경영유의사항 등 공개안

1. 금융기관명 : ㈜티머니

2. 조치일 : 2020. 2. 13.

3. 조치내용

대상	내용
기 관	경영유의사항 1건, 개선사항 6건

4. 조치대상사실

가. 경영유의사항

(1) 이상거래탐지시스템(FDS) 운영 실효성 제고

비정상 거래로 의심되는 전자금융거래에 대한 탐지·차단을 위해 이상거래탐지시스템(이하 “FDS”)을 구축하고 자체 수립한 탐지지표*를 총 4단계(차단, 경보, 예보, 주시)의 위험등급으로 분류하여 알림내역에 대한 모니터링을 수행하고 있으나,

* 교통, 충전, 유통, 환불, 모바일 거래에서 추출된 데이터를 활용하여 특이 거래, 특이 가맹점, 특이 카드, 정산 내용 등에 대한 이상거래 징후 설정

분실·도난카드에 대해서는 블랙리스트로 등재하는 등 카드 기반의 이상거래에 대해서는 사후 조치를 취하면서도, 접속에 사용된 스마트폰 단말정보에 대한 로그를 FDS와 연계하지 않아 단말기 기반의 공격 의심행위에 대해서는 대처가 어렵고

FDS에 등록된 탐지지표를 ‘차단’ 등급으로 설정하여 실제 사전조치가 가능토록 운영한 사례가 없어 FDS를 통한 사고예방 효과는 상대적으로 미흡하며, 2019년 탐지된 알림내역 총 OOO건 중 분석을 완료한 건은 OO OO여건으로 분석률이 56.7%에 불과하여 이상거래에 대한 적기 조치에 어려움이 예상되므로

스마트폰 단말기 기반의 공격의심행위에 대한 탐지를 위해 단말 관련 로그를 FDS와 연계하고, 이상거래에 대한 사전 ‘차단’ 효과를 거둘 수 있도록 탐지지표를 보완하는 한편, 이상거래 탐지 건에 대한 처리 결과 및 추이 분석 등에 대한 보고를 정례화하는 등 FDS운영의 실효성 제고 필요

나. 개선사항

(1) 스마트폰 앱 위·변조 방지 대책 불합리

스마트폰 전자금융 앱을 운영하면서 백신 프로그램, 앱 위·변조 방지 솔루션 등을 설치하고 앱 실행 시 프로그램 무결성 여부 및 백신 프로그램 설치 여부를 확인하는 등 보호대책을 적용하고 있으나,

'OOOOOOO' 및 'OOOOOOO' 앱에서는 앱 위·변조 방지 솔루션의 기능이 정상적으로 작동하지 않아 스마트폰 운영체제가 임의 개조된 상태 또는 앱 프로그램이 위·변조된 상태에서도 앱 실행이 가능하고

앱 개발·테스트 목적의 앱 OOOO가 배포된 'OOOOOOO' 앱에 남아있어 동 OO를 통해 백신프로그램 기동단계를 우회하는 경우 스마트폰에 대한 악성코드 감염 우려가 있는 등 공격자에 의해 앱 보안체계가 무력화될 가능성이 있으므로

스마트폰 운영체제의 임의개조 여부와 앱 프로그램 위·변조 탐지 등이 정상적으로 작동하도록 위변조 탐지 솔루션의 취약점을 보완하고, 배포된 'OOOOOOO' 앱에서 백신프로그램의 기동단계를 우회하는 OOOO를 제거하는 등 스마트폰 앱 위·변조 방지대책 개선 필요

(2) 스마트폰 앱 전자금융거래 보호대책 미흡

① 스마트폰 앱에서 ID 및 비밀번호 분실 시 이용자가 앱을 통해 이용자의 휴대폰번호를 전송하여 ID를 확인하고 OOOOOO를 동 휴대폰번호로 발송하는 절차를 운영하고 있으나,

휴대폰번호와 서버에 저장된 이용자의 휴대폰번호를 비교하지 않고 있어, 공격자가 OOOOO를 임의로 변조하여 전송하는 경우 OO의 ID 및 OOOOOO의 조회가 가능한 취약점이 있으므로 이용자의 계정정보 등 인증을 위한 수단 확인 시 서버에 저장된 휴대폰번호와의 일치 여부를 확인하는 등 본인확인 절차 개선 필요

② OOOOOO 앱에서 티머니 이용내역 조회를 제공하고, '티머니 선물하기 - 간편설정' 메뉴를 통해 타인의 휴대폰번호로 이용자의 티머니 잔액 송금이 가능하나,

이용내역 조회 시 OOOO 등 요청값에 대해 무결성 검증이 미흡하여 공격자가 동 요청값을 임의로 변조하여 전송하는 경우 OO의 모바일티머니 이용내역 조회가 가능한 취약점이 있고

‘OOOO’ 기능에도 무결성 검증이 미흡하여 공격자가 OO OOO 및 OOO의 OOOOO를 조작하는 경우 잔액송금 사고가 발생할 우려가 있으므로 스마트폰 앱 요청값에 대한 무결성 검증 절차를 개선하는 등 전자금융거래 보호대책 개선 필요

(3) 모바일티머니 앱 OOO 관리 불합리

모바일티머니 앱의 프로그램 소스코드 보호를 위해 난독화 프로그램을 설치하고 모바일티머니 카드번호 등 중요정보를 앱에 저장 시 암호화하고 있으나,

중요 소스코드, 문자열 등에 대해서는 난독화를 적용하면서도 중요정보 암호화에 사용하는 OOO에는 난독화를 적용하지 않아 스마트폰 앱 OOOO에 동 OOO 값이 평문으로 노출되어 있는 한편,

모바일티머니 이용자 모두에게 고정된 OOO를 공통으로 사용함으로써 공격자가 악성코드를 이용하여 이용자 스마트폰을 장악하거나, 모바일티머니 이용자의 암호화된 중요정보를 획득하는 경우 동 OOO를 이용해 중요정보를 쉽게 OOO 할 우려가 있으므로

모바일티머니 앱 이용자의 중요정보 보호를 위해 동 앱 내에 OOOO을 암호화하여 저장하고, 앱 서비스 이용시 OOO를 가변적으로 사용하는 등 앱 OOO 관리 방식 개선 필요

(4) 스마트폰 앱 취약점 보완조치 관리 불합리

스마트폰 앱의 취약점 분석·평가를 매년 실시하고 발견된 취약점에 대한 보완조치 이행계획을 수립하여 취약점을 보완하고 있으나,

일부 취약점은 ‘보안솔루션 적용 검토’ 등의 사유로 보완조치 이행이 지연되어 장기간(1년 이상) 조치되지 않는 상황임에도 이행 관리 부서에서는 이행기간내 조치 여부 확인 등을 체계적으로 통제·관리하고 있지 않고

조치완료 이후에도 일부 취약점이 반복적으로 재발견되는 사례가 있는 등 취약점 보완조치에 대한 이행결과 확인이 일부 미흡하며, 개발자를 대상으로 프로그램 개발보안 교육을 실시하지 않아 주요 취약점이 매년 발견되는 등 취약점 보완조치 이행 관리가 미흡하므로

발견된 취약점을 적기에 조치하고, 조치 이행결과를 명확하게 확인할 수 있도록 취약점 보완조치 이행관리 절차를 마련하고, 매년 재발견되는 주요 취약점에 대해 개발자를 대상으로 프로그램 개발보안 교육을 실시하는 등 취약점 보완조치 이행 관리 개선 필요

(5) 자체 보안성검토 운영 절차 불합리

전자금융 스마트폰 앱 개발시 자체 「앱 출시(배포) 가이드」에 따라 요건 정의, 개발, 테스트 및 출시 등의 절차를 거치고 있으나,

앱 개발 사항에 대한 '보안성 검토 요청' 및 '보안 부적합 사항에 대한 조치' 등 절차가 포함되지 않아 앱 개발에 대한 보안성 검토가 누락될 우려가 있고

내규 「보안점검 지침」 제10조에는 신규 전자금융업무 수행 및 전자금융거래 표준 등을 제정하는 경우 자체 보안성 검토를 수행하고 업무가 시행된 날로부터 7일 이내에 금융감독원에 결과 보고서를 제출하도록 정하고 있으나,

자체 보안성 검토 대상에 포함하는 신규 전자금융업무에 대한 기준이 명확하게 정의되지 않아 기존 전자금융서비스에서 부가되는 서비스를 출시하는 경우 또는 변경, 개편, 보안기능 추가에 따른 보안상 중요한 변경이 발생하는 경우 등의 사유로 앱 업데이트가 발생하는 경우에 대한 자체 보안성 검토가 누락될 우려가 있으므로

자체 출시(배포) 가이드에 '보안성 검토 요청' 및 '보안 부적합 사항에 대한 조치' 등을 추가하고, 자체 보안성 검토 대상의 선정 기준 및 절차를 명확히 하도록 내규를 보완하는 등 관련 절차 개선 필요

(6) 전자금융거래 이용약관 불합리

회사는 모바일티머니 서비스 등 전자금융업 영위를 위해 총 3종의 약관을 운영하고 있으나, 전자금융거래와 관련한 기본적인 사항에 대하여 회사의 「전자금융거래 이용약관」을 우선 적용한다는 문구가 나머지 개별 약관에 반영되어 있지 않아 약관 별로 내용이 상충되는 부분에 대한 혼란이 예상되고

「전자금융거래 이용약관」 제12조 등에 회사의 전자금융사고에 대한 손해배상 책임 및 면책 사유 등을 규정하고 있으나, 사고 발생에 있어서 '이용자의 고의나 중대한 과실이 있는 경우'로서 그 책임의 전부 또는 일부를 이용자의 부담으로 할 수 있다*는 취지의 회사 면책에 대한 법령상 '전제 조건'을 동 약관에 명시하지 않아 실무적으로는 회사가 이용자의 '고의 및 중과실' 여부를 증명하지 않고 배상 책임을 이용자에게 전가하게 될 여지가 있으므로

약관별 내용 상충을 방지하기 위해 「전자금융거래 이용약관」을 우선 적용한다는 문구를 개별 약관에 반영하고, 회사 면책에 대한 '전제 조건'을 법령상의 기준으로 약관에 명시하여 회사와 이용자 간의 불필요한 분쟁을 예방하는 등 약관 관리 개선 필요