경영유의사항 등 공개안

1. 금융기관명 : ㈜우아한형제들

2. 조치일 : 2019. 8. 28.

3. 조치내용

대상	내용
기 관	경영유의사항 2건, 개선사항 7건

4. 조치대상사실

가. 경영유의사항

(1) 클라우드 관련 전자금융거래 안전성 확보 대책 마련 필요

회사는 선불전자지급수단(포인트)을 이용하여 결제가 가능한 정보처리시스템을 OOO社의 클라우드컴퓨팅서비스(이하 “클라우드”) 환경에서 운영하고 있으나,

클라우드 이용절차에 대한 규정(「전자금융감독규정」 제14조의2)이 개정·시행(2019.1.1.)되기 이전에 동 시스템을 클라우드에 구축함으로써 클라우드 이용절차를 별도로 마련하지 않은 상태로 운영하여 전자금융거래의 안전성 확보가 어려울 수 있으므로,

「전자금융감독규정」 제14조의2에 따른 클라우드컴퓨팅서비스 이용절차를 면밀히 검토하여 수행하는 한편, 「금융분야 클라우드컴퓨팅서비스 이용가이드(금융보안원, 2019.1월)」 등을 참고하여 클라우드 관련 업무 절차를 IT내규에 반영하는 등 전자금융거래의 안전성 확보를 위한 대책을 마련할 필요가 있음

(2) 전자금융 및 IT부문 업무 내부통제 강화

회사는 ‘선불전자지급수단 발행 및 관리업’ 및 ‘전자지급결제대행업(PG)’ 등 전자금융업을 영위하고 있으나,

전자금융 및 관련 IT부문 업무에 대한 적정성을 주기적으로 점검하는 내부통제 체계가 갖추어져 있지 않아 전자금융 및 IT부문 업무 전반에 걸쳐 내부통제 미흡 사항이 발견되고 있으므로

전자금융 및 IT업무에 대한 적정성을 점검할 수 있도록 자체감사 등을 담당하는 내부통제 담당자를 지정하고 자체점검 항목 등을 마련하여 주기적으로 점검하는 등 내부통제 관리 체계를 강화할 필요

나. 개선사항

(1) 클라우드 관리시스템 접근통제 불합리

IT운영자가 OOO社의 클라우드컴퓨팅서비스(이하 “클라우드”) 환경에서 정보처리시스템을 생성·변경·삭제 또는 모니터링하기 위해 클라우드 관리시스템(OOO콘솔)에 접근하고 있으나,

동 관리시스템에 로그인이 가능한 위치를 회사 내부 네트워크 등으로 제한하지 아니하여 공격자가 악성코드 등을 통해 사외에서 접속하는 IT운영자의 단말기에서 로그인 정보를 탈취하는 경우 클라우드 환경에 구성한 모든 정보처리시스템에 위협을 가할 수 있는 보안 리스크가 있으므로

클라우드 관리시스템(OOO콘솔)에 로그인이 가능한 위치를 사내 IT관리 네트워크로 제한하고, 사외에서의 접속은 가상사설망(VPN)을 통해 장애 등 비상상황 대응 목적으로만 허용하는 한편, 접근이력에 대해서는 사후 확인하는 절차를 마련하는 등 클라우드 관리시스템의 접근통제를 개선할 필요

(2) 정보처리시스템 계정 관리 불합리

① 서버 최고관리자 계정 사용·통제 절차

내부사용자의 서버 계정에 대한 접근을 통제하고 접근이력 저장 등을 위해 접근통제 시스템을 설치·운영하고 있으나,

서버 최고관리자 계정 사용·통제를 위한 절차를 마련하지 않고 별도 승인 없이도 개발자가 본인 계정으로 로그인 후 사용자 전환 명령어를 통해 최고관리자 계정으로 전환이 가능한 상태로 운영하고 있어 개발자가 정당한 사유 없이 임의로 서버 위험 명령어를 사용할 위험이 있으므로

서버 최고관리자 계정으로 전환이 가능한 사용자를 제한하고, 동 계정은 장애 등 비상상황 발생 시에만 책임자의 승인 절차를 거쳐 사용토록 하는 등 서버 최고관리자 계정에 대한 사용·통제 절차 마련 필요

② 클라우드 서버 계정 분리 강화

클라우드 환경에서 운영되는 전자금융업무(OO포인트) 서버(OOOO-OOOO) 접속 시에는 개별 사용자 계정을 이용하여 접근통제시스템과 배스천 호스트(Bastion Host*)를 통한 사용자 인증 후에 접속하여 사용자별 접근이력에 대한 추적은 가능하나,

* 클라우드컴퓨팅서비스 환경에서 운영되는 정보처리시스템을 관리하기 위해 반드시 경유해야 하는 내·외부 네트워크 연결용(Gateway) 서버

시스템 관리자, 어플리케이션 개발자 등 주요 IT업무 역할에 따라 계정을 분리하지 않고 공용 어플리케이션 운영 계정(OOOOO)을 사용하고 있어 동일인이 여러 업무를 수행함으로 인하여 시스템 조작 등의 사고 발생 가능성이 있으므로

IT업무 역할별 상호견제 기능을 최대한 고려하여 클라우드 서버 계정을 IT업무 역할에 따라 분리·구성하는 등 작업 오남용에 따른 장애·사고 방지 대책을 개선할 필요

(3) 정보처리시스템 접근통제 절차 불합리

자체서비스 및 클라우드컴퓨팅서비스 환경에서 운영하는 전자금융 관련 정보처리시스템에 접근하기 위해서는 접근통제시스템 및 배스천 호스트 등을 경유하도록 통제 절차를 마련하고 있으나,

자체 및 클라우드컴퓨팅서비스 환경에서 운영하는 서버 모두 내부사용자가 서버접근통제시스템을 경유하여 서버에 접속한 후 다른 서버에 접속할 경우에는 동 시스템을 경유하지 않고 우회 접속이 가능하고,

클라우드컴퓨팅서비스 환경에서 운영하는 데이터베이스(DB)의 경우 접근통제시스템 구축 이전에 사용하던 경유 서버(OOOOO)를 통해 접속이 가능한 상태로 운영하여 회사의 서버 접근통제 및 모니터링 정책을 우회할 가능성이 있으므로

접근통제시스템을 경유한 접근 이외의 서버·데이터베이스로의 직접 접속 또는 우회 서버 접근경로(IP와 서비스 포트)를 모두 차단하는 등 정보처리시스템의 접근통제 절차를 개선할 필요

(4) 모바일 앱 정보보호 대책 불합리

모바일 앱 실행코드의 위·변조 방지를 위해 소스코드 난독화 프로그램을 모바일 앱(OOO OO)에 적용하고 있으나,

앱 구동 시 스마트폰 운영체제(OS)의 임의 개조(루팅, 탈옥 등) 여부 및 앱 프로그램의 위·변조 여부에 대한 검증 절차를 적용하지 아니하여

임의 개조된 운영체제가 설치된 스마트폰에서 앱 프로그램을 설치하거나, 공격자가 위·변조한 앱 프로그램을 설치하는 경우 스마트폰 및 모바일 앱의 보안 체계가 무력화될 수 있으므로

「스마트폰 전자금융서비스 보안가이드(금융보안원)」의 보안 권고사항 등을 참고하여 스마트폰 운영체제의 임의 개조 여부 및 앱 프로그램 위·변조 여부를 검증하는 절차 등을 추가하는 한편, 모바일 앱 위·변조 로그기록에 대한 모니터링 체계를 구축하여 이상거래 행위를 사전에 차단하는 등 모바일 앱 정보보호 대책을 개선할 필요

(5) 모바일 앱 부정사용 방지 대책 불합리

모바일 앱(OOO OO) 가입 및 접근매체(OO·OOOO) 발급 시 휴대폰 번호를 입력받고 이동통신사의 휴대폰 인증(SMS) 절차를 적용하고 있으나,

동 인증 절차는 모바일 앱이 구동되는 휴대폰의 OOO(OOO) 확인이 아닌 휴대폰 OO에 대한 OO(OO) 여부를 검증하기 위한 용도로 사용하고 있어 OO·OOOO 등 노출 시 OOO의 OOO에서 O OO된 OOOO으로 간편결제 도용이 가능하며

OO OO의 기기에서 OO OOO 기능을 허용하면서도 모바일 앱 결제 시 이용자 본인에게 별도 알림(SMS 또는 Push 메세지 등)을 실시하지 않아 이용자가 제3자에 의한 도용 상황을 사전 인지하기 어려우므로

모바일 앱(OOO OO)의 OOOOO 기능을 기본 제한하되 이용자가 O OO에서의 OOOOO 사용 여부를 선택할 수 있도록 구현하고, 앱 결제 시 이용자에게 별도 알림(SMS 또는 Push메세지 등)을 적용하는 등 모바일 앱 부정사용 방지를 위한 대책을 개선할 필요

(6) 포인트 관리 업무 절차 불합리

이벤트 또는 고객응대 등의 목적으로 이용자에게 포인트(OO포인트)를 부여하는 경우 담당자가 포인트 관리시스템에서 이용자 별 해당 포인트를 수작업으로 입력하여 충전하고 있으나,

포인트 관리시스템에는 이용자 별 포인트 충전 한도 등을 제한하는 등 입력 값의 유효성을 검증하는 절차를 적용하지 않아 담당자가 실수로 포인트를 오입력하는 경우 과다 충전·차감되는 등 사고의 우려가 있으므로

포인트 관리 업무의 특성을 감안하여 개별 포인트 충전 한도 및 누적 포인트 충전 최대한도(50만원, 실지명의로 발행된 경우에는 200만원) 등을 시스템에 설정하여 입력 값의 유효성에 대하여 검증하고, 수작업으로 포인트를 충전·차감하는 업무에 대한 적정성을 정기적으로 확인하는 등 포인트 관리 업무 절차를 개선할 필요

(7) 내부자료 반출 통제·관리 불합리

네트워크 장치 및 저장매체 통제, 불법 응용프로그램 차단, 악성코드 감염 방지 등을 위해 업무용 단말기에 PC보안프로그램을 설치·운영하고 있으나,

동 보안프로그램에서는 OOOO 및 OOO OOOO 연결, OOOO 사용 차단 등의 보안 정책을 주요 업무담당자(O명)에게만 제한적으로 적용하고 있어 다수 직원이 별도의 승인 없이 OOOO 이용이 가능하고

외부 이메일 발송에 대한 통제 정책을 마련하지 아니하여 업무 목적 이외에 개인정보 파일 등이 포함된 중요 내부자료가 외부로 반출될 우려가 있으므로

PC보안프로그램에서 OOOO 및 OOO OOOO 연결, OOOO 사용 차단 등의 보안 정책을 확대 적용하고, 외부 이메일 발송 통제 및 모니터링 정책을 마련하는 등 내부자료 반출 통제·관리를 개선할 필요