경영유의사항 등 공개안

1. 금융회사명 : KB증권㈜

2. 조치일 : 2018. 4. 9.

3. 조치내용

대상	내용
기 관	개선사항 7건

4. 조치대상사실

가. 개선사항

(1) 이용자정보 조회에 대한 모니터링 불철저

고객 관련자료 분석, 이벤트 지원 등을 위하여 온라인 분석시스템(OLAP)을 구축·운영하고, 임직원 등 내부 사용자가 시스템에서 고객명, 생일, 주소 등 이용자 정보를 조회하여 고객 홍보 등에 활용하고 있으나

이용자 정보 조회의 적정성, 과다조회 등을 모니터링하는 절차가 마련되어 있지 않아 업무에 필요하지 않은 이용자 정보 조회 등으로 이용자 정보가 외부에 유출될 우려가 있으므로

이용자정보 조회에 대한 모니터링 절차를 마련하여 정기적으로 실시하는 등 이용자정보 보호를 강화하시기 바람

(2) 서버 보안패치 및 기술지원 관리 불철저

서버의 중요 보안패치(patch) 작업은 심각한 취약점이 발견될 경우 수작업으로 실시하고 있으나

전체 서버에 설치된 소프트웨어 종류 확인 및 패치 적용대상 여부 등을 모니터링 하지 않는 등 서버 보안패치와 관련한 체계적인 관리가 미흡하고

대외 전단처리(Front-End Processor) 개발기 등 일부 시스템에서 기술지원이 종료된 운영체제를 사용하고 있어 취약점 보완 및 기능개선 등을 위한 보정이 불가능해짐에 따라 신규 취약점을 이용한 해킹 및 악성코드 등에 의한 침해 우려가 있으므로

서버 패치작업을 체계적으로 관리하기 위해 패치관리시스템을 도입하고, 기술지원이 종료된 운영체제의 구체적인 전환추진 계획을 수립하고

응용프로그램과의 호환성 문제로 업그레이드가 불가능한 경우 네트워크를 분리 구성하는 등 침해사고 발생 가능성을 최소화할 수 있도록 관련 시스템 보안대책을 마련할 필요가 있음

(3) 단말기 보안대책 불합리

정보처리시스템 및 데이터베이스에 직접 접속하는 관리자 단말기를 중요 단말기로 지정하고, 외부 반출, 인터넷접속, 그룹웨어 접속 금지 등 강화된 보호대책을 적용하고 있으나

재해복구시스템에 직접 접속하는 단말기 ▨▨대와 정보보호시스템(방화벽 등)에 직접 접속하는 단말기 ♤대에 대해서는 강화된 보호대책을 적용하지 않고 있으며

강화된 보호대책이 적용된 目目대에 대해서도 사내 메신저 접속을 허용하고 있어, 메신저를 통해 주요 전산자료 등이 유출될 우려가 있으므로

재해복구시스템에 직접 접속하는 단말기 ▨▨대와 정보보호시스템(방화벽 등)에 직접 접속하는 단말기 ♤대를 중요 단말기로 지정하여 강화된 보호대책을 적용하는 방안을 검토할 필요가 있으며, 중요 단말기를 통해 사내 메신저에 접속할 수 없도록 통제를 강화할 필요가 있음

(4) 백업자료의 소산 추가 및 데이터 검증 불합리

전산자료의 장애, 재해, 테러 등 비상사태에 대비하여 기간계 및 정보계 데이터베이스 및 주요 소스코드 등의 전산자료를 정기적으로 백업하여 소산하고 있으나,

콜센터 등 고객의 녹취파일, 주전산기기의 바이너리 파일 등에 대한 전산자료를 소산하지 않고 있으며

소산장소에 소산하고 있는 전산자료 중 기간계 및 정보계 원장 데이터베이스는 주기적으로 복구 테스트를 시행하여 정합성 검증을 시행하고 있으나,

데이터베이스 파일이 아닌 일부 소산 데이터(소스코드 등)에 대해서는 소산 데이터에 대한 복구 테스트를 시행하지 않아 데이터의 정합성이 확인되지 않으므로

비상사태 발생 시 고객 응대 및 서비스 연속성 확보를 위하여 콜센터 등 고객의 녹취파일, 주전산기기의 바이너리 파일에 대하여 소산을 실시하고, 데이터베이스 파일 외 소산 데이터에 대해서도 주기적으로 복구 테스트를 시행하여 정합성 검증을 실시하는 등 백업 데이터 검증을 강화할 필요가 있음

(5) 외부 PC의 가상사설망(VPN)을 통한 내부망 접속 관리 불철저

「전자금융감독규정시행세칙」 제2조의2(망분리 적용 예외) 제2항제3호에 따라 야간 또는 공휴일에 서비스 장애처리 등을 위해 외부에서 정보처리시스템에 접속 시 가상사설망을 통하여 내부망에 접속하여 업무를 수행하고 있으나

외부 PC에서 VPN을 통한 내부망 접속시 접속과 동시에 외부PC의 인터넷 연결이 차단되는 등의 보안대책을 적용하지 않아, 외부 PC가 악성코드에 감염되었을 경우 해킹의 경로로 악용될 가능성이 있으며,

VPN 접속을 위한 사전 승인 없이도 야간 또는 공휴일에 관제근무자에게 유선으로 신청하여 VPN 접속 권한을 부여받고, VPN관리자가 사후적으로 부서장에게 VPN 접속자 명단을 보고하고 있으나 VPN 접속 이후 수행한 작업 내역에 대해 점검하지 않고 있는 등 통제가 미흡하므로

외부 PC에서 VPN을 통한 내부망 접속시 접속과 동시에 외부 PC의 인터넷 연결이 차단되도록 하는 등 해킹을 방지할 수 있는 대책을 마련하고,

VPN을 통한 내부망 접속자에 대해 사전 승인절차를 마련하여 접속 권한은 최소 인력에게만 부여하여 관리자의 사전 승인을 득하도록 하고, VPN 접속 이후 작업 수행 내역에 대한 적정성을 점검할 수 있도록 관련 절차를 개선할 필요가 있음

(6) 인터넷망 통제 불철저

방화벽, 정보유출방지솔루션, 유해사이트 차단 솔루션 등의 정보보호시스템을 통해 비인가 사이트에 대한 접근을 차단하고 정보유출을 방지하고 있으나

검사착수일 현재 인터넷 전용 단말기에서 인터넷 통제정책을 우회하여 비인가 사이트 접속이 가능하며,

♧♧ 브라우저를 이용하는 경우 정보유출방지솔루션이 정상적으로 작동하지 않고 있으므로

인터넷 전용 단말기에서 불법 프로그램 다운로드 사이트 및 유해사이트 목록을 주기적으로 업데이트하고 불법프로그램 설치를 차단하도록 운영하며 보안프로그램 업데이트 적용 전 보안솔루션의 동작 여부를 사전에 확인하는 등 인터넷망 통제를 강화할 필요가 있음

(7) 서버 접근통제 불합리

정보처리시스템에 접속 통제를 위하여 서버 접근통제 솔루션을 도입하여 비인가자의 서버 접근을 차단하고 있으며,

유닉스, 리눅스 서버의 비밀번호 정책은 숫자, 영문자, 특수문자를 조합하여 8자리 이상으로 구성하고, 변경 주기는 90일로 지정하여 운영하고 있으나,

일부 윈도우즈 서버의 경우 서버 접근통제 솔루션을 우회하여 직접 접속이 가능하여 비인가자의 서버 접근통제 및 접근내역 기록관리가 제대로 이루어지지 않고 있으며

서버 계정의 비밀번호와 연동되어 구동되는 서비스가 비정상적으로 작동된다는 이유로 윈도우즈 서버에 대해 비밀번호 정책을 적용*하지 않고 있으므로

* 비밀번호 8자리 이상, 변경주기 90일 지정 등

윈도우즈 서버에 대해서 접근통제 솔루션을 우회하여 직접 접속이 되지 않도록 접근 통제를 강화하고

윈도우즈 서버의 계정 비밀번호 정책을 리눅스, 유닉스 서버와 동일하게 서버 접근통제 솔루션과 연동하여 비밀번호 변경주기에 맞춰서 변경하는 등으로 비밀번호 정책을 개선할 필요가 있음