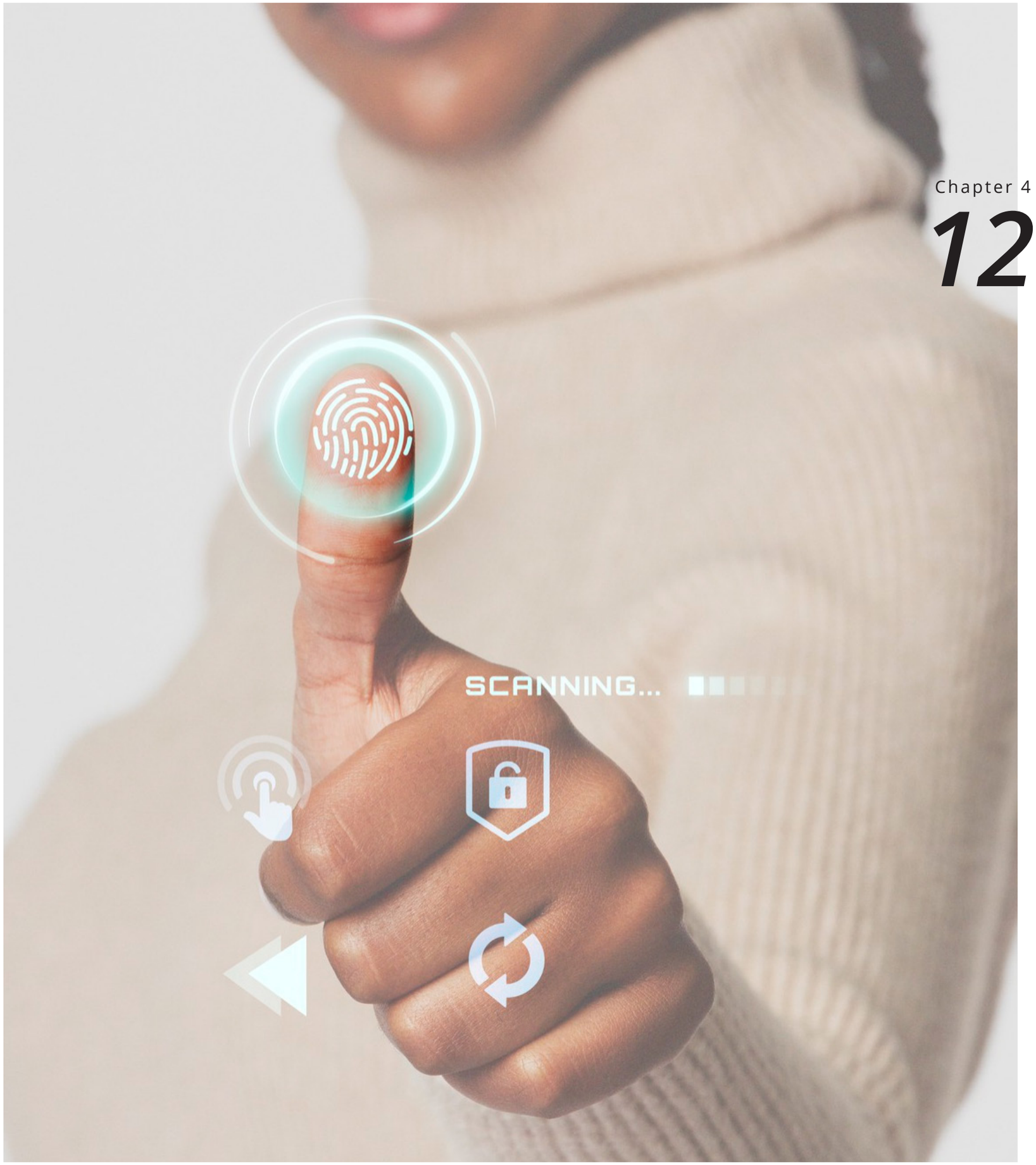


Chapter 4

12 스마트팩토리 시대, 랜섬웨어에 맞서는 OT사이버보안

이재웅 이사 I Deloitte Korea

미국 최대 정유제품 파이프라인(약 8,900km)을 운영하는 콜로니얼 파이프라인(Colonial Pipeline)은 미국 동부 해안 연료 수요량의 약 45% 수송을 담당하는 회사이다. 지난 5월 이 회사에서 파이프라인 운영이 중단되고 데이터가 유출되는 심각한 사이버 침해사고가 발생했다. 2019년에는 세계 4위의 합성 알루미늄 제조회사인 노르스크 하이드로(Norsk Hydro)에서는 일부 공장 생산이 중단되고, 여러 금속 압출 공장이 폐쇄되며, 자동화 공정의 일부가 중단되는 등 약 5,500만 달러의 대규모 피해가 발생하는 사이버 침해사고가 발생하였다. 우리나라의 경우에도 주요 제조/생산 기업에서 사이버 침해사고 피해 사례가 나타나고 있어 공격 타깃의 예외는 아니다.

기존에는 언론에서 드물게 접하던 제조/생산시설의 OT[1] (Operational Technology: 운영기술) 시스템에 대한 침해사고 사례가 최근에는 상당히 자주 들려온다. 위에서 언급된 두 건의 사이버 침해사고의 경우도 생산공정을 담당하는 산업 자동화 및 제어시스템(Industrial Automation & Control System, IACS)을 타깃으로 하고 있는데, 그 규모가 상당하여 OT 사이버 위협의 심각성을 다시 한번 실감하게 되는 계기가 되었다.

최근 몇 년 전까지만 해도 제조/생산공장을 운영하는 많은 조직의 보안통제는 대외적으로 공개된 IT시스템과 회계 및 재무관련 내부업무 지원을 위해 구축한 IT시스템이 대상이었다. 제조/생산시설의 운영과 관련된 산업 자동화 및 제어 시스템은 외부와 차단된 폐쇄망으로 구성되어 있어서 인터넷과 연결된 IT시스템과 비교하여 안전지대처럼 여겨졌기 때문에 보안이라고 하면 보통 물리적 보안의 대상으로만 인식하였다.

그러나, 최근 디지털 전환 및 빅데이터 활용, 클라우드 기술 등을 앞세운 4차 산업혁명은 제조/생산시설에도 많은 변화를 일으키고 있으며, 모든 것이 연결되고 있는 시대에 OT시스템도 더 이상 예외가 아니다. 산업용 사물인터넷(Industrial IoT, IIoT), 산업용 클라우드(Industrial Cloud), 빅데이터, AI 등 새로운 기술의 출현으로 OT시스템은 점차 외부와 연결되고 있으며, 이러한 변화 속에 OT시스템을 먹이감으로 삼는 사이버 위협 및 해킹은 적어도 줄어들지는 않을 것으로 보인다.

그 배경을 살펴보자면 제조/생산시설의 마비 및 설정 값 변경 등의 시스템 무결성 손상 등으로 인해 안전, 보건, 환경까지 영향을 미치는 경우 그 피해는 매우 심각한 산업재해로 전개될 수 있어 이러한 점을 악용한 금전적 이득 목적의 랜섬웨어 해킹피해가 늘어나고 있다. OT 사이버 위협에 효과적으로 대응하기 위해서는 사이버 보안 전략과 체계 수립이 필요한데, 본고에서는 이러한 전략과 체계 수립이 필요한 두 가지 이유와 보안체계 수립을 위한 방안 및 사례에 대해 살펴본다.

1 OT(Operational Technology: 운영기술): 제조/생산, 에너지(전기, 가스, 수력 등), 석유/화학 분야 등에서 공정 자동화 및 산업 제어를 위한 시스템과 이를 제어, 변경, 모니터링하기 위한 기술을 의미함. SCADA, DCS, PLC, SIS 등이 산업 자동화 및 제어시스템(Industrial Automation Control System, "IACS")으로 OT기술이 적용된 시스템에 해당된다.

Reason #1

OT환경의 사이버 위협이 증가하고 있음

- ☑ 금전적 이득을 목적으로 하는 OT환경의 사이버 위협 증대
- ☑ 서비스 형태로 발전한 랜섬웨어 해킹공격 (RasS: Ransomeware as a Service)

랜섬웨어란?(Ransomware)

몸값(Ransom)과 소프트웨어(Software)의 합성어로 특정 기관의 시스템 내 전자파일 또는 데이터를 암호화하여 정당한 사용자가 해당 정보를 사용하지 못하도록 만드는 악성 프로그램을 말한다. 랜섬웨어를 통하여 공격그룹은 피해자에게 암호화된 파일의 몸값을 요구하여 금전적 이득을 취하는 형태로, 잘 알려진 해킹공격 유형 중 하나이다.

랜섬웨어는 IT환경에서 이미 널리 알려진 해킹 유형의 하나로 인식되어 있으나, 최근에는 OT환경에서도 사이버 위협에 사용되는 대표적인 사이버 공격 유형으로 자리잡고 있다. 최근에는 해킹그룹이 피해 기업의 서버 및 단말기 내 전자파일을 암호화하고 몸값을 요구하는 것에 그치지 않고, 피해 기업의 내부 시스템 및 네트워크에 더 깊숙이 파고들어 추가로 금전적 수익을 창출할 수 있는 방향으로 진화하고 있다.

그 중에는 랜섬웨어를 통해 암호화된 파일의 몸값을 지불하지 않는 피해기관을 대상으로 피해자의 내부 시스템에서 탈취한 영업기밀이나 고객의 개인정보 등 중요 데이터를 유출하겠다는 위협을 하거나, DDoS(Distributed Denial of Service) 공격을 통하여 시스템 및 네트워크를 마비시켜 금전적 요구에 타협하도록 위협하는 패턴 등이 파악되고 있다.

그리고 랜섬웨어 공격의 경우 피해기관은 해킹 피해 사실이 언론에 노출되는 것을 원하지 않으며, 금전적 이익이 주된 목적의 공격그룹도 사회적으로 이슈화 되는 것을 원하지 않는다는 점이 매우 특징적인데, 이러한 특징 때문에 랜섬웨어를 이용한 해킹공격은 하나의 서비스 형태(Ransomeware as a Service, RaaS)로 발전하면서 그 규모와 세력을 키우고 있다.

RaaS 시장에는 랜섬웨어를 개발하고 배포한 그룹과 랜섬웨어를 구매하여 사용하는 공격그룹이 존재한다. 총과 같은 무기 판매상과 이를 구매하여 상점을 터는 강도가 존재하는 것과 같이 사이버 상에서도 하나의 생태계로 발전된 것이다.

특히 사이버 상에서의 익명성으로 인하여 사이버 범죄자를 잡기가 쉽지 않다는 점도 사이버 공격 시도가 점점 증가하는 배경 중 하나이며, 콜로니얼 파이프라인을 대상으로 사용된 다크사이드(DarkSide) 랜섬웨어의 경우도 랜섬웨어 개발그룹과 공격그룹이 다른 RaaS의 대표적인 최근 사례이다.

결과적으로 랜섬웨어 몸값으로 지불되고 있는 거래규모도 급격히 늘어나고 있는데, 더 큰 문제는 실제 피해사례와 거래규모는 공식적으로 집계된 수보다 훨씬 더 많을 것으로 예상은 되지만, 정확하게 그 규모가 식별되지 않는다는 것이다.

일각에서는 랜섬웨어의 몸값을 지불하는 것이 랜섬웨어 서비스 시장을 성장시키는 것이라는 메시지를 내세워 공격그룹과 타협하면 안 된다는 캠페인도 진행하고 있지만, 실제 피해기관의 입장에서는 랜섬웨어 공격피해로 인해 발생되는 재무적 손실, 평판 손실, 법적 규제준수 위반 및 계약 위반 등에 따른 손실을 계산하면 공격그룹과 타협하는 것이 문제를 훨씬 간단하고 저렴하게 해결하는 셈이다. 랜섬웨어 공격그룹도 이러한 점을 잘 알고 있다.

콜로니얼 파이프라인에 사용된 다크사이드 랜섬웨어 개발그룹은 자신들이 정치적, 지정학적으로 무관하며, 사회적 문제로 이슈화 되길 원하지 않고, 오로지 금전적 이익이 해킹의 목적임을 발표하였다. 결론적으로 콜로니얼 파이프라인은 타협의 대가로 약 500만 달러를 지불하였다.

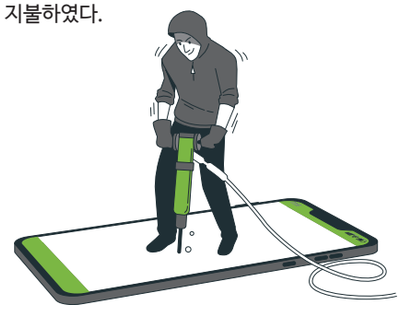


그림 1

ICS/OT 관련 사이버침해사고 사례

피해 조직	국가	피해 연도	공격 종류
콜로니얼 파이프라인(Colonial Pipeline)	미국	2021	랜섬웨어(Darkside)
솔 오리엔스(Sol Oriens)	미국	2021	랜섬웨어(REvil)
JBS 푸드(JBS Foods)	미국	2021	랜섬웨어(REvil)
혼다(Honda)	일본	2020	랜섬웨어(EKANS)
노르스크 하이드로(Norsk Hydro)	노르웨이	2019	랜섬웨어(LockerGoga)
레이크 시티(Lake City)	미국	2019	랜섬웨어(Ryuk)
우드 랜치 메디컬(Wood Ranch Medical)	미국	2019	랜섬웨어
사우디아라비아 석유화학공장	사우디	2017	지능형 지속 위협(Advanced persistent threat, APT) 공격(Triton)
우크라이나 지방 전력공급회사	우크라이나	2015/2016	APT 공격(Black Energy)
이란 부셰르 원자력 발전소	이란	2010	APT 공격(Stuxnet)

출처: 딜로이트 재구성

콜로니얼 파이프라인의 해킹그룹이 발표한 성명서

"우리는 어떠한 정당과도 관련이 없으며 지정학에 관여하지 않는다. 우리를 어떠한 정부와 결부시킬 필요가 없고 다른 동기를 찾을 필요도 없다. 우리의 목표는 돈을 버는 것이지 사회에 문제를 일으키는 것은 아니다. 오늘부터 우리는 중용의 입장을 가지며, 향후 사회적 결과를 피하기 위해 우리의 파트너가 암호화하고자 하는 각 회사를 확인한다."

출처: CNBC

공통적인 보안 문제로 인해 기업들이 랜섬웨어에 취약해지고 있다

- 중요한 네트워크와 제어 시스템으로 공격이 확대되는 것을 제한하기 위한 운영 기술(OT) 및 IT 네트워크 망 분리 미흡
- 핵심자산 및 시스템에 대한 침투경로와 취약점에 대한 인식 부족
- 회복탄력성 및 사업연속성의 효과성을 검증하기 위한 백업 및 복구테스트의 부족
- OT시스템의 관리자 권한 및 원격접속 시 강화된 인증 수단의 부재 (멀티팩터 인증 등)
- 부적절한 취약점 관리와 OT시스템 전반적인 패칭 사이클 및 테스트 관리 미흡
- 비즈니스 연속성을 지원하기 위한 랜섬웨어 사고 대응 계획 수립 및 이행 부족
- 비정상적인 업로드에 대해 제한적인 모니터링 역량
- OT와 IT의 제한적인 협업으로 사이버 위협에 대한 시각차이가 발생되며, 제각지 다른 '사고 대응 및 회복탄력성 계획' 수립

출처: 딜로이트 분석

IT시스템의 경우 노후화 주기가 약 3~5년 정도로 운영되는 반면, OT시스템의 교체주기는 약 15~20년 이상일 정도로 IT시스템에 비해 교체주기가 상당히 길다. 안전, 보건, 환경이 고려되는 제조/생산 인프라 시설과 관련된 시스템을 설계하고 구축하기 위한 내부 투자 심의 및 검토 프로세스도 IT시스템 투자보다 훨씬 더 많은 이해관계자와 내외부 전문가의 의견을 고려한다. 또한, IT시스템의 경우 시스템 하드웨어 및 소프트웨어 업데이트가 굉장히 빠르고 빈번하게 발생되는 반면, OT시스템의 경우, 인명피해 등 안전과 매우 밀접하게 관련된 산업에서는 특히 작은 변화라도 심각한 재해로 이어질 수 있어 시스템 변경 요청이나 소프트웨어 패치도 자주 발생하지 않는다.

꽤 오랫동안 정보보안이라는 용어를 사용하여 왔는데, 이는 정보를 보호하는 것이 주된 목적이라는 점을 내포하고 있다. IT의 발달로 인하여 시스템 내 데이터를 보호해야 하는 미션이 주어지기 시작했고, 기업들은 정보를 보호하기 위한 정보보안 관리체계를 수립하기 시작했다.

이에 따라 IT보안의 경우에는 영업기밀, 인사정보, 연구결과, 그리고 최근에는 고객의 개인정보 등을 보호하는 것이 정보보안의 최우선 과제였다고 할 수 있다. 최근에는 알고리즘에 기반한 데이터 분석을 통하여 타깃 마케팅, 개인화 광고 등이 발전하고 있는데 이러한 데이터의 활용 가치는 이제 기업의 생존을 좌우할 만한 핵심정보로 여겨지고 있으며, 이에 각 나라에서는 국가 차원의 데이터 보호와 활용을 활성화하기 위한 법과 정책을 마련하고 있다. 기업은 내외부에서 수집가능한 데이터를 모색하는데 열을 올리는 한편, 자신의 데이터 보호에도 사활을 걸고 있다.

OT의 경우에도 RTDB(real-time database) 등을 통해 수집하는 실시간 데이터와 로그 등을 활용하려는 움직임이 기존보다 활발해지고 있다. 그러나, 위에서 언급했던 것처럼 제조/생산을 위한 공장 및 시설의 간단없는 운영이 무엇보다 중요하다. 이렇듯 IT/OT는 환경적으로 기업의 목표와 전략이 다르기 때문에 기업의 목표를 달성하기 위해 보호해야 하는 자산의 특성을 고려하여 보안통제의 원칙과 기준을 마련해야 한다.

뿐만 아니라 IT환경에서는 잘 고려되지 않는 '안전(safety)', '보건(health)', '환경(environment)'과 관련된 경영 이슈는 OT시스템 운영환경에서는 매우 중요하게 다뤄지고 있다. 사이버 침해사고에 따른 OT시스템의 설정 값 등의 의도하지 않은 시스템 무결성 훼손 등으로 인해 안전, 보건, 환경에 피해가 간다면 이는 매우 심각한 산업 재해로 이어질 수 있다. 이렇듯 사이버 침해사고로 인해 발생할 수 있는 최악의 시나리오는 IT보안과 OT보안의 매우 큰 차이 중 하나이다.

따라서, 기존에 수립된 IT보안에 적용하던 보안관리 원칙과 기준, 보안통제를 OT보안에 그대로 적용하는 것은 매우 적절하지 않으며, 조직의 IT보안통제의 수준이나 운영의 성숙도 수준이 높다고 하여, OT보안의 수준이 금세 향상될 수 있는 것은 아니다.

IT와 OT(IACS)환경과 각 환경에서 요구되는 사항은 아래와 같이 4개 영역에서 차이점을 보인다.

그림 2

IT와 OT 환경의 차이점

	IT	OT
성능 요건	신뢰할 만한 응답	즉각적인 응답
	높은 처리량	적당한 처리량
	긴 지연 시간과 지터(jitter) 감내 가능	지연이 긴 경우 심각한 문제 발생
	비상시 상호 작용의 중요성 상대적으로 적음	비상 사태에 대한 대응 매우 중요
	IT 프로토콜	IT 및 산업 프로토콜
허용 요건	스케줄된 운영	지속적 운영
	간헐적 고장이 용납됨	중단 허용되지 않음
	재부팅 허용됨	재부팅이 허용되지 않을 수 있음
	허용 가능한 분야 내에서의 베타 테스트	비(非)생산 환경에서 철저한 QA 테스트
	적은 서류작업으로도 수정 가능	변경 후 공식 인증 필요할 수 있음
운영 환경	전형적인 오피스 어플리케이션	특수 애플리케이션
	스탠더드 운영체제(OS)	스탠더드 및 임베디드 운영체제(OS)
	간단한 업그레이드	업그레이드 어려우며, 하드웨어, 로직, 그래픽에 영향을 미칠 수 있음
	기술이 빈번하게 갱신됨 상용 소프트웨어 제품(COTS) (3-5년)	레거시 시스템(15-20년)
	풍부한 자원(메모리, 대역폭)	제한된 자원
	데이터 센터, 서버룸, 오피스 환경	산업 환경
리스크 관리 목표	데이터 기밀 유지와 무결성이 가장 중요	HSE 및 생산이 가장 중요
	리스크의 영향으로는 데이터 손실, 비즈니스 운영 지원이 있음	리스크의 영향으로는 인명 피해, 장비 또는 제품의 손실
	재부팅하여 복구	내결함성 필수

출처: ISA. 딜로이트 재구성.

랜섬웨어 대응을 위한 OT보안체계 수립의 시작점
(방안 및 사례)

- ☑ **사우디 아람코(Saudi Aramco), 허니웰(Honeywell) 등 Fortune 500 주요 기업, NIST의 CSF 및 ISA/IEC 62443 표준 시리즈 적용**
- ☑ **OT 사이버 리스크 관리전략 및 아키텍처 수립이 선행되어야 할 필수 과제**

미국 표준기술연구소(NIST)의 사이버보안 프레임워크(CSF)

미국 연방정부는 국가 중요기반시설을 대상으로 증가하는 사이버 위협으로부터 기반시설을 안전하게 보호하고운영하기 위한 목적으로 미국 표준기술연구소(NIST)의 사이버보안프레임워크(Cyber Security Framework, CSF)를 2013년 발표하였다. 각 기능 별 상세 통제 기준 및 요건을 기준으로 조직에서는 통제 운영 수준의 성숙도 레벨을 체크할 수 있어, 경영진 및 이사회에서 다뤄야 하는 상위레벨의 사이버 리스크를 관리하는 데 효과적인 관리체계 수단으로 활용 가능하다. 현재까지 사우디 아람코(Saudi Aramco) 등 다수의 글로벌 기업 및 이스라엘 국가사이버청(Israel National Cyber Directorate) 등의 정부 기관 등에서 본 프레임워크를 도입하여 사이버 리스크를 효과적으로 관리하기 위한 OT보안체계를 운영하고 있다.

NIST CSF는 조직의 사이버 리스크를 효과적으로 관리하기 위한 5대 핵심기능을 정의하고 있다. 사이버위협에 대하여 예방통제, 탐지 및 적발통제, 교정통제의 목적을 달성하기 위한 순서대로 5대 핵심기능을 '식별/보안통제/탐지 및 모니터링/대응/복구 및 개선'로 정의하였다. 5대 핵심기능, 23개 통제영역 및 108개 보안요건으로 구성되어 있으며, 5대 핵심기능은 아래와 같이 정의하고 있다.

그림 3

사이버보안 프레임워크의 5가지 기능

출처: NIST

산업용 시스템 및 네트워크 표준: ISA/IEC 62443 시리즈

- OT시스템 및 컴포넌트에 대한 상세 위험평가 및 분석
- OT보안 기술 아키텍처 분석을 통한 투자계획 수립
- 공장 운영자 및 유지보수 담당자를 위한 보안가이드 및 운영매뉴얼 제시 필요

산업용 시스템 및 네트워크와 관련된 기술적 보안 표준으로 ISA/IEC 62443 시리즈를 참고하여 조직의 보안 기준을 수립하는 것이 권고된다. 본 표준은 국제자동화협회(International Society of Automation, ISA)와 국제전기기술위원회(International Electrotechnical Commission, IEC)에서 공동 개발하여 국제표준으로 채택하고 있어 에너지, 석유, 화학, 생명공학, 제조부문 등 특정 산업에 국한되지 않고 사용된다.

ISA/IEC 62443 시리즈는 일반, 정책 및 절차, 시스템, 구성요소 4개의 그룹으로 구성되어 있으며, 각 그룹 별 표준문서를 다음과 같이 마련하고 있다. ISA/IEC 62443 시리즈는 기술적, 비기술적인 보안표준을 주제 및 독자에 따라 구성하고 있어 각 조직 별 필요한 표준문서를 선택하여 적용할 수 있다.

그림 4

ISA/IEC 62443 시리즈 표준문서

일반	IEC TS 62443-1-1 개념 및 모델 공시 (검토중)	IEC TR 62443-1-2 단어 및 약어 총괄 용어집 투표/ 논평 중	IEC 62443-1-3 시스템 보안 적합성 메트릭스 개발 계획 중	IEC 62443-1-4 IACS 보안 생명주기 및 사용 사례 개발 중	
정책 및 절차	IEC 62443-2-1 IACS 자산 소유자의 보안 프로그램 요구사항 공시 (검토중)	IEC 62443-2-2 IACS 보호 수준 투표/ 논평 중	IEC TR 62443-2-3 IACS 환경에서 패치 관리 공시 (검토중)	IEC 62443-2-4 IACS 서비스 공급자의 보안 프로그램 요구사항 채택	IEC TR 62443-2-5 IACS 자산 소유자의 구현 지침 개발 계획 중
시스템	IEC TR 62443-3-1 IACS 보안 기술 공시 (검토중)	IEC 62443-3-2 보안 위험 평가 및 시스템 설계 승인	IEC 62443-3-3 시스템 보안 요구사항 및 보안 수준 공시		
컴포넌트	IEC 62443-4-1 안전한 제품 개발 생명주기 요구사항 공시	IEC 62443-4-2 IACS 컴포넌트의 기술적 보안 요구사항 승인			

출처: 국가표준인증 통합정보시스템, 딜로이트 재구성.

OT시스템의 기술적 보안 강화를 위하여 ISA-62443-1-1, ISA-62443-3-3, ISA-62443-4-2의 요건을 중점적으로 적용하는 것이 필요하다.

- **ANSI/ISA–62443-1-1**
  산업 자동화 및 제어 시스템 보안 part 1: 용어, 개념 및 모델(Security for Industrial Automation and Control Systems: Part 1: Terminology, Concepts, and Models) (2007.10.29 승인)
- **ANSI/ISA-62443-3-3**
  산업 자동화 및 제어 시스템 보안 part 3-3: 시스템 보안 요건사항 및 보안 수준(Security for industrial automation and control systems Part 3-3: System security requirements and security levels) (2013.08.12 승인)
- **ANSI/ISA-62443-4-2**
  산업 자동화 및 제어 시스템 보안 part 4-2: IACS 구성요소의 시스템 보안 요건(Security for industrial automation and control systems Part 4-2: System security requirements for IACS Components) (2018.08.13 승인)

ISA/IEC 62443-1-1에서는 산업제어시스템과 관련된 7개의 기본 요건(Foundational Requirement, FR)을 정하고 있으며, ISA/IEC 62443-3-3에서는 시스템의 보안요건(System Requirement, SR)과 강화된 보안요건(Enhancement Requirement, ER)에 대하여 제시한다. 그리고, ISA/IEC 62443-4-2에서는 3-3에서 정의된 SR, ER에 대해 컴포넌트 레벨로 확장한 컴포넌트 요건(Component Requirement, CR)을 정의한다. 컴포넌트는 소프트웨어 어플리케이션, 호스트 장치, 임베디드 장치, 네트워크 장치 4개 유형으로 구분하고 있다.

ISA/IEC 62443 표준의 7개 기본 요건

01 식별 및 인증 (Identification and Authentication Control, IAC)
02 사용통제 (Use Control, US)
03 시스템 무결성 (System Integrity, SI)
04 데이터 기밀성 (Data Confidentiality, DC)
05 데이터 흐름제한 (Restrict Data Flow, RDF)
06 이벤트의 적시적 대응 (Timely Response to Events, TRE)
07 자원의 가용성 (Resource Availability, RA)

이는 시스템 및 컴포넌트의 기술적 보안요건을 제시함과 동시에 각 요건에 대하여 보안수준(Security Level)을 5단계로 측정할 수 있도록 각 보안요건에 대한 보안수준 척도를 제시하고 있으며, 기본적인 보안수준을 다음과 같이 정하고 있다.

보안 수준에 대한 정의[2]

- ☑ 보안 수준이란 IACS가 의도된 방식대로 취약점과 기능으로부터 자유롭다는 확신의 척도이다.
- ☑ ISA/IEC 62443 시리즈는 보안 수준을 5단계의 레벨로 정의하며, 숫자가 높을수록 보안 수준이 높음을 의미한다.

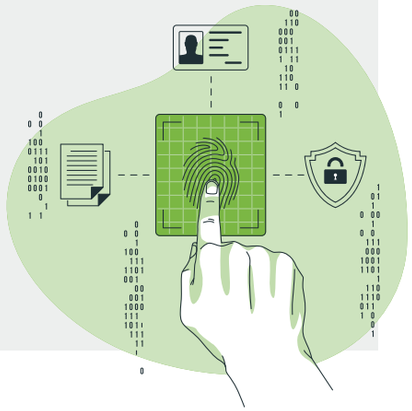
보안 수준 0 특정 요건이나 보호 통제가 필요하지 않음

보안 수준 1 일상적 또는 우연적 위반으로부터 보호 통제

보안 수준 2 적은 자원, 일반적인 기량, 낮은 수준의 적극성을 가지고 단순한 수단을 사용하여 고의적인 위반으로부터 보호 통제

보안 수준 3 적절한 자원, IACS 특정 기량 및 적절한 수준의 적극성을 가지고 정교한 수단을 사용하여 고의적인 위반으로부터 보호 통제

보안 수준 4 폭넓은 자원, IACS 특정 기량 및 높은 수준의 적극성을 가지고 정교한 수단을 사용하여 고의적인 위반으로부터 보호 통제



조직은 각 시스템 요건에 대해 5단계로 측정된 보안수준 결과 값을 가지고 시스템에 대한 상세 위험평가를 수행하여 시스템 레벨의 사이버 리스크를 관리할 수 있게 된다. 이러한 상세 위험평가 과정을 통하여 현재 조직의 보안수준과 리스크를 명확하게 알게 됨으로써 향후 조직의 목표 보안수준을 설정하여 사업 계획을 수립하는 데 활용할 수 있다.

또한, 이러한 기술 표준 아키텍처 분석 및 평가는 향후 조직에서 도입하거나 적용해야 하는 보안 기술 및 솔루션에 대한 단기, 중장기 투자계획을 수립하는 데 꼭 필요한 과정이다. 보안 기술 아키텍처 분석과정이 생략된 보안기술 및 솔루션 도입은 중복된 투자 또는 불필요한 투자 등의 시행착오가 발생할 가능성이 상당히 높아, 결론적으로 조직에서 목표하는 수준의 보안 통제를 구현하는 데 실패할 가능성이 존재한다.

최근 AI, 머신러닝 등의 새로운 기술이 접목된 장비 및 솔루션 등이 잇달아 소개되고 있다. 조직에서 투자해야 하는 보안 기술과 통제의 목표가 무엇인지 정확하게 파악하지 않은 채 OT영역에 대한 보안 강화가 필요하다는 당위성만 내세운 사이버 보안에 대한 투자가 '샤이니 오브젝트 신드롬'으로 기억되지 않도록 해야 한다.

2 ISA

적극적인 위기대응계획 수립: 사이버 리스크 전략 및 보안 거버넌스, 효과적인 측정 및 모니터링 정책 지원 등에 중점을 두고 사이버 침해 등의 기술적 중단 시나리오에 대비하기 위한 계획 수립

핵심 시스템과 자산 파악: 사이버 공격 표면을 파악하고 현재 자산 목록에 대해 지속적으로 취약성 검토를 실시함으로써 공격의 대상이 될 수 있는, 운영에 중요한 자산 파악

IT 위험이 OT로 확산되는 것을 방지: 핵심시스템과 OT네트워크를 별도의 망으로 분리하여 관리하고, 의심스러운 활동을 효과적으로 모니터링하는 체계도입, 접근통제를 위한 점프박스 사용

제로 트러스트의 도입: 기본적인 접근을 사이버 보안 침해로 가정하여 사용자, 워크로드, 네트워크, 장치에 대한 맹목적인 신뢰 배제. 레이어드된 접근제어 관리를 통하여 관리 자격 증명을 보호하고, 네트워크를 세분화 하고 그 우선순위를 구분하여 관리

비즈니스의 회복탄력성 향상: 사업연속성 계획 수립과 모의훈련 등을 포함한 예방 및 탐지활동 외에도 측정, 분석, 대응에 대한 활동을 강화

공격적인 최신 보안 원칙 채택: 사전 예방적인 위협 추적, 머신러닝 기반 사이버 애널리틱스, 자가회복 시스템 등의 최신 보안 원칙을 통하여 공격적인 접근방식을 취하는 방식을 도입

랜섬웨어에 대한 준비성 평가 수행: 사이버 보안 전략과 실제 조직의 역량 간의 격차를 파악하기 위해 랜섬웨어 공격 관련 대비, 대응, 복구를 위한 지속적인 사이버 보안 프로그램 평가를 수행

출처: 딜로이트 분석

마무리하며

- ☑ 공장 운영자, 유지보수 부서에서 보안업무 수행하는 현실
- ☑ OT보안 강화를 위한 사이버 보안 관리조직 및 체계수립이 최우선

OT보안 강화를 위해 현황 분석을 수행하던 중 가장 안타까웠던 부분은 OT보안조직과 담당자가 존재하지 않는다는 것이었다. 공장의 설계부서, 운영부서, 유지보수 담당부서 등의 담당자들은 보안이 중요하다는 것을 인지하고 있었다. 기존에 공장운영에서 강조되지 않았던 보안통제를 구현하는 데 왜 해야 하는지 묻지 않았다. 무엇을 어떻게 해야 하는지 모르는 상태로 책임만 가져가는 것은 용인할 수 없으며, 보안전문가가 공장의 보안업무를 수행하도록 조직을 만들 수 있게 경영진에게 보고해달라는 의견을 받았다. 현업 조직에서는 명확한 내부정책과 프로세스, 운영 매뉴얼 등이 존재하지 않는 상태로 도입되는 보안기술과 솔루션 등이 사이버 위협보다 두렵다는 것이었다.

OT영역에 대한 사이버 보안 이슈는 최고 경영진이 다뤄야 하는 중요한 안건이라는 인식이 빠르게 확산되고 있으며, 상당수의 기업들이 OT보안에 대한 투자 계획을 수립하고 있다. 고도화, 지능화된 사이버 위협에 맞서기 위해서는 자동화된 보안 기술과 솔루션 등이 필수적인 요소이나, 조직의 비즈니스 환경을 고려한 OT 사이버 리스크 전략 및 목표, 보안 통제 원칙과 기준, 그리고 관련 내부 정책/프로세스/기술요건을 수립하는 것이 필히 선행되어야 한다. 그리고, 이를 운영하고 관리하고 개선할 수 있는 OT보안조직이 매우 필요한 상황이다.

Contact

이재웅 이사

딜로이트 안진회계법인
리스크자문본부 정보보안 서비스 그룹
jaewoonlee@deloitte.com