

해사 사이버보안의 이해

최성민*

*(주)오렌지씨큐리티 대표이사

요약 : 선박에 IT/OT가 도입되면서 사이버 위협이 증가하고 있습니다. 선박에서의 사이버 리스크 관리를 위해 현존하는 선박 내 사이버 자산을 식별하고, 노출된 사이버 위협을 인지하고, 사이버 리스크 평가를 통한 대응방안을 이론적, 사례적으로 분석한 내용을 공유합니다.

핵심용어 : 선박 사이버보안, 선박 사이버리스크 평가, 선박 사이버 사고

CYBER-SECURITY
1. 사이버보안의 개념

사이버보안의 개념

Machine: 이송로그 방식, 물리적 접근
OT (Operational Tech): 디지탈 방식, 근거리 네트워크 및 통제
IT (Information Tech): 클라우드, 모바일, IoT 등, 클라우드 적용

P 14/22 | 해사 사이버보안의 이해 - 개념과 실례

CYBER-INCIDENTS
3. 사이버사고 사례

해사 사이버사고 사례

선박 사고 예방 피해

매출손실 | 선체손실 | 화물손실 | 인명피해 | 환경오염

국가재산급피해
전문학적경제손실

P 13/22 | 해사 사이버보안의 이해 - 개념과 실례

MARITIME CYBER-SECURITY
2. 해사 사이버보안이란?

사이버보안의 개념

효율성 VS 보안성

효율성: 과거까지 해를 운항하여 운항비를 아꼈다, 최적의 경로로 운항하여 연료를 최소화했다, 선박(중)시스템의 도입하여 승객편의를 높였다
보안성: 재해전후가 유출/타입은 사람에게 인접한 것은 아니다, 위치정보가 범죄자의 알람으로 활용될 경우 안전장, 재도청가 인접하여 사용할 수 없는 것은 아니다

기밀성 / Confidentiality
무결성 / Integrity
가용성 / Availability

보안성

옛날 기술 저효율 선택, 최신 기술 고효율 선택

P 19/22 | 해사 사이버보안의 이해 - 개념과 실례

CYBER-RISK-MANAGEMENT
4. 사이버리스크 관리방안

사이버 리스크 관리 방법론

공통적인 요구사항: 사이버보안 정책, 사이버 사고 대응, 사이버 보안 교육

Regulator	Regulation	Guide	Standards
IMO	ISM code	BIMCO	NIST CSF
DCIMF	TMSA	DCSA	ISO 27001
	SIRE	ENISA	
RIGHTSHIP	RIGHTSHIP		
FSC	USCG	Certification	
FLAG STATE	Marshall Islands	KR CS	LR CES
	Panama	DNV-GL	ABS
	Singapore	ClassNK	CCS

P 18/22 | 해사 사이버보안의 이해 - 개념과 실례

MARITIME CYBER-SECURITY
2. 해사 사이버보안이란?

해상산업의 특징

IT자산: 서버/PC, N/W보안장치, SW/Application
OT자산: ECDIS, AIS, VDR

고려사항: USB포류가 있는 장비, 내시 코류가 있는 장비, W/P가 되는 장비, Windows가 설치된 장비, Linux가 설치된 장비

P 10/22 | 해사 사이버보안의 이해 - 개념과 실례

CYBER-RISK-MANAGEMENT
4. 사이버리스크 관리방안

사이버 자산 식별 및 취약점 점검

사이버 자산 분류: 경이통신시스템, 기동및추진시스템, 조타시스템, 화물관리시스템, 화재방지 및 소화시스템

사이버 취약점 분류: CVE Details, CVE ID, product, vendor, vulnerability type...

P 22/22 | 해사 사이버보안의 이해 - 개념과 실례

4. 사이버 리스크 관리 방안



P 25/22 | 행사/이벤트의 이해 - 3페이지 3페이지

5. 결론



Point 02
사이버 공격/사고로부터
안전한 환경



Point 01
지식경제부/중소기업
합수용가결안 사이버보안



Point 03
보안환경 하에서
다양한 선택 기술 개발

P 27/22 | 행사/이벤트의 이해 - 3페이지 3페이지