KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 022

February 2020

오렌지 시큐리티에 회사 사이버보안 적합성 증서 발행

지난 2019년 11월 한국선급은 사이버보안 컨설팅 전문회사인 ㈜오렌지씨큐리티에 회사 사이버보안 적합성 인증서를 수여하였다. 한국선급이 ㈜오렌지씨큐리티에 발급한 회사 사이버보안 적합성 증서는 해사업계가 아닌 회사에 처음 발급한 사례 이다.

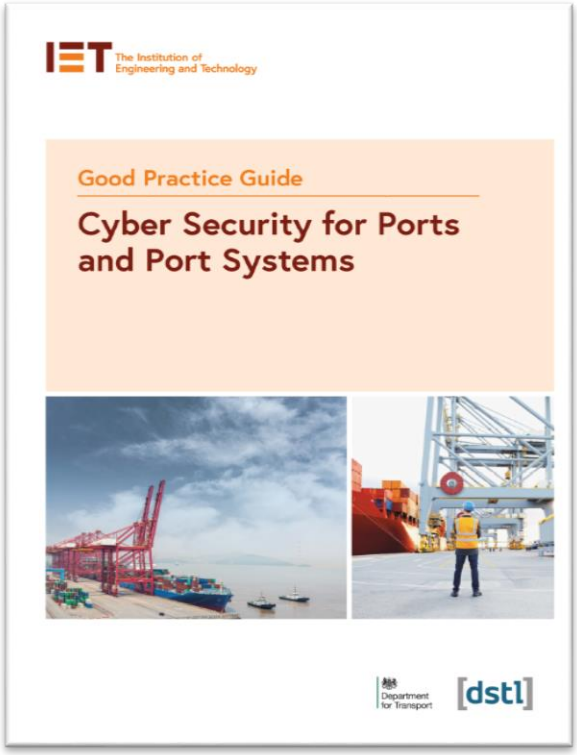
㈜오렌지씨큐리티는 다수의 금융기관과 정보통신사업자를 대상으로 사이버보안 컨설팅과 Information Security Management System(ISMS)인증, ISO27001 인증 심사를 수행하는 회사이고, 사이버보안 규제대응 솔루션을 개발하여 납품하는 등 그 영역을 확대하고 있으며, 최근 파나마에 자회사를 설립하여 글로벌 해사사이버보안 회사로의 도약을 준비하고 있다.

한국선급 사이버인증팀의 박개명 팀장은 “해운업계에는 대기업보다 중소기업이 대부분이기 때문에 IT부서가 없거나 클라우드만 사용하는 회사에 대한 통제를 어떻게 적용해야 할지 고민이 많았지만 이번 인증심사를 통해서 많은 부분이 정리되었다.”라고 하면서 “한국선급에서 수행하는 사이버보안 사업을 같이 해보자.”고 제안하기도 했다.

㈜오렌지씨큐리티 최성민 대표이사는 “인증을 준비하면서 해사산업 특히 선박에 대한 통제에 대해서 많은 도움을 받았다. 선박에서의 안전을 기준으로 구성되어 있는 보안통제가 기능위주로 구성된 육상의 통제와 그 개념이 달랐기 때문이다. 앞으로도 신설되는 국제규제를 모니터링하면서 한국선급의 도움을 받아 대한민국을 대표하는 해사 사이버리스크 전문회사로 거듭나겠다.”고 이번 인증의 의미를 밝혔다.

영국 교통부, 항만 사이버보안 가이드라인 발표

영국 교통부, 항만 사이버보안을 위한 'Good practice guide' 발표



영국 교통부(DfT)는 항만의 사이버보안을 위해 모범 사례 가이드(Good practice guide)를 발표하였다. 이는 사이버 보안 침해의 실제 위험과 재무, 보안 및 재산을 보호하기 위한 강력한 예방전략의 필요성을 강조하고 있다. 영국 교통국과 함께 엔지니어링 및 기술 연구소에서 발행한 '항만 시스템을 위한 사이버보안' 가이드는 항만에서 누가 어떤 조치를 취해야 하는지를 강조하고 있다. 지난 2017년 6월 Maersk사의 시스템에 NotPetya 바이러스에 의한 사이버 공격으로 약 2 억 ~ 3 억 달러의 손실이 발생하는 사이버 사고가 있었고, 이로 인해 전 세계 항만시스템에 대한 사이버 리스크 관리의 중요성을 지적하고 있다

또한 항만의 사이버 위협을 사전에 예방하지 않으면, 운영사는 사용 손실, 사업운영에 미치는 영향, 수익손실, 재정적 처벌 또는 소송으로 이어 질 수 있어 심각한 타격을 입게될 것이라고 하였다. 그 밖에 항만에 대한 사이버 공격은 샌디에고 항구, 바르셀로나 항구, Cosco Shipping Lines 및 APM 터미널 등에서 사이버 사고가 일어난 바 있으며, 이로 인해 항만의 사이버 보안의 중요성이 점점 더 중요하게 인식되고 있다. 또한, 항만시설이 점점 더 복잡해지고, 접안작업의 자동화 같이 항만 내 모든 작업단계에서 정보통신기술(ICT)의 의존도가 높아지고 있기 때문에 이 가이드에서는 효율적인 사이버보안을 강조하고 있다. 2019 년 10 월 사이버 위험 관리 (CyRiM) 프로젝트 보고서에 따르면 아시아 태평양 (APAC) 포트가 포함된 " 극단적 인 " 사이버 공격 시나리오에서 최대 1,100 억 달러의 손실이 발생할 것으로 예상하고 있다. 영국의 해양부 장관인 Nusrat Ghani 장관에 따르면, 이 가이드를 잘 지키면 해양산업이 21 세기 스타일의 공격으로부터이 중요한 수송 허브를 안전하게 유지할 수 있음을 강조하고, 항만의 사이버 보안 평가를 개발하는 데 도움이 되며, 보안의 격차를 효과적으로 식별 할 수있을 뿐만 아니라 사이버 보안 공격 관리에 대한 조언을 제공하고 있다고 밝혔다.

Source : https://www.hellenicshippingnews.com/cyber-security-guide-for-ports-released/

무선네트워크의 취약점 분석과 대응방안

본 기획시리즈는 일상생활과 회사, 선박 등에서 널리 사용되는 무선네트워크의 종류와 통신원리에 대해 알아보고, 무선 네트워크의 취약점과 대응방안을 소개하고자 한다. 따라서 본 뉴스레터 2020년 1월호에서는 ***'무선 네트워크의 종류와 통신원리'***에 대해 소개한다.

기획시리즈 순서

① **무선 네트워크의 종류와 통신원리**
② 무선랜(WIFI)의 기술적 보안 취약점과 대응방안-1
③ 무선랜(WIFI)의 기술적 보안 취약점과 대응방안-2
④ 무선랜(WIFI)의 기술적 보안 취약점과 대응방안-3
⑤ 기타 무선네트워크(Bluetooth, Zigbee 등)의 기술적 보안 취약점과 대응방안
⑥ 해상무선통신의 종류와 기술적 보안 취약점과 보안성 강화방안

무선 네트워크의 개요

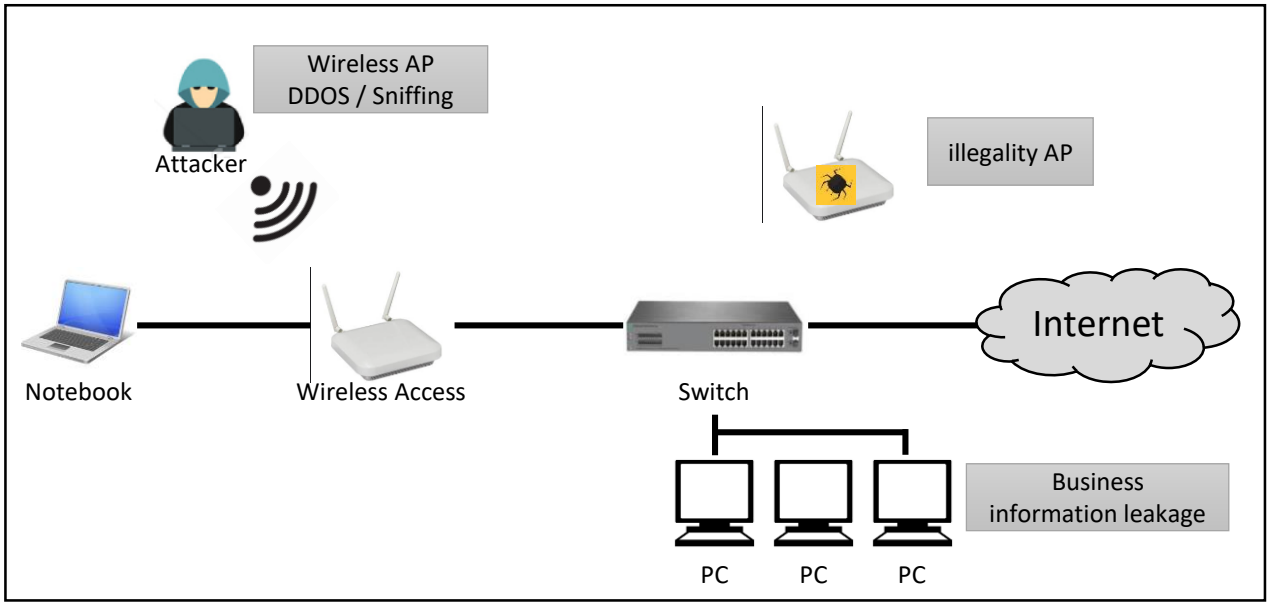
무선 네트워크란 네트워크 케이블을 사용하지 않고 컴퓨터, 모바일 기기 등과 네트워크 연결, 인터넷 엑세스를 할 수 있도록 하는 기술을 말한다. 흔히 무선 네트워크는 셀룰러 통신을 제외하고 일상생활에서 널리 사용되는 와이파이, 블루트스를 비롯하여 센서와 제어장차들과 저전력 네트워크를 제공하는 지그비, Z-웨이브 등과 같이 많은 종류의 무선 네트워크 기술들이 유선 케이블을 대체해 나가고 있다.

무선 네트워크의 원리

탐 색	인 증	결 합	데이터 전송
· AP는 SSID 등을 담고 있는 Beacon 메시지를 주기적으로 브로드 캐스트 · 단말은 주변을 탐색하여 AP를 찾아내고 AP를 선택 · 숨겨진 AP는 단말이 능동적으로 Probe 요청메시지를 AP에 전송하여 탐색	· 해당 AP에 접속권한이 있는 사용자 또는 단말인지를 검증하는 단계 · 보안 설정이 존재하지 않는 경우 개방 시스템 인증 절차수행 · MAC address 인증 등 존재	· 인증 성공 후 무선 단말은 AP와 연결하는 과정 · PC의 케이블을 스위치의 포트에 연결하는 과정과 비슷	· 위 3과정 이후 데이터 메시지를 AP를 통해 목적지로 전송 및 수신을 받는 단계

무선 네트워크의 취약점

무선 네트워크는 기존 유선랜의 확장 개념에서 가정 또는 일반 사무실 환경에서 사용되는 경우가 많아, 대부분 기존의 유선랜에 무선 AP를 연결한 후, 클라이언트에 무선 랜카드를 장착하여 적속하는 형태로 구성되고 있다. 따라서 유선랜과 무선랜의 분리는 전혀 고려되지 않는 경우가 많으며, 이로 인한 보안 상 문제점이 존재하게 된다.



Source : 한국인터넷진흥원 무선랜 보안 안내서

무선랜 암호화 방식

무선랜의 취약점은 크게 무선 네트워크 접속 시 인증과정에서의 문제점과 무선 전송 데이터의 암호화 취약점으로 나눌 수 있다. 최초 무선랜 표준인 IEEE 802.11에서는 별도의 무선랜 인증과 전송 데이터에 대한 암호화는 포함되어 있지 않았으나, IEEE 802.11b에서 처음 WEP 방식을 도입하였고, 현재는 WPA, WAP2 방식이 널리 사용되고 있다.

구 분	WEP (Wired Equivalent Privacy)	WPA (Wi-Fi Protected Access)	WPA2 (Wi-Fi Protected Access2)
개요	· 최초의 WIFI 보안	· WEP 방식 보완	· IEEE 803.11 준수
인증	· 사전 공유된 비밀키 사용 (64비트, 128비트)	· 별도의 인증서버를 이용하는 EAP 인증프로토콜(8021x) · WPA-PSK(사전 공유된 비밀키)	· 별도의 인증서버를 이용하는 EAP 인증프로토콜(8021x) · WPA-PSK(사전 공유된 비밀키)
암호화	· 고정 암호키 사용(인증키와 동일) · RC4 알고리즘 사용	· 암호키 동적 변경(TKIP) · RC4 알고리즘 사용	· 암호키 동적 변경(CCMP) · AES 등 강력한 블록암호 알고리즘 사용
보안성	· 64비트 WEP 키는 수분 내 노출 · 취약하며 널리 쓰이지 않음	· WEP 방식도바 안전하나 불완전한 RC4 알고리즘 사용	· 가장 강력한 보안기능 제공

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

취약점 1. 쉬운 암호, 유추할 수 있는 암호 도는 하드코딩된 암호

“ "무차별 대입 공격으로 손쉽게 노출되거나 펌웨어 또는 클라이언트 소프트웨어의 백도어를 포함하여 배포된 시스템에 대한 무단 액세스 권한을 부여하는 공개적인 인증 정보 또는 변경할 수 없는 인증 정보를 사용하는 것"

취약점 2. 안전하지 않은 네트워크 서비스

"디바이스 자체에서 실행되면서 정보의 기밀성, 무결성/신빙성 또는 가용성을 훼손하거나 무단 원격 제어를 허용하는 불필요하거나 안전하지 않은 네트워크 서비스(특히 인터넷에 노출되는 서비스)."

취약점 3. 안전하지 않은 생태계 인터페이스

"디바이스 또는 관련 구성요소의 침해를 허용하는 디바이스 외부 생태계의 안전하지 않은 웹, 백엔드 API, 클라우드 또는 모바일 인터페이스. 일반적인 문제에는 인증/승인의 부재, 암호화의 부재 또는 빈약함, 입출력 필터링의 부재 등이 포함된다."

취약점 4. 안전한 업데이트 메커니즘의 부재

"디바이스를 안전하게 업데이트할 수 있는 기능의 부재. 여기에는 디바이스의 펌웨어 검증 부재, 안전한 전송 방법의 부재(전송 중 암호화되지 않음), 롤백 방지 메커니즘의 부재, 업데이트로 인한 보안 변경 알림의 부재가 포함된다."

취약점 5. 안전하지 않거나 오래된 구성요소 사용

"디바이스 침해를 유발하는, 지원이 중단되거나 안전하지 않은 소프트웨어 구성요소/라이브러리 사용. 여기에는 운영 체제 플랫폼의 안전하지 않은 개조, 침해된 공급망에서 나온 서드파티 소프트웨어 또는 하드웨어 구성요소를 사용하는 것이 포함된다."

취약점 6. 불충분한 개인정보 보호

"사용자의 개인 정보가 디바이스 또는 생태계에 저장되어 안전하지 않게, 부적절하게 또는 사용자 허가 없이 사용되는 것."

취약점 7. 안전하지 않은 데이터 전송 및 저장

"보관, 전송 또는 처리 중을 포함하여 생태계 내의 어디서든 민감한 데이터의 암호화 또는 액세스 제어가 이뤄지지 않는 것"

취약점 8. 디바이스 관리의 부재

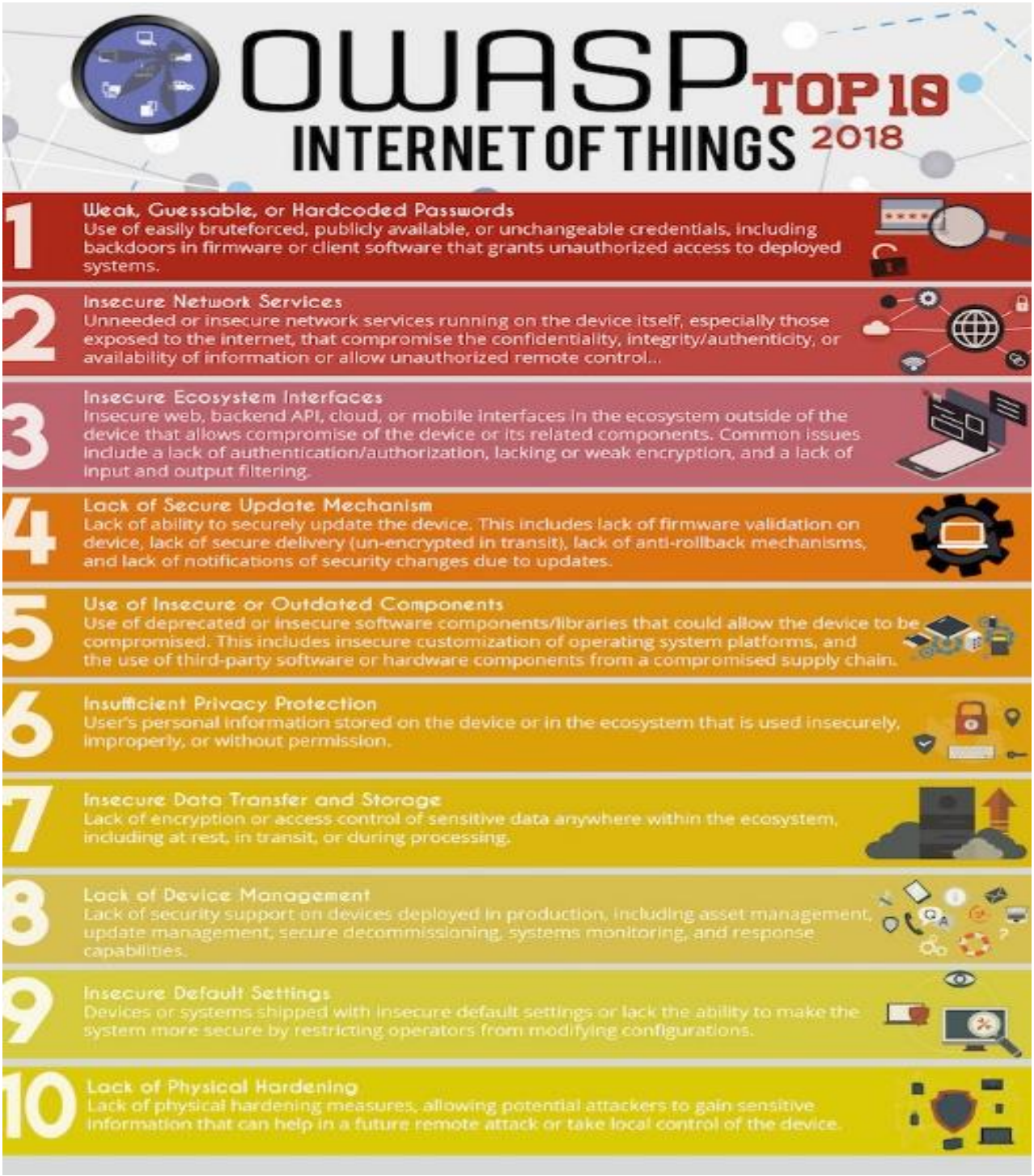
"프로덕션에 배포된 디바이스에 대한 자산 관리, 업데이트 관리, 안전한 폐기, 시스템 모니터링 및 응답 기능을 포함한 보안 지원의 부재"

취약점 9. 안전하지 않은 기본 설정

"안전하지 않은 기본 설정 상태로 출하되는 디바이스 또는 시스템. 또는 작업자에 의한 구성 수정을 제한하여 시스템을 더 안전하게 보호하는 기능의 부재"

취약점 10. 물리적 보호 수단의 부재

"물리적 보호 수단이 없어 잠재적 공격자가 미래의 원격 공격에 활용할 민감한 정보를 입수하거나 디바이스를 장악할 수 있도록 하는 것"



KR 해상 사이버보안 형식승인 가이드라인

사이버보안 형식승인 지침 이해하기

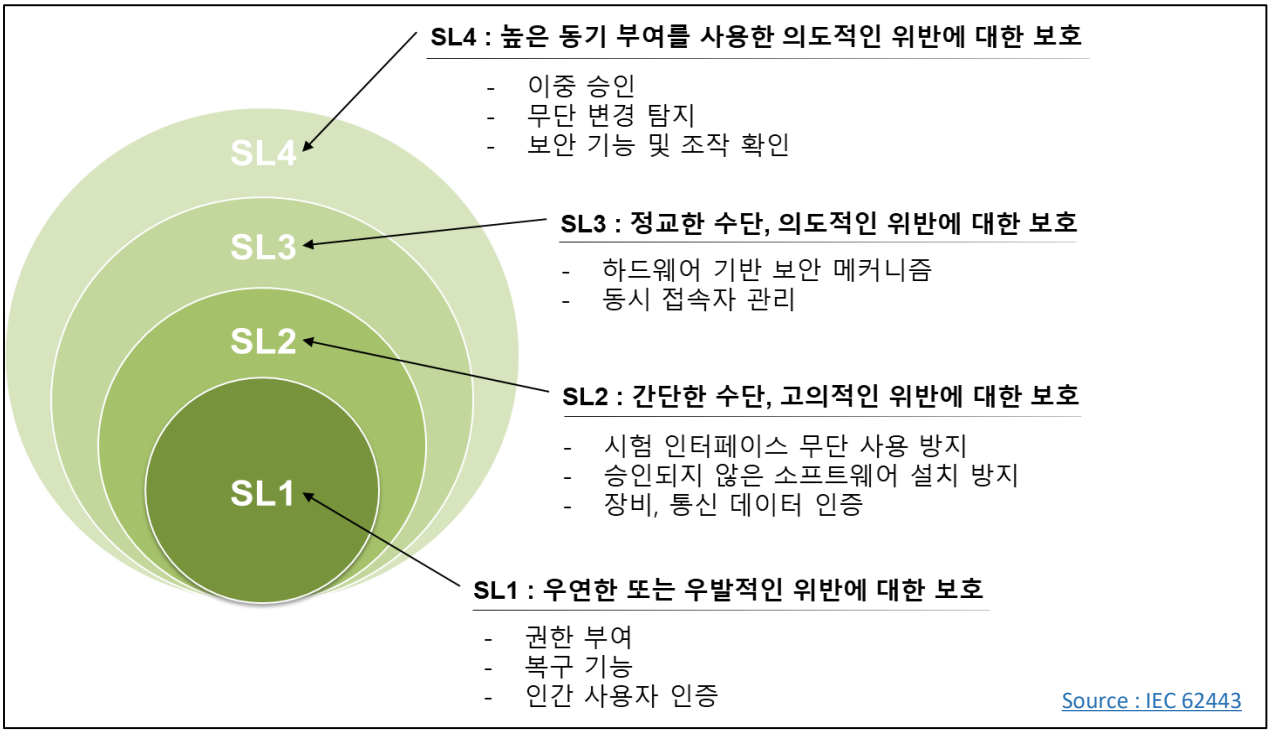
형식승인이란, 선박에 설치하기 전에 제품의 각 형식마다 미리 자료심사 및 승인시험을 하고 만족할 경우 제품이 규정에 적합하다는 것을 제조자에 대해서 증명하는 것을 의미한다. 사이버보안 형식승인은 ISA 62443 4-2, IEC 61162-460과 같은 국제표준을 기반으로 개발되었으며 선박에 탑재되는 원격 접속 장비, 통합 제어 및 모니터링 시스템 등을 포함하는 사이버 시스템의 사이버보안 수준 및 그 수준에 해당하는 요건을 12개의 범주 및 총 124개 항목의 요구 사항에 대한 검증을 통해 보안 기능과 그 수준을 확인한다.

<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

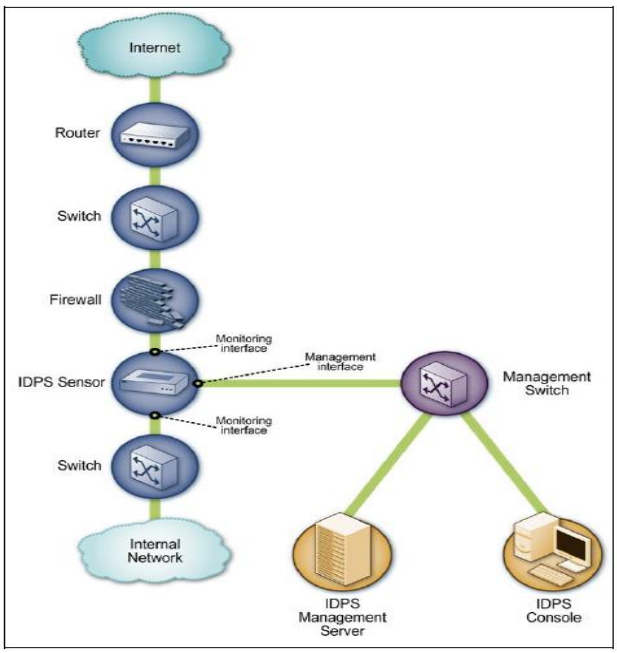
한국선급 해상 사이버보안 형식인증 검사항목

지속적인 모니터링 (702)

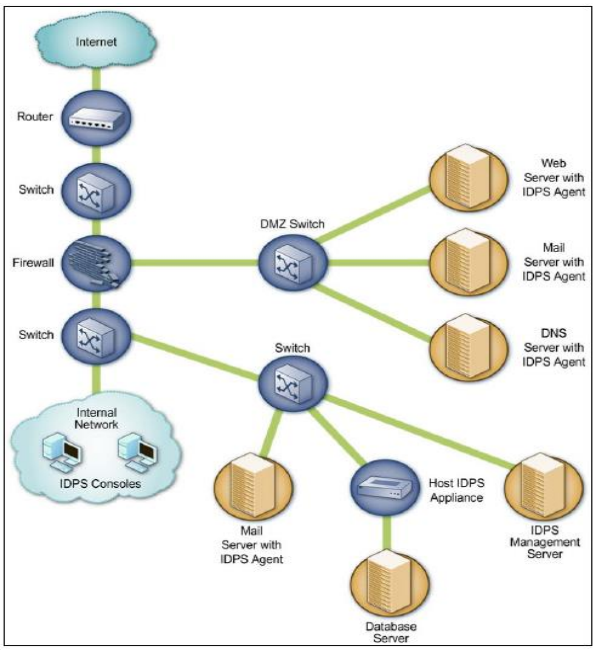
구성품은 보안 위반을 적시에 탐지 및 보고하기 위하여 일반적으로 인정되는 보안 산업 관행 및 권장사항을 사용하여 지속적으로 모니터링 하는 기능을 제공하여야 한다. (SL 2,3,4)

보안 위반 모니터링 도구

보안 위반을 모니터링 하기 위한 기능으로 IDS(침입 탐지 시스템 - Intrusion Detection System)가 있다. IDS의 사전적 의미는 칩입 탐지 프로세스를 자동화 하는 소프트웨어로써(출처 : NIST SP 800-94) IP 주소 혹은 네트워크 Port 기반의 차단 정책을 제공하는 방화벽의 한계를 보완하기 위해 사용될 수 있다. IDS는 패킷 분석을 통해 허용된 IP 및 Port를 통해 들어오는 데이터 패킷이라 할지라도 분석을 통해 칩입으로 간주 될 경우 이를 사용자에게 알리는 기능을 한다. IDS와 유사하나 탐지가 아닌 차단 기능을 제공하는 IPS(침입 차단 시스템 – Intrusion Prevention System)도 있으며 이를 통합하여 IDPS로 부르기도 한다. Security Level 2 이상을 받고자 하는 신청자는 보안 위반을 모니터링 하기 위해 IDS, IPS 혹은 이에 준하는 기능을 제공하여야 한다. IDS 및 IPS는 분석을 통해 칩입을 탐지 혹은 차단하므로 정상적인 데이터 패킷을 침입으로 간주하는 오탐의 가능성이 있으며, 구현방식은 네트워크 장비를 이용하는 네트워크 기반 방식(Network Based IDS/IPS), PC와 같은 단말기 상의 소프트웨어 어플리케이션을 이용하는 호스트 기반 방식(Host Based IDS/IPS) 등이 있다. 신청자는 보안위반에 대한 모니터링 기능을 위해 IDS 혹은 IPS의 종류 및 특성 등을 이해하고 적용 하여야 한다.



<네트워크 기반 IDPS 구성 예시>



<호스트기반 IDPS 구성 예시>

Source : https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

용어 설명

SSID(Service Set Identifier)

무선랜을 통해 전송되는 패킷들의 각 헤더에 덧붙여지는 32바이트 길이의 고유식별자로서, 무선 장치들이 BSS(Basic Service Set)에 접속할 때 마치 암호처럼 사용된다. SSID는 하나의 무선랜을 다른 무선랜으로부터 구분해 주므로, 특정 무선랜에 접속하려는 모든 AP나 무선장치들은 반드시 SSID가 일치하여야 한다.

MAC address 인증

컴퓨터 또는 모바일 기기의 모든 랜카드에는 MAC(Media Access Control) Address라는 것이 있다. 이 고유번호 체계를 이용한 인증방법으로서, 무선 AP에 등록된 기기만 무선 네트워크 사용이 가능하도록 하는 방법이다.

현재 AP에 접속되어 있는 디바이스 현황

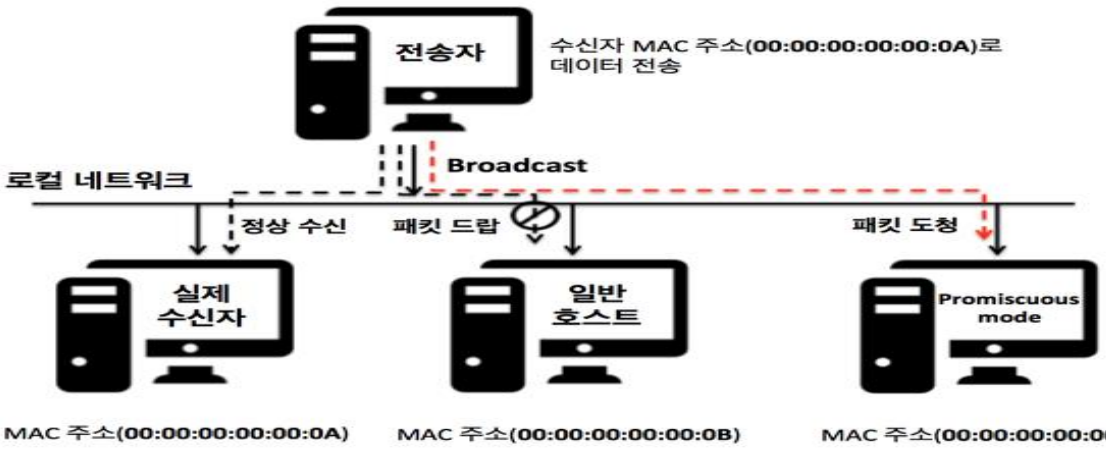
home_5G 무선인증 (MAC주소 인증 사용하지 않음)

연결된 MAC주소	연결상태	접속시간	설명
E0-[redacted]-2E	780Mbps	1분 31초	192.168.0.8(android-69bbe835163d829)
7C-[redacted]-E5	526Mbps	1분 8초	192.168.0.9(GLAM)
20-[redacted]-62	135Mbps	40초	192.168.0.12(Redmi5Plus-Redmi)

Source : https://honeycacao.tistory.com/94

Sniffing

사이버 해킹기법으로서 스니핑은 네트워크 상에서 자신이 아닌 다른 상대방들의 패킷 교환을 엿듣는 것을 의미한다. 간단히 말하면 네트워크 트래픽을 도청하는 과정을 스니핑이라고 할 수 있다.



Source : https://korea07.tistory.com/