경영유의사항 등 공개안

1. 금융기관명 : ㈜대신저축은행

2. 조치일 : 2020. 2. 13.

3. 조치내용

대상	내용
기 관	개선사항 6건

4. 조치대상사실

가. 개선사항

(1) 스마트폰 앱 고객정보 변경 인증절차 불합리

고객이 스마트폰 앱을 통해 OOOOO 등 고객정보를 변경하는 경우 O단계의 인증절차를 통과한 경우에만 고객정보를 변경 처리하고 있으나,

OOOOO 변경에 따른 고객정보 변경시 O단계 인증에서 OOO를 선택한 경우 휴대폰 소지인증만 확인하여 타인명의 OOOOO를 등록할 수 있고, 동 O단계 인증절차 수행중 스마트폰 앱의 메뉴를 변경해도 인증정보를 초기화하지 아니하여 인증절차 우회의 위험이 존재하므로

OOOOO 등 고객정보 변경시 통신사를 통해 휴대폰 명의자와 계좌 소유자의 일치 여부를 확인하고, O단계의 인증절차를 수행하고 있는 도중에 메뉴를 변경할 경우 인증정보를 초기화하는 등 고객정보 변경시 본인 인증절차를 개선할 필요

(2) 스마트폰 앱 위·변조 방지대책 불합리

스마트폰 앱 위·변조 방지를 위해 무결성 검증 보안솔루션을 적용하고 있으나,

OOO 기반의 앱에 대해서는 실행파일의 일부분에 대해서만 무결성 검증을 적용하여 악의적인 공격자에 의해 위·변조되어 실행될 우려가 있으므로

무결성 검증절차를 실행파일 전체영역으로 확대 적용하는 등 스마트폰 앱 위·변조 방지대책을 강화할 필요

(3) 스마트폰 앱 이용자 중요정보 보호대책 불합리

스마트폰 앱에서 이용자 본인인증시 촬영된 OOO 사진을 암호화하여 서버로 전송하고 OOOOO 비밀번호 등 중요정보의 노출을 방지하기 위해 가상 보안 키패드를 적용하고 있으나,

촬영된 OOO 사진 및 가상 보안 키패드를 통해 입력 받은 중요정보가 스마트폰에 평문으로 임시 저장되고 있어 악성코드가 설치되어 있을 경우 유출될 우려가 있으므로

OOO 촬영시 중요정보를 마스킹 처리하고, 메모리 초기화 등 메모리 보호기법을 적용하여 이용자의 중요정보가 노출되지 않도록 관련 프로그램을 개선할 필요

(4) 취약점 분석·평가 관리 불합리

취약점 분석·평가를 정기적으로 실시하여 취약점을 제거하고 잔여 취약점에 대해서는 단기 및 중기 조치계획 수립 후 정보보호위원회의 심의·의결을 거쳐 최고경영자에게 보고하고 있으나,

잔존 취약점에 대한 조치계획 수립시 구체적인 검토없이 조치 이행기한을 변경하는 등 장기간 미조치된 취약점에 대한 보안리스크가 높아질 우려가 있으며,

취약점 조치 후 조치결과의 적정성을 확인하지 않아 동일 취약점이 재발견되거나, 보안코딩 규칙을 소스코드 전반에 적용하지 않아 유사 취약점이 재발견되는 등 취약점 조치관리가 미흡하므로

조치계획 수립시 취약점의 위험도 및 위험 수용가능 여부 등에 따라 이행기간을 합리적으로 결정하고, 조치계획의 변경이 필요한 경우 정보보호위원회를 통해 보안리스크를 재검토하고 조치가 불가능할 경우 최고경영자의 승인을 득하는 한편, 취약점 조치내용의 적정성을 점검하여 조치결과의 완결성을 확인하고, 보안코딩 규칙을 소스코드 전반에 적용하는 등 취약점 분석·평가 관리절차를 개선할 필요

(5) 대고객서비스 통신회선 이중화 불합리

화재, 재해 등으로 인한 통신 장애시 스마트폰 앱의 안정적인 서비스 운영을 위하여 주요 업무는 통신회선을 이중화하여 운영하고 있으나,

대외기관과 연계하는 통신회선의 이중화가 일부 누락되어 회선 장애시 OOOOOO 업무가 중단될 수 있어 업무지속성 확보에 어려움이 예상되므로

장애 발생시 대고객 서비스 처리가 지연되지 않도록 단일회선으로 운영중인 업무에 대한 영향도를 분석하여 비상대책을 마련하거나 통신회선을 이중화하는 등 관련 업무를 개선할 필요

(6) 이상금융거래탐지시스템(FDS) 운영 불합리

OOOOO등 전자금융 거래시 비정상 거래행위에 대한 탐지·차단을 위해 이상금융거래 탐지시스템(FDS)을 구축하고 자체 수립한 이상거래 탐지정책을 적용하여 이상금융거래 로그를 기록·관리하고 있으나,

탐지되는 이상금융거래 로그에 대한 분석·보고 및 고객확인 절차 등의 조치는 이행하고 있지 않아 실제 이상금융거래 상황 발생시 즉각적인 대응에 어려움이 예상되므로

이상금융거래 로그에 대한 분석 및 고객확인 절차 등을 포함한 모니터링 절차를 마련하고, 탐지된 이상금융거래에 대한 분석·조치 결과를 주기적으로 책임자에게 보고하는 등 이상금융거래탐지시스템(FDS) 운영을 개선할 필요