KR Maritime Cyber Security

News from KOREAN REGISTER

June 2019

Vol. 014

한국선급 활동

● 현대일렉트릭 HYUNDAI-ISCS 대상 사이버보안 형식승인 증서 수여

한국선급은 지난 5일 노르쉬핑(Nor-Shipping) 전시회에서 현대일렉트릭이 개발한 차세대 선박용 스마트 통합 통신 시스템인 'HYUNDAI-ISCS (Integrated Smart Communication System)'에 대해 한국선급 최초로 사이버보안 형식승인 증서를 수여하였다.

최근 해사업계에 스마트 선박기술이 적용되는 등 기술의 고도화로 편의성이 증대된 반면 사이버위협에 노출될 가능성이 높아짐에 따라 사이버보안 인증 서비스에 대한 수요가 증가하고 있다. 이에 한국선급은 국제 표준(IEC 62443 4-2 및 IEC 61162-460 등)을 기반으로 자체 개발한 사이버보안 형식승인 서비스를 제공하고 있다.

한국선급의 사이버보안 형식승인 서비스는 사이버보안의 기본 요건인 기밀성, 무결성, 가용성에 대한 기술적 검토 및 사고 발생 시의 대응을 위한 감사, 백업 및 복구 기능에 대한 검사를 포함한다.

현대일렉트릭은 최첨단 기술을 사용하는데 따른 보안 위협을 인지하고 선제적으로 한국선급에 사이버보안 형식승인을 신청하였다. 그 결과 HYUNDAI-ISCS의 사이버보안 관련 기능이 충분히 구현됨을 검증 받았다.

이번 사이버보안 형식승인을 통해 현대일렉트릭의 HYUNDAI-ISCS은 보안 체계까지 갖추고 있음을 검증 받았기에 스마트 선박을 구축하려는 선주들에게 매력적인 대안이 될 수 있을 것으로 기대된다.

● KR 사이버보안 형식승인이란?

한국선급의 사이버보안 형식승인은 선박에 탑재되는 제품 또는 시스템이 선박에 설치되기 전에 시스템 내 각 세부 요소들이 사이버보안 기능을 갖추고 있는지에 대한 자료 심사와 승인시험을 하고, 이를 만족할 경우 해당 제품 또는 시스템이 한국선급의 사이버보안 규정에 적합하다는 것을 제조자에게 증명해 주는 것이다.

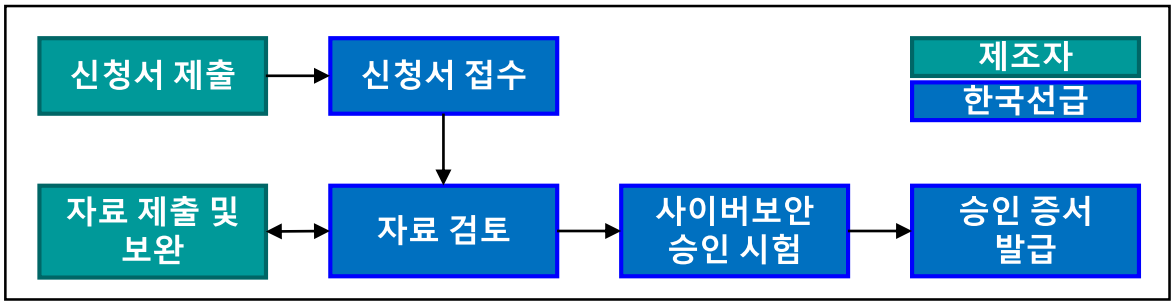
한국선급의 사이버보안 형식승인 규정은 국제기준인 IEC 62443 4-2와 IEC 61162-460을 기반으로 개발되었으며, 사이버보안 3요소인 기밀성, 무결성, 가용성에 대한 기술적인 기능을 확인하고 보안 사고 발생시의 대비한 감사 기능, 백업 및 복구 기능들을 확인한다.

Security level	Capabilities
SL1	Protection against casual or coincidental violation
SL2	Protection against intentional violation using simple means, low resources, generic skills, low motivation
SL3	Protection against intentional violation using sophisticated means, moderate resources, IACS specific skills, moderate motivation
SL4	Protection against intentional violation using sophisticated means, extended resources, IACS specific skills, high motivation

<한국선급 사이버보안 형식승인의 보안등급>

한국선급에 사이버보안 형식승인을 신청하고자 하는 제조자는 사이버보안 형식승인 신청서를 한국선급에 제출하고, 보안 기능에 대한 문서를 제출하여야 한다. 제출 문서를 통해 보안 기능의 적절성을 검토하고, 이를 검증하기 위하여 사이버보안 시험 절차서를 따라 사이버보안 시험을 수행한다. 자료 심사와 시험을 통해 모든 보안 기능이 검증되면 사이버보안 형식승인 증서가 발급된다.

사이버보안 형식승인과 관련한 문의 사항이 있으실 경우 한국선급 사이버인증팀 (cyber@krs.co.kr)에 문의하십시오.



<사이버보안 형식승인 절차>

실사례로 살펴보는 취약성 진단

● **취약성 진단 및 모의침투테스트란?**

취약성 진단 및 모의침투 테스트는 조직의 사이버보안 수준을 능동적으로 평가하기 위한 프로세스의 일환으로 실제 공격 행위(hacking)의 시뮬레이션을 의미한다.

최근 기반 시설에 대한 보안이 강화되면서 선박 및 해양 쪽 산업 시설의 제어 시스템에서도 실제 침투 테스트(Pen-Testing)을 통하여 사이버 위협을 사전에 진단하고 대응하는 기업과 기관들이 지속적으로 증가하고 있다.

● **취약성 진단 및 모의침투테스트의 필요성**

1. 정보 및 데이터의 무결성(Integrity)을 보장 받음으로써, 고객과의 신뢰 극대화
2. 네트워크 및 시스템에 내재된 위협과 취약점을 파악하여 침해 사고를 차단할 수 있는 보안 정책과 절차 작성 가능
3. 정기적인 모의침투 테스트 수행을 통해 기밀성, 무결성, 가용성을 수치로 측정하여 실제 위험을 우선순위 별로 식별하여 중복투자 방지

출처 : NSHC & Shield Consulting co.,ltd 허영일 대표 작성

● 취약성 진단 및 모의해킹의 분류

1. **Blind Test** : 검사 대상에 대한 정보 없이 수행. 수행 시 미리 검사 대상에 통보하고 수행합니다. 미리 통지한다는 윤리적 측면 때문에 많이 사용된다.
2. **Double Blind Test (Black Box Test)** : 해당 검사는 Pentester 도 정보를 알지 못하지만 검사 대상 역시 모의침투 테스트를 진행한다는 사실을 알지 못한다. 실제 환경에 가장 근접한 테스트이지만 짧은 시간 안에 결과를 도출하기가 어려워 프로젝트 기간이 길어질 수 있다. 프로젝트 기간은 비용과 연관되어 있어 비용 대비 성과를 충분히 고려하고 선택하여야 한다.
3. **Grey Box Test** : Pentester 는 제한적인 지식을 제공 받는다. 예를 들면 취약점 점검 결과를 넘겨 받거나 실제 수행할 수 있게끔 기회를 받는다. 해당 테스트 역시 모의해킹을 시작하기 전 검사 대상에 미리 통보한다.
4. **Double Grey Box Test (White Box Test)** : 검사 시간이 제한되어 있고 채널과 벡터는 검사하지 않는 점이 그레이 박스 테스트와 다르다.
5. **Tandem Test** : Tandem 테스트의 핵심은 pentester 가 모든 결과값을 볼 수 있다는 것이다. 검사 대상 역시 테스트 수행 전에 통보를 받는다. 해킹이 가능한 취약점을 다 확인 해볼 수 있다. 가장 이상적인 결과를 제출할 수 있다. Crystal box Test 가 그 예이다.
6. **Reversal Test** : Pentester 가 모든 정보를 알고 있지만 검사 대상은 검사가 실시 된다는 사실을 모른다. Red Team 테스트가 그 예이다.

● 실사례로 살펴보는 모의해킹 수행방법

1. 악성코드를 이용한 모의 침투 테스트 사례

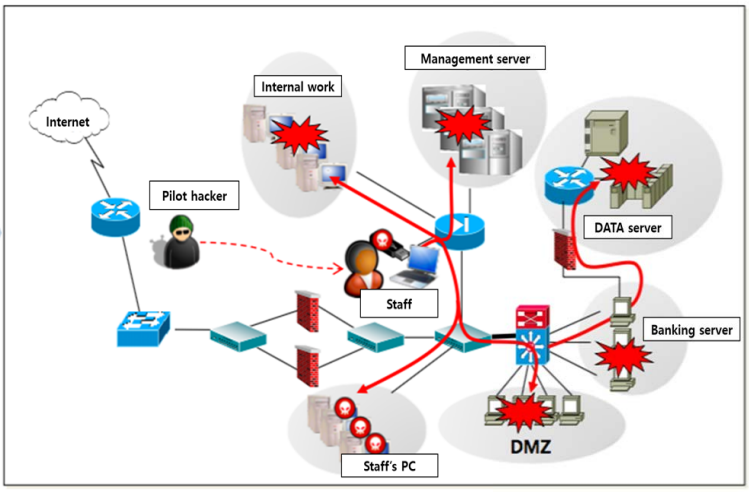
☞ **예상 시나리오 #1 : 악성코드 침투진단를 내부**
악성코드가 감염된 USB를 내부 직원을 통해 반입하여, 내부 네트워크에 연결해 악성코드를 유포하고, 감염된 PC로 부터 주요 정보를 획득한 후, 내부 보안 시스템을 우회하여 정보 유출

모의해킹 수행방법

- 악성코드 제작 및 내부반입
- 내부 네트워크에 연결된 PC를 통해 악성코드 유포
- 악성코드가 감염된 PC로 부터 주요 정보 획득
- 내부 보안시스템 우회를 통한 내부 주요 정보 유출

기대효과

- 주요 정보 암호화 여부 확인
- 내부 보안 시스템에 대한 안전성 확인
- 공격 대상 주위 시스템으로의 경유 공격 가능성 확인



2. 스피어 피싱 및 소셜 엔지니어링을 통한 모의침투 테스트 사례

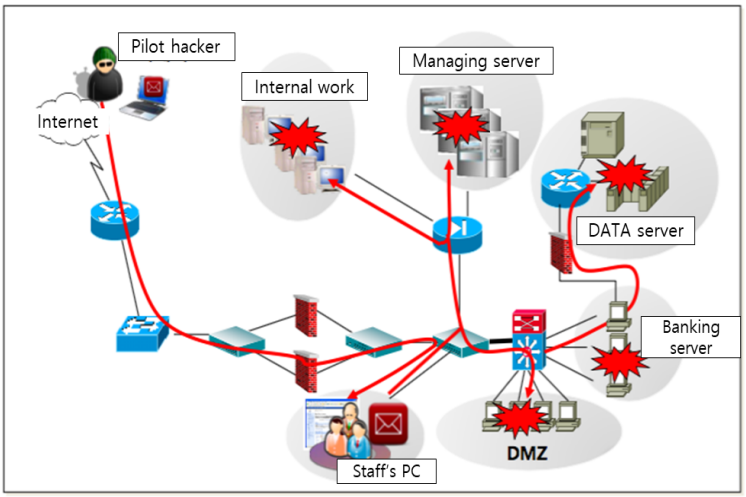
☞ **예상 시나리오 #2 : 메일 이용 악성코드 감염 및 침투 진단**
악성코드가 실행되는 메일 또는 악성코드가 있는 파일을 메일로 보내서 메일 수신인에 악성코드를 감염 시키고, 주요 정보를 수집하여 내부 보안 시스템을 우회하여 정보 유출

모의해킹 수행방법

- 악성코드가 삽입된 파일 제작
- 검색 또는 홈페이지를 통해 담당자 또는 관리자 이메일 주소 획득
- 악성코드를 포함하여 메일 발송
- 악성코드 감염된 수신인으로부터 주요 정보 획득
- 내부 보안 시스템 우회를 통한 내부 주요 정보 유출

기대효과

- 직원 보안 의식/관심 확인
- 내부 보안 시스템에 대한 안전성 확인
- 공격 대상 주위 시스템으로의 경유 공격 가능성 확인



3. 웹, 모바일 및 네트워크 방비에 대한 모의침투 테스트 사례

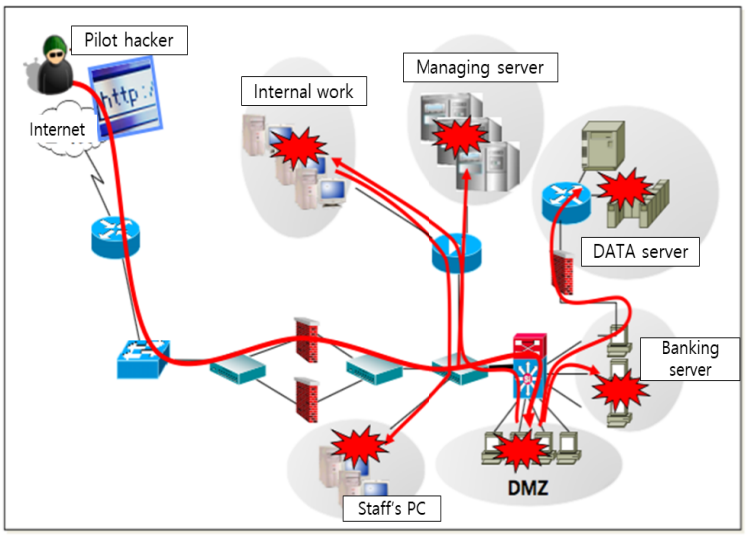
☞ **예상 시나리오 #2 : 웹 / 모바일 서비스 점령 이후 내부망 침투 진단**
공개용 웹/모바일 서비스의 취약점을 이용해 웹 서버에 접근하여 주요 정보를 획득하고, 연결된 내부 시스템에 접근하여 내부 보안 시스템을 우회하여 정보 유출

모의해킹 수행방법

- 웹 / 모바일 앱 취약점을 이용하여 웹 서버로 침투
- 침투한 웹 서버를 거점으로 DB 서버에 접근하여 주요 정보 수집
- 침투한 내부 웹 서버를 거점으로 내부 네트워크 상의 타 서버들을 침투하고 주요 정보 획득
- 내부 보안 시스템 우회를 통한 내부 주요 정보 유출

기대효과

- 직원 보안 의식/관심 확인
- 내부 보안 시스템에 대한 안전성 확인
- 공격 대상 주위 시스템으로의 경유 공격 가능성 확인



출처 : NSHC & Shield Consulting co.,ltd

USCG, 화물선에 대한 사이버 위협 발표

● **피싱 사기를 이용한 화물선 운항의 사이버 위협 사례 발표**

미국 해안경비대(이하, USCG)는 이메일 피싱을 통해 화물 선박의 운영 및 항법 정보를 해킹하는 사이버 위협 사례를 발표하였다.

5월 24일 미국 해안경비대의 안전게시판에 따르면, 해커들이 "이메일을 통해 NOA(Official Notice of Arrival) 내용을 포함한 민감한 정보를 얻으려고 하고 있다." 라고 전했다. 또한 USCG는 최근에 "선박용 컴퓨터 시스템을 교란시키기 위해 설계된 악성코드가 유포되고 있다는 보고를 받았다."고 하였다.

USCG는 선박 운영자와 선사의 관리자가 불필요한 전자메일에 응답하기 전 전자메일 발신지의 유효성을 확인할 필요성을 언급하였다. 선박 운영자와 선사의 관리자는 전자메일의 요청자가 불확실한 경우 확인된 연락처 정보로 PSC 기관에 직접 연락하는 것을 권장했다. 또한, 선주와 선박 운영자는 사이버 공격의 피해를 줄이기 위해 지속적인 사이버 방어 조치를 평가하도록 권장하였다.

USCG를 감독하는 소위원회 위원인 John Garamendi 의원은 4월의 공개포럼에서 스푸핑(Spoofing)을 포함하여 해상부문에서 사이버 위험이 증가하는 것에 대한 좀 더 많은 관심을 가져줄 것을 당부하였다.

USCG는 지중해 동부를 운항하는 선박에 의해 이집트 사이드 항구 근처에서 중대한 GPS 간섭 보고가 지속되고 있음을 2018년 10월과 11월에 경고하였다. USCG는 4 개년(2018-2022) 전략 계획에 따라 사이버 보안 예방 절차를 공유하여 사이버 보안 취약점을 해결하려고 시도하고 있다. 국제 해사기구 (International Maritime Organization)의 지침의 일환으로 선주들은 2021 년까지 선박의 안전 관리 시스템 내에서 사이버 리스크를 관리하도록 할 것이다.

출처 : https://www.freightwaves.com/news/phishing-scam-targets-cargo-ship-operations

사이버 위협의 이해(OWASP Top 10)

● 사이버 위협 이해하기

사이버 위협이란, 개인, 조직 또는 국가의 정보 또는 자산에 대해 사이버 시스템을 통한 무단 액세스, 파괴, 공개, 변조 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 목록화하고 주기적으로 최신화할 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

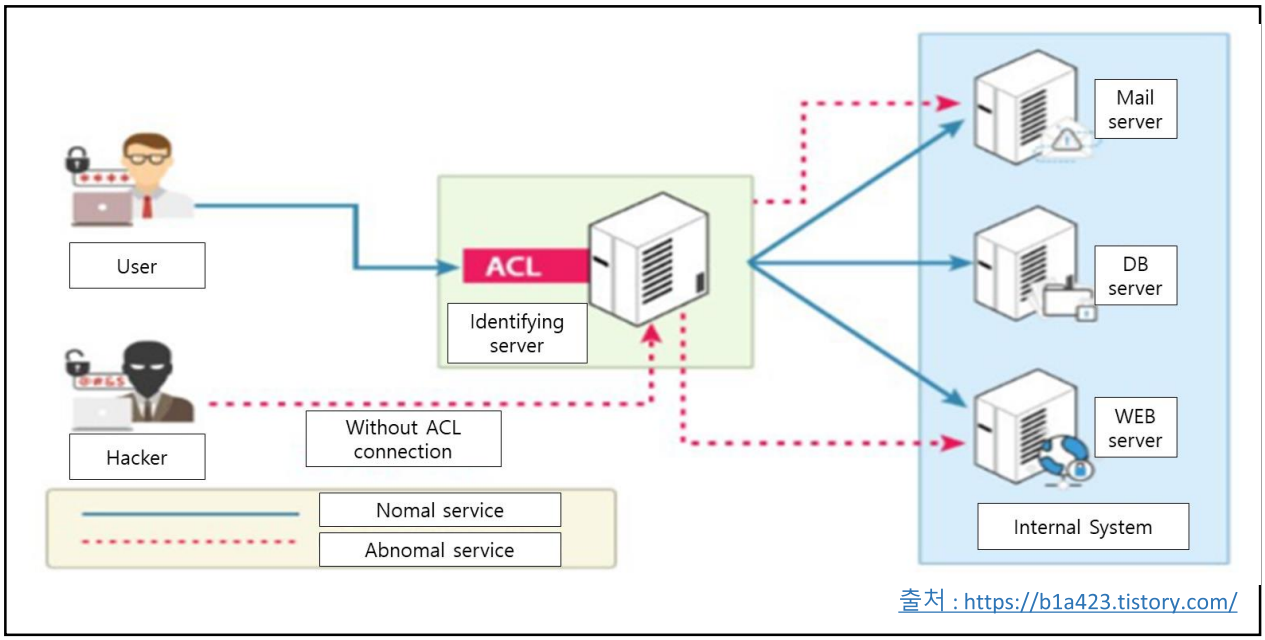
OWASP(Open Web Application Security Project)는 오픈소스 웹 어플리케이션 보안 프로젝트이다. 주로 웹에 관한 정보노출, 악성 파일 및 스크립트, 보안 취약점 등을 연구하며 웹 어플리케이션 취약점 중에서 빈도가 높고, 보안상 영향을 크게 줄 수 있는 10대 항목(OWASP Top 10)을 2004년, 2007년, 2010년, 2013년, 2017년 기준으로 발표하였다. 1월 뉴스레터에 이어 **'A5 : 2017 – 취약한 접근 통제'** 를 분석하고자 한다.

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – 인젝션	→	A1:2017 – 인젝션
A2 – 취약한 인증과 세션 관리	→	A2:2017 – 취약한 인증
A3 – 크로스 사이트 스크립팅 (XSS)	↘	A3:2017 – 민감한 데이터 노출
A4 – 안전하지 않은 직접 객체 참조 [A7 항목과 병합됨]	∪	A4:2017 – XML 외부 개체 (XXE) [신규]
A5 – 잘못된 보안 구성	↘	A5:2017 – 취약한 접근 통제 [합침]
A6 – 민감한 데이터 노출	↗	A6:2017 – 잘못된 보안 구성
A7 – 기능 수준의 접근 통제 누락 [A4 항목과 병합됨]	∪	A7:2017 – 크로스 사이트 스크립팅 (XSS)
A8 – 크로스 사이트 요청 변조 (CSRF)	☒	A8:2017 – 안전하지 않은 역직렬화 [신규, 커뮤니티]
A9 – 알려진 취약점이 있는 구성요소 사용	→	A9:2017 – 알려진 취약점이 있는 구성요소 사용
A10 – 검증되지 않은 리다이렉트 및 포워드	☒	A10:2017 – 불충분한 로깅 및 모니터링 [신규, 커뮤니티]

Ref. : OWASP Top 10 Project

● **OWASP 10대 위협 'A5 : 2017 – 취약한 접근 통제'**

취약한 접근 통제는 인증된 사용자만 접속할 수 있는 정보나 기능에 대한 통제가 제대로 적용되지 않는 것을 의미한다. 공격자는 이러한 취약점을 악용하여 사용자 계정 접속, 중요한 파일 보기, 사용자 데이터 수정, 접속 권한 변경 등과 같은 권한이 미부여된 기능, 또는 데이터에 접속할 수 있다. 접근통제 절차 무력화는 공격자들에게 요구되는 핵심 기술이다. 입력 값을 인증 절차 없이 사용자 계정 정보에 접근하는 용도의 SQL문에서 사용하는 애플리케이션이 있고, 공격자가 브라우저에서 서버로 전송되는 중간에 입력 값을 적절히 인증하지 않고 다른 사용자의 계정에 접근하는 것이 가능하다.



출처 : https://b1a423.tistory.com/

취약점 확인 방법

접근통제는 사용자들이 의도한 권한을 벗어난 행동을 할 수 없도록 정책을 시행합니다. 접근통제에 실패할 경우 일반적으로 인가되지 않은 정보 노출, 데이터 조작이나 파괴, 사용자에게 허용된 범위를 벗어난 사업적 기능 수행 등을 초래하게 됩니다. 흔하게 발생하는 접근통제 취약점들은 아래 사항들을 포함합니다:

- URL, 내부 애플리케이션 상태나 HTML 페이지 조작, 맞춤형 API 공격 툴을 통해 접근통제 절차를 우회할 수 있습니다.
- 기본 키가 다른 사용자의 레코드로 변경되도록 허용하고 다른 계정의 정보를 열람하거나 편집할 수 있도록 허용되어 있다면 접근통제에 실패한 것입니다.
- 로그인 하지 않고 활동하는 사용자나 일반 사용자로 로그인하여 관리자처럼 활동하는 사용자가 있다면 권한상승이 가능한 상태입니다.
- JSON 웹 토큰 (JWT)의 접근 통제 토큰 재전송이나 변경, 권한 상승 목적으로 쿠키나 감춰진 필드 조작, JWT 토큰 무효화 악용 등과 같은 메타 데이터 조작 행위가 허용된다면 접근 통제에 실패한 것입니다.
- CORS에 대한 설정이 잘못되어 있을 경우 인가되지 않은 API에 접근을 허용할 수도 있습니다.
- 인증 절차를 거치지 않은 사용자가 인증이 필요한 페이지를 둘러보게 하거나, 권한이 필요한 페이지에 일반 사용자가 접근해 보도록 하거나 POST, PUT, DELETE 메소드에 대한 접근통제를 적용하지 않은 API를 사용해 보게끔 함으로써 접근통제 실패 여부를 확인할 수 있습니다.

보안 대책

접근 통제는 공격자가 접근 제어 검사 또는 메타 데이터를 수정할 수 없는 신뢰할 수 있는 서버 측 코드 또는 서버가 없는 API에 적용될 경우에만 효과적입니다.

- 불특정 다수에게 공개된 자원을 제외하곤 디폴트 정책은 차단으로 운영해야 합니다.
- CORS 사용 최소화를 포함한 접근통제 절차를 구현하고 애플리케이션 전체에 적용해야 합니다.
- 접근통제 모델은 사용자에게 특정 레코드를 생성/열람/수정/삭제 할 수 있는 권한을 허용하기 보다는 레코드 소유자만 권한을 갖게 끔 강제해야 합니다.
- 유일한 애플리케이션 비즈니스의 제한 요구 사항들은 도메인 모델에 의해 적용되어야 합니다.
- 웹 서버상의 디렉토리 리스팅 기능을 비활성화 하고 .git과 같은 메타데이터와 백업파일들이 웹 루트에 존재하지 않게끔 운영해야 합니다.
- 접근 통제에 실패한 경우에는 기록되어야 하고, 반복적인 실패가 발생하는 것과 같이 적절한 시점에 관리자에게 경고 메시지가 전송되어야 합니다.
- 자동화 공격 툴로 인한 피해를 최소화 하기 위해 API와 컨트롤러에 대한 접근 임계치를 제한해야 합니다.
- JWT토큰은 로그아웃 이후 무효화 되어야 합니다.

개발자 및 품질보증 담당자는 기능적인 접근통제 부분과 통합 테스트를 포함시켜야만 합니다.

출처 : OWASP Top 10 - 2017

네트워크 보안 수립 가이드라인

● **네트워크 보안의 정의**

네트워크 보안은 물리적인 또는 소프트웨어 방어 도구를 이용해 기반 네트워크 인프라를 승인되지 않은 접속이나 오용, 오동작, 수정, 파괴, 부적절한 노출 등으로부터 보호하는 프로세스이다. 네트워크 보안의 목표는 비 인가된 사람이나 프로그램이 네트워크와 네트워크에 연결된 디바이스에 접속하는 것을 막는 것이다.

● **네트워크 보안의 방법**

보호 : 시스템과 네트워크를 최대한 올바르게 설정
탐지 : 설정이 변경되거나 일부 네트워크 트래픽 문제 시 신속히 파악
대응 : 대응 조치를 취하고 가능한 빨리 안전한 상태로 복구

이를 위해 액세스제어, 백신, 행위분석 이메일 보안, 방화벽 설정, 침입탐지 및 방지, 모바일 디바이스 및 무선 보안 네트워크 망 분리, SIEM, VPN, 웹 보안 등의 구현이 필요하다.

● **한국선급 해상 사이버보안 인증 검사항목(CS1)**

통신채널 보호(218.1) : 통신 채널의 결함으로 타 네트워크에 영향을 미치지 않도록 네트워크 장비의 취약성을 주기적으로 확인하여야 한다.

네트워크 침입 차단 및 모니터링(218,2) : 내부 네트워크의 보호를 위하여 외부 비인가된 접근을 차단하는 침입차단 시스템의 설치 및 운영 시 지속적 관리를 적용한다.

네트워크 유무선 망 분리(218.3) : 무선 네트워크 환경 구축 시 외부인이 접속 가능한 무선 네트워크를 분리되어 구성되어야 한다.

무선접속 제한(218.4) : 정보기술이 무선 네트워크를 통하여 접근되지 않도록 제한하여야 한다.

네트워크 구성 관리(218.7) : 네트워크 경로를 파악할 수 있는 도식화된 네트워크 흐름을 보유하여야 한다.

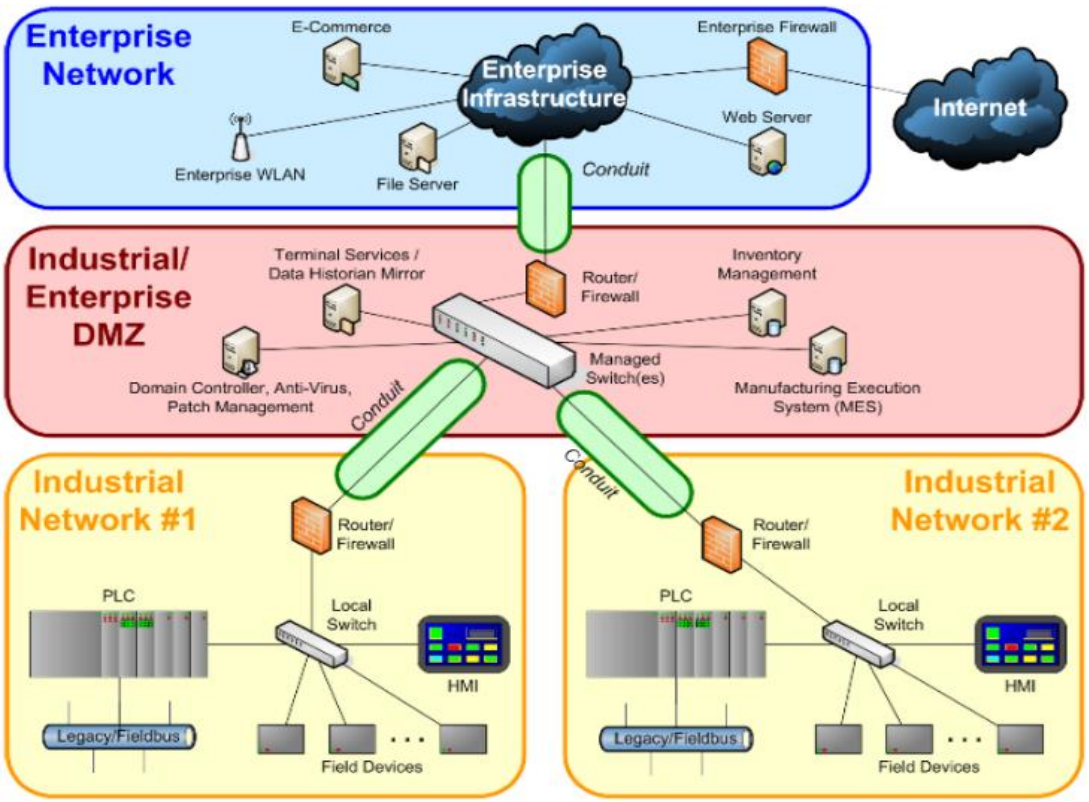
네트워크 장비 관리(218.8) : 네트워크 관련 장비 구축 시 기본 설정값(default)을 제거하고 보안 관련 기능을 활성화 하도록 하여야 하며, 필요 시 공급자에게 요구하여 적용하여야 한다.

● 네트워크장비 취약점 분석·평가 항목(예시)

네트워크장비 취약점 분석·평가 항목			
분류	**점검항목**	**항목 중요도**	**항목코드**
1. 계정관리	패스워드 설정	상	N-01
	패스워드 복잡성 설정	상	N-02
	암호화된 패스워드 사용	상	N-03
	사용자·명령어별 권한 수준 설정	중	N-15
2. 접근관리	VTY 접근(ACL) 설정	상	N-04
	Session Timeout 설정	상	N-05
	VTY 접속 시 안전한 프로토콜 사용	중	N-16
	불필요한 보조 입·출력 포트 사용 금지	중	N-17
	로그온 시 경고 메시지 설정	중	N-18
3. 패치관리	최신 보안 패치 및 벤더 권고사항 적용	상	N-06
4. 로그관리	원격 로그서버 사용	하	N-19
	로깅 버퍼 크기 설정	중	N-20
	정책에 따른 로깅 설정	중	N-21
	NTP 서버 연동	중	N-22
	timestamp 로그 설정	하	N-23

출처 : 한국인터넷진흥원(KISA), 주요정보통신기반시설 기술적 취약점 분석·평가 상세가이드

● 도식화된 네트워크 구성도(예시)



출처 : IEC 62443 2-1

용어 설명

- **기밀성(Confidentiality) :** 권한이 없는 개인, 단체, 또는 프로세스에 정보를 제공하거나 공개하지 않는 속성을 말한다. 방화벽이나 암호, 패스워드 같은 것들이 기밀성의 대표적인 예이다.
- **무결성(Integrity) :** 정밀성, 정확성, 완전성, 유효성의 의미로 사용되며, 데이터베이스의 정확성을 보장하는 문제를 의미한다. 예를 들어, 데이터 무결성은 데이터를 보호하고, 항상 정상인 데이터를 유지하는 것을 말하고, 이를 위한 여러 연구가 진행되고 있다.
- **가용성(Availability) :** 권한 있는 주체의 요청에 따라 접근 가능하고 사용할 수 있는 속성을 말한다. 예를 들어, 시스템이 장애(failure) 상태에 빠져 더 이상 서비스 혹은 자원을 제공하지 못하는 경우 가용성이 저하된다.
- **스푸핑(Spoofing) :** 승인 받은 사용자인 것처럼 시스템에 접근하거나 네트워크 상에서 허가된 주소로 가장하여 접근 통제를 우회하는 공격행위를 말한다. 예를 들어, 임의로 웹 사이트를 구성해 일반 사용자들의 방문을 유도하고, 인터넷 프로토콜인 TCP/IP의 구조적 결함을 이용해 사용자의 시스템 권한을 획득한 뒤 정보를 탈취하거나 허가 받은 IP을 도용해 접속한다.
- **스피어 피싱(Spear phishing) :** 특정한 개인이나 회사를 대상으로 한 피싱(Phishing) 공격을 말하며, 공격자가 사전에 공격 성공률을 높이기 위해 공격 대상에 대한 정보를 수집하고, 이를 분석하여 피싱 공격을 수행하는 형태이다.
- **소셜 엔지니어링(Social engineering 공격** : 시스템에 침입하는데 기술적인 해킹기법 대신 사람의 심리를 악용해 시스템 또는 데이터, 건물에 대한 출입권한을 확보하는 것을 말한다.
- **ACL(Access Control List)** : 엑세스 제어 목록은 개체나 개체 속성에 적용되어 있는 허가 목록을 말한다. 이 목록은 누가 객체 접근 허가를 받는지, 어떠한 작업이 객체에 수행되도록 허가를 받을지를 지정한다.