핀테크와 금융 보안

글_ 배경훈 한양대학교 교수

금융 정보가 통합되면 새로운 가치가 생기는 것과 동시에 새로운 위험이 발생한다. 정보가 모여 있는 곳은 해커들의 타깃이 되기 쉽기 때문이다. 핀테크 산업의 지속적인 성장을 위해서는 금융기관 및 핀테크 회사의 보안에 대한 인식 제고와 투자가 그 어느 때보다 필요하다.

F i n t e c h
F i n a n c i a l s e c u r i t y

○ 해커들의 먹잇감, 개인 금융 정보

핀테크는 빅데이터, 인공지능, 암호화폐 등의 최첨단 기술을 기반으로 금융시장에서 혁신을 만들고 있다. 핀테크 혁신의 핵심은 흩어져 있는 고객들의 정보를 연결하고 통합하여 새로운 정보를 생산하고 이를 바탕으로 고객들의 편의성을 극대화하는 것에 있다. 예를 들면, 오픈 뱅킹 시스템에서는 은행 계좌, 신용카드, 보험, 부채 등의 정보들을 통합하고 한 플랫폼 내에서 고객들이 필요한 대부분의 금융 서비스를 제공하고 있다. 핀테크의 혁신적인 서비스에 가장 큰 리스크는 보안성이다. 금융 정보가 통합되면 새로운 가치가 생기는 것과 동시에 새로운 위험이 발생한다. 정보가 모여 있는 곳은 해커들의 타깃이 되기 쉽기 때문이다. 특히, 핀테크 회사에 의해 통합된 개인의 금융 정보들은 해커들의 가장 좋은 먹잇감일 것이다. 약 1억 5천만 명의 개인 정보를 유출한 미국 에퀴팩스(Equifax) 해킹 사건, 일본 NTT 도코모 전자결제 부정 인출 사건과 같은 일들이 핀테크의 성장과 함께 지속적으로 발생할 것은 자명한 일이다.

○ 군데군데 도사린 보안 위험 요소

핀테크의 보안 문제는 다음과 같은 요소들에 의해 심화된다.

① 타사와의 파트너십 체결로 인한 고객 데이터 공유

은행과 핀테크 회사와의 파트너십으로 인해 고객들의 데이터가 은행, 금융기관, 핀테크 기업에 걸쳐 공유된다. 이 과정에서 고객들의 데이터가 유출될 가능성이 높아진다.

② 시스템의 복잡성

핀테크 회사의 소프트웨어와 연결되면서 은행이 보유하고 있는 시스템은 더 복잡해진다. 소프트웨어가 통합되는 과정에서 해커가 공격할 수 있는 빈틈이 생길 수 있다.

③ 보안에 대한 인식의 부재

직원들이 해킹에 취약한 단순한 비밀번호를 사용하거나, 비밀번호를 다른 동료들과 공유하는 경우가 많다. 이와 같은 직원들의 보안에 대한 낮은 인식으로 인해 시스템이 해킹당할 가능성이 높아질 수 있다.

○ 보안에 대한 인식 재고 및 투자 필요

핀테크의 보안성을 높이기 위해 다음과 같은 대응책이 존재한다.

① 코드 난독화

해커가 회사의 주요 프로그램의 취약점을 파악하기 어렵게 하기 위해서 프로그램의 코드를 읽기 어렵게 난독화할 수 있다.

② Runtime Application Self-Protection (RASP)

프로그램이 해커의 공격을 실시간으로 식별하고 차단할 수 있도록 시스템을 설계한다.

③ 화이트 박스 암호

해커가 암호화 키를 쉽게 유추할 수 없도록, 암호화 키 자체를 암호화한다.

핀테크의 가파른 성장과 함께 보안이 필요한 금융 정보가 급속히 증가하고 있다. 핀테크 보안은 그 어느 때보다 거대한 도전을 직면한 상태이다. 핀테크 산업의 지속적인 성장을 위해서는 금융기관 및 핀테크 회사의 보안에 대한 인식 제고와 투자가 그 어느 때보다 필요한 시기이다.