KR Maritime Cyber Safety News & Report

Vol. 056
Dec. 2022

Korean Register
www.krs.co.kr

CONTENTS

- 알림사항 -

내부 사정상 2023년부터 KR 해상 사이버안전 뉴스 및 보고서는
분기별로 발행될 예정이오니 구독자분들의 양해를 부탁드립니다.

알리안츠: 2022 사이버 위험 동향

Source : SAFETY4SEA

Allianz Global Corporate & Specialty (AGCS)의 새로운 보고서에 따르면 비즈니스 이메일 손상 사고가 증가하고 있는 반면에 랜섬웨어는 전세계적으로 기관들의 가장 큰 사이버 위험으로 남아 있으며, '딥페이크'시대에는 더욱 증가 할 것이라고 말합니다.

동시에 우크라이나 전쟁과 광범위한 지정학적 긴장은 적대 행위가 사이버 공간으로 확산되어 기업, 인프라 또는 공급망에 대한 표적 공격을 유발할 수 있기 때문에 주요 관심사입니다.

사이버 위험 환경에 대한 보험사의 연례 검토는 또한 클라우드 서비스에 대한 의존도 증가, 더 높은 보상 및 처벌을 의미하는 진화하는 제3자 책임 환경, 사이버 보안 전문가 부족의 영향으로 인해 발생하는 새로운 위협을 강조하고 있습니다.

이러한 잠재적 취약성은 오늘날 글로벌 투자자를 포함하여 그 어느 때보다 많은 당사자가 기업의 사이버보안 복원력을 면밀히 조사하고 있음을 의미하며, 이는 많은 기업들이 이를 주요 환경, 사회 및 거버넌스(ESG) 위험 문제로 꼽고 있음을 보고서는 지적합니다.

AGCS의 사이버 글로벌 책임자이자 사이버 역량 센터의 그룹 책임자인 스콧 세이스는 말합니다.

"사이버 위험 환경은 월계관에 안주하는 것을 허용하지 않습니다. 랜섬웨어 및 피싱 사기는 그 어느 때보다 활발하며 하이브리드 사이버 전쟁의 잠재성이 있습니다."

전세계적으로 랜섬웨어 공격의 빈도는 여전히 높으며 관련 청구 비용도 마찬가지입니다. 2021년에는 6억 2,300만 건의 공격이 기록되었으며 이는 2020년의 두 배에 달합니다.

2022년 상반기 동안 전세계적으로 빈도가 23% 감소했지만 연간 누계 총계는 여전히 2017, 2018 및 2019년 전체 연도를 초과하는 반면 유럽에서는 이 기간 동안 공격이 급증했습니다.

랜섬웨어는 2023년까지 전세계 기관 및 단체들에 300억 달러의 피해를 줄 것으로 예상됩니다. AGCS 관점에서 다른 보험사와 함께 관련된 랜섬웨어 피해 청구 비용은 2020년 및 2021년 동안 모든 사이버 청구 비용의 50% 이상을 차지했습니다.

"범죄자들이 대기업, 중요 인프라 및 공급망을 표적으로 삼으면서 랜섬웨어 공격 비용이 증가했습니다. 범죄자들은 더 많은 돈을 갈취하기 위해 전술을 연마했습니다."라고 세이스는 설명합니다.

"이중 및 삼중 갈취 공격은 이제 표준이 되었습니다 – 시스템 암호화 이외에도 민감한 데이터는 점점 더 유출되고 있으며, 비즈니스 파트너, 공급업체 또는 고객에 대한 갈취 요구의 지렛대로 사용됩니다. "

랜섬웨어의 심각성은 갱단의 정교함과 인플레이션 상승으로 인해 기업에 대한 주요 위협으로 남을 가능성이 높으며, 이는 IT 및 사이버 보안 전문가의 비용 증가에 반영됩니다.

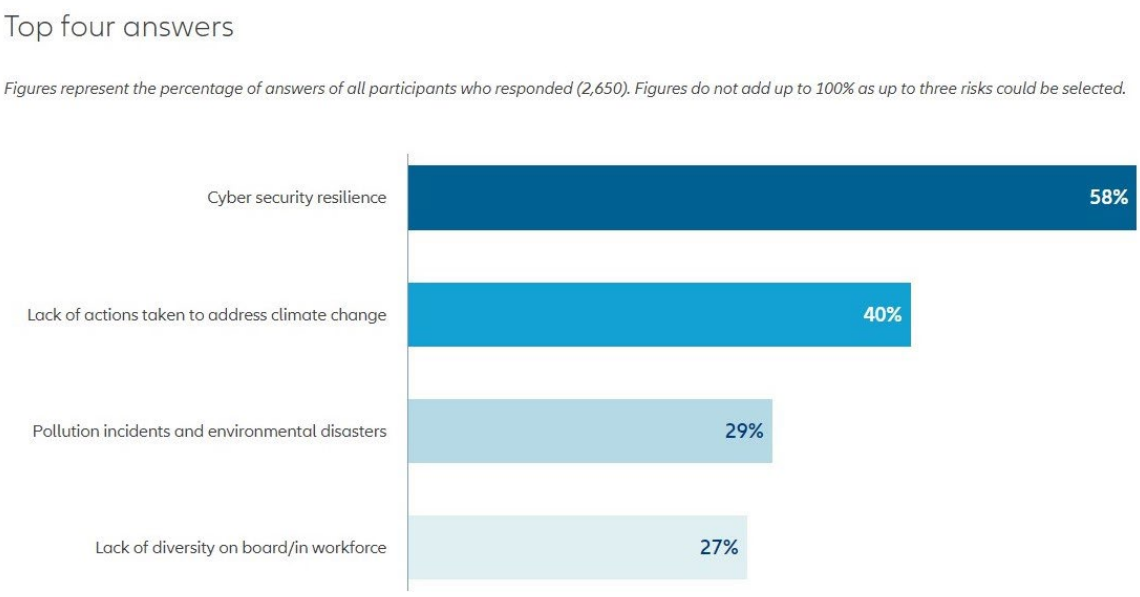
대기업들이 보안에 더 많이 투자함에 따라 사이버 보안에 대한 통제와 재원이 부족한 중소기업들이 갱단의 표적이 되고 있습니다. 갱단은 또한 광범위한 공격 기술을 사용하고 있으며 몸값 요구를 특정 회사에 맞게 조정하고 있으며 수익을 극대화하기 위해 전문 협상가를 활용하고 있습니다.

정교한 사기(Sophisticated scams)

비즈니스 이메일 침해(BEC) 공격은 데이터의 디지털화 및 가용성 증가, 원격 근무로의 전환 및 '딥 페이크' 기술 및 가상 회의로 인해 점진적으로 증가하고 있습니다.

FBI에 따르면 BEC 사기 피해액은 2016년부터 2021년까지 전세계적으로 총 430억 달러에 달했으며 2019년 7월과 2021년 12월 사이에만 사기가 65% 급증했습니다. 공격은 더욱 정교해지고 있으며 범죄자들은 이제 가상 회의 플랫폼을 사용하여 직원들을 속여 자금을 이체하거나 민감한 정보를 공유하도록 하고 있습니다.

점점 더 이러한 공격이 고위 경영진을 모방하는 ' 딥 페이크' 오디오 또는 비디오를 가능하게하는 인공 지능에 의해 가능해졌습니다. 작년에 아랍에미리트의 한 은행 직원은 회사의 복제된 목소리에 속아서 3천 5백만 달러를 이체를 했습니다.



사이버 전쟁의 위협

우크라이나 전쟁과 광범위한 지정학적 긴장은 러시아 및 우크라이나와 관련된 기업, 동맹국 및 인접 국가의 기업에 대한 스파이 활동, 사보타주 및 파괴적인 사이버 공격의 위험을 증가시키면서 사이버 위협 환경을 재편하는 주요 요인입니다.

국가가 후원하는 사이버 공격은 잠재적으로 중요 인프라, 공급망 또는 기업을 표적으로 삼을 수도 있습니다.

세이스는 다음과 같이 설명합니다.

"아직 러시아와 우크라이나 간의 전쟁으로 사이버 보험 청구가 눈에 띄게 증가하지는 않았지만 민족 국가로 인한 위험이 잠재적으로 증가할 수 있음을 지적합니다."

전쟁 행위는 일반적으로 전통적인 보험 상품에서 제외되지만 하이브리드 사이버 전쟁의 위험은 전쟁 및 국가 후원 사이버 공격 문제를 문구상에 해결하고 고객에게 명확한 보장을 제공하기 위한 보험 시장의 노력을 가속화했습니다.

AGCS는 '사이버: 변화하는 위협 환경' 보고서에서 여러 동향들을 식별하고 있으며, 다음을 포함하고 있습니다:

- **취약한 공급망에 초점을 맞춘 해커:** 콜로니얼 파이프라인과 같은 중요한 인프라 또는 클라우드 서비스에 대한 공급망 공격은 심각한 위험으로 부상했습니다. 점점 더 많은 랜섬웨어 갱단이 중단 위협을 이용하여 기업이 몸값을 지불하도록 압력을 가하고 있으며, 특히 제조 회사가 취약합니다.
- **클라우드 아웃소싱:** 기업은 보안 및 위험 집계에 대한 우려가 커지고 있음에도 불구하고 서비스와 데이터 저장소를 클라우드로 계속 전환하고 있습니다. 클라우드 서비스 또는 사이버 보안을 위해 소수의 공급자에 의존함으로써 사회는 몇 가지 단일 고장 지점에 더 큰 집중화를 일으키고 있습니다. 아웃소싱 또는 클라우드 공급업체가 사고 발생시 전적인 책임을 진다는 것은 일반적인 오해입니다.
- **벌금 및 처벌을 포함한 제3자 책임**은 기술 발전, 더 많은 정보를 수집하는 조직 및 시행된 데이터 개인 정보 보호 규정과 점점 더 관련성이 높아지고 있습니다. 이중 갈취 랜섬웨어를 포함한 거의 모든 사이버 사고는 소송으로 이어질 수 있으며 영향을 받는 당사자의 보상 요구로 이어질 수 있습니다.
- **전문가 부족**은 사이버 보안을 개선하려는 노력을 방해하고 있습니다. 경영층 사이에서 인식이 높아지고 있지만 전 세계적으로 채워지지 않은 사이버 보안 일자리 수는 지난 8년 동안 350% 증가하여 350만 명으로 추정되며, 이는 많은 기업이 고용에 어려움을 겪고 사이버 보안 태세를 개선하는 능력에 영향을 미친다는 것을 의미합니다.
- **ESG 렌즈를 통해 보여지는 사이버 보안.** 요즘 기업들의 사이버보안 복원력은 과거보다 훨씬 더 많은 이해 관계자 그룹에 의해 면밀히 조사되고 있습니다. 더욱더 사이버 보안 고려 사항이 데이터 공급자의 ESG 위험 분석 프레임워크에 통합되고 있으며, 데이터 제공업체는 사이버 범죄에 대한 준비 상태를 평가하기 위해 기업의 관행을 조사합니다. 회사의 사이버 프로세스와 정책을 경영층 수준에서 이해하고 위험 모니터링 프로세스를 갖추는 것이 그 어느 때보다 중요해졌습니다.

보다 복잡한 위험 환경과 증가하는 사이버 피해 청구 활동에 대응하여 보험 업계는 기업이 보안 및 위험 관리 통제방안을 개선하도록 장려하기 위해 회사의 사이버 위험 프로필을 보다 성실하게 평가하고 있습니다.

세이스는 다음과 같이 마무리하였습니다.

"우리는 훨씬 더 좋은 통찰력을 얻고 있으며 포괄적인 데이터를 제공하기 위해 더 많은 노력을 기울이는 고객에게 감사드립니다. 또한 이는 고객에게 더 많은 가치를 제공하고 어떤 방안이 가장 효과적인지 또는 위험 관리 및 대응을 위한 접근 방식을 더욱 개선할 수 있는 부분에 대한 유용한 정보와 조언을 제공하는데 도움을 주고 있습니다."

Source: https://safety4sea.com/allianz-cyber-risks-trends-2022/

사이버 공격을 받은 Voyager Worldwide

Source : Splash247.com

해양 기술관련 대기업인 Voyager Worldwide는 가장 최근에 사이버 공격을 받은 해양 분야에서 유명한 기업이 되었습니다.

12월 2일부터, 전 세계 1,000 개 이상의 해운 회사를 고객으로 자랑하는 내비게이션 서비스 및 솔루션 제공 업체에서 모든 시스템이 오프라인 상태가 되었습니다.

" 현재 조사 중에 있으며, 우리의 우선 순위는 사고의 영향을 억제하는 것이므로 복구 기간이 바뀔 수 있습니다.“ 라고 Voyager사는 설명하였으며, 이번 주까지 시스템을 다시 온라인 상태로 복구하는 것을 목표로 하고 있습니다.

사이버 보안 회사인 Mandiant는 Voyager사의 내부 팀이 공격에 대응할 수 있도록 지원하고 있습니다.

Voyager사의 서비스 범위 중에는 사이버보안 및 보호 포트폴리오가 있습니다.

해양 사이버보안 회사인 CyberOwl, 해양 혁신 기관인 Thetius, 법률 회사 HFW가 올해 초 발표한 해운 사이버보안 설문조사에 따르면 응답자의 44%가 지난 3년 동안 자신의 조직이 사이버 공격을 받은 적이 있다고 보고했습니다. 또한, 그 중 3%는 피해자가 공격자에게 몸값을 지불했으며 평균 비용은 3.1백만 달러인 것으로 조사되었습니다.

Source: https://splash247.com/voyager-worldwide-hit-by-cyber-attack/

LTE 구조와 5G 분산형 네트워크의 비교

Editor : 한국선급 유진호 책임검사원

기획시리즈 순서

① 5G란 무엇인가?

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

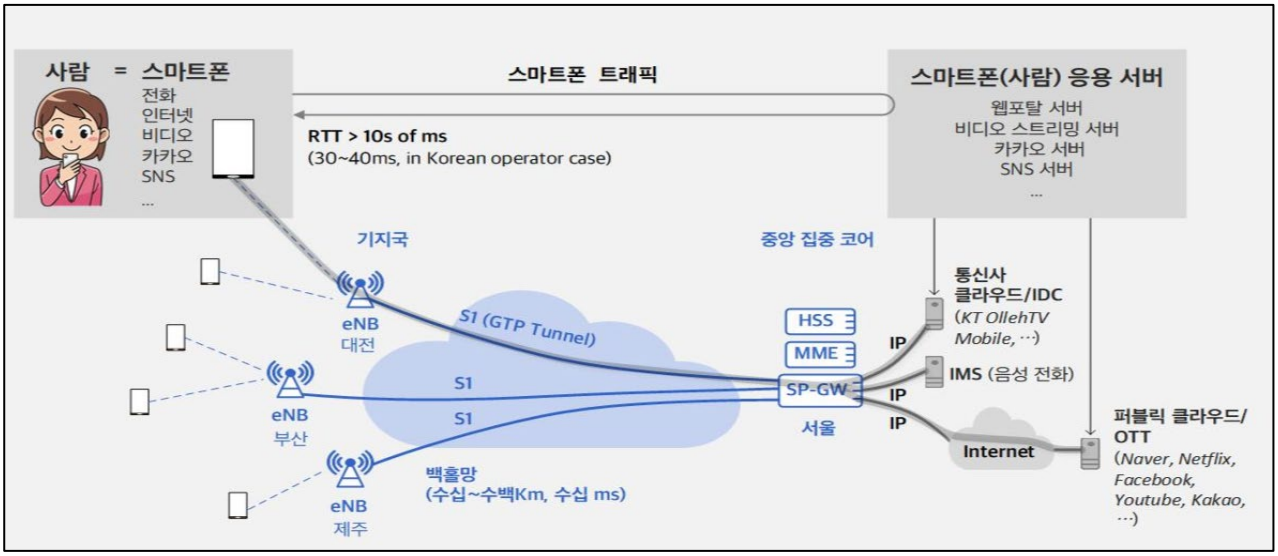
③ LTE의 중앙집중형 네트워크와 5G의 분산형 네트워크의 비교

④ 5G 표준에서 무선백홀 기술과 5G 위성의 역할

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

4G LTE 네트워크 구조

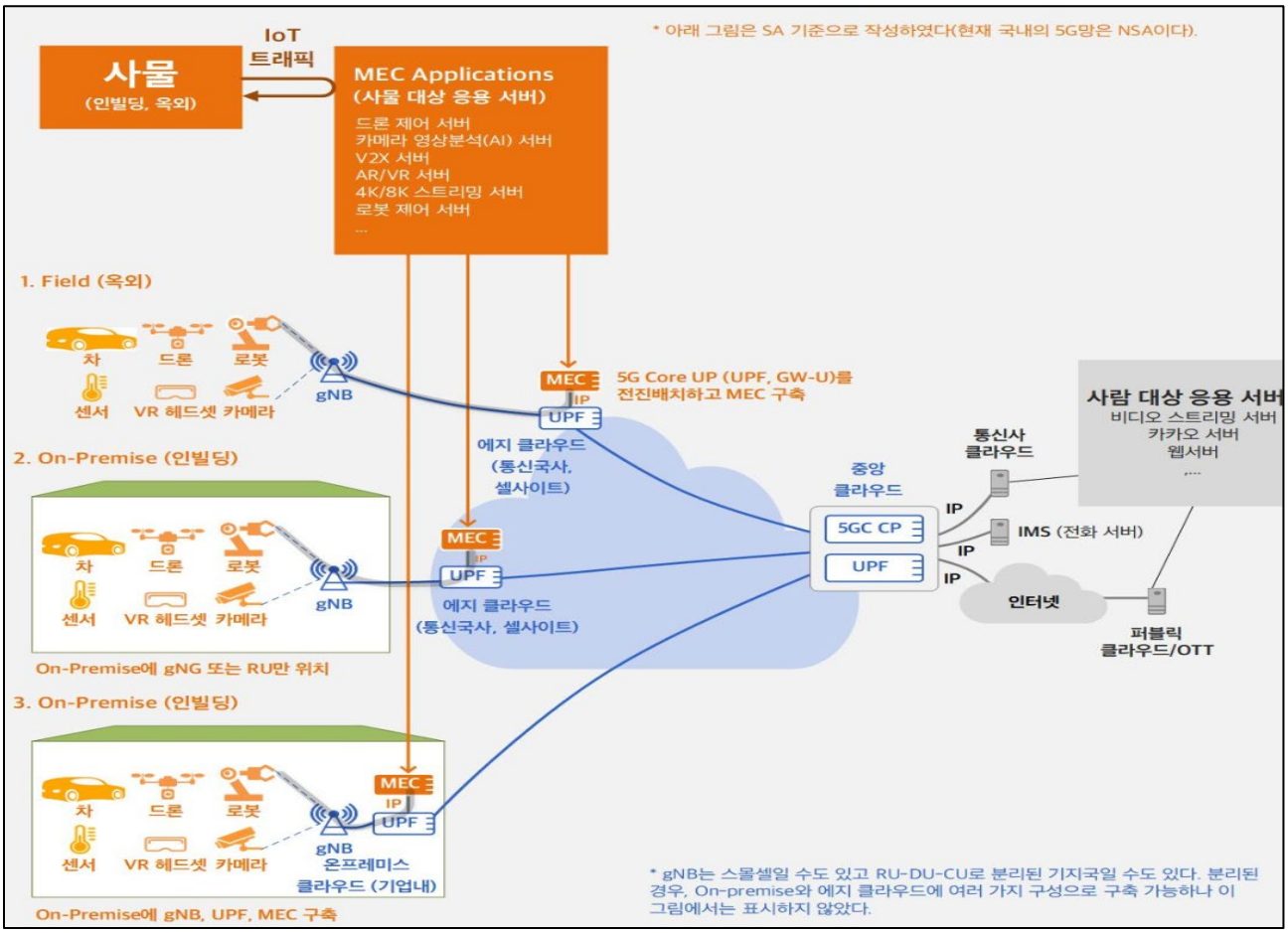
우리가 사용하고 있는 LTE 스마트폰의 네트워크는 무선통신뿐만 아니라 유선통신 네트워크를 포함하고 있다. 4G LTE 유무선 네트워크는 크게 기지국 장비(eNodeB)와 핵심망(Core Network)로 2단계 구조이다. 핵심망은 핸드오버, IP할당, 과금, 정책, 단말기 인증 등의 역할을 하며, LTE Core(SP-GW)는 전국에 몇 개의 사이트에 집중되어 있는 구조이다. 모든 모바일 트래픽이 중앙의 LTE Core(SP-GW)로 전달되며, 이후 IP 라우팅되어 IP 서비스(전화(IMS), 인터넷, OTT 등)를 받을 수 있다. 스마트폰 응용 서비스들이 지연에 매우 민감하지 않고 용량도 많아야 수십 Mbps 정도를 필요로 하므로 4G LTE 네트워크 구조는 스마트폰을 중심으로 특화되어 있다.



출처 : https://www.netmanias.com/ko/post/oneshot/14273/5g-iot-mec/mec-concept-and-deployment-architecture-in-4g-and-5g-network

5G 분산형 네트워크 구조

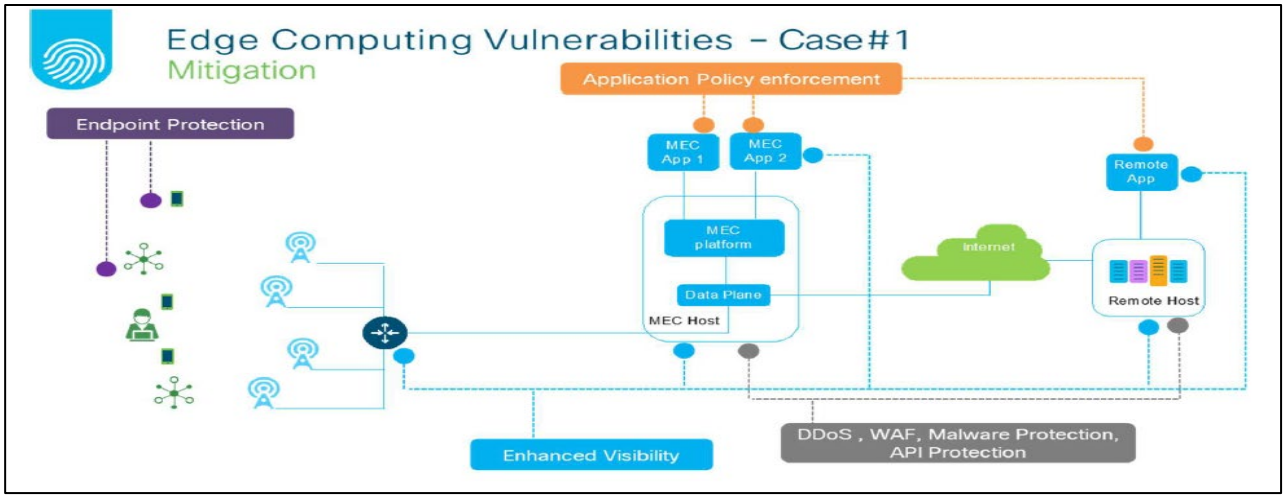
최근 수많은 사물인터넷(IoT; Internet of Things) 기기들이 출현하면서, 기기 간 통신의 신뢰성, 무결성이 중요한 시대가 다가 오고 있다. 예를 들어 자율주행차, 드론 및 로봇제어 등을 위해서는 단말기와 응용서버간의 지연시간과 트래픽 분산문제가 해결되어야 통신의 신뢰성과 무결성을 확보할 수 있다. 하지만 LTE 네트워크는 모든 트래픽들이 LTE Core(SP-GW)로 집중되었다가 IP 라우팅 되는 구조이므로 긴 지연시간이 발생하고, 백홀망 트래픽의 부하를 초래할 수 있다. 이러한 문제를 해결하기 위해 등장한 것이 5G 분산형 네트워크 구조이다. 사물 대상 응용서버(MEC; Mobile Edge Computing)를 단말 가까이 전진 배치하여 초저지연 응답을 제공하고, 백홀망의 트래픽을 절감할 수 있는 효과가 있다. 이러한 5G의 분산형 네트워크 구조를 선박 내부 네트워크에 적용한다면 선내의 수많은 센서와 기기제어, 선내 CCTV 영상분석을 통한 선내 모니터링 서비스를 효과적으로 구현하고, 화물(컨테이너 등)에 사물인터넷(IoT) 기기를 부착함으로써, 해운물류 서비스의 혁신을 초래할 수 있을 것으로 본다.



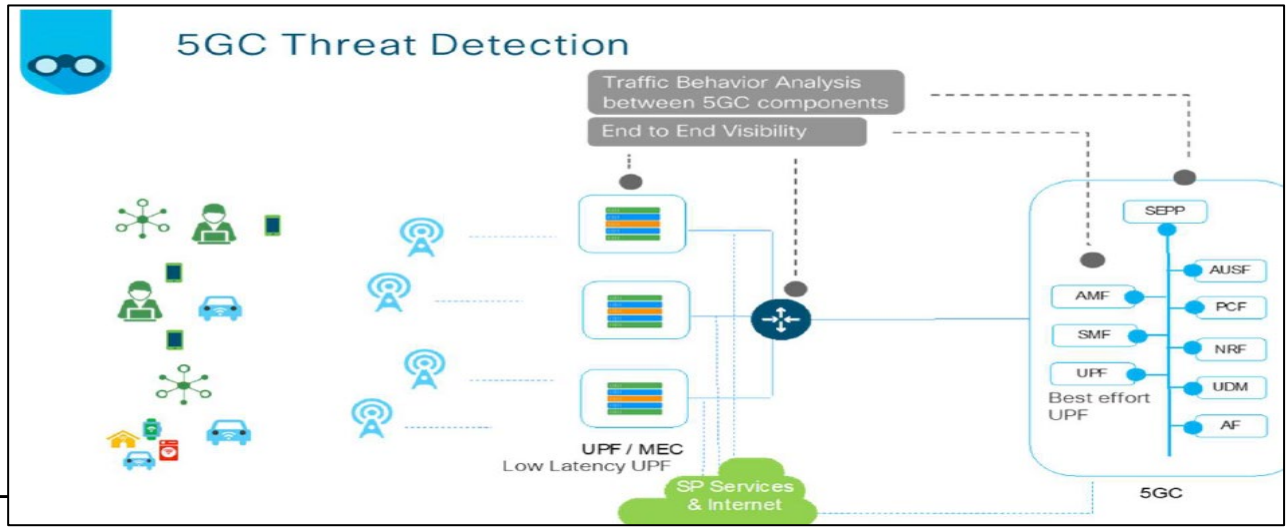
출처 : https://www.netmanias.com/ko/post/oneshot/14273/5g-iot-mec/mec-concept-and-deployment-architecture-in-4g-and-5g-network

5G의 사이버보안 위험요소 – 5G 분산형 네트워크 구조의 보안 취약점

5G 분산형 네트워크 구현하기 위해서는 다양한 네트워크 슬라이스가 서버, 메모리, 네트워크 및 스토리지와 같은 물리적 인프라를 공유하게 된다. 이러한 경우 각 슬라이스에 대한 자원 예약 및 격리는 본질적으로 가변적일 수 있으며, 공통 자원 풀 세트를 공유할 수 있다. 이러한 경우, 하나 이상의 슬라이스에 대한 DoS/DDoS 유형 공격은 간접적으로 다른 슬라이스에 영향을 줄 수 있다. 따라서 물리적 인프라는 다양한 슬라이스에서 공통 리소스를 공유할 때, 슬라이스 간에 적절한 리소스 격리를 제공해야 한다.



이러한 5G 분산형 네트워크의 보호를 위해서는 적절한 가시성, 세그멘테이션, DNS 레벨 보안(예 : 알려진 취약점, 악성 도메인) 및 비정상 네트워크 흐름탐지가 필수적이다.
적절한 가시성과 행동분석을 통해 운영자가 5G 네트워크 코어에 영향을 미치는 위협을 탐지 할 수 있다.

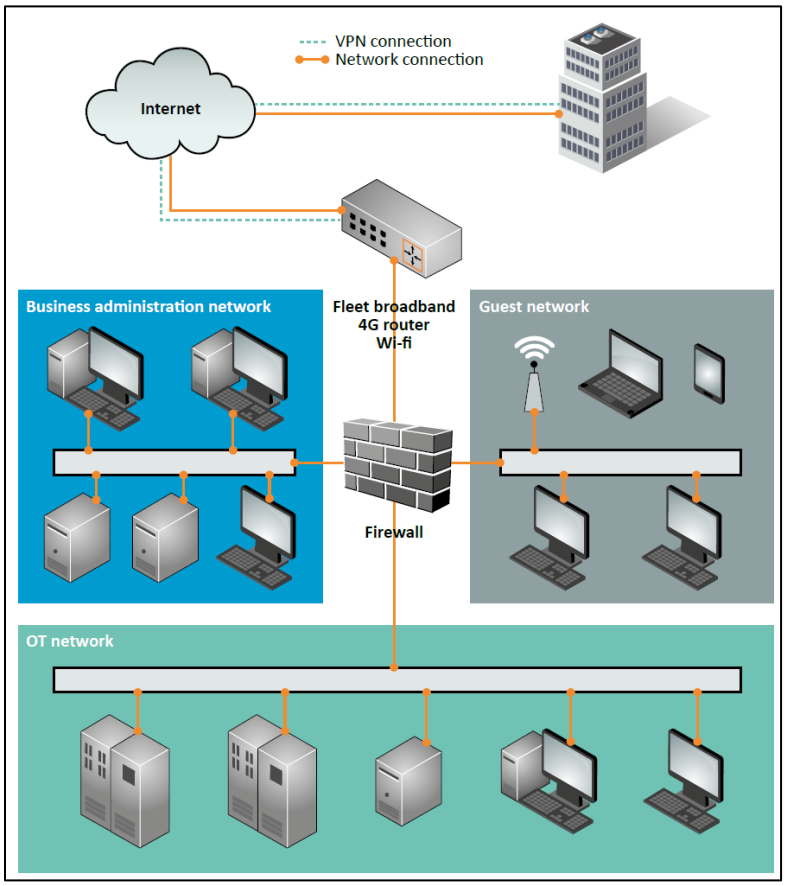


출처 : The Evolution of Security in 5G, 5G America white paper, July 2019

신뢰할 수 없는 네트워크와의 통신 보안

Editor : 한국선급 최상훈 책임검사원

올 해 4 월 국 제 선 급 연합회(IACS)에서 발행된 공통 규 칙 인 UR E27 은 선 박 에 탑 재 되 는 다 양 한 기 자 재 의 사 이 버 복 원 력 을 위 한 요 구 사항들을 담고 있으며, 신뢰할 수 없는 네트워크와의 통신을 수행하는 경우 추가 보안 기능을 요구한다. 이번호에서는 이에 대한 내용을 살펴보도록 하겠다. 우선 UR E27에서는 UR의 적용 범위 밖에 있는 모든 네트워크 신뢰할 수 없는 네트워크로 정의한다. 추가 보안 기능은 총 10가지 항목으로 IEC 62443 3-3의 요구사항 기준 Security Level 3 수 준 에 해 당 되 는 요 구 사항들도 포함된다.



< 선내 네트워크 예시 (source : BIMCO)>

UR E27에 따라 신뢰할 수 없는 네트워크와 연결되는 선내 시스템 및 기자재를 공급하는 제조사들에 요구되는 10가지 추가 보안 기능 요구사항은 다음과 같다.

1. 인간 사용자에 대한 다중요소 인증

다중요소 인증은 지식 기반, 소유 기반, 속성 기반의 세가지 팩터 중 두가지 이상을 사용하여 인증을 수행하도록 하는 것으로서 인증시 지식 기반인 비밀번호와 속성 기반인 지문 인식을 모두 사용하도록 하는 기능을 제공하는 것이 이에 대한 예시가 될 수 있다.

2. 소프트웨어 프로세스 및 장치 식별 및 인증

허가되지 않은 소프트웨어의 설치를 차단하거나 허가되지 않은 장치가 시스템에서 사용되지 않도록 해야 한다.

3. 로그인 시도 실패

신뢰할 수 없는 네트워크로부터 지정된 시간 동안 연속적으로 사전에 정해진 횟수 이상의 로그인 시도 실패 시 접속을 제한 하는 기능을 제공 해야 한다.

4. 시스템 사용 알림

사용자 인증 전 시스템 사용에 대한 알림 메시지를 표시할 수 있는 기능을 제공해야 하며, 알림 메시지 설정은 허가된 직원에 의해서 가능해야 한다.

5. 신뢰할 수 없는 네트워크를 경유한 접근

신뢰할 수 없는 네트워크를 경유한 접근에 대해 감시하고 통제하는 기능이 제공되어야 한다.

6. 명시적 접근 요청 승인

신뢰할 수 없는 네트워크를 통한 접근은 선내 허가된 직원의 승인을 통해서만 가능하도록 해야 한다.

7. 원격 세션 종료

설정된 시간동안 미사용 혹은 세션을 시작한 사용자가 수동으로 원격 세션을 종료 할 수 있도록 하는 기능을 제공해야 한다.

8. 암호화 무결성 보호

신뢰할 수 없는 네트워크와 통신하는 경우 정보 변경을 인지하기 위해 암호 메커니즘을 적용하여야 한다.

9. 세션 무결성

세션의 무결성을 보호하는 기능을 제공해야 하며, 유효하지 않은 세션 ID는 거부되어야 한다.

10. 세션 종료 후 세션 ID 무효화

사용자가 로그 아웃과 같은 세션 종료시에 시스템은 세션 ID를 무효화 해야 한다.

KR CS++
한국선급 사이버보안 교육도구

No.	교육 동영상 명
1	해사 사이버보안의 이해
2	해사 사이버보안 관리 실무
3	관리적 보안
4	사이버 자산/위협 및 기술적 보안
5	사이버보안 형식 승인
6	해사 사이버 리스크 평가의 이해
7	KR 원격 사이버 검사

한국선급은 USB 타입과 테블릿 타입의 해상 사이버보안 교육훈련도구인 KR CS++를 출시하였다.

KR CS++는 선박에서 인터넷 환경이 불안정하여 사이버보안 교육훈련이 어려운 환경에서 효과적으로 선원들의 사이버보안 교육훈련을 위해 USB 타입과 테블릿 타입으로 제작하였다.

또한, 한국선급은 다양한 방식의 서비스 제공을 통해 고객 만족을 위해 노력하고 있다. 현재 사이버보안 이러닝 교육을 통해 동일한 서비스를 제공하고 있다.

온라인 교육
KR 해사 사이버보안 이러닝 센터 교육 과정 운영

교육 문의 : https://edu.orangecq.com/

한국선급은 해사 사이버보안 전문업체인 오렌지씨큐리티와 협력하여 운영 중인 사이버보안 이러닝 교육 과정을 개편하였다. 이번 교육 과정 개편을 통해 교육 대상자별 맞춤형 교육을 제공하게 되었다.

새로운 교육 과정은 해사 사이버보안 인식 제고, 해사 사이버보안 실무 관리, 사이버보안 담당자, 사이버보안 형식승인으로 구성된다. 해사 사이버보안 인식 제고 과정은 선원들을 포함한 일반 임직원의 해사 사이버보안 인식을 증대 시키기 위한 과정으로 해사 사이버보안의 이해 및 해사 사이버보안 관리 실무 모듈로 구성된다. 해사 사이버보안 실무 관리 과정은 선박 사관 및 기술자를 위한 교육으로 해사 사이버보안 인식 제고 과정에 KR 원격 사이버 검사에 대한 모듈을 포함한다. 사이버보안 담당자 과정은 사이버보안 시스템 관리 및 선급 사이버 검사 준비를 담당하는 사이버보안 담당자 또는 관리자를 대상으로 한 과정으로 해사 사이버보안 실무 관리 과정과 함께 관리적 보안, 사이버 자산, 위협 및 기술적 보안, 해사 사이버보안 리스크 평가의 이해 교육을 포함한다. 마지막으로 사이버보안 형식 승인은 기자재업체를 대상으로 기자재의 보안 기능을 확인하는 국제 기준에 대한 소개 및 KR 사이버보안 형식 승인을 받기 위해 필요한 기능 및 제출 자료를 포함한다.

Providing the best services, Creating a better world

Cyber Certification Team, Korean Register
46762 부산광역시 강서구 명지오션시티 9로 36 (명지동)
(46762) 36, Myeongji ocean city 9-ro, Gangseo-gu, Busan Republic ok Korea
Tel +82 70 8799 8595
Fax +82 70 8799 8594
www.krs.co.kr