KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 025

May 2020

한국선급 활동

- ㈜썬에이스해운, 해사 사이버보안 맞춤형 교육 실시
- 한국선급, 사이버보안 서비스 KR-CS++ 출시

MSC 선사, 멀웨어 공격으로 '홈페이지 접속 중단' 사고 발생

디지털 컨테이너 해운협회, 사이버보안 가이드라인 발표

사이버 위협의 이해(OWASP Top 10 Internet of Things)

KR 해상 사이버보안 형식승인 지침의 이해

용어 설명

한국선급 활동#1

㈜썬에이스해운에 해사 사이버보안 맞춤형 교육 실시

한국선급은 지난 4월 2일, ㈜썬에이스해운에 사이버보안 맞춤형 교육을 실시하였다. 본 교육은 임직원 인식제고를 위한 '해사 사이버보안의 이해(8시간/1일)' 과정으로 해사 사이버보안에 대한 전반적인 이해, 해사 사이버 위협 및 대응 현황, 해사 사이버리스크 저감 방법 및 실 사례, 사이버 자산 목록 작성 및 사이버리스크 평가 실습을 포함하여 OCIMF의 TMSA, SIRE 검사 외에 국제해사기구(IMO) 해사안전위원회(MSC) 98차에서 결의한 '안전관리시스템에서의 사이버 리스크 관리(Resolution MSC.428(98))'에 대응 방법을 제공하였다.

한국선급은 이번 교육에 대한 고객 만족도 조사에서 교육 내용이 OCIMF 검사 및 ISM Code 사이버리스크 관리 관련 준비에 매우 도움이 되었으며, 사이버리스크 평가 실습 통해 사이버보안 역량 강화에 큰 도움이 되었다는 피드백을 수렴하였다.

한국선급은 고객에게 보다 전문적인 교육 서비스를 제공하기 위해 노력하고 있다. 2018년 '국가인적자원개발 컨소시엄 교육' 운영기관으로 지정되어 국내 해사분야 재직자를 대상으로 해사 사이버보안 교육을 무상으로 제공하고 있으며 영국 SONGA선사, 산쇼코리아㈜, 태국 V.L. Enterprise PLC 등 국내외 선사가 화주 사이버보안 검사에 대응할 수 있도록 맞춤형 사이버보안 교육을 진행한 바 있다. 특히 '해사 사이버보안의 이해' 과정은 싱가포르 해사청(MPA)에서 주관하는 교육지원사업(MCF : Maritime Cluster Funding)에 2020년 포함되어 싱가포르 유수 선사 임직원을 대상으로 맞춤형 사이버보안 교육을 제공하고 있다.

향후 선사 뿐만 아니라 조선소, 기자재업체를 대상으로 사이버보안 맞춤형 교육 서비스를 강화할 예정이다.

한국선급, 사이버보안 서비스 KR-CS++ 출시

한국선급(KR, 회장 이형철)은 사이버보안 서비스 브랜드인 KR-CS++를 출시했다고 밝혔다.

KR-CS++는 'Beyond KR Cyber Security Service'라는 의미로, 고객들이 2021년 1월 1일 부로 발효되는 국제해사기구(IMO)의 사이버 리스크 관리에 관한 결의(MSC 428(98)를 이행하는데 실질적인 도움을 제공하기 위한 서비스 이다.

이번에 출시한 KR-CS++ 2020은 사이버보안 인식제고 교육 동영상과 사이버보안 실무 해설서를 포함하고 있다. 사이버보안 인식제고 교육 동영상은 한국선급이 2017년부터 국내외 고객을 대상으로 제공해 왔던 사이버보안 교육 서비스를 교육 동영상으로 자체 제작하였으며, '해사 사이버보안의 이해(https://youtu.be/fSIDLMj4gho)' 와 '해사 사이버보안의 관리 실무(https://youtu.be/67t0ckrNtiA)' 로 구성되어져 있다. '해사 사이버보안의 이해' 는 전체 직원의 사이버 보안 인식제고교육을 위한 내용으로 해사 사이버보안의 개요, 사이버 사고 사례 등으로 구성하였으며, '해사 사이버보안의 관리 실무' 는 실무자를 위한 내용으로 사이버 리스크 관리 수행방법 등으로 구성되어 있다. 또한, 사이버보안 실무 해설서에는 회사 및 선박에서 사이버보안 실무자를 위한 해설서와 실무에 즉시 적용 가능한 샘플 문서 양식을 포함하고 있다.

한국선급은 향후 KR-CS++ 2021 버전에서 보다 더 다양한 사이버보안 교육 컨텐츠를 담을 예정이며, 보다 쉽게 해사 사이버보안 체계 수립을 돕기 위한 서비스를 개발하여 스마트 패드 형태로 제공할 예정이다.

MSC 선사, 멀웨어 공격으로 홈페이지 접속 중단

세계 2위 컨테이너 선사 MCS가 멀웨어 공격으로 인한 홈페이지 중단 사고 발생

세계 2위 컨테이너 선사인 MSC는 지난 4월 9일부터 13일 5일 간 홈페이지 접속이 중단되는 사고가 발생했다. MSC는 4월 10일부터 13일까지 부활절 휴일이었으며, 코로나19로 인해 대부분의 직원들이 원격이나 재택근무 중이었던 것으로 알려졌다. 이 회사 홈페이지 등은 4월 9일부터 시스템에 침투하거나 피해를 입히기 위한 멀웨어 공격을 받은 것으로 추정된다.

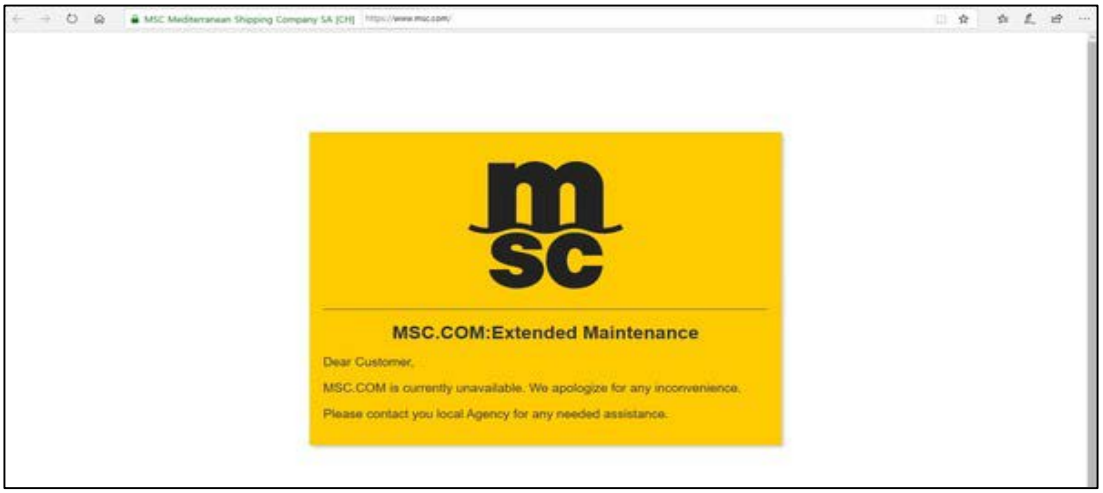
사이버 공격 대상은 제네바 본사에 집중되었으며, MSC는 본사와 지사 간 IT시스템이 분리되어 있어 사이버 공격으로 인한 피해는 본사의 데이터 센터에서만 발생 했다. 터미널을 비롯한 다른 IT 시스템은 정상 가동했다.

사이버 공격에도 타사의 온라인 플랫폼(인트라, GT넥서스, 카고스마트)를 이용하거나 전화를 통한 업무는 가능해 혼란을 최소화했다. 회사측은 "일부 디지털 툴의 이용 중단에도 모든 업무는 평소처럼 고객을 응대했으며, 화물의 이동도 평소와 다름 없었다."고 밝혔다. 이번 사이버 사고로 인해 회사에 적지않은 타격을 입었을 것으로 예상된다.

이번 사이버 공격은 글로벌 컨테이너 선사에 대한 세 번째 공격이다. 2017년 6월 랜섬웨어 페티야의 공격으로 IT시스템이 일부 중단된 머스크의 물동량은 20% 감소했다. 당시 추산 피해액은 2억 5000만 달러~3억 달러이다. 2018년 7월에는 COSCO의 미주 웹사이트와 이메일 시스템이 사이버 공격을 당했다. 미주지역 네트워크가 이상을 일으켜 미주 지역 이메일과 전화가 일시 마비되는 사건이 있었다.

기사출처 : http://www.cargonews.co.kr/news/articleView.html?idxno=43941

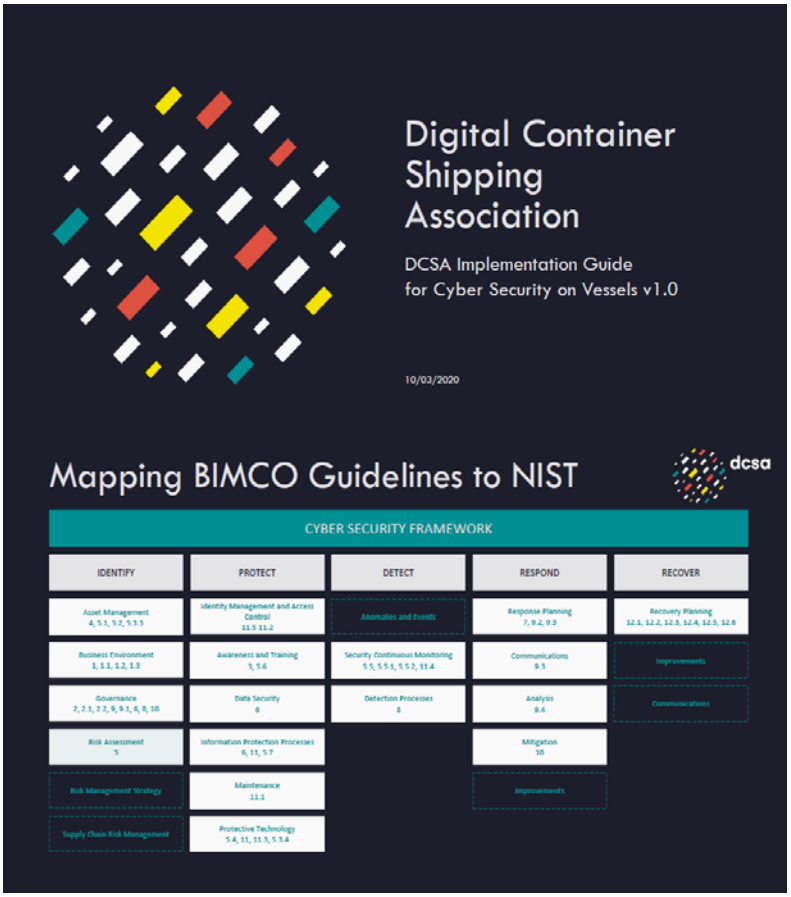
<4월 11일 22시 당시 MSC 홈페이지 접속 시 노출된 메인 화면 상황>



그림출처 : http://www.dailylog.co.kr/news/articleView.html?idxno=20057#09sf

DCSA, 사이버보안 가이드라인 발행

디지털 컨테이너 해운협회(DCSA), 사이버보안 가이드라인 발행



머스크라인(덴마크), MSC(스위스), 하팍로이드(독일), ONE(일본), HMM(한국) 등 세계 주요 9개 선사들은 기술표준화를 통한 컨테이너 운송의 디지털화를 위해 '디지털 컨테이너 해운 협회 (Digital Container Shipping Association)' 를 설립하고, 사이버보안 구현 가이드라인을 발표했다. 이 가이드라인은 안전경영시스템(SMS)의 해상 사이버 리스크 관리에 관한 IMO 결의 MSC.428(98)에 대응하기 위함이며, 기존 BIMCO와 NIST 사이버 리스크 관리 프레임워크와 일치하여 선주들이 사이버 리스크 관리를 기존 안전경영시스템(SMS)에 효과적으로 통합할 수 있게 한다. 또한, 선박의 사이버 위협을 완화시키거나 사이버 공격으로 인한 피해를 방지하고, 복구하는데 필요한 템플릿을 제공하고 있다.

DCSA 사이버 보안 구현 가이드 내용을 짧게 요약하자면, BIMCO의 지침과 IMO MSC428(98)에서 정의한 프레임워크(식별, 보호, 탐지, 응답, 복구)에 NIST 기능적 요소를 매핑하였다.

DCSA는 각 BIMCO 프레임워크 내에서 회사의 사이버 성숙도 수준에 따라 각 NIST 요소를 다루기 위해 취해질 비 기술적인 설명과 구체적인 조치를 제공하고 있다. DCSA 지침에 따라 선주는 사이버 리스크 평가에서 식별된 각 취약점에 대해 사이버 보안 대책을 마련하여 사이버 위협을 제거하는데 활용할 수 있는 템플릿을 제공하고 있다.

출처 : DCSA Implementation Guide for Cyber Security on Vessels v1.0, 10/03/2020

사이버 위협의 이해(OWASP Top 10-사물인터넷)

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 해상 사이버보안 시스템 인증 검사항목(CS1)

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

OWASP Top 10-사물인터넷 편

OWASP(Open Web Application Security Project)에 따르면 OWASP 사물 인터넷 프로젝트의 목표는 제조업체, 개발자, 소비자가 사물인터넷과 관련된 보안 문제를 더 정확히 이해하고 사용자가 IoT 기술을 구축, 배포 또는 평가할 때 보안 측면에서 더 현명한 의사 결정을 내리는데 도움을 제공하기 위함이다. 2020년 사이버보안 뉴스레터에서는 OWASP에서 선정한 사물인터넷(IoT)의 사이버 위협 Top 10과 대응방안을 살펴보고하 한다.

Top Ten	2014 IoT Top Ten	2018 IoT Top Ten
I1	Insecure Web Interface	Weak Guessable, or Hardcoded Passwords
I2	Insufficient Authentication/Authorization	Insecure Network Services
I3	Insecure Network Services	Insecure Ecosystem Interfaces
I4	Lack of Transport Encryption	Lack of Secure Update Mechanism
I5	Privacy Concerns	Use of Insecure or Outdated Components (NEW)
I6	Insecure Cloud Interface	Insufficient Privacy Protection
I7	Insecure Mobile Interface	Insecure Data Transfer and Storage
I8	Insufficient Security Configurability	Lack of Device Management
I9	Insecure Software/Firmware	Insecure Default Settings (NEW)
I10	Lack of Physical Hardening	Poor Physical Security

안전하지 않은 생태계 인터페이스(Insecure ecosystem Interfaces)

장치 외부의 생태계에 있는 안전하지 않은 웹, 백엔드 API, 클라우드 또는 모바일 인터페이스는 장치 또는 관련 구성 요소를 손상시킬 수 있다. 일반적인 문제로는 인증 / 권한 부족, 암호화 부족 또는 취약성, 입력 및 출력 필터링 부족이 있다. 다음 표는 ENISA에서 권고하는 "안전하지 않은 생태계 인터페이스"에 대한 보안조치의 예시이다.

도메인	보안조치	위협 그룹	참조 표준
보안 설계	인터페이스와 통신의 암호화 설계	· 정전 · 법률적 문제 · 재난	· ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls · NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations
클라우드 보안	클라우드 내의 모든 데이터와 전송 중인 데이터를 보호하도록 조치한다. 이상적인 보안조치는 모든 데이터를 암호화 하는 것이다. 응용 프로그램 및 인터페이스도 보호해야 한다.	· 악의적인 활동 · 도청 / 인터셉션 / 하이재킹	· IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program · ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements · NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security
접근 제어	로그인 시도 실패 횟수가 설정된 매개 변수 값을 초과한 후 활성화되는 장치에서 계정 잠금 기능을 사용한다. 이는 클라우드 및 모바일 인터페이스에서도 적용된다. 허용된 시도 횟수 및 잠금 시간과 같은 세부 사항을 지정하는 정책을 개발한다.	· 악의적인 활동	· IEC - IEC 62443-3-3:2013 System security requirements and security levels
네트워크 프로토콜 및암호화	IIOT(Industrial Internet of Things) 솔루션과 관련된 통신 채널의 보안을 유지하여야 한다. 안전과 가용성, 성능에 영향을 미칠 수 있는 중요한 데이터(예, 구성, 개인 데이터, 제어용 데이터)의 경우 통신을 암호화 해야 한다.	· 도청 / 인터셉션 / 하이재킹	· NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security

출처 : ENISA, Good Practices for Security of Internet of Things, NOVEMBER 2018

KR 해상 사이버보안 형식승인 가이드라인

사이버보안 형식승인 지침 이해하기

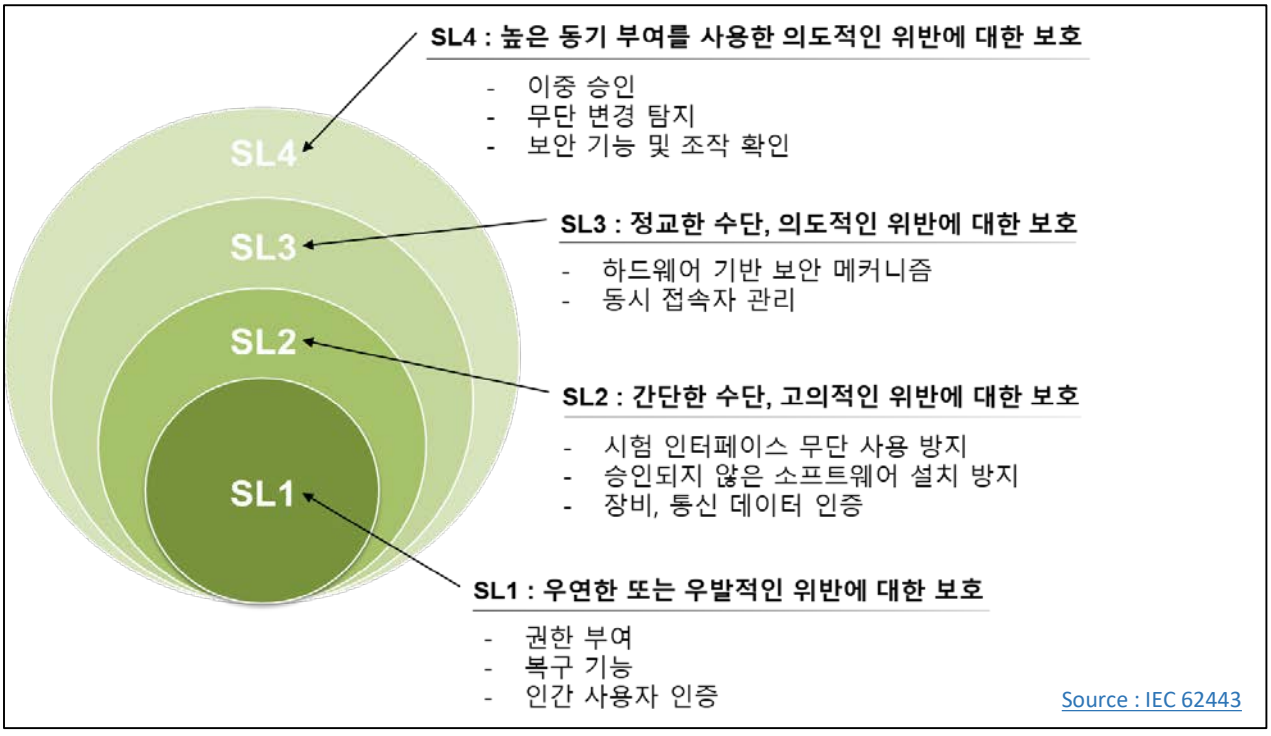
형식승인이란, 선박에 설치하기 전에 제품의 각 형식마다 미리 자료심사 및 승인시험을 하고 만족할 경우 제품이 규정에 적합하다는 것을 제조자에 대해서 증명하는 것을 의미한다. 사이버보안 형식승인은 ISA 62443 4-2, IEC 61162-460과 같은 국제표준을 기반으로 개발되었으며 선박에 탑재되는 원격 접속 장비, 통합 제어 및 모니터링 시스템 등을 포함하는 사이버 시스템의 사이버보안 수준 및 그 수준에 해당하는 요건을 12개의 범주 및 총 124개 항목의 요구 사항에 대한 검증을 통해 보안 기능과 그 수준을 확인한다.

<KR 사이버보안 형식승인 지침의 구성>

제1절 : 일반사항	제5절 : 데이터 기밀성	제9절 : SW 애플리케이션 요건
제2절 : 식별 및 인증	제6절 : 제한된 데이터 흐름	제10절 : 임베디드 장비 요건
제3절 : 사용 제어	제7절 : 사고에 대한 적시 대응	제11절 : 호스트 장비 요건
제4절 : 시스템 무결성	제8절 : 리소스 가용성	제12절 : 네트워크 장비 요건

Source : http://www.krs.co.kr/KRRules/KRRules2019/data/data_other/ENGLISH/gc31e000.pdf

보안등급(SL, Security Level)의 이해



Source : IEC 62443

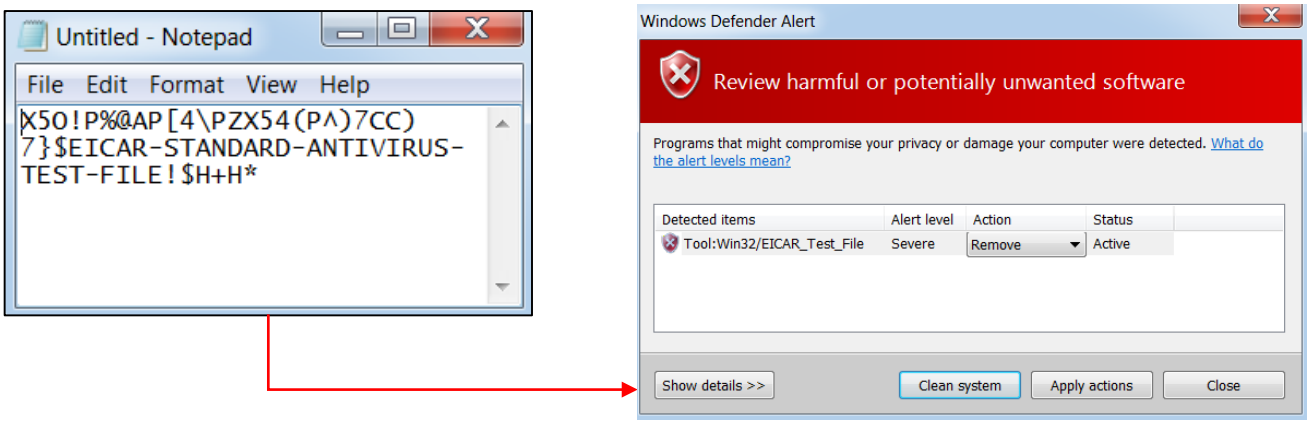
한국선급 해상 사이버보안 형식인증 검사항목

보안 기능성 검증 (402)

1. 의도된 보안 기능의 작동을 확인할 수 있는 기능을 제공하여야 한다.(SL 1,2,3)
2. 정상 작동 중 보안 기능의 작동을 확인할 수 있는 기능을 제공하여야 한다. (SL 4)

EICAR 테스트에 의한 보안 기능성 검증

제품 공급업체 혹은 시스템 통합업체는 설계한 보안 통제 장치를 시험하는 방법에 대한 지침을 제공해야 하며 자산 소유자는 정상 운용 중에 이러한 검증 시험을 실행할 때 발생할 수 있는 영향을 알아야 한다(출처 IEC 62443 4-2). 보안 기능 확인의 예시로 안티바이러스 백신의 경우 EICAR (European Institute for Computer Antivirus Research)에서 제공하는 테스트 파일을 이용할 수 있다.



<EICAR 시험 샘플을 이용한 보안기능 확인의 예시>

아래의 문장을 메모장 등에 작성한 후 저장 시 안티 바이러스 백신이 설치되어있는 경우 이를 바이러스로 감지하여 사전에 정의된 조치(eg. 경고문구 발생, 해당 파일의 삭제 처리 등)를 수행하게 된다.

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

(출처 www.eicar.org)

사이버보안 형식승인에서는 제품공급업체에서 사전에 정의한 보안 기능을 확인하고 이러한 기능을 확인할 수 기능이 제공되는지를 확인한다. SL4 등급을 만족하기 위해서는 가용성이 중요한 OT 시스템의 특성상 보안 기능 확인중에도 시스템의 정상적인 운영이 가능하도록 요구한다.

용어 설명

DCSA

- 디지털 컨테이너 해운협회는 머스크라인, MSC, 하팍로이드, ONE 등 세계 주요 선사 4곳에서 주도하여 창설되었으며, 선사마다 제각각인 데이터 형식으로 인한 비효율성을 극복하기 위해 데이터 표준화 작업을 위해 창성되었으며, 최근 사이버보안 가이드라인을 배포하였다.

멀웨어

- 멀웨어는 소유자의 동의 없이 컴퓨터 시스템을 침입하거나 손상을 입히도록 설계된 소프트웨어이다. 한 번 설치하면 제거하기가 매우 어렵고, 프로그램의 설치가 간단 하도록 설계되어 있다. 이것의 작업 결과는 조금 귀찮은 정도의 일로 분류되기도 하고, 회복 불가능한 손상으로 소유자의 하드 드라이브의 설치가 불가피한 것과 같은 큰 불편함을 주는 경우도 있다. 멀웨어의 예로는 바이러스나 트로이 목마를 말할 수 있다[WIKI]

랜섬웨어

- 랜섬웨어는 컴퓨터 시스템을 감염시켜 접근을 제한하고 일종의 몸값을 요구하는 악성 소프트웨어의 종류이다. 컴퓨터로의 접근이 제한되기 때문에 제한을 없애려면 해당 악성 프로그램을 개발한 자에게 지불을 강요받게 된다. 이때 암호화되는 랜섬웨어가 있는 반면, 어떤 것은 시스템을 단순하게 잠그고 컴퓨터 사용자가 지불하게 만들기 위해 안내문구를 띄운다[WIKI]