경영유의사항 등 공개안

1. 금융기관명 : NH저축은행

2. 조치일 : 2023. 2. 10.

3. 조치내용

대상	내용
기관	개선사항 6건

4. 조치대상사실

가. 개선사항

(1) 모바일 앱 고객 통지대책 미흡

회사의 자체 모바일 앱을 이용하여 금융소비자에게 다양한 모바일뱅킹서비스를 제공하고 있으며 동 모바일 앱을 최종적으로 설치·인증한 단말기를 통해서만 전자금융서비스를 이용할 수 있도록 멀티 디바이스 환경을 제한하고 있으나,

불상자가 인증정보를 도용하여 고객이 모바일 앱을 설치·인증하지 않은 다른 단말기에 모바일 앱을 설치하고, 인증을 우회하여 ◎◎◎ 서비스 등을 부정 가입할 가능성이 있음에도 고객통지 대책을 마련하지 아니하여 고객 피해가 확대될 소지가 있으므로

고객이 부정가입 사실을 조기에 인지할 수 있도록 모바일 앱 고객 통지대책을 마련하시기 바람

(2) 사이버 침해대응 모니터링 관리체계 미흡

① 회사는 내규에 따라 홈페이지 등 공개용 웹서버의 안전한 관리를 위하여 □□□ 구간에서 운영 중인 공개용 웹서버에 암호화 통신 기술을 적용하고 웹서버와 이용자간 ▼▼▼ 서비스에 대하여 구간 암호화 등 보호대책을 운용중에 있으나,

해킹 방지 등의 목적으로 도입·운영 중인 침입방지시스템(IPS)에서 ◈◈◈에 대한 해킹시도를 적절하게 탐지·방어할 수 있는 수단이 마련되어 있지 아니함에 따라 ◆◆◆ 구간에서 사이버 침해시도 발생시 침해대응을 위한 보안분석이 곤란하여 즉각적인 대응에 어려움이 예상되므로

□□□ 구간에서 처리되는 암호화된 트래픽에 대한 모든 보안이벤트를 확보하고 사이버 침해시도에 실시간 방어할 수 있도록 사이버 침해대응 모니터링 관리체계를 개선하시기 바람

② 사이버 침해사고에 대응하기 위해 보안관제서비스를 ㈜△△△에 위탁·운영하고 있으나,

보안관제 범위를 ♤♤♤ 구간에 한정함에 따라 ▣▣▣ 구간에서 발생한 바이러스 등 악성코드로 인한 감염사고 등 단말기 이상징후 발생시 사이버 침해사고를 실시간으로 인지할 수 있는 방안이 부족하므로

통합보안관제시스템 고도화 및 관제범위 조정 등을 통하여 ▣▣▣ 구간에서 발생할 수 있는 바이러스 등 이상징후도 실시간 모니터링이 될 수 있도록 보안관제 서비스 운용환경을 개선하시기 바람

(3) 시스템 접근통제 관리 미흡

① 내규에 따라 비인가자에 의한 침해를 방지하고 운영시스템에 대한 접근통제 강화를 위하여 서버접근통제시스템 및 DB접근통제시스템을 도입하고, 인가자에 대해서만 시스템 접근을 허용하는 등 비인가자가 운영시스템에 임의로 접근하는 것을 통제하고 있으나,

각 접근통제시스템에 접근이 가능한 단말기 IP를 개별로 지정하고 있지 아니하고 특정 IP대역으로 전부 허용하여 운영함에 따라 운영시스템에 대한 접근통제 정책이 소홀해질 우려가 있으므로

서버접근통제시스템 및 DB접근통제시스템에 접근 가능한 IP를 사용자별로 각각 지정하는 등 운영시스템에 대한 사용자 접근통제 관리체계를 개선하시기 바람

② 내규에 따라 서버에 대한 위협, 취약점 보호대책 등을 수립하고 서버접근통제시스템에서 관리자 권한 상승 등이 가능한 일부 명령어 실행을 통제하는 등 서버 보안대책을 마련·운영하고 있으나

일부 중요 명령어 실행을 통제하지 아니하여 고의·과실로 인해 서버 시스템의 데이터가 삭제되거나 시스템이 중단되는 등 보안상 위협이 발생 될 소지가 있으므로

서버접근통제시스템에서 보안위협을 야기할 수 있는 중요 명령어에 대한 실행을 추가로 통제하는 등 서버 보안대책을 개선하시기 바람

③ 내규에 따라 DB시스템 접근시 사용자 인증과정을 거치고 DB접근통제시스템에서 DB시스템에 대한 접근권한을 개인별로 차등 부여하고 있으나

♠♠DB에 IT직원이 접속하거나 조회하는 경우 접속사유 입력 등 별도 통제 절차를 마련하지 아니하여 업무목적 이외의 불필요한 DB조회 발생 및 접속 이력에 대한 사후관리의 어려움이 예상되므로

DB접근통제시스템을 통해 ♠♠DB에 접속하는 경우 사유입력 및 조회시 사전 승인 등의 충분한 통제를 거치도록 DB시스템에 대한 접근통제 절차를 개선하시기 바람

(4) 취약점 점검 업무 소홀

① 모바일 및 웹서비스에서 발생할 수 있는 웹취약점 공격에 대응하고 프로그램 개발 단계부터 소스코드에 존재할 수 있는 잠재적인 보안취약점을 제거하기 위해 ○○○○.○.○. 소스코드 취약점 분석 솔루션을 도입하였으나,

검사착수일 현재까지 동 솔루션을 이용하여 소스코드를 분석한 실적이 전무하므로,

운영 중인 모바일 및 웹서비스에 프로그램 추가·변경시 해당 소스코드에 대한 취약점 분석 및 조치를 완료한 뒤 운영시스템에 적용될 수 있도록 형상관리시스템에 소스코드 취약점 분석 솔루션을 연동하는 등 관련 업무절차를 개선하시기 바람

② 내규에 따라 전자금융기반시설에 대해 연1회 이상(홈페이지는 6개월에 1회 이상) 취약점 분석·평가를 실시하고 그 보완조치 이행계획을 수립·시행하고 있으나,

발견된 취약점에 대한 보완조치 이행 증적을 별도로 보관하고 있지 않아 취약점 조치 완결 여부를 확인하기 어렵고, 점검대상 시스템에 대한 지정기준이 마련되어 있지 아니하여 대상 시스템이 매년 큰 폭으로 변동되는 등 중요 시스템이 점검대상에서 누락될 소지가 있으므로

향후 취약점에 대한 조치 결과를 확인할 수 있도록 취약점 조치 완결 여부에 대한 증적자료를 별도로 확보하고, 전자금융기반시설 취약점 분석·평가시 중요 시스템이 점검대상에서 누락되지 않도록 점검대상 시스템 지정기준을 수립하여 내규에 반영하는 등 취약점 점검 관련 업무절차를 개선하시기 바람

(5) 단말기 내 개인정보 관리 미흡

내부 전산자료 보호를 위해 개인정보검출솔루션 및 문서보안솔루션 등 보안시스템을 도입·운영하고 있으나,

임직원이 단말기에 개인정보가 포함된 파일을 저장하는 경우 단말기 내

개인정보 보관에 관한 관리 책임자의 승인 등 별도의 관리절차가 존재하지 않아 단말기 내 개인정보가 포함된 파일이 개인정보 처리의 목적을 달성한 이후에도 파기되지 않고 존재할 가능성이 있으므로

단말기 내 개인정보가 포함된 파일을 저장하는 경우 관리 책임자에게 승인을 받도록 하고 감사부서 혹은 IT자체감사인이 개인정보 보관 여부를 점검하는 절차를 마련하여 내규에 반영하는 등 단말기 내 개인정보 보관에 대한 관리절차를 개선하시기 바람

(6) 중요단말기 보호대책 미흡

중요단말기로 지정된 단말기에 대해서는 외부반출, 인터넷 접속 금지 등 강화된 보호대책을 적용하고 있으나

검사착수일 현재 중요단말기 지정기준이 관련 내규에 반영되어 있지 않아 중요단말기 지정이 누락될 우려가 있으며,

중요단말기와 일반단말기가 동일한 IP대역에서 동시에 운용됨에 따라 중요단말기에 적용 중인 강화된 보호대책의 무결성이 저해될 소지가 있으므로

중요단말기 지정기준을 수립·마련하여 내규에 반영하고, 중요단말기와 일반단말기를 서로 다른 IP대역으로 분리하는 등 중요단말기에 대한 관리 정책을 개선하시기 바람