한국컴퓨터정보학회 동계학술대회 논문집 제24권 제1호 (2016. 1)

산업제어시스템을 위한 정보보호 관리체계 설계 방안 연구

조용현[O], 이은경[*]
[O*]소셜정보안전센터
e-mail: divayeyo@nposecurity.kr[O], yhjo@nposecurity.kr[*]

Design of Information Security Management for Industrial Control System

Young-Hyun Jo[O], Eun-Kyoung Lee[*]
[O*]NPO Security Center

● 요 약 ●

지난 5년간 대표적인 산업제어시스템(Industrial Control System)인 국내 원자력 발전소에 대한 해킹 시도는 총 1,843회로 사이버공격에 대한 위험은 날로 높아지고 있다. 이러한 공격은 사이버전, 테러, 사이버범죄자들에 의해 실행되고 있다. 이러한 위험을 통제하기 위해서는 산업제어시스템이 일반적인 IT시스템과 다른 운영체제, 네트워크 등 시스템 환경을 고려하여야 한다. 본 논문에서는 기존의 IT보안 대책과 산업제어시스템 보안 대책을 비교 분석하고, 국내외에서 발생하고 있는 산업제어시스템에 대한 공격 사례를 비교 분석하여 산업제어시스템 인프라에서 고려하고 통제해야 할 정보보호 요소들을 제언한다.

키워드: 산업보안(Industrial Security), ICS(Industrial Control System), 정보보호(Information Security)

I. 서론

산업제어시스템은 생산관리, 배치작업, 공작기계제어, 수송시스템과 전력시스템 등 석유, 가스, 식용수, 발전소 등의 산업 전반에서 사용되고 있다. 일반적인 IT 시스템에 비해 공중망과 분리되어 내부의 특정 장비들만 사용하는 내부 네트워크를 이용하고, 장비들은 임베디드 운영체제 및 통신 프로토콜을 이용하는데 사회기반시설 등 주요 기반시설은 서비스가 무중단 운영되도록 작동되고 있는 특징을 가지고 있다.

그러나, 시스템의 운영관리와 안전성을 이유로 지원이 종료된 윈도우 XP를 여전히 사용하고 있는 곳이 많으며, 폐쇄망이라는 이유로 이에 대한 보안관리를 소홀히 하는 곳도 많다. 이러한 위협은 내부자, 테러리스트, 사이버범죄자, 사이버전 국가 들에 의해 실행되고 있다.[1] 이러한 위험을 정보보호 관리 측면에서하기 위해서는 산업제어시스템의 보안환경의 특수성을 인지하여 기업의 IT보안 정책과의 비교를 통해 그 한계를 인지하고, 산업제어시스템의 가지는 취약한 보안이슈에 특화된 정보보호 관리 강화 방안을 모색하고자 한다.

II. 관련연구

1. 주요 정보보호 이슈 현황

산업제어시스템에 대한 공격을 통하여 공격자는 한 국가의 안보를 뒤흔들 수 있을 뿐 아니라 대혼란의 시기를 만들거나 사회 경제적 영향을 미칠 수 있으며, 다양한 방법으로 금전적인 이득과 해킹조직의 힘을 과시할 수 있는 수단이 될 수 있기 때문에 공격자의 주요표적이 되고 있다.

2010년 스턱스넷(Stuxnet)은 지멘스사의 SCADA시스템을 공격하는 독특한 악성코드가 발견되었다. 이 공격으로 이란의 5개의 핵시스템의 물리적 시설이 손상되었다.

2000년부터 2013년까지 JAPAN-CERTCC의 OSVDB에 등록된 제어시스템 취약점 추이에 따르면 이란 스턱스넷 사건이후로 취약점 발견건수가 급증하였다. 2014년 Dragonfly라는 공격은 공격자가 주로 에너지 기업을 목표로 하였다. 2010년 스턱스넷이 원자력 프로그램을 표적으로 하고 이를 파괴하는 것에 주력했지만, Dragonfly는 더욱 광범위한 표적을 노린 셈이다. 또한 샌드웜(Sandworm)은 GE 인텔리전트 플랫폼의 CIMPLICITY HMI 솔루션을 운영하는 윈도우 PC를 대상으로 공격하였다. 사람과 기계의 인터페이스인 HMI를 손상하는 악성코드를 유포하여 공격자가 또 다른 공격을 위한 백도어로 활용될 수 있었다.

미국 국토안전부 ICS-CERT는 2014년 10월부터 2015년 4월까지 모두 108번의 산업제어시스템을 공격하는 것에 대응하였다.

ICS-CERT는 에너지 부분의 산업제어시스템에서 가장 빈번한 공격을 받고 있다. 중요 제조부분과 물관련 산업에서 각각 20%와 19%를 차지하는 순으로 나타났다. 이러한 산업제어시스템에 대한 주요 공격 방법을 살펴보면 일반적으로 APT공격에 많이 활용되고 있는 Spear-Phishing이 가장 많은 비중을 차지하였다. 그 뒤를 네트워크 스캐닝을 통한 SQL 인젝션과 취약한 인증을 이용한 계정탈취 등의 공격으로 나타났다.

해외 사례를 통해 알수 있듯이 산업제어시스템의 경우 개인정보, 영업비밀정보를 외부로 유출하는 위협보다는 시스템 및 SW의 취약점이 악용되어 공정이 중단되거나 오동작을 유발하는 것을 가장 큰 피해로 볼수 있고, 국내 산업시설의 경우 메리츠 증권 리서치 센터에 따르면 글로벌 대기업 전자의 생산라인이 정전으로 일시 중단되어 생산중인 웨이퍼 손실, 생산 중단에 따른 손실, 라인 재가동에 따른 생산 효율 하락 손실 등으로 총 500억의 피해를 입은 것으로 조사되었다.

2. 산업제어시스템 보안사고 사례

2014년 일본 반도체 공장에서 품질 검사를 실시하는 검사 장치가 USB 메모리에 의해 악성코드에 감염되어 생산 라인이 정지된 사고 발생하였다.

2014년 공격자는 독일 제철소가 e메일에 첨부된 악성코드에 감염된 PC가 좀비PC가 되어 내부 정보를 수집하고 생산 설비의 제어 시스템을 해킹한 사고가 발생하여 용광로를 정상적으로 정지하지 못하고 생산 시설 손상되었다.

2010년 이란 원자력 발전소 SCADA 시스템이 이용하고 있는 운영체제 및 임베디드 OS의 보안 취약점을 이용하여 원심 분리기를 제어하는 PLC를 통해 주파수 변환 장치를 공격하여 원심 분리기에 과도한 부하 발생하여 원전이 중단되었다.

2008년 터키 파이프라인에 설치되어 있는 감시 카메라의 통신 소프트취약성을 이용하는 <표-2>와 같은 악성행위를 하는 코드를 추가한 공격으로 내부 네트워크에 침입한 공격자는 동작 제어 시스템에 접속하여 경보 장치의 동작 멈추고 관내의 압력을 이상으로 높이고 폭발을 유발하였다.

2005년 미국 다임러 크라이슬러 자동차 공장이 바이러스 감염에 의해 생산공정이 중지되는 사고가 발생하였다. 이로 인해 50,000명의 근로자가 50분간 생산을 중단하게 되어 약 1,400만달러의 금전적 손해가 발생하였다.

3. 해외 산업제어시스템 보안 동향

일본은 2014.4월 CSMS(Cyber Security Management System) 인증 제도를 통해 산업 제어시스템의 리스크 관리를 효과적, 효율적으로 실시하고 있다. 산업제어시스템의 보안 인증 규격은 산업 제어시스템의 특수성을 반영하여 기존의 ISMS(Information Security Management System)과 차별화된 규격을 가지고 있다. 두 개의 규격이 서로 다른점은 보안관리 대상의 범위로 ISMS는 정보 자산을 대상으로 하는 반면 CSMS는 산업 제어 시스템만을 대상으로 한다.

미국은 2003년 9월 국토안보부(DHS, Department of Homeland Security) 사이버보안부문에 US-CERT를 설립하였고 US-CERT내에 ICS-CERT를 운영하고 있다. 현재는 국토안보부 국가 사이버 보안 및 통신 통합 센터(NCCIC, National Cybersecurity and Communications Integration Center)의 부문으로 포함되어 미국 및 해외의 중요한 인프라섹터를 보호하기 위하여 법 집행기관 및 정보기관과 협력하고 연방정부와 주, 지역의 산업제어시스템 등 국가 및 민간부문의 산업제어시스템의 보안의 연구관리 및 개발, 취약점 분석 및 위협제거, 사고조사 및 지원하는 포괄적인 업무를 수행하고 있다.

III. IT보안 관리와의 비교

1. IT보안관리 사례

기업은 정보보호 관리체계를 구축하여 기술적, 관리적, 물리적 보안대책을 통해 외부위협과 내부정보유출을 방지하고 있다. 본 절에서는 기존의 기업의 정보보안 규정을 중심으로 한 IT보안 대책 및 사례가 산업제어시스템 환경에 적용하였을 때의 문제점을 살펴본다.

산업제어시스템은 일반적인 정보시스템과는 다른 서비스 응답, 통신 프로토콜, 네트워크 구조 등의 특성을 기반으로 하는 보안취약요인을 분석하고 그것을 토대로 사이버 공격에 대한 원격감시제어 시스템의 안전망 확보방안가 요구된다.[2]

SCADA 시스템 구축시 SCADA 네트워크에 연결되어 있는 모든 선로를 식별하고 불필요한 연결은 모두 차단하고 공인되지 않은 프로토콜에는 의존하지 않고 Backdoor에 사용되는 기능에 대한 통제와 내/외부 IDS를 설치, 운용함으로써 위험관리 프로세스를 적용해야 한다.[3]

SCADA 시스템은 SW적인 장애로 SW Fail, 통신 Fail, 이중화 동작오류, 오장비 이벤트 발생, 정상 이벤트 누락, 오장비 제어와 HW적인 장애로 통신 불량, 모듈 불량, 전원불량을 사례가 발생할 수 있어 이에 대한 서비스 가용성 대책이 요구된다.[4]

2. IT보안과 산업제어시스템보안과 비교

산업제어시스템의 보안관리는 기존의 IT 보안과의 차이점을 이해하고 시스템의 특수성을 바탕으로 새로운 관점에서의 접근이 필요하다.[5]

Table 1. IT보안과 산업제어시스템보안 비교

구분	ICS 보안	IT 보안
Security objectives	제조공정의 무결성, 가용성	자산의 비밀성
Network segmentation	모든 통신망으로 부터 ICS망의 분리	인터넷 연결과 내부 네트워크 연결
Network topology	네트워크 경로의 단순화	네트워크 경로의 복잡화
Functional partitioning	일반적인 TCP/IP아님	Ethernet 기반 ACL
Physical components	예) IT 기반에서 USB disable 불가	예) IT 기반에서 USB 통제 가능
User accounts	ICS에 특화된 계정을 사용	계정 변경이나 통제 IT관리자측에서 실시
Safety Instrumented Systems	안전한 공정을 위한 기능	없음
Untested software	화이트리스트 기반 SW 동작 조건	SW testing 환경 어려움
Patching	패치를 위한 시험, 승인, 일정, 검증 필요	신속한 패치 가능
Security inconveniences	보안이 적적성을 ICS운영팀과 협의 필요(예/패스워드 길이 등)	불편, 장애를 감수하고도 보호조치

3. 산업제어시스템 보안 고려사항

3.1 정보보호 관리체계

기존의 IT보안정책을 준용하였을 경우 가용성이 우선이 된 산업제어시스템 보다 비밀성 확보 조치의 영향으로 공정 시스템의 성능 저하, 품질 저하 등의 현상이 발생할 우려가 높다. 신규 생산라인의 구축이나 공장 설계 등에 있어서 보안정책이 수립, 반영되어야 하며 정보보호 부서는 도입되는 모든 생산, 제어 시스템의 입출력, 운영체제, 네트워크 구조의 BCP(Business Continuity Plan)을 최우선 순위에 두고 네트워크 이중화, 장애대책 마련, 백업 및 소산에 대한 검토가 요구된다.[6] 이와 유사한 정책으로 금융회사는 전자금융감독규정 제36조(자체보안성심의)에 근거하여 신규 서비스 및 대내외 영향도가 높은(전산센터의 신규 구축 등) 사업의 경우 중요정보자산에 대한 영향 및 보안성에 대한 분석을 통해 보안성을 확보하고 있다.

3.2 패스워드 설정 및 관리

검사장비, 측정장비, 제어장비 등 특수한 목적의 산업시스템들은 고유의 패스워드를 사용한다. 장비의 초기 패스워드는 변경하여 사용되어야 한다. 최근 발생한 기업의 폐쇄망 시스템의 해킹 경로도로 이 사고에서 IT Zone에서 사용되는 장비들의 Default password가 악성코드에 하드코딩된 형태로 전파되었고, 이 장비중 생산초기의 패스워드를 변경하지 않고 사용되던 시스템들이 피해를 입고 자동으로 전파되는 양상을 보였다.

3.3 아키텍쳐 및 디자인

산업제어시스템은 RTU and PLC Web을 사용하고 Ethernet port를 사용하면서 범용적인 시스템 형태로 변화되었다. 제어시스템도 Web 인증 및 page로 시스템의 동작과 운용을 제어할수 있기 때문에 OWASP(The Open Web Application Security Project)의 웹보안 표준안에 따른 접근통제 및 인증, 보안대책의 수립 여부, 장비 웹애플리케이션에 대한 보안 테스트가 요구된다. 폐쇄망 내에서의 악성행위 전이는 서버 Zone, IT Zone, 직원 Zone으로 각각 네트워크 분리된 것으로 판단된 환경에서 USB 및 보안관리상에 확인되지 않았던 네트워크 경로를 통해 발생하였다.

3.4 안티바이러스 탐지 및 차단

산업시스템망은 네트워크 구조가 다른 업무망 및 공중망과 차단된 환경이기 때문에 백신 업데이트 및 보안 패치 업데이트를 할 수 없다. 또한 이러한 안티바이러스의 설치, 동작에 따른 성능 이슈로 인해 보안관리자의 선택과 판단이 어렵다. 업데이트 또는 보안 패치되지 않은 시스템은 악성코드에 대한 탐지 및 차단이 불가하고, 제어시스템을 침투하는 악의적인 Zeroday 공격의 방어도 불가하다. 제어시스템망에서의 안티바이러스 대책을 수립하고 업데이트 및 보안패치에 대한 가시성을 확보하여 악성코드의 진입 초기 피해를 최소화 하고 시스템간의 전이, 생산라인간의 전이로 인한 피해가 확산되는 것을 방지하여야 한다.

3.5 운영체제 및 어플리케이션

제어시스템은 대부분 구동 연한이 일반 IT시스템에 비해 길기 때문에 오래된 버전의 운영체제를 사용하거나 패치 작업을 실시할 수 있는 환경을 구성하기에는 다양한 문제가 존재한다. 또한 보안설정 등의 강화조치가 생산 공정에 끼치는 영향을 예상할 수 없기 때문에 시스템 운영부서와 보안 부서간의 Role 충돌이 발생할 수 있다. 이를 위해서는 산업제어시스템은 Backup 시스템 및 DR 시스템과는 별도의 Test 시스템을 구성하여 안정화된 시스템 작업 환경을 구성하여야 한다.

Ⅳ. 결론

최근 발생한 원전 해킹 사례에서 볼수 있듯이 산업제어시스템에 대한 위협은 특정한 기업, 기관의 피해보다 조직 또는 국민의 재산과 생명과도 직결된다. 이 시스템은 전기, 수도, 자동차, 석유 등 산업의 기반시설로써 사이버 공격으로부터 보호해야할 핵심 기반시설이다. IT 시스템의 범용화로 지금까지 폐쇄적인 운영체제 및 통신방법을 사용하던 체계에서 오픈된 운영체제 및 범용망에서 사용되는 프로토콜로 변화되어 사이버 위협 또한 급증하고 있는 실정이다. 산업제어시스

템은 기존 IT보안 정책으로 보호대책을 수립, 적용하기에는 그 특수성 및 목적성이 큰 차이가 있어 그러한 요소를 고려한 정보보호 모델링이 필요하다.

본 논문에서는 이를 위해 산업제어시스템 및 위협사례, IT보안과 산업제어시스템 보안과의 차이점을 분석하고 산업보안 측면에서 고려해야할 주요 위협요인에 대해 제시하였다.

향후 연구로써 ISMS, ISO27001 및 일본의 CSMS와 같은 산업제어시스템의 보안표준과 인증방안을 마련이 산업보안 분야의 연구과제로 생각된다.

References

[1] Systems and Network Analysis Center, A Framework for Assessing and Improving the Security Posture of Industrial Control Systems (ICS), In National Security Agency at US, Release version1.1, 2010, p.2

[2] Kim Young Jin, A Study on the Secure Plan of Security in SCADA Systems, Korea Information Security Institute, Vol-No.19, 2009, p.145-p.152

[3] Kim Hueng Young, Information Security Strategy for The stability of SCADA System, Hanyang University, 2007

[4] Jung Sun Gil, A Study on Reliablity Improvement for SCADA System, Dankook University, 2011, p.15 - p.16

[5] Lee Neitzel, Bob Huba. Top ten differences between ICS and IT cybersecurity,2014, p.2-p.6

[6] Keith Stouffer. Joe Falco. Karen Scarfone. , NIST Special Publication 800-82, Guide to Industrial Control Systems Security, Recommendations of the National Institute of Standards and Technology 2: p.2.1 - p.3.6