KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 015

July 2019

한국요꼬가와전기 IAS에 사이버보안 AIP 증서 수여

한국선급은 지난 7월 5일, ㈜한국요꼬가와전기의 통합자동화시스템(IAS, Integrated Automation System)에 사이버보안 개념승인(AIP, Approval in Principle) 증서를 수여하였다. 한국선급의 사이버보안 개념승인(AIP)은 최근 조선·해양산업의 중요한 화두로 떠오르고 있는 사이버 위협에 대비하기 위해 사이버 안전성에 대한 기본설계를 승인해 주는 절차이다. ㈜한국요꼬가와전기의 통합자동화시스템(IAS)은 LNG 운반선에 주로 적용되는 시스템으로서, 화물시스템과 기계시스템을 제어하고 모니터링 하는 것은 물론 추진시스템에 따라 LNG 증발가스(BOG, Boil Off Gas)를 관리하는 시스템이다. 한국선급은 한국요꼬가와전기의 통합자동화시스템에 사이버보안 국제표준인 IEC 62443과 NIST 표준을 기반으로 기본설계에 대해 적합성 여부를 검증한 후 AIP 증서를 수여하였다. 국제해사기구(IMO) MSC.428(98) 결의안에 따라 2021년부터 사이버보안 리스크관리가 강화될 예정이므로, 선박에 적용되는 시스템도 사이버보안 형식승인 수요가 증가될 것으로 예상된다. 한국선급은 국제표준인 IEC 62443과 IEC 61162-460을 기반으로 자체 개발한 사이버보안 형식승인 서비스를 제공하고 있다. 사이버보안 형식승인은 사이버보안의 기본요건인 기밀성, 무결성, 가용성에 대한 기술적 검토와 사고발생 시 대응을 위한 감사, 백업 및 복구 기능에 대한 검사를 자료심사와 시험을 통해 검증하며 증서를 발급하는 절차이다.

한국선급 활동#2

산쇼코리아㈜ 맞춤형 해사 사이버보안 교육 실시

한국선급은 지난 7월 9일, 산쇼코리아㈜에 OCIMF TMSA(탱커선 화주검사) 대응을 위한 사이버보안 맞춤형 교육을 실시하였다.

본 교육은 '해사 사이버보안 실무 해설' 및 '해사 사이버보안 리스크평가' 과정으로 구성되었으며 한국선급은 이번 교육의 산쇼코리아㈜ 고객만족도 조사에서 큰 호평을 받았다.

한국선급은 지난 `18년 4월, 영국 글라스고에 위치한 SONGA 선사에 OCIMF TMSA 대응을 위한 사이버보안 맞춤형 교육을 진행하여 SONGA 선사 TMSA 수검을 지원한 바 있다. 한국선급은 향후 해사 사이버보안에 대한 선사와 조선소, 기자재업체를 대상으로하는 사이버보안 맞춤형 교육 서비스를 강화해 나갈 방침이다.

OCIMF TSMA(3판)	OCIMF SIRE VIQ (7판)
13.1.2 회사는 선박이 항행하는 구역 및 회사 사무실에 적용되는 보안 위협을 식별하는 절차가 있다.	7.14 사이버보안 정책/절차에 사이버보안 대응 계획이 포함 되어 있는가?
13.2.3 사이버 보안을 포함하고 있는 방침 및 절차를 통해 적절한 지침 및 경감 조치가 제공된다.	7.15 선상 IT / OT 시스템에 대한 물리적 접근 통제에 관한 회사 정책을 선원이 알고 있습니까?
13.2.4 회사는 적극적으로 사이버 보안 인식을 증진 시킨다	7.16 회사는 탑재된 개인 장치의 사용에 관한 정책이나 지침을 가지고 있습니까?
13.3.2 보안절차는 현행 지침을 고려하여 업데이트 된다.	7.17 사이버 보안에 대한 인식이 회사와 선원에 의해 적극적으로 홍보됩니까?
13.4.5 회사는 혁식적인 보안 기술 및 시스템을 테스트하고 회사에 시행하는데 참여하고 있다.	

한국선급 활동#3

국가인적자원개발 컨소시엄 해사사이버보안 교육 실시

지난 6월, 한국선급 사이버인증팀은 KR 교육훈련원에서 국가인적자원개발 컨소시엄 교육 과정인 '해사 사이버보안의 이해' 및 '해사 사이버보안 관리 실무' 과정 교육을 수행하였다.

'해사 사이버보안의 이해[8H]' 과정은 해사업계(선사, 선박, 조선소, 기자재업체)에 근무하는 임직원 및 선원들을 대상으로 사이버보안에 대한 이해를 증진시키고, 사이버보안에 필요한 사이버보안 조직, 사이버 자산관리 및 위협, 인적보안, 물리보안, 기술보안 교육을 통해 해사 사이버보안에 대한 인식 제고 향상을 목표로 한다.

'해사 사이버보안 관리 실무[16H]' 과정은 심화과정으로써 사이버보안 IT 해설 및 실습, 사이버 리스크평가 이해 및 실습으로 구성되어 있다. 특히 리스크평가 워크샵을 통해 회사 및 선박 사이버 취약점을 식별하고, 리스크 평가 절차 및 방법, 개선 방안 등을 직접 확인 할 수 있다.

한국선급은 본 교육과정을 통해 IMO와 OCIMF TMSA/SIRE 및 RIGHTSHIP 등의 화주검사에서 요구하고 있는 사이버보안 인식제고 교육 및 사이버 리스크 관리 방법을 국내 해사업계에 전파하였으며, 피드백 사항을 반영하여 다양한 사이버보안 실무 교육 과정을 2019년 개최할 예정이다.

2019년도 국가인적자원개발 컨소시엄 교육과정 안내

'해사 사이버보안의 이해(1일)', '해사 사이버보안 관리 실무(2일)' 과정을 포함한 2019년도 국가인적자원개발 컨소시엄 18개 교육과정이 개설되었다.

'해사 사이버보안의 이해[8H]' 과정은 해사업계(선사, 조선소, 기자재업체)에 근무하는 임직원을 대상으로 사이버보안에 대한 이해를 증진시키고, 사이버보안에 필요한 조직구성, 자산관리 및 위협, 인적보안, 물리보안, 기술보안 교육을 통해 인식 제고 향상을 목표로 한다. (교육일정 : 10.8)

'해사 사이버보안 관리 실무[16H]' 과정은 심화과정으로써 사이버보안 IT 해설 및 실습, 사이버 리스크평가 이해 및 실습으로 구성되어 있다. 특히 리스크평가 워크샵을 통해 회사 및 선박 사이버 취약점을 식별하고, 리스크 평가 절차 및 방법, 개선 방안 등을 직접 확인 할 수 있다. (교육일정 : 10.29-30)

한국선급은 지난 2018년 6월 국가인적자원개발 컨소시엄 운영기관으로 지정되어한국선급과 컨소시엄 체결 기업의 재직자를 대상으로 무상으로 교육을 제공하고 있으며, KR 컨소시엄 홈페이지(http://champ.krs.co.kr) 를 통해 접수할 수 있다.

2019년 국가인적자원개발 컨소시엄 교육과정 안내

교육 과정 명	교육시간	교육 일자	교육 장소
전기 방폭(화재폭발방지) 실무	2일(16h)	19.04.24 ~ 04.25 19.11.26 ~ 11.27	한국선급 국제교육 훈련센터
Design LNG/LPG Carrier(Hull &Equipment Part)	1일(8h)	19.04.29 ~ 04.29 19.08.27 ~ 08.27	
High Voltage(고전압) Switching	2일(16h)	19.05.09 ~ 05.10 19.11.05 ~ 11.06	
Design LNG/LPG Carrier(System Part)	1일(8h)	19.05.20 ~ 05.20 19.09.03 ~ 09.03	
품질 통합관리 시스템 구축 및 운영 실무	2일(16h)	19.05.27 ~ 05.28 19.09.23 ~ 09.24	
Fire Fighting System(FSS Code)	1일(8h)	19.05.29 ~ 05.29 19.09.20 ~ 09.20	
Low Voltage(저전압) 시스템	2일(16h)	19.06.03 ~06.04 19.12.03 ~12.04	
해사 사이버 보안의 이해	1일(8h)	19.06.10 ~ 06.10 19.10.08 ~ 10.08	
Rightship Inspection 요구사항 이해 및 실무	2일(16h)	19.06.18 ~ 06.19 19.10.16 ~ 10.17	
해사 사이버보안 관리 실무	2일(16h)	19.06.27 ~ 06.28 19.10.29 ~ 10.30	

한국선급 활동#4

Maritime Cyber Risk Management Forum 2019

한국선급은 지난6월 25일 영국 런던에서 개최된 Maritime Cyber Risk Management Forum 2019에 참석하여 사이버보안 최신 국제 동향 및 기술개발 현황을 모니터링하였다.
포럼은 총 6개의 세션으로 구성되어 해사업계 전문가들의 활발한 논의가 이루어졌다. 사이버 리스크관리를 위한 규정 및 법률 준수, 선주사 및 운영사 관점, 사이버보안 사고 실습, 항만 사이버보안 위협, 해상 사이버공격 대응방안에 대한 발표가 있었고 해사업계의 사이버보안 대응 및 전략 수립이 필요함을 확인할 수 있었다.

특히 [세션 2]에서는 머스크해운의 Andy Powell(CISO, 정보보호최고책임자)로부터 2017년 6월 발생한 사이버 공격 사례(랜섬웨어)와 이로 인해 머스크가 구현하고 있는 5가지 핵심운영 원칙(책임, 리스크관리, 신뢰, 복원성, 사이버보안 이점)가 소개되어 주목을 끌었다.

해상 사이버보안 대응 체계구축을 위해서는 해사업계의 다양한 이해관계자(항만, 선주, 선급, 조선소, 제조업체, 서비스업체 등)의 책임과 역할이 명확히 식별되어야 하며, 국가 차원에서 해사업계의 전략 수립이 필요할 것으로 예상된다.

구분	주요내용
[세션 1] 규정, 준수 및 리스크 관리	· 사이버 사건 대응 환경에서 법률 및 규정 준수 · 사이버 보안에 관한 가이드 라인 · 사이버 사건으로 인한 손해 및 보험
[세션 2] 선주사 및 운영사 관점	· 벤더 리스크 관리 · 주요 사이버 공격으로부터 얻은 교훈 구현 · 산업 제어 시스템(ICS)에서 배운 사이버 교훈
[세션 3] 사이버보안 사고 실습	· 사이버공격 시나리오를 기반으로 결과와 해결책 논의
[세션 4] 항만 사이버보안 위협	· 유럽 항구 및 공급망 보호를 위한 솔루션 · 항만 가상 물리 보안 : 융합된 리스크에 적합한 대응 필요 · OT & IT 시스템에서 실시간 위협 탐지에 AI 사용
[세션 5] 사이버공격 대응방안	· 리스크 관리를 위한 선원 인식의 중요성 및 선내 및 육상 직원을 훈련시킬 수 있는 도구 논의 · 해양 커뮤니티 형성 및 협업을 통한 보안 필요
[세션 6] 사이버보안 허브	· 해상 사고 대응의 과제 · 해양 전자 장비 및 서비스 제공 업체를 위한 CIRM 사이버 리스크 관행 지침 개발

출처 : https://www.shipcybersecurity.com/

IMO MSC 101차 회의 사이버보안 관련 논의 결과

제 101차 IMO 해사안전위원회, 해상 사이버 리스크관리를 위한 조치 발표

지난 2019년 6월, 영국 IMO 본부에서 개최된 제 101차 IMO 해사안전위원회(MSC)에서 해상 사이버 리스크관리를 위한 논의가 이루어 졌다. 특히 이번 회의에서 ISM과 ISPS의 요건을 모두 만족하는 해상 사이버 리스크 통합 관리의 필요성이 제기되었다.

IMO는 2017년 7월, 제 98차 MSC 회의에서 ISM코드의 선박 안전관리시스템(SMS)에 사이버 리스크를 포함하기로 결의서 MSC.428(98)를 채택하였고, 2021년 1월 1일 이후 사업장 안전관리 적합증서(DOC)의 첫번째 연차심사부터 이를 준수하도록 장려하고 있다.

하지만, ISM 코드의 안전관리시스템(SMS)과 ISPS 코드의 선박보안계획(SSP)에서 각각 별도의 사이버리스크 관리를 요구하게 됨에 따라 두 문서 간 내용이 일치하지 않는 우려가 제기되었다. 선박보안계획(SSP) 의 경우 변경될 때마다 정부의 승인을 받아야 하므로 선사에서는 행정적인 부담이 증가 될 수 있기 때문이다. 따라서 IMO는 이러한 문제를 해결하기 위해 물리적 보안사항은 ISPS 코드에 따라 선박보안계획(SSP) 에서 다루는 것을 원칙으로 하나, 안전관리시스템(SMS) 에서 사이버 보안 관리체계가 마련되어 있다면 별도의 리스크 관리체계를 요구하지 않기로 이번 101차 MSC회의에서 결정하였다. 이는 IMO 결의서 MSC.428(98)에 따라 ISM 코드가 발효되는 2021년 1월 1일 이후 사업장 안전관리적합증서(DOC) 및 안전관리증서(SMC)에 사이버 리스크 관리시스템을 보장하도록 하였기 때문에 ISPS 코드의 선박보안계획(SSP)는 ISM코드의 안전관리시스템(SMS)에서 발견된 사이버 리스크 관리절차를 참조만 하도록 한 것이다.

IMO 자율운항선박(MASS) 임시운항지침 내 사이버 리스크 관리를 포함

이번 IMO MSC 회의에서는 위에서 언급된 해상 사이버 리스크관리를 위한 조치와 별개로 자율운항선박(MASS, Maritime Autonomous Surface Ships)의 시범운항을 위한 해상 시운전 지침 초안을 마련하였다. 이 지침 초안에는 자율운항선박 시험을 수행할 때 사용되는 시스템과 인프라에는 사이버 리스크관리가 충분히 보장되도록 추가 반영하였다. 따라서 향후 추진이 예상되는 스마트 항만, 자율운항선박 등 정책개발과 기술표준 개발에 있어 초기단계에서부터 사이버보안을 고려할 필요가 있을 것이다.

사이버 위협의 이해(OWASP Top 10)

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

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 '**A6 : 2017 – 잘못된 보안구성**'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]

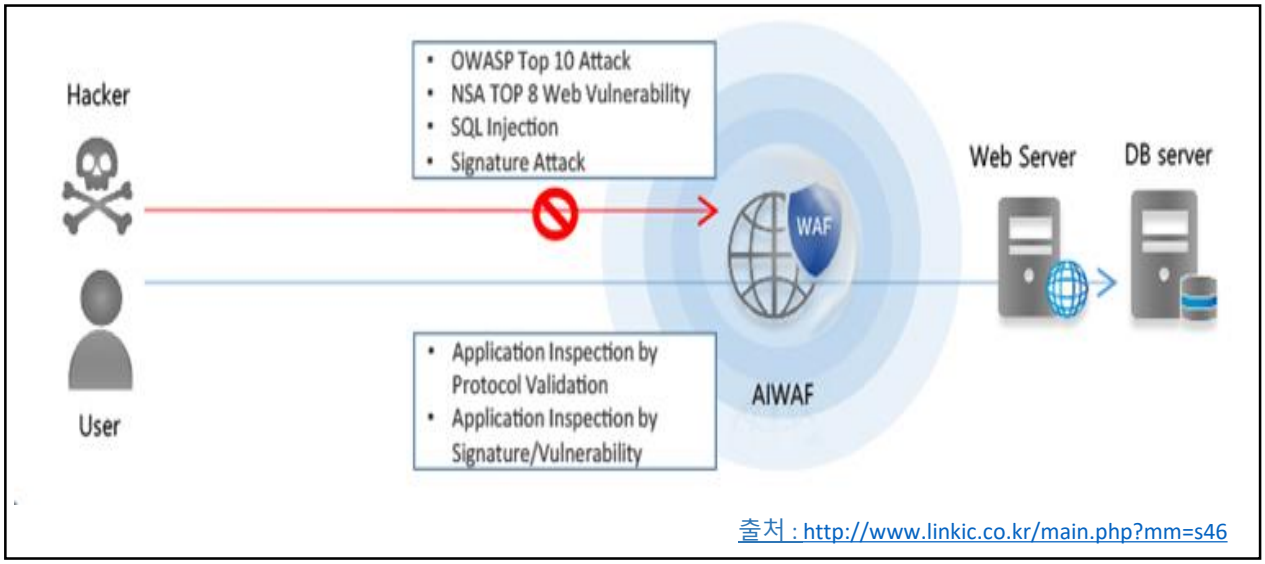
Ref. : OWASP Top 10 Project

OWASP 10대 위협 'A6 : 2017 - 잘못된 보안구성'

잘못된 보안구성은 가장 흔하게 보이는 이슈로서, 취약한 기본설정, 미완성(또는 임시 설정), 개방된 클라우드 스토리지, 잘못 구성된 HTTP 헤더 및 민감한 정보가 포함된 장황한 에러 메시지로 인한 결과 이다. 모든 운영체제, 프레임워크, 라이브러리와 앱을 안전하게 설정해야 할 뿐만 아니라 시기 적절하게 패치/ 업그레이드를 진행해야 한다.

<대응정책>

- **URL 확장자 접근 제어** : 클라이언트로부터 요청 가능한 확장자 정의
- **디폴트 페이지 접근 탐지** : 관리자 페이지 접근탐지
- **디렉토리 리스팅** : 웹 서버의 잘못된 설정에 의해 파일정보가 노출되는 것을 차단
- **에러페이지 클로킹** : 웹 서버의 응답코드를 확인하여 관리자가 지정한 문구를 전송



출처 : http://www.linkic.co.kr/main.php?mm=s46

취약점 확인 방법

애플리케이션이 아래 사항들에 해당할 경우 취약한 상태일 수도 있습니다:

- 애플리케이션 스택 전 영역에 적절한 보안 강화 절차가 누락된 상태이거나 클라우드 서비스 상에 권한이 부적절하게 설정되어 있습니다.
- 불필요한 기능(예: 포트, 서비스, 페이지, 계정, 특수권한 등)이 활성화 되거나 설치되어 있습니다.
- 디폴트 계정과 비밀번호가 활성화 되어 있거나 해당 정보들을 변경 없이 사용하고 있는 중입니다.
- 에러 처리 과정에서 스택 추적 정보나 공격에 도움이 될만한 다른 정보들을 노출하고 있습니다.
- 업그레이드된 시스템 상에 최신 보안 기능들이 비활성화 되어 있거나 안전하게 설정되어 있지 않습니다.
- 애플리케이션 서버, 프레임워크(예:Struts, Spring, ASP.NET), 라이브러리, 데이터베이스 상에 보안 설정이 되어 있지 않다.
- 서버가 보안 헤더, 보안 강화 수단을 보내지 않거나 안전한 값을 설정하지 않고 있습니다.
- 구 버전이나 취약한 버전의 소프트웨어를 사용하고 있습니다 (**A9:2017-알려진 취약점이 있는 구성요소 사용** 참고).

협력적이고 반복적인 애플리케이션 보안 설정 절차가 없다면 시스템은 높은 위험에 처해 있다고 봐야 합니다.

보안 대책

아래 사항들을 포함한 안전한 설치 과정이 시행되어야 합니다:

- 위험을 적절하게 차단할 수 있도록 빠르고 쉽게 다른 환경으로 전환할 수 있는 반복적인 보안 강화 절차를 적용해야 합니다. 개발, 품질 관리, 운영 환경은 환경 별로 상이한 자격 증명 정보를 사용하고 동등한 보안 수준으로 설정되어야 하며, 새로운 보안 환경을 구축하는데 소모되는 리소스를 최소화 하기 위해 절차를 자동화 해야 합니다.
- 불필요한 기능, 구성 요소, 문서, 샘플 애플리케이션 없이 최소한으로 플랫폼을 유지하고 사용하지 않는 기능과 프레임워크는 삭제하거나 설치하지 말아야 합니다.
- 패치 관리 절차의 일부분으로 모든 보안 정보, 업데이트, 패치를 대상으로 설정을 적절히 검토하고 갱신하는 절차가 필요하며, 특히 S3 버킷 권한과 같은 클라우드 스토리지 권한을 검토하는 절차가 중요합니다(**A9:2017-알려진 취약점이 있는 구성요소 사용** 참고).
- 세분화, 컨테이너화, 클라우드 보안 그룹과 같은 방법으로 구성 요소나 입주자들 간에 효율적이고 안전한 격리를 제공하는 세분화된 애플리케이션 아키텍처를 적용해야 합니다.
- 보안 헤더와 같은 보안 강화 수단을 사용자에게 전송해야 합니다.
- 모든 영역의 보안 설정이 적절히 반영되어 있는지 검증할 수 있는 자동화된 절차를 수립해야 합니다.

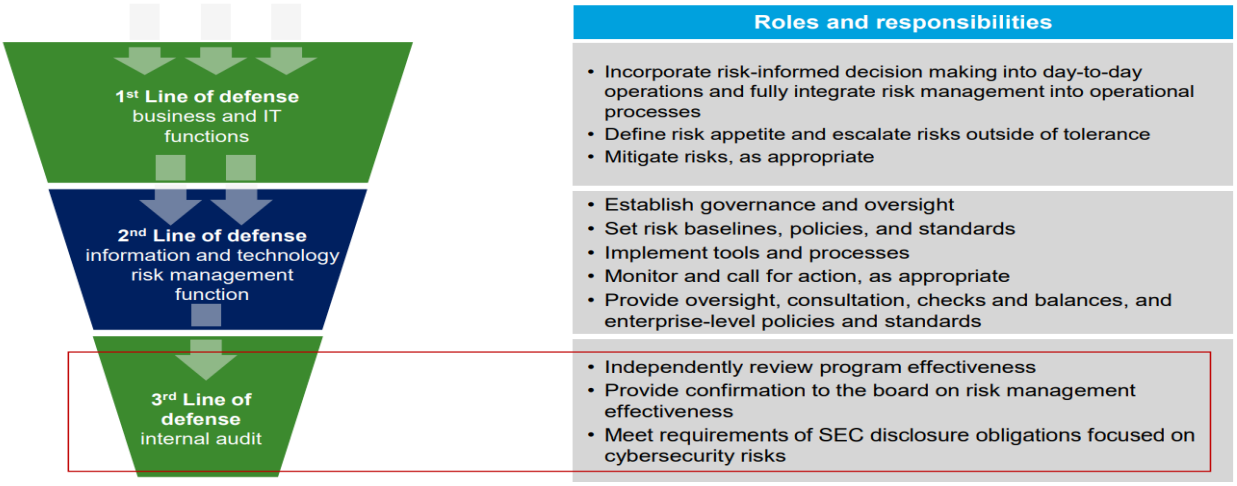
출처 : OWASP Top 10 - 2017

사이버보안 내부심사 수립 가이드라인

사이버보안 내부심사의 정의

사이버보안의 최대 위협은 내부 직원 또는 공급업체일 수도 있다. 내부자(직원, 공급업체, 또는 회사의 컴퓨터 시스템에 합법적으로 연결되는 다른회사들)가 개입된 사이버 공격은 치명적이며, 계속 늘어나는 추세이다. 이는 전체 사이버 공격의 20% 이상을 차지한다. 널리 사용되는 기존의 안전장치는 이를 막는데 효과가 없다.

내부자 공격에 대한 취약성을 줄이려면 기업들은 품질과 안전처럼 사이버 보안도 업무의 우선순위로 만들어야 한다. 즉 모든 직원이 보안도 업무의 일부라고 생각하게 해야한다. 의심스러운 활동이 감지되면 신고할 수 있도록 직원들을 엄격하게 모니터링하고 그들에게 어떤 위협들이 가해질 수 있는지 알려줘야 한다. 공급업체와 총판들에게 위험을 최소화 하도록 요구하고 정기적으로 감사를 실시해야 한다. 리더들은 회사의 주요 자산을 보호하기 위해 IT부서와 긴밀하게 협력해야 한다.



출처 : Deloitte, Cybersecurity The role of Internal Audit

한국선급 해상 사이버보안 인증 검사항목(CS1)

실태점검 실시(219.1) : 회사는 반기 별로 보안 실태점검을 실시하여야 한다.

위반사항 보고(219.2) : 사이버보안 정책 위반사항이 사이버보안 내부 심사 절차에 따라 보고되어야 한다.

사이버보안 내부심사 체크리스트

HUMAN SECURITY	Yes	No
1. Do visitors to the company wear security badges?		
2. Do you have a process for effectively cutting off access to facilities and information systems when an employee/ contractor terminates employment?		
3. Do you have policies addressing background checks for employees and contractors?		
4. Has a cyber security training list been established?		
5. Has there been any disciplinary action taken for cyber security breaches?		
PHYSICAL SECURITY	**Yes**	**No**
6. Do policies and procedures specify the methods used to control physical access to your secure areas, such as door locks, access control systems, security officers, or video monitoring?		
7. Is access to the computing area controlled (single point, reception or security)?		
8. Are visitors escorted in and out of controlled areas?		
9. Are your PCs inaccessible to unauthorized users (e.g. located away from public areas)?		
10. Is your computing area and equipment physically secured?		
ACCOUNT AND PASSWORD MANAGEMENT	**Yes**	**No**
11. Do policies and standards cover electronic authentication, authorisation, and access control of personnel and resources to company information systems, applications and data?		
12. Are controls in place to ensure only authorised personnel have access to company computers?		
13. Are controls in place to enforce appropriate passwords?		
14. Are passwords secure (not easy to guess, regularly changed, no use of temporary or default passwords)?		
DISASTER RECOVERY	**Yes**	**No**
15. Is there a business continuity plan?		
16. Is there a process for creating retrievable back up and archival copies of critical information?		
17. Do you have an emergency/incident management communications plan?		
18. Is there a procedure for notifying authorities in the case of a disaster or security incident?		
19. Does the procedure identify who should be contacted, including contact information?		
COMPLIANCE & AUDIT	**Yes**	**No**
20. Are security documents, such as: policies, standards, procedures, and guidelines, reviewed and updated on a regular basis?		
21. Do you audit the processes and procedures for compliance with established policies and standards?		
22. Are employees aware to keep their passwords secure?		
23. Are employees able to identify and protect classified data, including paper documents, removable media, and electronic documents?		
24. Does the awareness and training teach proper methods for managing personal private information?		
25. Do you test your disaster plans on a regular basis?		

용어 설명

SQL 인젝션(SQL Injection)

WEB 어플리케이션 뒤에 있는 Database에 질의(쿼리)를 하는 과정 사이에 일반적인 값 외에 악의적인 의도를 갖는 구문을 함께 삽입하여 공격자가 원하는 SQL 쿼리문을 실행하는 대표적인 WEB 해킹기법이다.

디렉토리 리스팅(Directory Listing)

취약한 서버설정으로 발생하는 취약점으로 파일 저장 및 열람이 WEB에서 보여진다. 백업파일 및 소스코드, 스크립트 파일의 유출로 인한 계정정보 유출과 다양한 정보를 공격자에게 제공하게 됨으로 제2, 제3의 공격에 이용될 수도 있다.

에러페이지 클로킹(Error page Clocking)

서버와 에러 페이지 설정을 통해서 웹 어플리케이션에서 클리어언트 측 에러와 서버측 에러 또는 디버깅 에러가 발생할때, 서버 설정 정보 및 민감한 데이터 등의 불필요한 정보가 외부 사용자에게 노출 되는 것을 방지 할 수 있다.