AI가 무너뜨린 보안의 상식… 이제는 '예측'보다 '적응'이다

이기혁 (중앙대학교 교수)

최근 몇 년 사이 사이버보안의 **패러다임**은 근본적으로 바뀌고 있다. 과거에는 방화벽을 구축하고 백신을 설치하며 알려진 공격을 차단하는 것이 보안의 핵심이었다. 하지만 인공지능(AI)의 등장으로 공격과 방어의 속도는 사람이 따라가기 어려울 만큼 빨라졌고, 이제 사이버보안은 **'예측 가능한 위험'**을 관리하는 영역이 아니라 **'끊임없이 변화하는 위협'**에 적응하는 경쟁이 되었다.

오늘날 공격자는 생성형 AI를 활용해 정교한 피싱 메일을 순식간에 작성하고, 악성코드를 자동으로 변형하며, 취약점을 탐색하는 시간을 획기적으로 줄이고 있다. 과거에는 대규모 공격을 위해 많은 시간과 전문 인력이 필요했지만, 이제는 AI가 이러한 과정을 자동화하면서 **공격의 문턱이 크게 낮아졌다.**

반면 방어 전략도 달라져야 한다. 더 이상 완벽한 보안을 기대하기는 어렵다. 중요한 것은 얼마나 빨리 이상 징후를 발견하고, 얼마나 신속하게 대응하며, 얼마나 빠르게 회복할 수 있는가이다. **사이버보안의 경쟁력은 '완벽한 예방'이 아니라 '민첩한 대응'에서 결정된다.**

기업과 공공기관 역시 기존의 보안 체계를 재점검해야 한다. 정적인 보안 정책만으로는 AI 시대의 지능형 공격을 막기 어렵다. AI 기반 위협 탐지, 실시간 모니터링, 제로트러스트(Zero Trust) 보안, 지속적인 보안 교육과 훈련이 조직의 새로운 기본 역량이 되어야 한다.

흥미로운 점은 AI가 가장 큰 위협인 동시에 가장 강력한 방어 수단이라는 사실이다. AI는 수많은 로그를 분석해 사람이 놓치는 이상 징후를 찾아내고, 공격 패턴을 예측하며, 보안관제의 효율성을 높이고 있다. **결국**

미래의 사이버보안은 AI를 배제하는 것이 아니라 AI를 얼마나 현명하게 활용하느냐에 달려 있다.

세계는 이미 '질서의 종말'을 경험하고 있다. 예측 가능한 환경은 사라지고 있으며, 사이버 공간 역시 예외가 아니다. 이제 보안은 과거의 성공 경험을 반복하는 것이 아니라 변화에 적응하는 능력을 키우는 과정이어야 한다.

AI 시대의 사이버보안은 더 이상 '예측'의 영역이 아니다. 변화에 가장 빠르게 적응하는 조직과 사람이 미래의 디지털 신뢰를 지켜낼 것이다.