SIBGÅRD

Institutionen för mekanik och maritima vetenskaper
Avdelningen för maritima studier
CHALMERS TEKNISKA HÖGSKOLA
Göteborg, Sverige, 2023

En studie av cybersäkerhet i svenska hamnar
En undersökning av organisationernas motståndskraft och ställningstagande till cybersäkerhetsriktlinjer i hamnar

WILLIAM GREGORSON
ADAM SIBGÅRD

Institutionen för mekanik och maritima vetenskaper
Chalmers tekniska högskola
SE-412 96 Göteborg
Sverige
Telefon: + 46 (0)31-772 1000

Omslag:
[Hackare som knäcker ett lösenord. Datahackare som använder en dator och en handhållen enhet som har använts till att lista ut ett lösenord.]
Science Photo Library.
https://quest-eb-com.eu1.proxy.openathens.net/images/search/cybersecurity/detail/132_3045985

Institutionen för mekanik och maritima vetenskaper
Chalmers tekniska högskola
Göteborg, Sverige 2023

FÖRORD

Detta kandidatarbete har skrivits på Chalmers Tekniska Högskola under våren 2023 på institutionen för mekanik och maritima vetenskaper. Skribenterna studerar programmet Internationell Logistik som är ett program på 180 högskolepoäng, där uppsatsen redogör för 15 av dessa.

Att skriva en akademisk uppsats är en intressant och utmanande process. Vi valde ämne kring uppsatsen utifrån någonting vi fann aktuellt och var intresserade att lära oss mer om. Vi har under uppsatsens gång lärt oss mycket om ämnet cybersäkerhet, både i det teoretiska och i det praktiska ute i näringslivet.

Vi vill tacka de som har hjälpt oss i processen att skriva denna uppsats. Både tack till handledare som genom kunnande och råd har visat oss i rätt riktning samt ett stort tack till de respondenter som tog sig tid att medverka i studien och dela med sig av deras kunskaper och värdefulla information.

Vi hoppas att denna uppsats kan bidra till att öka medvetenheten om betydelsen av cybersäkerhet inom den maritima sektorn och bidra till en fortsatt diskussion och forskning inom ämnet.

Göteborg, 2023.
William Gregorson, Adam Sibgård.

En studie av cybersäkerhet i svenska hamnar
En undersökning av organisationernas motståndskraft och ställningstagande till cybersäkerhetsriktlinjer i hamnar

WILLIAM GREGORSON
ADAM SIBGÅRD

Institutionen för mekanik och maritima vetenskaper
Chalmers tekniska högskola

SAMMANDRAG

Den globala världshandeln är i stor utsträckning beroende av sjöfartens tjänster. Detta då ungefär 90% av godset som fraktas världen över i något led av transportkedjan fraktats med hjälp av fartyg.

Den ökade digitaliseringen i maritima verksamheter har medfört stora förbättringar för sjöfarten men har också ökat riskerna för cyberattacker. Antalet rapporterade cyberattacker mot hamnar och fartyg har ökat kraftigt mellan 2017 och 2022. Stora sjöfartsorgan som IMO (International Maritime Organisation) har utfärdat riktlinjer för hantering av cybersäkerhet där de betonar vikten av att skydda de digitala system som används inom maritima verksamheter.

Författarna av studien undersöker nivån av organisationernas motståndskraft mot cyberangrepp och hur olika guider och lagar är utformade för att skydda sjöfartssektorn. Författarna undersöker hur hamnarna ställer sig till dessa guider och lagar. Cybersäkerhet i hamnar är ett viktigt ämne på grund av den ständiga utvecklingen av digital teknologi och dess påverkan på logistikkedjor.

Studien drar slutsatsen att samtliga av de tillfrågade organisationerna arbetar proaktivt med deras cyberförsvar. Studien konstaterar att arbetet med cybersäkerhet skiljer sig åt mellan organisationerna beroende på deras hotbild och resurser. Större hamnar har en mer omfattande cybersäkerhetsorganisation jämfört med mindre hamnar, utifrån principen att de är mer exponerade för eventuella attacker.

Studien visar att samtliga organisationer arbetar utifrån ledningssystemet ISO 27001, men samtidigt skiljer de sig åt i ställningstagandet kring andra riktlinjer och hur de ser på arbetet med cybersäkerhet.

Studien kommer avgränsa sig mot att undersöka svenska hamnar. Studien kommer inte heller djupdyka i de ekonomiska åtagandena som kommer med att inrätta och upprätthålla en cybersäkerhetsorganisation. Dock så kommer studien att göra hänvisningar till hamnars storlek och indirekt påvisa att deras resurser då är större än andras.

Nyckelord: Cybersäkerhet, hamnorganisationer, riktlinjer, cyberrisk, cyberhot, åtgärder.

A study of cybersecurity in Swedish ports
An investigation of organizations' resilience and stance on cybersecurity guidelines in ports

WILLIAM GREGORSON
ADAM SIBGÅRD

Department of Mechanics and Maritime Sciences
Chalmers University of Technology

ABSTRACT

Global world trade is largely dependent on shipping services, as about 90% of the goods transported worldwide at some point in the supply chain are shipped by sea.

The increased digitalization in maritime operations has brought significant improvements to shipping but has also increased the risks of cyber-attacks. The number of reported cyber-attacks against ports and ships has increased sharply between 2017 and 2022, and major shipping organizations such as IMO have issued guidelines for managing cybersecurity, emphasizing the importance of protecting the digital systems used in maritime operations.

The authors of the study investigate the level of organizations' resilience to cyber-attacks and how different guides and laws are designed to protect the maritime sector. The authors examine how ports respond to these guides and laws. Cybersecurity in ports is an important topic due to the constant development of digital technology and its impact on logistics chains.

The study concludes that all of the organizations surveyed are working proactively on their cyber defences. The study notes that the work on cybersecurity varies between organizations depending on their threat profile and resources, where larger ports have a more extensive cybersecurity organization compared to smaller ports, based on the principle that they are more exposed to potential attacks.

The study shows that all organizations work based on the ISO 27001 management system, but at the same time they differ in their stance on other guidelines and how they view their work on cybersecurity.

The study will focus on examining Swedish ports. The study will also not delve into the financial commitments that come with establishing and maintaining a cybersecurity organization. However, the study will make references to the size of ports and indirectly indicate that their resources are larger than others.

Keywords: Cyber security, ports, cyber threats, cyber risk, guidelines.

INNEHÅLLSFÖRTECKNING

FIGURFÖRTECKNING

Inga figurförteckningsposter.

TABELLFÖRTECKNING

FÖRKORTNINGAR OCH BEGREPP

Cyberattack	Försök att få obehörig åtkomst till datorsystem för att stjäla, ändra eller förstöra data.
Cyber Defence Center	En cybersäkerhetsavdelning som avser att minimera organisationens risk mot cyberhot genom att minska påverkan av säkerhetsintrång med effektiva procedurer för upptäckande och ge snabba gensvar på eventuella intrång genom goda processer och procedurer.
Cyber Security Risk	Risken för en organisations informationsteknologi och/eller operationella teknologi, samt dess resurser och tillgångar
IMO	International Maritime Organization
IT-system	Informationsteknologi utifrån detta arbete syftar till de programvaror, tillgångar, system, plattformar som skapar, utbyter, delar, styr, hanterar och lagrar elektronisk information. Exempelvis system som stöttar och hanterar landbaserad teknik och operationell miljö.
OT-System	Operationell teknologi. Kontrollsystem och enheter som är programmerade till att styra, övervaka eller interagera med system som styr fysiska processer, som lasthantering, maskinkontroller etc.
Ransomware	”Ransomware, även kallad gisslanprogram eller utpressningstrojan, är en form av skadlig kod som krypterar och låser dina filer och dator i syfte att begära en lösensumma för att få dessa tillbaka.” (F-Secure, 2023)
Upp-tid	Den tid som ett virtuellt system kan utföra det värdeskapande arbete som systemet i fråga är designerat att göra.
PC	Personal Computer

1. INLEDNING

I detta kapitel presenteras en övergripande inledning och bakgrund till hamnars betydande roll inom världshandeln och det ökande hotet från cyberrelaterande attentat. I detta kapitel presenteras även syftet, frågeställningarna och avgränsningar.

Den maritima sektorn utgör en stor del av den globala ekonomin. Den sträcker sig över hela världen och dess internationella status är påtaglig. Ungefär 90% av världshandeln mätt i volym fraktas med sjöfarten (Transportstyrelsen, 2021). Under den senare tiden inom sjöfarten har en snabb och kraftfull digitalisering pågått, och pågår kontinuerligt (Kapalidis m.fl., 2022). Behovet av fysiska dokument suddas ut, och inom en snarare framtid kan man vänta sig att alla operativa aktiviteter kommer stödjas av digitala system (Kechagias m.fl., 2022).

De digitala lösningar som implementeras inom en organisationens kan ta form av både IT- och OT-system. IT-system är de system som innefattar information, dokument, kommunikation och data. OT-system är hård- och mjukvara som kontrollerar de operationella systemen som mer fysiskt påverkar hamnar, som autonoma transportörer, digitalt styrda kranar etcetera. Risken för dessa system är av olika art, där cyberattacker mot IT-system kan leda till läckt information, medan attacker mot OT-system tenderar att påverka mer fysiskt, med risk för laster, personal och fysiska tillgångar (BIMCO m.fl., 2020). Enligt International Maritime Organization (IMO, 2017) bör riskhanteringen fokusera på båda delar, samt hur de olika systemen samverkar med varandra.

Den digitala utvecklingen med nya system och avancerad teknologi leder till stora förbättringar för den maritima industrin, med effektiviseringar och ökad produktivitet som resultat. Med dessa nya system medföljer dock risker. Mellan åren 2017 och 2022 så har antalet rapporterade fall av cyberattacker mot hamnar och fartyg ökat markant (Kapalidis m.fl., 2022). År 2020 rapporterades det på Port Security Seminar & Expo att man ser en ökning av mer omfattande cybersäkerhetsintrång av operationell teknologi på 900% från 2017 till 2020 (Hellenic Shipping News, 2020). Denna ökning påvisas också av att det var 50 attacker 2017, 120 attacker 2018 och fler än 300 år 2019 (Androjna m.fl., 2020). Tam och Jones (2018) menar också att cyberattackerna som riktas mot sjöfartsnäringen numera kommer ifrån en rad olika operatörer och organisationer. Där det kan variera från att vara aktivister, terrorister, konkurrenter och kriminella (Tam & Jones, 2018).

IMO upplyser om dessa risker från cyber-relaterade attacker som riktas mot digitala system i sina riktlinjer för hantering av cybersäkerhet (IMO, 2017). Dessa riktlinjer belyser vikten av att skydda dessa system som ombesörjer hela den maritima operationen av att frakta gods världen över.

Av dessa rapporterade fall finns det mer betydande cyberattacker som sticker ut, bland annat attacken som drabbade A.P. Möller-Maersk A/S. Maersk uttalade sig 2017 kring den cyberattack de utsattes för och bekräftade den 28 juni att de utsattes för Petya-attacken den 27e juni 2017. Flera IT-system över stora delar av verksamheten stängdes ner helt (Wagner, 2017). Cyberattacken fick stora konsekvenser och uppskattades enligt Maersk uppnå en kostnad av 300 miljoner USD (Wienberg, 2017).

1.1 Bakgrund

Digitalisering sprider sig fort inom samtliga delar av näringslivet. Företag och organisationer arbetar i stora delar numera via olika moln-lösningar och andra digitala hjälpmedel. Av denna anledning så finner författarna av denna studie det av vitalt intresse att utvärdera det faktiska arbete som görs inom dessa hamnorganisationer för att stärka deras motståndskraft mot cyberangrepp. Författarna avsikt med studien är också att undersöka närmare hur olika guider och lagrum är formulerade, och hur dessa sedan tolkas och implementeras av de berörda organisationerna.

Cybersäkerhet i hamnverksamheter är ett betydelsefullt ämne som behöver stort fokus utifrån att den digitala teknologin ständigt utvecklas och i samband med att logistikkedjor utvecklas uppkommer både positiva möjligheter samt negativa risker som behöver hanteras på rätt sätt (IAPH m.fl., 2020).

Den Europeiska unionen formulerade i direktivet 2016/1148 (European Parliament, 2016), att hamnverksamheter karaktäriseras av internationella, nationella och regionala myndigheter som väldigt viktiga som del i infrastrukturen för att hantera internationell handel i den globala ekonomin. Med detta i beaktning är cybersäkerhet ett aktuellt ämne för hamnverksamheter ur ett beslutsfattande myndighetsperspektiv, detta för att undvika stora operationella avbrott som påverkar både handel och ekonomi globalt.

Enligt rapporten Port Community Cyber Security (IAPH m.fl., 2020), krävs det att cybersäkerhetsfrågan måste lyftas och att samarbeten mellan olika hamnverksamheter är nödvändiga för att utveckla relationen och samarbetet mellan olika intressenter. Det huvudsakliga målet ska vara att utveckla och slå fast ett ramverk för hur cybersäkerhetshanteringen ska gå till och ge aktörer den kunskap och de verktyg som anses lämpliga för att hantera hoten. För att utveckla detta ramverk har EU sponsrat projektet MITIGATE som beskrivs av Polatidis m.fl. (2018) som en del i riskhantering av cyberhot i den maritima sektorn. Polatidis m.fl. (2018) förklarar att de utgår från de internationella standarderna ISO 27001 och NIST SP800-30 när de utvecklat ramverket för ledningssystemet för riskerna i den maritima cybermiljön.

1.2 Syfte

Syftet med studien är att undersöka hur hamnar hanterar de risker och hot som uppstår och kan uppstå vid cyberattacker samt om de har de lämpliga verktygen och kunskapen som krävs för att hantera dessa hot.

IT genomgår kontinuerligt en förändringsprocess, och med denna utveckling så uppdagas nya hot och problem som aldrig tidigare bemötts. För att möta dessa hot finns det stöd i lagar, regelverk och riktlinjer. Syftet med studien avser att redogöra för olika sätt att möta dessa hot. Samt att undersöka hur hanteringen av riskerna ser ut, om hamnorganisationerna arbetar reaktivt eller proaktivt. Studien ska undersöka vilka rekommendationer som finns för att hantera risker och hot i den maritima sektorn, samt undersöka hur specifika hamnar förhåller sig till dessa rekommendationer.

1.3 Frågeställning

- Hur arbetar hamnar och terminaler med cybersäkerhet?
    - Vilka åtgärder vidtas för att garantera säkerheten?

- Hur förhåller sig hamnorganisationer till förutsatta riktlinjer, resolutioner och lagkrav inom cybersäkerhet?

1.4 Avgränsningar

Studien kommer inte analysera närmare de faktiska tekniska system som tillämpas inom organisationen. Alltså vad för faktiskt system som tillämpas, vad för hårdvara som installerats, samt hur detta fungerar i praktiken. Studien kommer inte heller att djupare analysera de ekonomiska åtaganden som krävs för installation och upprätthållande av de system och procedurer som organisationerna använder sig av. Studien kommer dock dra paralleller till resurs-tillgångar, och hur detta kan återspegla sig på ens organisations cyberförsvars möjlighet. Studiens primära datainsamling sker genom intervjuer med organisationer i Sverige. Studien fokuserar på ledningsnivå inom organisationerna och hur deras syn är gällande cybersäkerhet.

2. TEORI

Teoridelen är uppdelad i tidigare händelser där cyberattacker haft stor påverkan på hamnverksamheter, för att i senare del av kapitel redovisa regelverk och rekommendationer från branschorganisationer.

2.1 Cyberattack

En cyberattack är en attack med syftet att störa, skada, inaktivera, förstöra eller kontrollera ett datasystem. Ayala (2016) beskriver att en cyberattack antingen är riktad eller oriktad. I den riktade cyberattacken väljs en specifik organisation eller måltavla ut, med syftet att komma åt eller störa specifika system för att möjliggöra en utbetalning eller förtjänst för den attackerande parten. Detta är ofta en mer utarbetad attack än den oriktade, och kräver en stor del förberedande arbete från den attackerandes sida. Denna typ av attacker är ofta mer omfattande än den oriktade attacken då hackaren direkt valt ut organisationen i fråga, och således format attacken på ett sätt som skall åsamka mest skada (Ayala, 2016). En oriktad cyberattack siktar i stället bredare med målet att påverka ett större antal parter, utan ett särskilt fokus mot en specifik part.

2.2 Tidigare cyberattacker mot hamnverksamheter

NotPetya är ett ransomware som ledde till ett stort avbrott i A.P. Möller-Maersks IT-system år 2017. Påverkan var både mot olje- och gasproduktion-avdelningar inom organisationen men även mot hamnverksamheter. Incidenten ledde till stora ändringar i Maersks IT-system i syftet att undvika denna typ av attacker framöver. Hela attacken resulterade i runt 300 miljoner USD i förlust för företaget.

Enligt Jadesköld & Zalitis (2019) ledde cyberattacken Notpetya till att APMs terminal, som är en del av A.P. Möller-Maersks verksamhet, i Göteborgs Hamn, i princip stod stilla i tre dagar, där endast manuell drift var i fokus för att primärt säkerställa hanteringen av farligt gods.

Attacken riktade sig mot filer och hårddiskar som krypterades där datorerna startades om och hamnade i ett uppstartsläge där verksamheten inte längre hade tillgång till sina IT-system. Användarna uppmanades av den attackerande parten att de genom betalning av en lösensumma så skulle de återigen få tillgång till filer och systemen som krypterats.

Enligt kommunikationsansvarig på Göteborgs hamn drivs hamnen numera av separata bolag som därmed har separata IT-system. De separata systemen leder till att det den fysiska kopplingen mellan olika aktörer i hamnen numera är i princip obefintlig vilket vidare leder till mindre sårbarhet, där en attack mot en viss verksamhet i hamnen inte drabbar samtliga aktörer (Jadesköld & Zalitis, 2019).

En ytterligare cyberincident inträffade 2012 hos den australiensiska tull och gränsbevakningen (Meyer-Larsen & Müller, 2018). Den brottsliga verksamhet som utförde intrånget kunde till följd kolla vilka transporter som rubricerats som misstänksamma av myndigheterna, och med hjälp av denna information smuggla narkotika i de transporter som inte var misstänksamma enligt tull- och gränsbevaknings myndigheterna (Meyer-Larsen & Müller, 2018).

Ytterligare en cyberincident inträffade i Antwerpens hamn mellan åren 2011 och 2013 där hackare rekryterades av en brottslig organisation. Denna organisation gömde narkotika i containrar som användes av legala transportörer. För att sedan få tillgång till narkotikan så hackade de sig in i hamnens PCS (Port Communication System) för att samla information om containerns säkerhetsnivå och vart containern befinner sig. Detta gjorde det möjligt för den

brottsliga organisationen att skicka egna förare till containern, ta hand om narkotikan och avlägsna sig innan den rättmätiga ägaren i sin tur kunde ta hand om containern(Meyer-Larsen & Müller, 2018).

2.3 IMO och dess krav

International Maritime Organization (IMO) är ett organ under FN. De utgör en stor del av reglementen kring sjöfart och maritima verksamheter. De två huvudsakliga koder som hanterar hamnsäkerhet är ”the International Ship and Port Facility Security” (ISPS) Code som är en del av SOLAS-konventionen samt International Safety Management (ISM) Code som har utvecklat riktlinjerna ”Guidelines on Maritime Cyber Risk Management”.

2.3.1 ISPS-koden

ISPS-koden är ett obligatoriskt säkerhetsreglement för internationell sjöfart och hamnverksamheter. Målet med koden är att säkerställa ett standardiserat ramverk för att utvärdera risker och implementera säkerhetsåtgärder i verksamheterna. Koden implementerades den 1 juli 2004. Koden är uppdelad i del A och del B där A-delen är obligatorisk och statuerar säkerhetsrelaterade krav för hamnar och terminaler och B-delen innehåller de riktlinjer och rekommendationer för hur man ska möta kraven i A-delen.

Huvudmålet med ISPS-koden är det fysiska skydd som krävs för fysiska hot i hamnar. Dock är flera delar i koden relevanta även för cybersäkerhet, bland annat i ISPS Code, Part B, 15.3 sub 5 (IMO, 2009) som identifierar radio, kommunikationssystem, datorsystem och nätverk som relevanta delar som ska ha relevant skydd. I samband med ISPS Code, Part A, 15.5 sub 2 (IMO, 2009) som lyfter identifiering av hot mot tillgångar och infrastruktur i hamnar och hantering av dessa risker, så blir cybersäkerhet en stor del av ISPS-koden (IAPH m.fl., 2020).

2.3.2 ISM-koden

ISM-koden är utfärdad av IMO med syftet att etablera en internationell standard gällande säkert handhavande och hantering av fartyg samt att förhindra utsläpp av miljöfarliga ämnen (IMO, 2018). ISM-koden dikterar att redare, eller någon annan organisation eller person som åtagit sig ansvaret för fartygets operationella drift från fartygets ägare, måste åta sig ansvaret att innehållet i ISM-koden efterföljs (IMO, 2018).

2.3.3 IMO – Maritime cyber risk management in safety management systems

Resolution MSC.428 (98) från IMO antogs i ISM-koden 2017 (IMO, 2017a). Resolutionen avser att hamnar och hamnverksamheter ska arbeta för att skydda sina verksamheter för att hantera cyber relaterade hot och svagheter.

Resolutionen syftar även till olika administrationer, rederier och organisationer inom sjöfarten att säkerställa att hanteringen av cyberhot är adresserat på lämpligt sätt i redan existerade ”Safety Management Systems”. Detta införlivades inom de olika påverkade organisationerna senast 1 januari 2021 vid den första verifieringen av företagens ”Document of Compliance” (IMO, u.å.).

2.3.4 IMO - Guidelines on Maritime Cyber Risk Management

IMO Faciliation Committee (FAL) formade tillsammans med Maritime Security Committee (MSC) MSC-FAL.1/Circ.3 - ”Guidelines on Maritime Cyber Risk Management”. Detta är en

samling av riktlinjer som belyser olika områden som bör evalueras vid förstärkandet av motståndskraft gällande cyberhot (IMO, 2017b). FAL och MSC såg ett behov av att öka medvetenheten kring cybersäkerhet, med rekommendationer för hantering av hot och sårbarheter inom maritima verksamheter. I riktlinjerna presenterar man specifikt att funktionell hantering av cyberhot kräver engagemang från högsta ledning till lägsta nivån av verksamheten. Riskhanteringen kräver att hela organisationer genomsyras av kunskap och medvetenhet, annars brister säkerhetstänket.

Riktlinjerna delar in rekommendationerna för riskhantering i fem olika delmoment, identifiera, skydda, upptäcka, reagera, återställa.

De fem punkterna syftar mer specifikt till följande:

- Identifiera
    - Definiera roller och ansvar för personal angående cybersäkerhetshantering. Identifiera vilka system, tillgångar, data och förmågor som utgör en möjlig risk för driften av verksamheten.
- Skydda
    - Implementera lämpliga processer och åtgärder för att kontrollera risker, samt planera för beredskapsfunktioner vid eventuella cyberattacker. Detta görs för att försäkra fortsatt möjlig drift utan störning.
- Upptäcka
    - Utveckla samt implementera nödvändiga aktiviteter för att upptäcka cyberattacker inom en rimlig tidsram.
- Reagera
    - Utveckla och implementera system med funktioner som skapar motståndskraft mot cyberattacker samt möjliggör återställning av dessa system vid en attack.
- Återställa
    - Åtgärder för att säkerställa möjlig åter-uppstart av system efter en attack.

Riktlinjerna bör enligt kommittéerna användas i samband med medlemsländernas respektive regeringars krav samt flaggstats-krav för fartyg.

2.4 ISO 27001

Internationella standardiseringsorganisationen (ISO) och Internationella elektroniska kommissionen (IEC) har tillsammans skapat ett speciellt system för internationell standardisering inom ett flertal branscher. Standardiseringen utarbetas tillsammans med nationella organ och tekniska kommittéer som inrättats av respektive nationell organisation för olika verksamhetsområden (ISO & IEC, 2022b).

Detta dokument har utarbetats av de ISO och IEC för att statuera krav för att upprätta, införa, upprätthålla och kontinuerligt förbättra ett ledningssystem för informationssäkerhet. Etableringen och integreringen av ett ledningssystem för informationssäkerhet av denna karakteristik har stor påverkan av organisationen i frågas behov och mål, dennes säkerhetskrav, tillämpade organisationsprocesser, samt storleken och formen på organisationen.

För att nå upp till denna standard så finns det ett flertal områden som skall utvärderas av den organisation som utfärdar standarden.

- Ledarskap

    - Den högsta ledningen skall visa prov på ledarskap och åtagande när det gäller ledningssystemet för informationssäkerheten genom att säkerställa och informera om olika ting, där bland annat man omnämna att man skall:
        - Säkerställa att informationssäkerhetspolicy och informationssäkerhetsmål upprättas och är förenliga med organisationens strategiska inriktning,
        - Säkerställa att kraven i ledningssystemet för informationssäkerhet integreras i organisationens verksamhetsprocesser,
        - Informera om vikten av verkningsfull ledning av informationssäkerhetsarbetet och att kraven i ledningssystemet för informationssäkerhet uppfylls, osv.
- Planering
    - Åtgärder för att hantera risker och möjligheter
- Stöd
    - Organisationen skall fastställa och förse de resurser som efterfrågas för att skapa, implementera, underhålla och förbättra de olika ledningssystem som ombesörjer informationssäkerheten.
- Verksamhet
    - Planering och styrning av verksamheten.
        - Organisationen i fråga skall planera, implementera och styra de processer som statueras i certifieringen för att denne skall vara gällande.
- Utvärdering av prestanda
    - Organisationen skall utvärdera arbetet genom övervakning, mätning, analys och olika metoder för utvärdering. Detta innefattar att organisationen skall avgöra vad som skall evalueras och granskas, vilka metoder och verktyg som skall användas för att få tillförlitliga resultat, vem som skall utföra övervakningen och mätningen osv.
- Förbättring
    - Organisationen skall kontinuerligt förbättra lämpligheten, tillräckligheten samt verkan av de ledningssystem som finns för informationssäkerheten.

2.5 NIST – United States National Institute of Standards and Technology – Framework for improving Critical Infrastructure Cybersecurity

Ytterligare ett ramverk med riktlinjer är framtaget av nationella institutet för standard och teknologi i USA," United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity" (the NIST Framework) (Institute of Standards, 2014).

Ramverket från NIST är framtaget för att hjälpa organisationer förstå, hantera samt minimera säkerhetsrisker från cyberhot. Det kan användas både för identifiering av risker och hantering av risker när de uppstår. Det är ett verktyg med flera funktioner som tillsammans ska leda till en säkrare cybermiljö. Ramverket grundar sig i följande fem huvudsakliga funktioner som är till för att uppnå cybersäkerhet i specifika områden (Institute of Standards, 2014).

- Identifiera
    - Utveckla en förståelse i organisationen för hantering av cybersäkerhetsrisker för system, människor, tillgångar, data och andra förmågor.
- Skydda

    - Utveckla samt implementera skyddsnät för att säkerställa kritiska funktioner. Skyddsfunktionen är till för att begränsa den inverkan en cyberattack kan ha på organisationen.
        - Exempel på skyddsfunktioner:
- Upptäcka
    - Utveckla samt implementera aktiviteter för att upptäcka cyberattacker.
- Reagera
    - Utveckla samt implementera aktiviteter för att kunna agera vid cyberattacker.
- Återställa
    - Utveckla samt implementera aktiviteter för att kunna upprätthålla motståndskraft och för att kunna återställa förmågor och funktioner i de system som påverkades av cyberattacken för att kunna återgå till en fungerande verksamhet.

2.6 Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster

Syftet med denna lag är att uppnå och tillhandahålla en hög nivå på säkerheten inom nätverk och informationssystem för samhällsviktiga tjänster (NIS) inom ett flertal sektorer. En av dessa betydande sektorer som lagen avser att tillämpas på är transportsektorn. I och med det så kan lagen tillämpas på svenska hamnar. Men det skall dock infalla vissa kriterier för hamnen i fråga för att lagen skall bli tillämpbar. Enligt lagens 3§ så skall leverantörer av de slag som anges i bilaga 2 till NIS-direktivet och som tillhandahåller en samhällsviktig tjänst som är verksam i Sverige samt att tjänsten i fråga är beroende av nätverk och informationssystem där följden av en incident skulle medföra betydande störning vid tillhandahållandet av tjänsten (*Lag om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174). Riksdagen*, 2018).

Lagens 4§ specificerar att regeringen, eller en myndighet designerad av regeringen, får meddela föreskrifter om vilka tjänster som är samhällsviktiga tjänster och vad som menas med en betydande störning. Detta styrks även i den 17§, då regeringen, eller den myndighet som regeringen designerar, får specificera säkerhetsåtgärder enligt de skyldigheter som specificeras i lagens 12–16§§(*Lag om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174). Riksdagen*, 2018).

De olika skyldigheter som åläggs en leverantör av samhällsviktiga tjänster specificeras i lagens 11 – 16§§. Dessa skyldigheter omnämner att leverantören av en samhällsviktig tjänst skall systematiskt och riskbaserat informationssäkerhetsarbete avseende informationssystem och nätverk som används för att tillhandahålla den samhällsviktiga tjänsten. Leverantören skall göra en riskanalys som skall vara innehållande av en åtgärdsplan. Denna plan skall utvärderas och uppdateras på en årlig basis. Lagen omnämner också att leverantören skall vidta ackurata och ändamålsenliga tekniska och organisatoriska åtgärder för att hantera de risker som hotar verksamhetens informationssystem och nätverk, det omnämns också att denne leverantör skall utföra lämpliga åtgärder för att både förebygga och minimera den verkningar av en eventuell incident på de nätverk och informationssystem som används för att leverera den samhällsviktiga tjänsten. Dessa åtgärder skall som grund säkerställa att kontinuiteten fortskrider för tjänsten (*Lag om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174). Riksdagen*, 2018).

Lagen dikterar också de skyldigheter som åläggs leverantörerna av dessa digitala tjänster. 15§ omnämner att leverantören av dessa digitala tjänster skall vidta tekniska och organisatoriska åtgärder som anses vara ändamålsenliga, proportionella samt hanterar de risker som hotar

säkerheten i informationssystemen och nätverken som de använder när de tillhandahåller digitala tjänster inom EU (*Lag om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174). Riksdagen*, 2018). Dessa åtgärder ska säkerställa en viss nivå på säkerheten som är proportionerlig i förhållande till risken. 16§ omnämner att leverantören av de digitala tjänsterna skall vidta åtgärder som avser att förebygga och minimera verkningar av cyberincidenter som påverkar nätverk och informationssystem som leverantören använder. Skyldigheten till detta gäller endast i de förhållanden till verkningar som de incidenterna har på digitala tjänster som leverantören erbjuder inom EU. Dessa åtgärder syftar till att säkerställa en viss kontinuitet i de levererade tjänsterna (*Lag om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174). Riksdagen*, 2018).

2.7 CIS Controls

CIS Controls (Center for Internet Security Critical Security Controls). CIS-kontrollerna har syftet att tillhandahålla ett tillvägagångssätt för att hjälpa organisationer att skydda sina verksamheter från cyberhot (CIS, 2023b).

Kontrollerna är uppdelade i tre implementeringsnivåer. Basnivå, grundläggande nivå samt organisatorisk nivå. De olika nivåerna är rangordnade där basnivån är den simplaste nivån av cybersäkerhet som alla organisationer bör implementera, medan den grundläggande och organisatoriska nivån tillhandahåller ytterligare säkerhetslager för mer mogna cybersäkerhetsprogram.

Den senaste versionen CIS Controls v8 har totalt 18 kontroller som är grupperade i de tre olika nivåerna (CIS, 2023a).

Basnivå: Dessa kontroller är fundamentala och utgör basen för organisationers cybersäkerhet. Kontrollerna fokuserar på att etablera grundläggande cybersäkerhetspraxis och inkluderar åtgärder som att inventera och kontrollera auktoriserade och obehöriga enheter och programvaror, säkra konfigurationer och underhålla skyddsåtgärder som brandväggar och antivirus (CIS, 2023a).

Grundläggande nivå: Dessa kontroller bygger på baskontrollerna och tillhandahåller ytterligare säkerhetsåtgärder för att förbättra organisationens cyberförsvar. Nivån inkluderar åtgärder som ska vidtas efter den kontinuerliga bedömningen av sårbarheten hos organisationen. Samt säker konfiguration av system och kontrollerad åtkomsthantering (CIS, 2023a).

Organisatorisk nivå: Dessa kontroller fokuserar på säkerhetspraxis på en högre nivå som involverar bland annat policy för organisationen, processer samt styrning. Åtgärder som inkluderas på denna nivå är utbildning i säkerhetsmedvetenhet, incidenthantering, testning av säkerhetsnivå (CIS, 2023a).

CIS-kontrollerna är designade på ett sätt som gör dem anpassningsbara och möjliga att implementera i olika sorters organisationer, oavsett storlek, bransch och funktion. Kontrollerna tillhandahåller en strategi för cybersäkerhet och är ett hjälpmedel för att organisationer ska kunna optimera sina resurser och ansträngningar för att på mest effektiva sätt skydda sig från cyberhot (CIS, 2023b).

2.8 Andra hamnars förhållningssätt till lagrum och riktlinjer

Enligt Senarak (2020) så har Port Authority of Thailand (PAT) införlivat olika åtgärder och policyer som skall, på ett förebyggande sätt, förhindra och försäkra att hamnarna skall fortsatt

vara verksamma vid eventuella framtida cyberattacker. En av dessa åtgärder som implementeras är ramverket ISO 27001. Ramverket skall göra så att man på ett proaktivt sätt kan hålla sig uppdaterad mot framtida cyberrelaterade hot hos Leam Chapang Port (LCP) och andra statligt ägda hamnar.

PAT följer även Maritime Cyber Risk Management riktlinjerna utfärdat av IMO. Detta med syfte av att förbättra hamnens riskbedömningsförmåga där avsikten är att titta på hamnens cybersituation i sin helhet, allt från cyberhoten som medföljer av digitalisering, integration, automation och andra nätverksbaserade system som hamnen kan använda sig av vid operationell drift (Senarak, 2020). Genom denna arbetsprocess skall PAT ha möjligheten att utveckla kris-åtgärdsplaner, lindrande åtgärder, Safety Management System samt strategier för att minska cyberhoten, men även öka medvetenheten gällande cyberhot genom hela organisationen. PAT och LCP tillhandahåller även olika kurser inom cyberhot för att medvetandegöra de som jobbar i hamnen (Senarak, 2020). Kurserna grundar sig i olika ämnesområden där man bland annat utbildar inom säkerhetsträning för IT-system, säkert handhavande och användande av IT-system, nätverkssäkerhet, efterlevande av standarder och regler samt även inom cyberrisk ledningssystem (Senarak, 2020).

PAT i LCP lägger mycket energi och kraft på att sammanfoga hamnsäkerhetsorganisationen med hamnens cybersäkerhetsorganisation genom inkorporering av ISPS-koden. Detta för att designa de olika interna hamnarbetsprocesserna så att dessa också stödjer deras cybersäkerhet (Senarak, 2020).

Enligt Port of Los Angeles (2023) var de den hamn i USA som var först med att skapa och etablera en egen ”*Cyber Security Operations Center*” där denna organisations mål och syfte är att verka som en central enhet som övervakar hamnens cyberstatus. Port of Los Angeles beskriver att målet är att förhindra och oskadliggöra möjliga hot och attacker innan de fått verklig påverkan på hamnen operation (Port of Los Angeles, 2023). Hamnen var också först med att få en ISO 27001 certifiering (Port of Los Angeles, 2023).

3. METOD

Forskningsmetoden kvalitativ metod beskrivs nedan. Samt studiens val av fallstudie som metod och urval av intervjuobjekt för de semistrukturerade intervjuerna. Vidare beskrivs insamlingen av primärdata från intervjuerna och hur informationen från intervjuerna har analyserats för att presenteras i studiens resultatdel. I senare delen av studien under diskussionskapitlet granskas metoden i en metoddiskussion utifrån syftet att ge reliabilitet och validitet för studien.

3.1 Kvalitativ fallstudie

Kvalitativ metod samlar in data för att vidare undersöka, förklara och beskriva olika fenomen. Den data som samlas in behöver analyseras för att på ett bra sätt ge insikt i området som forskas inom (Hammond & Wellington, 2020). Kvalitativ metod tar fram data som är i icke-numerisk form, exempelvis i form av bilder, texter och ljud (Hammond & Wellington, 2020). Denna undersökning använder sig av kvalitativ fallstudie för att djupdyka i specifika organisationers syn på cybersäkerhetsarbete.

Fallstudie är en forskningsstrategi vars syfte är att presentera ett detaljerat utfall av det som undersöks (Bryman, 2018). Bryman (2018) förklarar att fallstudien ska skilja mellan det som utreds i fallet och syftet med uppsatsen. Fallstudien utgår från att utreda hur specifika hamnar och organisationer arbetar med cybersäkerhet för att nå fram till studiens syfte att undersöka hur svenska hamnar förhåller sig till hantering av risker och hot vid cyberattacker. Fallstudien är lämplig som metod för att uppfylla syftet att få en övergripande förståelse kring ett ämne, i detta fall hamnars cybersäkerhetsarbete.

Vid undersökningen har fallstudie ansetts lämpligt då cybersäkerhet som ämne har egenskaper som kräver ett metodval där möjlighet ges till att forma ramverk för hur fallet ska utredas. I grunden från teoridelen i studien har intervjufrågor formats för att ge möjlighet till insamling av data till fallstudien. Fallstudien utförs med hjälp av att undersöka två större svenska hamnar och en IT-leverantör verksam inom cyberlösningar för den maritima sektorn.

3.1.1 Semistrukturerad intervju

En kvalitativ metod för datainsamling är intervjumetoden. Källan till svar blir den tillfrågade individen som svarar på forskarens frågor. Intervjumetoden är en lämplig form för att samla in data vid mindre forskningsprojekt och är den metod som passar bäst vid undersökning av komplexa frågor, exempelvis där den tillfrågade besitter erfarenhet kring ett ämne, eller även har specifik information inom ett område (Denscombe, 2018).

Undersökning använder sig av semistrukturerade intervjuer för att tillåta intervjuaren att forma en lista med ämnen och frågor som ska besvaras. Det ges möjlighet för flexibilitet i ordning av hur ämnen och frågor ska avverkas i en semistrukturerad intervju och den intervjuade ska ha möjligheten att utveckla sina svar utöver endast simpla svar på frågorna. Den tillfrågade ska vara i fokus och ska ha möjlighet att visa på sina kunskaper och syn på ämnet (Denscombe, 2018).

3.2 Insamling av data

Primärdata och sekundärdata är de två huvudsakliga tillvägagångssätten som finns vad det gäller insamling av data. Sekundärdata är data som genereras genom analys av data från tidigare studier inom ett visst ämne. Det finns flertalet fördelar med sekundärdata, där forskaren sparar både tid och arbetskraft (Hammond & Wellington, 2020). Primärdata i sin tur är data som vi

direkt har införskaffat hos källan i sig, via exempelvis intervjuer (Denscombe, 2018).Studien kommer använda sig av båda tillvägagångsätten för att skapa ett tillförlitligt resultat.

3.2.1 Primärdata

Arbetet använder sig av kvalitativ metod, där datan baseras på semi-strukturerade intervjuer med relevanta respondenter inom de tillfrågade hamnorganisationerna samt IT-leverantören. Detta med avsikt att undersöka deras arbete kring cybersäkerhet. I analysen av sekundärdata formas frågorna som kommer tas med vid intervjutillfället. De frågorna kommer bygga på de olika lagrum som hanterar säkerhet, samt rekommendationer från NIST, IMO och ISO.

Syftet med att använda oss av kvalitativ metod med semi-strukturerade intervjuer grundade sig i att de svar vi söker endast finns hos ett fåtal verksamheter/personer. En kvantitativ metod med exempelvis massutskick av enkäter hade inte hjälpt studien att nå sitt syfte och resultat.

3.2.2 Sekundärdata

Teoridelen samt bakgrund grundar sig i sekundärdata kring tidigare cyberattacker som har påverkat hamnar. Teorin bygger vidare med hjälp av undersökning av lagar och direktiv samt olika rekommendationer som finns för att motverka attacker och minska risker i hamnar och terminaler. Sekundärdatan bygger även på tidigare studier inom området. Den litteratur som bidragit till dessa kapitel har samlats in från databaserna Chalmers bibliotek och Scopus. Med hjälp av sökord som ”cyber security”, ”ports”, ”shipping”, ”ISO27001”, ”resolution”, ”cyber security in ports”, ”cyberattacks in ports”, ”digitalisation in ports” har författarna fått tillgång till relevanta artiklar och information kring ämnet. Sökningar har också gjort med funktionerna ”AND” och ”OR” som gjorde att fler källor kunde hittas.

Med dessa databaser som grund och med faktumet att de artiklar som tagits del av är peer-reviewed, erhålls bra kvalitét och trovärdighet från materialet.

Datainsamling har också utförts genom att granska lagrum, nyhetstidskrifter samt riktlinjer. Författarna har lagt stor vikt i att utvärdera de källor som sträcker sig ifrån att inte vara peer-reviewade, och således inte samlats in från de tidigare nämnda databaserna. Information och data om lagrum och riktlinjer har samlats in ifrån de utgivande organisationernas samt riksdagens egenförvaltade hemsidor. Organisationerna och riksdagen erhåller ett gott renommé och författarna ansåg den delade datan och informationen från dessa som relevant för att svara på studiens syfte och frågeställning.

Insamlingen av information från hemsidor gjordes av författarna med vetskapen att den kan vara svår att validera i viss bemärkelse. I och med detta så strävade författarna att tillämpa krossvalidering av den information som erhölls. En klar majoritet av den data som delats ifrån hemsidor kunde också styrkas ifrån andra källor. Även nyhetsartiklar som använts i datainsamlingen styrks av peer-reviewed forskning.

Anledningen till att använda material som inte är peer-reviewed forskning grundades med anledningen att ge en djupare förståelse med information som ger kontext till det ämnet som behandlas. Detta till skillnad från inhämtad data från peer-reviewed forskning som ofta mer fokuserar på resultat och slutsatser.

3.3 Urvalsmetod

Vid urval tas ett strategiskt beslut att endast fokusera på en del av populationen. Fokuset ska ligga på att samla in data från de medlemmar i populationen som anses bringa bäst information. Detta kallas för subjektivt urval och innebär att urvalet handplockas utifrån deras relevans och kunskap inom området som undersöks (Denscombe, 2018).

3.3.1 Val av organisationer för undersökningen

Valet av organisationer grundar sig i att försöka besvara de frågeställningar vi har presenterat i studien. Dessa frågeställningar är riktade på ett tydligt och rakt sätt mot organisationer som bedriver hamnverksamhet och vad dessa gör för arbete för att stärka deras cyber-motståndskraft. Av denna anledning har studiens skribenter valt två aktörer inom hamnverksamhet på den svenska kusten samt ett företag som specialiserar sig på IT-lösningar och IT-säkerhet riktat mot sjöfarten. Hamnarna är både en större hamn som är verksam inom alla sorters lastsegment, och en mindre hamn där en viss typ av lastsegment används. Storleken på dessa hamnar är således olika och detta kan medföra en intressant skildring av att se hur de arbetar, om de är lika, eller olika, i deras cybersäkerhetsorganisationer inom respektive företag.

Valet av företaget som specialiserar sig inom IT-lösningar för sjöfartsbranschen var för att få en utomståendes parts insikt om vad trenden är gällande cybersäkerheten inom sjöfartsnäringen samt för att undersöka hur de i sin tur arbetar med cybersäkerhet.

3.3.2 Val av deltagare för intervjuer

Vid kontakten med dessa organisationer och företag föll det sig naturligt att respondenterna blev de som i sina tjänster arbetar med cybersäkerhetsfrågor inom verksamheten. Det resulterade i att författarna tog kontakt med de individer som besitter kunskapen om ämnet. Detta grundades utifrån respondenternas arbetstitel och efter samråd med deras verksamhet. Författarna blev därefter hänvisade till lämplig respondent. Genom att respondenten besitter rätt erfarenhet och kunskap för att besvara frågorna ges det en tydlig validitet för att primärdatan ska vara användbar för studien.

Tabell 1: Sammanställning av intervjurespondenter

Respondent	Befattning	Företag/Organisation
1	IT-chef	RoRo-hamnen
2	IT-chef	Multi-purpose hamnen
3	CEO	IT-leverantören

3.4 Genomförandet av intervjuer

Vid utförandet av en intervju samlas data in med hjälp av frågor ställda av intervjuaren. För att få den frihet som behövdes vid insamlingen av data användes semi-strukturerad intervju, som enligt Denscombe (2018) leder till att studien på ett bra sätt kan få svar på huvudfrågorna men även ge utrymme för följdfrågor efter hand. Enligt Denscombe (2018) ska intervjufrågorna grundas i studiens frågeställning. Genom att utgå från frågeställningen tillsammans med den teoretiska delen som baseras på regelverk, rekommendationer och lagar formades ett frågeformulär. Frågorna delades in i olika kategorier, där det fanns huvudrubriker för att täcka in olika delar i frågeställningen, utifrån hamnens situation, åtgärdsplaner, lagar och riktlinjer. Eventuella följdfrågor utifrån vilka svar författarna kunde få formades också, där exempelvis en huvudfråga kunde vara: ”Arbetar ni utifrån någon av IMO, NIST eller ISOs riktlinjer?” Vid

eventuellt svar som: ”Ja, vi arbetar utifrån IMO”, kunde följdfrågan vara om hur respondenten tolkar IMO:s riktlinjer angående punkter som identifiering av risker eller hur de arbetar med skydd mot dessa risker med hjälp av riktlinjerna från IMO. Och om svaret var nej på ovan fråga blev en naturlig följdfråga ”varför jobbar ni inte mot några av dessa rekommendationer och regelverk?”

För att kunna analysera de frågor som besvaras rekommenderar Denscombe (2018) att intervjun ska spelas in för att ge möjligheten att transkribera materialet. Transkribering är ett väldigt tidskrävande arbete men är nödvändigt enligt Denscombe (2018) för att ge möjligt till god dataanalys i efterhand. För att studien skulle bli så tillförlitlig som möjligt tillämpades denna arbetsmetodik för samtliga intervjuer.

Efter att ha fått kontakt med olika respondenter bokade författarna tillsammans med respektive respondent in möte för intervjuer. Båda hamnarna ville genomföra mötet på distans, vilket ledde till kontakt med hjälp av det digitala programmet Microsoft Teams. Mötet inleddes båda gångerna med kort beskrivning av oss själv samt en presentation av respondenten, för att sen ta tag i de formade intervjufrågorna. Då författarna redan varit i kontakt med respondenten via mailkorrespondens hade det redan förklarats vad syftet med studien var, vad den handlar om samt vad författarna i breda drag var ute efter. Detta gav en möjlighet för respondenten att i stora drag vara redo för intervjufrågorna. Frågorna delades upp mellan skribenterna av studien och ställdes i tur och ordning till respondenten. I vissa fall fångade respondenten in flera svar på kommande frågor i mer utmålande svar av en fråga, vilket gav möjlighet till flexibilitet i följden av intervjufrågorna.

Mötet med IT-leverantören skedde till skillnad från de andra intervjuerna på plats hos företaget. Detta gav en annan insyn i företagets organisation men öppnade även upp för större delar av samtal som kretsade strax utanför fokusområdet för forskningen, då respondenten gärna visade upp hela företaget i sin helhet, även de delar som inte berörde cybersäkerheten. Även denna intervju spelades in för att sedan transkriberas för att kunna vidare analyseras enligt Denscombe (2018).

3.4.1 Analys av intervjudata

Enligt Denscombe (2018) bör transkribering av materialet från intervjun ske snarast möjligt efter intervjutillfället för att ge författarna god möjlighet att minnas specifika detaljer från intervjun. För att ge god kvalité till vår dataanalys transkriberade författarna intervjumaterialet tätt efter intervjuerna. För att ge god möjlighet till att analysera den insamlade datan på korrekt sätt skrevs transkriberingen på ett levande sätt med fetmarkerad text på viktiga delar, kursiv text vid våra frågor, samt citationstecken när respondenten på ett särskilt sätt uttryckte sig. Detta gav författarna möjligheten att även i efterhand läsa texten och få en god förståelse för på vilket sätt vissa saker sas för att innebörden ska fångas på ett korrekt sätt. Detta i enlighet med hur Denscombe (2018) beskriver att innebörden och meningen med respondentens svar är huvudpoängen.

Efter att transkriberingen utförts följdes det angreppssätt som Bryman (2018) beskriver, med att läsa igenom texterna ett par gånger för att familiera oss med innehållet samt för att bibehålla minnet av den kontext som intervjun hölls i. Detta gjordes enligt Brymans första steg i den tematiska analysen, där det är viktigt att göra sig bekant med allt material. Författarna valde efter det att analysera det transkriberade materialet med hjälp av en tematisk analysmetod. Enligt Bryman (2018) ska forskaren i steg två av tematisk analys inleda kodningen av materialet. Vid granskning av det transkriberade materialet användes en mängd sökord för att

på ett effektivt och genomgående sätt analysera materialet. Sökorden valdes från att gå djupare ner i de olika delar som bygger upp vår frågeställning. Detta resulterade i sökord i form av de olika lagrummen och riktlinjerna som nämnts, cybersäkerhetsorganisations relaterade termer och åtgärdsplaner, sökorden nämns nedan som koder i tabellen (se tabell 2). Enligt Bryman (2018) ska forskaren i det tredje steget av tematisk analys bryta ner antalet koder till större teman. Författarna markerade därför dessa stycken samt meningar som fångade in dessa koder, och delade in de olika koderna i specifika delteman för att ge möjligheten att namnge teman och dela in de i olika nivåer. Genom att strukturera det transkriberade materialet på sådant vis kan författarna i och med det navigera och referera i materialet på ett effektivt sätt. Bryman (2018) beskriver i det fjärde steget att genom att namnge och sätta etiketter på delteman ges forskaren möjligheten att knyta an de olika koderna till undersökningens fokus. I det femte steget läggs fokus på att koppla samman olika begrepp som kan falla in under samma tema, exempelvis där författarnas analys visar att ena respondenten pratar om riktlinjer och den andra respondenten om rekommendationer, men de syftar på samma tema. I det sjätte och sista steget av den tematiska analysen ska forskaren enligt Bryman (2018) koppla sina teman till forskningsfrågorna, samt kunna försvara och förklara varför dessa specifika teman har valts. Forskarna har i detta skede kopplat de olika temana direkt till forskningsfrågorna och studiens syfte, för att efter analysen kunde presentera det mest relevanta resultatet utifrån det material som samlats in från intervju-tillfällena.

Tabell 2: Tematisk dataanalys enligt Bryman (2018)

Koder	**Deltema**	**Tema**
Restore Backup Redundans Policy Reservrutiner Tekniska system Reservlösningar Störningar Lösningar	Cybersäkerhetsskydd IT-systemskydd	Åtgärdsplaner
IMO ISPS MSB NIS ISO CIS Controls	Regler Riktlinjer Lagrum Rekommendationer	Lagkrav & riktlinjer
System Kommun Ägandeform Tillväxt Digitalisering Organisationer Teknisk utveckling	Nuläget Syn på säkerhet	Hamnens situation

3.5 Etik

Enligt Bryman (2018) finns det flera centrala områden som berör etik i en vetenskaplig undersökning. Den första är om respondenten i en undersökning kan komma till skada eller uppleva obehag på grund av sin medverkan i studien, en annan etisk princip är om forskningen

inkräktar på privatlivet hos respondenten. Båda dessa aspekter anses av forskarna ha god etik, då forskningen inte syftar till att redogöra för personliga ting som åsikter, personlighet eller i någon vinkel avslöja personliga detaljer om respondenten i fråga. Andra stora delar i det etiska perspektivet handlar om informationskrav, samtyckeskrav samt konfidentialitetskrav och nyttjandekrav. Dessa aspekter syftar till att forskaren ska göra respondenten medveten om syftet med undersökningen och delge olika moment som ingår i studien. Genom att vara öppna har författarna gett respondenterna tydliga riktlinjer i vad undersökningen handlar om och vad deras roll som respondenter är. Samtycket, konfidentialiteten samt nyttjandekravet berörs av forskarna genom att tydligt fråga om tillåtelse där vi formulerat oss utifrån etiska mallar från Bryman (2018) på följande sätt inför intervjuer:

”För att veta mer om hur er organisation och verksamhet arbetar med cybersäkerhetsfrågor vill vi som studenter vid Chalmers Universitet göra en intervju med er. Är du villig att medverka vid en intervju så kommer vi att spela in samtalet och i ett senare skede transkribera samtalet för att kunna analysera den insamlade datan från intervju-tillfället. Intervjun kommer att pågå i drygt en timme och all information som presenteras i intervjun kommer att användas enbart i forskningssyfte. Vi kommer utgå från intervjun när vi skriver resultat och använda oss av citat från intervjun. Dina svar kommer vara anonyma och presenteras i resultatet för studien under namnet ”respondent”

Eftersom samtliga respondenter varit medvetna om syftet med intervjuerna och varit villiga till intervjuer anses forskningen ha god etik utifrån dessa aspekter.

4. RESULTAT

Resultatet presenteras utifrån det material och den data och som samlats in från de semi-strukturerade intervjuerna. För att på ett lämpligt sätt presentera den data som samlats in är resultatdelen indelad utifrån de olika respondenterna. Ordningen är satt till den ordning intervjuerna utfördes och varje respondents data är uppdelat i olika segment för att på ett tydligt sätt presentera resultatet.

4.1 RoRo-hamnen

Det första intervjuobjektet var en större RoRo-hamn (hamn som hanterar rullande gods) i Sverige. Efter mailkorrespondens med hamnens säkerhetsansvarig bestämdes det att hamnens IT-chef skulle vara respondenten för intervjun, för att på bästa möjliga sätt delge oss den information och dela den kunskap som hen besitter i ämnet.

4.1.1 Hamnens situation

Respondenten inleder med att förklara att hamnen ägs till 100% av kommunen som hamnen befinner sig i. Kommunen äger även flera andra bolag och i samband med alla kommunens förvaltningar är de sammanlagt fem bolag och sju förvaltningar som använder sig av samma tekniska plattform. Hamnen arbetar enligt respondenten under samma nätverk, servrar och säkerhetsnivå som alla andra inom kommunen. Enligt respondenten innebär detta att de 135 användarna som arbetar i hamnens IT-system lyder under samma regler som drygt 6000 andra användare i kommunen.

För att ge en bakgrund till den tekniska utveckling och den digitalisering som sker beskriver respondenten att de senaste 10 åren har de haft i snitt en 7%-ökning varje år av gods som hanteras av hamnen. Nyckeln till att hantera denna påtagliga tillväxt förklarar respondenten ligger i att använda ny teknik.

”Vi har implementerat nya nätverk, nya uppkopplingar, intelligenta gate-system, intelligenta terminalsystem, allt detta underlättar för oss som jobbar i systemet att få upp informationen, kunna ta ett beslut som bara en människa kan göra, trycka på en knapp, PANG. Så tar systemet hand om resten.”

Respondenten ger en tydlig bild av att nyckeln till att hantera dessa ökade volymer inte ligger i att anställa fler, då de sedan han anställdes 2009 i princip har varit lika många anställda under alla dessa år, utan om att ständigt utveckla den tekniska delen av hamnen.

4.1.2 Åtgärdsplaner

Denna tekniska utveckling leder till frågan om riskerna med att arbeta mycket med digitalisering, teknik och IT, och hur hamnen förlitar sig på dessa funktioner.

Respondenten förklarar att detta är en stor del av deras arbete. Vid beskrivning av reservrutiner som finns i hamnen är skillnaden enorm från när 2009 när IT-chefen anställdes. Då var reservrutinen att vid eventuella problem med de tekniska systemen övergick arbetet till att utföras med papper och penna. Då hamnens huvudsakliga syfte är att lasta och lossa gods från fartyg, gick hamnarbetarna enligt respondenten runt manuellt utan hjälpsystem och bockade av manuella papperslistor, *”den var lastad, den var klar, den ska också lastas”.* Det här systemet har lämnats och vid störningar av de tekniska systemen idag går hamnen aldrig längre tillbaka

till manuella listor. Nu bygger reservlösningar i stället på redundanta anslutningar, att när något system börjar krångla tar ett annat över.

”När vi pratar säkerhet så finns det ju två sidor av säkerhet, den ena är den interna, att vi som jobbar här kan öppna upp oss eller exponera oss eller göra nånting fel, men sen finns det ju även dem utifrån.”

Respondenten beskriver hur det finns två olika sätt att tolka ett cybersäkerhetshot. Den interna delen, där respondenten belyser att individerna själva inom organisationen skulle kunna göra fel. Där kan det handla om brist i försiktighet med sitt lösenord, öppnade länkar som leder till att virus eller andra skadliga program sprider sig inom systemet, men respondenten belyser även den sortens cybersäkerhetsrisk där hotet kommer utifrån.

I den tekniska utveckling som hamnen kontinuerligt genomgår beskriver respondenten att det genomförs utbildningar för e-learning med jämna mellanrum. Det är en del av hamnens säkerhetspolicy och innehåller kunskap och utbildning om säkerhetsaspekten för IT-systemen. Detta görs enligt respondenten för att kunna minimera risken för exempelvis intrång i systemen. Respondenten beskriver säkerhetsarbetet som en lök där varje lager skyddar verksamheten, där ett lager är lösenordshantering, ett annat lager är filter för att hålla bort specifika mejl, ett tredje lager är brandvägg för att skydda mot intrång.

”Det här blir ju lager på den här löken då, det blir ju väldigt jobbigt, men samtidigt ***blir det väldigt säkert här innanför bubblan****”*

Som omnämndes tidigare är RoRo-hamnen 100% ägd av kommunen den är verksam inom. Med detta ansvarar inte hamnen i sig själv över deras direkta cybersäkerhet. Det är i stället kommunen som tillhandahåller cybersäkerhetslösningar för samtliga av kommunens förvaltningar.

”Som jag sa så är det så att jag beställer inga säkerhetssystem själv till … hamn, det enda jag beställer själv till min hamn det är sånt som är specifikt för min verksamhet. Alltså terminalsystem, gatesystem, o mitt affärssystem, som fakturerar här. De här tre här är ju inte en del av kommunens plattform, det är ju mina system. Men allting som har med brandväggar, eller säkerhet att göra, det är ju gemensamt för kommunen.”

Respondenten förklarar att en stor del av deras åtgärdsplan är riskanalyser. Att kontinuerligt arbeta med dem gör att de hittar risker och kan arbeta med eliminering och minimering av dem.

”Så varenda år så tittar man genom den här riskanalysen och gör om den och alla systemen jag har, är då dokumenterade där vi har sagt, vilken data finns där, vilka risker finns där, vilka åtgärder ska vi göra ifall nåt/nån av de här riskerna blir aktiva”

IT-chefen belyser ett exempel där deras beredskapsplan aktiverades. Händelsen inleddes av att verksamheten drabbades av ett ransomware som krypterade och låste filer på en gemensam hårddisk. Respondenten förklarar att de i samband med attacken krävdes på en lösensumma för att återställa filerna.

”… meddelande att om inte vi betalar X pengar så skulle vi inte få tillgång till våra filer.”

Respondenten förklarar vidare att i deras säkerhetspolicy står det att de aldrig ska betala sådana krav, och de gick i stället vidare med sina rutiner vid en attack. Rutinen innebär att den attackerade hårddisken kopplades bort från nätverket, vilket i sin tur kopplade bort hela hamnen från det andra nätverket inom kommunen. Efter detta rensades först den drabbade datorn på det skript som hade

smittat den, sedan resten av berörda datorer på nätverket och samtliga klienter skannades och rensades. Den attackerade hårddisken raderades totalt och återställdes till senaste säkerhetskopian ifrån tidigare natt.

Respondenten förklarar att detta intrång upptäcktes på förmiddagen och på eftermiddagen var verksamheten fullt funktionell igen.

En av de mer viktiga åtgärderna för att bibehålla säkerheten för hamnens olika system är att de har redundanta brandväggar, som går igenom all inkommande datatrafik. Brandväggarna arbetar i par vilket enligt respondenten innebär att det inte går att överbelasta, då de samarbetar med varandra.

4.1.3. Förbättringsområden

IT-chefen förklarar att verksamhetens säkerhetsarbete till stor del styrs av den ekonomiska faktorn. Efter att riskanalyser har utförts beskriver respondenten att på beslutande nivå finns det en tendens att säga *”japp, jag har identifierat att om jag vill ha min internetanslutning uppe 24/7, 365 dagar om året då kostar det 100 000 extra”.*

Respondenten förklarar att ledningen i det läget gör en avvägning där de bara är beredda att betala 50 000 extra för att höja säkerhetsnivån, vilket leder till en lägre budget för säkerhetsarbetet.
Där möts alltid säkerhetsnivån med budgetnivån enligt respondenten, att identifieringen av risker och hot är en sak, och att faktiskt lägga den budgeten för att bibehålla exempelvis redundans för systemet på 100% inte alltid är prioriterat.

Respondenten refererar till tidigare nämnd ransomware-attack och förklarar att den attacken gick genom säkerhetssystemet på grund av ett icke-uppdaterat antivirus-program på en av klienterna. Då den senaste definitionen av programmet saknades öppnades det en möjlighet för ett ransomware att smitta hårddisken vilket ledde till de krypterade och skadade filerna.

IT-chefen förklarar att framsteg och förbättringar kommer när verksamheten efterfrågar mer. Ny teknik används inte för sakens skull, utan investeringar sker när verksamheten ser behov av det.

4.1.4. Regler och riktlinjer som iakttas

Respondenten förklarar att hamnen arbetar enligt kommunens riktlinjer. Kommunen har ett ledningssystem för informationssäkerhet som baseras på ISO 27001.

”Det finns ett ledningssystem för informationssäkerhet inom kommunen, där det är specificerat klart och tydligt hur det här ska gå till, och vi följer ju den fåran. I dem ingår det ju riskanalyser, och de har ju också de här rollerna som ni nämnde”

”… kommun har ju ett lease, alltså ett ledningssystem för informationssäkerhet. Den följer vi.”

Respondenten beskriver att kommunen som äger hamnen har en säkerhetsavdelning som respondenten i sin roll som IT-chef samarbetar nära tillsammans. Där syftet är att följa kommunens processer för att utföra de olika steg som krävs för att uppfylla de regler och riktlinjer som finns i ledningssystemet för informationssäkerhet, bland annat genom att utföra riskanalyser för hamnen.

Respondenten förklarar att kommunens ledningssystem kontinuerligt har revisioner mot sig, där verksamheten blir granskad utifrån. Där revisionen utvärderar den kommunala verksamheten, och granskar deras arbetssätt kring IT.

”… det gör de ju kontinuerligt, och även IT, och IT-säkerhet och informationshantering, allt det här blir utsatt för revision.”

”Vi sitter i ett väldigt stabilt och robust system och vi har bra rutiner, bra processer.”

IT-chefen förklarar att hamnen är en strategiskt viktig hamn och därför arbetar nära med Myndigheten för samhällsskydd och beredskap, (MSB). Samarbetet syftar mest till att hamnen måste rapportera till MSB, om incidenter, hot och attacker som hamnen utsätts för.

”Alla incidenter ska inom en viss tidsram rapporteras till MSB”

Utöver säkerhetsarbetet för den digitala informationssäkerheten där hamnen arbetar via kommunens processer beskriver respondenten att det även finns en fysisk aspekt att ta hänsyn till när det gäller säkerheten. Hamnen lyder under ISPS-koden och där beskriver respondenten att hamnen ansvarar för sina egna rutiner. I hamnen finns det en säkerhetschef som arbetar över en säkerhetsavdelning som bevakar all fysisk aktivitet i terminalerna. Respondenten förklarar att det rör sig om trafikrörelser från båtar, tåg och rullande trafik samt även det fysiska skalskyddet, grindar, bommar och passeringar. IT-chefen beskriver att samtliga personer som blir insläppta på området har blivit kontrollerade och har rätt att befinna sig där. På området finns det teknikhus som har delar av IT-systemet, strömförsörjning till system, switchar etc. Respondenten beskriver vidare att de mer viktiga delarna som server-rummet finns i själva hamnkontoret som utomstående ej har tillgång till. Respondenten belyser även säkerhetsnivån kring detta, då det dels är låsta rum som är otillgängliga, men att det även finns ytterligare ett skydd där vid försök av att koppla in utomstående utrustning i dessa system ignoreras utrustningen och nekas kontakt med resten av nätverket.

”… det ger liksom ingenting att koppla in någon liten grej i vår switch, man får ingen kontakt ändå”

Respondenten klargör att den fysiska cybersäkerheten är minst lika viktig som den virtuella, men att verksamheten likt den virtuella aspekten även här arbetar i flera-lager-principen. Först se till att det inte händer, men om det händer ska det finnas ytterligare skydd.

4.2 Multi-purpose hamnen

Respondenten arbetar som IT-chef på hamnorganisationen. Multi-purpose hamnen är en stor hamn som är verksam inom flera olika slags lastsegment. Staden där hamnorganisationen är verksam äger också hamnmyndigheten i sin helhet.

4.2.1 Hamnens situation

Respondenten börjar med att förklara hur hamnen över en tioårsperiod fått en betydligt motståndskraftigare organisation i förhållning till den fysiska säkerheten. Respondenten beskriver att cyber- och informationssäkerhet relativt nyligen hade hamnat under dennes ansvar inom organisationen. Respondenten nämner att detta ansvarsområde har varit på olika håll inom verksamheten tidigare, men inte fallit riktigt väl ut. Respondenten grundar detta i att denna uppgift har legat för långt ifrån avdelningarnas fokus.

”Av två anledningar tror jag, den ena är … att det har varit för långt ifrån de avdelningarnas fokus, de man själv mäts på som chef så att säga. och med mäts på så menar jag uppdraget, vi har ju inga incitamentsmodeller så att man tjänar liksom inte mer pengar på och göra de ena eller de andra. Men man leverera liksom på de som ligger närmast hjärtat och så har man lite grann fått det här som en bonus …”

Respondenten belyser också vikten av att behålla kompetent och driven personal. Detta kopplas enligt denne direkt till hur framgångsrik man är inom området.

”… man måste ha rätt folk, och de är idag väldigt svårt att behålla rätt folk.”

Vid frågan om respondenten upplevt en speciell händelse eller tidpunkt som avgörande för ett ökat cybersäkerhetsorienterat arbete svarar respondenten:

”Njea de kan jag inte riktigt säga, de är klart att de har trappats upp för att de är mer i, de är fler aktiva grupper idag än va de var för tio år sedan. Men jag har varit på hamnen i snart fem år och under den här tiden, när jag kom in för fem år sedan då hade vi väldigt lite förmåga att se va som knackade på vår port liksom. Vem försökte och vad försökte man med. Vi var relativt blinda då. och de har ju gjort att vi har insikter idag som inte alls hade för fem år sedan. Men i takt med att vi fick de här förmågorna, vi skaffat oss hjälpmedel och tagit hjälp av externa partners som vi vill kanske ha haft en förmåga i tre, tre och ett halvt år ish. Under den perioden, för de är egentligen den jag kan redogöra, innan de var de betydligt mer av ett svart hål.”

Respondenten nämner att dennes organisation, ihop med ett nätverk av andra organisationer, har en viss omvärldsbevakning gällande cyberattacker för att granska hotnivån de befinner sig på. Denna omvärldsbevakning resulterar i att hamnen kan gå upp, eller gå ned, i beredskap beroende på vad granskningen ger för resultat.

4.2.2 Åtgärdsplaner

Respondenten beskriver också att det finns strukturer och arbetssätt som implementeras vid bortfall av centrala och viktiga system. Där man vid bortfall av ett sådant system aktiverar en procedur som skall tillhandahålla en lösning vid bortfall av IT-systemet i fråga. Respondenten beskriver att detta fungerar till viss grad men att det blir svårare och svårare idag. Respondenten beskriver hur man tillfrågat chefer inom organisation om hur viktigt ett visst system är för dem i deras dagliga operation. Svaren var svåra att få fram men det slutade med att de tillfrågade cheferna sa att de skulle de klara sig utan systemet i fråga i två veckor. Som av en händelse försvann en mejlklient från systemet ett par dagar efter denna fråga ställdes och detta resulterade i totalt kaos inom organisationen. Felet gick fort att åtgärda, men den inträffande händelsen belyser också den okunskap som var rådande inom organisationen när frågan först ställdes.

”Vi lärde oss av den, de va något så otroligt fånigt och enkelt så att vi har alltid efter det pratat om svarta skärmar i de här workshopparna. asså alltså att datorn blir svart. Ingenting finns, det finns inget IT-stöd. Och när vi gjorde de i stället då blev folk vita i ansiktet och började säga "kan de hända?””

Respondenten beskriver att man med hjälp av dessa procedurer skall klara sig utan IT-stöd. Men belyser även att det kan vara mer invecklat, till exempel att systemen kanske hänger ihop med mejl, telefon, webbsida och liknande. Respondenten nämner också att man inom deras organisation fokuserar mycket på funktionen av återställande av de olika systemen där man på månads-, kvartals- och årsbasis gör olika tester för att se till att leverantörerna av dessa system kan återställa systemen på ett effektivt sätt.

”Vi jobbar med restore tester varje månad, där vi testar leverantör, … Månads-, kvartals- och årsbasis kan jag säga, för vi gör olika tester. Varje månad så provar vi att vi kan läsa tillbaka filer, varje kvartal så provar vi att man kan läsa även databaser och två gånger per år att man kan läsa tillbaks hela system, som att en hel server, ett helt system har blivit taget eller försvunnit.”

Respondenten belyser vidare att de kan initiera rutiner vid totalt bortfall av IT-system. Dessa procedurer är placerade i vad hen kallar ”röda pärmar”. Dessa pärmar är innehållande av rutiner och procedurer som kan användas vid ett totalt haveri av ens virtuella system, vare sig de kommer ifrån ett cyberangrepp, strömbortfall eller att internetuppkopplingen försvunnit.

”Vissa system, som är väldigt väldigt viktiga, där har vi en kontinuitetsplan som säger att det måste finnas röda pärmar kallar vi det, och det är en last resort, där ska vi klara oss utan IT stöd.”

Utöver att arbeta med åtgärdsplaner görs även proaktivt arbete inom hamnen för att utbilda personal angående problematiken kring cyberhot. Respondenten förklarar att all personal genomgår obligatorisk utbildning kontinuerligt. Detta för att vara medvetna om hur de kan undvika att drabbas av eventuella intrång via till exempel mejl.

”User-awareness är superviktigt tycker vi ju för tekniska skydd gör det så svårt att ta sig in i en miljö idag så att man gör det ju oftast genom en människa, man försöker lura någon av oss.”

Respondenten upplyser också om att denne försöker nu införa så kallade ”*dry-run*” övningar, eller skrivbordsövningar. Ambitionen med dessa övningar är att testa kris-hanterings färdigheterna hos de ledande personerna inom organisationen. Detta för att i viss mån bli familjära vid sådana situationer, men också för att kunna utvärdera själva övningen och således se vad för aspekter som fungerar bra, och vilka som behöver ses över.

”*... att göra en skrivbordsövning där vi har en spelledare från en leverantör, vi kommer då ha ett scenario där vi råkar ut för en attack ... vilka vi ska kontakta, hur funkar kris-ledningen för sånt här*”

4.2.3 Förbättringsområden

Respondenten iakttar själv att de inom organisationen fortfarande har en lång väg kvar vad det gäller cybersäkerheten.

”För det är en katt- och råtta-lek med det här, och vi ligger alltid efter”

Hen förutspår också att man inom fem år kommer att ha erfarenhet om att ha blivit utsatta för lyckade intrång, och belyser även att hen tror att det är naivt att tro något annat.

”Men jag tror det är naivt att tro att vi kommer klara oss helskinnade för rätt som det är ... det är ett alldeles för komplext område så man kan inte tänka på allt, ...”

Respondenten nämner också som sista del av intervjun att denne tror att det är jätteviktigt att vara pragmatisk. Hen belyser att det finns bra ramverk och regelverk, men att det är viktigt att ta i beaktning att de som faktiskt jobbar inom organisationen är de som skall utföra det skyddande arbetet.

” ... men jag tror att det viktigaste är att vara pragmatisk och inte fastna i analyze, paralyse.”

Respondenten belyser också det faktum att deras cybersäkerhetsorganisation skiljer sig ifrån de större hamnnoderna i världen. Respondenten berättar att dessa hamnar har upprättat egna

”*Cyber Defence Centers*” där de aktivt sitter och analyserar omvärldshot samtidigt som de sitter och bryter ner kod för att klargöra vem, eller vilka, som spridit denna programvara.

”… så de är bara för att ge en bild då att de har ju liksom hundra pers där vi har en 20% heltid.”

Respondenten belyser också en situation denne finner talande för en organisations oförmåga att inse vilka följder det kan bli efter ett cyberattentat. Respondenten nämner att denne satt i ett möte med individer som jobbar på olika avdelningar runt om i verksamheten. Tanken med detta möte var att diskutera eventuella följder vissa cyberincidenter kunde få på organisationen. Dessa olika avdelningar landade i att de kunde klara sig ungefär två veckor utan vissa system. Det respondenten finner talande i detta scenario är att bara dagar efter detta möte faller ett system bort, en mejl-brevlåda som används för orderhantering.

”Och jag kan säga att efter 30 minuter så va de fullständig panik i bolaget.”

Respondenten belyser dock att korrekta procedurer initierades och problemet kunde avvärjas inom en timme efter att man märkt att problemet uppstått.

”*Och det var ett väldigt talande exempel tycker jag, två veckor klarar vi oss utan det här, men när det väl bränner till, som tur var det extremt begränsad skala. Vi var ju i gång igen efter mindre än en timme när vi förstod vad som hade hänt.”*

4.2.4 Regler och riktlinjer som iakttas

Respondenten beskriver att hamnen utgår från ISO 27 001 samt en standard som heter CIS Controls. ISO 27 001 är enligt respondenten mer övergripande och beskriver vilka områden som ska arbetas med, samt hur du ska hantera olika teman.

CIS Controls är enligt respondenten ett mer handgripligt ramverk, där det är lättare att följa upp för att mäta de framsteg som görs. Respondenten förklarar att de använder CIS Controls för att stämma av att de gjort rätt saker som ska göras varje månad exempelvis. De utför även en årlig utvärdering på CIS Control-ramverket för att mäta hur deras cybersäkerhetsarbeta förhåller sig till ramverket.

Vid utfrågning kring om hamnen arbetar med IMO:s riktlinjer, ISPS-kodens regler, förklarar respondenten att de inte direkt arbetar med detta, men att dessa riktlinjer och regler passar och faller in under krav från andra mer krävande direktiv. På grund av hamnens signifikans angående Sveriges import och export nämner respondenten att deras verksamhet är påverkade utav NIS-direktivet. Respondenten förklarar att man även har kontakt med MSB, SÄPO, Försvarsmakten, Transportstyrelsen samt Energimyndigheten. Där Transportstyrelsen samt Energimyndigheten har tillsyn på att NIS-direktivet följs upp och svarar mot MSB.

4.3 IT-leverantören

Respondenten som intervjun hölls med är VD för ett företag som tillhandahåller IT-lösningar för den maritima sektorn. Företaget erbjuder kompletta lösningar av ett fartygs IT-behov och erbjuder även support under alla årets dagar. Respondenten var den person som grundade företaget och har således följt organisationen under hela dess resa.

4.3.1 Organisationens situation

IT-leverantören tillhandahåller lösningar inom IT för ett flertal större maritima organisationer där det levereras en rad olika system och program för att säkerställa drift. Respondenten förklarar att deras cybersäkerhet är på en väldigt hög nivå och beskriver en incident som drabbade ett större rederi under senare del av 2010-talet. Vid detta tillfälle levererade respondentens organisation IT-lösningar till en del av detta rederi, och denna del av organisationen fungerade helt utan avbrott under hela cyberangreppet.

”Alla våra … båtar gick ju inte ner. Alla våra funkade. Vi var uppe direkt. Vi hade 100% upp-tid.”

4.3.2 Beredskapsåtaganden / syn på säkerhet inom IT

Respondenten nämner att deras system som används är konstruerat på ett sådant sätt att det enbart skall tillåta system och hemsidor som behövs för att utföra det värdeskapande arbetet i fråga. Respondenten menar att de system, datorer, telefoner och andra digitala lösningar som köps in för att uppfylla en viss funktion i arbetet skall användas uteslutande för arbetet. Respondenten menar att precis som radarn är de lösningar som de som leverantör tillhandahåller ett arbetsverktyg som skall utföra en funktion vid olika arbetsmoment. Respondenten menar på att deras lösningar de levererar kan upplevas stränga, men deras system kommer i och med det att på lång sikt fortsätta leverera och subventionera hög upp-tid.

”… då är det en tråkig burk, men allt funkar varje dag alltid. Det är lika roligt som radarn brukar jag säga. Så vi inte börjar spela MP3 på radarn bara även om det råkar vara en skärm.”

Respondenten förklarar vidare att de olika systemen ombord på ett fartyg omedvetet säkerhetsklassats olika av manskapet ombord. Respondenten ger ett exempel på att det inte skulle komma på fråga att ladda ner olika programvaror på radarn trots att det också är en PC. Men att göra det på bryggdatorn, eller andra jobbrelaterade digitala medier ses enligt respondenten som icke-problematiskt hos besättningen. Det råder alltså en viss slags naivitet hos många där olika system hamnar på olika hierarkiska säkerhetsnivåer trots att de alla fyller en funktion för att på ett säkert och effektivt sätt framföra fartyget.

”Mejl och det här är lika viktigt idag som din radar. Att den ska funka, då är det inte öppet för fria tolkningar, egna skärmbakgrunder…”

Respondenten förklarar vidare i temat angående synen på cybersäkerhet och ger exemplet att en kapten alltid kan välja att köra fartyget till vilken hamn han känner för. Men han kör till den hamn som är utsatt, för där finns det en respekt. Respondenten menar att denna respekt behöver finnas angående IT-systemen och datorerna också. Bara för att det finns möjlighet att använda datorn till nöje, är detta inte syftet med datorn, och därför bör det undvikas.

”Det är som att vi skickar iväg en båt härifrån Göteborg till Rotterdam, men är den kapten sugen på att åka till Immingham så kommer den båten att åka till Immingham, det kan jag garantera”

Respondenten förklarar att de arbetar med beredskapsplaner och att de lägger stor vikt vid att kunna återställa sina system utifrån kontinuerlig backup på systemen. Genom att ständigt spara ner filer i systemet kan de vid en eventuell cyberattack återskapa tidigare system på ett fåtal minuter, där de korrumperade filerna och systemen raderas och återställs genom backupen.

4.3.3 Trenden inom sjöfartsnäringen

Respondenten menar att många organisationer inom sjöfartsnäringen tänker för smalt. Och med det att organisationerna inte tänker på helheten vad det gäller cybersäkerhet.

”… de flesta fokuserar så smalt. "Vi har 10 dörrar i det här huset, jag har ett superbra lås på 9 av dem men en glömmer jag öppen", då spelar det ingen större roll att man har ett jävligt superskydd på resten. Det kanske är bättre att säga att det är 95% på alla dörrarna, …, och det är en riskanalys som görs som vi har tagit”

Respondenten belyser även att denne tycker det är viktigt att konstruera ens cybersäkerhetsorganisation på ett sätt där det inte överdrivs på vissa säkerhetsåtaganden och negligeras på andra, utan att i stället iaktta att det är ett helhetsåtagande som skall utvärderas, att organisationen bara är lika stark som sin svagaste länk.

”*Jag tycker alltid att det går tillbaka till, bygg lagom. Inte överdriva någonstans, men tänk på allt i stället. För att den supergrejen du köpt in, den jättedyra programvaran, du har köpt bästa jävla autocad, du är inte arkitekt för det”*

4.3.4 Regler och riktlinjer som iakttas

Respondenten förklarar att de arbetar enligt ISO 27001 samt följer de riktlinjer som utfärdats av IMO, men påpekar också att de alltid inom företaget har strävat efter högre mål än de som sätts upp av olika organisationer och riktlinjer.

”Ja det har alltid varit så, att det här som de har kommit på, det är mycket lägre.”

Respondenten beskriver vidare deras syn på hur de arbetar, och förklarar att alla de olika riktlinjer, regler och krav som finns angående riskhantering handlar i regel om samma principer. Inled med riskanalys för att sedan utföra arbetet. Respondenten förklarar att olika riktlinjer tillhandahåller liknande strukturerade tillvägagångssätt baserat på de risker som finns, och ramverken från ISO och IMO grundas i att hantera cybersäkerhetsrisker, där fokus ligger på att utföra ständiga förbättringar och stor vikt läggs på att organisationerna regelbundet ska granska och uppdatera sina säkerhetspolicyer, procedurer och kontroller för att säkerställa att de förblir effektiva i sitt arbeta med att begränsa cybersäkerhetsrisker.

”Tänk först, gör riskanalys, sen kör vi”

Respondenten förklarar detta utifrån att det alltid är en balans mellan riskanalys, ekonomisk aspekt, säkerhetsarbete som utförs, och det faktiska arbete som utförs i verksamheten inom de berörda systemen. Där det krävs att det finns ett litet utrymme för att det kan gå fel, men att systemen då ska vara tillräckligt väl konstruerade för att hantera dessa fel.

”Om det skiter sig, vad är din disaster/recovery-plan. För det gör det ju alltid någång, annars får du inte röra nånting”

5. DISKUSSION

I diskussionskapitlet lyfts studiens frågeställningar och vilka resultat som erhållits utifrån dessa, där de baserats på de intervjuer som utförts. Resultatet diskuteras utifrån grunden i den teori och bakgrund som ges i studiens inledning. För att styrka validitet samt reliabilitet ingår en diskussionsdel kring metodiken som använts under studiens gång.

5.1 Diskussion kring resultat

Utifrån studiens frågeställningar har detta kapitel delats upp utifrån de teman som resultatet presenteras i. Genom att jämföra det resultat som erhållits med den teori och de riktlinjer som lyfts tidigare, angående hur hamnar ska arbeta med cybersäkerhet, analyserar vi hamnars förhållning till risker med cyberhot i enlighet med studiens syfte. För att presentera ett bredare perspektiv diskuteras två hamnar utifrån det resultat som samlats in från intervjuer med dem, samt en IT-leverantör för att få en infallsvinkel från ett annat perspektiv. Utifrån tidigare forskning tas det även med en hamn och deras syn på cybersäkerhet.

5.1.1 Hamnarnas situation

Resultat från intervjuerna visar i enlighet med tidigare forskning från Kechagias m.fl. (2022) och Kapalidis m.fl. (2022) att IT-system får en allt större roll inom hamnverksamheter, och att detta i sin tur leder till ett utökat arbete med cybersäkerhet. Det samlade resultatet för studien visar att de tillfrågade hamnarna arbetar aktivt med IT och att de har en stor medvetenhet kring att deras organisation påverkas av denna expandering av IT-användning. Respondent 1 förklarar att deras hanterade volym har växt i snitt 7% under de senaste 10 åren utan att behöva anställa fler. Denna tillväxt förklaras enligt respondent 1 av effektivare system och nyttjandet av ny teknik. Denna förändring har inom båda hamnarna påverkat deras arbete med cybersäkerhet och tänket kring risker och hot har ändrats påtagligt under senare år. Den tredje respondenten IT-leverantören beskriver att efterfrågan på säkra IT-system har ökat och att medvetenheten i branschen är större nu är för några år sedan.

IMO:s resolution MSC.428 (98) (IMO, 2017a) som uttrycker att hamnar och hamnverksamheter ska arbeta med att skydda sina verksamheter mot cyberhot, togs fram för att IMO såg ett behov av öka medvetenheten kring cybersäkerhet. Vilket visar sig i studiens resultat att hamnarna är medvetna om risken från cyberhot och att det är något de behöver arbeta kontinuerligt med i samband med att deras IT-system växer och allt fler funktioner i hamnarna digitaliseras. Detta fokus på cybersäkerhet går också att se på en global basis. PAT i LCP har inkorporerat riktlinjer för stärkande av cybersäkerhet i deras säkerhetsorganisation. Denna trend av ökat cybersäkerhetsorienterat arbete går också att se i Port of Los Angeles där även de stärkt sitt cyberförsvar genom olika åtgärder och åtaganden. Den uppenbara trenden utifrån den sekundära datainsamlingen är att intresset och medvetenheten för cyberförsvar ökar, men att detta också sker på olika villkor och i olika takt. Detta utökade intresse för att arbeta med cybersäkerhet stärks av tidigare forskning som visar att antalet cyberattacker har ökat påtagligt de senaste åren (Androjna m.fl., 2020). Respondent 3 belyste ofta under intervjun att dennes företag kunde upprätthålla en god upp-tid för deras kunder. Att arbete aktivt inom området av såväl fysisk som virtuell säkerhet grundar sig i att man som en vinstdrivande organisation aspirerar att tillhandahålla sina tjänster i den utsträckning som efterfrågas av ens kunder och andra intressenter.

Respondent 2 belyser också hur viktigt hen tycker det är med att behålla, och anställa, kompetent personal, samt hur viktigt det är att kunna vara handelskraftig och pragmatisk inom

dennes organisation. Respondent 2 omnämner också att när hen skall anställa en resurs för att fylla en roll så faller de primära arbetsuppgifterna hellre i att anställa en individ som på ett konkret sätt arbetar med cybersäkerheten, i stället för att uppdatera procedurer, förnya certifieringar och andra rent administrativa uppgifter. Hen ser det alltså av större vikt att arbeta aktivt med cyberförsvaret och att det rent administrativa vad det gäller driften av cybersäkerhetsorganisationen blir en sekundär prioritet.

Författarna delar också den filosofin, att man inte får gräva ned sig för mycket i det byråkratiska utan att faktiskt ta ett steg tillbaka för att i sin helhet förstå vad man skall göra inom organisationen för att öka sin förmåga gällande cyberförsvar. Detta går även hand i hand med vad respondent 3 belyser med att man skall ”*bygga lagom*”, och att ”*de flesta fokuserar så smalt*”. I stället för att ha det dyraste och modernaste systemet på en del av organisationen måste man ha helheten i åtanke. Respondent 2 för resonemanget att denne föredrar att fylla en roll som på ett mer direkt sätt arbetar med cybersäkerheten, och respondent 3s resonemang om att bygga lagom och att kolla bredare på begreppet cybersäkerhet, blir således ett sätt att bygga upp ens cybersäkerhetsorganisation på ett mer effektivt sätt då man verkar under begränsade resurser. Detta i anslutning till att respondent 1 och 2 beskriver att de arbetar med kontinuerlig utbildning av personal leder till att cybersäkerhetens helhetsbild blir mer omfattande. Respondent 3 belyser att det finns ett problemområde då det råder en viss naivitet kring hur mycket vissa system påverkas vid felaktigt handhavande av dem. Detta fångas in av processen att utbilda och sprida kunskap inom organisationerna för att på det sättet minska risken för att specifika individers brist på kunskap ska leda till svagheter i säkerhetsnivån.

5.1.2 Åtgärdsplaner

Det framgick genom intervjuerna med hamnorganisationerna att de båda är välmedvetna om hur beroende deras respektive organisationer är av virtuella system. Dessa system stödjer en majoritet av de aktiviteter som utförs i hamnen för den säkra och effektiva operationen av hamnens olika arbetsuppgifter.

Båda hamnorganisationerna arbetade genom ett ledningssystem för informationssäkerhet där det statueras olika krav på organisationens i frågas möjlighet att avvärja, men också svara upp emot ett bortfall av vissa system. Hamnarna belyste olika processer som har som avsikt att möjliggöra att hamnen fortsatt kan vara operationell i händelsen av ett cyberattentat.

Båda hamnorganisationerna belyser att deras respektive cybersäkerhetsorganisationer har olika åtgärdsplaner som kan träda i kraft vid bortkopplingar av system. Multi-purpose hamnen förklarar att de har ”röda pärmar” som skall tillhandahålla olika procedurer som skall kompensera för de system som fallit bort. Även ro-ro-hamnen tillhandahåller en policy med procedurer som förklarar tillvägagångssättet att hantera en eventuell cyberattack. Enligt tidigare forskning från Senarak (2020) arbetar även PAT utifrån procedurer som ska försäkra att hamnar ska fortsätta sin verksamhet vid eventuella attacker. Denna standard gällande informationssäkerhet följs även av Port of Los Angeles (Port of Los Angeles, 2023). Port of Los Angeles har även upprättat ett eget ”Cyber Security Operation Center”. Avsikten med införandet av en sådan avdelning inom hamnorganisationen är att verka som en central enhet som övervakar hamnens cybersäkerhetsstatus. Detta är innefattande av att utföra en kontinuerlig omvärldsbevakning, men också att aktivt analysera skadlig programvara för att konstatera vem, vilka, eller vilken verksamhet som hade som avsikt att infiltrera verksamheten. Respondent 2 beskriver ett liknande arbetssätt där deras cybersäkerhetsorganisation samarbetar via ett nätverk av flera organisationer där de bedriver omvärldsbevakning utifrån syftet att analysera hotnivån mot respektive hamn.

Den tredje respondenten förklarar att även de har en beredskapsplan som aktiveras när någonting i systemen går fel, och att de kan återställa systemen på ett fåtal minuter för att garantera att verksamheten kan fortlöpa även vid en attack. Dennes organisation drev också filosofin om att tillämpa redundanta system. Mycket av den hårdvara som installerades hos de olika kunderna de ombesörjde hade dubbel uppsättning. Detta var av, enligt hen själv, för att i största möjliga mån subventionera 100% upp-tid av systemen. Denna syn på att både mjuk- och hårdvara är lika utifrån att ha bästa möjliga säkerhet var respondent 3s organisation den enda som påvisade i studien.

Båda hamnrespondenterna förklarar att de utför utbildningar för personal för att sprida kunskap om säkerheten för handhavandet av IT-systemen. Enligt tidigare forskning från Senarak (2020) arbetar även PAT med att kontinuerligt utbilda personal för att möjliggöra god cybersäkerhet. Respondent 3 beskriver detta som en del i att systemet är bara så bra som sin svagaste länk. Det gäller att ha helheten, inklusive att personalen har starkt säkerhetstänk. Respondent 1 förklarar deras syn på helhetsbilden, där säkerhetsarbetet beskrivs som en lök med flera lager, där alla lager ifrån lösenordshantering till brandväggar blir en del av helhetsbilden. Respondent 2 förklarar att de även utför övningar där systemen och användarna testas, vilket leder till en tryggare situation vid eventuella framtida attacker, då personalen genom dessa övningar fått kunskap i hur de ska hantera situationen. Övningarna leder även till förbättringsarbeten, då övningarna snabbt visar vilka brister som finns, och kan i och med det åtgärda dessa.

Dessa beredskapsplaner och åtgärder visar att hamnorganisationerna samt IT-leverantören arbetar proaktivt för att konstant vara förberedda på eventuella hot mot cybersäkerheten. Vikten av att ha fungerande system är så betydande att det ges utrymme för säkerheten att arbeta med att skydda sig och att ha färdiga procedurer för att hantera olika slags attacker.

Det finns en viss skillnad i synen på åtgärdsplaner och hur de olika respondenterna hanterar dessa, framför allt i att respondent 1 och 3 båda fokuserar mer på redundanta system, där ett annat system tar över funktioner när ett system faller bort, medan respondent 2 förklarar att de fortfarande arbetar mer manuellt med fysiska pärmar som någonting de faller tillbaka på vid eventuellt bortfall av ett tekniskt system. Respondent 2 förklarar att detta beror på att de vill kunna klara sig utan IT-stöd och att verksamheten skall fungera även vid totalt bortfall av viktiga virtuella system.

5.1.3 Lagar och riktlinjer

Resultatet visar att den första av de två tillfrågade hamnorganisationerna ägs av kommunen den befinner sig i och arbetar med cybersäkerhet enligt kommunens ledningssystem som baseras på ISO 27001. Respondent 1 beskriver att en stor del av deras säkerhetsarbete styrs av kommunens säkerhetsavdelning, medan respondent 2 förklarar att även de arbetar utifrån ISO 27001 men att de har i sin roll som större hamn en något större verksamhet i själva hamnen. Respondent 2 arbetar även ihop med säkerhetsavdelningen i staden som också äger hamnorganisationen i sin helhet. Även respondent 3, IT-leverantören, förklarar att de arbetar enligt ISO 27001. Enligt tidigare forskning från Senarak (2020) arbetar även Port Authority of Thailand i Leam Chapang Port utifrån ramverket ISO 27001. PAT har även inkorporerat IMO ”*Maritime Cyber Risk Management*” riktlinjerna i deras säkerhetsorganisation. Port of Los Angeles utför också arbete utifrån riktlinjerna i ISO 27001 och får enligt studien ses som det system som främst når fram till hamnorganisationerna (Port of Los Angeles, 2023).

Som IT-leverantören dock beskriver det fungerar flera av de olika nämnda riktlinjerna i teorin, IMO Guidelines, ISO 27001 samt NIST Framework i stora drag på samma sätt med liknande

funktioner som varandra. Att de olika systemen och riktlinjerna bygger på samma principer kan förklara varför respondenterna i de båda hamnorganisationerna svarar att de inte arbetar med IMO:s riktlinjer, då de fångas in under större krav från mer krävande direktiv. Kraven från de olika riktlinjerna är väldigt godtyckliga och det kan vara svårt att konkret veta vad som behövs för att fylla upp dessa krav. Till exempel meningen ”arbeta med cybersäkerhet” från IMO kan man som hamnorganisation hävda att man gör genom att använda lösenord för att logga in, medan en annan hamnorganisation kan tolka det som ett mycket större krav. Respondent 2 arbetar under NIS-direktivet som uppfyller funktioner från både IMO, ISO samt NIST. Enligt tidigare forskning från Polatidis m.fl. (2018) är det lämpligt att använda sig av flera riktlinjer för att forma sitt ramverk kring cybersäkerhet, där de lyfter att deras ramverk i studien byggts utifrån ISO 27001 samt NIST Framework, där de båda standarderna följs åt och i stora drag uttrycker samma mål. Även respondent 3 förklarar att även om de arbetar enligt ISO 27001 har deras mål och egna krav en högre standard där de uppfyller fler krav utöver de formulerade i ISO 27001.

Respondent 2 belyste också att de i samröre med att arbeta med ISO 27001-ramverket även arbetar med CIS-controls. Detta är enligt denne ett mer handgripligt ramverk där det är lättare att utvärdera de åtaganden som utförs. Detta ramverk tillhandahåller en mer aktiv och konkret beskrivning av hur hamnorganisationen skall arbeta, och respondentens resonemang om att denne föredrar ett mer aktivt och pragmatiskt cybersäkerhetsarbete går således hand i hand med att arbeta med detta ramverk.

Tidigare forskning från Senarak (2020) förklarar att de utöver ramverket i ISO 27001 även samarbetar mellan cybersäkerhetsorganisationen och hamnsäkerhetsorganisationen som lyder under ISPS-koden, detta för att få de olika processerna att stärka cybersäkerheten. Respondent 1 tillämpar samma strategi där de ser ett tydligt samband mellan fysisk och virtuell säkerhet.

5.2 Metoddiskussion

Författarna av denna studie har kontinuerligt under skriv- och informationsinsamlings processen grundat sig i vald metod. Det huvudsakliga syftet med studien var att tillhandahålla en kartläggning av hur hamnorganisationer arbetar och förhåller sig till de lagrum och riktlinjer som finns gällande cybersäkerhet. Utifrån detta syfte fann författarna det av mest relevans att använda sig av en kvalitativ forskningsmetod där införskaffandet av rådata samlades in från intervjuer med personer från relevanta hamnorganisationer samt en IT-leverantör. Därav valde författarna att använda sig av en kvalitativ fallstudie för att kunna djupdyka inom ämnet. Viktigt att utvärdera vid användandet av en fallstudie som forskningsstrategi är att ämnet som skall granskas har egenskaper av att ha en gräns, alltså att ämnet inte har egenskapen av att kunna sammanflätas eller blandas ihop med andra sociala fenomen (Denscombe, 2014). Då studiens granskningsområde och syfte isolerar sig i den utsträckningen av att undersöka ett enskilt fall tillåter det en djupare analys inom ämnet. Detta kan medföra att studien genererar mer djupgående insikter, kontra att använda sig av en bredare forskningsstrategi (Denscombe, 2014).

Bryman (2018) förklarar vidare de nackdelar som finns med fallstudieforskning som metod. Han lyfter frågan, hur kan ett specifikt fall vara representativt för en större massa, samt hur kan ett resultat tillämpas i generella drag på andra fall? Enligt Bryman (2018) är svaret på de frågorna att det inte går att få ett resultat utifrån en respondent.

Enligt Bryman (2018) handlar reliabilitet om att bedöma om en studie är tillförlitlig och om resultatet skulle vara repeterbart vid olika tillfällen eller av olika forskare. Inom intervjuer kan

reliabilitet förstås som graden av konsistens eller överensstämmelse i de svar som erhålls från respondenterna. Respondenterna i studien tillfrågades genom semistrukturerade intervjuer. Samtliga intervjuer använde sig av en gemensam frågemall som utefter svaren från de respektive respondenterna hade möjliga följdfrågor. Utifrån principen att en annan forskare ska kunna få fram ett liknande resultat ställs det höga krav på att samtliga intervjuer följde denna mall. De två första intervjuerna med respondenterna från hamnarna genomfördes helt enligt mallen vilket försvarar reliabiliteten. Den tredje intervjun genomfördes till skillnad från de tidigare två inte genom videosamtal online, utan på plats, vilket i sin tur ledde till viss flexibilitet i tillvägagångssättet på hur intervjun genomfördes. Det längre samtalet med den tredje respondenten ledde till att flera av de formade intervjufrågorna i underlaget svarades på redan innan de hann ställas. Denna variation från de andra intervjuerna kan ha haft en påverkan på reliabiliteten och svaren från tredje respondenten sticker även ut från de andra två tillfrågade respondenterna som var mer konsekventa i sina svar. Att vara säkra på huruvida reliabiliteten är stark är svårt, det hade varit intressant att låta en annan person utföra intervjuerna med samma frågeformulär och samma deltagare och jämföra det resultatet med det insamlade från denna studie.

Enligt Bryman (2018) så handlar validitet om att kunna bedöma i vilken utsträckning en studie faktiskt granskar det den konkret avser att undersöka. Validiteten är således ett mått på hur väl intervju-frågorna besvarats, och att utvärdera graden av generalisering som kan göras utifrån studiens slutsatser. Validitet handlar både om intern samt extern validitet. Där den interna validiteten kan påverkas av författarnas förståelse för ämnet. Den interna kunskapen påverkades under arbetets gång då varje genomförd intervju ökade författarnas förståelse kring cybersäkerhet och kring ämnena som diskuterades. Detta faktum kan ha påverkat intervjuerna då det var lättare att förstå vissa resonemang som fördes och att det fanns bakomliggande kunskap kring flera av svaren som de senare respondenterna gav. Denna förförståelse inför de senare intervjuerna kan ha påverkat författarnas följdfrågor till respondenterna vilket kan försämra validiteten.

För att få extern validitet var ambitionen med studien att utföra flera intervjuer med hamnorganisationer, där förfrågan om intervjuer skickades ut och flertalet hamnar kontaktades. Bristen på svar från dessa hamnar kan förklaras på flera sätt, dels utifrån perspektivet att de tillfrågade hamnarna inte anser sig själva vara tillräckligt förberedda inom området cybersäkerhet och därför varit ovilliga att dela med sig av deras arbete, men det kan även bero på flertalet andra anledningar, där brist på tid och intresse från hamnarna förklarar deras icke-intresse att delta i intervjuer kring dessa frågor.

De intervju-frågor som hade konstruerats inför de möten som hölls med respektive hamn/IT-leverantör besvarades i hög grad av de tillfrågade respondenterna. I och med detta så kan slutsatser i viss mån dras ut efter det.

Sammanfattningsvis så är slutsatserna som formats ifrån studien begränsade i och med de brister i reliabilitet och validitet som lyfts i ovanstående stycken, vilket i samband med det begränsade tillfrågade urvalet gör att större generaliserande slutsatser för en större population blir svårt. Studien är isolerad emot hamnar i Sverige som (i relativa termer) hanterar större volymer gods och slutsatserna grundas kring dessa specifika verksamheter.

Enligt Denscombe (2014) svarar respondenten olika beroende på vem, eller vilka, som utför intervjun. Den data som den respondenten är villig att dela med sig av är således beroende av olika karakteristik som innehas hos de som utför intervjun. Detta kan vara i from av kön, etnicitet eller ålder (Denscombe, 2014). Detta var något som studiens författare vad medvetna

om vid intervjutillfällena. Författarna innehar ingen extraordinär kunskap om cybersäkerhet eller hur arbetsprocesserna ser ut för en hamn och dess säkerhetsorganisation. Författarna strävade i och med det att komma väl förberedda till intervjuerna med strukturerade frågor som ledde samtalen in på de områden där författarna kände sig mer familjära, trots att intervjuerna hölls semi-strukturerade.

Intervjuerna utfördes både på plats och virtuellt via en digital media som erbjuder videosamtal. Dessa intervjuer spelades in via en röstmemo applikation på författarnas respektive mobiltelefon. Enligt Denscombe (2014) erbjuder denna sorts inspelning sina klara fördelar då det gör det möjligt för författarna att återvända till materialet samtidigt som det erhåller den hela konversationen för andra granskare. Dock belyser Denscombe (2014) att denna sort av inspelning bara erbjuder den verbala konversationen av intervjun och missar således den icke verbala konversationen och andra kontextgrundande faktorer. Författarna av denna studie var medvetna om denna problematik men gjorde avvägningen att detta var den mest lämpliga väg att utföra inspelningen av intervjuerna på. Enligt Denscombe (2014) är det relativt ovanligt att använda sig av videoinspelade intervjuer då detta kan medför en efterhållsamhet hos respondenterna av att bli inspelad. Författarna av denna studie insåg detta också och landade då i slutsatsen att audio inspelning tillhandahöll tillräckligt med kontextgrundande information samtidigt som att intervjuerna kunde hållas i en mer lättsam och familjär miljö. För att kompensera för detta transkriberades intervjuerna på ett sådant sätt att de belyser den kontext som uppfattades under de olika delarna av intervjun, till exempel om det förekom skratt, eller om respondenten var ironisk.

Denscombe (2014) nämner att det föreligger en risk i att respondenten som intervjuats delade information inte stämmer, och att det då finns olika metoder som kan utföras för att validera informationen. Dock är inte dessa metoder helt felfria och kan i och med det ibland fortfarande inte garantera att den delade informationen är korrekt (Denscombe, 2014). Författarna av denna studie var medvetna om att denna risk förelåg innan intervjutillfällena, och visste också att informationen som delades skulle bli svår att validera.

Urvalet av respondenter grundade sig i att söka efter kompetent personal verksamma inom IT hos diverse hamnorganisationer. Förfrågan om att sätta sig ner för en intervju med författarna skickades ut till ett flertal hamnar i Sverige, men fick enbart gehör ifrån två. En förfrågan om intervju med författarna skickades även till en IT-leverantör som också tackade ja. Författarna upplevde respondenterna ifrån dessa intervjuer som kompetenta. Respondenterna belyste också under intervjutillfällena att man inte såg några problem med att dela denna information med oss, och författarna fick även intrycket om att det mesta gick att diskutera och prata vidare om.

6. SLUTSATSER

I det avslutande kapitlet så kommer studiens frågeställningar att besvaras utifrån den tidigare presenterade datan i teori-, resultat- och diskussions-kapitlen.

Studien drar en slutsats i att de tillfrågande hamnorganisationerna arbetar aktivt med deras respektive cybersäkerhetsorganisation. Med detta sagt förekommer det vissa skiljaktigheter mellan de olika respondenternas organisationer. Studien iakttar att cybersäkerhet får olika utrymme och vikt beroende på hur hamnorganisationen och hur dess hotbild ser ut. Detta stödjs även av att Port of Los Angeles, som mätt till volym och omsättning är en stor och betydande hamn-nod, har upprättat en helt egen ”*Cyber Security Operations Center*”. Det hade inte varit försvarbart eller ens möjligt för studiens två tillfrågade hamnorganisationer att ha en egen CSOC utifrån deras storlek. Att författarna inte heller fått något gehör från svenska hamnar av mindre storlek öppnar för tanken om att de inte vill prata cyberförsvar för att deras nuvarande organisation inom ämnet är mindre utvecklat samt att uppbyggandet av det således tar längre tid. Man ser en klar skillnad i de granskade hamnorganisationernas cybersäkerhet. Denna skillnad kan vara beroende av ett flertal parametrar där tidigare terror-historik och större resurser ses av författarna som två signifikanta faktorer till en ökad cybersäkerhetsorganisation. Att Port of Los Angeles har en större cybersäkerhetsorganisation än de hamnar som studien tillfrågat ses av författarna som bevis på att detta resonemang kan gälla.

En slutsats av detta resonemang är att relationen av arbetet med cybersäkerhet är en balansgång mellan hotbild, storlek och förutsättningar. Samtliga hamnorganisationer arbetar med cybersäkerhet och hanterar de risker som uppstår mot deras verksamhet. Men hur hanteringen ser ut beror på nivån av hot, där större hamnar globalt arbetar mer utvecklat med sin cybersäkerhet utifrån premissen att de utsätts för större exponering mot eventuella attacker. En insikt är faktumet att även om en större hamn arbetar mer utökat med cybersäkerhet innebär inte det att den mindre hamnen har ett otillräckligt cybersäkerhetsarbete, utan arbetet är i stället balanserat utifrån dess risker och specifika förutsättningar. Att definiera om organisationerna i fråga har de lämpliga verktyg och kunskap som krävs för att hantera hoten kan göras utifrån argumentationen att de tillfrågade organisationerna, enligt datan från intervjuerna, inte har påverkats nämnvärt av de intrång och hot mot verksamheten som de utsatts för under senare år. De incidenter som respondenterna beskriver i resultatet har bemötts på ett effektivt och lämpligt sätt för fortsatt drift av verksamheten.

Studien visar att samtliga av de granskade organisationerna arbetar aktivt med beredskapsplaner som en åtgärd för att garantera säkerheten. Resultatet visar att beredskapsplanerna skiljer sig åt i viss bemärkelse utifrån hur deras respektive hotbild ser ut. Det visar sig bland annat att respondent 1 samt 3 arbetar utifrån värderingen att backup-system är en god åtgärd för att återställa funktioner efter en attack, medan respondent 2 fokuserar på fysiska dokument vid bortfall av IT-system. Detta ger respondent 2 en möjlighet att även bedriva viss mån av verksamhet vid exempelvis bortfall av ström eller internetuppkoppling. Respondent 1 och 3 har filosofin att använda sig av redundanta system, vilket möjliggör att de kan upprätthålla en mer normal drift av organisationens olika uppgifter även vid bortfall av vissa IT-system. De utförda intervjuerna med hamnorganisationerna belyser också att utbildningar för de anställda, och de som jobbar i hamnen, sker med jämna intervall. Dessa utbildningar grundar sig mycket i att öka medvetenheten och kunskap i hur man skall använda de virtuella systemen på ett säkert sätt. Senarak (2020) redogör att PAT också utförde utbildningar inom säkert handhavande av diverse IT-system hos deras organisation. Respondent 2 uppmärksammar också att dennes hamnorganisation är i tagen av att initiera

skrivbordsövningar hos de seniora ledande positionerna inom organisationen. Detta var något som inte förekom hos de andra tillfrågade respondenterna och den faktiska övningen med tillämpande av diverse säkerhetsprocedurer var något som endast omnämndes existera hos hamnorganisationen respondent 2 var verksam inom.

Att utföra utbildningar på detta sätt leder till en slutsats där organisationerna arbetar i linje med riktlinjerna som utfärdats av IMO. I och med att dessa uttrycker att ”r*iskhanteringen kräver att hela organisationer genomsyras av kunskap och medvetenhet, annars brister säkerhetstänket.”*

En tydlig koppling och slutsats vid analys av resultatet är att samtliga hamnorganisationer från både den primära samt den sekundära datan är att organisationerna grundar sitt arbete kring cybersäkerhet utifrån ramverket ISO 27001. De krav som ställs på hamnorganisationerna utifrån ledningssystemet visar att de ska arbeta med ledarskap, planering, stöd, verksamhet, utvärdering av prestanda samt förbättringsarbete inom informationssäkerhet. Dessa punkter fångas upp under intervjuerna där respondenterna förklarar deras arbete kring cybersäkerhet.

En vidare slutsats som studien belyser är att IMO når inte direkt fram med sina direktiv till de tillfrågade hamnorganisationerna, de når däremot indirekt fram genom att de krav de har fångas in av andra regelverk och direktiv. Detta är inget problem i nuläget, men vid en förändring av IMO:s krav kan det bli svårt att få hamnorganisationer att applicera sig utifrån detta. IMO säger att deras resolution MSC.428 (98) avser att hamnar och hamnverksamheter ska arbeta för att skydda sina verksamheter mot cyberrelaterade hot, men enligt studien når man inte fram till de tillfrågade hamnorganisationerna. Enligt Senarak (2020) arbetar PAT utifrån de riktlinjer som tillhandahålls av IMO gällande cybersäkerhet. Respondent 3 nämner också vid intervjutillfället att de också arbetar med IMO:s riktlinjer gällande cybersäkerhet. Utifrån studien är det svårt att dra en generell slutsats men det som presenteras visar att IMO når fram till vissa hamnorganisationer och företag, men inte andra.

6.1 Rekommendationer till fortsatt arbete

Rekommendation till fortsatt arbete är att fortsätta på författarnas spår av struktur och intervjufrågor, men att även få till möten och samtal med mindre hamnar i Sverige. Med datainsamlingen från ett sådant arbete, tillsammans med resultatet från denna studie, skulle kunna möjliggöra att man i stället också använder sig av frågeställningen ”hur bör man arbeta med cybersäkerhet”. Detta med syftet för att kunna utföra förbättringsarbete för hamnar, och eventuellt bygga upp en struktur i hur, vad och vilka processer som borde övervägas när man skall bygga upp sin cybersäkerhetsorganisation.

KÄLLFÖRTECKNING

Androjna, A., Brcko, T., Pavic, I., & Greidanus, H. (2020). *Marine Science and Engineering Assessing Cyber Challenges of Maritime Navigation*. https://doi.org/10.3390/jmse8100776

Ayala, L. (2016). *Cybersecurity Lexicon* (1:a uppl.). Apress. https://doi.org/10.1007/978-1-4842-2068-9

BIMCO, ICS, INTERCARGO, CLIA, INTERTANKO, OCIMF, & IUMI. (2020). *THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS Produced and supported by The Guidelines on Cyber Security Onboard Ships*. https://www.bimco.org/-/media/bimco/about-us-and-our-members/publications/ebooks/guidelines-on-cyber-security-onboard-ships-v4.ashx?rev=e86ee4330cce44d7b90ad718e8af3c2e

Bryman, A. (2018). *Samhällsvetenskapliga metoder* (3:e uppl., Vol. 2). Liber AB.

CIS. (2023a). *CIS Critical Security Controls FAQ*. https://www.cisecurity.org/controls/cis-controls-faq

CIS. (2023b). *CIS Critical Security Controls Version 8*. https://www.cisecurity.org/controls/v8

Denscombe, M. (2014). *The good research guide : for small-scale research projects*. Open University Press. https://r3.vlereader.com/Reader?ean=9780335264711

Denscombe, M. (2018). *Forskningshandboken* (4:e uppl.). Studentlitteratur AB.

European Parliament, C. of the E. U. (2016, juli 6). *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. https://eur-lex.europa.eu/eli/dir/2016/1148/oj

F-Secure. (2023). *Vad är ransomware? | F-Secure*. https://www.f-secure.com/se-sv/home/articles/what-is-a-ransomware-attack

Hammond, M., & Wellington, J. (2020). Research methods: The key concepts. *Research Methods: The Key Concepts*, 1–198. https://doi.org/10.4324/9780429058165

Hellenic Shipping News. (2020, juli 21). *Maritime Cyber Attacks Increase By 900% In Three Years | Hellenic Shipping News Worldwide*. https://www.hellenicshippingnews.com/maritime-cyber-attacks-increase-by-900-in-three-years/

IAPH, ICHCA, TT CLUB, & WPSP. (2020). *PORT COMMUNITY CYBER SECURITY Courtesy Port of Los Angeles*. https://www.weforum.org/centre-for-cybersecurity/

IMO. (u.å.). *Maritime cyber risk*. u.d. Hämtad 10 februari 2023, från https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

IMO. (2009). *International Ship and Port Security Code (ISPS Code)*. http://dmr.regs4ships.com.eu1.proxy.openathens.net/docs/international/imo/codes/isps.cfm

IMO. (2017a, juni 16). *MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems*. http://dmr.regs4ships.com.eu1.proxy.openathens.net/docs/international/imo/resolutions/msc/msc_428_98.cfm

IMO. (2017b, juli 5). *GUIDELINES ON MARITIME CYBER RISK MANAGEMENT*. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

IMO. (2018). *The International Safety Management (ISM) Code*. https://www.imo.org/en/ourwork/humanelement/pages/ISMCode.aspx

Institute of Standards, N. (2014). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. https://doi.org/10.6028/NIST.CSWP.04162018

ISO, & IEC. (2022). *Standard - Informationssäkerhet- Cybersäkerhet och integritetsskydd - Ledningssystem för informationssäkerhet - Krav (ISO/IEC 27001:2022, IDT) SS-ISO/IEC 27001:2022 - Svenska institutet för standarder, SIS*. https://www-sis-se.eu1.proxy.openathens.net/produkter/informationsteknik-kontorsutrustning/allmant/ss-isoiec-270012022/

Jadesköld, M., & Zalitis, E. (2019, februari 3). *Cyberattacken mot Göteborgs hamn - IT-säkerhetspodden | Lyssna här | Poddtoppen.se*. https://poddtoppen.se/podcast/1444914571/it-sakerhetspodden/cyberattacken-mot-goteborgs-hamn

Kapalidis, C., Karamperidis, S., Watson, T., & Koligiannis, G. (2022). A Vulnerability Centric System of Systems Analysis on the Maritime Transportation Sector Most Valuable Assets: Recommendations for Port Facilities and Ships. *Journal of Marine Science and Engineering*, *10*(10), 1486. https://doi.org/10.3390/jmse10101486

Kechagias, E. P., Chatzistelios, G., Papadopoulos, G. A., & Apostolou, P. (2022). Digital transformation of the maritime industry: A cybersecurity systemic approach. *International Journal of Critical Infrastructure Protection*, *37*. https://doi.org/10.1016/J.IJCIP.2022.100526

Lag om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174). *Riksdagen*, (2018). https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-20181174-om-informationssakerhet-for_sfs-2018-1174

Meyer-Larsen, N., & Müller, R. (2018). Enhancing the Cybersecurity of Port Community Systems. I *Dynamics in Logistics* (Vol. 1, s. 318–323). https://doi.org/10.1007/978-3-319-74225-0_43

Polatidis, N., Pavlidis, M., & Mouratidis, H. (2018). Cyber-attack path discovery in a dynamic supply chain maritime risk management system. *Computer Standards and Interfaces*, *56*, 74–82. https://doi.org/10.1016/J.CSI.2017.09.006

Port of Los Angeles. (2023). *Cybersecurity | Business | Port of Los Angeles | Port of Los Angeles*. https://www.portoflosangeles.org/business/cybersecurity

Senarak, C. (2020). Port cybersecurity and threat: A structural model for prevention and policy development. *The Asian Journal of Shipping and Logistics*, *37*, 2021–2041. https://doi.org/10.1016/j.ajsl.2020.05.001

Tam, K., & Jones, K. (2018). Cyber-Risk Assessment for Autonomous Ships. *2018 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2018*. https://doi.org/10.1109/CYBERSECPODS.2018.8560690

Transportstyrelsen. (2021). *Miljö och hälsa - Transportstyrelsen*. https://www.transportstyrelsen.se/sv/sjofart/miljo-och-halsa/

Wagner, S. (2017). *Cyber attack update - A.P. Møller - Mærsk A/S*. Maersk News Release. https://investor.maersk.com/news-releases/news-release-details/cyber-attack-update

Wienberg, C. (2017, augusti 16). *Maersk Says June Cyberattack Will Cost It up to $300 Million - Bloomberg*. https://www.bloomberg.com/news/articles/2017-08-16/maersk-misses-estimates-as-cyberattack-set-to-hurt-third-quarter?leadSource=uverify%20wall

INSTITUTIONEN FÖR MEKANIK OCH MARITIMA VETENSKAPER
CHALMERS TEKNISKA HÖGSKOLA
Göteborg, Sverige 2023
www.chalmers.se

CHALMERS