

핵심망 대신 업무망 노린 해커… 금융권 ‘AI 다층 방어’ 절실

비대면 계좌·업무 지원망 집중 공격
증권업권 보안 예산·인력 비중 최저
망분리 넘어 AI 탐지·다중 인증 강화
CEO·이사회 책임 강화 등 통제 개선

증권사와 운용사·가상자산업계 등을 포합한 국내 금융투자업계가 인공지능(AI) 해커들의 ‘먹잇감’이 됐다. 전문가들은 최고경영자(CEO)와 이사회의 책임을 강화하고, AI를 활용한 해킹 등 갈수록 복잡 다양해지는 보안 공격에 대비한 인력 및 기술 지원 확대가 필요하다고 한목소리를 냈다. 인터넷과 연결된 외곽 시스템의 보안을 강화하고, AI 기반 탐지·대응과 다층 방어 체계를 갖춰야 한다는 지적이다.

◆전 금융권으로 확산되는 해킹

28일 금융위원회에 따르면 신한은행 정보 유출 사고 전후로 정보 유출이 확인된 주요 금융사는 총 20곳이다. 업권별로는 은행 4곳(신한·국민·부산·하나), 보험 1곳(미래에셋생명), 금융투자 2곳(대신증권·미래에셋자산운용), 저축은행 4곳(에가람·웰컴·DB·OK), 여신전문금융회사 2곳(현대캐피탈·산은캐피탈), 온라인투자연계금융업체 2곳(PFCT·모우다), 전자금융업체 1곳(브라이트픽스), 가상자산사업자 3곳(빗썸·스트림·프라뱅), 상호금융 1곳(새마을금고중앙회)이다. 해킹 피해를 입은 금융사에 대한 확인 작업이 진행 중이어서 유출 규모는 더 늘어날 전망이다.

기존 금융권 유출된 정보에는 성명과 연락처, 주민등록번호, 이메일 주소 등이 포함됐다. 이번 금융투자업계의 경우에는 공격자가 인터넷·모바일 뱅킹 관련 입출금 계좌번호와 고객 전화번호, 주민등록번호·여권번호·운전면허번호·외국인등록번호 등 고유식별정보와 민감정보, 개인신용정보에는 접근하지 못한 것으로 알려졌다.



고객들의 정보가 해킹으로 인해 탈취되는 모습을 상징적으로 형상화한 이미지. /ChatGPT로 생성한 이미지

하지만 금융투자 및 가상자산 업계 안팎에서는 확산하는 보안 공격에 우려의 시선을 보낸다. 고객 금융거래 정보까지는 유출되지 않았지만, 해커가 AI 에이전트를 활용해 비대면 증권 계좌 개설 연계 서버, 직원용 모바일 업무 지원 시스템 등 상대적으로 관리가 허술한 곳을 찾아 반복적인 공격을 벌였기 때문이다.

시장에서는 예견된 사태라는 지적이다. 강민국 국민의힘 의원이 금융감독원으로부터 파악한 자료를 보면 올해 6월 말 기준 증권업권의 정보보호 예산은 3276억원이다. 전체 IT 예산(2조9967억원)의 10.9%다. 은행·저축은행·생명보험 손해보험·카드·자산운용 등 7개 금융업권 중 가장 낮다. IT 보안 인력 비중도 가장 적다. 올해 6월 기준 증권업권의 IT 인력은 5063명이다. 이 중 정보보호 업무 담당은 480명(9.5%)으로 전체 금융업권 평균인 9.6%보다 낮다.

◆망분리만으로 안심 못 해… AI 대응·다층 방어 시급

금융투자업계에서는 피해가 없는 회사도 안심하기 어렵다는 우려가 나온다. 한 증권사 관계자는 “피해 여부가 보안을 잘하고 못하고의 차이라고만 보기는 어렵

다”며 “해커가 마음먹고 공격하면 다른 회사도 피해를 볼 수 있다”고 말했다. 이어 “그동안 망분리에 의존한 측면이 있다”며 “업무 과정에서 내·외부망 사이로 자료를 주고받는 점점의 보안도 살펴야 한다”고 덧붙였다.

염흥열 순천향대 정보보호학과 교수는 “현재는 금융거래를 처리하는 핵심망보다

인터넷 접점을 가진 업무 지원망이 공격받고 있는 상황”이라며 “지원망의 보안 대책을 강화해야 한다”고 말했다. 특히 비대면 계좌 개설 연계 시스템에 대해서는 “핵심망에 접근하는 통로가 될 가능성이 있는 만큼 불법 자금·증권 이체로 이어질 수 있는지 면밀히 점검해야 한다”고 강조했다.

금융투자업계 안팎에서는 문제를 근본적으로 개선하려면 내부 책임과 통제 시스템을 강화해야 한다고 지적한다. 최고경영자(CEO)와 이사회의 책임을 명확히 규정하고, 정보보호최고책임자(CISO)의 권한을 강화해야 한다는 얘기다. 씨티그룹·모건스탠리·HSBC 등 해외 주요 금융회사는 이사회 산하에 별도의 기술위원회(Technology Committee)를 두고 사이버 보안 사고에 대응하고 있다. 그러나 국내 금융투자업계와 가상자산 업계에는 이런 위원회를 둔 곳이 전무하다.

그나마 이사회 책임 강화 등을 포함한 전자금융거래법 개정안이 지난해 11월 말

발의됐지만 국회에선 논의조차 안 되고 있다. 개정안은 해킹 사고로 정보 유출 사고가 나면 총매출액의 3% 이하의 과징금을 부과하는 내용도 담고 있다.

AI 공격에 대응할 기술적 방어 체계도 과제다. 엄 교수는 “구체적인 원인은 조사가 필요하지만 동시다발적인 공격 양상은 해커들이 자동화 도구로 취약점을 빠르게 찾고 있음을 시사한다”며 “금융사도 AI로 취약점을 먼저 찾아 보완해야 한다”고 말했다. 이어 “2차·다중 인증을 우선 적용하고, 접근을 지속 검증하는 제로 트러스트와 실시간 이상행위 탐지·대응을 통해 한 단계가 뚫려도 다음 단계에서 막는 다층 방어 체계를 갖춰야 한다”고 주문했다.

금융위는 이익원 금융위원장 주재로 관계 부처·기관과 금융권 업권별 협회장이 참석하는 ‘AI 보안위협 대응 금융권 간담회’를 열 계획이다.

/허정윤 기자

zolkova@metroseoul.co.kr



metro

북한 IP 440만건 접속 시도 전산망 취약점 탐색 정황

21일 새벽부터 스캔성 접근 탐지
당국, 접속 이력·보안 점검 요청
실제 피해 없고 공격 주체 미확인

국내 금융회사의 전산망 취약점을 탐색하는 북한 인터넷주소(IP) 대역의 접속 시도가 440만건 넘게 포착됐다. 금융당국은 금융회사에 접속 이력 확인과 보안 체계 점검을 요청했다. 다만 해당 접근으로 인한 피해 신고는 아직 없으며, 공격 주체도 확인되지 않았다.

28일 금융업계에 따르면 금융당국은 지난 21일 금융보안 통합관제시스템 ‘퍼스트(FIRST)’를 통해 가상자산거래소 등 금융회사에 북한 IP 대역의 스캔성 접근에 대한 주의를 당부하는 공문을 전달했다.

공문에 따르면 같은 날 오전 3시부터 북한 IP 대역에서 금융권을 겨냥한 접근이 지속적으로 탐지됐다. 공문을 보낼 때까지 집계된 접근 시도는 440만4101건이다.

스캔성 접근은 외부에서 시스템의 접속 통로나 보안상 허점을 살펴보는 행위다. 네트워크에서 열려 있는 포트 등을 확인해 공격 가능한 지점을 찾는 데 활용될 수

있다. 다만 접근 시도 자체가 전산망 침입이나 정보 유출을 뜻하는 것은 아니다.

당국은 금융회사에 해당 IP의 접근 기록을 살피고 정보보호·내부통제 체계를 점검하도록 요청했다. 이상징후를 실시간으로 감시하고, 특이사항이 확인되면 당국에 알리도록 했다.

현재까지 해당 IP를 이용한 접근이 실제 침해사고로 이어졌다는 피해 신고는 없는 것으로 전해졌다. 북한 IP 대역이 탐지됐다는 사실만으로 북한 해커의 공격이라고 단정하기도 어렵다. 접속 경로를 우회하거나 IP 정보를 조작할 가능성이 있어 공격 주체를 판단하려면 추가 분석이 필요하다는 게 당국의 설명이다.

한편 청와대 국가안보실은 이날 오후 송기호 3차장 주재로 금융위원회 관계자 등이 참석하는 긴급 대응회의를 열 예정이다. 빗썸과 미래에셋자산운용 등에서 발생한 해킹 관련 사고의 피해 현황을 점검하고 추가 피해를 막기 위한 대응책을 논의할 계획이다.

/허정윤 기자 zolkova@



metro

나무꾼의 투자에 날개를 달아 줄

선녀금 혜택

신규·휴면 최대 24개월간
국내주식 수수료 0원

이벤트 기간: ~12/31

※ 투자 전 설명 청취 및 상품설명서·약관 필독 ※ 이 금융상품(주식)은 예금자보호법에 따라 보호되지 않습니다. 다만, 예탁금 중 증권매수 미사용 현금 잔액은 예금자보호법에 따라 원금과 소정의 이자를 합하여 1인당 1억원까지(본 금융회사의 여타 보호상품과 합산) 보호됩니다. ※ 자산가격변동, 환율변동, 신용등급 하락 등에 따른 원금손실(0~100%) 발생가능 및 투자자 귀속 ※ 국내주식(ETF포함) 매매 시 수수료 온라인 0.01%~0.50%, 오프라인 0.40%~0.50%(KRX, NXT 포함)이며, 홈페이지 등 참고 ※ 당사가 부담하는 유관비용은 재산상이익 제공에 해당합니다.(동일인에 대한 재산상이익 제공 한도는 연간 최대 2억원) ※ 한국금융투자협회 심사필 제26-04352호(2026-09-23~2027-09-22)