KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 017

September 2019

아태지역 e-Navigation Underway 2019 참석

한국선급은 9월 2일~3일 한국에서 개최된 e-Navigation Underway Asia-Pacific 2019에 참석하여 해상 사이버보안의 국제 정책 동향 및 기술개발 현황을 모니터링 하였다.

이번 컨퍼런스는 아태지역의 'e-Navigation 이행 : 새로운 디지털 해사서비스' 라는 주제를 가지고 항해 및 통신의 혁신, 사이버보안, 자율운항선박, 스마트 해상물류체계, 해양 디지털 정보통신 서비스 국제플랫폼 등 해양분야 4차 산업혁명과 관련된 핵심기술들이 논의 되었다. [세션 4]에서 해사분야 사이버보안에 대한 발표가 이루어 졌으며, 기술동향과 정책동향이 소개되었다.

특히, 덴마크 해사청에서 해상부분의 사이버 위협을 예방하기 위한 전략을 소개하였다. 덴마트 해사청은 사이버보안 대응을 위한 부서를 설립하였고, 덴마크 정부차원의 사이버보안 중장기 로드맵을 발표하였다.

향후 선박 사이버보안을 위해서는 해사업계의 다양한 이해관계자(항만, 선주, 선급, 조선소, 제조업체, 서비스업체 등)의 책임과 역할이 명확히 식별 되어야 하며, 덴마크와 같이 각 국가차원에서 해사업계의 전략수립이 필요 할 것으로 예상된다.

출처 : https://www.e-navap.org/cop/bbs/selectENUWinfo.do?cttDiv=ENUWA_000000003&siteId=1

구 분	주요 내용
세션1	디지털 해사서비스의 개발 및 제공 (좌장: Michael Bergmann / PortCDM)
세션2	2-1. 해상통신 및 항해의 혁신 (좌장: Nick Lemom / AMSA) 2-2.. 해상통신 및 항해의 혁신 (좌장: Jon-Leon Ervik / NCA)
세션3	이네비게이션 역량강화 및 국제협력 (좌장: Javier Yasnikouski / IMO)
세션4	해사분야의 사이버 보안 (좌장: Tomas Christensen / MCP Consortium)
세션5	차기 이내비게이션 토론 방향 및 계획 (좌장: Omar Eriksson /IALA)
세션6	종합토론 및 콘퍼런스 결과 채택 (좌장: 홍순배 팀장 / 해양수산부)

태국 VL Enterprise PLC 선사에 사이버보안 맞춤형 교육 실시

한국선급은 지난 9월 19일, 태국 VL Enterprise PLC 선사에 OCIMF TMSA (탱커선 화주검사) 및 ISM 코드 대응을 위한 사이버보안 맞춤형 교육을 실시하였다. 본 '해사 사이버보안 인식제고 교육'은 선사 사이버보안 체계 구축을 위한 관리적보안, 물리적보안, 기술적보안 관련 주요사항 및 리스크평가 이해 과정으로 구성되었으며 임직원들이 해사 사이버보안 이슈에 대응할 수 있도록 가이드라인을 제공하여 교육 만족도 조사에서 큰 호평을 받았다.

한편, 정보통신기술(ICT)이 해사업계에 적용되면서 사이버 위협과 취약성이 증가하고 있어 선사 및 선박 사이버보안에 대한 중요성이 점점 더 강화되고 있다. 국제해사기구(IMO)는 ISM 코드 내 안전관리시스템(SMS)에서 사이버 리스크 통합·관리에 관한 MSC.428(98) 결의안을 채택하여 2021년부터 발효될 예정이며, 해운업계 역시 화주검사(OCIMF TMSA/SIRE)에 사이버보안 항목을 요구하고 있다. 따라서 이러한 국제 사이버보안 요구사항에 대응하기 위해서는 임직원 '사이버보안 인식제고 교육'이 반드시 필요할 것으로 예상된다.

한국선급은 그 동안 SONGA 선사와 산쇼코리아㈜에 맞춤형 사이버보안 교육을 실시하여 TMSA 수검 및 선사 사이버보안 체계구축을 지원한 바 있다. 한국선급은 향후 해사 사이버보안에 대한 선사와 조선소, 기자재업체를 대상으로하는 사이버보안 맞춤형 교육 서비스를 강화해 나갈 방침이다.

Maritime Cyber Security Awareness Training

19-Sep. at Bangkok, V.L. Enterprise PLC.

Course Introduction and Time Table

Trainer: Jeoungkyu Lim(Korean Register)
Sanghoon Choi(Korean Register)

1 Course Introduction

As the Information and Communication Technology (ICT) applied to shipping industry, cyber threats and vulnerabilities related to digitalization, integration and automation of processes and system in shipping have been emerged. According the IMO Resolution MSC.428(98), administrations to ensure that cyber risks are appropriately addressed in existing safety management systems (as defined in the ISM Code) no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

This one day awareness training course provides the trainees with the knowledge and method to respond to the maritime cyber security issues.

2 Time Table

Time	Category	Details	Trainer
09:00 - 09:50	Maritime cyber security overview	• Introduction • International response in maritime industry • KR cyber security activities	JK Lim
10:00 - 10:50	Administrative security	• Cyber security management system • Maritime cyber security organization • Human security • TMSA Element 13 : Maritime Security	JK Lim
11:00 - 11:50	Cyber Asset / Cyber Threat	• Cyber asset management overview • Identify asset • Asset criticality • Maritime Cyber threat • Threat list	SH Choi
12:00 - 13:00	Lunch Break		
13:00 - 13:50	Physical security	• Purpose and method of physical security • KR Server room physical security • Physical security by risk assessment	JK Lim
14:00 - 14:50	Technical security	• Network security • Vulnerability diagnosis • PC security vulnerability diagnosis	SH Choi
15:00 - 15:50	Understanding of maritime cyber security risk assessment	• Understanding of maritime cyber security and risk assessment • KR cyber security risk process • Application cases	JK Lim
16:00 - 17:00	Workshop	• Hands-on	SH Choi

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 지정되어, 한국선급과 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	

악성 메일 대응 훈련, APT 공격도 막을 수 있다

"의심스라운 이메일은 열어보지 않기", "이메일에 포함된 의심스러운 인터넷 주소는 클릭하지 않기" 등과 같은 이메일과 관련된 내용은 항상 빠짐없이 등장하는 보안 수칙일 것이다. 이는 여전히 많은 사람이 의심스러운 이메일을 열어보고 있으며, 해커와 사이버 범죄자들에게 효과좋은 관문이기 때문이다.

피싱 VS 스피어 피싱

피싱(Phshing)은 전자우편 또는 메신저 등을 사용해서 신뢰할 수 있는 단체 및 기업이 보낸 메시지인것처럼 가장함으로써, 비밀번호 개인정보와 같은 기밀을 필요로 하는 정보를 부정하게 얻으려는 오늘날 대표적인 사기방식(사회 공학기법, Social Engineering)의 한 종류 이다. 특히 과거에는 누가 봐도 수상하고, 뜬금없는 제목의 피싱 메일이 주를 이뤘다면 요즘은 비슷한 발신자 주소로 위장하거나 업무와 관련된 제목으로 위장하는 등 사회적인 이슈를 이용하거나 특정한 공격 대상을 노리는 스피어 피싱까지 끊임없이 진화하고 있다.

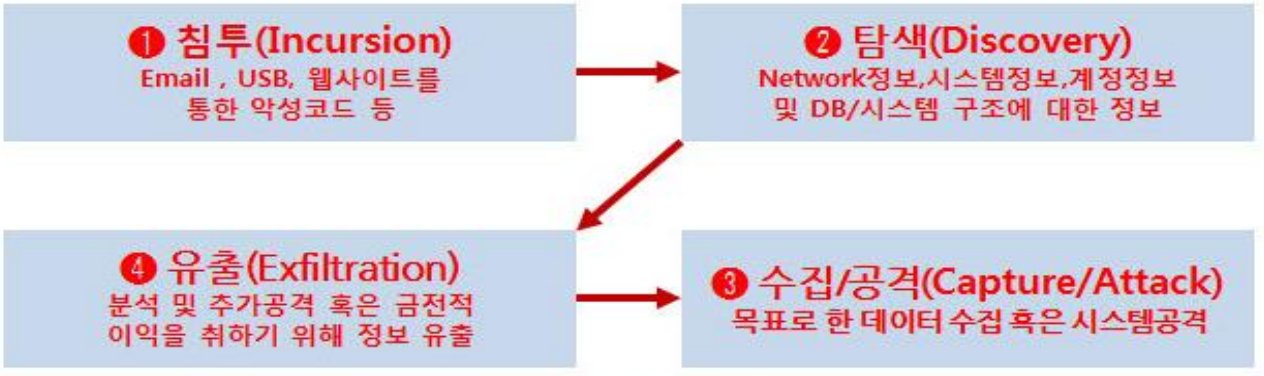
스피어 피싱 메일의 특징

- 불특정 다수가 아닌 특정 기관 및 기업을 노리는 표적성
- 일반적인 광고, 애드워드보다 훨씬 심각한 정보 유출 등을 노리는 악성코드의 심각성
- 내용을 의심할 수 없을 정도로 정상 메일과 유서한 정교성

특히, 해외 통계에 다르면 지금까지 밝혀진 APT(Advanced Persistent Threat) 공격의 90% 이상은 악성 메일부터 시작되거나 공격에 사용되었다고 한다.

출처 : https://blog.lgcns.com/2064?category=604440

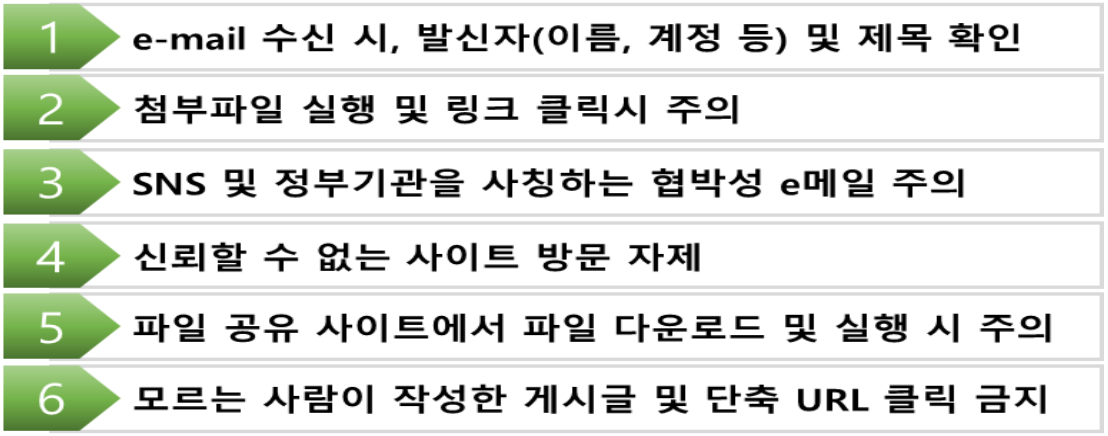
APT 공격의 단계



스피어 피싱 메일은 정말 예방 할 수 없는 것인가?

해커가 특정 조직 또는 인물을 표적으로 삼으면 해커는 관련자를 사칭하거나 상대의 관심과 호기심을 자극하는 사회 공학적(Social Engineering) 기법으로 이에 맞춤화된 내용의 스피어 피싱 메일을 시도한다. 이런 정교하게 조작된 메일을 받았을 때 개인이 이를 구별해 내기란 쉽지 않다.

이는, 스피어 피싱메일은 보안 솔루션의 탐지를 피하고자, 실행 파일 형태에서 문서 형태의 비실행 파일 형태로 등의 사용자 PC에 악성코드를 전파하기 위해 끊임없이 진화하고 있다. 또한 조직 구성원을 대상으로 하는 공격이기 때문에, 내부직원을 대상으로 하는 정기적 보안 교육이 가장 효과적이다. 즉, 스피어 피싱 메일 공격 위협에 대한 인식 제고와 회사 내부직원의 관심과 노력으로도 스피어 피싱 메일의 피해를 예방하는 데 상당한 효과를 거둘 수 있는 가장 좋은 방어 대책인 것이다.



출처 : https://blog.lgcns.com/2064?category=604440

효과적인 악성 메일 대응훈련을 위해서는 사고 예방 중심으로 조직의 보안 의식을 향상시키는데 초점을 두고, 전사적으로 기업의 내·외부 환경을 고려해 수행해야 하며, 훈련에 다른 평가결과는 다음의 훈련에 반영되어 지속적으로 수행해야 할 것이다.

구 분	예·방탐지
훈련 계획	· 훈련목적, 일정 수립 및 훈련대상자 선정 · 최근 악성메일 사례, 기업의 ·내외부환경, 훈련 대상자를 고려해 시나리오 작성 · 평가 항목 선정9열람, 입력, 실행, 보안팀 신고여부 등)
훈련 수행	· 악성 메일 훈련 전, 훈련환경(보안 장비 차단, PC 등) 점검 수행 · 훈련 대상자의 행위 추적을 통한 유의사항 안내 · 훈련 통계 및 보고서 작성
훈련 평가	· 평가 항목 및 등급에 따른 훈련 평가 · 후속 조치 대상자 선정 및 정보보안 교육 수행
개선 계획	· 평가 결과에 따른 개선 계획 반영(교육, 절차·지침 보완 등) · 평가 결과를 후속 시나리오에 반영

출처 : https://blog.lgcns.com/2064?category=604440

[기획시리즈]②

5G의 네트워크 구조와 사이버 위협

본 기획시리즈는 4차산업혁명과 관련한 핵심 통신인프라인 5G가 해양산업에 미칠 긍정적 파급효과와 이에 따른 사이버 위협에 대해 다뤄보고자 한다. 따라서 본 뉴스레터 2019년 9월호에서는 ***'5G 네트워크 구조와 네트워크 슬리이싱 기술***에 대해 소개한다.

기획시리즈 순서

① 5G란 무엇인가?

② 5G의 네트워크 구조와 네트워크 슬라이싱(Network Slicing) 기술, 그리고 해양산업 변화

③ LTE의 중앙집중형 네트워크와 5G의 분산형 네트워크의 비교

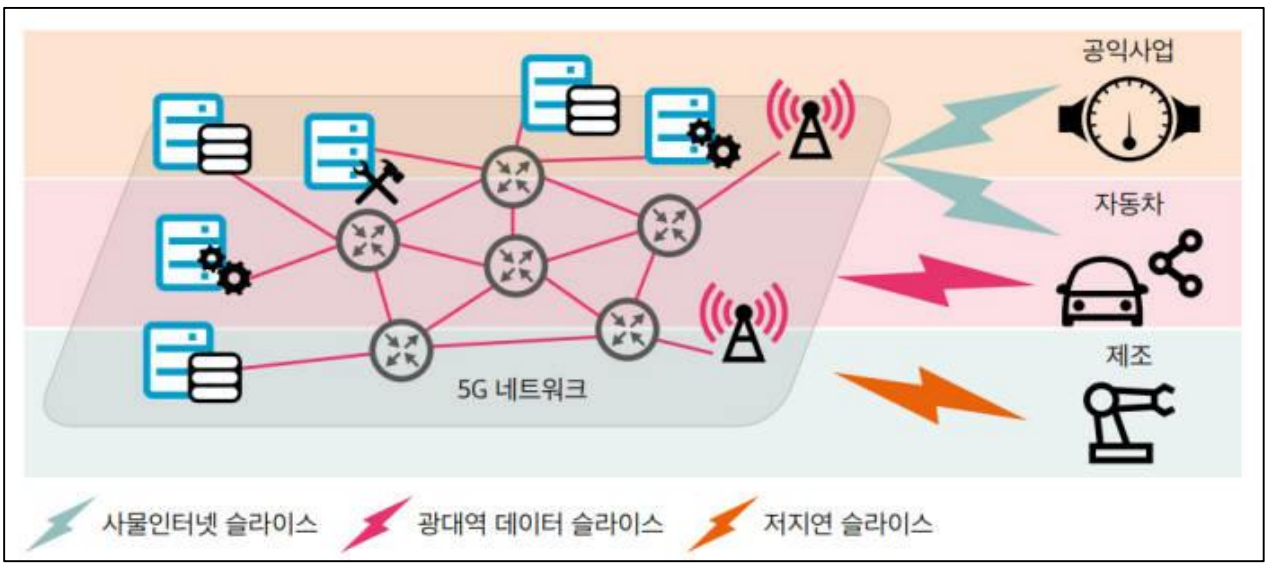
④ 5G 표준에서 무선백홀 기술과 5G 위성의 역할

⑤ 선박과 항만에 효과적으로 활용하기 위한 5G 표준의 Private Network 참조모델

5G 네트워크 구조와 네트워크 슬라이싱(Network Slicing) 기술

5G의 네트워크 구조는 8월 뉴스레터에서 설명한 바와 같이 5G는 기본적으로 각 산업의 요구사항을 기반으로하는 서비스 기반 구조(Service-Based Architecture)를 가진다. 또한, CP/UP(Control Plane/User Plane) 기능의 분리와 NF(Network Function) 모듈화 등이 주요 특징이다. 이러한 5G 네트워크 구조의 장점은 선박, IoT 기기, 자동차, 공장 등 각각의 서비스가 요구하는 네트워크 기능을 모듈화 하여 최적화된 네트워크로 가상화 시킬 수 있다.

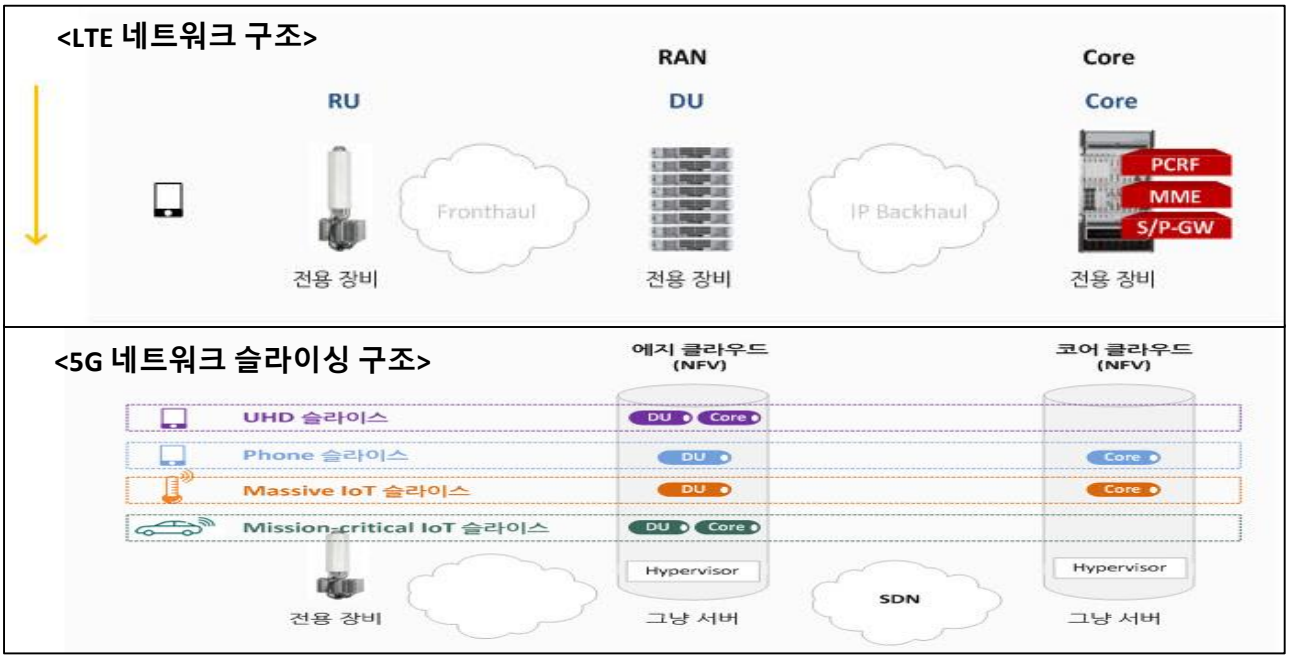
이렇게 하나의 Physical Network를 다수의 Logical Network로 분할하여 서비스 그룹별로 통신성능을 보장하도록 가상의 전용 네트워크 기술을 네트워크 슬라이싱 기술이라 한다.



출처 : https://blog.naver.com/tech-plus/221207863455

5G 네트워크 구조와 네트워크 슬라이싱(Network Slicing) 기술(Continue Page)

즉, HDD를 C와 D로 파티셔닝해서 쓰는 것처럼 네트워크를 가상화하여 서로 다른 특성을 갖는 다양한 서비스들에 대해 그 서비스에 특화된 전용 네트워크를 제공해주는 것이다. 예컨대 자율주행차와 관련된 네트워크는 도로 위에서 발생하는 위험에 즉각적으로 반응하기 위해 1ms(0.001초)의 초저지연 성능이 가장 중요하다. 반면 스마트 시티와 관련된 상수도 회사는 속도는 다소 느리더라도 수천 개 장치에서 소량 데이터를 동시에 전송할 수 있는 초대용량 연결 성능이 중요하다. 그럼 5G 폰망, 5G Massive IoT망, 5G mission-critical IoT망을 따로 만드는 것인가? 그렇지 않고 하나의 물리적인 망상에 여러 개의 논리적인 망을 만들어 비용을 절감해주는 것이 네트워크 슬라이싱 기술이다.



출처 : https://www.netmanias.com/ko/post/blog/8292/5g-data-center-iot-network-slicing-sdn-nfv/5g-and-e2e-network-slicing

5G가 해양산업에 미치는 영향은 무엇일까?

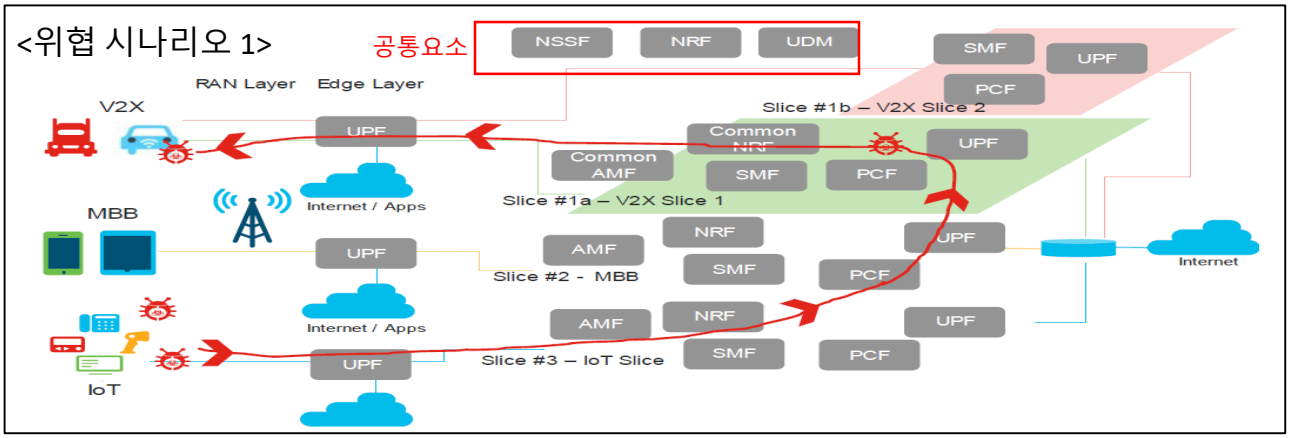
2019년 6월, 국제해사기구(IMO) 해사안전위원회 101차 회의(MSC 101)에서 자율운항선박(MASS, Maritime Autonomous Surface Ship)의 시험운항 임시지침이 승인되었다. 해양산업도 자율운항선박, 스마트 항만, 스마트 해운물류 등 기존 해양관련 산업들의 자동화, 스마트화를 위한 연구가 전 세계적으로 진행되고 있다. 이러한 기존 해양산업과 서비스들의 스마트화를 위해서는 통신 인프라의 개발 및 구축이 핵심요소 중 하나이며, 이에 5G를 적용하기 위한 국제표준화 연구도 진행되고 있다. 5G 국제표준화는 3GPP(3rd Generation Partnership Project)에서 이루어 지고 있다. 즉, 5G 네트워크 슬라이싱 구조에서 해상환경에 특화된 Maritime 슬라이스의 요구사항을 정의하고, 기술개발이 이루어진다면, 해양산업도 스마트화를 위한 상용기술과 솔루션들이 출현될 것으로 기대된다.

5G의 사이버보안 위험요소 - 5G 네트워크 슬라이싱 구조의 보안위협요소

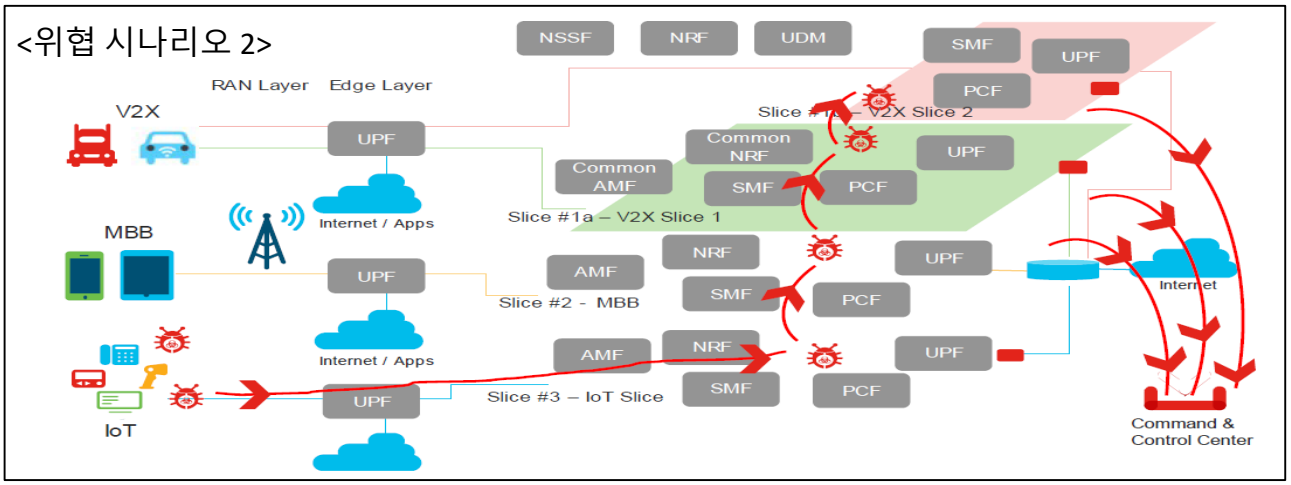
5G 네트워크 슬라이싱 구조에서 아래 그림의 NSSF(Network Slice Selection Function)와 같은 모든 슬라이스간에 공유되는 공통 리소스와 구성요소가 있다. 나머지 슬라이스들은 특정 슬라이스에 맞게 전용기능인 AMF, SMF, PCF 레이어와 같은 개별 리소스를 할당 한다.

이 때, 네트워크 슬라이스 간 부적절한 격리 또는 동일한 구성요소 간 부적절한 격리로 인해 위협이 발생할 수 있다. 예를 들어, IoT 슬라이스에서 IoT 기기의 취약성을 이용하여 일부 IoT가 맬웨어에 감염될 경우, 그 위협이 다른 슬라이스로 전이되어 결과적으로 중요한 슬라이스인 자율주항차 서비스에도 영향을 줄 수 있는것이다.

<위협 시나리오 1>에서 공격자는 여러 슬라이스에 공통적 인 리소스를 소모하여 다른 슬라이스에서도 서비스 거부 또는 서비스 저하를 일으킬 수 있다.



<위협 시나리오 2>에서 슬라이스와 슬라이스 간 적절한 격리가 되지 않을 경우 공격자는 감염된 장치 또는 다른 슬라이스의 엔드 포인트를 사용하여 다른 슬라이스 구성요소에 접근 할 수 있다. 궁극적으로 다른 슬라이스가 노출되어 데이터 유출이 제어센터로 진행 될 수 있다. 공격자가 방화벽 뒤에 있는 모든 네트워크 정보를 수집하면 유출된 정보를 기반으로 가입자를 공격할 수 있고, 침입자는 사기성 금융이익을 위해 정보를 이용할 수 있다.



출처 : The Evolution of Security in 5G, 5G America white paper, July 2019

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 **'A8 : 2017 – 안전하지 않은 역직렬화'** 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]

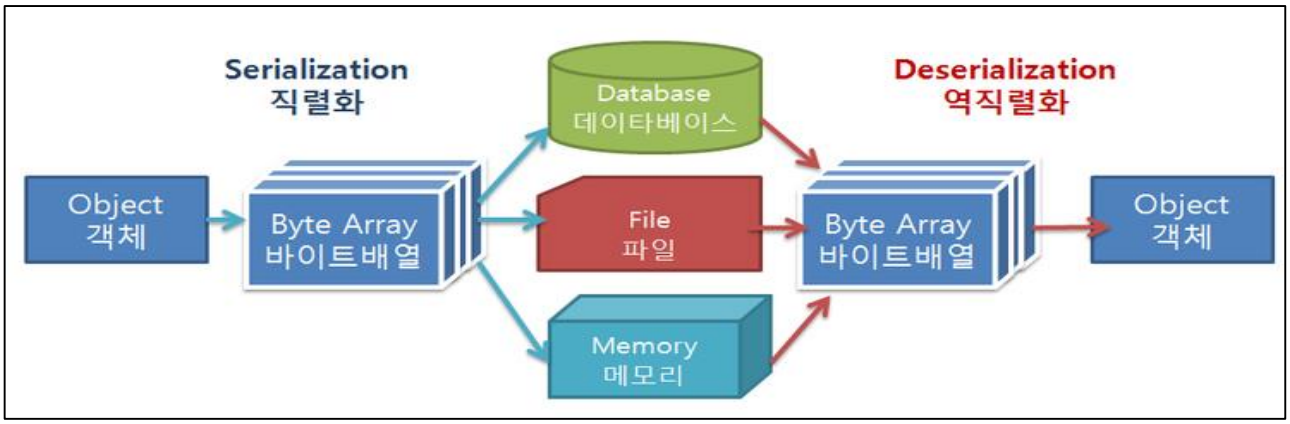
출처 : OWASP Top 10 Project

OWASP 10대 위협 'A8 : 2017 - 안전하지 않은 역직렬화'

직렬화(Serialization)란 객체(Object)를 10100011 처럼 8비트 2진 숫자의 조합인 바이트(Byte) 배열로 변환을 해서 파일이나, 메모리, 데이터베이스 등이 저장을 하는 과정을 말한다. 반대로 역직렬화(Deserialization)란 저장된 것을 다시 객체로 변환하는 과정이다.

애플리케이션에서 신뢰할 수 없는 사용자의 입력을 파싱 하는 것이 기존까지 주요 보안 취약점이 만들어지는 원리였다. 역직렬화도 이와 크게 다르지 않다. 해커가 악의적으로 위조한 직렬화된 입력을 애플리케이션이 처리하도록 할 수 있기 때문이다.

Java에서 Object Deserialization을 이용한 원격코드 실행하는 공격이 잘 알려진 취약점 이다. Serialization/Deserialization 원리를 바탕으로 TCP/IP 프로토콜을 통해 공격자가 서버에 원격 코드를 실행하는 공격을 말하며, 공격자는 서버에 실행할 명령어를 Serialization하여 바이트 단위로 변환하여 전송하고, 이를 서버에서 입력받아 Deserialization으로 복원하여 입력 받은 명령어가 실행되도록 하는 취약점이다.



출처 : https://blog.naver.com/kkson50/220564174258

취약점 확인 방법

애플리케이션 및 API가 공격자의 악의적이거나 변조된 객체를 역직렬화하면 취약해질 수 있습니다.

이로 인해 크게 두가지 유형의 공격이 발생할 수 있습니다:

- 객체 및 데이터 구조 관련 공격입니다. 공격자가 애플리케이션 로직을 수정하거나 애플리케이션에 사용 가능한 클래스가 있는 경우 임의의 원격 코드를 실행하여 역직렬화 중이나 이후에 동작을 변경할 수 있습니다.
- 접근 통제 관련 공격과 같이, 기존 데이터 구조가 사용되지만 내용이 변경되는 일반적인 데이터 변조 공격입니다.

직렬화는 다음 용도의 애플리케이션에서 사용될 수 있습니다:

- RPC(Remote-Process Communication)/IPC(Inter-Process Communication)
- 유선 프로토콜, 웹 서비스, 메세지 브로커
- 캐싱/ 지속 연결
- 데이터베이스, 캐시 서버, 파일 시스템
- HTTP 쿠키, HTML 양식 파라미터, API 인증 토큰

보안 대책

신뢰할 수 없는 출처로부터 직렬화된 객체를 허용하지 않거나 원시 데이터 유형만을 허용하는 직렬화 매체를 사용하는 것이 안전한 아키텍처의 유일한 패턴입니다.

그럴 수 없다면 다음 중 하나 이상을 고려하십시오.

- 악성 객체 생성이나 데이터 변조를 방지하기 위해 직렬화된 객체에 대한 디지털 서명과 같은 무결성 검사를 구현합니다.
- 객체 생성 전 코드가 일반적으로 정의할 수 있는 클래스 집합을 기대하므로 역직렬화하는 동안 엄격한 형식 제약 조건을 적용합니다. 이 기법에 대한 우회가 입증되었으므로 여기에 의존하는 것은 바람직하지 않습니다.
- 가능하다면 낮은 권한 환경에서 역직렬화하는 코드를 분리하여 실행합니다.
- 예상하지 않은 형식이 들어올 경우나 역직렬화가 예외를 생성할 경우 등 예외나 실패에 대한 로그를 남깁니다.
- 역직렬화하는 컨테이너 또는 서버에서 들어오고 나가는 네트워크 연결을 제한하거나 모니터링 합니다.
- 역직렬화를 모니터링하여 사용자가 역직렬화를 지속적으로 할 경우에 경고합니다.

출처 : OWASP Top 10 - 2017

KR 해상 사이버보안 형식승인 지침의 이해

사이버보안 형식승인 지침 이해하기

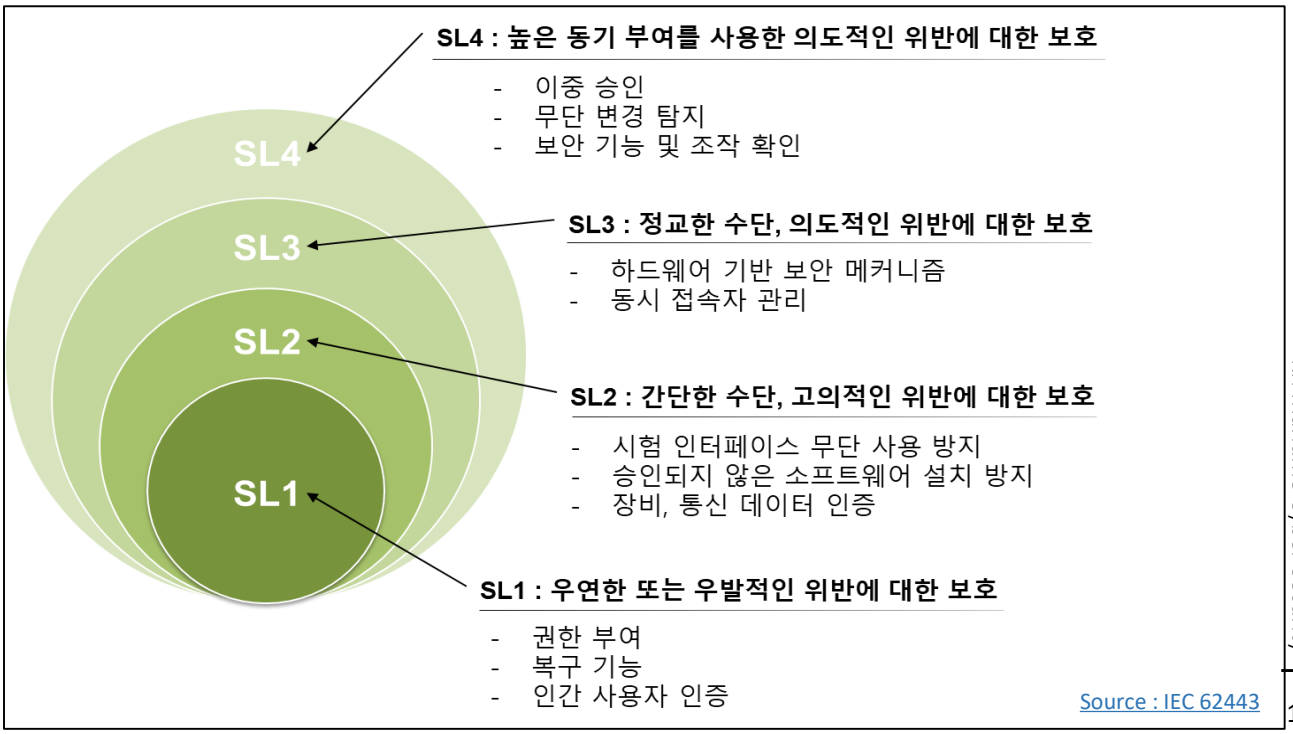
형식승인이란, 선박에 설치하기 전에 제품의 각 형식마다 미리 자료심사 및 승인시험을 하고 만족할 경우 제품이 규정에 적합하다는 것을 제조자에 대해서 증명하는 것을 의미한다. 사이버보안 형식승인은 ISA 62443 4-2, IEC 61162-460과 같은 국제표준을 기반으로 개발되었으며 선박에 탑재되는 원격 접속 장비, 통합 제어 및 모니터링 시스템 등을 포함하는 사이버 시스템의 사이버보안 수준 및 그 수준에 해당하는 요건을 12개의 범주 및 총 124개 항목의 요구 사항에 대한 검증을 통해 보안 기능과 그 수준을 확인한다.

<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

권한 부여 시행(301)

1. 구성품은 사용자에 대하여 권한 부여 시행 메커니즘을 제공하여야 한다.(SL1)
2. 모든 사용자들에게 권한 부여 시행 메커니즘을 제공하여야 한다.(SL2)
3. 사용자들의 역할에 대한 매핑을 정의하고 수정할 수 있는 역할을 제공하여야 한다.(SL2)
4. 일련의 이벤트에 대하여 관리자 수동 오버라이드를 지원하여야 한다.(SL3)
5. 산업 프로세스에 심각한 영향을 미칠 수 있는 경우 이중 승인을 지원하여야 한다.(SL4)

권한 부여의 필요성

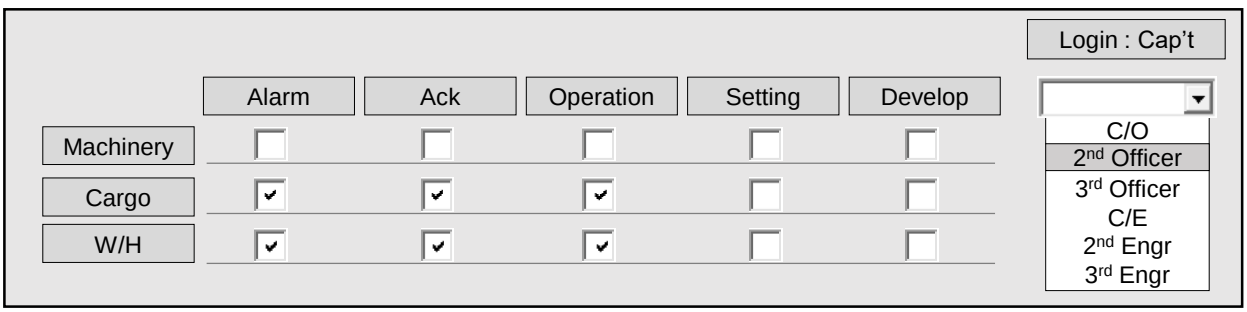
권한 부여의 주요 목적은 무단 작업을 방지하는 것이다. 작업의 예로는 데이터 읽기, 쓰기, 프로그램 다운로드 및 구성 설정이 있다(출처 IEC 62443-4-2). 선박에 탑재되는 장비들의 특성상 안전을 위해 허가된 사용자에게만 제한적으로 기능이 사용되어져야 한다. 하지만 위험 상황에서 비상조치를 위해서 특정 기능을 제한적으로 열어주어야 할 경우도 있다.

'SL 1'에서는 사용자별로 권한을 부여할 수 있는 기능을 요구한다. 이를 통해 일부 작업은 인가받지 않은 사용자는 사용할 수 없도록 하여 무단 작업을 방지한다.

'SL 2'에서는 모든 사용자들에게 권한 부여를 시행하며 역할을 정의하고 수정할 수 있는 기능을 요구한다. 권한은 그룹으로 관리 될 수 있으나 SL2를 만족하기 위해서는 모든 사용자가 하나 이상의 그룹에 매핑 될 수 있도록 하여야 한다. 또한 역할을 변경 및 관리할 수 있는 기능을 제공하여야 한다.

'SL 3'에서는 오버라이드 기능을 요구한다. 오버라이드의 사전적 의미는 '무시하다 혹은 무효로 하다' 로 정의된다. 선박의 장비들은 안전을 위해 많은 기능들이 제공되며, 일반적인 조건에서는 허용되지 않아야 할 권한이 위험 상황에서는 허용되어야 할 수 있으며 제조자는 이를 사전에 정의하고 사용자가 알 수 있도록 하여야 한다.

'SL 4'에서는 오버라이드와 반대되는 개념인 이중 승인을 요구한다. 이중 승인은 작업을 수행하기 위해 두번의 승인이 필요함을 의미한다. 다만 이중 승인은 안전시스템과 같은 즉각적인 대응이 필요한 경우에는 적용되지 않아야 한다.



[씨드젠] 중소기업 정보보안 컨설팅 지원사업 소개

중소기업 대상

정보보호 컨설팅 및 솔루션 구입비용 지원 안내

목적

정보보호에 관심과 의지는 있지만 적용에 어려움을 느끼는 중소기업 대상 법률 준수, 관리·물리· 기술 취약점 진단 등 전사적 맞춤형 컨설팅 지원할 뿐만 아니라 발견된 취약점 조치를 위한 솔루션 구입비용도 원스톱으로 지원하여 수혜기업의 보안수준 강화

신청 대상

- **중소기업법 제2조에 해당하는 기업 중**
  - 소규모의 ICT시설을 보유한 **중소기업 중 정보보호 활동 의지가 있는 기업**
  - ICT인프라 및 서비스를 운영중인 **중소기업 중 고수준의 정보보호 컨설팅이 필요한 기업**

※ 250개 기업 선착순 모집

※본 사업은 컨설팅부터 결과조치를 위한 솔루션 도입까지 완료할 업체만을 선정하며, 솔루션 도입시 정부지원금 외 일부 업체 부담금이 발생함

신청 방법

- http://smb.isconsulting.kr 접속 ▶ 메인화면 컨설팅 신청서 다운 ▶ 작성 후 이메일 전송

담당자	이메일	전화번호
모집담당자 (씨드젠)	SMB.consult@krcert.or.kr	02-405-6696

신청 기한

- 6월 14일 ~ 10월 31일

지원 내용

- 컨설팅 지원

구분	기간	컨설팅 지원
약식 컨설팅	약 1일	체크리스트 기반의 정보보호 컨설팅 지원
종합 컨설팅	약 3~5일	전사적인(관리적·물리적·기술적)보안 종합 컨설팅

- 솔루션 구매비용 지원 (매칭형태로 지원)

보안 솔루션 — 정부지원금 최대 300만원

SECaaS — 정부지원금 최대 180만원

※ SECaaS : 클라우드 형태로 제공되는 보안 서비스

상세 진행 절차

대상 선정 → 맞춤형 컨설팅 수행 → 결과 보고 → 솔루션 매칭 지원

단계	상세 내용
대상 선정	• 기업 규모, ICT시설 보유여부 등 본 사업 지원 적격 심사 수행
컨설팅수행 (약식, 종합)	• 사전 컨설팅 질의문 배포 회신 • 맞춤형 정보보호 컨설팅 수행
결과 보고	• 컨설팅 결과 보고 및 발견된 개선사항 조치 지원
솔루션 매칭 지원	• 적합 솔루션 및 SECaas 매칭 • 선정 솔루션·SECaas 도입 및 운영 지원

※본 사업은 컨설팅 후속조치를 위한 솔루션 도입시 업체 부담금이 발생하며, 이를 원치 않는 기업은 신청이 불가함

용어 설명

피싱(Phishing)

전자우편 또는 메신저를 사용하여 신뢰할 수 있는 기업이 보낸 메시지인 것처럼 가장함으로써, 비밀번호 및 신용카드 정보와 같이 기밀을 필요하는 정보를 부정하게 얻으려는 사회공학 기법(Social Engineering)의 한 종류이다.

스피어 피싱(Spear Phishing)

신뢰할 만한 발신인이 보낸 것처럼 위장한 기존의 피싱 공격과 동일하지만, 특정인 또는 특정 조직을 대상으로 시도하는 피싱이다.

오버라이드

어떠한 2가지 시스템이 존자핼 때, 하나의 시스템이 다른 시스템을 우선시 하도록 설계된 소프트웨어 용어이다. 주로 비상상황에서 안전시스템의 우선권을 주기위해 사용되는 개념이다.

5G 표준 관련 용어

- CP : Control Plane
- UP : User Plane
- NF : Network Function
- 3GPP : 3rd Generation Partnership Project,
- NSSF : Network Slice Selection Function
- AMF : Access and Mobility Management Function
- SMF : Session Management Function
- V2X : Vehicle-to-Everything
- MBB : Mobile Broadband
- IoT : Internet of Things