KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 030

October 2020

초대형 LPG 운반선에 사이버보안 부기부호(CS Ready) 세계 최초로 수여

한국선급(KR, 회장 이형철)은 현대LNG해운(사장 이규봉), 현대중공업(사장 한영석), 한국조선해양(회장 권오갑) 관계자가 참석한 가운데 초대형 액화석유가스운반선(LPG Carrier)에 사이버보안 부기부호(CS Ready)를 한국선급 본사에서 수여했다고 18일 밝혔다.

이번에 세계 최초로 사이버보안 부기부호를 획득한 선박은 현대중공업이 건조하여 이달 중 인도 예정인 현대LNG해운의 초대형 LPG운반선이다. 한국선급은 이 선박에 탑재된 Kongsberg Maritime 社의 선박경보감시시스템(AMS, Alarm and Monitoring System), 현대글로벌서비스의 통합스마트십솔루션(ISS, Integrated Smart ship Solution) 등에 대해 문서검사 및 현장검사 등을 수행하고 부기부호를 수여하였다. 사이버보안 부기부호는 리스크·자산 관리, 사고대응 및 복구 등 총 12개 카테고리의 49개 검사항목을 통과한 신조선 선박에 부여된다.

각 사는 지난 8개월('20.1~9)간 한국선급의「신조선 사이버보안 규칙」을 적용·검증하기 위해 공동연구 개발을 진행해 왔다. 현대중공업과 한국조선해양은 선박의 주요 시스템을 중심으로 사이버보안 네트워크를 구축하고 보안 위협에 대한 리스크 평가 및 취약성 진단을 수행하였으며, 한국선급에서 사이버보안 검사를 진행하였다. 특히 한국선급은 최초로 MITRE社의 ATT&CK* 기반 침투테스트까지 수행하여 사이버보안 시스템 안전성을 검증함으로써 해상 사이버보안 기술력을 입증하였다.

한국선급 김대헌 디지털기술원장은 "이번 조선-해운업계 간 공동연구의 성공적인 결과는 전 세계에 우리의 우수한 사이버보안 기술 위상을 높이는 계기가 되었다."며, "앞으로도 신조선 사이버보안 기술 및 인증 역량을 강화하여 사이버보안 분야 기술 리더십을 더욱 공고히 해나갈 것이다"고 밝혔다.

현대LNG해운 최장팔 사업운영본부장은 "세계적으로 우수한 인증 역량을 보유한 한국선급의 선박 사이버보안 부기부호를 최초로 획득하게 되어 기쁘다"며, "앞으로도 선박 사이버리스크 관리의 중요성을 인식하고 선제적으로 대응하는 우량선사가 되겠다"고 소감을 전했다.

* 미국 MITRE社가 개발한 모델로 Adversarial Tactics, Techniques, and Common Knowledge을 말하며, 사이버 공격자의 침투 이후(또는 이전)활동의 사례분석을 통해 공격전술, 침투기술 등을 프레임워크로 제시

이어 현대중공업 김재을 기술본부장도 "한국조선해양 디지털기술연구소와 함께 협업하여 해상 사이버보안과 안전성이 인증된 선박을 인도하게 되어 뜻깊게 생각한다"며, "향후에도 선제적 기술 개발로 차별화된 사이버보안 시스템을 갖춘 스마트 선박을 건조하기 위해 노력하겠다."고 말했다.

최근 고도화된 자동화·통합 제어시스템 등 디지털 기술이 선박에 본격 적용되고 있고 국제해사기구(IMO)의 사이버보안 리스크 관리에 대한 요구가 21년부터 강화될 것으로 예상됨에 따라 신조선 사이버보안 부기부호 수요는 점차 증가할 것으로 전망된다. 이에 한국선급은 '18년부터 해상사이버보안 관리 시스템 인증 체계를 구축하고 사이버보안 인증, 형식승인 서비스 등을 제공하고 있다.

위성인터넷은 편리하지만 해킹도 쉽다.

Black Hat 2020 컨퍼런스 위성 인터넷을 통한 선박 사이버 해킹 실험결과 발표

옥스퍼드의 연구진은 최근 Black Hat 2020 컨퍼런스에서 위성 인터넷을 통한 선박, 항공기의 사이버 해킹 실험 결과를 발표하였다.

위성 인터넷은 최근 Elon Musk가 Starlink 네트워크를 구축하기 위해 저궤도 위성을 계속 발사함에 따라 지구 궤도를 도는 위성에서 인터넷 연결을 제공하는 것이 점점 현실화가 되어가고 있다. 오늘날 위성을 통한 인터넷 연결은 국제항해선박, 해양플랜트 원격 석유 굴착장치, 항공기 등 해사 산업을 비롯한 다양한 분야에서 이미 널리 사용되고 있다.

최근 Black Hat 2020 컨퍼런스에서 옥스퍼드의 한 연구진은 위성 광대역 통신의 보안되지 않은 특성을 다시 살펴볼 가치가 있다고 밝혔다. 몇 년 동안 이 연구진은 영국의 고정 된 물리적 위치에서 100m 평방 킬로미터에 걸쳐 인터넷을 전송하는 18 개의 위성 신호를 성공적으로 가로 챌 수 있었다. 실험 과정에서 암호화되지 않은 위성 인터넷 연결을 통해 중국 여객기로 보내진 항해 정보, 선박에 대한 정보 해독과 심지어 선원에 대한 개인 식별 가능한 정보까지도 전달할 수 있는 이집트의 한 유조선에서 전달된 메시지 등 온갖 종류의 통신을 엿볼 수 있었고, 그리스 억만장자 요트의 네트워크 비밀번호를 재설정하기도 하였다.

위성 인터넷 트래픽 차단

옥스퍼드의 연구진에 따르면 위성 인터넷 트래픽은 당사자들이 암호화 된 위성 연결의 무결성을 검증 할 수 있는 기술이 현재 존재하지 않기 때문에 쉽게 가로 챌 수 있다고 한다.

이 연구진은 $90의 위성 접시와 $ 200의 비디오 방송 위성 튜너를 기성품으로 구입하여 위성 인터넷 트래픽을 가로챌 수 있었다고 한다. 공개적으로 사용 가능한 소스를 사용하여 위성 궤도를 식별하고 위성 접시를 방향으로 가리 켰습니다.

이 연구진이 사용한 기술은 특별히 높은 수준의 기술력을 요구하지 않았고, 총 8TB 이상의 정보를 자신의 위를 도는 위성에서 다운로드 할 수 있었다. 전송되는 데이터를 기록하기 위해 신호 기록 소프트웨어를 사용하였고, HTTP 프로토콜을 사용하여 인터넷 트래픽에 집중하도록 조정하였다고 한다.

이 연구진은 올해 Black Hat 2020 컨퍼런스에서 그의 실험과 프레젠테이션이 위성 인터넷 연결의 잠재적인 보안 부족에 대한 인식을 가져 오기를 희망한다고 밝혔다.

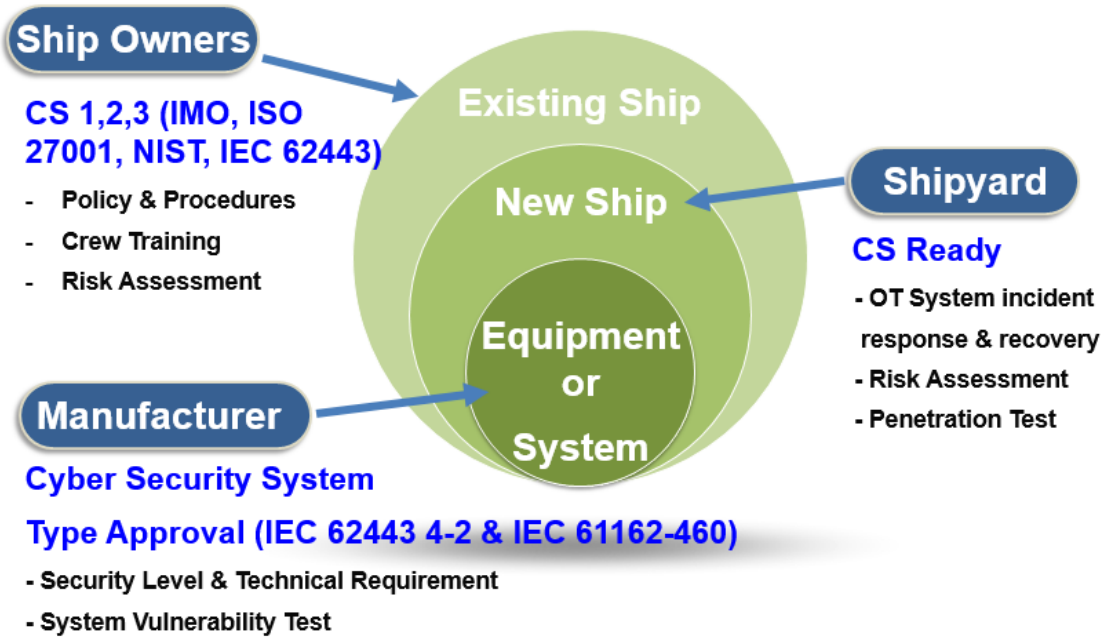
Source : https://www.techradar.com/news/hacking-satellite-internet-connections-is-a-lot-easier-than-youd-think

KR 신조선 사이버보안 부기부호(CS Ready)의 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 검사 영역, 144개 검사 항목으로 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)**



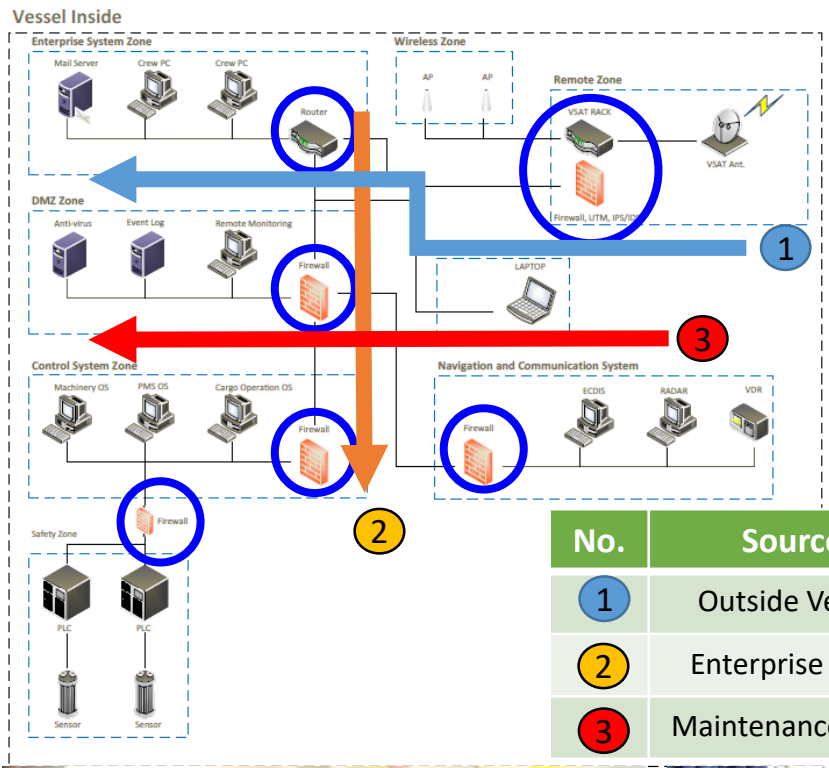
신조선 사이버보안 부기부호[CS Ready]의 필요성

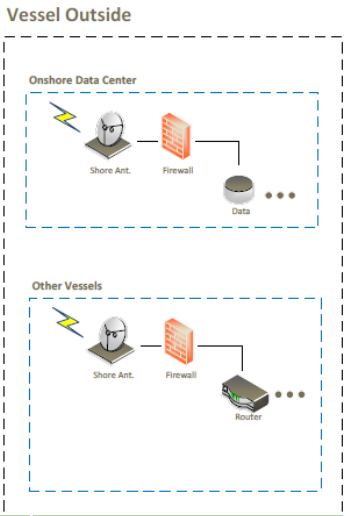
해상 비즈니스 환경의 변화로 인해 고도화된 자동화 · 통합 제어시스템이 선박에 탑재되고 있으며 육상에서 선박 내 시스템 원격 접속 및 제어, 유지보수 등이 가능해짐에 따라 선박 사이버리스크는 점점 더 증가하고 있다. 따라서 사이버사고를 예방하고 대응할 수 있는 통합 시스템을 선박 건조단계에서부터 구축 · 검증하는 것은 해사 안전을 위해 매우 중요하다. 한국선급에서는 사이버보안 시스템을 갖춘 신조선에는 [CS Ready] 부기부호를 부여하고 있으며, 본 뉴스레터를 통해 각 검사 요건에 대해 소개하고자 한다.

[CS Ready] Activity : 침투테스트

선박 네트워크 및 시스템 사이버보안 안전성을 검증하기 위한 방법으로 침투테스트를 활용할 수 있다. 침투테스트란 최신 해킹 기법을 이용하여 네트워크 및 시스템에 존재하는 취약점을 식별하고 실제 악용 가능여부를 파악하기 위해 평가자가 직접 침투를 실시하는 테스트를 말한다. 침투테스트를 통하여 잠재적인 사이버보안 취약성을 제거, 종합적인 대응방안을 마련함으로써 선박 사이버보안 수준을 향상 시킬 수 있다. 한국선급에서는 MITRE ATT&CK 기반 침투테스트를 실선에 적용하며 상세사항은 다음과 같다.

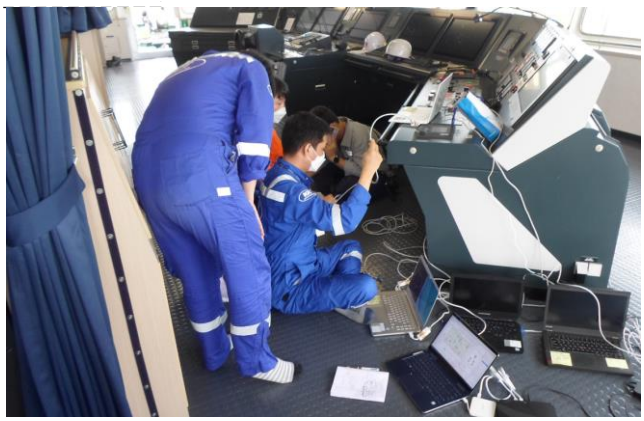
- **침투테스트 시험장비를 사용하여 각 Zone 별 보안장비(Firewall, IPS, IDS 등)의 성능을 점검**
- **시험대상 네트워크에 시험벡터(Cyber Attacks)*을 입력하여 Block되는 공격의 수와 비율을 측정하여 보안능력을 판단** * CVE(Common Vulnerabilities and Exposures)기반 Attacks





No.	Source	Destination
1	Outside Vessel	Remote Zone
2	Enterprise Zone	Control System Zone
3	Maintenance Zone	DMZ Zone

침투테스트(ECR)

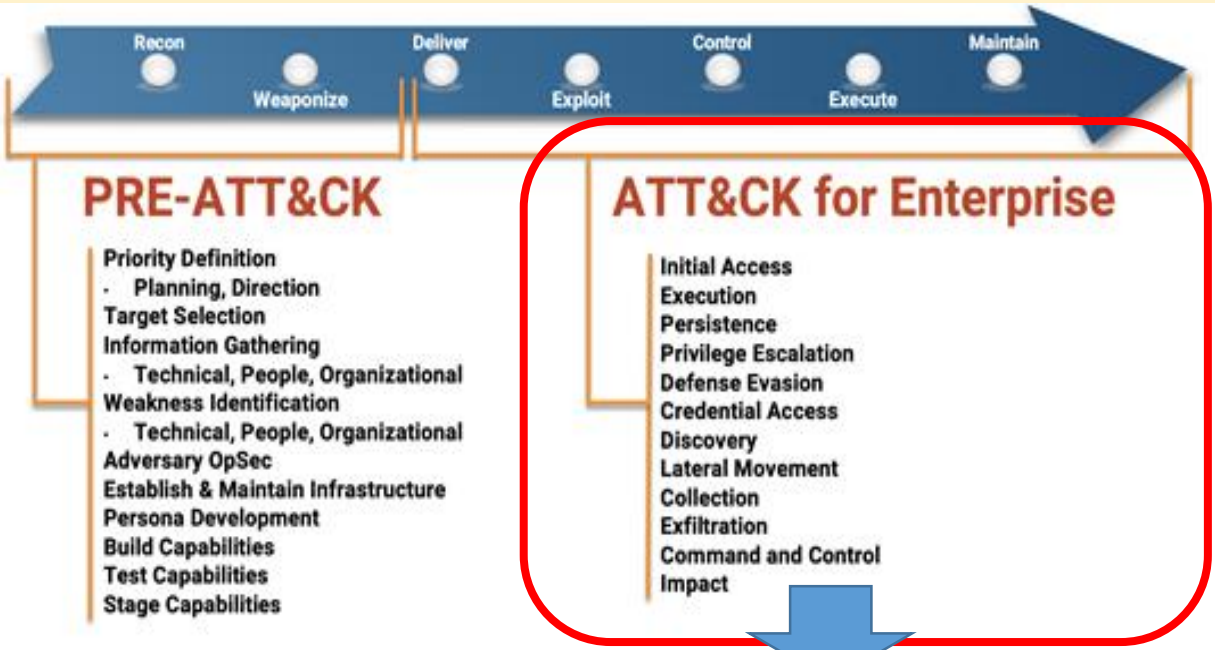


침투테스트(W/H)

[CS Ready] Activity : MITRE ATT&CK 기반 침투테스트

MITRE ATT&CK은 미국 MITRE社가 개발한 모델로 ATT&CK(Adversarial Tactics, Techniques, and Common Knowledge)을 말하며, 사이버 공격자의 침투 이후(또는 이전)활동의 사례분석을 통해 공격전술, 침투기술 등을 프레임워크로 제시하고 있다. PRE-ATT&CK(15개 전술, 148개 기술) 과 Enterprise ATT&CK(12개 전술, 184개 기술) 카테고리로 분류되는 7가지의 단계에서 사전에 공격을 파악하고 대응하는 Cyber Kill-Chain 전략을 기반으로 구성되어 있다. Cyber Kill-Chain 전략을 통해 각 단계별로 공격을 빠르게 발견하고 다음 단계로의 전파를 차단할 수 있다.

- **전술(Tactics)** : 공격자의 전술적 목표 설명
- **기술(Technics)** : 전술적 목표를 달성하기 위해 적들이 취한 행동과 방법을 설명
- **완화(Mitigations)** : 특정 기술에 대응하는 방법
- **그룹(Groups)** : 활동 클러스터 및 보안 커뮤니티에서 공통되는 이름으로 공격자를 추적



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking		Multilayer Encryption		System Shutdown/Reboot
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content		Port Knocking		Stored Data Manipulation
	Mshta	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation
	PowerShell	Emond	New Service	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote File Copy		
	Regsvcs/Regasm	External Remote Services	Parent PID Spoofing	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Standard Application Layer Protocol		
	Regsvr32	File System Permissions Weakness	Path Interception	Execution Guardrails	Securityd Memory				Standard Cryptographic Protocol		
	Rundll32	Hidden Files and Directories	Plist Modification	Exploitation for Defense Evasion	Steal Web Session Cookie				Standard Non-Application Layer Protocol		
	Scheduled Task	Hooking	Port Monitors	Extra Window	Two-Factor Authentication Interception						
	Scripting	Hypervisor									

Source : https://attack.mitre.org/

ENTERPRISE ATT&CK 12가지 전술

ENTERPRISE ATT&CK은 12가지 전술과 184개의 기술로 구성되며, 12가지 전술의 상세내용은 다음과 같다.

ID	전술	상세내용
TA0001	**초기접속 (Initial Access)**	▪ 악성코드를 유포하거나 첨부파일에 악성코드를 심어 공격 대상이 직접적인 파일을 실행하도록 유도하는 기법 등 악성 행위를 위한 초기 진입 방식 예) 이메일, 웹 애플리케이션 공격, Exploit 공격
TA0002	**실행 (Execution)**	▪ 공격자가 로컬 또는 원격 시스템을 통해 악성코드를 실행하기 위한 전술 예) 악성스크립트, Powershell 등을 이용한 payload 공격
TA0003	**지속 (Persistence)**	▪ 공격 기반을 유지하기 위한 전술 ▪ 운영체제에서 사용하는 파일을 공격자가 만든 악의적인 파일로 대체하여 지속적인 악성행위를 수행하거나 높은 접근 권한을 가진 계정을 생성하여 쉽게 재접근하는 방법 등이 해당 예) 서비스, 레지스트리 등록, 하이재킹, 계정등록 공격
TA0004	**권한 상승 (Privilege Escalation)**	▪ 공격자가 시스템이나 네트워크에서 높은 권한을 얻기 위한 전술 ▪ 시스템의 취약점, 구성 오류 등을 활용 ▪ 높은 권한을 가진 운영체제로 악의적인 파일을 삽입하는 기법 또는 시스템 서비스 등록 기법 등으로 권한 상승 예) UAC, 권한 약화 코드 실행 공격
TA0005	**방어 회피, 보안 우회 (Defense Evasion)**	▪ 공격자가 침입한 시간 동안 탐지 당하는 것을 피하기 위해 사용하는 전술 ▪ 보안 소프트웨어 제거/비활성화, 악성코드의 난독화/암호화 ▪ 신뢰할 수 있는 프로세스를 악용한 악성코드 위장 기법 등으로 유지 예) Pass the hash, 코드샤이닝 우회 공격 수행
TA0006	**접속 자격 증명, 계정 탈취 (Credential Access)**	▪ 공격자가 계정 이름이나 암호 등을 훔치기 위한 전술 ▪ 정상적인 자격 증명을 사용하면 공격자는 시스템 접속 권한을 부여받고, 목적을 달성하기 위해 더 많은 계정을 만들 수 있음 예) 크리덴셜덤핑, 키보드 캡쳐 등
TA0007	**탐색, 내부 정찰 (Discovery)**	▪ 공격자가 시스템과 내부 네트워크에 대한 정보를 습득하여 공격 대상에 대한 환경을 파악하기 위한 전술 ▪ 공격자는 행동 방식을 결정하기 전에 주변환경을 관찰하고 공격 방향을 정할 수 있음 예) 포트스캔, 공유폴더 확인, 브라우져 정보 수집
TA0008	**내부 확산, 측면 이동 공격 (Lateral Movement)**	▪ 공격자가 네트워크에서 원격 시스템에 접근한 후 이를 제어하기 위해 사용하는 전술 ▪ 공격자는 자신의 원격 접속 도구를 설치하여 내부 확산을 수행하거나, 운영체제에 포함된 도구를 이용하여 정상적인 자격 증명으로 접근함 예) Window adminshare, 이동식디스크쓰기, mimikatz
TA0009	**수집, 중요정보수집 (Collection)**	▪ 공격자가 목적과 관련된 정보 또는 정보의 출처가 포함된 데이터를 수집하기 위해 사용하는 전술, 데이터를 훔치고 유출하는 것이 목적 예) 클립보드 데이터, 이메일, 스크린캡쳐, 로컬 데이터 수집
TA0011	**명령 및 제어, 제어 서버통신 (Command and Control)**	▪ 공격자가 침입한 대상 네트워크 내부 시스템과 통신하며 제어하기 위해 사용하는 전술 예) 랜섬웨어 C&C 등 알려진 악성 URL 접속 테스트
TA0010	**유출 (Exfiltration)**	▪ 공격자가 네트워크에서 데이터를 훔치기 위해 사용하는 전술 ▪ 공격자는 데이터를 탐지되는 것을 피하기 위해 데이터를 압축/암호화 후 전송하거나 데이터의 크기 제한 설정을 통해 여러 번 나누어 전송하는 방식을 사용 예) http, dns, ssh, telnet 등으로 정보 유출 테스트
TA0040	**임팩트 (Impact)**	▪ 공격자가 가용성을 낮추고 무결성을 손상시키기 위해 운영 프로세스, 시스템, 데이터를 조작 및 중단시키고 나아가 파괴하는데 사용되는 전술 ▪ 랜섬웨어 등 시스템 자체를 파괴하는 공격 유형 테스트

KR 해상 사이버보안 형식승인 가이드라인

사이버보안 형식승인 지침 이해하기

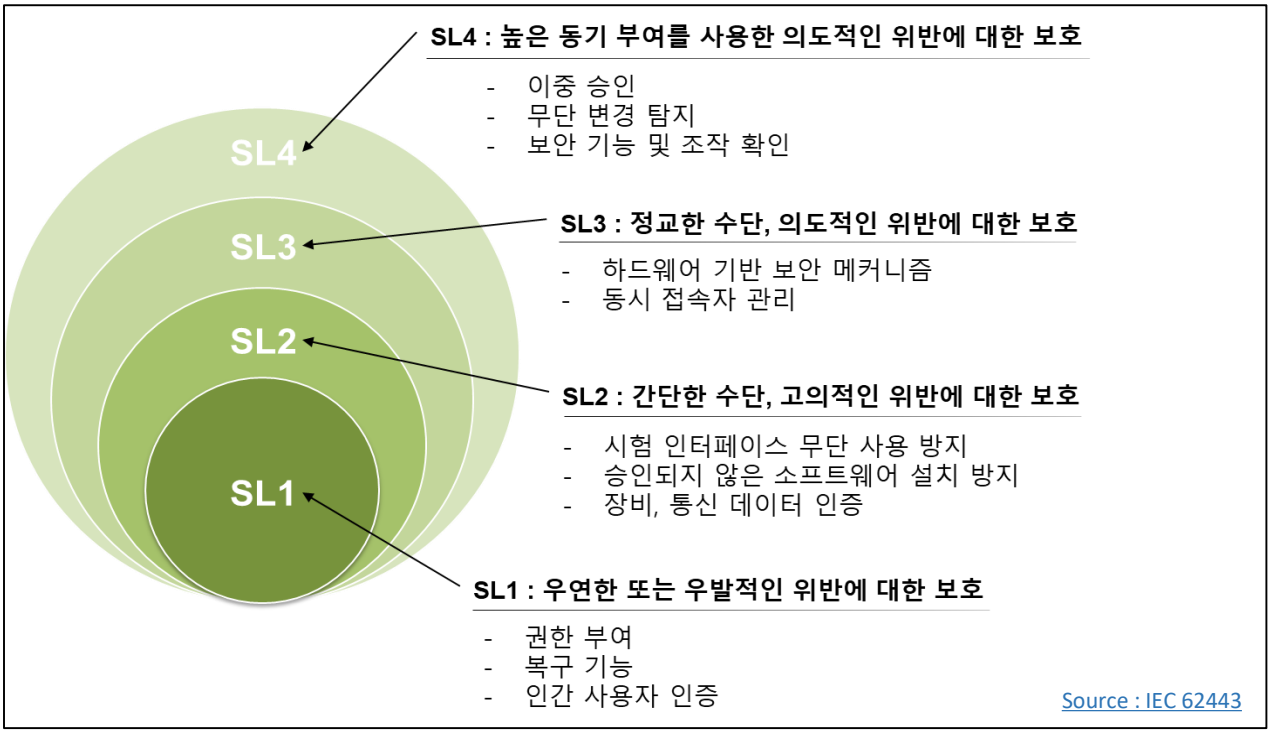
형식승인이란, 선박에 설치하기 전에 제품의 각 형식마다 미리 자료심사 및 승인시험을 하고 만족할 경우 제품이 규정에 적합하다는 것을 제조자에 대해서 증명하는 것을 의미한다. 사이버보안 형식승인은 ISA 62443 4-2, IEC 61162-460과 같은 국제표준을 기반으로 개발되었으며 선박에 탑재되는 원격 접속 장비, 통합 제어 및 모니터링 시스템 등을 포함하는 사이버 시스템의 사이버보안 수준 및 그 수준에 해당하는 요건을 12개의 범주 및 총 124개 항목의 요구 사항에 대한 검증을 통해 보안 기능과 그 수준을 확인한다.

<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

인증자 관리 (205)

1. 구성품은 다음의 기능을 제공하여야 한다. (SL 1,2)

(1) 최초 인증자 콘텐츠 사용 지원

(2) 설치 시 이루어진 기본 인증자에 대한 변경 사항 인식 지원

(3) 정기적인 인증자 변경/교체 작업에 적합한 기능

(4) 인증자를 저장, 사용 및 전송할 때 허가받지 않은 공개와 변경으로부터 인증자 보호

2. 구성품이 의존하는 인증자는 하드웨어 메커니즘을 통해 보호되어야 한다. (SL 3,4)

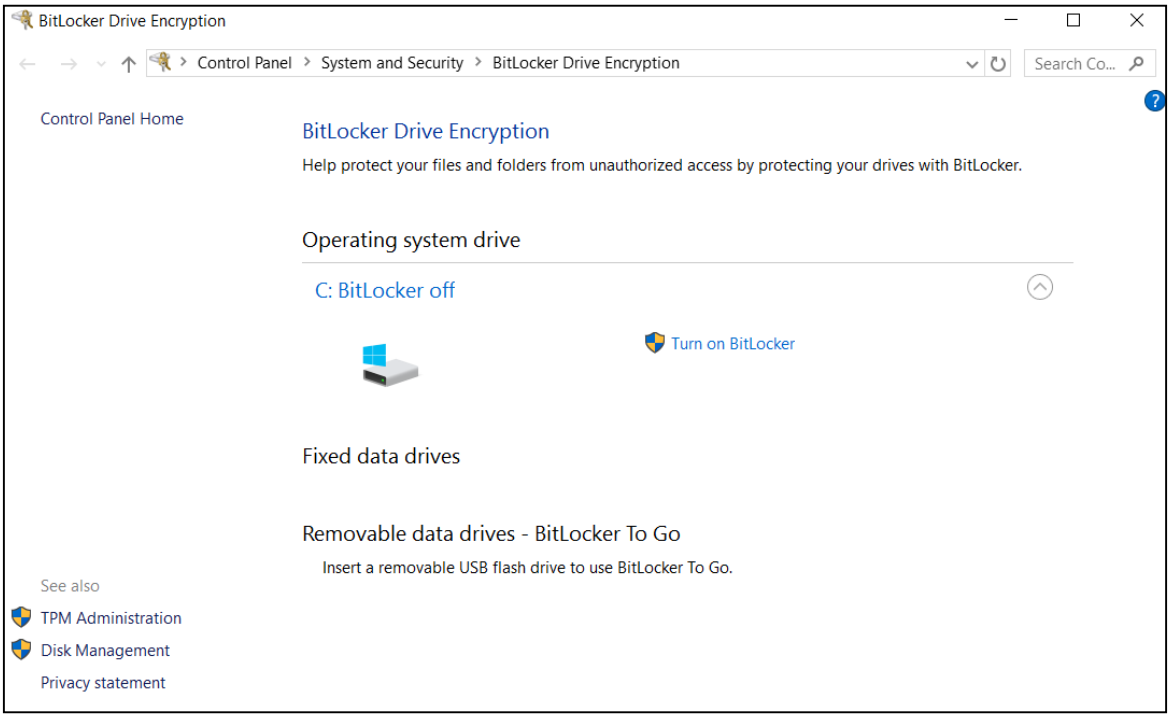
인증자 요구 사항

인증자(Authenticator)는 개체의 신원을 확인하는데 사용되는 수단이다(출처 IEC 62443 4-2). 웹싸이트의 로그온 시에 ID와 PASSWORD를 사용하게 되는데 이 때 PASSWORD가 인증자의 한 예시가 된다. 그 외에도 토큰, 디지털 서명, 암호화된 인증키 등이 인증자의 예시가 된다.

<인증자 관리 기능의 예시>

위 그림은 라우터에서 제공되는 화면으로써 Password 기반의 인증자 관리 기능을 제공함을 알 수 있다. 관리자가 아닌 일반사용자에 대해서는 Password를 잊은 경우 등록된 e-mail 주소를 사용하여 초기화 할 수 있음을 알 수 있다. Password 설정 시에는 영문 대소문자, 숫자, 특수문자 등을 사용하고 최소 자릿수를 설정하는 복잡성 기능이 제공됨을 알 수 있다.

인증자는 보호되어야 하며, 암호화 기능이 이에 대한 예시가 될 수 있다. 인증자에 대한 암호화는 S/W 어플리케이션을 이용하여 자체적으로 구현할 수도 있지만 OS에서 제공하는 암호화 기능을 활용할 수도 있다.

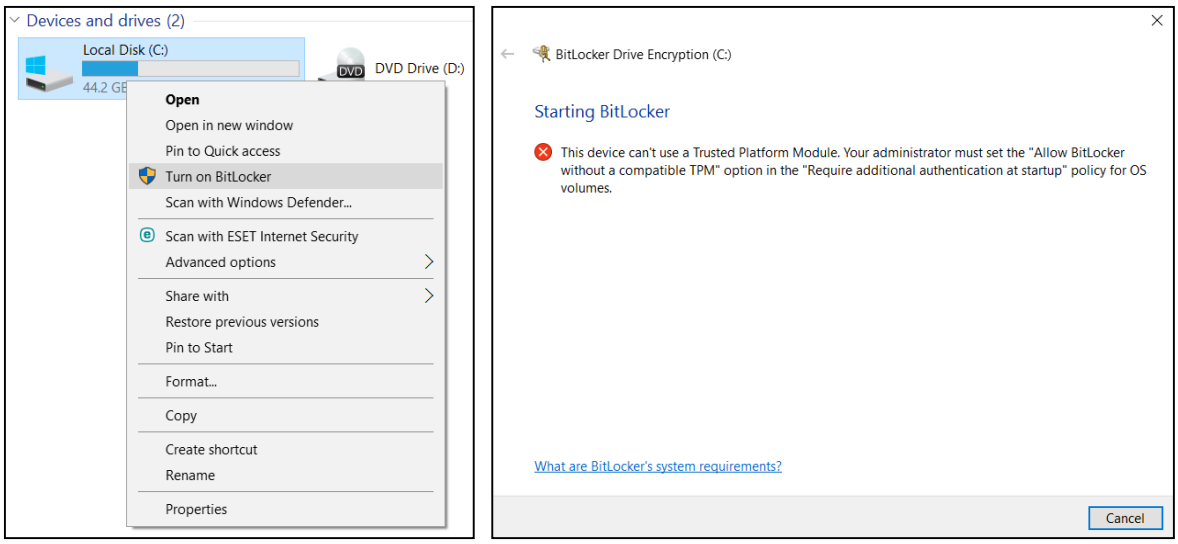


<윈도우 OS에서 제공하는 암호화 기능인 BitLocker의 예시>

윈도우 OS에서 제공하는 암호화 기능인 BitLocker는 드라이브 전체를 암호화하는 기술로써 저장되어있는 인증자를 보호할 수 있으며 폴더/파일 단위의 암호화 기능을 활용할 수도 있다.

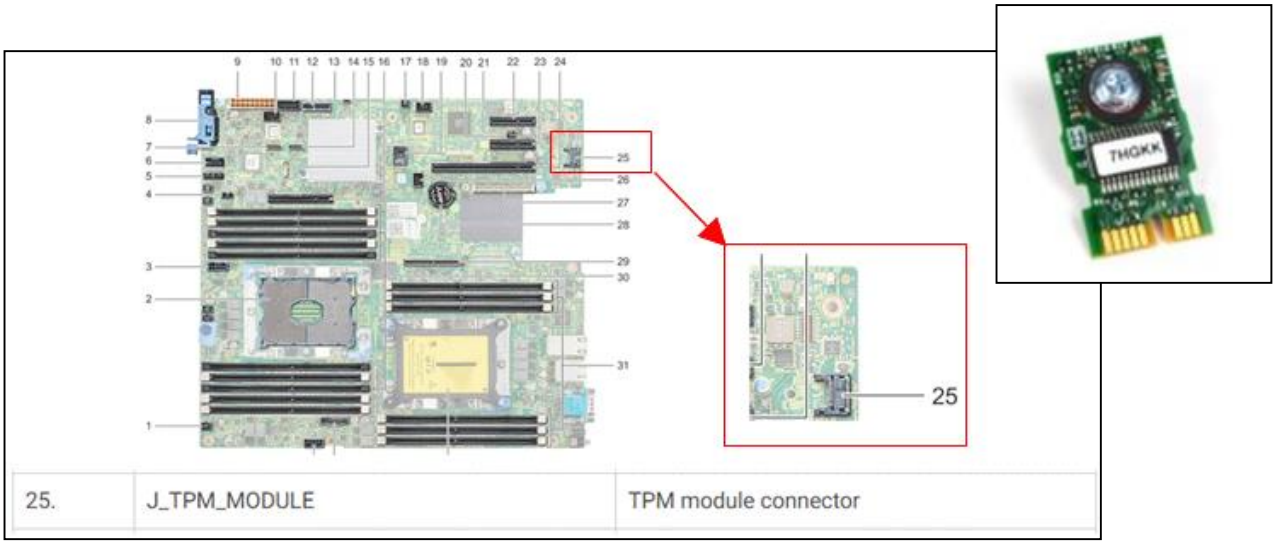
TPM(Trusted Platform Module) - 하드웨어 기반 인증자 보호

윈도우 OS에서 제공하는 드라이브 전체 암호화 기능인 BitLocker를 설정하는 경우 TPM이 설치되어 있지 않은 경우 다음과 같은 메시지가 뜨는 것을 볼 수 있다.

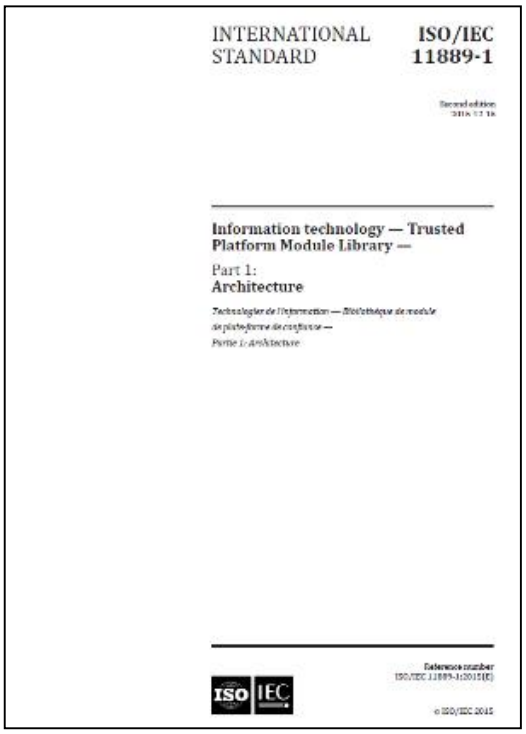


<윈도우 OS에서 제공하는 암호화 기능인 BitLocker의 예시-TPM이 설치되어 있지 않은 경우>

TPM은 Trusted Platform Module의 약자로 결론적으로 이야기하면 물리적인 칩을 이용하여 암호화를 수행하여 이 칩이 없는 경우 복호화가 불가능하도록 하는 하드웨어 기반 암호화 방식의 한 예이다. 최근에 제조되는 고사양의 노트북 등에는 이 TPM 칩이 이미 메인보드에 설치되어 양산되는 경우가 많다. 일부 PC 들에서는 해당 칩을 옵션사양으로 제시하기도 한다. 이 경우 별도의 TPM 칩을 구매하여 메인보드의 슬롯에 꽂아주기만 하면 TPM의 기능을 활용할 수 있다.



<TPM 칩의 예시>


INTERNATIONAL STANDARD
ISO/IEC 11889-1

Information technology — Trusted Platform Module Library —
Part 1: Architecture

ISO IEC

<IEC 11889-1>

TPM에 대한 내용은 이미 국제표준으로 제정이 되어 있으며 TPM의 기능을 활용하기 위해서는 관련된 S/W가 필요하다. 윈도우 OS에서 제공하는 BitLocker가 그 예시이며, 그 외 별도의 상용 프로그램도 있다. TPM 칩이 설치되고 이를 기반으로 한 S/W를 통해 암호화를 진행한 경우 해당 칩이 없으면 복호화가 불가능하다. 예를 들어 TPM 기반의 암호화가 된 하드디스크 드라이브를 도난 당한 경우, 하드디스크만으로는 그 안의 내용을 복호화 하여 볼 수 없다. 강력한 보안을 위해 이러한 하드웨어 기반의 암호화 기능을 사용할 수 있다. 마지막으로 TPM 기능이 제공되는지(TPM 칩이 설치되어있는지) 여부는 PC 혹은 노트북의 사양 정보나 혹은 운영체제 상의 메뉴에서 확인 할 수 있다.

IEC 62443 4-2의 이해

IEC 62443 이해하기

한국선급은 사이버보안 서비스를 위해 ISO 27001, IEC 62443 3-3 & 4-2, IEC 61162-460을 채택/적용하고 있다. 특히, IEC 62443 4-2는 사이버보안의 기술적 요건으로 사이버보안 형식승인 서비스에서 대다수가 적용되고 있다. 이에 폭넓은 이해 증진을 위해 IEC 62443의 개념 그리고 IEC 62443 4-2의 요건에 대해 기고하고자 한다.

IEC 62443의 목적

IEC 62443은 제품 공급자(Product Supplier) 및 시스템 통합자(System Integrator) 를 대상으로 산업 통신망 내 리스크 완화를 위해 사이버보안에 대한 전체적인 접근방식을 제공하는 산업 자동화 및 제어시스템(IACS, Industrial Automation and Control System) 보안에 관한 규격이다.

<IEC 62443 시리즈 부문>

Source : IEC 62443-4-2

적용 범위

IEC 62443은 산업 제어시스템, 네트워크로 연결된 지원 시스템, 원격 운영과 관련된 관계자 및 소프트웨어 등 산업 공정에서 안전하고 신뢰할 수 있는 운영에 영향을 미칠 수 있는 시스템을 대상으로 한다.

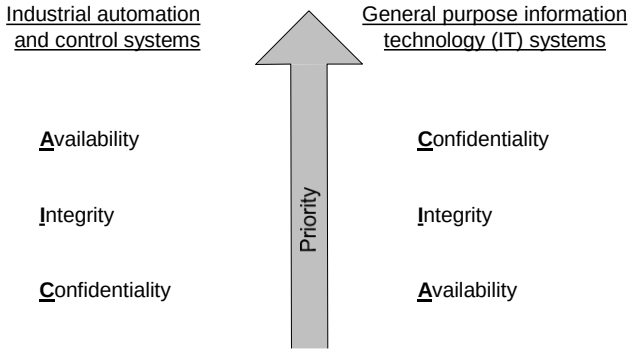
Source : IEC 62443-1-1

보안의 목적

전통적 정보 보안의 요구사항은 기밀성, 무결성 및 가용성 달성을 목적으로 하고 있으나, 산업 자동화 및 제어 시스템 환경에서의 보안은 모든 시스템 구성 요소의 가용성을 유지하는것과 관련이 있다. 이와 함께 산업 자동화 시스템에 의해 제어/감시되는 산업 장비의 리스크 완화를 위해 무결성 또한 중요하게 다뤄지고 있으나, 대부분의 산업 자동화 및 제어시스템의 교환 데이터가 원시 데이터 형식으로 구성되어져 있기 때문에 기밀성은 크게 다뤄지고 있지는 않다.

Source : IEC 62443-1-1

<산업 자동화 및 제어시스템과 일반적인 IT 시스템 간 보안 목적 비교>



산업 자동화 및 제어시스템에 관한 최소한의 보안 요구사항

IEC 62443은 산업 자동화 및 제어시스템 보안을 위해 다음과 같은 기본 요구사항을 제시하고 있다.

- 접근 제어(AC): 선택된 장치 또는 정보에 대한 비허가된 접근으로 부터 보호하기 위한 접근 제어
- 제어 사용(UC): 장치의 무단 제어 또는 정보 사용을 방지하기 위해 선택된 장비 또는 정보의 사용 제어
- 데이터 무결성(DI): 허가 받지 않은 변경으로부터 보호하기 위해 선택된 통신에 대한 데이터 무결성 보장
- 데이터 기밀성(DC): 도청으로 부터 보호하기 위해 선택된 통신에 대한 데이터 기밀성 보장
- 데이터 흐름 제안(RDF) 비허가된 정보의 공개로부터 보호하기 위한 통신 상에 데이터 흐름 제한
- 시기 적절한 이벤트 대응(TRE): 적절한 권한 부여 및 위반 사항 보고, 위험한 상황에서 적시에 시정조치 자동 대응 등을 통해 보안 위반에 대응하기 위한 시기 적절한 이벤트 대응
- 자원 가용성(RA) 서비스: 서비스 거부 공격(DOS) 등으로부터 보호하기 위한 모든 네트워크 자원의 가용성 보장

용어 설명

CVE(Common Vulnerabilities and Exposures

CVE(Common Vulnerabilities and Exposures)는 공개적으로 알려진 컴퓨터 보안 결함 목록이다. CVE를 지칭할 때는 일반적으로 보안 결함에 할당된 CVE ID 번호를 뜻한다. CVE는 IT 전문가들이 이러한 취약점에 우선 순위를 지정하고 해결하기 위해 협력하여 컴퓨터 시스템을 보다 안전하게 관리하도록 지원한다.

Source : RedHat

Payload

운영체제(이하 OS)나 웹 브라우저, 워드 프로그램 등 애플리케이션의 취약점을 이용해 프로그램의 흐름을 변경하고 공격자가 심어놓은 악의적인 코드가 사용자 몰래 실행되도록 하는 공격 기법인 익스플로잇이 발생된 후 생성되거나 추가로 다운로드되는 악성코드 및 공격자의 의도에 따라 발생하는 추가적인 행위 또는 피해를 말한다.

Source : AhnLab

Pass-the-Hash Attack

Pass-the-Hash (PtH) 공격은 공격자가 암호 문자에 해당하는 암호 해쉬를 캡처한 다음 이를 활용하여 인증 및 다른 네트워크 시스템에 접속하는 기술이다. 위협 행위자는 일반 텍스트 암호를 얻기 위해 해쉬의 암호를 해독할 필요가 없다. PtH 공격은 암호가 변경될 때까지 암호 해시가 모든 세션에 대해 정적 상태를 유지하므로 인증 프로토콜을 이용한다. 공격자는 일반적으로 시스템의 활성 메모리 및 기타 기술을 스크랩하여 해시를 얻는다.

Source : BeyondTrust

credential dumping

Credential dumping은 시스템의 운영 체제(OS)와 소프트웨어로부터 로그인 정보(사용자 이름 및 암호)를 얻는 것을 말한다. 그런 다음 이러한 자격 증명을 사용하여 제한된 정보에 접속하고 다른 악성 프로그램을 설치한다.

Source : MITRE ATT&CK, 2020

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. 해사 사이버보안 이러닝 과정은 ㈜오렌지씨큐리티의 사이버보안 이러닝 아카데미 (https://edu.orangecq.com/)를 통해 신청할 수 있다.

교육 과정 샘플은 유튜브에서 '해사 사이버보안의 이해 (https://youtu.be/fSIDLMj4gho)' 와 '해사 사이버보안의 관리 실무 (https://youtu.be/67t0ckrNtiA)' 이 확인 가능하다.