# KR Maritime Cyber Security

News from KOREAN REGISTER

Dec 2018

Vol. 008


한국선급 활동
2018 국제조선해양기자재컨퍼런스 발표

글로벌 해양 이슈 모니터 2018 동향

ISF가 예상하는 2019년 글로벌 보안 위협

선박 OT 시스템 백신 업데이트 가이드라인

선박 OT 영역에서의 사이버보안 이슈 및 대응방안

사이버 위협의 이해
- 엑스트라넷 및 클라우드 구성 요소의 손상

접근 통제 정책 수립 가이드

용어 설명

# 한국선급 활동

## ● 2018 국제조선해양기자재컨퍼런스(Kormarine Conference 2018) 발표

한국선급은 지난 11월 20일부터 21일까지 부산 해운대그랜드호텔에서 개최되는 2018 국제조선해양기자재컨퍼런스(Kormarine Conference 2018)에 참가하여 사이버보안, 황산화물 등 최근 해사업계의 주요 관심사를 발표하였다.

국제조선해양기자재컨퍼런스는 산업통상자원부, 부산광역시가 주최하고 한국조선해양기자재공업협동조합이 주관하는 행사로 '조선해양산업의 새로운 길을 묻다'를 주제로 하여, 국내외 25명의 연사들과 함께 환경규제 변화에 따른 조선해양산업의 동향 등을 다루었다.

한국선급에서는 김연태 상무가 첫 번째 세션인 '조선해양산업의 대변화'의 좌장을 맡아 자율운항선박, LNG 연료추진선, 사이버보안 등 해사업계의 최신 기술에 대한 논의를 이끌었다. 이 세션에서 박개명 사이버보안대응팀장은 국내외 기업의 사이버보안 시스템을 구축하고 관리한 경험을 바탕으로 사이버 보안의 실사례를 공유하고, 전망을 예측하였다. 김현태 책임검사원은 두 번째 세션인 '환경규제와 선박추진연료의 변화'에서, 최근 개최된 제 73차 해양환경보호위원회(MEPC)의 회의 결과를 포함하여 황산화물(Sox) 규제 등 국제해사기구(IMO)의 환경규제 동향에 대해 다루었다. 2018 Kormarine Conference와 관련된 보다 자세한 사항은 컨퍼런스 공식 홈페이지(www.kormarineconferences.org)에서 확인 할 수 있다.

# 글로벌 해양 이슈 모니터 2018 동향

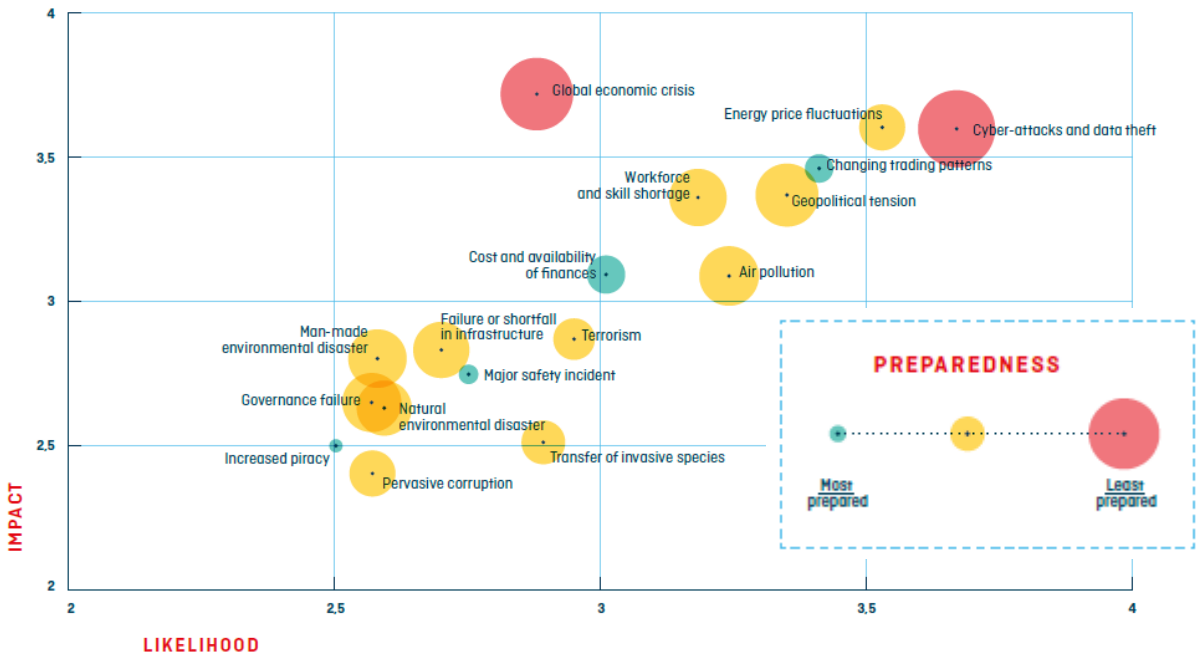
● **'사이버 공격 및 데이터 도용'이 가장 큰 영향 예상**

지난 10월 3일 홍콩에서 열린 글로벌 해양 포럼(Global Maritime Forum)에서 제공한 글로벌 해양 이슈 모니터(Global Maritime Issues Monitor) 2018 보고서에 따르면, 50개국 이상의 해양 관련 주요 이해 관계자에 대한 조사에서 '사이버 공격 및 데이터 도용'이 향후 10년동안 17가지 주요 글로벌 쟁점에서 가장 큰 영향을 미칠 가능성이 높은 것으로 나타났다. 순위는 잠재적으로 세계 해양 산업에 영향을 미칠 수 있는 다수의 쟁점에 대한 **영향력, 가능성, 준비성 측면**을 고려하여 산정되었다.

**1) 영향력(Impact) 측면 :** 해상 부문에서 가장 큰 잠재적 영향력을 가진 것으로 간주되는 상위 3가지 이슈는 글로벌 경제 위기(1), 에너지 가격변동(2), 사이버 공격 및 데이터 도용(3)로 나타났다.

**2) 가능성(Likelihood) 측면 :** 10년 내에 가장 많이 발생한다고 간주되는 상위 3가지 이슈는 사이버 공격 및 데이터절도(1), 에너지 가격 변동(2), 변화하는 거래패턴(3)으로 나타났다.

**3) 준비성(Preparedness) 측면 :** 준비가 미흡하다고 간주되는 상위 3가지 이슈는 사이버 공격 및 데이터절도(1), 세계경제위기(2), 지정학적 긴장감(3)으로 나타났다.




Ref. : Global Maritime Issues Monitor 2018

# ISF가 예상하는 2019년 글로벌 보안 위협

● **2019년 기업들이 직면할 4가지 보안 위협 요소**

정보 보안 포럼(ISF : Information Security Forum)에서는 기업들이 2019년 직면하게 될 보안 위협 요소 4가지를 다음과 같이 공개하였다.

- **사이버 범죄와 랜섬웨어 정교화 :** 범죄 조직들은 계속 발전할 것이고 공격 방법은 점점 더 정교해질 것이다. 2017년에는 랜섬웨어 공격으로 전 세계적으로 5조 이상의 손실이 발생하였다. 2019년에는 모바일 악성코드 및 모바일 랜섬웨어 등 개인 스마트 기기 대상 공격이 증가할 것으로 예상된다.
- **입법의 영향 :** 기업은 현재 및 계류중인 법률을 준수하기에 충분한 지식과 자원이 부족하다. 또한 법률은 특성상 정부와 규제 당국이 주도하고 있어 국가 간 협력이 필요한 시점에 국가 규제로 옮겨 가고 있다. 기업은 비즈니스 모델에 영향을 미칠 수 있는 변화를 계속 따라가기 위해 애쓸 것이다.
- **스마트기기 데이터 무결성 문제 :** 기업은 스마트기기가 설계의 불안전으로 인해 공격자에게 많은 기회를 제공한다는 사실을 인식하지 못하고 사용 할 것이다. 또한 기업이 고객이 의도하지 않은 방식으로 개인 데이터가 사용될 수 있는 사물인터넷(IoT)의 투명성 결여가 증가 할 것이다. 기업이 어떤 정보가 외부로 유출 될 것인지 또는 스마트 폰, 스마트 TV 또는 회의 전화기와 같은 기기에 의해 비밀리에 캡처되고 전송되는 정보를 아는 것은 문제가 된다. 투명성 위반이 발생하면 기업은 고객의 부적절한 데이터 보호에 대한 책임을 져야 한다.
- **공급망 신뢰성 보증 :** 공급망은 모든 조직의 글로벌 비즈니스 운영과 오늘날 세계 경제의 중추적인 요소다. 그러나 가치 있고 민감한 정보의 범위는 종종 공급자와 공유되며, 그러한 정보가 공유될 때 직접적인 통제는 상실된다. 2019년에는 공급망 보안을 확보하는 것이 중요함을 알게 될 것이며, 핵심 데이터를 관리하고 공급망 제공자와 관계 없이 여러 채널과 경계에서 공유된 위치와 방법을 파악하는데 다시 초점을 맞춰야 할 것이다. 이로 인해 많은 기업이 이미 과중한 보안 부서에 부담을 더하게 될 것이다. 자체 인증 감사 및 보증과 같은 전통적인 접근 방식은 단기간 공급망 보안을 유지할 수 있지만 근본적인 해결책이 아님을 깨닫게 될 것이다.

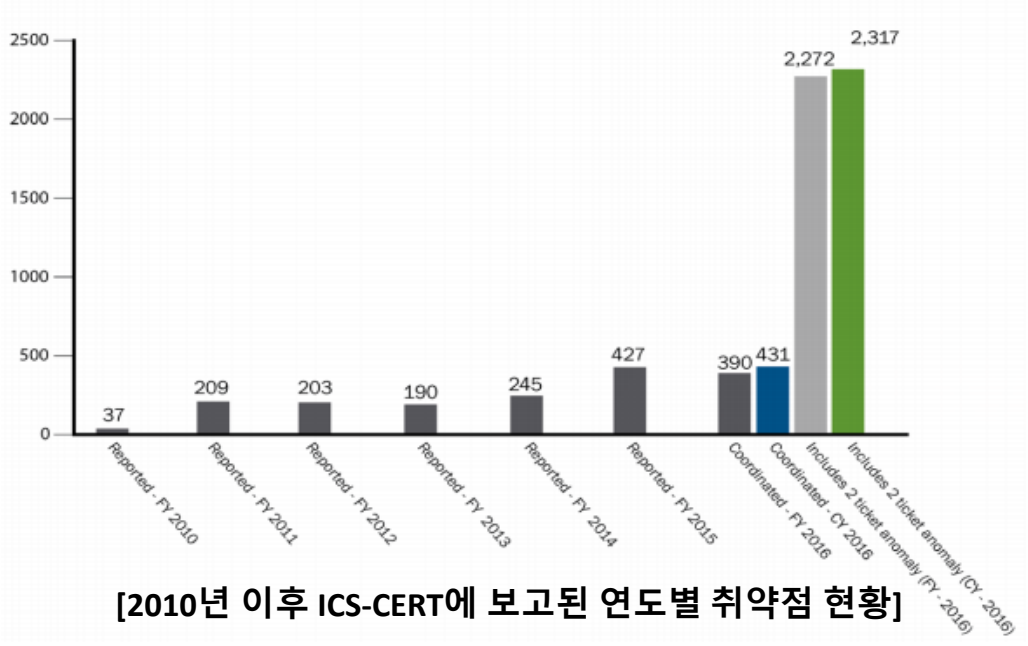
Ref. : Information Security Forum Forecasts : 2019 Global Security Threatt Outlook

# 선박 OT 시스템 백신 업데이트 가이드라인

## ● 선박 OT 시스템 백신 업데이트 어떻게 해야할까?

Zero-Day 취약점을 이용한 공격, 다양한 악성코드 변종의 등장으로 안티 바이러스 백신(이하 백신)의 필요성에대해 많은 논쟁이 있음에도 불구하고 백신은 사이버보안에 있어 가장 기초적인 보호 수단이라는 사실은 변함이 없다. 하지만 PC와 서버와 같은 정보시스템과 달리 선박 등에 사용되는 선박 운영 시스템(OT : Operating Technology)에서는 백신이 제한적으로만 운영되고 있다. 대표적인 이유는 아직까지 백신의 필요성을 느끼지 못했거나 관리 어려움이 가장 큰 이유일 것이다. 통상적으로 SW 개발회사는 보안패치를 정기적으로 발표하여 SW 이용자를 보호하게 되는데 Zero-Day 공격은 특정 SW가 가진 보안 취약점을 회사가 인지하지 못하거나 회사의 공식적인 보안 패치가 나오지 않은 시점에서 이루어지는 공격을 말한다.

정보시스템에 비해 덜 알려져 있기는 하지만 OT 보안 취약점은 꾸준히 등장하고 있으며, 특히 2016년 이후 큰 폭의 증가세를 보이기도 했다. 아래 그래프는 2017년 미국 ICS-CERT가 발표한 취약점 보고서의 내용으로 일정한 수의 취약점이 2016년 급격한 증가가 이뤄진 것을 알 수 있다. OT 보안에 있어 SW 취약점이 계속적으로 주목 받을 것이라는 사실과 이런 문제에 백신 또는 보안 패치와 같은 보호수단의 운영이 필요하다는 점은 분명해 보인다.




**[2010년 이후 ICS-CERT에 보고된 연도별 취약점 현황]**

Ref. : Recommended Practice: Updating Antivirus in an Industrial Control System

다만, OT 시스템을 관리하는 관점에서 무조건적으로 백신을 업데이트하거나 보안 패치를 적용하는 것이 능사는 아니다. 가용성이 가장 중요한 OT 시스템의 경우 백신 설치 및 업데이트(보안 패치) 과정에서의 설치 오류, 타 시스템 기능과의 충돌, 오래된 SW 버전 사용으로 인한 이슈 등이 발생할 수 있기 때문이다. 이는 선박 관리 회사의 입장에서 가장 큰 우려사항이기도 하다.

이에 대해 ICS-CERT는 2018년 8월 다음과 같은 백신 업데이트의 설치 및 적용에 필요한 보안절차를 권고사항(Recommended Practice : Updating Antivirus in an ICS) 을 제시하고 있어 유용하게 참고 할 수 있다.

- 백신의 업데이트 출처에 대한 확인하고 업데이트 파일을 전용 호스트(서버 또는 워크스테이션)로 다운로드 : 백신 회사의 배포 여부 확인 필요
- 다운로드한 파일에서 악성코드 검색 : 바이러스 토탈(https://www.virustotal.com)
- 다운로드한 각 파일의 암호화 해시 확인
- 다운로드된 백신 업데이트 파일을 저장할 이동식 저장매체의 무결성 확인
- 백신 업데이트 파일의 저장 후 저장매체 파일 잠금 장치 적용
- 선박과 유사한 OT 시스템으로의 업데이트를 통해 해당 파일의 악영향 확인
- 중요하지 않은 엔드포인트(PC) 또는 시스템부터 업데이트를 실시하고 오류 등 이슈사항 검토
- 시스템의 비정상적인 작동 상태를 모니터링하고 OT시스템의 정상동작 여부 확인

이와 같은 업데이트 과정 및 절차는 선박 관리회사의 환경과 선박에 따라 조금씩 차이를 보일 수 있지만 핵심은 외부로부터 전달받은 파일의 무결성의 유지 여부, 파일을 옮기는 과정에서의 악성코드 감염 여부 그리고 적용 후 장애 등의 이슈 발생 여부에 대한 지속적인 관리이다. 선박의 사이버보안은 선박 운항의 안전과 직결되는 중요한 요소인 만큼 단순한 업데이트라고 치부하는 것이 아닌 체계화된 절차를 수립하고 운영하는 노력이 필요하다.

▪ 본 기사는 (㈜ 씨드젠 임재우 이사에 의해 작성되었습니다.

씨드젠은 정보보안 및 개인정보보호 컨설팅, 정보보안 교육 서비스를 제공하는 정보보안 전문업체이다. 공공기관 및 산업분야의 400여개 기업을 대상으로 ISO 27001 및 정보보호 관련 컨설팅을 수행하였으며, 정보보안 인식제고 및 교육 훈련을 위한 SETA(Seedgen Education Training Awareness)를 운영하여 정보보호 인식제고 훈련, 온·오프라인 교육, 모의훈련 등의 실습 서비스를 제공하고 있다.

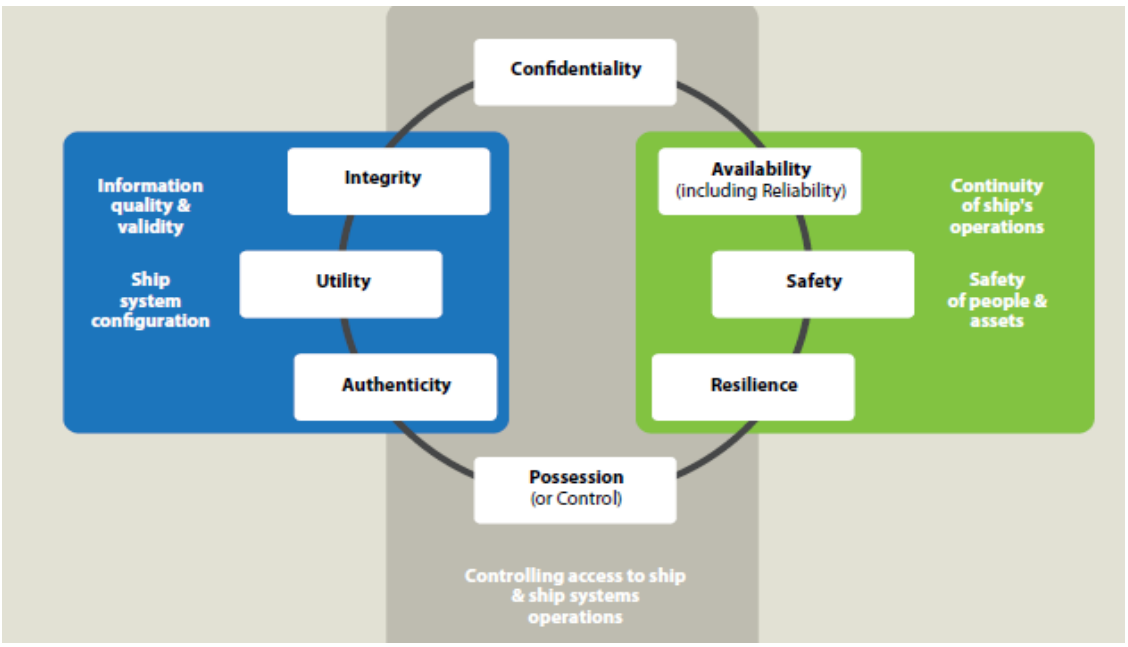
# 선박 OT 영역에서의 사이버보안 이슈 및 대응방안

## ● ICS/SCADA 영역에서의 사이버보안 담당자의 역할은?

선박에서의 OZ(Operation zone, 운영환경) 영역에서의 ICS/SCADA 보안은 다른 중요 기반 시설의 OT(Operation Technology, 운영환경)과 마찬가지로, 인터넷 환경과 별도의 운영 환경이므로 해운업계 종사자의 대부분은 자신들의 선박에 있어서 크게 고려할 사항이 아니라고 생각한다.

ICS/SCADA 보안을 논의하려면 선박이나 항만 뿐만 아니라 중요 기반시설 전반에 걸쳐서 활용되는 산업 제어 시스템에 대한 이해가 선행되어야 한다. ICS/SCADA는 산업 제어 시스템(ICS: Industrial Control System)과 감시 제어 및 데이터 취득(SCADA: Supervisory Control And Data Acquisition)의 약어로서, SCADA는 물리적으로 떨어져 있는 여러 플랜트의 생산 공정을 중앙에서 감시 제어하는 소프트웨어로서 무인 장소의 PLC(Programmable Logic Controllers)와 센서로부터 수집된 정보를 중앙에서 처리·분석해 설비를 제어하는 시스템이라고 볼 수 있다. 육상에서는 전기 배선망, 폐수처리 시스템, 전철관리 시스템등의 중요 사회 인프라망에 쓰이고 있다.

선박에서는, GICOMS, AIS, LRIT, SSAS 들도 광범위하게 보면 ICS/SCADA 영역 내에 포함되고, 최근 유행하는 모바일 어플리케이션을 이용해서 육상에서 선박 데이터를 실시간 확인하는 것도 포함된다.




Ref. : IET Standard : Code of Practice Cyber Security for Ships

사실 ICS (산업 제어 시스템)이 네트워크에 연결되기 전에는 사이버 위협에 대해서 걱정할 필요가 없었고. 선박에서는 제한된 네트워크 연결과 전송속도, 전송량으로 인하여 문제가 될 수 없는 부분이였다. 하지만 운영기술(OT)은 정보기술(IT)과 융합을 지속적으로 발전되어 왔다. 이렇게 OT를 위해서 IT를 활용하지만, 정작 IT 담당자들은 선박네트워크에 대한 다양한 운영상의 요구사항을 충분히 이해하지 못한 상태에서 사이버보안에 대한 책임을 요구 받고 있다. 선사에서는 이미 안전품질관리팀에게 ICS 운영자로서 사이버보안에 대한 역할을 요구하고 있다.

그렇다면, ICS/SCADA 영역에서의 사이버보안 담당자는 무엇을 해야 될까? ICS에서의 사이버 공격 가능성을 줄이고 공격이 발생해도 신속하게 복구를 하려면, 취약성 평가를 통한 지속적인 모니터링과 로그관리를 시행해야 한다.

- **취약성 평가 :** 알려진 취약점을 수정하는 것은 ICS보안의 필수이다. ICS 운영자는 Siemens, ABB, Honeywell 및 ICS-CERT와 같은 주요 Vendor 사가 공개한 취약점에 대해 확인을 하고, 사이버보안 관련 업체 또는 조직에서 공개하는 취약점을 분석할 수 있는 능력을 갖추어야 한다.
- **지속적인 모니터링 :** 스위치, 라우터 및 방화벽등과 같은 장치들에서 발생되는 상황을 항상 확인하기는 어렵다. 그러나 SCADA 또는 MES 응용 프로그램을 실행하는 서버, 워크스테이션, Intelligent Ethernet 장치 및 PLC와 같은 네트워크에 연결된 장비들은 더 어렵다. 지속적인 모니터링은 보안구성관리(SCM)를 이용해서, 보안기준을 설정하여 ICS에서 발생하는 모든 변경사항을 검색하는 것이다.
- **로그 관리 :** ICS의 다양한 장치들은 네트워크 작동 방식, 작동 중단과 관련된 잠재적인 오류 및 여러 가지 실패한 로그인과 같은 보안 이벤트에 대한 정보가 포함된 로그를 보낼 수 있다. 로그관리는 서버, 애플리케이션, 네트워크 장치, 방화벽 및 데이터베이스와 같은 다양한 종류의 자산에서 중앙 저장소로 로그를 수집하여 포렌식 분석에 사용할 수 있도록 하는 기능이다.

▪ 본 기사는 (㈜ NSHC & Shield Consulting co.,ltd 이승준 책임연구원에 의해 작성되었습니다.

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.

# 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 '**엑스트라넷 및 클라우드 구성 요소의 손상**'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 : 엑스트라넷 및 클라우드 구성 요소의 손상**

기존의 IT 부서에서 IT 구성 요소를 아웃소싱하는 추세는 ICS 부문에서도 점차 커지고 있다. 일반적으로 지연 시간은 실시간 요구 사항이 충족되지 않도록 하기 때문에 실제 프로세스를 직접 제어하는 구성 요소는 관련이 없다. 그러나 기계 구성이나 제조 프로세스 최적화를 위한 복잡한 모델 계산 (Big Data)을 위해 데이터 캡처 및 처리 분야에서 외부적으로 운영되는 소프트웨어 구성 요소 공급 업체 수는 지속적으로 증가하고 있다.

보안 관련 구성 요소는 클라우드 기반 솔루션으로 제공되는 경우도 있다. 예를 들어, 원격 유지보수 솔루션 공급업체는 원격 액세스 용 클라이언트 시스템을 클라우드에 배치하여 유지 보수 기술자가 여러 구성 요소에 액세스 할 수 있다. 그러나 이러한 클라우드 솔루션은 자산 소유자가 이러한 구성 요소의 안정성에 대한 제어 권한을 제한적으로 가지고 있지만 여전히 로컬 프로덕션에 직접 연결될 수 있다.

**<가능 시나리오>**

▣ 서비스 거부 공격(DoS)과 같은 로컬 프로덕션과 아웃소싱 된(클라우드) 구성 요소 간의 통신 방해 또는 캐스케이드 효과는 로컬 프로덕션을 저해할 수 있다.

▣ 외부에 저장된 데이터(도난, 삭제)에 액세스하기 위한 구현 오류 또는 불충분한 보안 메커니즘을 악용할 수 있다.

▣ 클라우드 제공자의 클라이언트가 충분히 분리되지 않으면 다른 클라우드 서비스에 대한 공격으로 인해 간섭(부수적인 손상)을 초래할 수 있다.

**<대책>**

- 서비스 수준 계약(SLA)을 통해 충분한 수준을 제공하기 위한 외부 구성요소 운영자의 계약상 의무를 명시한다.
- 신뢰할 수 있고 가능한 공인 서비스 공급자를 사용한다.
- 제어 능력을 유지하고 프로세스 노하우를 보호하기 위한 사설 클라우드를 운영한다.
- 클라우드에 저장된 데이터를 보호하기 위해 충분히 강력한 암호화 메커니즘 (암호화, 무결성 보호)을 사용한다.
- 가상사설망(VPN)을 사용하여 로컬 프로덕션과 외부 구성 요소 간의 연결을 보호한다.

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

# 접근 통제 정책 수립 가이드

## ● 접근 통제 정책 수립 필요성

비 인가자가 손쉽게 네트워크 및 파일에 접근하면 회사의 기밀 정보가 유출 될 수 있으므로 적절한 접근 통제 정책 수립이 필요하다. 정책서에는 접근 통제가 요구되는 업무가 정의되어 있고, 이 업무에 대한 접근 통제 방법과 범위 등을 문서화해야하며, 데이터, 프로그램, 주요 시스템, 네트워크 등의 접근 통제 대상을 명확하게 식별할 수 있도록 정의하여야 한다. 보안상 중요한 접근통제 규칙의 경우, 관리자의 승인을 거쳐서만 설정 또는 변경되어야 하며, 접근통제 정책이 주변 환경의 변화 또는 사업 내용이나 정보시스템 환경의 변화에 따라 적정한지를 검토하며, 사용자 접근권한에 대한 모니터링 수행을 정기적으로 검토하고 승인하여야 한다.

## ● 한국선급 해상사이버보안 관리시스템 인증 검사항목(CSMS1)

**접근 통제 정책 수립(206.1) :** 운영시스템 접근권한에 대한 기준, 원칙, 절차 등을 포함한 접근통제 정책을 수립하여야 한다.

**접근 통제 실행 (206.3) :** 일반 사용자와 관리자의 권한을 차등 부여하고 업무별 권한 기준을 정의하여야 한다.

## ● 접근 권한의 정의 (예시)

| 구 분 | 정의 | 부여 대상 |
|---|---|---|
| 시스템 최고 관리자 | 시스템 또는 서비스의 모든 계정관리, 데이터 조회 및 삭제, 접근권한 설정에 대하여 읽기, 쓰기, 실행 권한을 모두 가진 사용자 | 시스템 관리자 |
| 중간 관리자 (운영자) | 시스템 또는 서비스의 계정 부여, 계정별 접근권한 부여 관리 등에 대하여 읽기, 쓰기 권한을 가진 관리자 | 유관 부서별 관리자 |
| 일반 이용자 | 중간 관리자로부터 권한을 부여받아 실무를 수행하며, 데이터 읽기 · 쓰기 · 다운로드 등의 권한을 가진 이용자 | 시스템 및 서비스를 통하여 업무를 수행하는 담당자 |
| 특수권한 관리자 | 특수권한 예 : SetID, SetGID<br>- SetID : 소유자만 접근 가능한 파일에 일반 유저로 접근이 필요할 때 사용하는 계정<br>- SetGID : 소유 그룹만 접근 가능한 파일에 일반 유저로 접근이 필요할 때 사용하는 계정 | 시스템 관리자 |

● **접근 권한의 기준 (예시)**

| 자산 유형 | 권한 부여 유형 | | | |
|---|---|---|---|---|
| | 최고관리자 | 중간관리자 | 일반 이용자 | 특수권한 관리자 |
| 네트워크 장비 | O | O | - | △ |
| 시스템(서버) | O | O | - | O |
| 애플리케이션 | O | O | O | O |
| DB | O | O | - | O |

● **접근 통제를 위한 보안시스템 목록(예시)**

| 접근통제를 위한 보안시스템 목록(예시) | 설치 위치 |
|---|---|
| 방화벽/UTM/IPS(Intrusion Prevention System) | 네트워크 |
| ACL(Access Control Layer) | 네트워크 |
| DB 접근제어 | 시스템 or 네트워크 or 애플리케이션 |
| 시스템 접근제어(Secure OS) | 시스템 |

● **접속기록의 검토방안 양식(예시)**

| 점검시스템 | | 점검범위 | |
|---|---|---|---|
| 점검 날짜 | | 점검자 | |

| 체크리스트 | 점검결과 | 비고 |
|---|---|---|
| 1. 허용된 IP 주소 이외의 주소지에서의 접근 시도 | | |
| 2. 근무시간 이외의 시간 내 접속 시도 | | |
| 3. 반복된 로그인 실패 여부 | | |
| 4. 비인가된 시스템으로의 접속 시도 여부 | | |
| ... | | |
| ... | | |

# 용어 설명

- **Global Maritime Forum :** 글로벌 해양 포럼은 세계 해양 산업의 잠재력을 증진하는데 전념하는 비영리 국제기구이다. 미션을 수행하기 위해 정책 입안자, 전문가, NGO 및 기타 영향력 있는 해양 공동체 지도자들을 모아 집단적 과제를 논의하고 새로운 해결책 및 행동 권고안을 개발하기 위해 협력하고 있다. 연례 정상회의는 2018년 10월 3일 홍콩에서 개최되었다.
- **DoS(Denial of Service) :** 네트워크에 데이터가 가득 차서 합법적이고 인증된 사용자가 정보에 액세스하지 못하도록 한다. 분산 서비스 거부(DDoS) 공격은 DoS 공격을 실행하기 위해 여러 컴퓨터 및/또는 서버를 제어한다. [BIMCO]
- **VPN(Virtual Private Network) :** 사용자가 자신의 컴퓨팅 장치가 사설 네트워크에 직접 연결되어있는 것처럼 공유 또는 공용 네트워크를 통해 데이터를 보내고 받을 수 있으므로 사설 네트워크의 기능, 보안 및 관리 정책의 이점을 얻을 수 있다. [BIMCO]
- **ICS-CERT :** 미국 국토안보부(DHS : Department of Homeland Security)는 2003년 9월 사이버 공격 방어 및 대응을 위한 미국 인터넷 인프라를 보호하기 위해 US-CERT를 창설하였다. 2009년 국가 사이버보안 및 커뮤니케이션 통합 센터(NCCIC)를 설립하였으며 US-CERT는 NCCIC 산하기관으로써 산업 제어 시스템 위기대응팀(ICS-CERT : Industrial Control Systems Cyber Emergency Readiness Team)과 함께 24시간 사이버 사건을 접수 및 대응하고 있다.
- **클라우드 :** 소프트웨어와 데이터를 인터넷과 연결된 중앙 컴퓨서에 저장하여 인터넷에 접속하기만 하면 언제 어디서든 데이터를 이용할 수 있는 기술을 의미한다. 클라우드 서비스는 기존 웹 환경의 보안 취약점을 그대로 가지게 되므로, 도난, 유출 및 삭제로부터 저장된 데이터를 보호하기 위한 클라우드 보안이 필요하다.