경영유의사항 등 공개안

1. 금융기관명 : 롯데멤버스㈜

2. 조치일 : 2019. 3. 25.

3. 조치내용

대상	내용
기 관	경영유의사항 2건, 개선사항 5건

4. 조치대상사실

가. 경영유의사항

(1) 모바일 앱 부정사용 방지 대책 강화

앱 로그인 후 OOOO OOOO 등 OOOO 없이 오프라인 가맹점에서 포인트 사용이 가능하고, 2대 이상의 기기에서 동시에 OO OOO 접속을 허용하면서 포인트 사용 시 별도의 OOO 기능 등을 적용하지 않아 이용자가 제3자에 의한 도용 상황을 인지하기 어려우며

앱 부정사용을 방지하기 위해 자체 검토한 대책을 검사착수일 현재까지 적용하지 않아 모바일 앱 부정사용 사고 발생 위험이 있으므로

기 등록 스마트폰 이외의 앱 로그인 또는 포인트 사용 시 OOO OO 기능을 적용하는 한편, OOOOO을 제한적으로 허용하는 등 모바일 앱 부정사용 방지를 위한 보완 대책을 강화할 필요

(2) 포인트 소멸에 대한 이용자 안내 강화

「L.POINT 서비스 이용 약관」에 의하면 롯데멤버스 포인트의 유효기간은 적립월로부터 최대 O년(OO개월)으로 유효기관 경과 시 자동 소멸하고, 소멸 포인트에 대한 안내는 홈페이지 및 모바일 회원 정보에서 확인하거나 매월 발송하는 이메일 명세서를 통해 별도로 안내하도록 정하고 있는데,

약관에 따른 유효기간이 경과하여 소멸 포인트가 최초 발생한 2018.1.31.부터 현재까지 총 OOO원(OO명) 규모의 포인트가 소멸되어 회사의 잡이익으로 처리하였으나, 소멸

포인트에 대한 이메일 안내를 적시에 확인하지 못하여 이용자가 포인트 소멸에 대한 불만을 제기한 사례가 다수 존재하므로

소멸 포인트 안내 방법을 이메일 이외에 문자메세지(SMS) 또는 모바일 앱 Push 메세지 등으로 확대하는 등 이용자 안내 절차를 강화할 필요

나. 개선사항

(1) 모바일 앱 정보보호 대책 불합리

모바일 금융서비스 제공을 위해 iOS(애플社) 및 Android(구글社) 기반의 앱(L.POINT, L.pay) 프로그램을 개발·운영하고 있으나, 다음과 같은 보안 취약점을 개선할 필요

① 앱 소스코드(모듈) 위·변조 방지 대책

모바일 앱 소스코드에 대한 위·변조 방지를 위해 난독화* 프로그램을 적용하고 있으나,

Android 기반의 앱에 대해서는 기본적인 수준의 OO OOO 기능만 제공하고 OOO 기능 등을 미제공하여 소스코드 상의 OO OO 등이 해커에 의해 쉽게 해독될 수 있고,

iOS 기반의 앱에 대해서는 OOO가 되지 않아 앱 소스코드가 해킹 공격 등에 노출될 우려가 있으며 앱 취약점 분석·평가 결과 앱 배포 파일에 OOOOO를 이용하여 OOOO OO이 가능한 취약점이 발견되었으므로

앱 소스코드 보호기술 적용 시 OO OOO 이외 OO OOO 등 기능을 보완·적용하고, OOO 기반의 앱에 대해서도 OOOO 위·변조 방지 대책을 개선할 필요

② 중요 입력정보 보호 대책

모바일 앱 간편결제 비밀번호 등 중요 입력정보의 노출을 방지하기 위해 가상 보안키패드 솔루션을 적용하고 있으나,

L.pay 앱의 경우 OOOO OOOO 입력 시 OO O이 OO로 노출되고 있어 OO OOO를 감지하여 OOOO를 하는 악성코드가 설치되는 경우 OOOO가 노출될 우려가 있으므로

OOOO OOOO 등 중요 입력정보가 모바일 앱 화면상에 노출되지 않도록 마스킹 처리를 개선할 필요

③ 악성코드 감염 방지 대책

스마트폰 악성코드 감염 방지를 위해 앱 구동 시 OO OOOO의 설치 여부를 확인하고 최신 상태로 자동 업데이트 하고 있으나,

앱 구동 이후 이용자가 OO OOOO을 강제로 종료하거나 삭제하는 경우에도 앱이 실행되는 취약점이 있으므로

이용자가 OO OOOO OO OO하거나 OO하는 경우 앱 서비스 이용이 제한되도록 프로그램을 개선할 필요

④ 스마트폰 내 중요정보 저장·관리 대책

이용자에게 L.POINT 앱 OOOOO 기능을 제공하고 오프라인 가맹점에서 포인트를 이용한 바코드 결제 등을 위해 스마트폰 앱 디렉토리 내 OOO OOOO 및 OOO OOOO 등 주요 정보를 암호화하여 저장하고 있으나,

OOO OOO, OO OOO OO 등 일부 정보를 평문으로 저장하여 동 정보가 유출될 가능성이 있으므로

모바일 서비스 제공에 필수적인 항목 이외의 정보에 대한 스마트폰 내 저장을 최소화하고, 저장이 필요한 경우 안전한 알고리즘으로 암호화하여 관리하는 등 중요정보 저장・관리 대책을 개선할 필요

(2) 모바일 앱 취약점 분석·평가 관리 불합리

모바일 앱 취약점 분석·평가를 매년 정기적으로 실시하고 그 결과 및 보완조치 이행계획을 정보보호위원회 심의·의결을 거쳐 최고경영자에게 보고하고 있으며 취약점 제거 불가 시 '위험 수용'으로 최고경영자의 승인을 받고 있으나,

일부 취약점의 경우 보안 리스크가 높고 기술적으로 조치 가능한 항목임에도 '원활한 서비스 제공 목적' 등의 사유로 위험 수용으로 처리하였고, 취약점 미조치로 인해 발생 가능한 문제점을 상세하게 보고하지 않아 최고경영자가 보안 리스크를 인지하지 못할 우려가 있으며

취약점 보완조치 이행점검 후 관련 증빙을 확인하는 절차 없이 완료 여부에 대해서만 기록·관리하고 있어 취약점 제거 여부에 대한 객관적인 보증이 어려우므로

위험수용 사유에 대해 엄격히 판단하고 위험 수용으로 처리시 취약점에 대해서는 보안 리스크 평가 후 상세 내역을 최고경영자에게 보고하여 승인받으며, 취약점 보완조치 확인을 철저히 수행하는 등 관련 절차를 개선할 필요

(3) 자체 보안성 검토 운영 절차 불합리

내규 「정보보호지침」에 의해 중요 어플리케이션의 신규 개발 및 인증, 암호화 등 어플리케이션의 보안 기능 추가 등의 경우 자체 보안성 검토를 수행하고 보안 요건이 충족되지 않는 경우 해당 서비스 오픈을 제한 할 수 있으나,

'모바일웹 리뉴얼 오픈' 및 '간편결제 서비스에 결제방식 추가' 등 내규 상 보안성 검토가 필요한 어플리케이션 개발 건이 일부 발생하였음에도 자체 보안성 검토가 누락되었고

보안성 검토 결과 부적합한 것으로 도출된 항목에 대해서 최종 조치완료 여부 확인 없이 서비스 오픈을 허용하는 등 보안성 검토 절차에 대한 관리 미흡으로 인해 보안사고가 발생할 우려가 있으므로

보안에 중요한 영향을 미치는 어플리케이션 개발 건 등에 대한 보안성 검토 절차가 누락되지 않도록 보안성 검토 대상 선정 절차를 보완하고, 보안성 검토 결과 부적합 사항이 도출되는 경우 조치완료 여부에 대한 최종 확인 후 서비스가 오픈되도록 관련 절차를 개선할 필요

(4) 포인트 적립 처리 절차 불합리

마케팅 등을 목적으로 포인트(L.POINT)를 이용자에게 적립해주는 경우 마케팅 시스템을 통해 적립 대상자 및 적립 포인트를 추출·등록하고 책임자 승인 후 포인트를 일괄 적립하고 있으나,

포인트 적립 처리 과정에서 최대 포인트 적립 한도를 제한하는 등 입력 값 이상 여부를 검증하는 절차가 없고, 책임자 본인이 포인트 적립 대상자를 추출하여 등록하는 경우 자가 승인처리가 가능하여 포인트 적립 통제 절차를 우회할 가능성이 있으므로

포인트 적립 처리 과정에서 건별, 이용자별 최대 포인트 적립 한도를 제한하는 등 시스템 입력 값에 대한 검증 절차를 추가하는 등 포인트 적립 처리 절차를 개선할 필요

(5) 전산자료 백업·소산 관리 불합리

주전산센터(OO OOO 소재)의 데이터, 프로그램, 설정파일 등 주요 전산자료를 정기적으로 백업하고 원격지 본사(OO OO 소재)에 주 O회 소산하고 있으나,

모바일 관련 프로그램 및 설정 파일을 정기적인 소산 대상에 포함하지 아니하여 주전산센터에 재해 발생 시 데이터 복구에 어려움이 예상되므로

소산 정책을 재점검하여 전산자료 소산이 누락되지 않도록 하고, 소산 대상에서 누락된 모바일 관련 프로그램 및 설정 파일에 대해서 정기적인 소산을 실시할 필요