산업제어시스템 사이버침해사고 대응체계 프로그램 개발

김은지, 김주연, 윤선우, 윤주혜
성신여자대학교 융합보안(공)학과
e-mail : eungimin@naver.com, juyeon967@gmail.com, nus0205@naver.com, wngp0805@naver.com

Development of Cyber Incident Response System Program of Industrial Control System

Eun-Ji Kim, Ju-Yeon Kim, Seon-Woo Yun, Joo-Hye Yoon
Dept. of Convergence Security, Sungshin Women's University

요 약

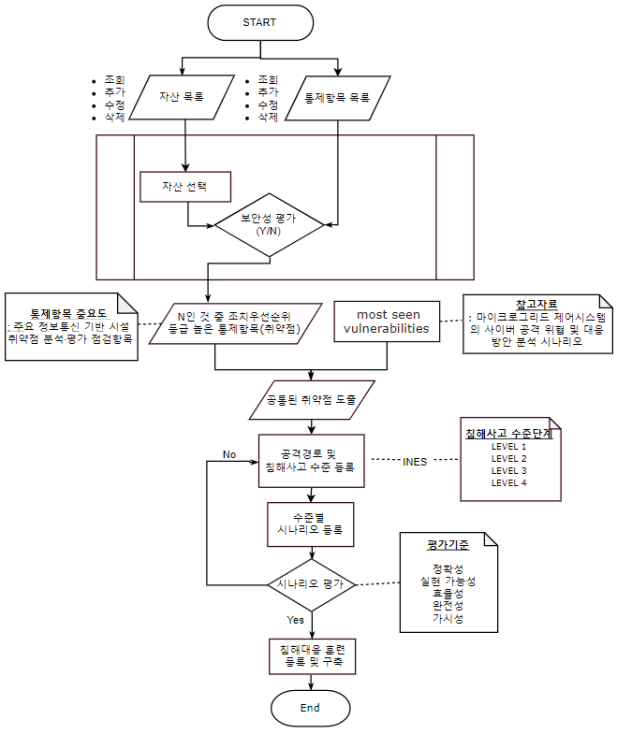
최근 국가기반시설 산업제어시스템은 시나리오를 기반으로 시뮬레이션 훈련을 진행한다. 그러나 국내 ICS 보안 기술은 외부 경계 보호에 중점을 둔 시나리오가 대다수였기 때문에 내부에서 발생할 수 있는 시나리오 가이드라인이 상대적으로 부족하고 이를 평가하는 기준 또한 제대로 정의되어 있지 않다. 내부 공격이 증가함에 따라 국내에서도 사회공학적 기법에 초점을 둔 시뮬레이션 훈련을 진행할 필요가 있다. 이에 본 논문은 NEI 08-09 의 운영·관리항목 중 가장 빈번하게 발생하는 위협을 바탕으로 한 시나리오 및 구성요소를 개발하고, 이를 평가할 수 있는 명확한 기준을 제시하여 효과적인 비상대응 훈련을 수행할 수 있도록 한다.

1. 서론

산업 제어 시스템(Industrial Control System, ICS)은 국가적 규모의 산업기반시설 및 그 규모에 따라 원거리에 산재한 여러 산업 설비들을 감시하고 제어하는 시스템을 통칭한다[1]. 과거 산업제어시스템은 폐쇄적이고 독점적인 제어 프로토콜을 활용하는 시스템이었지만, 여기에 IT 시스템을 결합하며 네트워크화가 이루어졌다. 이에 따라 기업들은 외부 공격에 초점을 맞춘 시나리오를 중점으로 시뮬레이션 훈련을 진행했다. 외부 대응체계가 구축되었지만 여전히 산업제어시스템은 사회공학적 공격 기법에 의해 쉽게 공격받고 있다. 실제로 산업제어시스템은 사회공학적 공격 기법에 취약한 모습을 보이곤 한다. 이는 산업제어시스템 내부에도 취약점이 존재하며, 운영·관리적 조치가 미흡한 상황임에도 불구하고 대응체계가 제대로 검증되어 있지 않기 때문이다. 이에 본 논문은 보안 취약점을 활용한 사이버 공격 시나리오 개발 절차와 시나리오 평가 기준을 포함한 '산업제어시스템 사이버침해사고 대응체계 프로그램'을 제안한다. 또한, 본 프로그램을 통해 국내 산업제어시스템의 운영·관리적 보안성 평가를 수행하고 시나리오를 작성할 수 있도록 한다. 이는 향후 사이버 공격 침해사고에 능동적이고 체계적인 훈련을 수행함으로써 대응 능력 향상을 기대해 볼 수 있다는 결론을 제시한다.

2. 본론

2.1 시스템 기능



<그림 1> 시스템 흐름도

본 논문은 과학기술정보통신부 정보통신 창의인재양성사업의 지원을 통해 수행한 ICT 멘토링 프로젝트 결과물입니다.

본 프로그램은 NEI 08-09 기반의 통제항목을 바탕으로 산업제어시스템의 자산 취약점을 평가할 수 있다. 또한, '주요 정보통신 기반 시설 취약점 분석평가 점검항목'과 '마이크로그리드 제어시스템의 사이버 공격 위협 관련' 논문에서 공통되는 주요 취약점을 찾아 취약점이 가장 빈번하게 발생한 횟수 기준으로 우선순위를 매겼다. 이 우선순위에 따라 보안성 평가 결과(Y/N) 중 'N'으로 평가된 취약점을 바탕으로 공격 시나리오를 개발할 수 있다. 이때, 시나리오를 개발하기 전에 침해사고 수준단계(Level1~4)를 먼저 설정하기 때문에 사고 수준이 편중되는 것을 막아 다양한 사고 유형의 시나리오를 작성할 수 있도록 하였다. 작성이 완료된 시나리오는 세 편의 논문 및 연구결과를 통해 도출된 다섯 가지의 평가기준에 의해 상, 중, 하로 평가된다. 이처럼 체계적인 과정으로 개발된 시나리오를 기반으로 침해대응 훈련 프로세스를 구축할 수 있도록 한다.

프로그램 기능은 다음 <표 1>과 같이 크게 7가지로 나누어진다.

<표 1> 프로그램 기능

프로그램 기능	상세 기능
통제항목 관리	• NEI 08-09 기반의 운영·관리적 통제항목 등록/조회/수정/삭제
통제항목 기준 자산 평가	• 통제항목에 대한 자산의 평가 • 점검항목 및 조치사항 기입
보안성 평가 결과	• 운영·관리적 통제항목 기반 보안점검사항에 따른 취약점 평가 수행 및 점검 결과 제시 • 취약점 제거 위한 조치사항 제시
비상사건 관리	• 기존에 발생했던 침해사고 관리
시나리오 관리	• 도출된 취약점을 통한 사이버침해사고 수준 별 시나리오 등록/조회/수정/삭제
시나리오 평가	• 연구를 통해 도출된 평가기준을 통한 시나리오의 정량적 평가
침해사고 대응 훈련 관리	• 침해사고 대응 훈련 일정 및 훈련 종류 • 훈련 대상 및 경로 등록

2.2 시나리오 관리 기능

위 프로그램의 기능을 효과적으로 사용하기 위해서는 몇 가지 연구결과가 필요했다.

먼저 시나리오의 침해사고 수준을 개발하기 위해 관련 지표를 참고하였다. 원자력 발전소에서는 침해사고 수준을 INES의 7단계로 분류하여 사고 등급평가를 수행한다. 설비의 고장 또는 기능을 상실한 경우 고장(Incident)으로 정의하여 1~3등급을 부여하고, 실제 방사선 노출 사건 및 발전 설비 정지는 사고(Accident)로 정의하여 피해 정도에 따라 4등급 이상으로 분류하고 있다. 이외에 안전에 중요하지 않은 사건에 대해서는 등급 이하(0등급)로 분류하고 있다. 이처럼 국제 원자력 기구(IAEA)의 국제 원자력 사고 등급(INES)은 고장 및 사고 분류체계 관점에서 기준을 7단계로 정의하였지만, 본 프로그램에서의 사이버 침해사고 수준 등급은 IAEA의 4등급 수준으로 축소하여 재정의하였다. 이는 단일 시스템을 대상으로 한 사이버 공격에 의해 Level 5, 6 수준의 방사선 노출 사건이 발생할 확률은 낮기 때문에 IT 관점에서 보았을 때 적합할 수 있게끔 Level 4 이하 수준으로 재정립한 것이다.

이를 바탕으로 본 논문에서는 다음 <표 1>과 같이 제어시스템에 범용으로 적용할 수 있는 사이버 침해사고 수준 등급 기준을 설계하였다.

<표 2> 침해사고 수준 등급

분류	침해사고 수준	기준
사고	LEVEL 4	사이버 공격으로 인해 시스템 설비 정지 발생
고장	LEVEL 3	사이버 공격으로 인해 시스템 설비 성능 저하 발생
	LEVEL 2	사이버 공격으로 인해 제어시스템 단순 고장 발생
	LEVEL 1	사이버 공격 정황 발견

본 논문에서 제시하는 프로그램은 보안성 평가에서 도출된 취약점을 침해사고 등급 기준에 따라 분류하고, <그림 2>과 같은 시나리오를 작성하는 것을 목적으로 한다.

본 논문은 과학기술정보통신부 정보통신 창의인재양성사업의 지원을 통해 수행한 ICT 멘토링 프로젝트 결과물입니다.

ICS 설비는 패치 업데이트를 위해 180일에 한 번씩 외부망과 연결된다. 해커는 이를 노리고 외부망에 연결된 시스템을 장악하기 위해 수 개월 전부터 APT 공격을 준비했다. 해커는 키로거를 이용해 관리자의 이메일 계정을 탈취해 ICS 설비들의 업데이트 시기를 유추했다. 쇼단(Shodan) 검색엔진을 이용하여 산업제어시스템과 인터넷 망과의 연결 경로를 확보하고 유추한 업데이트 시기를 기준으로 해서 지속적으로 침입을 시도했다. ICS 설비가 업데이트를 위해 외부망에 연결됨과 동시에 해커는 ICS 침입에 성공하고 최상위 권한을 탈취해 내부 시스템을 장악했다. 해커는 C&C서버 통신을 이용해 지속적으로 ICS 정보를 수집하고 ICS의 기능을 마비시켰다. 해커는 최종적으로 ICS의 안전장치를 파괴하려고 시도했지만 관리자가 백업되어있던 OS를 통해 설비 안정화 조치를 취하고 ICS는 다시 정상 작동되었다.

<그림 2> 시나리오 Level2(단순 고장) 요약 예시

<그림 2>은 사이버 공격을 당했지만, 해당 설비 하나만 마비됐기 때문에 침해사고 수준이 Level 2(단순 고장)에 속한다. 이처럼 시나리오의 침해사고 수준을 설정할 시 사고의 심각도가 일관성 있게 작성된다. 이때 시나리오를 평가할 수 있는 객관적인 기준이 존재한다면, 시나리오를 작성할 때 평가기준을 고려하며 작성할 수 있어 실제 시나리오 기반 훈련 시 발생할 수 있는 오류를 최소화할 수 있다. 본 논문에서는 시나리오 평가 방안을 연구한 세 편의 논문 및 연구 결과 중 2개 이상 공통되는 사항을 바탕으로 다음과 같은 평가기준을 개발하였다.

2.3 시나리오 평가 기준

기준	설명	대표 참고 문헌
정확성	시나리오에 기술된 설비 및 기능, 취약점 등이 제어시스템 상황과 정확하게 일치하는지 여부	・원자력시설의 사이버보안 훈련을 위한 시나리오 평가 방법에 관한 연구[2] ・사이버 보안실 2016년도 운영 보고서[3]
실현 가능성	사이버 공격의 발생 원인과 결과가 실제 실현 가능한지 여부	・원자력시설의 사이버보안 훈련을 위한 시나리오 평가 방법에 관한 연구 ・사이버 보안실 2016년도 운영 보고서
효율성	초동조치 설정과 해당 조치의 피해 경감 여부	・원자력시설의 사이버보안 훈련을 위한 시나리오 평가 방법에 관한 연구 ・서울시 시나리오 개발방안[4]
완전성	시나리오에 기술된 Task 별 Activity 및 R&R 등이 빠짐없이 기술되어 있는지 여부	・사이버 보안실 2016년도 운영 보고서 ・서울시 시나리오 개발방안
가시성	Timeline에 따른 대응임무 나열 및 임무의 목표 도출 여부	・사이버 보안실 2016년도 운영 보고서 ・서울시 시나리오 개발방안

<표 3> 시나리오 평가 기준

첫째, 제어시스템의 환경에 적합하게 공격 시나리오를 작성해야 한다는 사항은 시나리오에 기술된 위협, 공격 대상 시스템, 공격 기법이 해당 제어시스템의 상황을 정확하게 반영하였는지 검토하는 '정확성'으로 해석하였다.

둘째, 현실적인 공격기법 및 피해 규모를 산정하는 사항은 실제로 실현 가능한 공격인지, 피해 규모가 해당 공격으로 발생 가능한 결과인지 등을 검토하는 '실현 가능성'으로 해석하였다.

셋째, 각 주관 기관, 주체별로 초동조치방법을 명시하고 해당 조치가 피해를 경감해야 한다는 사항은 '효율성'으로 해석하였다.

넷째, 시나리오에 각 주체별, Task 별로 임무가 명시되어 있으며, 임무 수행을 통해 달성해야 하는 목표를 빠짐없이 설정해야 한다는 사항은 '완결성'으로 해석하였다.

마지막으로, Timeline에 따라 대응 절차를 순차적으로 나열하는 것은 대응 임무의 시간 흐름을 한 눈에 직관적으로 파악할 수 있다는 점에서 '가시성'으로 해석하였다.

2.4 프로그램 상세 로직

2.4.1 시나리오 관리 기능

<그림 3-1> 시나리오 관리

시나리오 관리 기능에서는 보안성 평가 기능에서 도출된 취약점을 활용하여 사이버 침해사고 수준별 시나리오를 등록할 수 있다. 본 프로그램에서는 과학기술부가 발간한 「사이버 안전분야 위기대응

본 논문은 과학기술정보통신부 정보통신 창의인재양성사업의 지원을 통해 수행한 ICT 멘토링 프로젝트 결과물입니다.

실무매뉴얼」부록에 기재된 프로세스 기반으로 시나리오를 작성하도록 한다. 시나리오 Activity에서는 Timeline 별 대응 방법을 상세히 기재할 수 있다. 이 기능을 통해 Timeline에 따른 시나리오의 흐름을 한 눈에 파악할 수 있다. 또한, Timeline에 따른 시나리오의 완료조건을 통해 정확한 훈련 프로세스를 구축할 수 있도록 한다.

2.4.2 시나리오 평가 기능

<그림 3-2> 시나리오 평가 결과

등록된 시나리오는 평가 기준(정확성, 실현 가능성, 완전성, 효율성, 가시성)에 따라 정량적으로 평가된다. 이를 통해 시나리오의 품질 수준을 보장하여 완성도 있는 대응 훈련을 기대할 수 있다.

2.4.3 침해대응훈련 기능

<그림 3-3> 침해대응 훈련 목록

침해사고 대응 훈련 관리 기능은 등록된 시나리오에 해당하는 침해사고 대응 훈련을 진행하여 실제 유사 사건 발생 시 능동적인 대응을 할 수 있게 한다. 침해사고 대응 훈련을 등록할 때 훈련종류, 일정, 장소, 부서 등 자세한 정보를 기재할 수 있도록 하여 사용자는 정교한 계획을 세울 수 있다. 또한, 침해사고 대응 훈련 프로그램은 일자 별 훈련 등록 기능을 포함하고 있다. 이로 인해 사용자는 Timeline 순으로 정렬된 훈련 내용을 순차적으로 확인하고 수행자들은 해당 날짜에 수행해야 할 훈련을 상세히 확인할 수 있어 체계적인 훈련을 진행할 수 있다.

2.4.4 비상사건 관리 기능

<그림 3-4> 비상사건 관리

실제로 발생했던 침해사고를 등록, 조회할 수 있는 기능이다. 등록 화면에서 해당 사건이 발생했던 날짜, 영향을 받은 자산과 침해수준을 선택하고, 사건의 Timeline을 단계별로 작성한다. 이 기능을 통해 침해사고가 가장 많이 발생했던 자산과 기간을 확인할 수 있어 추후 침해대응 훈련 계획을 수립하는 데 도움을 준다.

3. 결론

본 논문에서는 사회공학적 공격으로부터 위협받는 산업제어시스템의 '사이버 침해사고 대응체계 프로그램'을 제안한다. 제안하는 프로그램은 시나리오의 평가 지표가 될 연구 결과를 바탕으로 새로운 평가 기준을 제시해 체계적인 시나리오 및 훈련의 질을 보장할 수 있다. 그 결과 기존 프로그램과 비교했을 때 보다 완성도 있는 평가기준을 통해 효과적인 시나리오 작성을 할 수 있을 것이라 기대한다. 향후 외부 뿐만 아니라 내부 위협을 함께 줄여 나가는 것이 국내 ICS 산업의 연구과제로 생각된다.

4. 참고 문헌

[1] 김현석, 박동규, "산업 제어 시스템 보안을 위한 패킷 분석 기반 비정상행위 탐지 시스템 구현", 2018

[2] 한국원자력통제기술원, "원자력시설의 사이버보안 훈련을 위한 시나리오 평가 방법에 관한 연구"

[3] 한국원자력통제기술원, "사이버 보안실 2016년도 운영보고서", 2017

[4] 원종석, "현장대응자료 연계 서울시 재난사고 시나리오 개발방안", 2017

본 논문은 과학기술정보통신부 정보통신 창의인재양성사업의 지원을 통해 수행한 ICT 멘토링 프로젝트 결과물입니다.