# **KR** Maritime Cyber Security

News from KOREAN REGISTER

Oct 2018

Vol. 006


한국선급 활동

- NSHC & SHIELD CONSULTING과 사이버보안 MOU 체결
- IACS 선박 사이버시스템 안전 핵심 권고서 배포

샌디에고 항구, 사이버 공격 당하다

사이버 위협의 이해

물리보안 체계 수립 가이드

용어 설명

# 한국선급 활동

## ● NSHC SECURITY & SHIELD COUNSULTING과 사이버보안 MOU 체결

지난 9월, 한국선급과 NSHC SECURITY & SHIELD CONSULTING은 선박 사이버보안 분야의 공동 연구 개발을 위해 상호 기술 교류 및 협력 강화를 위한 MOU를 체결하였다. 주요 MOU 체결 항목은 다음과 같다.

- 해상 사이버보안 관리 시스템 회사 인증 획득
- 선박 사이버보안 OT 시스템 규칙 적용 및 침투테스트 기술협력
- 선박 사이버보안 교육 컨텐츠 공동 개발

NSHC SECURITY는 ICS/SCADA(OT)사이버보안 분야에서 국내 및 아시아에서 유일하게 사이버 침투테스트 수행가능한 회사이며, 랜섬웨어, APT 공격과 같은 악성코드 분석 및 산업용 기기 대상 침투테스트 및 소스코드 진단을 수행하고 있다. SHIELD CONSULTING은 사이버보안에서 요구되는 물리적 보안(CCTV, 외부자 출입, 전자기기 반입 통제, 잠금장치) 컨설팅을 제공하고 있다.

이번 MOU 체결을 통해 한국선급은 선박 OT 시스템 침투테스트 기술력 확대 및 규칙 고도화가 예상되며, 미래선박(자율운항선박・무인화선박) 사이버안전 기술 기반을 마련할 것으로 판단된다.

## ● IACS, 선박 사이버시스템 안전 핵심 권고서 배포

국제 선급협회에서는 지난 9월 27일 선박 사이버시스템의 안전성 보장을 위한 12건의 핵심 권고안 중 9건을 배포하였다. 12건의 권고안은 소프트웨어 유지보수, 수동 백업 장치, 고장 시 비상계획, 네트워크 구조, 데이터 보증, 물리적 보안, 네트워크 보안, 선박 시스템 설계, 컴퓨터시스템 인벤토리, 시스템 통합, 원격 업데이트 및 접근, 통신 및 인터페이스 등으로 구성되며 한국선급은 **'고장 시 비상계획'** 권고서를 주도적으로 개발하였다.

사이버시스템 패널은 2016년 7월 신설되었으며 선박 사이버시스템(소프트웨어, 하드웨어, 네트워크, 데이터 등)의 사이버 안전이 주요 논의 대상이다. 3건의 권고서는 올해말까지 배포 예정이며, 향후 12건의 권고서를 하나의 문서로 통합하여 사이버 시스템 적용에 대한 통합 가이드라인 개발을 목표로 하고 있다. 권고서는 IACS 홈페이지를 통해 확인할 수 있다.

| Rec No | Title | Status |
|---|---|---|
| Rec 153 | Recommended procedures for software maintenance of shipboard equipment and systems | Published |
| Rec 154 | Recommendation concerning manual / local control capabilities for software dependent machinery systems | Published |
| Rec 155 | Contingency plan for onboard computer based systems | Published |
| Rec 156 | Network Architecture | Published |
| Rec 157 | Data Assurance | Published |
| Rec 158 | Physical Security of onboard computer based systems | Q4 2018 |
| Rec 159 | Network Security of onboard computer based systems | Published |
| Rec 160 | Vessel System Design | Q4 2018 |
| Rec 161 | Inventory List of computer based systems | Published |
| Rec 162 | Integration | Published |
| Rec 163 | Remote Update / Access | Published |
| Rec 164 | Communication and Interfaces | Q4 2018 |

Ref. International Association of Classification Societies

# 샌디에고 항구, 사이버 공격 당하다

샌디에고 항구 IT 시스템이 랜섬웨어 사이버 공격을 받은 것으로 확인되었다. 항구측은 지난 9월 25일 처음 시스템 붕괴에 대한 보고를 받았으며, 공공 안전 시스템을 최우선적으로 고려하여 영향을 최소화하고 시스템 기능을 복원하기 위해 업계 전문가 및 지역, 주, 연방 및 파트너 팀을 동원했다.

항구의 IT 시스템 중 일부가 공격에 의해 손상되었지만 다른 시스템도 예방책으로 폐쇄되었다. 항만 측은 사건의 범위와 시기, 피해 규모 및 복구 계획을 수립하고 있다고 밝혔다.

● **항구, 사이버공격 대상이 되고 있다.**

불과 일주일 전인 9월 20일, 바르셀로나 항구 또한 랜섬웨어 사이버 공격을 받은 것으로 나타났다. 현재까지 사이버 공격에 대한 기술적인 세부사항은 공개되어 있지 않지만 항구 보안 인프라의 여러 서버를 공격한 것으로 알려졌다. 지난 7월, 캘리포니아 롱비치 항구의 COSCO 해양 운송 회사의 항구 터미널이 랜섬웨어 공격을 받기도 했다. 3개 포트가 2개월만에 사이버 공격을 보고함에 따라, 일부에서는 위협 그룹이 의도적으로 표적으로 삼지 않았느지 의문을 품고 있다. 항구의 어떠한 혼란도 심각한 재정적 및 사회적 손실을 초래 할 수 있어 적절한 대책 마련이 필요하다.

**대응 방안 및 시사점**

사이버 위협에 대응하기 위해서는 체계적인 보안 시스템 운영 및 관리가 필요하며, 보안요원의 위기관리 대응과 신속한 초동조치 능력 향상을 위한 정기적인 훈련이 필요하다. 또한 임직원의 인식제고 교육 및 전문성 교육이 필요하며 침해사고 사례분석과 분기별 해킹방어 훈련을 통한 사이버 위협 대응이 필요하다.

Ref. www.zdnet.com

# 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 '**사람의 실수 및 파괴**'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 : 사람의 실수 및 파괴**

ICS 환경에서 근무하는 직원은 보안과 관련하여 특별한 위치에 있다. 이것은 사내 직원뿐만 아니라 모든 외부 직원에게도 적용된다. 예를들어, 유지 보수 또는 구축을 위해 시설에 접근 할 수 있거나 원격으로 업무를 할 수도 있다. 기술적 통제만으로 보안을 보장 할 수 없으므로, 항상 조직의 규제가 필요하다.

**<가능 시나리오>**

▣ 보안과 관련된 구성요소 (예 : 방화벽) 또는 네트워크 구성요소, ICS 구성요소 업데이트 또는 패치 설치로 인해 개별 구성 요소의 기능과 상호 작용에 문제 발생

▣ 의도적인 행동의 부작용 (장치 및 설비의 손상, 청취 장치 및 탭의 설치 등)

▣ 승인되지 않은 소프트웨어 또는 하드웨어로 인한 시스템 손상

(예 : 디지털 카메라, 스마트 폰 또는 운영자가 소유한 기타 USB 장치)

▣ 인프라 및 보안 구성 요소들에 대한 미사용 구성의 생성

(예 : 모바일을 통한 외부로부터의 무단 액세스를 허용하는 방화벽 규칙 추가)

위의 시나리오는 일반적으로 내부자 거래뿐만 아니라 부주의와 인적 실수로도 발생 할 수 있다. 특히 이러한 사고는 조직의 결점으로 인해 가용성이 크게 제한 될 수 있다.

**<대책>**

- 필요한 경우에만 민감한 데이터에 대한 액세스를 할 수 있다.
- 기능 및 보안 관련 구성 요소에 대한 운영자 및 관리자 권한을 보장하기 위해 자격 및 훈련 프로그램 및 인식 제고 조치는 지속 가능하도록 고안되어야하며 의무화되어야 한다.
- 운영 환경에 근접한 제어 시스템 및 운영자의 인터넷 액세스를 비활성화한다.
  - 전자 메일, ERP 등은 보안성이 뛰어난 별도의 네트워크에서 연결된다.
- 외부 계약자(제품 공급 업체, 서비스 제공 업체)뿐만 아니라 퇴직자 보안 관리가 필요하다.
- 임직원의 기술적 보안을 위한 적절한 정책 및 절차가 필요하다.
  (예 : 이동식 미디어 처리, 전자 메일 및 소셜 네트워크에서의 통신, 암호 정책, 개별 소프트웨어 설치 등).
- ICS 시스템 상태 및 구성 자동 모니터링

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

# 물리보안 체계 수립 가이드

## ● 물리보안 체계 수립의 필요성

주요시설의 보안구역에 대해 출입통제 및 시설보안에 관한 제반 절차와 기준을 정함으로써 훼손·변조·도난·유출 등의 다양한 형태의 위협으로부터 사무실 및 주요 사이버자산을 보호하기 위함이다. 회사 및 선박은 물리 및 환경 보안 기준을 적용하여 물리적 접근통제에 대한 분석 및 통합적 보호대책을 수립해야 한다.

## ● 한국선급 해상사이버보안 관리시스템 인증 검사항목(CSMS1)

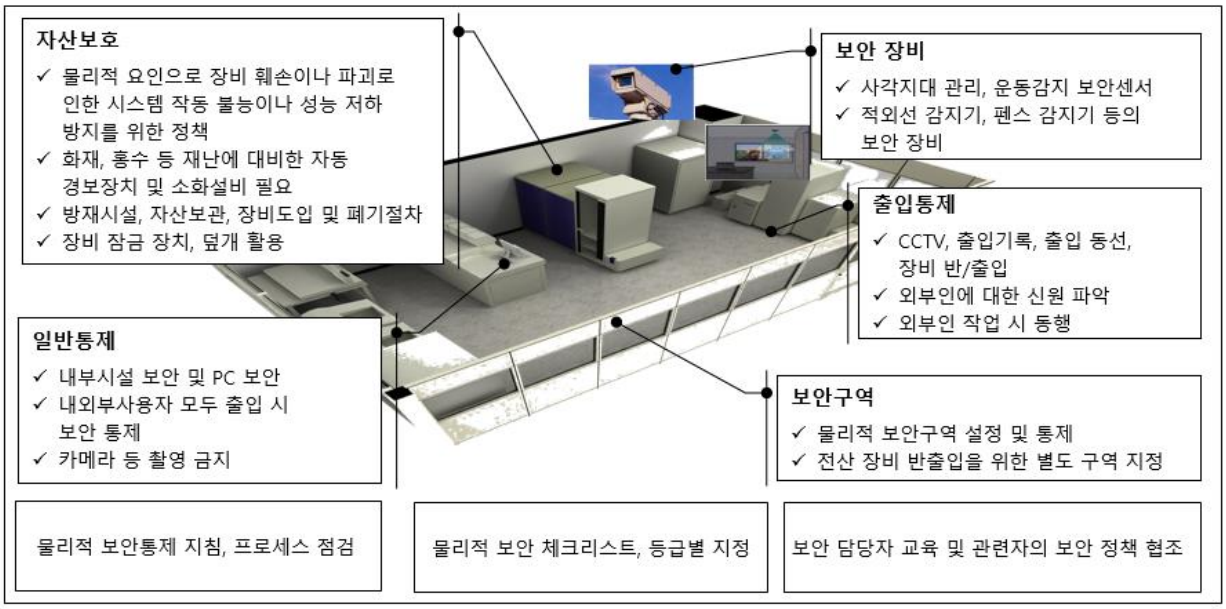
**물리보안 정책의 수립 (207.1) :** 회사는 시스템 장비, 설비, 시설 등에 대한 물리적 보안 기준을 정의한 정책을 수립하여야 한다.

**보호구역 통제 (207.2) :** 회사는 자산이 포함된 보호구역에 대해 인가된 자만 접근할 수 있도록 물리적 통제방안을 마련하여야 한다.

**휴대용 저장매체 통제 (207.8) :** 회사는 USB 등 휴대용 저장매체를 통한 내부 자산 및 네트워크 연결을 통제하여야 한다.

**휴대용 저장매체 통제 (207.11) :** 서류 및 휴대용 저장 매체가 보관된 공간의 클린데스크 운영 및 단말기 화면보호 정책이 마련되어 적용되어야 한다.

## ● 물리보안 용어 설명



● 제한구역 출입 통제(예시)


● 휴대용 장비 통제(예시)

# 용어 설명

- **사이버시스템 :** 정보 또는 데이터를 획득, 처리, 저장 또는 교환하기 위한 하드웨어 또는 소프트웨어 시스템 또는 서브시스템을 의미함(IMO MSC 94차)
- **사이버보안 :** 비인가된 사용자에 의해 의도적인 장애, 손상 또는 악의적인 사용으로부터 컴퓨터 네트워크 및 제어시스템을 보호하는 것을 말한다. 사이버 공간을 구성하는 시스템, 네트워크,응용 프로그램, 데이터 등을 보호하기 위한 기술적, 물리적, 관리적 활동을 의미한다.
- **사이버안전 :** 소유자, 운영자를 포함한 인가된 사용자에 의한 우발적인 사고 또는 사이버 시스템의 장애로 인한 의도하지 않은 결과로부터 컴퓨터 네트워크 및 제어시스템을 보호하는 것을 말한다. 사이버안전은 사이버보안을 포함하는 넓은 개념이며, 사이버 사고가 일어나지 않도록 온전한 상태를 의미한다.
- **침투테스트 :** PEN Test 또는 모의침투 테스트로 불리며, 사이버보안 수준을 살펴보기 위하여 사전에 협의된 시뮬레이션 공격이다. 경우에 따라 테스트 대상 시스템의 정보를 제공하는 화이트 박스 방식과 어떤 정보도 사전에 제공하지 않는 블랙박스 방식으로 구분된다.