KR Maritime Cyber Security

News from KOREAN REGISTER

Aug 2018

Vol. 004

한국선급 활동

● **선박 사이버보안 점검**

지난 7월 29일, 한국선급 사이버보안 대응 TFT에서는 기술컨설팅의 일환으로 SONGA 社 SONGA HAWK를 방선하여 사이버보안 현장 점검을 수행하였다. 주요 점검 사항은 다음과 같다.

- OCIMF SIRE VIQ 사이버보안 항목 사전 점검 및 가이드라인 제공
- 선박 리스크평가 개선조치 현황 파악
- KR 사이버보안 인증 항목 체크리스트 기반 점검 : PC 보안 취약점 진단 수행

본 방선에서 사이버보안 검사원은 선급 사이버보안 체크리스트 기반 물리보안**(해상 사이버보안 관리시스템 지침 : CSMS1 207)** 점검과 패스워드의 주기적 변경, 화면보호기 대기시간 설정 등을 포함한 PC 취약점을 **PC 보안 취약점 진단 프로그램**을 통해 진단하였다.

한국선급은 축적된 지식과 경험을 바탕으로 선주사에 선박 사이버보안 개선을 위한 가이드라인 제공을 통해 선급 사이버보안 신뢰성이 향상될 수 있을 것으로 기대되며, PC 보안 취약점 진단 프로그램 실제 적용을 통해 선급 사이버보안 기술력을 제고할 것으로 판단된다.

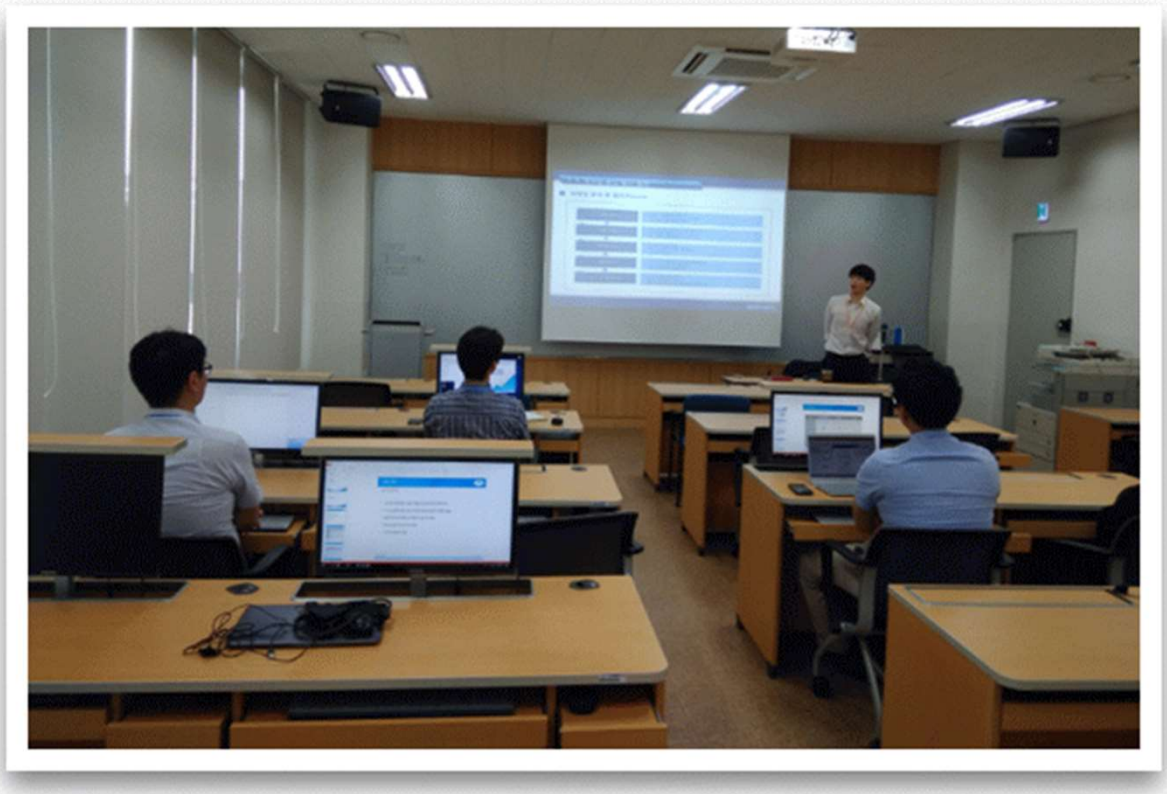
● **사이버보안 검사원 양성 교육 실시**

지난 7월, 한국선급에서는 사이버보안 검사에 대한 기술적 이해도를 높이고 실제 선박 및 회사 검사를 수행하기 위한 사이버보안 검사원 양성 교육을 진행하였다. 교육은 5일동안 진행되었으며 교육 커리큘럼은 다음과 같다.

날짜	교육 내용	상세 내용
7.19 – 7.20	기술분야 교육	- PC 기술 취약점 진단 - 모의해킹 개요
7.23	관리분야 교육	- 사이버보안의 이해 - KR 사이버보안 부기부호
7.24 – 7.25	KR 사이버보안 검사 핵심 사항	- 사이버 자산 식별 및 분석 - 사이버보안 리스크평가

특히 기술분야 교육인 PC 기술 취약점 진단 및 모의해킹 교육은 검사원이 선박 및 회사 사이버보안 검사 시 활용될 것으로 예상된다.

아울러 해사업계(선사, 선박, 조선소, 기자재업체)에 근무하는 임직원 및 선원들을 대상으로 '해사 사이버보안의 이해' 및 '해사 사이버보안 관리 실무' 교육과정이 각각 9월, 10월에 한국선급 본사에서 제공될 예정이다.



● **2018년 동남 아시아 기술 세미나 개최**

한국선급은 지난 24일부터 26일까지 싱가포르 및 태국 방콕에서 동남아시아 해사 업계를 대상으로 'KR 싱가포르 기술세미나'와 'KR 방콕 기술세미나'를 개최했다.

지난 26일 개최된 KR 싱가포르 기술세미나에는 Navig8, Bernhard Schulte 등의 해운회사, 싱가포르 해사청 관계자 등 200여 명이 참석하였다. 또한 대표적인 세계 해운전문지인 로이즈리스트(Lloyd's List)와 페어플레이(Fairplay)에서도 자리하여 관심을 보였다. 또한 지난 24일 개최된 KR 방콕 기술세미나에는 Thoresen & Co., Precious Shipping Public, Nathalin Management 등의 해운회사와 조선소, 태국 선주협회 등의 해사업계 관계자 70여 명이 참석하였다.

이번 동남아시아 해사업계 대상 기술세미나에서 한국선급은 국제해사기구(IMO)의 황산화물 규제(Global Sulphur Cap) 동향과 선박 사이버 보안에 대해 발표했으며, 캄사르막스(KAMSARMAX) 벌크선 디자인도 소개하였다.

한국선급 이정기 회장은 "최근 세계 해사산업은 환경규제, 사이버 위협 등 그 어느 때보다 많은 도전에 직면하고 있다"고 하며 "이러한 상황에서 해사업계의 최근 동향과 대응방안을 공유하기 위해 세미나를 마련했다"고 말했다

COSCO 시스템 장애, 사이버공격 추정

2017년 6월 머스크 Line 랜섬웨어 감염 사고에 이어 지난 7월말 업계 규모 4위에 해당하는 중국 국적 선사 COSCO Shipping에서도 랜섬웨어 계열 악성코드 감염사고가 발생한 것으로 알려졌다.

● **선박 운항은 문제 없지만 특정 지역 시스템 장애**

언론에 보도된 사항을 종합해 보면, COSCO는 대외적으로 랜섬웨어 감염을 직접적으로 언급하지 않은 채 미주 지역 네트워크 장애라는 사실만을 공개했으나, 회사 내부에서는 악성메일에 대한 경고와 함께 악성코드 감염 확산을 방지하는 체계를 강화하고 있는 것으로 알려졌다. 회사 측은 미주 지역의 이메일과 전화서비스가 복구되지 않고 있지만 전세계 COSCO 선박 운항이 정상적으로 이뤄지고 있고, 비즈니스의 핵심 운영 시스템 역시 안전적으로 운영되고 있다고 설명했다. 다만 사고 발생 후 미주 지역 네트워크 장애 따른 6페이지 비상 대응 문서를 발표하고 화물 운송 시점, 인보이스, 빌링 등의 커뮤니케이션을 위하여 야후와 지메일 등 임시 외부 이메일 주소를 공개하는 조치를 취하기도 했다.

(Frequently Asked Questions about Network Problem within America Area)

● **NotPetya 랜섬웨어 감염 피해**

COSCO 시스템을 감염시킨 것으로 알려진 NotPetya는 COSCO 뿐만 아니라, 2017년 머스크 Line의 시스템과 항공 물류 운송업체 Fedex 시스템도 감염시켜 각각 약 3억 달러에 이르는 피해를 발생시킨 전력이 있다. 뿐만 아니라, 우크라이나에 위치한 많은 기업을 대상으로 광범위한 피해를 입힌 주요한 원인이었다.

NotPetya는 윈도우 SMB(Server Message Block) 취약점을 악용해 MBR(Mater Boot Record) 파일 전체를 암호화해 복호화 비용으로 비트코인을 요구하는 랜섬웨어 'Petya'의 변종으로, 윈도우 운영체제에서 동작하는 악성코드이다. 다만 Petya와 달리 NotPetya는 암호화된 데이터를 복구(복호화)하는 것이 원천적으로 불가능할 수 있어 더욱 치명적이다.

특히 NotPetya가 Petya와 결정적으로 다른 점은 사용자의 개입 없이도 스스로 전파될 수 있다는 점이다. 이런 전파 방식은 이메일의 첨부된 Petya가 실행되어야 악성코드가 동작하는 것과 대비되는 큰 차이점이다.

● **정확한 피해 규모 파악에 많은 시간 소요될 듯**

이번 사태로 인한 COSCO의 피해는 2017년 머스크 선사나 페덱스의 피해액보다는 적을 것으로 예상되고 있지만 정확한 피해 규모 파악에는 상당한 시일이 소요될 것으로 예상된다. 일부 언론에 따르면, COSCO가 복구해야 할 시스템의 범위가 서버 4,000여대, PC 45,000대, 그리고 2,500여개의 프로그램에 이를 것으로 예상하고 있으며, 이로 인하여 또다른 매체에서는 구체적인 피해 규모는 회계연도가 지난 시점에서야 명확해질 것이라고 전망했다.

대응 방안 및 시사점

윈도우 시스템 환경에서 동작하는 Petya/NotPetya는 윈도우의 파일이나 디렉토리 및 주변 장치들을 공유하는데 사용되는 메시지 형식인 SMB(Server Message Block) 취약점을 악용한 것으로, MS로부터 2017년 5월 긴급 보안 패치가 발표되었다. 감염대상은 윈도우 XP에서부터 윈도우 7, Vista, 8 등이며, 이중 윈도우 10 버전은 대상에 포함되지 않았다. 윈도우 계열의 서버나 PC를 사용하는 기업 중 보안 패치를 적용하지 않은 기업이라면 신속하게 보안패치를 적용하여야 하며, 필요 시 구 버전의 운영 체제를 업데이트하여야 한다.
보안패치를 위한 다운로드 링크는 여기에서 참고 가능하다.

Ref. : **COSCO Ransomware Spreads, Hazardous Cargo Bookings Cancelled,** Computer Business Review, July, 2018

사이버보안, 기후 위험, 인적 오류 3가지 해상 물류의 주요 위협

선박 물류 손실이 지난 10년간 꾸준히 감소해 38%까지 내려가고 있지만 이런 긍정적인 흐름을 방해할 요인으로 사이버보안, 기후 위험, 인적 오류 등의 위험이 예상되는 것으로 조사되었다.

● **사이버보안 법적 강화로까지 이어질 가능성 높아**

보험사 알리안츠가 발표한 보고서 'Safety & Shipping Review 2018'에 따르면 지난 10년간 해상 물류 분야의 손실 감소가 이어지고 있지만 선박 신기술 사용 증가에 따라 해상 손실 부분도 변화를 겪게 될 것으로 전망했다. 특히 NotPeyta와 같은 악성코드는 물류 분야에서 사이버보안 위협이 얼마나 중요한 요소인지 알려주었다고 설명하고, NIS와 같은 지침이 화주나 선사들을 대상으로 한 사이버보안에 대한 벌칙 또는 벌금 부과로 이어질 것으로 예상하였다.

● **사람에 의한 실수, IT와 데이터가 도움을 줄 듯**

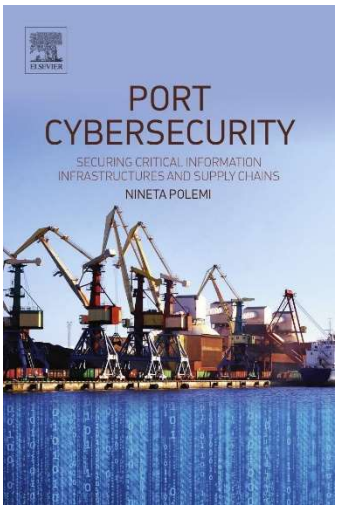
사이버보안과 함께 인적 오류, 즉 Human Error에 대한 문제도 함께 제기되었다. 보고서에 따르면 지난 수년간 반복된 개선에 불구하고 인적 오류에 대한 개선은 만족할만한 성과를 거두지 못하고 있다고 분석하고, 해운 업체가 쌓아놓은 상당한 양의 데이터를 활용하는 것이 필요하다고 강조하고 있다. 이외에도 여전히 해양 사고의 가장 큰 비중을 차지하는 것으로 기후변화로 인한 손실이 꼽혔다.

대응 방안 및 시사점

해양 물류 분야와 함께 선박 운항에 대한 IT 의존도는 지속적으로 높아질 수밖에 없으며, 이로 인하여 각국 정부기관은 선박 및 물류 IT에 사이버보안 요구사항 역시 강화되는 흐름으로 이어질 것으로 예상된다. 선주와 선사는 이를 위하여 각 대륙 및 국가별 사이버보안 요구사항에 대한 흐름을 지속적으로 관리하는 준비가 요구된다.

Ref : Cyber, Climate Risks and Human Error Threaten Shipping's Safety Progress, Business Wire, July, 2018

항만 사이버보안



2017년 10월 발행된 'Port Cybersecurity'에서는 물리적 보안에 중심을 둔 항만 보안이 ICT 발전과 더불어 사이버보안 표준화와 법적 요구사항을 고려해야 할 것이라고 전망했다. Port Cybersecurity 저자 Nineta Polemi에 따르면, ISPS 중심의 항만 보안이 사이버보안까지 고려해야 할 것이라고 강조하고 새로운 법적 프레임워크들을 수용하는 방향으로 이어질 것이라고 예측했다.

● **CIIP Directive eIDAS, NIS Directive 등 다양한 고려요소**

Nineta Polemi이 SearchSecurity에 기고한 내용에 따르면 각 항만이 준수해야 할 요구사항으로 다양한 보안 규정(Regulation)을 언급했으며 일부 내용을 소개하면 다음과 같다.

- **CIIP Directive** (2012) : 주요기반시설 보안 규정
- **The Cybersecurity Strategy for the European Union** (2013) and the **European Agenda on Security** (2015) : 사이버보안과 사이버범죄에 대한 사이버보안 프레임워크 이니셔티브
- **eIDAS Regulation** (2014) : 전자상거래 분야의 안전한 거래 보증
- **NIS Directive** (2016) : 공공분야에 적용되는 필수 보안 요구사항
- **Enhanced Privacy Directive** (2016) : 보안사고 발생 시 강제 보고 요구사항
- **USA H.R. 3878 :** 사이버보안에 대한 강력한 정보 공유 및 협력 체계

이외에도 사이버보안에 필수적인 요구사항인 ISO/IEC 27001와 위험관리 관련 시리즈(ISO/IEC 27005, ISO/IEC 27005) 역시 사이버보안 표준으로 고려되어야 한다고 설명하고 있다.

대응 방안 및 시사점

2017년 해상 분야에서 발생한 사이버보안 사고는 각 선사 뿐만 아니라, 각 국가별 항만 분야에서도 사이버보안 요구사항을 강화하는 계기가 되고 있다. 이런 법적 요구사항은 항만에 접안하는 모든 선박에도 유효하게 적용될 가능성이 높아 각 기업별 지속적이고 단계적 접근이 필요하다.

Ref. Port Cybersecurity, TechTarget, July, 2018

사이버 위협의 이해

● **사이버 위협 이해하기**

사이버 위협이란, 조직 운영, 조직 자산, 개인, 기타 조직 또는 국가에 대해 사이버 시스템을 통한 무단 액세스, 파괴, 공개, 정보 수정 또는 서비스 거부와 같은 잠재적으로 악영향을 미칠 수 있는 상황이나 사건을 의미한다. (출처 : NIST SP : 800-128)

사이버위협은 ICT 기술이 발전함에 따라 자산에 미치는 영향이 변화하므로 자산의 취약점을 파악하기 위해 주기적으로 목록화 할 필요가 있다.

● **한국선급 해상사이버보안 관리시스템 인증 검사항목(CSMS1)**

204.1 위험관리 : 내부 정보기술 및 운영기술 환경에 의한 영향을 미치는 외부 환경 요인을 위협으로 식별하고 목록화하여야 한다.

● **BSI 10대 위협**

ICS에 대한 위협은 기존의 취약성으로 인해 ICS 및 관련 기업에 잠재적으로 손상을 줄 수 있는 공격 또는 이벤트로 인한 것이다. 다음 표는 독일 연방정보 보안국에서 발표한 ICS에 대한 가장 중대한 위협 목록이다. 지난 7월 뉴스레터에 이어 BSI 10대 사이버 위협 중 '**원격 액세스를 통한 침입**'에 대해서 분석하고자 한다.

No. (old No.)	Top 10 2016	Top 10 2014
1 (3)	Social Engineering and Phishing†	Malware Infection via Internet and Intranet
2 (2)	Infiltration of Malware via Removable Media and External Hardware	Infiltration of Malware via Removable Media and External Hardware
3 (1)	Malware Infection via Internet and Intranet	Social Engineering
4 (5)	Intrusion via Remote Access	Human Error and Sabotage
5 (4)	Human Error and Sabotage	Intrusion via Remote Access
6 (6)	Control Components Connected to the Internet	Control Components Connected to the Internet
7 (7)	Technical Malfunctions and Force Majeure	Technical Malfunctions and Force Majeure
8 (9)	Compromising of Extranet and Cloud Components	Compromising of Smartphones in the Production Environment
9 (10)	(D)DoS Attacks	Compromising of Extranet and Cloud Components
10 (8)	Compromising of Smartphones in the Production Environment	(D)DoS Attacks

Ref. : Industrial Control System Security – Top 10 Threats and Countermeasures 2016

● **BSI 10대 위협 : 원격 액세스를 통한 침입**

유지 보수를 위한 외부 액세스는 ICS 설치에서 매우 일반적이다. 보안이 취약한 액세스, 예를 들어 초기(default) 암호 또는 하드코드 된 암호를 통한 보안 문제가 널리 퍼져 있다. 각 제품 공급 업체와 외부 서비스 공급 업체는 종종 구성 요소의 유지 관리 및 프로그래밍 계약을 체결한다. 이것은 여러 당사자들의 보안 개념의 일치를 요구하기 때문에 보안 관리에 추가적인 어려움을 야기한다.

<가능 시나리오>

▣ 유지 관리 엑세스 포인트에 대한 직접 공격

- 암호로 보호된 액세스 포인트에 대한 무차별 공격(brute-force attack)
- 유지 관리에 사용되는 액세스 지점에 대한 웹 공격(주입 또는 CSRF)

▣ 서비스 공급자의 IT 시스템을 통한 간접 공격

- 외부 유지 관리 컴퓨터에서 직접 액세스를 이용하는 트로이 목마,
- 패스워드, 인증서 또는 다른 토큰의 도난 또는 로그인 세부 사항을 획득
- 외부 액세스 용으로 구성된 소프트웨어가 포함된 도난 노트북 컴퓨터 사용.

<대책>

- 제품 공급자의 초기 계정 / 암호는 비활성화, 차단 또는 삭제
- 충분히 안전한 인증 절차의 사용 : 사전 공유 키, 인증서, 하드웨어 토큰, 다중 요소 인증
- 암호화에 의한 전송 경로 보호 : SSL / TLS
- 원격 액세스의 "도달 범위"를 최소화하기 위해 네트워크를 세분화
- DMZ에서 원격 유지 보수를 위한 액세스 포인트를 설정, 서비스 제공 업체가 먼저 ICS 네트워크 대신 DMZ에 연결하고 필요한 액세스 권한을 획득
- 원격 액세스는 항상 방화벽을 통해 라우트되어야 함. (유지 보수에 필요한 IP 주소, 포트 및 시스템만 노출)
- 원격 유지 보수 기간 및 목적으로만 내부 직원이 원격으로 액세스
- 한 번에 한 사용자 당 하나의 로그인만 허용
- 이러한 시스템의 감사 / 접근 수단

Ref. : Industrial Control System Security – Top 10 Threats and Countermeasures 2016

사이버 리스크평가 가이드

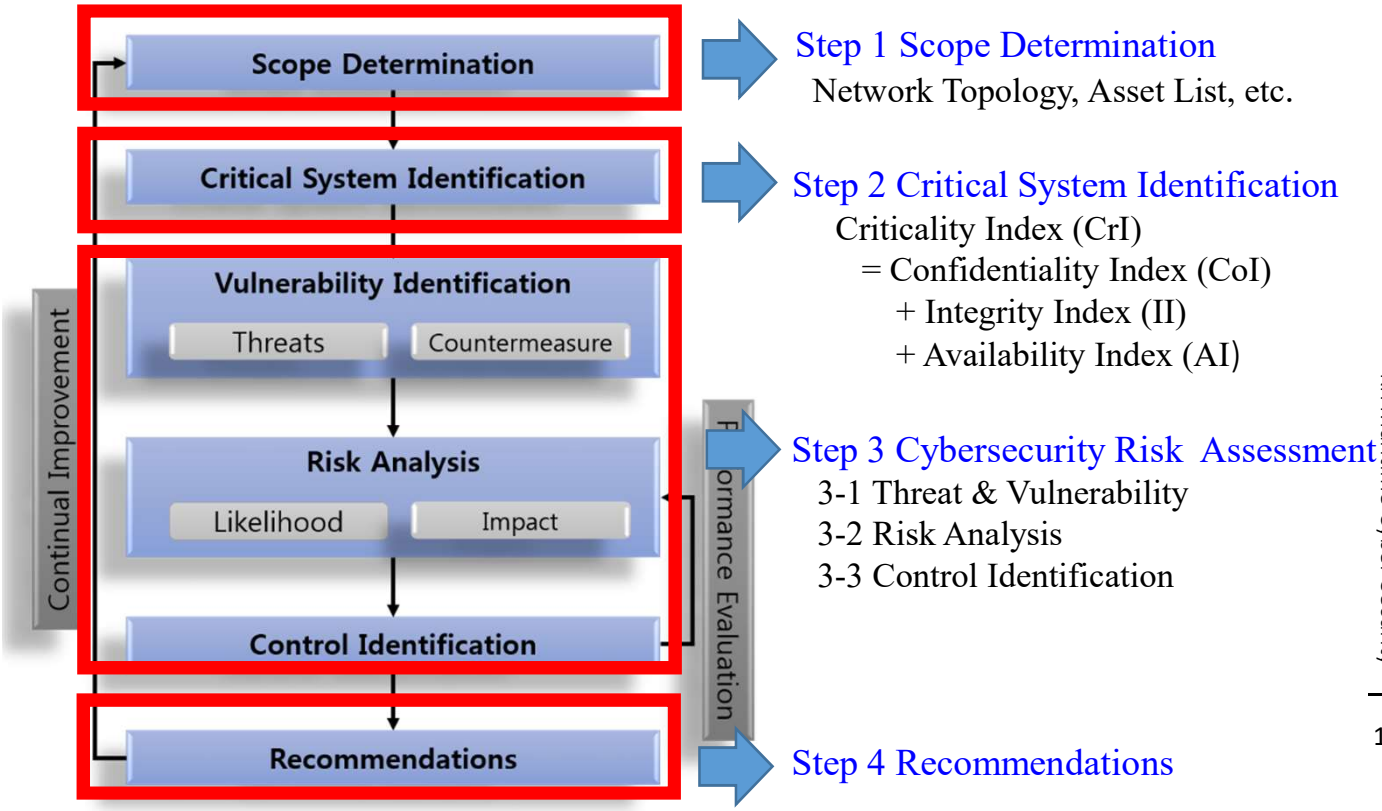
● **사이버 리스크평가의 필요성**

선박 및 회사의 자산을 사이버 위협으로부터 보호하고 사이버보안의 지속적인 향상 및 관리를 위해서 사이버 리스크평가가 필요하다. 선박 및 회사의 주요 시스템 중 위협에 취약한 부분을 식별하고 사이버 위협에 대한 리스크 감소 방안을 마련하여 사이버보안을 강화화기 위해 구조화되고 체계적인 리스크 평가 방법론을 사용한다. 체계적인 사이버보안 리스크 평가를 통하여, 선박 및 회사의 주요 시스템에 대한 사이버보안 리스크 수준을 확인하고, 목표로 하는 리스크 수준과의 차이(Gap)를 분석하여 사이버보안 수준을 향상시킬 수 있도록 전략적 결정을 수행할 수 있어야 한다.

● **한국선급 해상사이버보안 관리시스템 인증 검사항목(CSMS1)**

204.4 위험관리 : 모든 자산에 대해 위협식별, 취약성 진단 결과를 연계하여 정기적으로 위험평가를 실시하여야 한다.

● **한국선급 사이버보안 리스크평가 프로세스 : 4단계로 구성**



● **STEP 1 : SCOPE DETERMINITATION**

목적 : 필요한 정보를 수집하여 위험 평가 및 위험 기준의 목적 및 범위를 명확하게 이해하는 것

준비사항 : 네트워크 토폴로지, 자산목록, 리스크 허용 범위

● **STEP 2 : CRITICAL SYSTEM IDENTIFICATION**

목적 : 자산 (결과)이 비즈니스 활동에 미치는 영향을 분석하여 주요 시스템 식별

준비사항 : CIA를 통한 자산평가(7월 뉴스레터 자산 작성 가이드 참조)

● **STEP 3 : CYBER SECURITY RISK ASSESSMENT**

목적 : 워크샵을 통해 주요 시스템에 대한 위협을 식별, 사이버 공격 시나리오 작성 및 리스크 수준 확인, 리스크를 줄이기 위한 개선 사항 도출

준비사항 : 위협목록, 워크샵 진행

● **STEP 4 : RECOMMENDATION**

목적 : 조치를 위해 사이버보안 리스크평가의 결과(사이버보안 리스크 수준, 리스크 감소를 위한 개선조치, 책임자)를 문서화

Impact	5	5 Significant	10 Significant	15 Major	20 Major	25 Major
	4	4 Low	8 Significant	12 Significant	16 Major	20 Major
	3	3 Low	6 Significant	9 Significant	12 Significant	15 Major
	2	2 Low	4 Low	6 Significant	8 Significant	10 Significant
	1	1 Low	2 Low	3 Low	4 Low	5 Significant
Index		1	2	3	4	5
		Probability				

Cybersecurity Risk = (Threat x Vulnerability) x Consequence

Ref. : IEC 62443, ISO 2705 : 2011, API STD 780

용어 설명

- **SMB(Server Message Block) 취약점 :** 윈도우 운영체제 내에서 파일 또는 디렉터리 및 주변 장치들을 공유하는데 사용되는 메시지 형식(프로토콜)으로, 초기 마이크로소프트의 규격이지만 파일과 주변장치를 공유하는데 편리하게 활용되기 때문에 유닉스, 리눅스와 같은 운영체제가 윈도우와 호환되는 과정에서 프로토콜이다. 다만 이 프로토콜의 경우, 클라이언트가 특정한 요청을 할 경우 서버가 응답하는 구조로 이뤄져 많은 보안 취약점이 존재해 왔다. Petya 이전에도 워너크라이 랜섬웨어 등도 SMB 취약점을 통해 악용되어 왔다.
- **MBR(Mater Boot Record) :** PC에 전원을 연결하면 읽히는 첫번째 영역. 간단하게 말해 하드디스크 맨 처음 기록된 시스템 영역으로 MBR의 정보가 파괴되거나 문제가 발생할 경우, PC 가동이 이뤄지지 않으며 흔히 부팅이 되지 않는 문제가 발생한다.
- **보안 패치(Security Patch) :** 운영체계나 응용프로그램에 내재된 보안 취약점을 보완하는 소프트웨어. 보안패치를 할 경우 취약점을 악용하는 사이버공격 및 악성코드 감염을 방지하고, 각종 PC 오류의 원인을 제거해 준다. 윈도우 계열의 보안패치는 마이크로소프트사를 통해 자동으로 업데이트가 가능하다.
- **ISO/IEC 27001 :** 국제 표준화 기구(ISO, International Standard Organization)가 제정한 정보보호 관리체계(ISMS, Information Security Management System)에 대한 요구사항을 규정한 국제 표준. 2005년 영국의 표준인 BS7799를 기반으로 만들어졌으며, 정보보호에 대하여 기업의 위험관리와 보안정책, 자산관리 등에 대한 규격을 담고 있다.
- **DMZ(Demilitarized zone) :** 네트워크에서 중립지역을 뜻하며, 외부에 서비스를 제공해야 할 때 내부 자원을 보호호기 위해 내부네트워크와 분리시킨 공간을 말한다. 즉, 내부 네트워크와 외부 네트워크 사이에 DMZ라는 구간을 두어서 DMZ 내 서버의 침입으로부터 내부 네트워크를 보호 할 수 있다.