KR Cybersecurity

News from KOREAN REGISTER

June 2018

Vol. 002

한국선급 활동

● **한국선급, 티원아이티와 사이버보안 MOU 체결**

지난 5월 18일, 한국선급과 ㈜티원아이티는 선박 사이버보안 분야의 공동 연구 개발을 위해 상호 기술 교류 및 협력 강화를 위한 MOU를 체결하였다. 티원아이티는 선박 전산장비 유지보수, SW개발 전문업체로서 현대상선, 에이치라인, 현대글로비스, KTSAT 등 해운, 통신, 조선 분야에서 고품질 IT 서비스를 제공하고 있다.

KR과 티원아이티간 기술 협력 내용은 아래와 같다.

- 선박 유지보수 업체를 위한 사이버보안 인증 기술 협력
- 육상 및 선상 실무적 사이버보안 교육 자료 구축
- 선상 사이버보안을 위한 기술 협력

이번 MOU 체결을 통해 한국선급의 사이버보안 인증 영역 확대가 예상되며, 실제 선박에 탑재되는 IT 시스템 사이버 취약점 및 사이버 공격 사례 분석을 통해 사이버 리스크평가 기술이 향상 될 것으로 예상된다. 분석된 자료는 8월부터 실시되는 KR 아카데미 교육자료 활용될 예정이다.

Increasing reliance on IT is going to mean increasingly big risk

EU 집행위원회 소속 사이버보안 담당기구 ENISA가 2016년 5월 제정해 2018년 5월부터 적용된 EU NIS(Network Information Security) Directive 가 장기적으로 선박 운항 시스템에도 영향을 미칠 것으로 예상된다.

- **EU NIS Directive, 선주 보다는 항만과 물류기업에 초점**

NIS Directive는 운송, 전력, 교통망, 금융 시장 인프라, 의료 및 디지털 인프라 등을 마비시킬 수 있는 사이버공격에 대응하여 보안 수준 강화를 요구한 지침으로, 서비스 운영자 및 디지털 서비스 제공 업체의 공통 최소 용량 구축 및 계획 요구 사항, 정보 교환, 협력 및 공통 보안 요구 사항을 담고 있다.

- **Increasing reliance on IT = Increasing big risk**

이에 따라 일부 선주 및 선박 운항 회사들은 본 지침이 GDPR과 마찬가지로 선박 내 시스템에 적용되는지 여부에 대해 높은 관심을 보였다. 이에 대해 European Maritime Cyber Risk Management Summit 의장 Philip Roche(Norton Rose Fulbright partner)은 해당 지침은 항만과 물류 시스템에 적용되는 반면, 해상 사이버보안은 여전히 IMO와 기국의 법률 중심이 될 것이라고 밝혔다. 다만, 2017년 Maersk 선사의 랜섬웨어 감염 사고에서 알 수 있드 항만과 물류 시스템의 보안 수준 강화 움직임은 IT 의존도가 높아지는 선박 운항과 화물 관리 분야의 산업 경쟁력에도 큰 영향을 미칠 것이라고 전망했다.

대응 방안 및 시사점

EU NIS Directive가 단기간 내 선주와 선박 운항회사에 영향을 미치지는 않겠지만 장기적으로 사이버보안 관련 Compliance 경쟁에 뒤쳐지지 않도록 각 대륙 또는 각 지역, 기업 등의 사이버보안 활동의 모니터링이 필요하다. 이를 위하여 KR 해상 사이버보안 가이드나 EU NIS 지침에 대한 이해도를 높여 나가야 한다.

Ref. : Cyber changes : the NIS Directive and the role of tech in transforming shipping, Marine Electronic & Communications, May, 2018

2018 Critical Infrastructure Attack Trend

전력망 뿐만 아니라, 의료, 제조, 에너지, 운송 분야 등 국가 기반시설에 대한 사이버 공격이 2018년에도 지속될 것으로 예상된다.

- **인터넷 연결을 고려하지 않았던 ICS, 사이버보안에 취약**

몇 년 전까지 기반시설의 사이버보안은 중요하지 않은 것으로 간주되었지만 미래에는 제어시스템 역시 사이버 공격에 예외가 아님을 이란 스턱스넷, 2015년 우크라이나 전력회사 해킹, 머스크 선사 랜섬웨어 감염사고 등이 입증해 왔다. 이러한 문제는 제어시스템에 사용되는 ICS 장비가 최근 인터넷 연결에 연결되고 있는 반면, 장비의 초기 설계 시에는 이런 문제를 전혀 고려하지 않았던 것에서 기인한다.

- **Supply Chain Threat & Security**

회사와 연관된 서비스, 장비 수급 회사의 사이버보안 수준은 하드웨어와 소프트웨어 보안 수준만큼 중요하다. 예를 들어 시스템을 잘 아는 관리인(또는 청소부)가 야간 시간에 무단으로 네트워크나 시스템에 접근할 수 있는 위협이 존재하듯 모니터링 또는 관리되지 않는 Supply Chain 또는 협력업체 인력의 사이버보안 수준은 의도하던 의도하지 않았던 회사와 선박의 사이버보안에 커다란 위협이 될 수 있다.

대응 방안 및 시사점

2018년 역시 피싱 공격의 비중이 여전히 높을 것으로 예상되는 만큼 임직원과 협력업체 직원의 사이버보안 인식제고 교육과 훈련이 이뤄져야 한다. 또한 인프라 보안 관점에서 외부와 통신하는 네트워크에는 접근통제 기술을 적용하고 협력회사들을 대상으로 사이버보안의 요구사항이 점검 및 관리되어야 한다. 특히 신규 및 기존 정보자산에 대하여 HW/SW 보안성 검토 실시가 요구된다.

Ref. : Critical infrastructure attacks on the rise, welivesecurity. May, 2018

Cybersecurity, A key factor to the Growth of Maritime Information

기술분야 시장 분석기관 Technavio가 Global maritime information market 분야가 2022년까지 연평균 10% 이상 성장할 것이라고 전망했다.

- **Communication, Navigation, and to Monitor and Control ships 성장 주도**

해상 정보 시장을 Platform(On-Shore, Vessel), Tracking Technology (AIS, SAR, LRIT), Application, End-users, and Region 등으로 구분한 이번 보고서는 해양 운송 분야를 중심으로 한 해양 산업의 성장을 예상하고 있다. 특히 해상정보 분석 기술, 선박 추적, 자동인증 시스템 등 해상 IT 분야는 해상 무역의 증가와 함께 4차 산업의 발전이 결합되어 금전적 인적 자원을 절약할 수 있을 것이라고 분석하고 이런 기술 발전은 해상 운송의 기회를 확대시켜 무역활동을 증가시키는 선순환을 이룰 것으로 전망했다.

- **Key Factor, Cyber Security**

다만 보고서는 해상 분야의 디지털화를 진척시키는데 있어 중요한 열쇠는 사이버 보안이 가지고 있다고 강조했다. 최근 선박 내 적용되는 대표적인 정보기술인 통신, 네비게이션, 선박 모니터링 및 통제 기술은 사이버보안이 전제되어야 하기 때문이다.

대응 방안 및 시사점

정보기술은 비용절감, 자원의 효율적 배치 등을 목적으로 도입되고 있으며, 해상 분야도 예외없이 적용될 수밖에 없다. 다만 이런 IT 자원의 도입은 사이버보안이 전제되어야 하며, 이를 위하여 선박 운영 회사 등은 IT 자원의 도입 시 사이버보안 보안성 검토, SW 개발물의 개발 보안 등을 적용하여 생산성에 대한 차질이 발생하지 않도록 유의하여야 한다.

Ref. : Global Maritime Information Market Analysis 2018 Forecast to 2022 with Inmarsat, Business Wire, May, 2018

사이버보안 조직 구성 가이드

● 사이버보안 조직 운영 지침 필요성

사이버보안 위협으로부터 대응하고 사이버보안 수준을 유지 및 향상 시키기 위해 회사는 사이버보안 활동을 수행하는 조직을 구성하고 관리하기 위한 책임과 역할을 정의하여야 하며, 조직 운영지침에는 사이버보안 조직 구성에 필요한 직무의 식별, 구성, 역할, 주요 기능이 지정되어야 한다. 조직 구성의 예시는 다음과 같다.

● 사이버보안 조직 구성도 및 역할과 책임

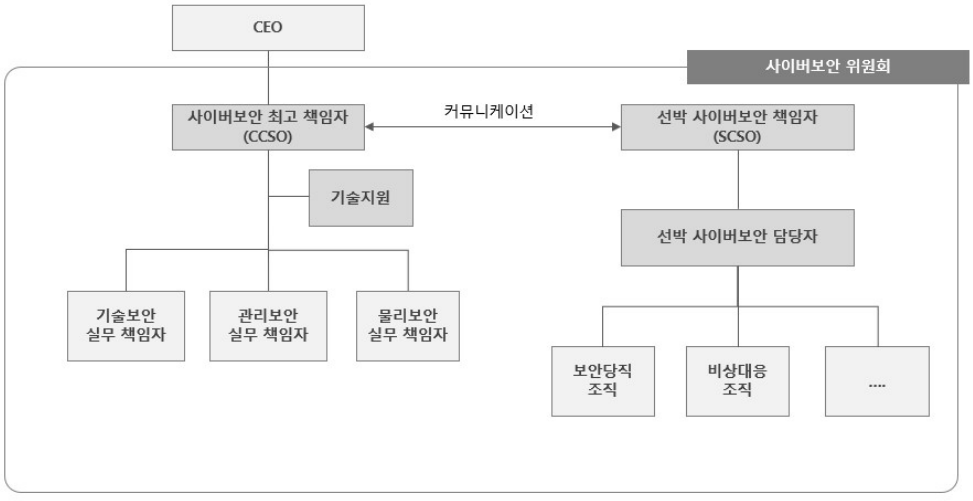
1) 사이버보안 최고 책임자(Chief Cyber Security Officer : CCSO)
사이버보안 정책의 수립, 사이버보안 조직 구성, 위험관리, 운영 등의 회사 전반에 걸친 사이버보안 관련 업무를 총괄 관리 (NIST 표준 : CIO)

2) 기술보안 실무 책임자
회사의 사이버보안 기술파트 총괄, 사이버보안 리스크평가 분석, 평가, 개선조치 이행, 사이버보안 사고 대응 및 복구, 교육 훈련 관리

3) 관리보안 실무 책임자
회사의 사이버보안 관리파트 총괄 계획과 집행의 조정 등의 역할을 총괄 수행, 보안점검 실시

4) 물리보안 실무 책임자
물리적 위험에 대한 사이버보안 물리파트 총괄 계획과 집행의 조정 등의 역할 및 보호대책의 강구와 이행 등의 총괄 업무를 수행

5) 선박 사이버보안 책임자(Ship Cyber Security Officer)
선박 내 사이버보안 조직의 구성과 운영 및 활동 총괄, 선박과 회사 간 사이버보안 활동 이슈 조정 및 보안 관리 프로세스 개선, 선박 사이버보안 위기 대응 관리체계 구축



Ref. : NIST SP 800-16 : A Role-Based Model for Federal Information Technology/ Cybersecurity Training

용어 설명

- **NIS Directive** : 정식명칭은 'The Directive on security of network and information systems'으로 2016년 5월 EU 사이버보안 산하기구 ENISA (European Union Agency for Network and Information Security) 중심으로 제정된 사이버보안 지침. 기업이나 정부기관 등 시스템 운영주체가 사이버보안을 위해 해야 할 조치를 명시하고 있다. 다만 EU 개인정보보호 관련 법률인 GDPR과 다르게 법률 수준은 아닌 지침의 수준으로 의무적 준수 조항은 아니다.
- **GDPR(General Data Protection Regulation) :** EU의 강력한 데이터 및 개인정보보호 법률. 지난 2018년 5월부터 시행되어 EU 영토 내에서 비즈니스가 이뤄지는 기업의 98% 이상이 해당 법률에 적용된다고 알려져 있으며, 개인정보를 제공하는 정보주체의 권리를 보장하는 초점을 맞추고 있다. 5월 27일 법 발효 첫날부터 페이스북, 구글 등 대형 IT 기업이 GDPR 위반으로 피소되었으며, 미국 주요 언론사는 제소를 피하기 위해 EU로부터 홈페이지 접속을 중단시키기도 했다.
- **Supply Chain Security** : Supply Chain Management라는 불리는 공급망 관리는 부품제공업자로부터 생산자, 배포자, 고객에 이르는 물류 흐름을 하나의 가치 사슬 관점에서 바라보는 일련의 관리과정에서 비롯된 것으로 Supply Chain에 속한 다양한 기업 중 일부 기업의 사이버보안 위협이 전체 사슬의 위협으로 나타날 수 있음을 의미한다.
- **피싱 공격(Phishing Attack) :** 이메일 메신저, 문자 등을 이용하여 신뢰할 수 있는 사람 또는 기업이 보낸 메시지인 것처럼 가장함으로써, 비밀번호 및 신용카드 정보와 같이 기밀을 요하는 정보를 부정하게 얻게 하거나 악성코드를 감염시키는 사회공학적 사이버 공격의 한 유형이다.