원자력시설에 대한 설계기준위협 중 내부자 위협에 대한 사이버보안 강화 방안

송동훈*
한국원자력통제기술원, 대전광역시 유성구 유성대로 1534
*igiveitashot@kinac.re.kr

1. 서론

원자력시설의 주요 기능을 담당하는 컴퓨터 및 정보 시스템이 아날로그에서 디지털로 변화함에 따라, 이란 부세르 원전을 감염시킨 스턱스넷(Stuxnet), 일본 몬주 원전에서의 정보 유출 및 한수원 해킹 사건 등과 같이 사이버공격의 대상이 되고 있다.

이에 대한민국 정부는 원자력시설에 대한 사이버보안을 강화하기 위해 원자력시설 등의 방호 및 방사능 방재 대책법령(이하 방사능방재법령)을 개정함으로써 원자력시설에 대한 사이버보안을 강화해 나가고 있다.

근래 들어 사이버보안의 중요성이 대두됨에 따라 사이버보안에 대한 인식이 재고되었고, 사이버보안 요건이 강화되는 등 사이버공격의 주경로인 인터넷망 등 외부 위협에 대한 사이버보안이 강화되었다. 하지만 원자력시설에 접근 가능한 내부자에 의한 내부 위협은 여전히 사이버보안 강화가 필요한 실정이다.

본 연구에서는 한국원자력통제기술원의 기술기준(KINAC/RS-015)을 토대로 내부자 위협에 대한 사이버보안 요건을 도출하여 원자력시설에 대한 사이버보안을 강화하는 것을 목적으로 한다.

2. 본론

2.1 내부자 위협 반영 절차

Fig. 1은 방사능방재법령에 따른 위협 평가 절차를 나타낸다. 원자력시설은 신규 위협의 요인, 발생 가능성 및 발생에 따른 결과를 평가하여 3년 또는 필요시 설계기준위협을 개정하여야 한다. 개정된 설계기준위협에 따라 시나리오별 위협·대응 시나리오를 작성 및 평가하여, 설계기준위협을 방호할 수 있는 사이버보안 방호체계를 구축하여야 한다. 내부자 위협 평가 역시 Fig. 1과 같이, 동일한 절차를 따른다.

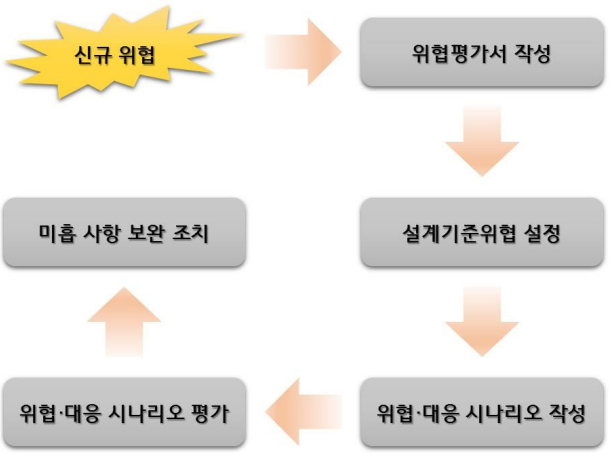

Fig. 1. Process of a Risk Assessment.

2.2 내부자 위협에 대한 사이버보안 요건

KINAC/RS-015의 기술적, 운영적 및 관리적 사이버보안 요건 중 내부자 위협을 방호하기 위한 요건들을 Table 1과 같이 도출하였다.

Table 1. Minimum Requirements of KINAC/RS-015 to Protect an Insider Cyber Threat

RS-015 No.	Name of Security Controls
1.1.16	Access Control for Portable and Mobile Devices
1.3.4	Resource Priority
1.4.1	User Identification and Authentication
1.5.2	Host Intrusion Detection System
2.2.2	Malicious Code Protection
2.3.1	Maintenance Tool
2.4.4	Physical Access Control
3.1.4	Developer Security Testing

2.2.1 기술적 보안통제

내부자는 원자력시설에 접근할 수 있는 사람으로서 물리적방호 요소인 검문, 검색 등을 어렵지 않게 통과할 수 있다. 따라서 컴퓨터 및 정보 시스템을 내부자 위협으로부터 보호하기 위해서는 시스템상의 기술적 사이버보안 대책이 필요하다.

2.2.1.1 휴대용 매체 접근 통제

컴퓨터 및 정보 시스템에 등록된 휴대용 매체만을 사용할 수 있도록 설정하여, 내부자가 악성코드가 담긴 휴대용매체를 접속하여 사용할 수 없도록 차단해야 한다.

2.2.1.2 필수 프로세스 목록에 대한 우선권 부여

컴퓨터 및 정보 시스템의 정상 운전 시 실행되는 프로세스 간의 우선순위를 설정하여, 내부자가 악성코드와 같은 우선순위가 낮은 프로세스를 실행시킬 수 없도록 차단해야 한다.

2.2.1.3 사용자에 대한 식별 및 인증 체계

컴퓨터 및 정보 시스템의 등급에 따라 사용자를 식별할 수 있는 다중 인증 체계를 사용하여, 내부자의 불법적인 접근을 사전 차단하고 시스템에 접속 시에 인지할 수 있도록 감시해야 한다.

2.2.1.4 호스트기반 침입탐지시스템 구축

컴퓨터 및 정보 시스템에 호스트기반 침입탐지시스템을 구축하여, 사용자 계정 관리, 불법적 코드 실행 방지, 비정상적인 상황 탐지 등을 통해 내부자의 사이버공격을 차단해야 한다.

2.2.2 운영적 및 관리적 보안통제

내부자의 사이버공격을 차단하기 위한 기술적 사이버보안 통제가 적용 불가능할 경우, 대안적 조치로 원자력시설의 설계 및 운영 단계에서의 운영적 및 관리적 사이버보안 통제가 필요하다.

2.2.2.1 악성코드 유입 방지를 위한 주기적 점검

컴퓨터 및 정보 시스템에 접속 가능한 비승인 휴대용 매체를 점검하고 악성코드 감염 여부를 주기적으로 검사하여, 내부자 위협을 사전 차단하고 잠복하고 있는 악성코드를 제거하여야 한다.

2.2.2.2 유지보수 도구 관리

컴퓨터 및 정보 시스템에 접속되는 유지보수 도구를 식별하고 시스템 접속 전 사이버보안 조치를 수행하도록 하여 내부자의 공격 경로를 사전 차단하여야 한다.

2.2.2.3 물리적 접근 통제

컴퓨터 및 정보 시스템에 접근 가능한 인원을 식별하고 출입 전 보안 점검 절차를 거치도록 하여 내부자의 접근을 차단하여야 한다.

2.2.2.4 개발자 보안 검사

컴퓨터 및 정보 시스템의 개발 단계에서 취약점 및 악성코드가 포함되지 않도록 검사 및 평가를 진행하고 설계 시 사이버보안 보안 요건들을 반영하여 내부자의 사이버공격 경로를 사전 차단하여야 한다.

3. 결론

본 연구에서는 KINAC/RS-015 부록2의 기술적, 운영적 및 관리적 보안통제 요건 중 내부자에 의한 사이버공격을 효과적으로 방호하기 위한 최소한의 사이버보안 요건들을 도출하였다. 도출된 기술적 사이버보안 요건들 중 일부는 가동 중인 원자력시설의 설비 노후화 및 설계단계에서 사이버보안이 고려되지 않아 적용하기 힘들기 때문에 대안적 조치인 운영적 및 관리적 사이버보안 요건을 통해 사이버보안을 강화해 나가고 있다.

본 연구에서 도출된 사이버보안 요건들을 적용하기 위해서는 사이버보안이 적용되어야할 컴퓨터 및 정보 시스템이 식별되고, 건설 단계부터 사이버보안 요건이 적용되어야 한다. 따라서 내부자 위협에 대한 사이버보안을 강화하기 위해서는 원자력시설의 사이버보안 적용 범위를 현재의 가동 단계에서 건설 단계로 확장할 수 있도록 법적 개정이 필요하다.

4. 감사의 글

본 연구는 원자력안전위원회 재원으로 한국원자력안전재단의 지원을 받아 수행한 원자력안전연구사업의 연구결과입니다 (과제번호 : 1305034).

5. 참고문헌

[1] 한국원자력통제기술원, “원자력시설 등의 방호 및 방사능 방재 대책법령집”, 2016.

[2] 한국원자력통제기술원, “원자력시설등의 물리적 방호 관련 사무편람”, 2016.

[3] 한국원자력통제기술원, “원자력시설등의 컴퓨터 및 정보시스템 보안 기술기준”, KINAC/RS-015, 2014.

[4] U.S. NRC, “Cyber Security Programs for Nuclear Facilities”, Regulatory Guide 5.71, 2009.