정 보 보 호 학 회 지
제 30 권 제5호, 2020. 10

IT와 OT의 연계 증가에 따른 보안 취약점 개선 방안

한 은 혜*

요 약

본 논문에서는 일반적으로 외부와 격리된 환경이라고 생각하는 발전소, 공장과 같은 OT(Operational Technology) 환경에서 IT(Information Technology) 환경과 커넥션이 많아짐에 따라 각종 악성코드, 해커, Threat Actor 등으로 인해 취약해질 수밖에 없는 보안환경과 이에 대한 대응 방안을 소개하고자 한다. 본고에서는 최근 있었던 OT 관련사고 사례와 OT의 구성 항목에 대한 정의, IT와 차별되는 OT의 특징, 그리고 대응 방안으로써 보안 아키텍처, 가시성 확보, 관리 및 거버넌스에 대해 살펴보았다.

Ⅰ. 서 론

발전소, 공장 시설 등 OT(Operational Technology) 영역은 과거 폐쇄 망이라 외부로부터의 접근이 엄격히 통제되기 때문에 바이러스 등 악성코드의 위협에서 안전하다고 인식되어 왔다. 하지만, 새로운 기술 및 기능의 적용, 효율성 개선 추구 등의 영향으로 기존의 IT(Information Technology) 영역과 접점이 늘어나고, 연결이 많아짐으로 인해 더 이상 안전한 영역이 아닌 시대가 되었다. 발전소나 공장 시설의 경우, 장애 발생 시 기업에게는 엄청난 경제적 손실을, 국가에게는 거의 재난에 가까운 상황을 가져오게 된다. 외부에서 내부로 침투하기 위해 담을 넘고 수중으로 잠입하지 않고도 컴퓨터 앞에서 재난 상황을 일으킬 수 있는 시대가 온 것이다. 이에 OT는 무엇이고, OT보안 구축에 있어서 고려해야 할 부분이 무엇인지 짚어보자.

Ⅱ. OT 사고 사례

최근의 OT 시스템과 관련한 사고 사례를 살펴보자. 2019년 3월, 일주일간의 대규모 정전 사태는 베네수엘라의 위기라고 불려 질 정도로 심각했던 상황이었다. 이 사태는 세계에서 4번째로 큰 수력발전시스템인 베네수엘라의 구리(Guri Dam)에서 발생되었다. 구리 댐은 베네수엘라 전체 전기의 70~80%를 담당하고 있었다. 이 블랙아웃으로 인해 대중교통과 신호등이 멈추면서 교통 및 국가시설이 마비되었고, 병원 의료기기가 멈추면서 중환자 사망까지 이르는 상황이 발생했다. 해킹이라고도 했고, 테러리스트의 소행이라고도 했고, 방화라고도 했고 노후 시설로 인한 고장이라고도 했다. 원인이 뭐든 해당 사고로 인한 손실은 재앙에 가까운 수준이었다[1].

2019년 10월, 인도에서 발생한 원자력 발전소 사고는 백도어 악성코드를 활용한 해킹으로 원전관리 연결망을 감염시켰고 원전 1기 네트워크 가동이 중단되었다. 이 사고에서 북한 추정 해킹 조직 “라자루스”의 연루가 의심될만한 정황들이 나왔다.

당시 발견된 악성코드에서 2009년 한국에서 발생한 DDoS공격 때와 동일한 암호 코드가 발견되었다[2].

```
}
dword_4BEC7C = fopen(&FileName, "wb");
if ( dword_4BEC7C )
{
  sub_401F10(lpString2, 0);
  fclose(dword_4BEC7C);
  String1 = 0;
  v10 = 0;
  v11 = 0;
  v12 = 0;
  v4 = strrchr(a2, 92);
  lstrcpyA(&String1, v4 + 1);
  v5 = strrchr(&String1, 46);
  lstrcpyA(v5 + 1, "dat");
  v13 = sub_491DA0(a2, "dkwero38oerA^t@#");
  sub_491E30(v13, (int)&String1, &FileName);
  sub_491E70(v13);
  DeleteFileA(&FileName);
  Sleep(0x3E8u);
  result = 1;
}
else
{
  result = 0;
```

〔그림 1〕 인도 발전소 사고 관련 악성코드 (암호코드)

* 에스에스앤씨 주식회사 (대표이사, nonehan@secnc.co.kr)

미국에서도 2019년 방화벽(Firewall)의 취약점을 이용한 DDoS 공격으로 풍력·태양광 발전소 가동이 중단된 사례가 있었다[3].

에너지를 생산하는 발전소와 같은 OT환경에서 사고나 장애로 인한 가동 중단 사태는 엄청난 파급효과를 유발하게 되며, 만약 이런 거대한 사건의 시작이 작은 프로그램 코드에서 비롯되었다고 하면 OT에서의 보안은 새삼 중요하게 여겨질 것이다. 이처럼 OT와 기존의 IT와는 다른 접근 방식이 필요하다. 그럼 무엇이 이런 차이를 가져오는지 OT의 정의부터 알아보자.

Ⅲ. OT란?

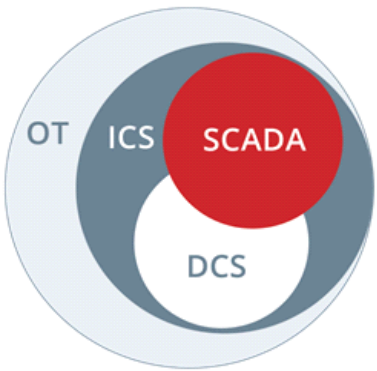
가트너에서 정의하기를 “OT란 산업 장비, 자산, 프로세스 및 이벤트를 직접 모니터링 또는 제어하여 변경을 감지하거나 유발하는 하드웨어 및 소프트웨어”라고 하고 있으며, 기존의 전통적인 IT(Information Technology)와의 기술적 기능적 차이를 나타내기 위해 만들어진 용어이다.

OT는 ICS, SCADA, DCS 등으로 구성되어 있으며, 각각의 구성요소에 대해서 알아보자.

* OT는 석유, 가스, 전기, 스마트 그리드, 제조 등 산업 운영을 관리하는 컴퓨팅 시스템을 말하며, 우리가 집에서 사용하는 전기나 수도 같은 시설이 잘 운영되도록 해당 시스템, 네트워크를 관리한다.
* ICS(Industrial Control System)는 시설이나 공장의 기계, 설비를 제어하는 미션 크리티컬한 시스템이다.
* SCADA(Supervisory Control and Data Acquisition)는 산업 현장 전체 또는 지리적으로 넓게 퍼져있는 산업 단지를 전반적으로 감시하고 제어하는 집중화된 시스템을 주로 일컫는다.

중앙처리센터, 로컬 컨트롤 시스템, 커뮤니케이션 시스템 등 3개의 구성요소로 이루어져 있다.

* DCS(Distributed Control System)는 컨트롤러, 센서, 터미널, 액츄에이터를 연결하는 프로세스 제어시스템이다. 이는 SCADA와 기능적으로 매우 유사하지만 중앙집권적인 시스템과 대조되는 개념으로 중앙조작자의 감시 제어가 존재하지 않는다.



〔그림 2〕 OT 영역 및 구성

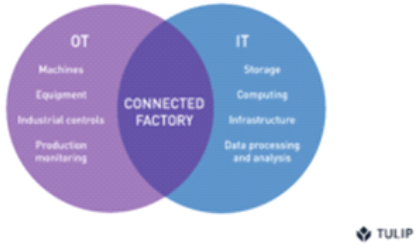
이처럼 OT는 에너지, 통신, 물, 폐기물 등 중요한 인프라를 직접 모니터링하고 제어하는데 사용된다. 이런 복잡한 시스템은 산업 현장에 필요한 발전기, 펌프, 밸브, 액추에이터 등의 장비에 필수적이다.

ICS 같은 경우 구축 및 유지에 비용이 많이 들어가며 100% 수준의 고가용성이 필요하다. 만약 이런 인프라가 공격을 받으면 앞에서 본 베네수엘라의 사태처럼 큰 재앙이 올 수도 있다.

3.1. IT보안 vs. OT보안

IT 시스템과 OT 시스템의 차이가 있듯이 보안의 관점에서도 차이가 있다.

IT보안은 기밀성이 최우선 순위이지만, OT 보안은



〔그림 3〕 IT와 OT 영역 및 컨버전스〔4〕

〔표 1〕 IT와 OT의 차이〔5〕

		IT	*OT*
기본 관점	보안의 우선 순위	C-I-A	A-I-C
	위협에 노출되는 요소	데이터	물리적인 대상
	패치 사이클	빠름	상황에 따라 대응
목적 기반 기술	기본 전략	데이터 보호	프로세스 보호
	프로토콜	표준화	등록(독자적 방법)
	위협성 분석 방법	위협성 기반	취약성 기반
사이버 보안 전문성	경험	IT 스택에 특화	특정 산업에 특화
	인증	IT 전반	도메인에 특화

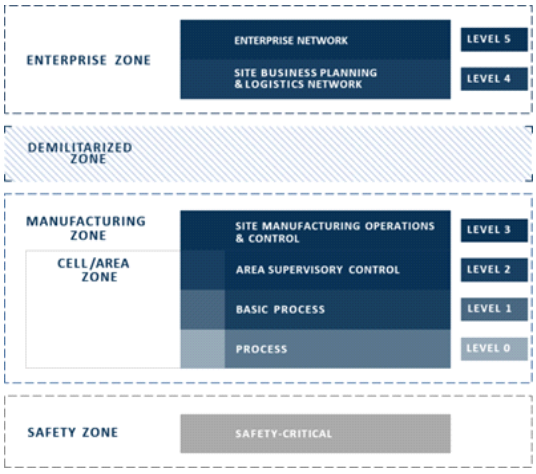
가용성과 무결성을 유지하면서 무엇보다 인간의 생명을 보호하기 위해 정보 위험을 줄이는 것을 목표로 하고 있다.

3.2. OT 환경의 변화

OT는 일반적으로 엄격하게 물리적인 통제가 시행되었으나, 이런 고립적 세계에도 극적인 변화가 일어나고 있다. 엔터프라이즈 네트워크 및 클라우드에 연결되어 빅데이터, 예측 관리, 스마트 분석 등에 활용되고 있다. 기업들은 경쟁에서 우위를 확보하기 위해 기술의 통합을 통해 새로운 기능과 효율성을 채택하고 있다. 오퍼레이션의 효율성은 증가하지만 사이버 위협에 대한 노출은 증가하고 있는 것이다.

이러한 IT와 OT의 컨버전스는 적절한 자산 인벤토리의 부족, OT 에 대한 가시성의 부족, 보안에 대한 제어 부족과 같은 새로운 보안 위험을 가져오게 되었다. 기존의 방화벽이나 네트워크 접근 제어 같은 표준 엔터프라이즈 보안 도구는 OT 영역에는 효과적이지 않을 수 있다.

학계 및 관련 보안 업계에서 OT 보안에 대한 이론적 참고 모델로 퍼듀 모델을 사용하고 있다. 퍼듀의 논리적 프레임 워크는 2004년 ISA99위원회에서 제정되었고, 5개의 구역과 6개 오퍼레이션 레벨로 구성되어 있다.ICS와 SCADA 보안 솔루션 등은 이 퍼듀 모델에 기반해 기술구조와 보안 요구 사항에 대응하는 제품을 출시하고 있다.



〔그림 4〕 제어 계층에 대한 전통적인 퍼듀 모델〔6〕

위의 모델에서 OT 의 영역은 Safety Zone에서 Manufacturing Zone 까지이고 IT 영역은 Enterprise Zone에 해당한다. 이 두 영역의 사이 즉 레벨 3과 레벨 4 사이에 이를 연결하는 DMZ가 존재할 수밖에 없고, 이는 결국 OT 환경에 영향을 주게 된다.

OT영역은 과거의 생각처럼 누구로부터의 침해도 받지 않는 영역이 아니라, 외부에 노출된 환경이 되었고 더 이상 불가침의 안전한 영역이 아닌 것이다.

그렇다면, 이 영역에 대한 보안은 어떻게 해야 할까?

Ⅳ. 보안 아키텍처

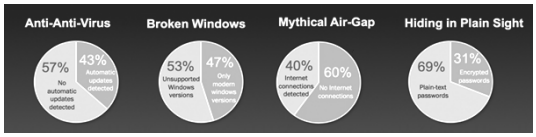
위의 퍼듀 모델에 기반한 보안 아키텍처의 설계가 필요하다.

다만, 해당되는 솔루션의 도입만이 중요한 것은 아니다. 예를 들어 가장 기본적인 보안 수단인 방화벽만 하더라도 기존의 IP, Port의 개념으로 차단/허용 대상을 인식하는 것이 아니라 실제 사용자, 어플리케이션으로 인식하는 것이 필요하고, 기업에서 최근 많이 도입하고 있는 SD-WAN 과 같은 가변적이고 효율적인 네트워크 환경에 대응하는 차세대의 방화벽 등이 요구될 수도 있다.

CyberX의 2020년 조사에 따르면 비즈니스 생존 가능성을 위협하는 OT의 취약성이 엄청나게 많음을 알 수 있다.

백신의 경우도 살펴보면 기존의 패턴을 지속적으로 업데이트해야 하는 시그니처 기반 블랙리스트 백신과 다르게 사전 정해진 프로세스만 허용하고 Lockdown할 수 있는 화이트리스트 기반 백신도 고려해 볼 필요가 있다. 이는 산업 환경 자체가 관련 시스템의 업그레이드

〔그림 5〕 퍼듀 모델에 기반한 보안 아키텍처〔7〕



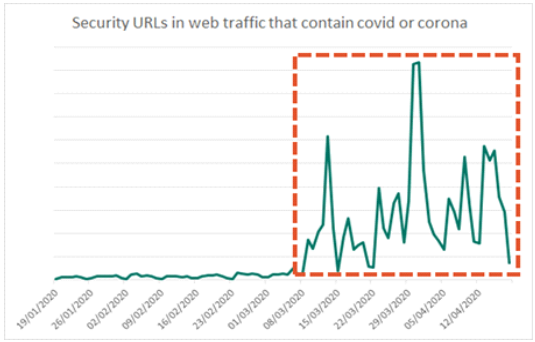
〔그림 6〕 2020 global IOT/ICS risk report〔8〕

가 10년 이상 비교적 장기간이며, 이에 따라 EOSL로 인해 더 이상 보안 업데이트가 진행되지 않는 경우가 다분하기 때문이다. 더 이상 보안 패치가 나오지 않고, 기술지원 조차 되지 않는 Windows XP 같은 OS의 사용이 이런 사례이다. 이런 경우 긴 프로젝트가 될 시스템 재구축시까지 화이트리스트 기반의 백신을 적용하면 리스크를 줄일 수 있을 것이다.

결국 모델의 개념에 맞게 솔루션을 도입하는 것과 병행하여 각각의 솔루션에 각 기업의 상황과 현재의 사이버 위협에 대한 트렌드를 반영하여 이에 맞는 솔루션의 선택이 필요하다.

최근의 악성코드는 엄청나게 빠른 속도로 진화하고 있다.

코로나 이후, 이와 관련한 악의적 웹 트래픽이 증가하고 있고, 암호화된 트래픽을 통해 전송되는 악성코드, 파일이 없는 Fileless 형태의 공격, 메일 전송 후 메일을 수신할 때쯤 URL의 실체를 바꾸는 기법, 웨일링 같은 이메일 해킹 기법처럼 수많은 공격 기법이 넘쳐나고 있다. 신기술을 이용한 빠른 공격이 늘어나고 있기 때문에 과거처럼 악성코드의 시그니처를 기반으로 한 방어로는 한계가 있다. 그래서 처음부터 아무것도 신뢰하지 않는다는 접근방식인 Zero Trust 모델이 보안솔루션에 적용이 되고 있다. 예를 들면 웹서핑을 하더라도 격리된 환경에서 해당 내용을 파싱하고 렌더링된 그래픽만 PC같은 엔드포인트에 전송해 줘서 악성코드의 실행 자체를



〔그림 7〕 COVID-19관련 악의적 웹 트래픽의 증가〔9〕

원천 봉쇄하는 기술 등이 그것이다. 일반적으로 RBI(Remote Browser Isolation) 라고 불리 우는 솔루션들이 이런 기능을 하는 솔루션 들이다. 이런 솔루션은 기존의 SWG(Secure Web Gateway) 가 가질 수밖에 없는 태생적인 한계인 악성코드의 발생과 발견 후 차단하기까지 걸리는 시간적인 갭을 없앨 수 있는 획기적인 솔루션이다. 다만, 다량의 트래픽 발생 시의 성능 저하 문제를 SWG 같은 다른 솔루션과의 결합 등으로 헷지할 수 있는 구성이 필요하다.

4.1. 가시성의 확보

아키텍쳐의 구현에 있어서 중요한 요소는 가시성의 확보이다.

피터 드러커의 말처럼 “측정할 수 없으면 관리할 수 없고 관리할 수 없으면 개선할 수 없다.” 라는 말에 덧붙여, 가시성을 확보하지 못하면 측정할 수도 모니터링할 수도 통제할 수도 없기 때문이다. 가시성이 확보되지 않으면, 최첨단 이지스함에 레이더가 없는 셈이다.

적재적소에 장비를 배치하고 Port Mirroring 등으로 트래픽을 모으고, 분석해야 하고, HTTPS (SSL/TLS) 같은 암호화 트래픽의 경우에도 이에 대한 가시성 확보는 꼭 필요하다.

지속적인 가시성을 확보해 비정상·이상 징후를 탐지해야 하고, 사고가 발생하더라도 원인 파악이 가능한 환경을 운영해야 한다.

4.2. 관리 및 거버넌스

관리 및 거버넌스 개선을 위해 R&R을 정의하고, 정책과 지침을 마련해야 한다.

OT보안 거버넌스에 대한 평가 및 설계, 그리고 원칙, 정책, 가이드, 운영 지침에 대한 문서화가 필요하다. OT보안 절차를 개선하기 위해 거버넌스 체크리스트, 설비변경 관리절차, 자산분류 관리절차, 사고 대응절차, 이동매체 관리절차, 협력사 보안관리 절차에 대한 검토 및 정책 수립이 필요하다. 또한 조직에 이를 적용하기 위해 조직 업무 프로세스 분석, OT신규 업무 정의 및 R&R의 설계가 되어야 한다.

OT보안의 추진은 People → Process → Technology의 순서로 진행하며, 아키텍처는 Network 설계 → 공정 Data 분석 → 자산 배치의 순으로 설계해야 한다.

OT보안과 관련한 국제 표준으로는 ISA/IEC 62443, NIST 800-82등이 있다. 국내에서는 한국인터넷진흥원(KISA)에서 만든 “스마트 에너지_사이버보안_가이드” (2019.12) [10] 가 있다. 이 가이드에서는 아래의 총 6개의 분야에 대한 보안 위협 및 보안 대책에 대해서 가이드를 제시하고 있다.

(1) 첨단 계량 인프라 (AMI)
(2) 에너지 저장 장치(ESS)
(3) 전기차(EV) 충전시스템
(4) 셀프 주유기 및 셀프 충전기
(5) 댁내 에너지 기기
(6) 에너지 관리 시스템(EMS)

Ⅴ. 결 론

금융이나 리테일에도 OT영역처럼 폐쇄 망이라고 여겨진 영역이 있다. 그래서 보안 프로그램의 설치나 패치, 보안 업데이트 등을 소홀히 하는 경우가 있었다. 내가 아는 어느 사이트의 경우에도 그런 영역에 WannaCry 랜섬웨어가 대규모로 감염되었고 심지어 다른 계열사까지 전파되어 감염된 사례가 있었다. 이런 사태가 일어나기 위해서 보안 홀(Hole) 은 하나면 충분하다. 99개를 막더라도 한 개만 열려 있으면 모든 게 점령되는 상황이다. 시대는 개방형으로 가고 있고, 클라우드가 대세고, 더 이상 on-premise만 고집할 수 없으며, 변화와 빠른 속도를 요구하며 효율성까지 만족시켜야 하는 상황이다. 따라서 우리는 기존 퍼듀 모델을 고집할 수는 없는 상황이고, 현재의 데이터 처리 환경에 맞는 새로운 프레임웍 모델을 구성해야 할 것이다.

일반적으로는 각 Zone마다 보안 제어는 방화벽으로 하게 되지만 클라우드 환경이나 인터넷 환경에서 정보를 처리해야하는 Level 4, 5와 핵심 Operation Process가 동작 및 제어하는 Level 0~3 간 트래픽을 완전히 차단을 할 수 없는 상황을 인지하고, 각 Zone 간의 DMZ 구간에 데이터 통신을 할 수 있는 ODTS (Operational Data Transformation System)이 필요하다. OT 기업 내에서의 더 많은 실시간 운영 데이터 처리에 대한 요구는 Level 3~4 에서 IT.보안 기술을 통해 위협 및 취약점을 제거한 환경에서 실시간 운영 데이터를 처리하고, 그보다 낮은 Level 0~3에서는 IT계층과는 분리하여 OT 영역으로의 Traffic을 차단하거나 강력한 통제를 적용하고, 낮은 계층 간의 Access만 이루어지게 하고 IT영역과 OT영역간의 데이터 통신은 각 기업 별 정규 화된 데이터로만 ODTS를 통해서만 이루어지게 한다. 이렇게 되면 IT영역과 OT영역 간의 장애 포인트가 달라서 IT 영역에서의 공격이나 장애사항이 OT로 영향이 직접 가지 않아 중요 업무 프로세스 및 데이터를 보호할 수 있다. IT영역에서는 Legacy 보안활동, 예를 들면, 관리 및 거버너스 체계의 개선, 보안 아키텍처의 수립, 조직 내부 상황과 외부 환경에 맞는 솔루션의 선택과 구축, 관련 조직의 R&R 정립, 등을 지속적으로 추진하여 보안 수준을 유지하는 활동을 꾸준히 진행하여야 한다.

참 고 문 헌

[1] wikipedia, https://en.wikipedia.org/wiki/2019_Venezuelan_blackouts
[2] VOAKorea, https://www.voakorea.com/korea/korea-politics/5147801
[3] ZDNET, https://zdnet.co.kr/view/?no=20191101154350
[4] Tulip, https://tulip.co/blog/iiot/it-ot-convergence/
[5] GE, https://www.gereports.kr/ot-security/
[6] https://owlcyberdefense.com/blog/how-iiot-and-the-cloud-are-upending-the-purdue-model-in-manufacturing/
[7] LGCNS, https://blog.lgcns.com/2021
[8] ARUBA networks, https://blogs.arubanetworks.com/solutions/use-automation-to-address-your-ot-security-challenges/
[9] Forepoint https://www.forcepoint.com/blog/x-labs/covid-coronavirus-web-email-traffic-analysis
[10] KISA, http://kisa.or.kr

〈저 자 소 개〉

한 은 혜 (Han Eun Hye)

정회원

2017년 2월 : 고려대학고 정보보호 대학원 석사

2020년 2월 : 고려대학교 정보보호 대학원 박사 수료

2018년 3월~현재 : 에스에스앤씨 대표이사

<관심분야> 전자공학, 통신공학, 정보보호