KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 029

September 2020

SC Shipmanagement와 사이버보안 적합성 인증 계약 체결

한국선급(KR, 회장 이형철)은 영국의 컨테이너선사인 SC Shipmanagement 사와 회사 및 선박 사이버보안 적합성 인증에 관한 계약을 체결하였다고 밝혔다.

이번 계약에 따라 한국선급은 SC Shipmanagement 사의 본사 내 사이버보안 관리 시스템에 대해 관리적, 기술적, 물리적 측면에서 사이버보안 역량을 검증하고, 컨테이너선 4척에 대해 선박 사이버보안 적합성 인증을 위한 검사를 진행한다.

특히 코로나 19로 인하여 사이버보안 검사원의 현장 검사가 어려워짐에 따라 SC Shipmanagement 사에 대한 사이버보안 적합성 인증을 위한 현장 검사는 한국선급 본사에서 원격사이버보안 검사로 진행될 예정이다.

원격사이버보안 검사는 검사원이 회사나 선박에 직접 입회하여 검사하는 대신 회사나 선박 소유자가 제출한 전자파일 형태(사진, 비디오, 문서 사본 등)의 자료를 검토하고, 필요한 경우 실시간 영상으로 해당 회사 또는 선박과 통신하여 수행하는 검사를 말한다. 코로나19(COVID-19)로 인해 전 세계적으로 비대면 활동이 중요해지고 있는 가운데, 이러한 원격사이버보안 검사는 최첨단 디지털 기술을 검사에 활용하여 효율성을 개선함으로써 전통적인 현장검사 역량을 강화할 것으로 예상된다.

앞으로 한국선급은 해사산업계의 안전 향상 및 비용절감을 위해 회사・선박 사이버보안 적합성 인증 검사 시 현장검사와 원격사이버보안 검사를 병행하여 안전성 및 효율성을 높여 스마트하고 안전한 선박검사라는 새로운 옵션을 제시할 예정이다.

세계 최대 레저 여행사 카니발 랜섬웨어 공격에 당하다

크루즈 라인 운영사인 카니발 코퍼레이션은 저번 달 자사 브랜드 중 한 곳이 랜섬웨어 공격을 받았다고 밝혔다. 카니발 코퍼레이션은 “2020년 8월 15일 카니발 코퍼레이션 및 카니발 PLC가 한 브랜드의 정보기술 시스템의 일부분에 접속하여 암호화한 랜섬웨어 공격을 탐지하였다. 또한 비인가된 접속에 의해 데이터 파일이 다운로드 되었다.“라고 밝혔다.

Information Security Forum의 상무이사인 Steve Durbin은 “랜섬웨어는 조직의 정보에 대한 가장 보편적인 위협 중의 하나이며 범죄자들에게 점점 더 이익이 되고 있다. 이러한 위협의 규모와 범위로부터 조직을 보호하기 위하여 조직은 방어 모델, 특히 사업 연속성과 재해 복구 계획을 재고할 수 밖에 없을 것이다. 집에서 일할 수 있는 직원들에 의존하는 기존 계획들은 기업 인프라에 랜섬웨어를 심는 것을 통해 연결성을 제거하거나 개인적으로 개인들을 대상으로 하는 공격에 대항할 수 없다. 개정된 계획은 인프라, 장비 또는 사람에 대한 공격에 의한 운영 중단 시간에 대한 위협을 다루어야 한다.”고 말했다.

Thycotic 사의 최고 정보보안 책임자인 Terence Jackson에 따르면 “랜섬웨어는 코드 작성에 상당히 숙련된 사람이 필요한 것으로부터 랜섬웨어 서비스 (RaaS) 제공으로 수년 동안 발전했다. 또한 랜섬웨어 공격을 시작하는데 필요한 기술은 줄어들었다.”라고 지적하였다. 다른 상용 기성 소프트웨어(COTS)처럼 이제 웹에서 쉽게 이용할 수 있는 악용 키트를 구입할 수 있다. 피싱은 렌섬웨어를 위한 가장 선호되는 방법이며 앞으로도 그럴 것이다. 문을 여는데 한 명의 직원만 있으면 된다. 이것은 공격자들이 훨씬 더 쉽게 침입할 수 있게 하고 다시 공격을 저지하기 위한 기술적 진입봉을 낮추게 한다. 사람이 이 방어선에서 가장 약한 고리로 남아 있는 한 랜섬웨어 공격은 계속 거세질 것이다.” 라고 언급했다.

Accepto의 CEO인 Shahrokh Shahidzadeh는 “유효한 디지털 자격 증명을 활용했을 때 랜섬웨어 공격이 더 성공하는 것으로 보이며, 불행히도 현재의 인증에 대한 이진법 접근법은 너무 많은 사이버 범죄자들을 네트워크에 허용하여 랜섬웨어를 효과적으로 심을 수 있게 한다. 암흑 웹에서 구매했거나 유출 후 바로 도용한 유효한 디지털 자격 증명의 사용은 대상 조직이 부적절한 자격 증명 사용을 포착할 수 있는 지속적인 행동 기반 인증 솔루션을 갖추지 못했을 때 랜섬웨어를 심을 수 있는 최상의 접근 권한을 제공한다. 랜섬웨어 공격은 특히 도난당한 디지털 자격 증명에 대한 접근 용이성과 지속적인 인증 솔루션의 배치와 함께 계속해서 적응하고 진화할 것이다. 한마디로 조직에서 모든 디지털 자격 증명을 지속적으로 인증하지 않으면 랜섬웨어 공격이 성공할 가능성은 기하급수적으로 높아진다."고 말했다.

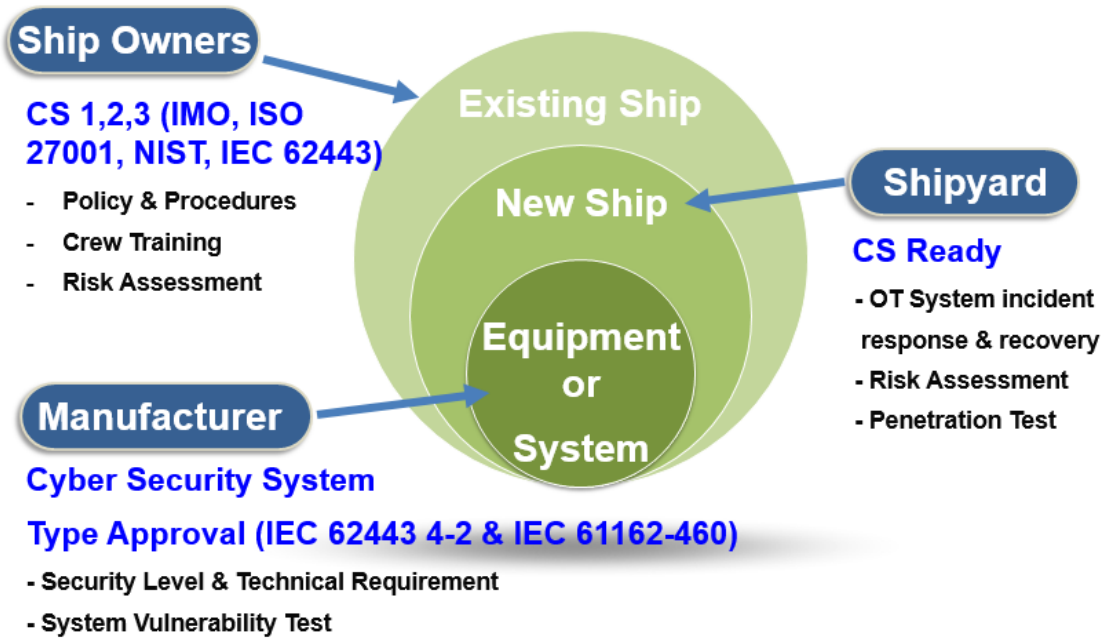
Source : SECURITY Magazine, 2020

KR 신조선 사이버보안 부기부호(CS Ready) 이해

한국선급 사이버보안 인증 체계

한국선급 해상 사이버보안 인증은 사이버보안 관리 시스템을 갖춘 회사 또는 선박에 적용되며, 인증심사(문서검사, 현장검사)를 통과하면 회사/현존선은 적합성 인증서, 신조선은 [CS Ready] 부기부호가 부여된다. 회사/현존선은 사이버보안 성숙도에 따라 3단계 [CS1,CS2,CS3]로 구분되며, 36개 검사영역, 144개 검사항목으로 구성되어 있다.

- **[CS1, CS2, CS3]** : 현존선 운영을 위한 사이버보안 요구사항**(선사 주관)**
- **[CS Ready]** : 신조선 통합 사이버보안 시스템 구축을 위한 요구사항**(조선소 주관)**
- **[CS 형식승인]** : 기자재 시스템의 사이버보안 기능에 대한 요구사항**(제조업체 주관)**



신조선 사이버보안 부기부호[CS Ready]의 필요성

해상 비즈니스 환경의 변화로 인해 고도화된 자동화 · 통합 제어시스템이 선박에 탑재되고 있으며 육상에서 선박 내 시스템 원격 접속 및 제어, 유지보수 등이 가능해짐에 따라 선박 사이버 리스크는 점점 더 증가하고 있다. 따라서 사이버사고를 예방하고 대응할 수 있는 통합 시스템을 선박 건조단계에서부터 구축 · 검증하는 것은 해사안전을 위해 매우 중요하다. 한국선급은 사이버보안 시스템을 갖춘 신조선에는 [CS Ready] 부기부호를 부여하고 있으며, 본 뉴스레터를 통해 각 검사 요건에 대해 소개하고자 한다.

[CS Ready] 제출문서 이해하기 : #1 자산 목록

선박은 다양한 IT/OT 시스템으로 구성되어 있다. 각 시스템의 사이버자산을 자산목록을 통해 식별·분류하는 것은 사이버공격벡터를 확인하고 훼손·변조·유출 등의 사이버사고로부터 효율적으로 대응할 수 있는 첫 단계로 볼 수 있다.

▪ **자산(Asset)** : 개인, 조직 또는 정부의 가치 있는 모든 것[ISO 27032], 가치가 있는 물리적/논리적 객체[IEC 62443]

▪ **정보기술(Information Technology)** : 데이터 또는 정보의 자동 수집, 저장, 조작, 관리, 이동, 제어, 디스플레이, 스위칭, 교환, 전송 또는 수신에 사용되는 장비, 상호 연결된 시스템 또는 장비의 하위 시스템 (예) 라우터, 스위치, 방화벽, 서버, 프린터, 데스크탑, 노트북 등

▪ **운영기술(Operation Technology)** : 내장된 시스템을 모니터링하고 제어하는 장치, 센서, 소프트웨어 및 관련 네트워킹 (예) ICS, SCADA, DCS, PLC, Data historian, Sensor, Actuator 등

Zone	Asset	Manufacturer	Software	OS	Port	Location	PIC
Enterprise System	Mail Server	HP	PMS	Windows Server 2016	USB : 3 LAN : 2	Accomm.	2nd officer
	PCs	HP	PMS	Window 10	USB : 3 LAN : 2	Accomm.	2nd officer
	Printers	HP	-	-	USB : 2 LAN : 2	Accomm.	2nd officer
	Router	CISCO	CISCO	-	USB : 1 LAN : 20	Accomm.	2nd officer
DMZ	Firewall	CISCO	CISCO	-	USB : 1 LAN : 20	W/H	2nd officer
	Event Log	Advantech	-	Windows Server 2016	USB : 4 LAN : 2	W/H	2nd officer
	Anti-virus	HP	-	Windows Server 2016	USB : 4 LAN : 2	W/H	2nd officer
Control System	No.1 O/S	HP	KC 600	Windows Embedded	USB : 5 LAN : 3	ECR	1st engineer
	No.2 O/S	HP	KC 600	Windows Embedded	USB : 5 LAN : 3	ECR	1st engineer
	OS Switch	Moxa	Phoenex	-	-	ECR	1st engineer
	Firewall	Fortinet	Forti	-	USB : 1 LAN : 20	ECR	1st engineer
Wireless	A.P.	CISCO	CISCO		USB : 1 LAN : 4	W/H	2nd officer
Remote System	Vsat Rack	Intellian	-	-	USB : 3 LAN : 10	W/H	2nd officer
	Router	CISCO	CISCO	-	USB : 1 LAN : 20	W/H	2nd officer
	Firewall	CISCO	CISCO	-	USB : 1 LAN : 20	W/H	2nd officer
Navigation and Communication System	No.1/2 ECDIS	JRC	-	Windows Embedded	USB : 3 LAN : 4	W/H	2nd officer
	No.1/2 Radar	JRC	-	Windows Embedded	USB : 3 LAN : 4	W/H	2nd officer
	Firewall	Fortinet	Forti	-	USB : 1 LAN : 20	W/H	2nd officer

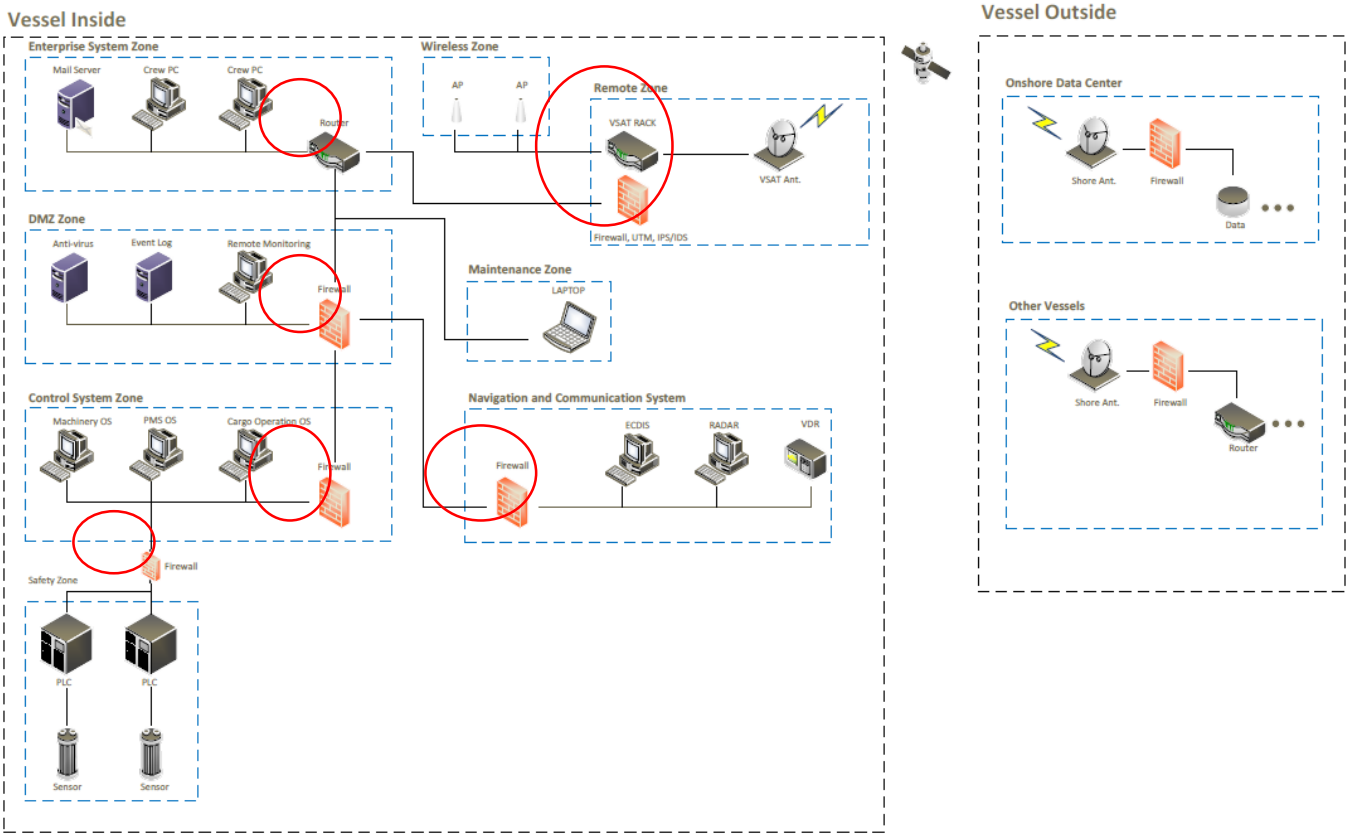
[CS Ready] 제출문서 이해하기 : #2 선박 네트워크 구성도

선박 네트워크 구성도를 통해 사이버 자산의 구역, 통신경로, 경계보호장치(게이트웨이, 라우터, 방화벽, VPN 등) 및 데이터 흐름(단방향, 양방향)을 파악할 수 있다. IEC 62443 3-2 표준에서는 구역과 통신경로의 분할 요구사항을 제시하고 있으며, 이를 참조한 선박 네트워크 구성도(예시)는 다음과 같다.

- **구역(Zone)** : 기능적, 논리적 그리고 물리적(위치를 포함하여) 관계를 기반으로 시스템의 분할을 표현하는 개체의 집합. 구역을 분리하는 기준은 IEC 62443 3-2 표준을 참조한다.
- **통신경로(Conduit)** : 공통 보안요구사항을 공유하는 둘 이상의 구역을 연결하는 통신 채널의 논리적 그룹화. (예) 스위치, 라우터, 방화벽,UTM, IPS/IDS 등

No.	요구사항	설명
ZCR 3.2	비즈니스 시스템과 제어 시스템 자산 분리	제어 시스템은 비즈니스 시스템과 분리한다.
ZCR 3.3	SIS 자산 분리	안전(Safety) 시스템은 비안전 시스템과 분리한다.
ZCR 3.4	임시 연결 장비 분리	임시 연결 장비(노트북, USB등)는 제어시스템과 분리한다.
ZCR 3.5	무선 통신 장비 구역 분리	무선 통신은 유선 통신과 분리된 구역으로 분리 한다.
ZCR 3.6	외부 네트워크 연결 장비 분리	원격 접속은 물리적으로 분리한다.

[IEC 62443 3-2 구역과 통신경로의 분할 요구사항]



[선박 네트워크 구성도 예시]

KR 해상 사이버보안 형식승인 가이드라인

사이버보안 형식승인 지침 이해하기

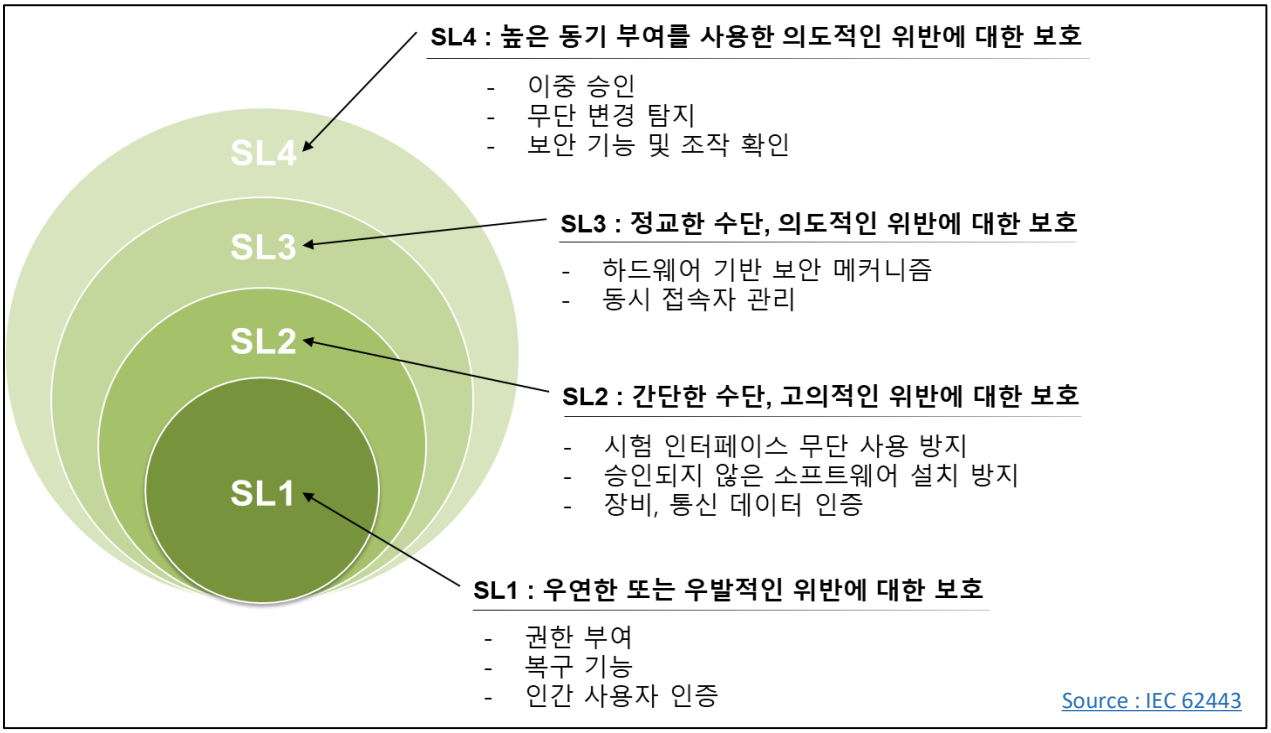
형식승인이란, 선박에 설치하기 전에 제품의 각 형식마다 미리 자료심사 및 승인시험을 하고 만족할 경우 제품이 규정에 적합하다는 것을 제조자에 대해서 증명하는 것을 의미한다. 사이버보안 형식승인은 ISA 62443 4-2, IEC 61162-460과 같은 국제표준을 기반으로 개발되었으며 선박에 탑재되는 원격 접속 장비, 통합 제어 및 모니터링 시스템 등을 포함하는 사이버 시스템의 사이버보안 수준 및 그 수준에 해당하는 요건을 12개의 범주 및 총 124개 항목의 요구 사항에 대한 검증을 통해 보안 기능과 그 수준을 확인한다.

<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

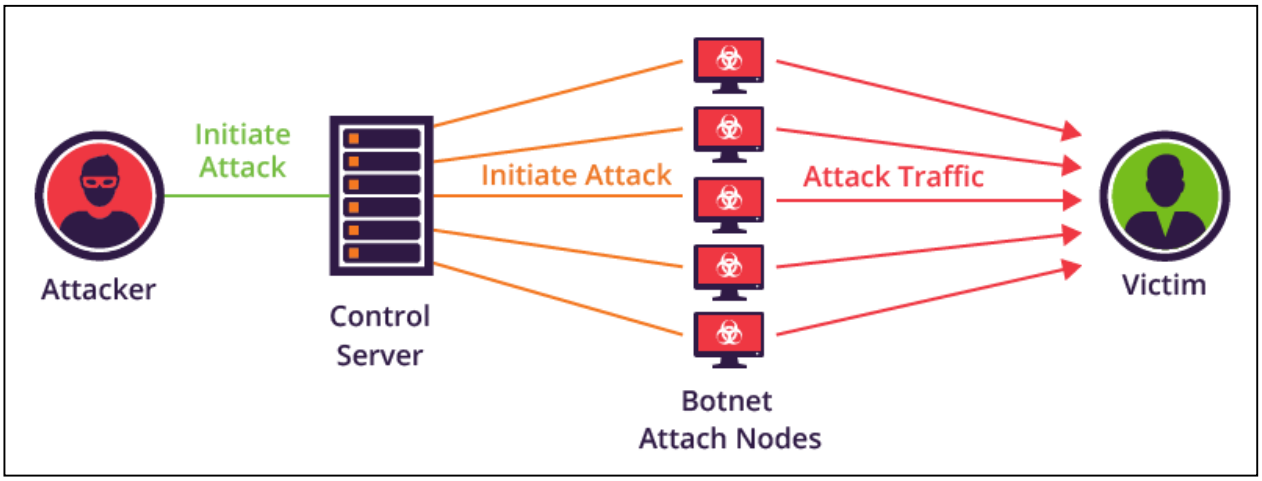
한국선급 해상 사이버보안 형식인증 검사항목

서비스 거부(DoS) 보호 (801)

1. DoS 이벤트의 결과로 저하된 모드에서 작동할 때 필수 기능을 유지할 수 있는 기능을 제공하여야 한다.(SL 1)
2. DoS 이벤트의 정보 및 메시지 범람 유형의 영향을 완화하는 기능을 제공하여야 한다. (SL 2,3,4)

서비스 거부(Dos) 보호 요구 사항

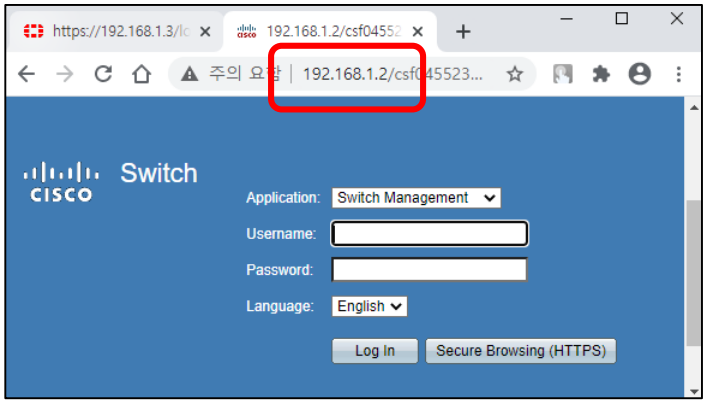
Denial of Service의 약자인 DoS 는 시스템을 악의적으로 공격해 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격을 의미한다. 특정 웹사이트의 서버에 대량의 트래픽을 발생시켜 과부하 상태를 일으키고 이로 인해 고객에게 원활한 서비스 공급을 불가능 하도록 하는 것이 이에 대한 예시가 될 수 있다. 이에 대한 보안 대책이 나오게 되고 해커들은 좀 더 진화된 방식의 Dos 공격을 만들게 된다. Distributed Denial of Service라고 불리는 DDoS 공격은 기존의 웹서버를 직접 공격하는 방식에서 한 차원 더 진화된 방식의 공격 기법을 사용하게 된다. 좀비 PC를 이용하는 방법인데 원리는 생각 보다 간단하다. 우선 특정한 악성코드 프로그램을 배포하여 무작위의 PC들을 대량 감염시킨다. 감염된 좀비 PC는 해커의 명령이 있기 까지는 별도의 행위를 수행하지 않으므로 감염된 좀비 PC들의 소유자는 감염사실을 모를 수 있다. 해커가 목표로 잡은 일정 수준이상의 PC가 감염이 된 것을 확인하고 해커는 Control Server를 통해 좀비 PC들에게 공격 대상이 되는 목표를 일제히 공격할 것을 지시한다. 특정 IP 차단 등을 통해 간단히 해결될 수 있었던 기존의 DoS공격에 비해 DDoS 공격은 무작위적이고 대량의 위치로 부터 공격이 들어오게 되며, 심지어 공격하는 대상이 해커가 아닌 피해자인 것이 차이점이다.



<DDoS 공격 방식의 예시>

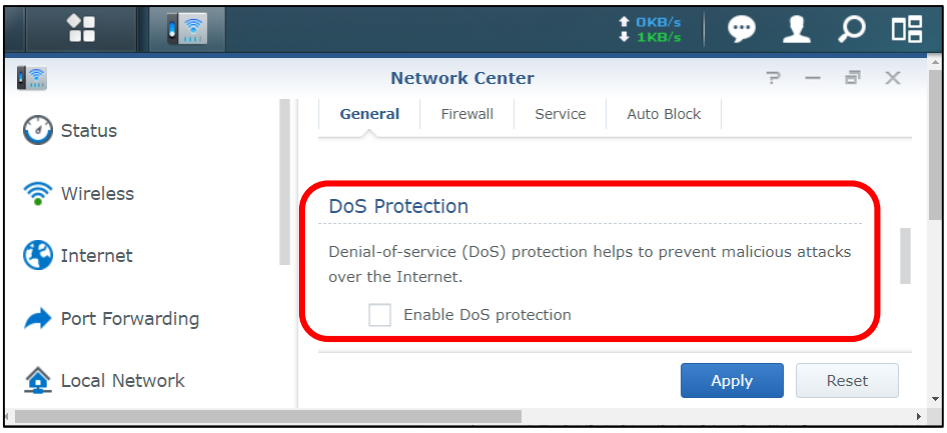
서비스 거부(Dos) 보호 요구 사항

DoS 공격에 의한 결과로 서비스 공급이 지연 혹은 불가능하게 되는 경우 이는 가용성에 문제를 초래하게 되므로 사이버보안 형식승인에서는 이에 대한 보호 기능을 제공할 것을 요구하고 있다. DoS 및 DDoS 공격은 오랜 기간에 걸쳐 진행되어왔으며 이로 인해 다행히도 방화벽, 라우터와 같은 다양한 네트워크 장치에서 이에 대한 보호 기능을 기본 기능으로 제공하고 있는 경우가 많다. 아래 사진은 라우터에서 제공되는 DoS 보호 기능의 예시이다.



<네트워크 장치의 설정 화면 예시>

우선 네트워크 장치에서 일반적으로 제공하는 설정화면을 이용하기 위해 인터넷 익스플로러 혹은 크롬과 같은 웹 브라우저에서 해당 장치의 주소를 입력한다. 관련 주소는 장치 제공자의 매뉴얼 등에 설명이 되어있는 경우가 많으며 특별한 설정이 없는 경우 192.168.0.1 주소가 많이 사용된다. 해당 주소에서 아이디와 패스워드를 입력하여 로그인 한 뒤 보안 설정을 할 수 있다.



<DoS 보호 기능의 예시>

많은 상용 네트워크 장비들에서 DoS 보호 기능을 기본 기능으로 제공하며 기본 설정이 비활성화로 되어있는 경우가 많으므로 설정 화면에서 이를 활성화 시키는 것을 통해 해당 요건을 만족할 수 있다.

용어 설명

원격사이버보안 검사

회사나 선박의 사이버 시스템 검사 시 검사원이 직접 입회하여 검사하는 대신에 선급이 회사나 선박 소유자가 제출한 전자파일 형태(사진, 비디오, 문서 사본 등)의 자료를 검토하고, 필요한 경우 회사 또는 선박과 통신하여 수행하는 검사

Source : KR Guidance for Maritime Cyber Security System 2020

랜섬웨어(Ransomware)

컴퓨터를 감염시키고 시스템이 다시 작동하기 위해 비용을 요구하는 메시지를 표시하는 악성 소프트웨어

Source : Kaspersky

서비스 거부 공격(DoS Attack)

공격 대상이나 주변 인프라를 인터넷 트래픽의 폭주로 압도하여 표적 서버, 서비스, 네트워크의 정상적인 트래픽을 방해하는 악의적인 공격

Source : CLOUDFLARE

침입탐지시스템(IDS)

의심스러운 활동이 발견되면 네트워크 트래픽을 모니터링하고 경보를 발령하는 시스템

Source : GeeksforGeeks

침입방지시스템(IPS)

네트워크 또는 시스템 활동을 모니터링하는 네트워크 보안 응용 프로그램. 침입 방지 시스템의 주요 기능은 악성 활동을 식별하고, 이 활동에 대한 정보를 수집하고, 이를 보고하고, 이를 차단하거나 중지하려는 것임.

Source : GeeksforGeeks

해사 사이버보안 교육 소개

KR 사이버보안 교육

국제해사기구(IMO)의 '안전관리시스템에서의 해사 사이버 리스크 관리 결의(Resolution MSC.428(98)'에 따라 싱가포르, 마샬 아일랜드 등 기국에서는 국제안전경영코드(ISM code) 대상 기업들에게 2021년 1월 1일 이후 첫 연차 심사 전까지 안전관리시스템에서의 사이버리스크 관리를 요구하고 있다. 이에 해사 사이버보안에 대해 이해하고 적절한 사이버보안 시스템을 구축하기 위한 해사 사이버보안 교육에 대한 수요가 증가하였다.

한국선급은 2015년부터 국내외 선사, 조선소, 기자재업체, 서비스공급업체를 대상으로 사이버보안 교육을 제공하고 있다. 특히 지난 3월에는 싱가포르 MPA에 해사 사이버보안의 이해 과정에 대해 승인을 받아 해양 클러스터 기금을 통해 싱가포르 선사들에 사이버보안 교육을 제공하였다.

한국선급은 코로나19로 인해 집체교육이 어려운 고객들을 위하여 사이버보안 컨설팅 전문회사인 ㈜오렌지씨큐리티와 협력하여 해사 사이버보안 이러닝 과정을 제공한다. 해사 사이버보안 이러닝 과정은 '해사 사이버보안의 이해', '해사 사이버보안의 관리 실무' 과정으로 구성되어 있다. '해사 사이버보안의 이해' 는 전체 직원의 사이버 보안 인식 제고를 목적으로 해사 사이버보안의 개요, 사이버 사고 사례 등으로 구성되어 있으며, '해사 사이버보안의 관리 실무' 는 실무자를 위한 내용으로 사이버 리스크 관리 수행 방법 등으로 구성되어 있다. 현재 국내 고객들을 위한 해사 사이버보안 이러닝 과정은 ㈜오렌지씨큐리티의 사이버보안 이러닝 아카데미 (edu.orangecq.com)를 통해 신청할 수 있으며, 해외 고객들을 위한 교육 사이트는 준비 중이다. 교육 과정 샘플은 유튜브에서 '해사 사이버보안의 이해(https://youtu.be/fSIDLMj4gho)' 와 '해사 사이버보안의 관리 실무(https://youtu.be/67t0ckrNtiA)'이 확인 가능하다.