경영유의사항 등 공개안

1. 금융기관명 : 갤럭시아커뮤니케이션즈
2. 제재조치일(검사서 통보일) : 2017. 7. 31.
3. 제재조치내용

제재대상	제재내용
기 관	경영유의사항 2건, 개선사항 3건

4. 제재대상사실

가. 경영유의사항

(1) 간편결제 서비스 이용자보호 대책 강화

㈎ 간편결제 모바일 앱(OOOOO OOOO) 서비스 가입 시 휴대폰(SMS) 인증을 거치고, 사이버머니 충전을 위한 출금계좌 등록 시 휴대폰 명의자와 계좌번호 명의자 일치여부 및 계좌비밀번호(O자리)를 검증하고 있으나

해커가 피싱·파밍 등으로 수집한 고객정보(OOOOOO, OOOO, OOOOOO)를 도용하여 OOO을 OO하거나 OOO·OOO 인증을 우회하여 출금계좌를 등록하고 포인트 충전, 상품권 구입 등에 부정 사용할 우려가 있으므로

모바일 앱(OOOOO OOOO) 서비스에 취약점이 있는지 점검하여 보완이 필요한 경우 계좌 유효성 검증* 등을 통해 본인인증 절차를 강화할 필요

* 서비스 이용자에게 소액을 적요(난수)와 함께 송금하고, 이용자가 인터넷 뱅킹 등을 통해 동 송금내역을 조회하여 적요와 송금액을 입력하게 함으로써 본인 계좌에 대한 실제 점유 여부를 확인

㈏ 간편결제 관리시스템(https://OOO.OOOOO.co.kr)에서 고객정보 일괄조회 시 성명, 휴대폰 번호는 마스킹 처리하고 있으나, 조회 내용을 OO로 OOOO 하는 경우는 마스킹이 해제되어 성명, 휴대폰번호 등의 정보가 노출될 우려가 있음

간편결제 관리시스템에서 고객정보 OOOO에 대한 권한 통제 및 OOOO OO에서도 고객정보를 마스킹 처리하는 등 간편결제 서비스에 대한 이용자보호 대책을 강화할 필요

(2) IT부문 내부통제 강화

□ 전자금융업을 영위하면서 보안 담당자가 '정보보안점검의 날'에 주요 정보보안 관련 사항을 매월 점검·보고하고 있으나 IT부문 업무*에 대한 상시감사 체계가 마련되어 있지 않으므로

* 전산원장 변경 통제, 프로그램 변경 통제, IT장애·사고 관리, IT사업 추진 통제 등

점검항목, 점검방법, 점검주기 등을 포함한 IT자체감사 운영 절차를 마련하여 리스크가 높은 IT부문 업무에 대한 주기적인 감사를 실시하는 등 IT부문 내부통제를 강화할 필요

나. 개선사항

(1) 서버 접근통제 대책 불합리

□ 서버접근통제솔루션(OOO)을 도입하여 계정별로 서버 접근을 통제하고 있으나, 개인 계정으로 접속한 후 계정전환 명령어(OO, OOOO 등)를 입력하여 관리자 계정 또는 공용 서비스 계정으로 전환하여 관리자 권한 등을 사용하는 것이 가능하므로

개인 계정 및 공용 서비스 계정전환 명령어(OO, OOOO 등)의 사용 권한을 통제하여 권한 없는 자가 관리자 계정 등으로 접속하는 것을 차단할 필요

(2) 정보처리시스템 보안 대책 불합리

㈎ 내부직원만 이용하는 전자금융업무 관리자 사이트를 대고객 서비스를 위한 OOOO와 동일한 OOOO(OOO)에 설치·운영하고 있어 해킹 등 전자적 침해행위에 의한 사고가 발생할 우려가 있으며

㈏ OO 및 OOOO 등에 이용하는 OOOO(https://OO.OOOOOOOOOOOO.co.kr)는 적절한 보안 통제절차 없이 외부 인터넷망에서 접속을 허용하고 있어 내부정보가 외부로 유출될 우려가 있으므로

전자금융업무 관리자용 사이트는 내부망으로 이전하고, OOOO에 대한 접근은 가상사설망(VPN)을 이용하는 등 외부 인터넷망을 통한 시스템 접속을 통제하여 정보처리시스템 보안대책을 개선할 필요

(3) 업무용 단말기 보안대책 불합리

□ 기획·영업 업무를 담당하는 일부 직원의 업무용 단말기에 업무상 필수적으로 연결해야 하는 외부기관 이외에도 접속을 허용하고 있어 악성코드 감염 등에 취약할 우려가 있으므로

개인정보취급자 이외의 본사 직원의 내부 업무용 단말기에 대한 보안 대책을 강화하여 운영할 필요