KEPCO Journal on Electric Power and Energy
p-ISSN 2465-8111, e-ISSN 2466-0124
Volume 6, Number 3, September 2020, pp. 321-322
DOI 10.18770/KEPCO.2020.06.03.321

Toward a New Risk-Informed Approach to Cyber Security

EPRI Guidelines Equip Electric Power Industry to Address Growing Risks and Vulnerabilities

사이버 보안을 위한 새로운 위험도정보 기반 접근법을 향하여

EPRI의 가이드라인을 통해 전력 산업은 증가하는 위협과 취약점에 대응할 수 있다.

Electric Power Research Institute

발전소의 사이버 보안은 얼마나 제어시스템을 안전하게 지키는가에 달려있다. 그 중 핵심적인 장비의 예가 엔지니어링 워크스테이션Engineering Workstation이다

[역주] 엔지니어링 워크스테이션: 제어시스템 계층구조의 최상위에 위치하여, 제어시스템 및 제어용 장비와 소프트웨어 등의 구성, 유지보수, 모니터링 등을 위한 최상위 컴퓨터 시스템

엔지니어링 워크스테이션은 프로그래밍이 가능한 발전소 제어 로직에 연결되어 있기 때문에 엔지니어링 워크스테이션을 보호하는 것이 중요하다. 또한 엔지니어링 워크스테이션은 최고의 공격 목표가 된다. 공격자가 엔지니어링 워크스테이션에 침입해 악성 소프트웨어를 심어 놓을 수 있다면 발전소의 중요한 제어 기능을 저해해 결국에는 발전소를 정지시킬 수도 있다.

발전소의 디지털 제어 장치를 공격자로부터 보호하는 전통적인 심층 방어defense-in-depth 접근법은 다양한 보안 대책을 층층이 설치하는 매우 복잡한 작업이다. 가장 최적의 방법과 몇 개의 층을 설치할지 신속하게 결정하는 것은 어려운 일이다.

북미의 대형 전력시스템 운영자는 반드시 북미신뢰도위원회North American Electric Reliability Corporation, NERC의 중요 기반시설 보호 표준Critical Infrastructure Protection, CIP을 준수해야 한다. NERC의 기준은 미국 국립표준기술연구소National Institute of Standards and Technology, NIST 및 미국 원자력규제위원회Nuclear Regulatory Commission의 사이버 보안 관련 규제와 함께 목록 실행Committed catalog 접근법이라고 알려져 있는데, 이 기준은 모든 장비에 대한 목록화된 보안 대책을 구현하도록 지시하고 있다. 이 방법이 어느 일정 수준의 보안은 제공하겠지만, 현재 전력 산업의 이해관계자들은 훨씬 더 목표 지향적인 접근법이 가져올 수 있는 편익에 주목하고 있다. 이 접근법에서는 발전소 제어시스템의 특정한 취약점에 대한 보안 대책을 적용한다.

표준과 규제가 사이버 보안의 기반을 구성하는데 핵심적 역할을 해왔다. 또한 이해관계자들을 회의 테이블 앞에 모아 핵심 자산을 어떻게 보호할지 토론하게도 했다. 하지만 표준과 규제의 준수만으로 보안을 확보할 수는 없다. 발전소 운영자들은 규제가 요구하는 것 이상으로 더 복잡한 대책을 구현하기 위해 사이버 보안에 대한 기대치를 올리고 있다.

이는 증가하는 사이버 위협과 궤를 같이 한다. 미국 에너지부 릭 페리Rick Perry 장관은 작년 국회의원들에게 미국의 전력망에서는 매일 수 십만건의 사이버 공격이 발생하고 있다고 언급한 바 있다. 에너지부의 에너지 분야 사이버 보안을 위한 다년간의 계획Multiyear Plan for Energy Sector Cybersecurity에 따르면 사이버 위협의 빈도, 규모, 복잡성이 증가해 왔으면 공격은 훨씬 쉬워졌다. 정부는 물론 범죄자, 테러리스트는 주기적으로 에너지 시스템을 훼손하거나, 혼란에 빠뜨리고 파괴하기 위해 사이버 보안의 취약점을 찾아 에너지 시스템을 탐지한다.

뉴욕시와 웨스트체스터 카운티에 전력을 공급하는 콘에디슨Con Edison의 제어 프로젝트 전문가 윌리엄 베슬리William Vesely에 의하면, 사이버 위협은 지속적으로 상승하고 있다. 전력 분야의 핵심 인프라가 공격의 1차적 목표로, 이 경기에서 앞장서 나아가는 것은 힘든 일인 동시에 잠시의 방심도 없어야 한다.

Risk-Informed Cyber Security
위험도정보 기반 사이버 보안

EPRI는 전력 회사, 제어 시스템 제작사, 정책 입안자, 규제 당국 등과 함께 핵심적인 발전소 자산을 보호하기 위해 새로운 사이버 보안 접근법을 개발하고 있다.

Article Information

이 보고서는 Electric Power Research Institute와의 협약에 의해 한국어로 번역되어 게재되었습니다. Electric Power Research Institute와 한국전력공사는 원문 및 한국어판의 저작권을 보유하고 있습니다. 원문은 Electric Power Research Institute 홈페이지 https://epri.com에서 보실 수 있습니다. 한국전력공사는 본 원고에 포함된 내용 또는 번역의 정확성을 보장하지 않습니다.

현재 EPRI는 전력 회사가 사이버 보안 대책을 평가할 수 있는 위험도 정보 기반 방법론을 개발하고 있다. 이 단계별 접근법은 잠재적 보안 침해와 가능성, 방사선 누출이나 정전 또는 기업 이미지 훼손 등 보안 침해가 가져올 만한 결과 등을 고려하여 대책의 우선 순위를 정하는 방법이다.

모든 구성품이 동일 수준으로 만들어졌거나 같은 기능을 수행하지는 않는다. 따라서 지금까지의 접근법은 구성품을 항상 동일하게 취급한다는데 한계가 있다. EPRI의 새로운 접근법에서는 개별 구성품의 특정 취약점을 평가하고 위협을 완화하기 위한 최선의 방법을 찾아낼 수 있다. 핵심 운영 장비를 보호하고 표준과 규제의 적용 우선 순위를 평가하는데 더 많은 시간을 쏟을 수 있다. 표준은 "무엇"을 제공하며 EPRI의 접근법은 "어떻게"를 제공한다.

Risk-Informed Approach in Action
위험도정보 기반 사이버 보안 적용

EPRI 접근법의 첫 단계는 발전소 제어 시스템을 구성하는 각 구성품이 사이버 공격을 당하는 곳의 특징을 정의하는 것이다. 공격당하는 곳은 물리적 지점, 네트워크, 무선연결점 등 구성품이 공격당하는 모든 지점을 포함한다.

다음 단계는 정보를 훔치거나, 설정 파일을 바꾸는 것과 같은 가능한 공격 목표와 공격 순서를 찾아내는 것으로, 이 단계는 목표와 취약성에 따라 변할 수 있다. 어디서, 왜, 어떻게 공격이 이루어지는 완전히 이해함으로써 발전소 운영자는 가장 효과적인 방어를 계획할 수 있다.

위험도 정보 기반 접근법의 세 번째 단계는 가장 가능성 높은 공격으로부터 시스템 보호, 공격 감지 및 대응, 공격으로부터 복구 등 각 보안 대책의 역량을 평가하는 것이다.

공격을 방해할 수 있는 수 많은 잠재적 방법이 있으며, 가장 효과적인 조합을 적용할 수 있다. 엔지니어링 워크스테이션에는 악성 소프트웨어를 효과적으로 감지하여 운영자에게 경고를 보낼 수 있는 바이러스 프로그램이 이미 설치되어 있을 수 있다. 하지만 대응과 복구에는 별로 도움이 안 될 수 있다.

효과와 구현 측면에서 각 보안 대책에 대한 평가 점수가 계산된다. 이 평가 점수는 각 공격에 대해 얼마나 잘 준비되었는지를 보여준다. 발전소 운영자가 이 평가 점수를 수용할지 여부는 자산의 중요도와 공격이 성공했을 때 발생할 결과에 좌우된다. 각 발전소는 수용할 수 있는 위험도 기준을 결정해야만 한다.

위험도정보 기반 접근법은 규제가 요구하는 바를 만족할 수 있다. 이 접근법은 훨씬 효율적이고 효과적으로 규제를 준수하는 방법이 된다.

Risk-Informed Cyber Security at Vogtle
Vogtle의 위험도정보 기반 사이버 보안

Southern Nuclear는 Vogtle 3, 4호기를 건설하면서 보안 규제를 준수하는 동시에 EPRI의 사이버 보안 접근법을 채택하였다.

Vogtle 3, 4호기 사이버보안 책임자 브래드 예이츠Brad Yeates에 의하면 Vogtle는 EPRI 방법론의 첫 상업적 적용 사례이다. Vogtle는 이 접근법이 가장 직접적이고 비용효과적이라 결론 내렸다.

Vogtle은 EPRI와 협력하여 16,000개에 달하는 디지털 발전소 구성품을 보호하기 위한 위험도정보 기반 보안 계획을 개발하였다.

사이버 보안 평가 및 대책에 이 방법론을 적용한 세계 첫 사례이다. Vogtle은 다른 발전소가 참조할 수 있는 사례를 만들고 있는 것이다. Vogtle의 사례를 따라오는 모든 이들은 쉽고 빠른 길을 가게 될 것이다.

Vogtle은 EPRI 연구진과 함께 16,000개의 디지털 자산을 분석하는 절차를 개발하여, 약 400개의 개별 구성품을 골라냈다. 이 정도는 초기 기술 평가에서 충분히 다룰 수 있는 규모였다. 일단 400개의 구성품의 평가가 완료되자, 이 구성품들은 발전소 구성에 따라 맞춤형으로 더 큰 디지털 시스템에 넣어 조립할 있는, 마치 레고LEGO 블록처럼 보였다.

Vogtle은 각 자산의 취약점을 분석하고, 가용한 최고의 보호 대책을 고르는데 EPRI의 위험도정보 기반 방법론을 활용하고 있다. Vogtle은 2020년초까지 최종 사이버 보안 프로그램을 수립하고 2020년말까지 평가를 완료할 것으로 기대하고 있다.

일단 발전소에 연료가 공급되면 발전소는 상업 운전의 전단계인 전면적인 시범 운전에 들어갈 것이기 때문에 Vogtle은 발전소에 연료가 공급되기 전까지 반드시 사이버 프로그램이 동작하도록 만들어야 한다.

2019년 EPRI는 제작사, 전력 회사들과 함께 위험도정보 기반 접근법의 구현 방법 및 장점을 문서화하는 연구를 진행 중이다. 연구 결과에 따라 협력 중인 이해관계자들은 EPRI에게 접근법을 개선할 수 있는 피드백을 제공할 것으로 예상된다.

콘에디슨의 윌리엄 베슬리는 다른 전력 회사도 위험도정보 기반 사이버 보안 접근법을 받아들이고, 현 업무를 상당히 개선할 수 있는 방법으로서 이 접근법을 인식할 수 있기를 희망한다.

전력 회사가 직면하는 현안은 새로운 디지털 기술을 통해 얻는 장점과 사이버 보안 사이의 균형을 맞추는 것이다. 윌리엄 베슬리는 국제 표준이 EPRI 접근법의 기반을 구성하는 개념을 많이 활용하길 희망한다고 한다.

EPRI는 전력 분야에서 사이버 위험을 평가하는 데 더 많은 공학적 기술을 포함해왔다. EPRI의 접근법은 발전소 운영자가 최고의 보호 방법을 정확히 찾고 발전소를 안전하게 유지하기 위해 취약점을 심도 깊게 이해할 수 있도록 한다. EPRI