KR Maritime Cyber Security

News from KOREAN REGISTER

Apr 2019

Vol. **012**

한국선급 활동

● SEA ASIA 2019, KR 사이버보안 기술 세미나 개최

한국선급 사이버인증팀은 싱가포르에서 개최한 아시아 해양박람회인 SEA ASIA 2019에서 한국선급 부스 사이버보안 기술 세미나를 개최하였다.

기술세미나는 두 세션으로 구성되었으며 첫 번째 세션에서는 전반적인 해사업계 사이버보안 주요 이슈 및 KR 사이버보안 활동, 두 번째 세션에서는 최근 발간된 KR 사이버보안 시스템 형식승인이 소개되었다. 금번 부스 기술 세미나는 한국선급에서 최초로 도입된 시스템으로, 현장 관객들의 해사업계 사이버보안 이슈에 대한 궁금증을 해소시켜 큰 호평을 받았다.

이 밖에도 사이버인증팀은 기술서비스 항목인 사이버보안 갭 분석(8개항목)과 한국선급이 제공하는 사이버보안 교육 프로그램(인식제고 과정, 고급 과정, 규칙 해설 과정) 등에 대한 정보를 제공하였다.

한국선급은 세계적으로 사이버보안의 중요성이 높아짐에 따라 사이버보안 분야의 전문성 강화에 심혈을 기울이고 있으며, 이번 전시회를 통해 그간 쌓아온 경험을 공유함으로써 고객들의 만족도를 높일 것으로 기대한다.

● **Sea Asia 2019 KR Cyber Security Technical Seminar**

Sea Asia 2019 Korean Register Cyber Security Technical Seminar

9th – 11th April,
Singapore Korean Register Booth
[No.L1-E01]

▪ Cyber Security Technical Seminar

- Date : **9th to 10th April**
- Place : **Korean Register Booth** No. L1-E01
- Team : Cyber Certification Team
- Contents & Presenter
  1) KR Cyber Security Overview (JK Lim, Senior Surveyor)
  2) KR Cyber Security System Type Approval (SH Choi : Senior Surveyor)

Date	Time	Topic
9th April	14:00 – 14:30	Cyber Security Overview
	14:30 – 15:00	Cyber Security System Type Approval
10th April	10:00 – 10:30	Cyber Security Overview
	10:30 – 11:00	Cyber Security System Type Approval
	14:00 – 14:30	Cyber Security Overview
	14:30 – 15:00	Cyber Security System Type Approval

▪ Provide KR Cyber Security Technical Support (in KR Booth)

1) Gap Analysis for Company & Ship Cyber Security

Korean Register will provide Gap Analysis on 8 main categories* for company & ship cyber security for our client based on KR cyber security checklist.

*Security Policy, Security Organization, Risk Management, Asset Management, Human Security, Physical Security, Technical Security, Incident Response

2) Training Course Introduction

Korean Register will introduce cyber security training course for our client to enhance maritime cyber security capabilities.

● 티원아이티에 국내 최초 회사 사이버보안 적합성 증서 발급

한국선급은 선박전문 IT관리사인 ㈜티원아이티에 대하여 18년 10월부터 회사 IT 시스템 및 선박 IT 시스템 유지보수 시스템에 대한 사이버보안 적합성 검사를 수행하고, 모든 요건을 만족한 ㈜티원아이티에 19년 3월 회사 사이버보안 적합성 증서를 국내 최초로 발급하였다.

㈜티원아이티는 선박 IT시스템의 개발과 관리가 전문인 회사이며, 국내외 유수의 선사와 선박이 ㈜티원아이티의 IT관리 서비스를 받고 있다. 또한 2021년선사와 선박관리사들의 ISM Code에서의 사이버 리스크 관리를 앞두고 선사와 선박을 대상으로 사이버보안 관련 컨설팅과 솔루션을 제공하기 위한 준비를 진행 중이다.

한국선급 박개명 사이버인증팀장은 "한국선급은 선사 대상으로 Songa Shipmangement에 회사 사이버보안 인증을 수행하여 사이버보안 적합성 증서를 발급하였고, 이번 ㈜티원아이티 사이버보안 적합성 증서 발급을 통해 Third party에 대한 사이버보안 리스크 관리에 대한 대안을 제시했다"라고 말했다.

㈜티원아이티 박규태 대표이사는 "(주)티원아이티는 작년부터 사이버보안 시스템을 구축하기 위하여 많은 노력을 기울여 국내 최초로 한국선급의 사이버보안 적합성 인증을 받을 수 있었다. 인증을 준비하면서 얻은 경험과 지식을 바탕으로 선사에서 사이버보안 적합성 인증을 위한 준비를 쉽게 할 수 있는 솔루션을 제공하겠다."라고 말했다.

● DSME 임직원 대상 KR 사이버보안 기술 세미나 개최

한국선급 사이버인증팀에서는 DSME, KONGSBERG, 마린웍스, 한화시스템, LIG 넥스원, 한국해양수산개발원(KMI) 등 조선소 및 국내 기자재 공급업체, 해양정책 연구기관 임직원들을 대상으로 'KR 해상 사이버보안 기술 세미나'를 개최하였다.

날짜	일정	내용
3.27(수)	13:00 - 13:50	KR 사이버보안 개요
	14:00 – 16:00	KR 해상 사이버보안 시스템 규칙(CS Ready)
	14:00 – 16:00	KR 해상 사이버보안 형식승인 규칙
3.28(목)	09:00 – 12:00	사이버보안 리스크평가 방법

본 세미나에서는 조선소 및 기자재 공급업체가 신조선에 사이버보안 기술적 요건을 적용할 수 있도록 KR 해상 사이버보안 시스템 규칙(CS Ready) 및 KR 사이버보안 시스템 형식승인 규칙, 사이버보안 리스크평가 방법 등이 소개되었다. 특히 사이버보안 리스크평가 방법은 한국선급에서 4단계로 구성된 독자적인 사이버 리스크평가 프로세스를 2017년 12월 구축하여 실제 선박에 적용한 사례를 설명하여 큰 호평을 받았다. 향후 한국선급에서는 이와 같은 사이버보안 기술세미나를 제공함으로써 고객들의 만족도를 높일 수 있을 것으로 기대한다.

● 2019년도 국가인적자원개발 컨소시엄 교육과정 안내

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

'해사 사이버보안의 이해[8H]' 과정은 해사업계(선사, 조선소, 기자재업체)에 근무하는 임직원을 대상으로 사이버보안에 대한 이해를 증진시키고, 사이버보안에 필요한 조직 구성, 자산관리 및 위협, 인적보안, 물리보안, 기술보안 교육을 통해 인식 제고 향상을 목표로 한다. (교육일정 : 6.10, 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 : 6.27-28, 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	

선박 IT/OT 시스템 내부자 위협 및 고려사항

● 선박 IT/OT 시스템 내부자 위협

해양 산업은 전세계 공급 체인의 약 90%를 책임지고 있는 방대한 분야이다. 해상 운송 산업은 GPS, AIS 및 ECDIS 등의 다양한 운영기술(OT) 및 정보기술(IT)을 사용한다. 이러한 시스템이 손상되면 데이터 유출 위험뿐만 아니라 선박에 물리적 손상을 초래하고 모든 선상의 생명을 위험에 빠뜨릴 수 있다. 내부자 위협은 의도적 여부에 관계없이 기업의 가장 큰 사이버 위협 중 하나로 간주된다.

1. 사람의 실수 - 피싱 (Phishing) 캠페인, 과실 (원격으로 액세스 가능하게 열어놓는), 노트북 혹은 전화와 같은 기술 사용으로 인한 사이버공격 노출

2. 악의적인 내부자 - 민감한 데이터 유출, 악성 코드로 컴퓨터 시스템 감염, 내부 권한 및 불만을 품은 직원의 남용

3. 사회 공학 - 민감한 정보를 얻기 위해 조작하는 것. 이것은 스피어 피싱, 고위 관리 스푸핑, smishing 및 vishing 공격에 기여한다.

● 고려사항

1. **선원 및 항만직원을 대상으로 하는 교육 및 훈련**은 사이버공격에 능동적으로 대응하고, 실수를 찾아내고, 위기 상황에서 작동하는 능력을 향상시킬 수 있다.

2. **리스크 관리 전략**은 정보 및 운영 자산을 보장하는 데 중요하다. 효과적인 리스크 관리 프레임워크는 사람, 프로세스 및 기술에 탄력성을 창출 할 수 있다.

3. **사건 대응 계획 (IRP)을 수립**하여 적시에 신속하고 효과적으로 대응할 수 있는 능력을 선박에 제공해야 한다. IRP를 구현하면 선원을 위한 정책, 절차 및 지침이 제공되어 사이버 보안 전략의 토대가 마련된다.

4. **지역 사회와 정보 공유가 중요**하다. 이것은 필연적으로 비즈니스 복구 프로세스를 최적화하고 비즈니스 연속성을 가능한 한 빨리 보장하는 데 도움이 된다.

5. **감사 및 침투테스트를 수행**한다. 윤리적 해커에 의한 침투 테스트가 조직 네트워크의 취약성을 찾아 낼 수 있다.

Ref. : PHISH & SHIPS NEWSLETTER(APR. 2019)

궁극적으로 사람은 효과적으로 관리하지 않으면 조직의 가장 큰 위험 중 하나가 될 수 있으며 끊임없이 변화하는 위협 환경에 대한 적절한 교육 및 인식 변화가 필요하다.

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 **'A3 : 2017 – 민감한 데이터 노출'** 을 분석하고자 한다.

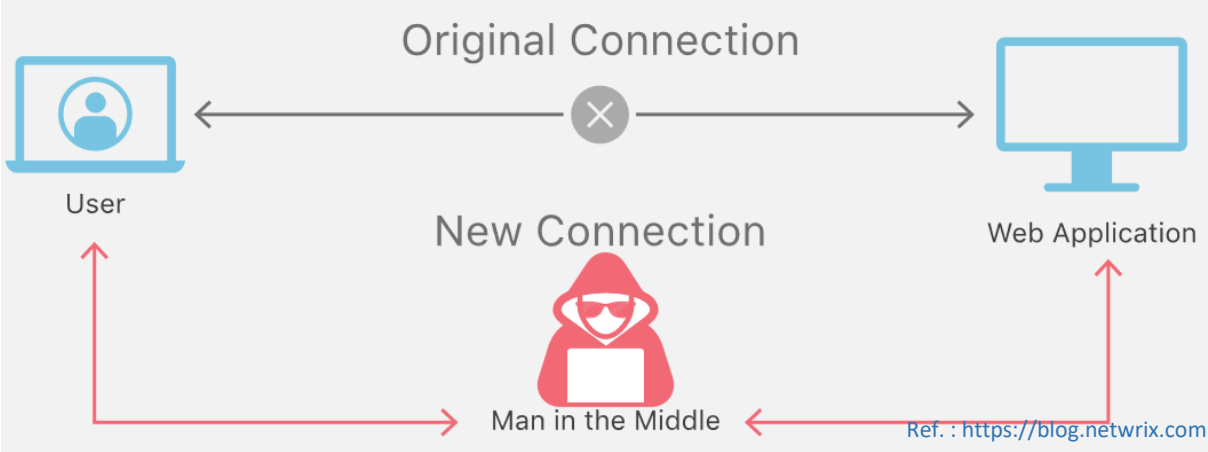
OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – 인젝션	→	A1:2017 – 인젝션
A2 – 취약한 인증과 세션 관리	→	A2:2017 – 취약한 인증
A3 – 크로스 사이트 스크립팅 (XSS)	↘	A3:2017 – 민감한 데이터 노출
A4 – 안전하지 않은 직접 객체 참조 [A7 항목과 병합됨]	∪	A4:2017 – XML 외부 개체 (XXE) [신규]
A5 – 잘못된 보안 구성	↘	A5:2017 – 취약한 접근 통제 [합침]
A6 – 민감한 데이터 노출	↗	A6:2017 – 잘못된 보안 구성
A7 – 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 'A3 : 2017 – 민감한 데이터 노출'**

클라이언트와 서버가 통신할 때 암호화 프로토콜(SSL)을 사용하여 중요한 정보를 보호하여야 한다. 또한 사용자가 민감한 정보를 입력할 때는 암호화되어 저장되어야 하며 이때 데이터 처리와 암호화 저장은 서버 기반에서 실행되어야 한다.

민감한 데이터 노출은 클라이언트와 서버가 통신할 때 SSL을 사용하여 중요한 정보를 보호하지 않을 때 발생하는 취약점이다. 특히 사용자가 민감한 정보를 입력할 때 암호화 저장이 이루어지지 않으면 공격자가 중간에서 정보를 탈취할 수 있다. (중간자 공격) 또한 데이터 처리와 암호화 저장이 클라이언트에서 이루어질 경우에도 공격자는 클라이언트 PC를 장악하여 정보 탈취가 가능하므로 데이터 처리와 암호화는 반드시 서버 측에서 이루어져야 한다.



1. 공격자가 두 장치 (웹 브라우저와 웹 서버) 사이의 통신을 가로채거나 수정
2. 공격자는 두 에이전트 중 하나를 가장하거나 정보를 지속적으로 수집
3. 이러한 공격은 웹 사이트 외 전자 메일 통신, DNS 조회, 공용 WiFi를 대상으로 함

취약점 확인 방법

우선 전송을 하거나 하지 않거나 데이터 보호 요구사항을 확인합니다. 패스워드, 신용카드 번호, 건강기록, 개인정보, 업무 기술들은 특별한 보호가 필요하며, EU의 General Data Protection Regulation(GDPR)와 같은 개인보호법이나 PCI Data Security Standard(PCI DSS)와 같은 금융 데이터 보호 규정에 해당된다면 특별히 보호해야 합니다. 보호가 필요한 데이터의 경우:

- 평문으로 데이터를 전송합니까? HTTP, SMTP, FTP와 같은 프로토콜이 그런 경우입니다. 외부 인터넷 트래픽은 특히 위험합니다. 로드 밸런서, 웹 서버, 백엔드 시스템 간의 내부 트래픽도 확인합니다.
- 백업을 포함하여 저장할 때 평문으로 처리하는 민감한 데이터가 있습니까?
- 오래되거나 취약한 암호 알고리즘을 이전 및 현재 소스 코드에 적용하고 있지 않습니까?
- 디폴트 암호 키 사용 및 약한 암호 키를 생성 및 재사용하거나 적절한 키 관리 및 변경이 이루어 집니까?
- 사용자 프로그램(브라우저)에서 보안 디렉티브나 헤더와 같은 암호화를 적용하고 있습니까?
- 사용자 프로그램(앱, 메일 클라이언트)에서 서버 인증이 유효한지 확인합니까?

ASVS Crypto (V7), Data Prot (V9), SSL/TLS (V10)를 참조

보안 대책

최소한 다음 내용을 준수하고, 레퍼런스를 참고합니다:

- 애플리케이션에서 사용하는 데이터를 처리, 저장, 전송으로 분류합니다. 개인정보 보호법, 법률, 업무 필요에 따라 어떤 데이터가 민감한지 파악합니다.
- 분류에 따라 통제합니다.
- 불필요한 민감한 데이터는 저장하지 않습니다. 가능한 빨리 그런 데이터를 폐기 및 PCI DSS 규정을 준수하거나 불필요한 내용을 줄입니다. 가지고 있지 않으면 도둑맞을 일도 없습니다.
- 모든 민감한 데이터들을 암호화하는지 확인합니다.
- 최신의 강력한 표준 알고리즘, 프로토콜, 암호 키를 사용하는지 확인합니다; 적합한 키 관리를 사용합니다.
- Perfect Forward Secrecy(PFS) 암호를 사용하는 TLS, 서버의 암호 우선 순위 지정 및 보안 매개 변수와 같은 보안 프로토콜로 전송 중인 모든 데이터를 암호화 하십시오. HTTP Strict Transport Security(HSTS)와 같은 지시문을 사용하여 암호화를 시행합니다.
- 민감한 데이터를 포함하는 응답 캐시를 비활성화합니다.
- Argon2, scrypt, bcrypt, PBKDF2와 같은 워크 팩터(딜레이 팩터)를 가진 적응형 솔트된 해시 함수를 사용하여 패스워드를 저장합니다.
- 개별적으로 설정들의 유효성을 검증합니다.

악성코드 대응책 수립 가이드라인

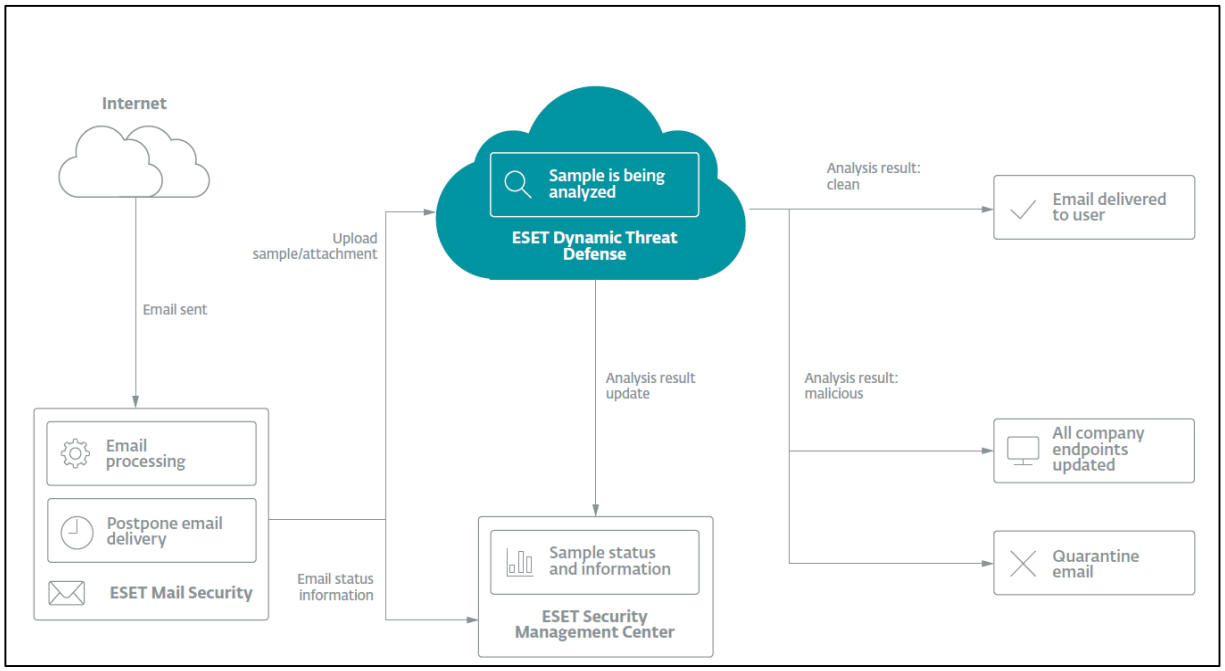
● 악성코드 대응책 수립 필요성

악성코드란 의도적으로 사용자에게 피해를 주고자 만든 모든 악의적 목적을 가진 프로그램 및 매크로, 스크립트 등 컴퓨터 상에서 작동하는 모든 실행 가능한 형태를 말한다. 2017년 머스크해운 랜섬웨어 감염 사건에 사용된 NotPetya는 윈도우 SMB(Server Message Block) 취약점을 악용해 MRB(Master Boot Record) 파일 전체를 암호화해 복호화 비용으로 비트코인을 요구하는 랜섬웨어 'Petya'의 변종으로, 윈도우 운영체에서 동작하는 악성코드였다. 이러한 악성코드는 기업의 비즈니스 운영에 막대한 영향을 발생시킬 수 있어 적절한 대응책 수립이 요구된다. PC, 서버, 모바일 단말기 등에 최신 백신 프로그램(Norton, McAfee, ESET 등)을 설치하거나, 샌드박스 보안 등의 조치가 요구된다.

● 한국선급 해상 사이버보안 인증 검사항목(CS1)

악성코드 대응(217) : 악성코드로부터 네트워크, 정보기술시스템, 단말기를 보호하기 위한 통제장치가 마련되어야 된다.

● 샌드박스 개념도(예시)



Ref. : ESET-Solution-Overview-Dynamic-Threat-Defense

용어 설명

- **SSL(Secure Sockets Layer)** : 웹 서버와 브라우저 간에 암호화된 링크를 설정하기 위한 표준 보안 기술이다. 이 링크는 웹 서버와 브라우저 간에 전달되는 모든 데이터가 개인 데이터 및 통합 데이터로 유지되도록 보장한다. SSL은 업계 표준이며 고객과의 온라인 거래를 보호하기 위해 수백만 개의 웹 사이트에 의해 사용된다. SSL 연결을 만들려면 웹 서버가 SSL 인증서를 필요로 한다. SSL 인증서 신청 프로세스 중에 인증 기관은 사용자의 세부 정보를 확인하고 사용자의 세부 정보가 포함된 SSL 인증서를 발급하며 SSL을 사용할 수 있도록 한다. 웹 서버는 발급된 SSL 인증서를 개인 키와 일치시킬 것이다. 그러면 웹 서버와 고객의 웹 브라우저 간에 암호화된 링크를 설정할 수 있다.
- **중간자 공격(Man in the middle attack)** : 중간자 공격은 통신을 연결하는 두 사람 사이에 중간자가 침입하여, 두 사람은 상대방에게 연결했다고 생각하지만 실제로는 두 사람은 중간자에게 연결되어 있으며 중간자가 한쪽에서 전달된 정보를 도청 및 조작한 후 다른 쪽으로 전달한다. 많은 암호 프로토콜은 중간자 공격을 막기 위하여 인증을 사용한다. 예를 들어, TLS/SSL 프로토콜은 공개 키를 기반으로 한 인증을 사용한다.
- **샌드박스** : 외부로부터 들어온 프로그램이 보호된 영역에서 동작해 시스템이 부정하게 조작되는 것을 막는 보안 형태이다. 샌드박스는 내부시스템과 동일하게 가상화된 환경으로 구성돼 있다. 해커가 심어놓은 악성코드가 샌드박스 안으로 진입했을 때 내부 시스템을 파괴하거나 혹은 정보를 유출하거나 잠복하도록 설정된 해커의 명령을 수행하려는 시스템으로 '착각'하게 된다. 파일이 실행되면 샌드박스 내 보안 솔루션이 악성코드나 사이버 위협을 제거한다.