경영유의사항 등 공개안

1. 금융회사명 : 키움증권㈜

2. 조치일 : 2018. 8. 16.

3. 조치내용

대상	내용
기 관	경영유의사항 3건, 개선사항 4건

4. 조치대상사실

가. 경영유의사항

(1) 전산사업계획 및 수행관리 강화

내규「전산운영위원회 규정」에 따라 전산관련 중요사항을 심의·결정하기 위해 검사대상기간 중 전산운영위원회를 총 O회 개최하였으나,

전산사업계획 수립 후 별도의 검토 절차 없이 일부 사업 일정을 연기하는 등 수립된 전산사업계획에 대한 사후관리가 소홀하고,

내규상 장단기 IT추진계획 수립, 전산사업 계획 대비 지연사항에 대한 검토, 전산사업의 비용대비 효과 분석 등 의사결정이 필요한 중요사항이 전산운영위원회 안건에 포함되어 있지 않는 등 전산사업계획 및 수행 관리가 다소 미흡하므로

전산사업계획의 수립 및 이행 관리가 적절히 될 수 있도록 전산운영위원회 심의대상을 확대하고, 수립된 전산사업계획에 대한 사후관리를 강화할 필요가 있음

(2) 취약점 분석·평가 절차 관리 강화

전자금융기반시설 취약점 분석·평가를 연 1회 이상(홈페이지에는 6개월에 1회 이상) 실시하고 미흡사항에 대한 이행계획을 수립·시행하고 있으나

취약점 분석·평가 결과에 따라 보완조치 이행계획을 수립·시행하였음에도 동일한 취약점이 재발견 되는 등 보완조치가 적정하게 이루어지지 않고 있으며,

전자금융거래에 직접적으로 이용되지 않은 시스템을 취약점 분석·평가 대상에 포함하지 않아 동 시스템의 취약점을 통해 전자금융거래 관련 시스템이 악성코드 등에 감염될 우려가 있으므로

취약점 분석·평가시 전자금융거래에 직접적으로 이용되지 않은 시스템 등도 점검할 수 있도록 점검대상을 확대하고 취약점의 영향도를 분석하여 중대 취약점에 대해서는 즉시 조치하는 한편 조치가 적정하게 이루어졌는지 여부를 정기적으로 점검하는 등 관련 절차를 강화하여 이행할 필요가 있음

(3) 정보처리시스템 운영체제 관리 강화

서버, 네트워크, 보안 등 정보처리시스템의 긴급하고 중요한 패치작업에 대하여 시스템 작업 계획서를 사전 작성하여 패치를 실시하고 있으나 일부 보안패치 적용이 누락된 사례가 있고

일부 시스템에서 기술지원이 종료된 운영체제를 사용하고 있어 취약점 보완 및 기능개선 등을 위한 보정작업이 어려워 신규 취약점을 이용한 해킹 및 악성코드 등에 의한 침해 우려가 있으므로,

신규 취약점에 대한 보안패치 적용시 누락되는 정보처리시스템이 발생하지 않도록 사전에 보안패치 적용대상을 확인하는 등 보안패치 관련 관리·운영을 강화하고,

기술지원이 종료된 운영체제의 구체적인 전환 추진 계획을 수립하고 전환이 이루어지기 전까지 보안대책을 마련하여 이행하는 등 침해사고 발생 피해를 최소화 할 수 있도록 관련 시스템 보안대책을 마련할 필요가 있음

나. 개선사항

(1) IT감사업무 운용 미흡

감사부서는 매년 IT부문 종합감사를 수행하는 한편, IT부서 내 자체감사(이하 'IT 자체감사')를 수행하도록 부서내 IT 자체감사인을 지정하고 있으나,

감사부서가 IT부문 종합감사를 위해 사용하는 체크리스트에 전자금융거래 및 신용정보 관련법규 등의 준수 여부에 대한 점검항목이 일부 누락되어 있고, IT 자체감사를 위한 별도 내규가 마련되지 않아 IT 자체감사인이 실제로 IT 자체감사를 실시한 바 없는 등 관련 제도가 미흡한 수준이므로,

앞으로 IT부문 종합감사 시 관련 법규의 준수 여부를 확인할 수 있도록 체크리스트를 개선하고, 관련내규 마련 등을 통해 IT 자체감사 실시를 활성화하는 등 IT감사업무 운용을 개선할 필요가 있음

(2) IT업무 외부주문 관련 내부통제 미흡

회사는 모든 IT업무를 외주업체(㈜□□□□□)에 위탁·운영하고 ◇◇◇◇팀에서 외부주문에 대한 내부통제 업무를 수행하고 있으나, 다음과 같은 미흡사항에 대해 개선이 필요함

① 회사는 IT업무 외부주문과 관련하여 내규 「IT아웃소싱 업무 통제지침」을 제정·운영하고 있으나,

동 지침에는 외주업체에 대한 기본적인 통제절차만을 정하고 있고, 중요 IT업무 운영과 관련된 기준 등이 회사 자체 내규로 제정되어 있지 않아 외주업체가 수행하는 IT업무의 적정성 등을 점검하는데 어려움이 있으므로

앞으로 중요 IT업무에 대한 운영 기준을 회사 자체 내규 등으로 제정하고, 동 내규 등을 기반으로 외주업체가 수행하는 IT업무의 적정성을 정기적으로 점검하는 등 외부주문에 대한 통제를 강화할 필요가 있음

② 긴급 장애처리를 위해 외주업체 담당자가 가상의 전용회선(SSL VPN)을 통해 원격으로 내부시스템에 접속하여 작업을 수행하는 경우, 작업 수행 내역에 대한 사후 검토를 외주업체에서만 수행하고 회사 내부 담당자가 확인하지 않아 장애처리 이외에 인가받지 않은 작업을 수행할 우려가 있으므로

앞으로 외주업체의 원격 접속 관리를 통한 전산 변경작업 수행 시 회사 내부 담당자가 작업 수행 내용을 확인하는 절차를 마련할 필요가 있음

③ 외주업체 담당자가 테스트를 위한 고객정보 변환을 신청하거나 주민등록번호 등의 마스킹 처리된 고객정보 데이터의 마스킹 해제가 필요한 경우

내부 담당자의 확인 및 검토 없이 외주업체 책임자의 승인 하에 마스킹 해제 및 고객정보 열람이 가능하여 외주직원에 의해 고객정보가 유출될 우려가 있으므로

외주업체에서 고객정보 열람 업무 수행 시 회사 내부 담당자가 확인 및 검토하는 등 내부통제 관리를 강화할 필요가 있음

(3) 업무 연속성 확보방안 미흡

장애·재해 등 긴급한 상황이 발생하더라도 업무가 중단되지 않도록 내규 「위기대응행동매뉴얼」을 제·개정 하고, 매년 1회 이상 재해복구전환훈련을 수행하는 등 업무연속성 확보방안을 마련하고 있으나,

일부 핵심업무에 대해 재해복구센터에 서버만 구축하고 네트워크 통신망을 미구축하여, 주전산센터의 재해 발생시 재해복구센터에서 정상적으로 서비스가 수행되지 않을 우려가 있으며,

전산자료의 유출, 파괴 등을 방지하기 위하여 ◎◎◎◎, ◆◆◆◆ 등 중요 데이터에 대해 주기적으로 백업을 실시하고, ◍◍◍◍◍◍, ▧▧▧ ▧▧▧▧, ■■■■■ 등은 추가적으로 안전한 원격지(▦▦ ▦▦ IDC 내화금고)에 소산하고 있으나,

소산 대상에 ◎◎◎◎가 포함되어 있지 않아 해킹 등으로 인해 전체 데이터 유실시 관련 업무가 중단될 우려가 있으므로,

핵심업무에 대한 업무연속성이 확보될 수 있도록 재해복구센터를 개선·운영하고, ◎◎◎◎ 등 중요 데이터가 재해 등으로 인해 유실되지 않도록 소산절차를 강화할 필요가 있음

(4) 프로그램 테스트 및 변경통제 관리 미흡

내규「개발 및 응용보안 관리지침」에 따라 프로그램 개발을 수행하는 경우에는 응용프로그램을 실제 운영환경에 적용하기 전 충분한 테스트 과정을 거쳐야 함에도

검사대상기간 중 일부 응용프로그램(□□□□)을 개발하는 과정에서 개발(테스트)환경을 구축하지 않아 충분한 테스트를 수행하지 못한 사례가 있었고

변경 담당자가 개발된 프로그램을 수동으로 운영서버에 적용하던 중 조작 실수로 시스템 장애가 발생한 사실이 있으므로

전자금융거래 관련 시스템은 모두 개발(테스트)환경을 구축하여 운영환경에 적용하기 전에 충분한 테스트를 수행할 수 있도록 하고, 프로그램 등록·변경을 자동화된 방법으로 수행하여 프로그램 오류로 인한 장애발생을 최소화하는 등 예방대책을 마련할 필요가 있음