ICS 거버너스에 대한 연구

김경태, 박양훈, 최선오
호남대학교 컴퓨터공학과
e-mail : kindking0787@naver.com, didgnsd16784@naver.com, suno@honam.ac.kr

A Study on ICS Governance

KyungTae-Kim, Yanghun-Park, Suno-Choi
Honam University Computer Engineering

요 약

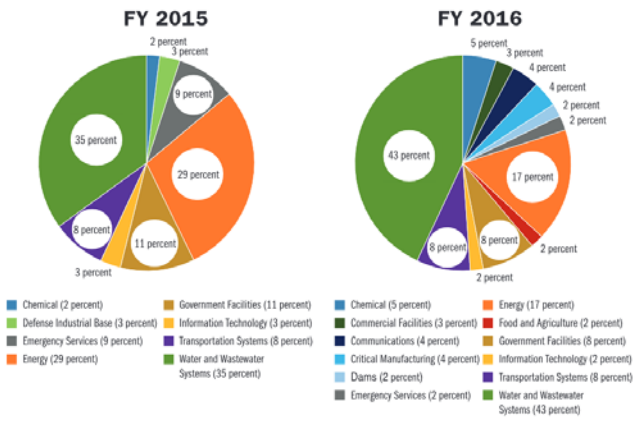
산업 제어 시스템(ICS, Industrial Control System)은 전력 생산, 물 관리, 석유 및 가스 생산, 원자력 발전 같은 국가 주요 인프라에 수많은 장비들이 제어시스템을 통해 관리 및 운영되고 있다.ICS 거버너스는 이러한 산업 현장에 적용되는 규제 및 정책으로써 사건사고 예방 및 사고 발생시 효과적인 대처방안에 대해서 설명한다.

1. 서론

전력 생산, 물 관리, 석유 및 가스 생산, 원자력 발전 같이 국가 중요 인프라을 제어하는 제어시스템은 정보통신기술을 활용하여 제어되고 있다. 이미 산업현장에서 장비들이 네트워크에 연결되어 효율적으로 제어되고 있지만, 네트워크에 연결된 이상 사이버 보안으로부터 안전하지 못하게 되었다.

미국의 경우, 제어 시스템 침투 및 파괴 가능성을 시험하여 취약점을 식별하고 대책을 세우기 위해 다양한 노력을 진행하고 있으며, 미국 원자력 규제 위원회(NRC)에서는 '원자력 설비를 위한 사이버 보안 프로그램'(RG, Regulateory Guide) 5.71과 같은 사이버 보안에 대한 새로운 규정 지침을 제시하고 있다[1].

본 논문에서는 효과적인 거버너스 수립을 통해 보안문제를 개선시켜 보안사고를 사전에 예방하고 사고 발생시 효과적인 대처방안으로 기업의 손실을 최소화하는 방법에 대해 연구하려고 한다.



<그림 1> ICS-CERT에서 대응한 사건 비율(2015~2016년)[2]

2. ICS 환경에서 다루는 데이터

보호해야 할 데이터는 ICS 환경내 여러 위치에 존재하며 시설 또는 엔터프라이즈 네트워크에 존재할 수 있다. 고려해야 할 데이터로는 운영 데이터, 프로젝트 파일, 펌웨어, 구성 및 설정파일, 논리/명령/프로그램, 프로세스 데이터, 기밀 자료등이 있다.

3. 보안 정책

3.1 정책 계층 구조

정책 계층 구조는 크게 3가지로 나뉘며, 최상위 조직에 대한 정책, 경영진에 의한 표준, 지침은 실무자 수준에 의해서 구현된다.

- 정책은 사업 목표와 목적를 자세히 설명하는 고급 문서를 말한다. 일반적으로 표준, 지침 및 절차를 언급하고 있으며 때때로 표준, 지침 및 절차가 관리 정책을 지원하기 위해 존재한다.
- 표준은 정책을 지원하기 위해 할 일에 대한 지침을 제공하는 일련의 요구사항이나 프레임워크를 말한다.
- 지침은 표준에서 확인된 항목을 달성하기 위한 접근 및 관행을 의미한다.

3.2 정책의 핵심 특징

정책은 책임 및 규정 준수에 대한 개요이다. 즉, 세부적으로 작성되지 않으며 "누군가가 해야 할일"을 다룬다. 또한 특정 절차가 개발될 수 있는 충분한 지침을 제공해야 한다.

3.3 정책이 고려해야 할 점

정책이 만들어질 때 여러가지를 고려해야한다. 법과 규정에 위배되지 않아야 하며, 다른 정책 수준(사명 선언문, 프로그램별 정책, 문제별 정책, 시스템별 정책)과 일치하는지 확인해야 한다. 또한 정책은 누구나 공평하게 적용되야 하며, 연중 검토를 통해 보완해야 한다.

3.4 보안 정책

보안 정책은 기본적으로 해당 지역의 컴퓨터 범죄법에 따라야 한다. 정보보호관리체계(ISMS, Information Security Management System)는 조직이 ISO 27001 표준을 기반으로 보안 정책을 공식화하는 과정이다. 보안이 필요한 정보와 수준을 고려한 다음 정책을 검토하여 정보가 사명 선언문 및 다음과 같은 다른 정책이 일치하는지 확인해야 한다.

- 프로그램별 정책 : 조직의 보안 접근 방식의 전반적인 톤을 설정한다. 일반적으로 이 정책은 다른 유형의 정책을 제정하고 책임 여부에 대한

지침을 제공한다.

- 이슈별 정책 : 조직내 특정 욕구사항을 해결하기 위한것으로 암호절차, 인터넷 사용 설명서등이 포함될 수 있다.
- 시스템 특정 정책 : 각 시스템에 개별적으로 적용되는 정책으로 모든 시스템을 관리하는 정책이 적절치 않을 때 사용한다.

4. 암호관리

4.1 ICS 환경에서의 암호

산업 제어 시스템은 이러한 환경 특유의 방식으로 비밀번호를 활용한다. 엔터프라이즈 응용 프로그램에 사용하는 것과 같은 방식으로 ICS에서 응용 프로그램 수준의 암호를 사용하지만 장소 및 암호 기능에 차이가 존재한다.

ICS는 다음과 같은 환경에서 암호를 사용한다.

- HMI 프로그램
- 장비 키패드
- 임베디드 웹 서버
- 진단 인터페이스(Telnet, RS232등)

4.2 IT 시스템과 ICS환경의 암호 기능 차이 비교

산업제어 시스템의 구조는 일반적인 IT시스템과 비교했을때 목적의 특성상 차이점이 있으므로 암호기능에 차이가 존재한다. 제어시스템은 특정한 장비를 전용으로 제어하기 위해 사용하므로 IT시스템보다 상대적으로 사양이 낮다. 그러므로 불필요한 리소스 낭비가 없어야 하며, 솔루션 패치나 업데이트로 인하여 장애를 최소화해야하는 특수성을 갖고 있다[3].

NERC CIP-007 표준은 가능한 경우 대화식 인증을 시행하기 위해 책임있는 방법론을 요구한다. 예를 들어 비밀번호 복잡성, 비밀번호 변경빈도, 인증 시도횟수 제한등

다음 <표 1>은 IT시스템과 ICS환경을 비교한 내용이다.

IT 시스템	ICS 환경
상대적으로 긴 비밀번호 길이	제한된 길이
복잡성(특수문자, 알파벳/숫자, 대소문자)	제한된 복잡성(일부 대소문자/일부 숫자)
자유로운 비밀번호 재사용 횟수 및 만료기간	제한된 비밀번호 재사용 횟수 및 만료기간
비밀번호 해쉬화	상대적으로 취약한 암호화의 광범위한 사용
기본 비밀번호 제한	하드코딩되지 않은 기본 암호의 광범위한 사용
디렉토리에 암호 통합	RADIUS 프로토콜을 통한 디렉토리 통합 지원

<표 1> IT시스템과 ICS환경의 암호기능 차이 비교

5. 위험 평가 및 검사

5.1 위험접근

두 가지의 위험 평가 방법이 있다. 첫번째로 정량적 위험평가에서는 객관적인 수치 값을 할당하려고 할 때 일반적으로 이값을 금전적 손실 값이라고 하는데 정성적 위험평가보다는 무형의 가치를 다루고 금전적 손실뿐만 아니라 변수에 초점을 맞춘다.

두번째로 정성적 위험평가는 수행하기가 훨씬 쉽고 위험이 높은 영역을 식별 할 수 있다. 예를들어, 조직에 무선 LAN 액세스 포인트 설치로 인한 영향을 확인하려면 위험평가 과정을 수행해야 한다. 비즈니스의 첫번재 순서는 취약점, 위협 및 무선 LAN 사용의 위험을 파악하는 것이다. 그런 다음에 해당 위험이 조직에 적용되는지 판단하고 위험에 처할 가능성을 결정합니다 무선 LAN을 사용하는 위험 중 하나는 누군가가 무선 네트워크 트래픽을 스니핑 할 수 있고 액세스 포인트가 잘못 구성된 경우 불량 클라이언트 연결을 허용 할 수있다는 점입니다. 위험을 수용, 경감 또는 이전하는 것을 결정하려면 위험을 잘 이해하고 우리에게 어떤 영향을 끼치는지 알아봐야 한다.

5.2 위험우선순위

ICS 응용 프로그램은 시스템이 제대로 작동하지 않거나 잘못 사용될 수 있는 경우 관련된 결과로 측정할 때 특정 시스템이 제공하는 기능에 의해 우선 순위가 결정된다.

- 레벨0 - 안전 및 비상조치 및 종료
- 레벨1 - 제어
- 레벨2 - 감독 통제
- 레벨3 - 모니터링 및 경고
- 레벨4 - 원격 측정 전용
- 레벨5 - 보조서비스

5.3 위험계산

단일 손실 기대 계산법 (SLE)

➔ 자산 가치($) x 노출 계수(EF)

연간 손실 기대치 (ALE)

➔ 단일 손실 기대 x 연간 요금 발생률(ARO)

6. 결론

본 논문에 나온 것처럼 ICS 환경은 일반적인 IT시스템과 다른 특성을 가진 탓에 ICS 환경에 맞는 거버너스가 수립되어야 한다. ICS/SCADA는 주로 국가 기반시설을 다루기 때문에 고려해야 할 항목들이 많다.

이미 알려져 있는 보안문제의 취약점을 미리 인지하여 사전에 방지하고, 사고가 일어날 시에는 기업에 최대한 피해가 가지 않는 방향으로 오류를 즉시 발견해서 피해가 더 커지는걸 막아야한다.

참고 문헌

[1] U.S NUCLEAR REGULATORY COMMISSION, “REGULATORY CUIDE 5.71”, JANUARY 2010.

[2] U.S CERT z`NCCIC, ICS-CERT (FY 2016 Assessment Report)

[3] 한경수외, "산업제어시스템을 위한 사이버 보안 시스템적용 방안", 한국정보처리학회 논문집, 2011, 11, P775