경영유의사항 등 공개안

1. 금융회사명 : ㈜신세계아이앤씨

2. 조치일 : 2019. 4. 22.

3. 조치내용

대상	내용
기 관	경영유의사항 2건, 개선사항 6건

4. 조치대상사실

가. 경영유의사항

(1) 이상금융거래 탐지시스템 운영 강화

전자금융거래시 비정상 행위 등에 대한 이상금융거래 탐지 및 예방을 위해 이상금융거래탐지시스템(FDS)을 구축·운영하고 있으나,

분실도난, 명의도용, 계좌탈취에 의한 이상거래 등의 탐지정책을 등록하여 총 OOOOOO건의 이상금융 의심거래가 탐지되었음에도, 실제 부정사용 여부에 대한 확인 및 거래 차단 등의 사후처리가 다소 미흡하여 유사 이상금융거래가 반복적으로 발생할 우려가 있으므로

앞으로 이상금융거래에 대한 신속한 탐지·차단을 위해 탐지정책을 추가·보완하고 분석 및 조치방안 등을 포함한 모니터링 절차를 마련하여 탐지된 의심거래에 대한 분석·조치 결과를 주기적으로 최고경영자에게 보고하는 등 이상금융거래 탐지시스템 운영을 강화하시길 바람

(2) 업무연속성 확보대책 강화

내규「업무연속성 관리 지침」에 따라 장애 등 비상상황 발생시 시스템 중단시간을 최소화하기 위하여 전체시스템에 대하여 재해복구시스템을 갖추고 연 1회 비상대응훈련으로 재해복구시스템 가동 및 전자적 침해 대응 훈련을 실시하고 있으나,

재해복구시스템 가동 훈련시 재해복구시스템을 실제 가동시키지 않았고, 일부 직원만 훈련에 참여하고 있어 비상상황 발생시 실질적인 대응이 곤란해 질 우려가 있으므로

내규 「재해복구 운영계획서」 및 「재해복구 시스템 기동 절차서」에 따라 재해복구 훈련을 계획·진행하고 모의훈련시 IT부서 직원이외에 현업 인력 등이 참여하도록 하여 재해복구훈련의 실효성을 강화하시기 바람

나. 개선사항

(1) 전자금융업무에 대한 보안성 검토 미흡

내규「정보보호시스템 관리지침」,「서버 보안관리 지침」에 의하면 서버, 보안장비 등 정보시스템은 구축전에 시스템 보안성에 대한 검토를 실시하여야 하고

「개발보안지침」 및 「모바일보안지침」에 따라 전자금융거래 관련 프로그램을 개발 또는 변경시 취약점 점검 등을 포함한 자체 보안성 검증을 실시하여 발견된 미흡사항에 대한 보완조치를 완료한 후 운영시스템에 이관하여야 하는데도

OOOOOO 모바일 앱 신규기능 확대 및 고도화, OOOOOOO 구축 등 내규 상 보안성 검토 및 검증이 필요한 총 O건의 전자금융서비스 또는 앱 변경 건에 대해 자체 보안성 검토 및 검증을 수행하지 아니하고 서비스를 오픈하였고

OOOOOOO 서비스 구축사업은 자체 보안성 검토 및 검증을 실시하였으나, 검증결과 발견된 미흡사항에 대한 최종 조치완료 여부 확인 없이 서비스 오픈을 허용하는 등 보안성 검증 및 검토가 일부 미흡하여 보안사고가 발생할 우려가 있으므로

전자금융거래 관련 프로그램 신규 개발 또는 변경 등 보안성 검토 및 검증이 필요한 경우 보안성 검토를 철저히 실시하고, 보안성 검토 실시 결과 발견된 미흡사항에 대한 보완조치 완료 후 운영시스템에 이관할 수 있도록 관련 절차를 개선하시기 바람

(2) 모바일 앱 취약점 분석·평가 미흡

모바일 앱에 대한 취약점 분석·평가를 매년 정기적으로 실시하고 업무담당자가 취약점을 제거한 후 취약점 잔존여부에 대해 재점검을 실시하여 점검결과를 최고경영자에게 보고하고 있으나,

취약점 조치여부에 대한 증빙자료를 확인하지 아니하고 취약점 별 조치완료 여부를 최고경영자에게 보고하고 있어 취약점 제거 여부에 대한 객관적인 보증이 어렵고

'OOOOOOOOOOOO' 등 일부 취약점은 최고경영자에게 조치완료로 보고되었으나, 검사착수일 현재 취약점이 잔존하고 있어 최고경영자가 보안 리스크를 인지하지 못하여 전자금융서비스의 보안이 취약해질 우려가 있으므로

취약점 분석·평가 결과에 따른 이행계획을 수립하여 취약점 제거 또는 이에 상응하는 조치 후 최고경영자에게 보고하고, 발견된 취약점에 대한 조치 증빙을 확인하여 취약점을 체계적으로 추적·관리하여 상세 내역을 최고경영자에게 보고하는 등 취약점으로 인한 IT보안사고가 발생하지 않도록 취약점 분석·평가 및 사후관리를 개선하시기 바람

(3) 모바일 프로그램 변경관리 미흡

내규 「변경관리프로세스」에 프로그램 변경, 구현, 테스트의 절차가 정의되어 있고 모바일 앱 프로그램 개발시 프로그램 변경 전후 내용을 기록하기 위해 형상관리 프로그램을 이용하고 있으나,

내규에 개발, 변경, 테스트 관련 절차가 구체적으로 명시되어 있지 않아 업무수행이 일관되게 이루어지지 않고 있으므로

프로그램 변경시 테스트 관련 절차 등을 프로그램 개발 관련 내규에 구체적으로 반영하고 동 절차에 따라 형상관리프로그램을 개발 및 관리하시기 바람

(4) 전산장애 기록 관리 미흡

내규「정보보호시스템 관리 지침」및 「전결합의규정」에 따라 각 시스템 담당자는 장애조치 후 장애영향도 및 조치내역을 업무주관 부서에 통지하고, 장애보고서를 작성하여 담당임원에게 보고·결재하여야 하는데도

장애발생시 업무 영향도, 심각도 등에 따른 장애등급 등을 포함한 지침을 마련하지 아니하여 부서별로 장애보고서 양식이 상이하고 장애발생 시 장애일시, 장애내용 및 조치사항 등을 기록한 장애상황기록부를 작성·보관하지 아니하였으며

정보처리시스템 장애 등으로 10분 이상 전산업무가 중단 또는 지연된 장애사고 O건은 장애발생 사실 및 조치내역이 담당임원에게 보고되지 않는 등 장애사고에 대한 관리통제가 미흡하므로

전산장애에 대해 자체 장애등급·분류 기준을 마련하고 장애일시, 장애내용 및 조치사항 등을 장애보고서에 상세히 기록·관리하는 한편 장애보고서의 임원 보고가 누락되지 않도록 보고절차를 강화하는 등 장애관리 프로세스를 개선하여 운영하시기 바람

(5) 백업데이터 검증·소산 미흡

(가) 내규「시스템 운영 지침서」에 따라 서버에 저장된 소스, 로그 및 데이터베이스 데이터 등을 재해복구센터에 백업·소산하고 백업 완료시 데이터 정상여부를 주기적으로 확인하고 재해복구센터로 전환훈련시 모바일 전자상품권 데이터의 검증을 실시하고 있으나,

모바일 전자상품권 이외의 백업된 자료에 대한 복구테스트는 누락하여 재해 발생시 백업데이터가 복구되지 않을 우려가 있으므로,

백업된 데이터에 대해서 정기적인 검증시 전체 백업·소산매체에 대해 누락없이 복구 테스트를 실시하시기 바람

(나) 내규「시스템 운영 지침서」에 따라 서버 및 데이터베이스의 설정파일 및 로그 등 전산자료를 일·주 단위로 테이프에 백업하여 보관하고 있으나,

백업테이프의 경우 내화 금고에 보관하지 않아 화재 등 재해발생시 백업 데이터 복구에 문제가 생길 우려가 있으므로,

백업테이프를 내화금고 등 안전한 장소에 보관하는 등 전산자료 소산 관련 절차를 개선하시기 바람

(6) 모바일 앱 부정사용 방지대책 미흡

모바일 앱 부정사용을 막기 위해 중복 로그인을 차단하고 기등록된 휴대폰 번호의 명의인이 다른 휴대폰 번호로 로그인하는 경우 기충전한 선불전자지급수단을 즉시 사용할 수 없도록 제한하고 있으나,

타인이 명의를 도용하여 휴대폰을 개설하고 동 휴대폰을 이용해 도용된 명의인의 정보로 앱에 로그인하는 경우에 기등록된 명의인에게 타 기기의 로그인에 대한 추가통지를 하지 않아 명의가 도용된 사용자는 앱을 실행한 경우에만 팝업을 통해 도용된 사실을 알 수 있어 모바일 앱 부정사용 발생 가능성에 대해 사용자가 즉시 인지하기 어려우므로

타 기기에서 로그인 시 기존 등록된 명의인의 정보를 이용하여 사용자에게 추가 통지하는 절차를 추가하는 등 모바일 앱 부정사용 방지 대책을 개선하시기 바람