신재생 에너지 배터리 및 저장 시스템의 사이버 위협

한진용, 이용준
극동대학교 해킹보안학과
e-mail:namema98@naver.com

Responding to cyber threats from batteries and storage systems

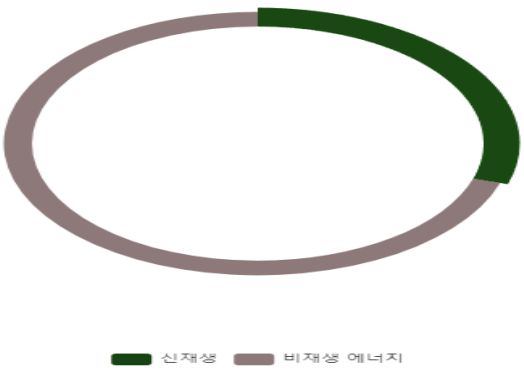
Han Jin Yong, Lee Yong Jun
Dept. of Hacking Security, Far East University

요 약

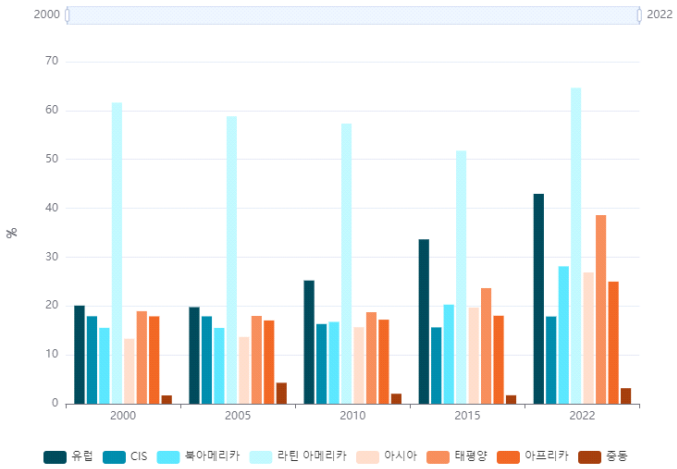
고갈되어 가고 있는 화석 연료를 대비하여 기존의 화석 연료에 의존하지 않고 재생 가능한 에너지원을 활용하는 신재생 에너지 시스템이 가속화 되고 있다. 이 시스템의 많은 구성요소들이 있지만 배터리 및 저장 시스템은 신재생 에너지의 중요한 구성 요소로 전력 공급의 신뢰성과 안정성을 보장한다. 하지만 중요한 구성요소인 만큼 의존성이 높고 사이버 공격으로 중요한 전력공급이 중단될 수 있다. 배터리 및 에너지 저장 시스템의 사이버 취약성과 위협을 식별하고 분석하여 대응책을 제안한다.

Ⅰ. 서론

현재 전 세계적으로 재생에너지 비중이 계속 증가하고 있다. 2021년 기준 세계 평균 재생에너지 발전 비중은 10.3%이다. 하지만 한국은 4.7%에 불과하다. 이처럼 전세계적으로 재생에너지 발전에 힘쓰고 있다. IEA는 2025년 현 최대전력인 석탄을 제치고 재생에너지가 최대 전력원이 된다고 보고 있다. 한국은 2030년까지 발전 비중을 원자력 32.4%, 액화천연가스(LNG) 22.9%, 신재생에너지 21.6%, 석탄 19.7% 로 가져간다는 목표를 가지고 있다.
세계 신재생 에너지 비율을 29.8%이다.



[그림 1] 세계 신재생 에너지 비율



[그림 2] 2000-2022년 지역별 에너지 변화 비율

Ⅱ. 취약점

2.1 인터넷 연결성

보통 배터리 및 저장 시스템은 원격 모니터링 및 제어를 위해 인터넷에 연결된다. 이 연결은 취약점을 해커들에게 좋은 먹잇감이 된다.

2.2 원격 관리 취약점
원격관리 도구는 사용자들을 도와 편리하게 사용되지만 이를 통해 해커가 시스템에 액세스할 수 있다.

2.3 악성코드 및 랜섬웨어
악성코드나 랜섬웨어는 배터리 및 에너지 시스템에 침입하여 데이터 손실, 시스템 마비 또는 금전적 손실을 초래한다.

2.4 약한 인증 및 암호화
사용자 인증 및 데이터 암호화에 대한 부적절한 구현은 사이버 공격자에게 쉬운 접근을 제공한다.

2.5 주기적 업데이트 부재
보안 패치와 업데이트가 제때 적용되지 않으면 알려진 취약점을 악용하는 공격자에게 공격을 당할 수 있다.

2.6 약점 스캐닝
해커는 시스템에 자동화된 스캐닝 도구를 사용하여 시스템의 취약성을 식별하고 공격 포인트를 찾는다.

2.7 피싱 공격
피싱 이메일이나 사회 공학 기술을 사용한 공격으로, 사용자를 속여 개인정보나 암호가 유출된다.

2.8 물리적 보안 부족
시설에 대한 출입 통제 부족은 물리적 공격의 위험을 증가시킨다.

2.9 데이터 무결성 문제
데이터릐 무결성을 보장하지 않으면 시스템의 조작이나 데이터 변조가 일어난다.

2.10 제조사 백도어
제조사가 시스템에 백도어를 남겼을 경우, 악용될 수 있다.

2.11 개발자 실수
소프트웨어 및 하드웨어 개발 과정에서의 실수, 버그, 백도어는 공격자에게 취약점을 제공할 수 있다.

Ⅲ. 사례

3.1 인터넷 연결성
2015년에는 우크라이나의 전력 그리드가 사이버 공격에 강타당했습니다. 해커들이 전력 그리드 제어 시스템에 침투하여 시스템을 끄거나 제어했습니다. 이 공격은 인터넷 연결성을 통해 전력 그리드에 침투했으며, 실질적인 전력 중단을 초래했습니다.

3.2 악성코드 및 랜섬웨어
2016년에는 화석 연료 및 신재생 에너지 시스템을 타겟으로 하는 랜섬웨어 공격이 발생했습니다. 공격자는 태양광 패널 제조사와 태양광 발전소를 겨냥하여 랜섬웨어를 전파하고, 시스템을 암호화한 후 금전적 보상을 요구했습니다.

3.3 암호화 및 인증 취약성
2017년에는 허드슨 인스투루먼트스 (Hudson Institute)와 존 매카인 상장 연구소 (John McCain Institute for International Leadership)의 보고서에 따르면, 중국 기반의 해커 그룹이 태양광 발전소와 그리드 운영자를 표적으로 하는 공격을 수행했습니다. 이들은 피해자의 인증 자격증을 훔치고, 이를 통해 시스템에 침입하여 제어할 수 있었습니다.

3.4 물리적 보안 부족
2019년, 일본의 태양광 발전소에 대한 공격이 발생했습니다. 공격자는 발전소 내부에 침입하여 통제실의 컴퓨터를 파괴하고 시스템을 중단시켰습니다. 이러한 물리적 침입은 시설의 물리적 보안 부족을 드러냈습니다.

3.5 데이터 무결성 문제
2018년, 미국 내 태양광 발전소와 전력 그리드 제어 시스템에 대한 침입 사례가 보고되었습니다. 공격자가 데이터를 변조하여 발전소 운영자에게 잘못된 정보를 제공하고, 그 결과로 전력 그리드에 영향을 미쳤습니다.

Ⅳ. 대응 방안
4.1 인터넷 연결성 대안
4.1.1 에어 갭(Air Gapping)
중요한 에너지 시스템을 오프라인으로 유지하고 인터넷과 완전히 분리하여 사이버 공격의 위험을 줄인다. 중요 제어장치는 물리적으로 접근이 제한된 장소에 설치한다.
4.1.2 가상 사설 네트워크(VPN)
원격 접속 시 VPN을 사용하여 안전한 연결을 설정하고 보안 검증을 통해 무단 접근을 방지한다.

4.2 악성코드 및 랜섬웨어 대안

4.2.1 정기적인 보안 업데이트

시스템 및 소프트웨어의 보안 업데이트를 정기적으로 설치하여 악성 코드 및 랜섬웨어 공격으로부터 보호한다.

4.2.2 업데이트된 백업

정기적인 데이터 백업 및 데이터 무결성 확인을 통해 데이터 손실을 최소화하고 복구시간을 단축한다.

4.3 암호화 및 인증 대안

4.3.1 다중 인증 요소(MFA)

다중 인증은 사용자가 비밀번호 외에도 다른 인증 요소를 제공해야하는 보안기술로 이를 통해 보안을 강화한다.

4.3.2 암호화 업데이트

최신 암호화 알고리즘을 사용하고, 정기적으로 업데이트 및 강화하여 데이터 보호를 강화한다.

4.4 물리적보안 대안

4.4.1 물리적 접근 제어

시설 내에 출입 통제 시스템 및 보안 카메라를 설치하여 물리적 보안을 강화한다.

4.4.2 보안 센서 및 경보 시스템

물리적 침입을 감지하고 보고하는 센서 및 경보 시스템을 구축하여 물리적 보안을 강화한다.

4.5 데이터 무결성 문제 대안

4.5.1 블록체인 기술

데이터의 변경 내역을 블록체인에 저장하여 데이터 무결성을 보장한다.

4.5.2 디지털 서명 및 해시 기술

데이터의 무결성을 검증하기 위해 디지털 서명 및 해시함수를 사용한다.

V. 결론

본 논문에서 신재생 에너지 시스템 공격사례들과 문제가 되는 취약점, 그리고 대안을 분석하였다. 전세계적으로 신재생 에너지 시스템의 점유율은 증가할 것이다. 현재 점유율 증가 속도에 비해 보안수준이 낮다. 신재생 에너지의 배터리 및 저장 시스템에 대한 규정을 마련하고 취약점을 보완하고 해커들의 공격을 차단할 수 있는 자체 보안시스템 또는 외부 보안 시스템을 사용하여야 한다. 현재 보안시스템이 있더라도 정기적인 관리와 업데이트가 필요하다. 또한 관련 직원들의 보안의식교육도 꾸준히 이루어져야 한다.

보안시스템의 발전만큼 해커들의 공격방법도 발전하므로 현재 상황에 안도하지말고 항상 해커들의 공격에 대비해야 한다.

참고문헌

[1] https://www.esgeconomy.com/news/articleView.html?idxno=2895

[2] https://yearbook.enerdata.co.kr/renewables/renewable-in-electricity-production-share.html

[3] https://www.itworld.co.kr/news/157327