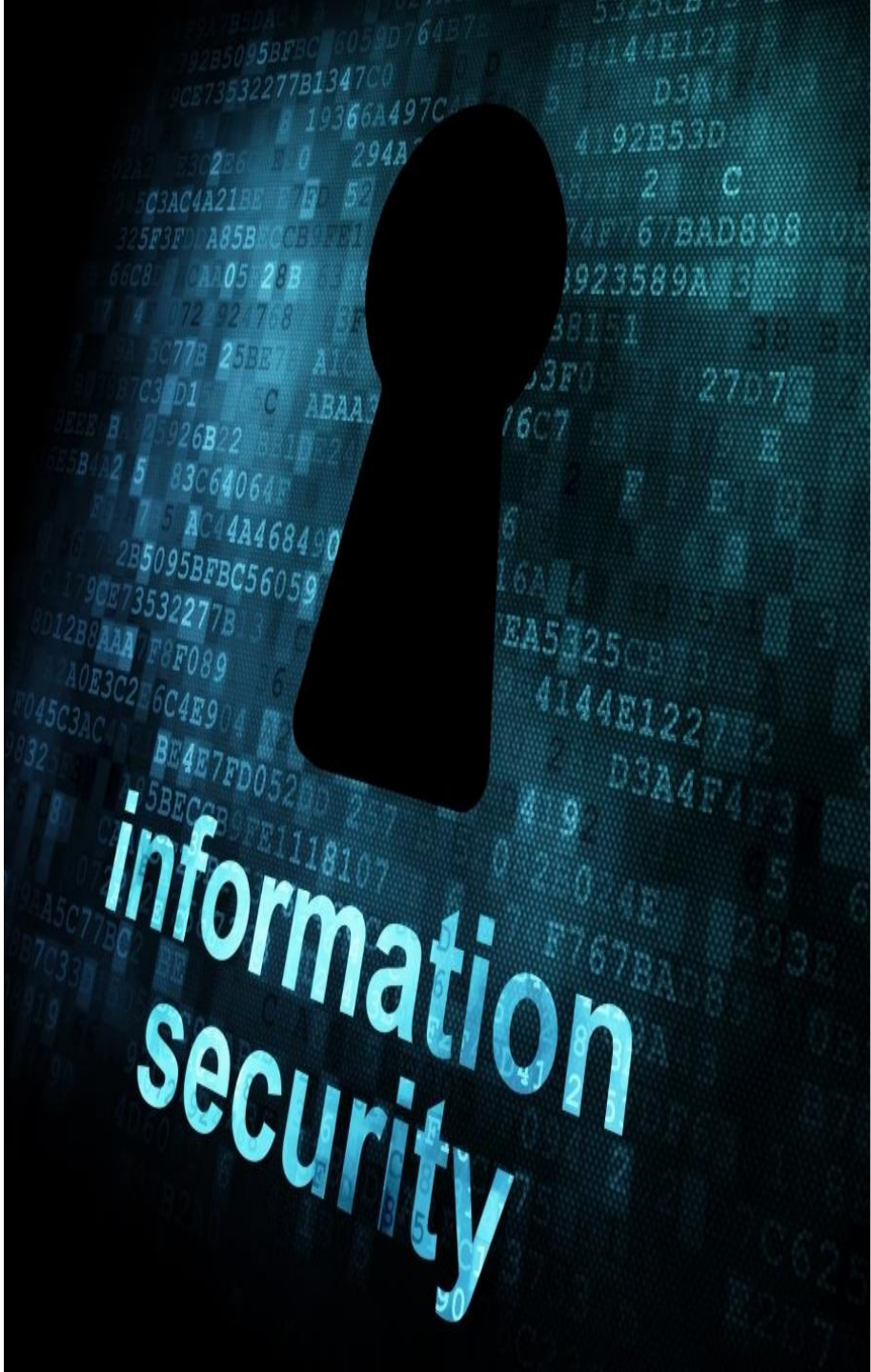
전지적 참견 시점에서 바라본 제조업 OT / ICS 보안

김 재 수



OT & ICS - 개요

OT | (Operational Technology)

산업용 장비, 자산, 프로세스 및 이벤트의 직접 모니터링/제어를 통해 변경을 감지하거나 변경하는 하드웨어 및 소프트웨어

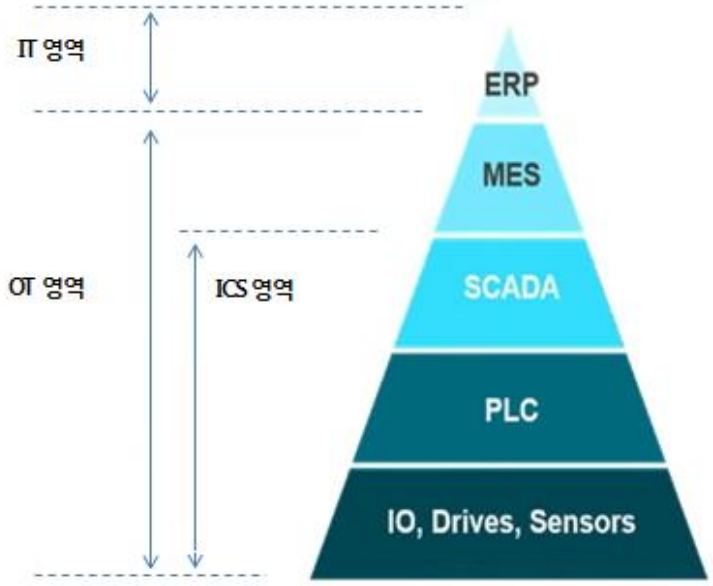
※ 출처 : Gartner IT Glossary

Vs

ICS | (Industrial Control Systems)

전력, 가스, 원자력, 제조 등의 산업현장을 모니터링하고 제어하는데 사용되는 시스템

※ 출처 : TTA 표준 산업제어시스템 보안요구사항



산업 제조/제어 공장 계층도

IT와 OT/ICS의 비교

구분	IT	OT/ICS
보안 목적	기밀성 중시	가용성 중시
보안 인식	필수 사안	성능 영향 우선
패치 방법	정기적 자동 업데이트	벤더의존적, 수동 업데이트
보안솔루션	IPS, DRM, DLP 등	설치 불가
OS	Win10, Win2012 등 최신 OS 사용 가능	Win NT, XP도 존재
장비 사용기간	3~5년	10~30년
네트워크 프로토콜	HTTP 등 범용 프로토콜 사용	비공개 제어 전용프로토콜 사용
소프트웨어	개방형 시스템	폐쇄형 시스템
안전계측 시스템(SIS)	없음	있음
H/W 구축	네트워크 장비, PC, 서버	HMI, PLC 등 제어특화 장비

주요 OT/ICS 보안 현황

40 %	망분리(Air Gap) : 40% 사이트가 외부 인터넷과 연결
53 %	취약 Windows OS : 53% 사이트가 단종된 OS(XP 등)를 사용 중
57 %	방역 대응 : 57% 사이트가 방역 솔루션을 미운영
69 %	취약 패스워드 : 69% 사이트가 평문 패스워드 사용 중
84 %	원격 연결 : 84%사이트가 원격 연결(RDP, VNC, SSH)를 사용 중

※ 출처 : 2019 Global ICS & IIoT Risk Report

OT/ICS 환경 변화

" 수동제어에서 스마트팩토리 등 ICT기술이 결합된 환경으로 변화됨에 따라 ICS 보안 사고 사례 증가 "

제조업 환경 변화

수동제어에서 스마트팩토리 등 ICT 기술이 결합된 환경으로 변화

- **Smart Factory 진화**
  - 생산량 증가, 품질 향상을 위한 IT기술 적용
- **IT영역 위협의 제조영역 확대**
  - FA망 변화 : 폐쇄망 → 개방형 네트워크

ICS 보안 사고 증가 추세

	2000	2003	2008	2011	2013	2015	2016	2017
대상	Russia 천연가스회사 (Gazprom)	USA Ohio Nuclear Plant	USA Nuclear Plant	USA Water Utility	Germany, Australia Power Grid	Australia Dept. of Energy	Israel Electronic Authority	Saudi Arabia 15개 부서
피해	Pipline 통제권	Worm 감염	BlackOut	SCADA 통제권	일부 전력망 다운	전력망 다운	전력망 다운	-
원인	Trojan	Slammer Worm	Cyber Attack	Cyber Attack	잘못된 제어명령	Hacking/Virus	Hacking/Virus	Shamoon/Virus

	2001	2007	2009	2012	2013~2015	2015	2018
대상	USA California 배전센터	Iran Nuclear Plant	Global Oil Comp.	Saudi Arabia Oil & Gas Comp.	USA / Canada 50개 power Plant 운영社	Korea 한수원	Italy Oil Service firm
피해	2개 웹서버	시설 마비	업무 마비	30k+ device wiped	설계 및 패스워드 유출		서버/터미널 감염
원인	보안설정 취약	Stuxnet/Worm	NightDragon/Malware	Shamoon/Virus	Shamoon/Virus		Shamoon Variant

OT/ICS 보안 사고 사례 – TSMC

“반도체 업계 OT보안 사고 사례”

2018년 대만의 반도체업체 TSMC가 랜섬웨어(워너크라이 변종)에 감염되어 48시간 공장 가동 중단

- 감염 경로 : 유지보수업체 USB를 통해 랜섬웨어(워너크라이 변종) 감염
- 감염 범위 : 외부와 차단된 폐쇄망의 생산용PC(1만대 이상 감염)
- 피해 규모 : 48시간 공장 가동 중단으로 약 3000억원(연매출 3%) 손해 발생

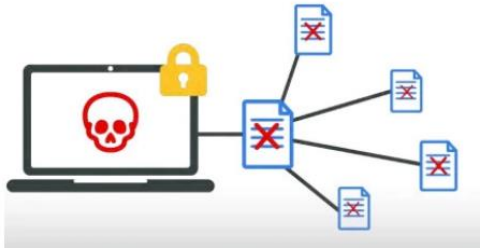
1

STEP 1. 랜섬웨어 감염

- USB사용 시 별도 바이러스 검사 없이 감염된 SW설치, 랜섬웨어(워너크라이) 감염

  → 생산용PC 데이터 암호화/무결성 손상

2



STEP 2. 감염 확산

- SMB취약점을 사용하는 이터널블루 취약점을 통해 감염확산

3

STEP 3. 생산공장 가동 중단

- 생산공장의 기기 1만대 이상 감염

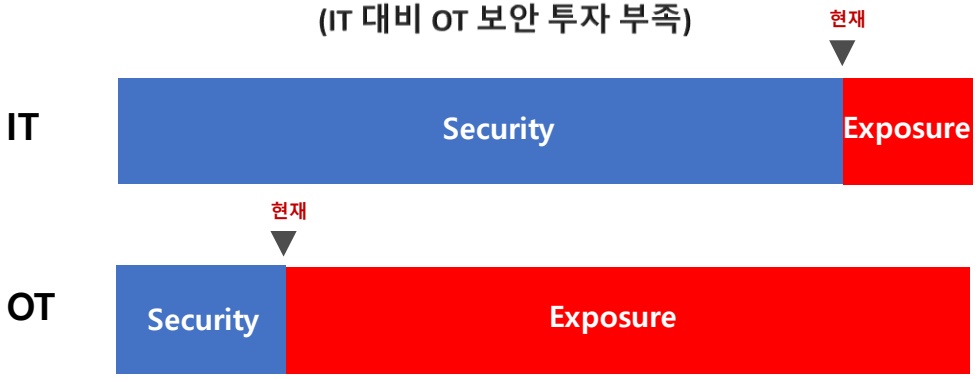
  -> 이틀간 가동 중단

OT/ICS 보안 이슈 및 사고시 영향

"OT 관련 사고 시 간접적인 여파가 아닌 직접적으로 생산환경에 영향 발생"

ICS 보안, 現 이슈

IT/OT 보안 투자 불균형
(IT 대비 OT 보안 투자 부족)



- 백신 위주의 보안 솔루션 운영
- 설계 단계에서부터 보안 고려/투자 無
- 생산 차질 우려로 보안솔루션 적용 회의적

생산망 랜섬웨어 감염시 영향

생산망 랜섬웨어 예상 피해 규모

- 연 매출 40조, 일 평균 매출량 약 1000 억원 규모 회사 기준

(가정) 랜섬웨어 감염으로 10일간 생산 차질 시

조 단위 손실액 발생 가능

OT/ICS 보안

“제 3자의 시각에서 바라보면 OT/ICS 보안을 위해 할 일이 명약관화함 "

[OT보안 리포트] 사이버위협에 노출된 스마트공장, OT/ICS 보안이 답이다

좋아요 147개 | 입력 : 2020-10-05 01:01

가 가

#스마트공장 #Smart Factory #스마트산업단지 #중기부 #TSMC #노르스크 하이드로 #랜섬웨어 #OT보안

2022년까지 스마트공장 3만개, 스마트 산업단지 10개 조성... 하지만 보안은?

[보안뉴스 원병철 기자] 정부가 2022년까지 스마트공장(Smart Factory) 3만개를 짓고 10개의 스마트산업단지(이하 스마트산단)를 조성하겠다고 밝히면서 전국은 지금 ‘스마트공장’의 이슈에 빠져들고 있다. 정부는 스마트공장 전용 대출자금으로 3년간 3,000억원을 제공하고, 스마트공장을 전담할 ICT 코디네이터도 지원한다는 방침을 내세웠다. 중기부는 ‘중소기업 스마트제조혁신 정책 컨트롤 타워’ 역할을 할 ‘중소기업스마트제조혁신기획단’을 신설하고, 산업부·과기부·고용부 등 관련 부처와의 협업을 통해 정책결정을 신속하게 하는 한편, 민간기관과 협업을 통해 정책 효율성을 제고하겠다고 밝혔다.

가장 많이 본 기사 [주간]

1 [긴급] 해킹그룹 탈륨, 통일부 북한인권
2 코로나19로 지각변동! 통합보안·생체
3 [OT보안 리포트] 사이버위협에 노출된
4 패러다임 전환기 맞은 국내 영상보안
5 랜섬웨어 공격으로 코로나 백신 임상실
6 [개인정보보호 연차보고서 톺아보기-1
7 스마트시티형 규제 샌드박스로 승인된
8 랜섬웨어에 돈 내는 것이 불법으로 규
9 [주말판] 허위 정보와 가짜뉴스, 인공지
10 우리나라의 디지털 경쟁력은 세계 몇
11 [한국정보보호학회칼럼] 국가기반시설

“제 3자의 시각에서 바라보면 OT/ICS 보안을 위해 할 일이 명약관화함 "

첫 번째는 OT와 IT는 다르다는 사실이다. 같은 기계장비라고 하지만 양방향 네트워크를 기본으로 하는 IT와 달리 OT는 생산망과 설비망, 공정망이 전용 프로토콜을 통해서 단방향으로만 이뤄진다. 게다가 생산에 필요한 작업만 하는 장비들이기 때문에 IT와는 아예 결이 다르다. 이러한 점 때문에 공장에는 보안, 더 나아가 IT에 대해 잘 아는 사람이 없으며, 반대로 IT에 속한 사람들은 OT에 대해 잘 모른다.

두 번째는 그럼에도 불구하고 생산설비에서 사이버위협이 발생하는 이유는, 기술이 발전하면서 OT 장비들도 ‘디지털화’됐고, 랜 포트나 와이파이 연결이 가능해졌기 때문이다. 공장 직원들은 공장이 폐쇄망이라고 굳게 믿고 있지만, 기술의 발전에 따라 장비들이 기본적으로 네트워크 연결이 가능해졌다. 이런 상황에서 장비를 업데이트 하거나 패치할 때 노트북이나 USB 등 외부 장비를 연결하면, 이미 감염된 장비로 인해 생산설비가 감염돼 생산이 멈춰버릴 수 있다. 대만 TSMC도 이런 방식으로 랜섬웨어에 감염됐다.

세 번째는 생산설비에 대한 파악이 어렵다는 사실이다. 대부분의 생산설비는 최초 설치 후 구동이 잘 이뤄지면 그 이후에는 관리가 되지 않는다. 게다가 생산설비는 생산에 문제가 없으면 10년 이상을 사용하기 때문에 업데이트 등 후속 서비스를 받기도 어렵다. 이렇게 계속되다보면 결국 공장에 어떤 장비가 얼마만큼 있는지 파악조차 어렵게 된다는 것이 OT보안 관계자들의 설명이다. 실제로 모 대기업의 보안전문가 역시 “OT보안에서 가장 어려운 것이 바로 생산설비에 대한 분석”이라며, “어떤 설비가 있는지 알아야 보안위협이 발생할 수 있는 지 분석할 수 있는데, 애초에 우리가 어떤 설비를 갖고 있는 지조차 모르기 때문에 위협을 분석할 수도 없다”고 지적했다.

OT/ICS 보안

“제 3자의 시각에서 바라보면 OT/ICS 보안을 위해 할 일이 명약관화함 "

사실 현장에서의 가장 큰 문제는 '생산'이 최우선인 공장운영자에게 OT보안 솔루션을 도입하도록 설득하는 것이다. 윈도우나 리눅스를 OS로 사용하는 보통의 생산설비는 한 번 설치하면 10~15년은 기본으로 사용하는데, 큰 고장만 없으면 시스템을 업그레이드하거나 심지어 펌웨어도 업데이트하지 않는다. 시스템이나 펌웨어를 업그레이드 하려면 반드시 생산설비를 멈출 수밖에 없고, 생산설비가 멈추면 생산이 멈추기 때문이다. 게다가 대부분의 생산설비가 서로 연결되어 있어서 한 번 업데이트를 하게 되면 그에 맞춰 다른 장비도 업데이트해야 하기 때문에 공장운영자는 아예 하지 않는 것을 선택한다. 대규모 생산설비에서는 한 번 생산을 멈추면 그 피해가 천문학적이기 때문이다.

이와 관련 한 OT보안 전문가는 “지금도 현장에 있는 생산설비는 대부분 윈도우 95나 윈도우 ME 같은 오래된 버전의 OS를 사용하고 있다”면서, “IT보안에서는 상상할 수도 없는 일이지만 생산시설에서는 당연한 일상”이라고 설명했다.

이에 보안전문가들은 OT보안 전문 컨설팅을 통해 먼저 생산시설 현장의 상황을 파악하는 것이 중요하다고 설명한다. 최근 OT보안 컨설팅에서 두각을 나타내고 있는 컨설팅 기업의 담당자는 “실제 생산시설의 보안컨설팅을 나가보면, 대기업도 100점 만점에 20점 이하가 대부분”이라며 현재 생산시설의 보안에 낙제점을 줬다.

“OT보안 컨설팅은 크게 4단계로 이뤄집니다. 자산식별과 업무분장, 디지털 자산 안전점검과 보안 솔루션 추천 순입니다. 생산시설에서는 수많은 장비와 기기들이 설치되어 있는데, 전부 파악이 안됩니다. 커다란 기계도 있지만, 온도를 재는 작은 센서와 같은 장비도 많기 때문이죠. 이에 먼저 자산을 식별한 후 업무를 분장하게 됩니다.”

OT/ICS 보안

“사고는 발생 가능하며 회복력 있어야 대응 가능, 제 시기에 맞는 업데이트 "

IT와 OT, 융합되는 상황...사고 발생 후 회복력 향상시킬 방안 찾아야

HOME > 이슈 > 주의

안티바이러스 제품 보안취약점 주의...최신 버전 업데이트 필수

길민권 기자 | 승인 2020.10.07 22:01

안티바이러스 제품에서 발생하는 보안 취약점을 악용해 권한상승 등 사이버공격 피해를 입을 수 있어 이용자들은 최신 버전으로 업데이트해야 안전할 수 있다.

최근 공개된 글로벌 안티바이러스 보안 취약점 내용은 다음과 같다.

OT/ICS 보안

“OT보안 관제 우선 구축 후 IT & OT 보안관제 통합관리”

원자위 보안장비 해킹시도 5년 간 약 17배 증가

중국 최근 5년간 해킹시도 80건…이중 80% 지난해에 집중

오유진 기자 | euj@newsprime.co.kr | 2020.10.02 11:07:32

[프라임경제] 국내 원자력 발전소 등에 대한 안전규제를 관장하는 원자력위원회(이하 원안위)의 보안장비에 대한 해킹시도 국가 중 중국이 전년 대비 1725% 증가한 69건을 시도한 것으로 드러났다.

국회 과학기술정보방송통신위원회 박대출 의원(국민의힘)이 원안위로부터 제출받은 자료에 따르면, 원안위 보안장비에 대한 연도별 해킹시도는 최근 5년간 △9건(2015) △9건(2016) △33건(2017) △59건(2018) △152건(2019) 매년 급증했다. 올 8월 기준 해킹시도는 72건에 달하는 것으로 확인됐다.

"랜섬웨어 감염돼 시스템 마비되자 응급환자 사망"

최은정 기자 입력 2020.09.25 18:00

독일 뒤세도르프대 병원…사이버 공격으로 사망자 나온 첫 사례

[아이뉴스24 최은정 기자] 랜섬웨어로 인해 병원 시스템이 마비되면서 응급환자가 다른 병원으로 이동 중에 사망하는 사건이 발생했다.

25일 뉴욕타임즈 등 외신 및 업계에 따르면 지난 10일(현지시간) 독일 뒤셀도르프대 병원 서버 30대가 랜섬웨어에 감염돼 데이터가 암호화됐다. 이로 인해 병원 IT시스템 등 상당 서비스가 불가능해졌다.

일주일 뒤인 지난 17일, 해당 병원은 시스템이 여전히 마비된 상태에서 한 여성 응급환자를 받지 못했고, 이 환자를 약 32km 떨어진 독일 서부 도시 부근 병원으로 이송 조치했다. 그러나 이 여성은 병원에 도착하기 전 사망한 것으로 알려졌다. 사이버 공격으로 인해 사람이 사망한 첫 공식 사례다.

OT/ICS 보안

“산업제어 시스템 보안 솔루션 활용한 보안 자산 및 취약점 발굴이 최우선 과제”

HOME > 뉴스 > 보안

“코로나19, 에너지·제조업 ICS도 위협”

김선애 기자 | 승인 2020.08.31 16:39 | 댓글 0

클래로티 “코로나19로 ICS 원격 액세스 증가하며 악용 공격 늘어”
상반기 발견된 취약점 70% 원격에서 악용…에너지·제조 수자원 분야 위험

[데이터넷] 에너지, 중요 제조업, 수자원 분야 산업제어시스템(ICS)도 코로나19로 촉발된 중대한 이버 위협에 직면했다. OT 보안 전문기업 클래로티의 '2020 상반기 ICS 리스크와 취약점 리포트 따르면 코로나19로 인해 이동이 제한되면서 ICS 네트워크에 대한 원격 액세스가 증가하면서 를 악용한 공격이 증가한 것으로 나타났다.

보고서에 따르면 상반기 ICS에서 발견된 취약점 70% 이상이 원격에서 악용될 수 있었으며, 특 에너지, 중요 제조업, 수자원 분야에서 심각한 취약점의 영향을 받는 것으로 분석됐다. 취약성 75% 이상이 높거나 중요한 CVSS 점수가 할당됐다. 미국 취약성 데이터베이스(NVD)의 ICS 취약 은 전년대비 10.3% 증가한 331, 산업제어 시스템 사이버 비상 대응팀(ICS-CERT) 권고 32.4% 증 한 105였다.

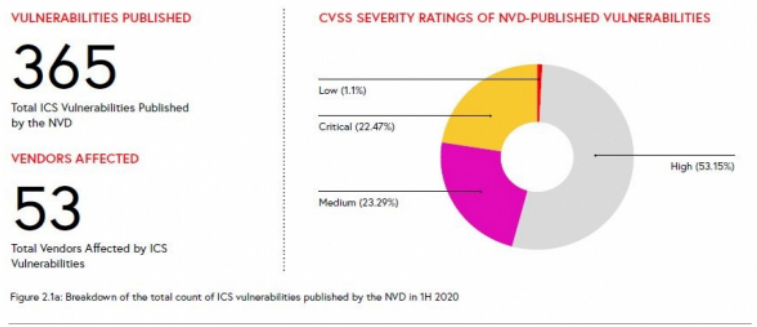


Figure 2.1a: Breakdown of the total count of ICS vulnerabilities published by the NVD in 1H 2020

[OT보안②] IT 보안 접근법, OT에 맞지 않아

김선애 기자 | 승인 2020.09.07 10:00 | 댓글 0

가용성 중요한 OT, IT 보안 기술 적용 어려워
IT-OT 보안 갭 줄여야…OT 보안 전문가 부족

[데이터넷] OT 보안 사고를 막기 위해서는 보안 체계를 갖추고 보안 시스템을 구축해야 하지만, OT는 IT와 같은 보안 체계를 갖추기가 어렵다. OT는 가용성이 생명이기 때문에 시설에 조금이라도 영향을 주는 조치를 취하지 못한다.

그래서 OT 네트워크의 이상행위나 침해 여부를 탐지하는 모니터링 시스템을 적용하기 어렵고, 네트워크가 어떻게 연결돼 있으며 어떤 기기가 접속돼 있는지 가시성을 파악하기도 힘들다. 각 설비마다 다른 프로토콜과 비표준 기술을 사용하고 있어 통합과 자동화가 쉽지 않다. 심지어 알려진 취약점 패치도 쉽지 않다. 패치 적용으로 인해 장애가 발생할 가능성이 있기 때문이다.

감사합니다.