인공지능시대의 보안

막는 시대는 끝났다, 이제는 회복이다

우리는 지금 현실 세계와 디지털 세계가 완전히 결합된 시대를 살고 있다. 전력망과 가스 공급망, 정유 시설과 같은 핵심 인프라는 더 이상 물리적 설비에 머물지 않는다. 수많은 센서와 제어 시스템, 네트워크와 AI가 결합되면서 물리와 사이버의 경계는 사실상 사라졌다. 이 융합 환경에서 보안은 가상의 위험을 막는 기술이 아니라, 현실의 생존을 좌우하는 핵심 조건이 되었다.

최근 중동 정세가 보여주듯 에너지 안보는 군사적 충돌을 넘어 사이버 공간으로 빠르게 확장되고 있다. 전력망과 에너지 시설을 겨냥한 공격은 더 이상 보조 수단이 아니라 전략 그 자체다. 특히 사이버 공격이 물리적 설비를 직접 통제할 수 있는 구조가 형성되면서, 단 한 번의 침해가 대규모 정전이나 설비 사고로 이어질 수 있는 위험이 현실화되고 있다.

문제는 공격의 양상이다. 생성형 AI의 등장으로 사이버 위협은 이전과 전혀 다른 차원으로 진화했다. 공격은 스스로 학습하고 변형되며, 인간의 심리와 조직의 취약성까지 정밀하게 파고든다. 과거처럼 알려진 패턴을 탐지하고 차단하는 방식만으로는 대응이 불가능하다. 방어 체계가 완성되는 순간 이미 다음 공격이 시작되는 구조다. '완벽한 방어'는 더 이상 유효한 목표가 아니다.

필자는 과거 에너지 기업의 보안 체계를 점검하고 원자력 관련 법·제도에 따른 보안 감독 업무를 수행하면서 중요한 한 가지 사실을 확인했다. 보안의 실패는 기술의 부족이 아니라, 사람과 조직에서 비롯되는 경우가 많다는 점이다. 형식적인 절차, 부서 간 단절, 책임의 공백은 아무리 정교한 보안 시스템도 무력화시킨다. 특히 IT와 OT가 분리된 환경에서는 작은 침해가 전체 시스템 붕괴로 이어질 수 있는 구조적 취약성이 존재했다.

이제 질문을 바꿔야 한다. **"어떻게 막을 것인가"**가 아니라 **"침해 이후에도 어떻게 유지하고 회복할 것인가"**다.

필자의 인공지능시대의 보안인문사회학에서 강조했듯, 보안은 기술이 아니라 신뢰의 문제다. 완벽한 방어는 존재하지 않는다. 중요한 것은 침해를 전제로 설계된 시스템, 즉 뚫려도 무너지지 않는 구조다. 이것이 보안 회복탄력성의

본질이다.

이를 위해서는 제로 트러스트 기반 접근과 융합보안 체계가 필수적이다. 모든 접근을 검증하고 최소 권한을 적용하며, IT와 OT 전 영역을 통합적으로 관리해야 한다. 네트워크 분리와 핵심 자산 격리, 다중 백업 체계는 침해 상황에서도 핵심 기능을 유지하게 하는 기반이 된다. 동시에 IT 보안과 OT 운영 조직을 하나의 대응 체계로 통합하는 구조적 변화가 병행되어야 한다.

그러나 기술만으로는 충분하지 않다. 위기 상황에서 조직을 지키는 것은 결국 사람의 대응 능력이다. 경영진의 인식 전환, 반복적인 모의훈련, 공급망 전반을 아우르는 보안 관리, 그리고 보안을 조직 문화로 내재화하려는 노력이 함께 이루어져야 한다.

에너지 인프라는 국가의 생명선이다. 사이버 공격은 더 이상 가상의 위협이 아니라 현실의 재난으로 이어진다. 이제 보안의 패러다임은 분명하다. 막는 시대는 끝났다. 공격을 견디고 빠르게 회복하며 신뢰를 재구성하는 능력, 그것이 에너지 기업의 생존을 결정짓는 새로운 기준이다. (끝)